# Scan MMS DCP - Brivo Brispot -NEW -2 Scan Report

| | |
|---|---|
| Project Name | Scan MMS DCP - Brivo Brispot -NEW -2 |
| Scan Start | Wednesday, September 7, 2022 9:05:45 AM |
| Preset | Checkmarx Default |
| Scan Time | 05h:17m:43s |
| Lines Of Code Scanned | 1215797 |
| Files Scanned | 3557 |
| Report Creation Time | Thursday, September 8, 2022 10:56:05 AM |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881 |
| Team | Divisi APP |
| Checkmarx Version | 8.9.0.210 HF29 |
| Scan Type | Full |
| Source Origin | LocalPath |
| Density | 2/100 (Vulnerabilities/LOC) |
| Visibility | Public |

## Filter Settings

**Severity**

Included: High, Medium, Low, Information

Excluded: None

**Result State**

Included: Confirmed, Not Exploitable, To Verify, Urgent, Proposed Not Exploitable

Excluded: None

**Assigned to**

Included: All

**Categories**

Included:

| | |
|---|---|
| Uncategorized | All |
| Custom | All |
| PCI DSS v3.2 | All |
| OWASP Top 10 2013 | All |
| FISMA 2014 | All |
| NIST SP 800-53 | All |
| OWASP Top 10 2017 | All |
| OWASP Mobile Top 10 2016 | All |
| OWASP Top 10 API | All |
| OWASP Top 10 2021 | All |

Excluded:

| | |
|---|---|
| Uncategorized | None |
| Custom | None |
| PCI DSS v3.2 | None |

| | |
|---|---|
| OWASP Top 10 2013 | None |
| FISMA 2014 | None |
| NIST SP 800-53 | None |
| OWASP Top 10 2017 | None |
| OWASP Mobile Top 10 2016 | None |
| OWASP Top 10 API | None |
| OWASP Top 10 2021 | None |

**Results Limit**

Results limit per query was set to 50

**Selected Queries**

Selected queries are listed in Result Summary

## Result Summary

## Most Vulnerable Files

## Top 5 Vulnerabilities

# Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2017

| Category | Threat Agent | Exploitability | Weakness Prevalence | Weakness Detectability | Technical Impact | Business Impact | Issues Found | Best Fix Locations |
|---|---|---|---|---|---|---|---|---|
| A1-Injection* | App. Specific | EASY | COMMON | EASY | SEVERE | App. Specific | 2996 | 168 |
| A2-Broken Authentication | App. Specific | EASY | COMMON | AVERAGE | SEVERE | App. Specific | 208 | 78 |
| A3-Sensitive Data Exposure | App. Specific | AVERAGE | WIDESPREAD | AVERAGE | SEVERE | App. Specific | 313 | 146 |
| A4-XML External Entities (XXE) | App. Specific | AVERAGE | COMMON | EASY | SEVERE | App. Specific | 0 | 0 |
| A5-Broken Access Control* | App. Specific | AVERAGE | COMMON | AVERAGE | SEVERE | App. Specific | 3362 | 449 |
| A6-Security Misconfiguration | App. Specific | EASY | WIDESPREAD | EASY | MODERATE | App. Specific | 62 | 24 |
| A7-Cross-Site Scripting (XSS)* | App. Specific | EASY | WIDESPREAD | EASY | MODERATE | App. Specific | 8257 | 490 |
| A8-Insecure Deserialization | App. Specific | DIFFICULT | COMMON | AVERAGE | SEVERE | App. Specific | 0 | 0 |
| A9-Using Components with Known Vulnerabilities | App. Specific | AVERAGE | WIDESPREAD | AVERAGE | MODERATE | App. Specific | 1386 | 1386 |
| A10-Insufficient Logging & Monitoring | App. Specific | AVERAGE | WIDESPREAD | DIFFICULT | MODERATE | App. Specific | 0 | 0 |

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

# Scan Summary - OWASP Top 10 2021

| Category | Issues Found | Best Fix Locations |
|---|---|---|
| A1-Broken Access Control* | 2793 | 287 |
| A2-Cryptographic Failures | 208 | 122 |
| A3-Injection* | 10741 | 561 |
| A4-Insecure Design | 3191 | 539 |
| A5-Security Misconfiguration* | 14 | 14 |
| A6-Vulnerable and Outdated Components | 1348 | 1348 |
| A7-Identification and Authentication Failures* | 79 | 77 |
| A8-Software and Data Integrity Failures* | 40 | 25 |
| A9-Security Logging and Monitoring Failures | 0 | 0 |
| A10-Server-Side Request Forgery | 0 | 0 |

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

# Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2013

| Category | Threat Agent | Attack Vectors | Weakness Prevalence | Weakness Detectability | Technical Impact | Business Impact | Issues Found | Best Fix Locations |
|---|---|---|---|---|---|---|---|---|
| A1-Injection* | EXTERNAL, INTERNAL, ADMIN USERS | EASY | COMMON | AVERAGE | SEVERE | ALL DATA | 2378 | 34 |
| A2-Broken Authentication and Session Management | EXTERNAL, INTERNAL USERS | AVERAGE | WIDESPREAD | AVERAGE | SEVERE | AFFECTED DATA AND FUNCTIONS | 194 | 72 |
| A3-Cross-Site Scripting (XSS)* | EXTERNAL, INTERNAL, ADMIN USERS | AVERAGE | VERY WIDESPREAD | EASY | MODERATE | AFFECTED DATA AND SYSTEM | 8257 | 490 |
| A4-Insecure Direct Object References* | SYSTEM USERS | EASY | COMMON | EASY | MODERATE | EXPOSED DATA | 558 | 137 |
| A5-Security Misconfiguration | EXTERNAL, INTERNAL, ADMIN USERS | EASY | COMMON | EASY | MODERATE | ALL DATA AND SYSTEM | 51 | 14 |
| A6-Sensitive Data Exposure | EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS | DIFFICULT | UNCOMMON | AVERAGE | SEVERE | EXPOSED DATA | 221 | 103 |
| A7-Missing Function Level Access Control* | EXTERNAL, INTERNAL USERS | EASY | COMMON | AVERAGE | MODERATE | EXPOSED DATA AND FUNCTIONS | 0 | 0 |
| A8-Cross-Site Request Forgery (CSRF)* | USERS BROWSERS | AVERAGE | COMMON | EASY | MODERATE | AFFECTED DATA AND FUNCTIONS | 1589 | 2 |
| A9-Using Components with Known Vulnerabilities | EXTERNAL USERS, AUTOMATED TOOLS | AVERAGE | WIDESPREAD | DIFFICULT | MODERATE | AFFECTED DATA AND FUNCTIONS | 1348 | 1348 |
| A10-Unvalidated Redirects and Forwards | USERS BROWSERS | AVERAGE | WIDESPREAD | DIFFICULT | MODERATE | AFFECTED DATA AND FUNCTIONS | 6 | 2 |

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

# Scan Summary - PCI DSS v3.2

| Category | Issues Found | Best Fix Locations |
|---|---|---|
| PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection | 2467 | 64 |
| PCI DSS (3.2) - 6.5.2 - Buffer overflows | 0 | 0 |
| PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage | 402 | 194 |
| PCI DSS (3.2) - 6.5.4 - Insecure communications | 0 | 0 |
| PCI DSS (3.2) - 6.5.5 - Improper error handling* | 255 | 218 |
| PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS) | 8253 | 486 |
| PCI DSS (3.2) - 6.5.8 - Improper access control* | 7779 | 803 |
| PCI DSS (3.2) - 6.5.9 - Cross-site request forgery* | 1588 | 1 |
| PCI DSS (3.2) - 6.5.10 - Broken authentication and session management | 14 | 6 |

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

# Scan Summary - FISMA 2014

| Category | Description | Issues Found | Best Fix Locations |
|---|---|---|---|
| Access Control | Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. | 431 | 87 |
| Audit And Accountability* | Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. | 0 | 0 |
| Configuration Management | Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems. | 803 | 251 |
| Identification And Authentication | Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | 222 | 101 |
| Media Protection | Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse. | 171 | 43 |
| System And Communications Protection | Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems. | 9 | 9 |
| System And Information Integrity* | Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response. | 13479 | 1207 |

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

# Scan Summary - NIST SP 800-53

| Category | Issues Found | Best Fix Locations |
|---|---|---|
| AC-12 Session Termination (P2) | 0 | 0 |
| AC-3 Access Enforcement (P1) | 0 | 0 |
| AC-4 Information Flow Enforcement (P1) | 0 | 0 |
| AC-6 Least Privilege (P1) | 0 | 0 |
| AU-9 Protection of Audit Information (P1) | 0 | 0 |
| CM-6 Configuration Settings (P2) | 0 | 0 |
| IA-5 Authenticator Management (P1) | 0 | 0 |
| IA-6 Authenticator Feedback (P2) | 0 | 0 |
| IA-8 Identification and Authentication (Non-Organizational Users) (P1) | 0 | 0 |
| SC-12 Cryptographic Key Establishment and Management (P1) | 90 | 4 |
| SC-13 Cryptographic Protection (P1) | 80 | 80 |
| SC-17 Public Key Infrastructure Certificates (P1) | 0 | 0 |
| SC-18 Mobile Code (P2) | 4 | 4 |
| SC-23 Session Authenticity (P1)* | 1588 | 1 |
| SC-28 Protection of Information at Rest (P1) | 126 | 118 |
| SC-4 Information in Shared Resources (P1) | 51 | 19 |
| SC-5 Denial of Service Protection (P1)* | 206 | 205 |
| SC-8 Transmission Confidentiality and Integrity (P1) | 134 | 12 |
| SI-10 Information Input Validation (P1)* | 6329 | 965 |
| SI-11 Error Handling (P2)* | 51 | 14 |
| SI-15 Information Output Filtering (P0)* | 8253 | 486 |
| SI-16 Memory Protection (P1) | 0 | 0 |

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

# Scan Summary - OWASP Mobile Top 10 2016

| Category | Description | Issues Found | Best Fix Locations |
|---|---|---|---|
| M1-Improper Platform Usage | This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk. | 0 | 0 |
| M2-Insecure Data Storage* | This category covers insecure data storage and unintended data leakage. | 0 | 0 |
| M3-Insecure Communication | This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc. | 0 | 0 |
| M4-Insecure Authentication | This category captures notions of authenticating the end user or bad session management. This can include:<br>-Failing to identify the user at all when that should be required<br>-Failure to maintain the user's identity when it is required<br>-Weaknesses in session management | 0 | 0 |
| M5-Insufficient Cryptography | The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly. | 0 | 0 |
| M6-Insecure Authorization | This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.).<br>If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure. | 0 | 0 |
| M7-Client Code Quality* | This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device. | 0 | 0 |
| M8-Code Tampering* | This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or | 0 | 0 |

| | | | |
|---|---|---|---|
| | modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain. | | |
| M9-Reverse Engineering | This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property. | 0 | 0 |
| M10-Extraneous Functionality | Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing. | 0 | 0 |

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

# Scan Summary - OWASP Top 10 API

| Category | Issues Found | Best Fix Locations |
|---|---|---|
| API1-Broken Object Level Authorization | 0 | 0 |
| API2-Broken Authentication | 0 | 0 |
| API3-Excessive Data Exposure | 0 | 0 |
| API4-Lack of Resources and Rate Limiting | 0 | 0 |
| API5-Broken Function Level Authorization | 0 | 0 |
| API6-Mass Assignment | 0 | 0 |
| API7-Security Misconfiguration* | 0 | 0 |
| API8-Injection | 0 | 0 |
| API9-Improper Assets Management | 0 | 0 |
| API10-Insufficient Logging and Monitoring | 0 | 0 |

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

# Scan Summary - Custom

| Category | Issues Found | Best Fix Locations |
|---|---|---|
| Must audit | 0 | 0 |
| Check | 0 | 0 |
| Optional | 0 | 0 |

## Results Distribution By Status First scan of the project

| | High | Medium | Low | Information | Total |
|---|---|---|---|---|---|
| New Issues | 10,462 | 5,641 | 7,072 | 16 | 23,191 |
| Recurrent Issues | 0 | 0 | 0 | 0 | 0 |
| Total | 10,462 | 5,641 | 7,072 | 16 | 23,191 |
| | | | | | |
| Fixed Issues | 0 | 0 | 0 | 0 | 0 |

## Results Distribution By State

| | High | Medium | Low | Information | Total |
|---|---|---|---|---|---|
| Confirmed | 0 | 0 | 35 | 2 | 37 |
| Not Exploitable | 2 | 11 | 0 | 0 | 13 |
| To Verify | 10,458 | 5,641 | 7,037 | 14 | 23,150 |
| Urgent | 0 | 0 | 0 | 0 | 0 |
| Proposed Not Exploitable | 4 | 0 | 0 | 0 | 4 |
| Total | 10,464 | 5,652 | 7,072 | 16 | 23,204 |

## Result Summary

| Vulnerability Type | Occurrences | Severity |
|---|---|---|
| Stored XSS | 4740 | High |
| Reflected XSS All Clients | 3082 | High |
| SQL Injection | 1804 | High |
| Second Order SQL Injection | 378 | High |
| File Manipulation | 264 | High |

| | | |
|---|---|---|
| File Disclosure | 85 | High |
| Command Injection | 73 | High |
| Code Injection | 38 | High |
| Trust Boundary Violation | 2804 | Medium |
| XSRF | 1588 | Medium |
| Path Traversal | 558 | Medium |
| Stored File Manipulation | 234 | Medium |
| Use of Hard coded Cryptographic Key | 90 | Medium |
| Header Injection | 89 | Medium |
| Stored Code Injection | 70 | Medium |
| Privacy Violation | 51 | Medium |
| Insecure Randomness | 48 | Medium |
| Client Use Of JQuery Outdated Version | 23 | Medium |
| Client Use Of JQuery Outdated Version | 23 | Medium |
| HTTP Response Splitting | 20 | Medium |
| Deserialization of Untrusted Data | 13 | Medium |
| Stored XPath Injection | 13 | Medium |
| Inappropriate Encoding for Output Context | 8 | Medium |
| Reflected File Download | 7 | Medium |
| HttpOnlyCookies | 4 | Medium |
| Client Potential XSS | 3 | Medium |
| Client Reflected File Download | 2 | Medium |
| Cross Site History Manipulation | 2 | Medium |
| Client Potential Code Injection | 1 | Medium |
| Object Injection | 1 | Medium |
| Possible Flow Control | 4018 | Low |
| Client JQuery Deprecated Symbols | 1325 | Low |
| XSS Evasion Attack | 428 | Low |
| Unsafe Use Of Target blank | 267 | Low |
| Unsafe Use Of Target blank | 267 | Low |
| Improper Exception Handling | 204 | Low |
| Unsafe Use Of Target Blank | 184 | Low |
| Insufficiently Protected Credentials | 124 | Low |
| Use of Broken or Risky Cryptographic Algorithm | 80 | Low |
| Use Of Hardcoded Password | 70 | Low |
| Information Exposure Through an Error Message | 51 | Low |
| Reliance on Cookies in a Decision | 14 | Low |
| Unprotected Cookie | 9 | Low |
| Use Of Hardcoded Password | 9 | Low |
| Hardcoded Absolute Path | 8 | Low |
| Client DOM Open Redirect | 4 | Low |
| Client Use Of Iframe Without Sandbox | 3 | Low |
| Client Potential DOM Open Redirect | 2 | Low |
| Client Potential ReDoS In Match | 2 | Low |
| Client Hardcoded Domain | 1 | Low |
| Client Insufficient ClickJacking Protection | 1 | Low |
| Client Overly Permissive Message Posting | 1 | Low |
| Possible Global Variable Overwrite | 16 | Information |

# 10 Most Vulnerable Files

## High and Medium Vulnerabilities

| File Name | Issues Found |
|---|---|
| system/core/Input.php | 6528 |
| system/database/DB_driver.php | 3999 |
| system/database/drivers/oci8/oci8_result.php | 2174 |
| application/models/maintenance_model.php | 860 |
| application/models/maintenance_model_20190610.php | 574 |
| application/models/interface_scheduler_model.php | 544 |
| application/models/chargeback_model.php | 385 |
| BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php | 278 |
| application/controllers/maintenance.php | 278 |
| application/controllers/maintenance_20190524.php | 252 |

# Scan Results Details

## Stored XSS

Query Path:
PHP\Cx\PHP High Risk\Stored XSS Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
OWASP Top 10 2021: A3-Injection

*Description*

**Stored XSS\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2643 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method patching_tid at line 806 of BACKUP_DEPLOY_FMS_20210407/models/models/aplikasi_daftar_model_backup20171221.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/models/models/aplikasi_daftar_model_backup20171221.php |
| Line | 155 | 837 |
| Object | oci_fetch_assoc | print_r |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/models/models/aplikasi_daftar_model_backup20171221.php
Method public function patching_tid($app_id){

```
....
837.                print_r($mid_temp);
```

**Stored XSS\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2644 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method deploy_mid at line 44 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_super_script.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_super_script.php |
| Line | 155 | 60 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_super_script.php

Method public function deploy_mid()

```
....
60.                 echo 'Jumlah Grup Merchant: '.$jml_prefix.'<br>';
```

**Stored XSS\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2645 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method deploy_mid at line 44 of application/controllers/admin_super_script.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/admin_super_script.php |
| Line | 155 | 60 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/admin_super_script.php

Method public function deploy_mid()

```
....
60.             echo 'Jumlah Grup Merchant: '.$jml_prefix.'<br>';
```

**Stored XSS\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2646 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method delete_uploads at line 164 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_temp.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_temp.php |
| Line | 155 | 229 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_temp.php

Method public function delete_uploads($maxdate)

```
....
229.            echo "TOTAL INISIASI: {$list_init->num_rows()}<br>";
```

**Stored XSS\Path 5:**

| | |
|---|---|
| Severity | High |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2647 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method delete_uploads at line 164 of application/controllers/script_temp.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/script_temp.php |
| Line | 155 | 229 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/script_temp.php

Method public function delete_uploads($maxdate)

```
....
229.            echo "TOTAL INISIASI: {$list_init->num_rows()}<br>";
```

**Stored XSS\Path 6:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2648 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1268 of application/controllers/maintenance.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance.php |
| Line | 155 | 1280 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance.php

Method function get_pemasang()

```
....
1280.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 7:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2649 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1221 of application/controllers/maintenance_20181213.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_20181213.php |
| Line | 155 | 1233 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_20181213.php

Method function get_pemasang()

```
....
1233.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 8:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=2650 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1237 of application/controllers/maintenance_20190524.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_20190524.php |
| Line | 155 | 1249 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_20190524.php

Method function get_pemasang()

```
....
1249.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 9:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2651 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1237 of application/controllers/maintenance_20190610.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_20190610.php |
| Line | 155 | 1249 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_20190610.php

Method function get_pemasang()

```
....
1249.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 10:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2652 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1135 of application/controllers/maintenance_bck07112017.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_bck07112017.php |
| Line | 155 | 1147 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_bck07112017.php

Method function get_pemasang()

```
....
1147.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 11:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2653 |

| | |
|---|---|
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1221 of application/controllers/maintenance_bck20180906.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_bck20180906.php |
| Line | 155 | 1233 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_bck20180906.php

Method function get_pemasang()

```
....
1233.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 12:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2654 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1235 of application/controllers/maintenance_bck20190114.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_bck20190114.php |
| Line | 155 | 1247 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_bck20190114.php

Method function get_pemasang()

```
....
1247.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 13:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2655 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1268 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php |
| Line | 155 | 1280 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php

Method function get_pemasang()

```
....
1280.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 14:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=2656 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1221 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php |
| Line | 155 | 1233 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php

Method function get_pemasang()

```
....
1233.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 15:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2657 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1237 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php |
| Line | 155 | 1249 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php
Method function get_pemasang()

```
....
1249.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 16:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2658 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1237 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php |
| Line | 155 | 1249 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php
Method function get_pemasang()

```
....
1249.             echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 17:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2659 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1135 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php |
| Line | 155 | 1147 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php

Method function get_pemasang()

```
....
1147.             echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 18:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2660 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1221 of

BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php |
| Line | 155 | 1233 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php

Method function get_pemasang()

```
....
1233.               echo form_dropdown('kode_pemasang', $opt_pemasang,
$kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 19:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2661 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method get_pemasang at line 1235 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php |
| Line | 155 | 1247 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php

Method function get_pemasang()

```
....
1247.               echo form_dropdown('kode_pemasang', $opt_pemasang, $kode_pemasang, 'id="kode_pemasang" class="required"');
```

**Stored XSS\Path 20:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2662 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method syncron_to_detail at line 171 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler_msrp_param.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler_msrp_param.php |
| Line | 155 | 187 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler_msrp_param.php

Method private function syncron_to_detail($isi, $tabel_detail, $kolom_detail, $tahun)

```
....
187.                echo date('Y-m-d H:i:s')."| FINISH SYNCRONIZED DATA {$tabel_detail} ON {$kolom_detail} ID {$isi->id} : ".$total_updated." DATA <br>".PHP_EOL;
```

**Stored XSS\Path 21:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2663 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method syncron_to_detail at line 171 of application/controllers/scheduler_msrp_param.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/scheduler_msrp_param.php |
| Line | 155 | 187 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/scheduler_msrp_param.php

Method private function syncron_to_detail($isi, $tabel_detail, $kolom_detail, $tahun)

```
....
187.                echo date('Y-m-d H:i:s')."| FINISH SYNCRONIZED DATA
{$tabel_detail} ON {$kolom_detail} ID {$isi->id} : ".$total_updated."
DATA <br>".PHP_EOL;
```

**Stored XSS\Path 22:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2664 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method syncron_to_detail at line 171 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler_msrp_param.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler_msrp_param.php |
| Line | 155 | 173 |

| | | |
|---|---|---|
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler_msrp_param.php
Method private function syncron_to_detail($isi, $tabel_detail, $kolom_detail, $tahun)

```
....
173.            echo date('Y-m-d H:i:s')."| STARTING SYNCRONIZED DATA
{$tabel_detail} ON {$kolom_detail} ID {$isi->id} <br>".PHP_EOL;
```

**Stored XSS\Path 23:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2665 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method syncron_to_detail at line 171 of application/controllers/scheduler_msrp_param.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/scheduler_msrp_param.php |
| Line | 155 | 173 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/scheduler_msrp_param.php
Method private function syncron_to_detail($isi, $tabel_detail, $kolom_detail, $tahun)

```
....
173.                echo date('Y-m-d H:i:s')."| STARTING SYNCRONIZED DATA
{$tabel_detail} ON {$kolom_detail} ID {$isi->id} <br>".PHP_EOL;
```

**Stored XSS\Path 24:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2666 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method delete_pengajuan_merchant at line 483 of application/controllers/script_migrasi.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/script_migrasi.php |
| Line | 155 | 513 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/script_migrasi.php

Method function delete_pengajuan_merchant()

```
....
513.                            echo $str.'<br>'.PHP_EOL;
```

**Stored XSS\Path 25:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2667 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method save_reasoncode at line 168 of application/controllers/chargeback.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_resul | application/controllers/chargeback.php |

| | | |
|---|---|---|
| | t.php | |
| Line | 155 | 180 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/chargeback.php
Method function save_reasoncode()

```
....
180.            echo $res;
```

**Stored XSS\Path 26:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2668 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method save_reasoncode at line 170 of BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php |
| Line | 155 | 182 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php
Method function save_reasoncode()

```
....
182.                echo $res;
```

**Stored XSS\Path 27:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2669 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method save_reasoncode at line 170 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php |
| Line | 155 | 182 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php

Method function save_reasoncode()

```
....
182.                echo $res;
```

**Stored XSS\Path 28:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2670 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method delete_reasoncode at line 182 of application/controllers/chargeback.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_resul | application/controllers/chargeback.php |

| | | |
|---|---|---|
| | t.php | |
| Line | 155 | 188 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/chargeback.php

Method function delete_reasoncode()

```
....
188.                echo $this->chargeback_model-
>delete_reasoncode($data);
```

**Stored XSS\Path 29:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2671 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method delete_reasoncode at line 184 of BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php |
| Line | 155 | 190 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php

| | |
|---|---|
| Method | function delete_reasoncode() |

```
....
190.                echo $this->chargeback_model-
>delete_reasoncode($data);
```

**Stored XSS\Path 30:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2672 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method delete_reasoncode at line 184 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php |
| Line | 155 | 190 |
| Object | oci_fetch_assoc | echo |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php |
| Method | function delete_reasoncode() |

```
....
190.                echo $this->chargeback_model-
>delete_reasoncode($data);
```

**Stored XSS\Path 31:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2673 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of

BACKUP_DEPLOY_FMS_20210407/controllers/controllers/Qris_mms.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/Qris_mms.php |
| Line | 155 | 81 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/Qris_mms.php
Method function send_to_qris(){

```
....
81.                     echo "TID ".$tid." not found. ";
```

**Stored XSS\Path 32:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2674
Status New

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms.php |
| Line | 155 | 92 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | application/controllers/Qris_mms.php |
| Method | function send_to_qris(){ |

```
....
92.                                         echo "Update MPAN Gagal.
Message : " . $update_mpan['response'];
```

**Stored XSS\Path 33:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2675 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms.php |
| Line | 155 | 144 |
| Object | oci_fetch_assoc | echo |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.              return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | application/controllers/Qris_mms.php |
| Method | function send_to_qris(){ |

```
....
144.                          echo "TID ".$tid." not found. ";
```

**Stored XSS\Path 34:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2676 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms.php |
| Line | 155 | 78 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/Qris_mms.php
Method function send_to_qris(){

```
....
78.                                 echo "SUCCESS - " . $out_api-
>response_desc . "<br>";
```

**Stored XSS\Path 35:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2677 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms.php |
| Line | 155 | 105 |
| Object | oci_fetch_assoc | print |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/Qris_mms.php

| | |
|---|---|
| Method | function send_to_qris(){ |

```
....
105.
      print("<pre>".print_r($out_api->response_data, true)."</pre>");
```

**Stored XSS\Path 36:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2678 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms.php |
| Line | 155 | 104 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name application/controllers/Qris_mms.php

Method function send_to_qris(){

```
....
104.                                    echo "[QRIS-MMS] : FAILED -
".$out_api->response_desc."<br>";
```

**Stored XSS\Path 37:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2679 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms.php |
| Line | 155 | 103 |
| Object | oci_fetch_assoc | print |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name application/controllers/Qris_mms.php
Method function send_to_qris(){

```
....
103.
      print("<pre>".print_r($out_api, true)."</pre>");
```

**Stored XSS\Path 38:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2680 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms_backdate.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms_backdate.php |
| Line | 155 | 93 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name application/controllers/Qris_mms_backdate.php

| | |
|---|---|
| Method | function send_to_qris($backdate){ |

```
....
93.                                         echo "Update MPAN Gagal.
Message : " . $update_mpan['response'];
```

**Stored XSS\Path 39:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2681 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms_backdate.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms_backdate.php |
| Line | 155 | 145 |
| Object | oci_fetch_assoc | echo |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.              return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | application/controllers/Qris_mms_backdate.php |
| Method | function send_to_qris($backdate){ |

```
....
145.                          echo "TID ".$tid." not found. ";
```

**Stored XSS\Path 40:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2682 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms_backdate.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms_backdate.php |
| Line | 155 | 79 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/Qris_mms_backdate.php
Method function send_to_qris($backdate){

```
....
79.                                 echo "SUCCESS - " . $out_api->response_desc . "<br>";
```

**Stored XSS\Path 41:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2683 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms_backdate.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms_backdate.php |
| Line | 155 | 106 |
| Object | oci_fetch_assoc | print |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/Qris_mms_backdate.php
Method function send_to_qris($backdate){

```
....
106.
      print("<pre>".print_r($out_api->response_data, true)."</pre>");
```

**Stored XSS\Path 42:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2684 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms_backdate.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms_backdate.php |
| Line | 155 | 105 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name application/controllers/Qris_mms_backdate.php

Method function send_to_qris($backdate){

```
....
105.                                    echo "[QRIS-MMS] : FAILED -
".$out_api->response_desc."<br>";
```

**Stored XSS\Path 43:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2685 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of application/controllers/Qris_mms_backdate.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/Qris_mms_backdate.php |
| Line | 155 | 104 |
| Object | oci_fetch_assoc | print |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name application/controllers/Qris_mms_backdate.php
Method function send_to_qris($backdate){

```
....
104.
      print("<pre>".print_r($out_api, true)."</pre>");
```

**Stored XSS\Path 44:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2686 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method send_to_qris at line 12 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/Qris_mms_backdate.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/Qris_mms_backdate.php |
| Line | 155 | 81 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/Qris_mms_backdate.php

| | |
|---|---|
| Method | function send_to_qris($backdate){ |

```
....
81.                     echo "TID ".$tid." not found. ";
```

**Stored XSS\Path 45:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2687 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method main at line 25 of application/controllers/dashboard_settlement.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/dashboard_settlement.php |
| Line | 155 | 115 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name application/controllers/dashboard_settlement.php

Method public function main()

```
....
115.                          echo array_to_csv($csv_array,
"Dashboard_Settlement_".date('Ymd').".csv", ";");
```

**Stored XSS\Path 46:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2688 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method update_signer_settle_debit at line 452 of application/controllers/dashboard_settlement.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/dashboard_settlement.php |
| Line | 155 | 561 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/dashboard_settlement.php
Method public function update_signer_settle_debit(){

```
....
561.                                        echo '0|Push settle gagal
'.$msg_aksi.'. Gagal settle : '.$msg_settle.'.';
```

**Stored XSS\Path 47:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2689 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method main at line 25 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard_settlement.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard_settlement.php |
| Line | 155 | 115 |
| Object | oci_fetch_assoc | echo |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard_settlement.php |
| Method | public function main() |

```
....
115.                            echo array_to_csv($csv_array,
"Dashboard_Settlement_".date('Ymd').".csv", ";");
```

**Stored XSS\Path 48:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2690 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method update_signer_settle_debit at line 452 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard_settlement.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard_settlement.php |
| Line | 155 | 561 |
| Object | oci_fetch_assoc | echo |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.              return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard_settlement.php |
| Method | public function update_signer_settle_debit(){ |

```
....
561.                                    echo '0|Push settle gagal
'.$msg_aksi.'. Gagal settle : '.$msg_settle.'.';
```

**Stored XSS\Path 49:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2691 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method daily_update_msrp_merchant at line 14 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/msrp_scheduler.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/msrp_scheduler.php |
| Line | 155 | 23 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/msrp_scheduler.php

Method function daily_update_msrp_merchant()

```
....
23.          echo "Inserted MSRP Data : ".$insert_msrp."<br>";
```

**Stored XSS\Path 50:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2692 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets data from the database, for the oci_fetch_assoc element. This element's value then flows through the code without being properly filtered or encoded and is eventually displayed to the user in method daily_update_msrp_merchant at line 14 of application/controllers/msrp_scheduler.php. This may enable a Stored Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/msrp_scheduler.php |
| Line | 155 | 23 |
| Object | oci_fetch_assoc | echo |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/msrp_scheduler.php

Method function daily_update_msrp_merchant()

```
....
23.          echo "Inserted MSRP Data : ".$insert_msrp."<br>";
```

## Reflected XSS All Clients

Query Path:
PHP\Cx\PHP High Risk\Reflected XSS All Clients Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
OWASP Top 10 2021: A3-Injection

*Description*

**Reflected XSS All Clients\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7385 |
| Status | New |

Method <?php at line 1 of application/third_party/dompdf/dompdf.php gets user input for the _GET element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <?php at line 1 of application/third_party/dompdf/dompdf.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 202 | 260 |
| Object | _GET | echo |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
202.      $paper = rawurldecode($_GET["paper"]);
....
260.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**Reflected XSS All Clients\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7386 |
| Status | New |

Method <?php at line 1 of application/third_party/dompdf/dompdf.php gets user input for the _GET element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <?php at line 1 of application/third_party/dompdf/dompdf.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 207 | 260 |
| Object | _GET | echo |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
207.      $orientation = rawurldecode($_GET["orientation"]);
....
260.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**Reflected XSS All Clients\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7387 |
| Status | New |

Method <?php at line 1 of application/third_party/dompdf/dompdf.php gets user input for the _GET element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <?php at line 1 of application/third_party/dompdf/dompdf.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 212 | 260 |
| Object | _GET | echo |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
212.      $base_path = rawurldecode($_GET["base_path"]);
....
260.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**Reflected XSS All Clients\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7388 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/dompdf.php gets user input for the _GET element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <?php at line 1 of system/helpers/dompdf/dompdf.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 203 | 261 |
| Object | _GET | echo |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
203.      $paper = rawurldecode($_GET["paper"]);
....
261.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**Reflected XSS All Clients\Path 5:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7389 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/dompdf.php gets user input for the _GET element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <?php at line 1 of system/helpers/dompdf/dompdf.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 208 | 261 |
| Object | _GET | echo |

Code Snippet
File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
208.      $orientation = rawurldecode($_GET["orientation"]);
....
261.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**Reflected XSS All Clients\Path 6:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7390 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/dompdf.php gets user input for the _GET element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <?php at line 1 of system/helpers/dompdf/dompdf.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 213 | 261 |
| Object | _GET | echo |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
213.      $base_path = rawurldecode($_GET["base_path"]);
....
261.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**Reflected XSS All Clients\Path 7:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7391 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/www/controller.php gets user input for the _POST element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <?php at line 1 of system/helpers/dompdf/www/controller.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/controller.php | system/helpers/dompdf/www/controller.php |
| Line | 21 | 70 |
| Object | _POST | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | system/helpers/dompdf/www/controller.php |
| Method | <?php |

```
....
21.      $family = $_POST["family"];
....
70.          echo "The <strong>$family $weight $style</strong> font was
successfully installed !<br />";
```

**Reflected XSS All Clients\Path 8:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7392 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/www/controller.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <?php at line 1 of system/helpers/dompdf/www/controller.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/controller.php | system/helpers/dompdf/www/controller.php |
| Line | 22 | 67 |
| Object | _FILES | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | system/helpers/dompdf/www/controller.php |
| Method | <?php |

```
....
22.      $data = $_FILES["file"];
....
67.          echo $data["name"][$name]." is not a valid font file";
```

**Reflected XSS All Clients\Path 9:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7393 |
| Status | New |

Method upload at line 547 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |

| | | |
|---|---|---|
| Line | 558 | 590 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
558.                    $config['file_name'] = $app_id . '_' .
date('Ymd_His') . '.' . (end(explode(".", $_FILES['foto']['name'])));
....
590.                          echo $label;
```

**Reflected XSS All Clients\Path 10:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7394 |
| Status | New |

Method upload at line 547 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 558 | 583 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
558.                    $config['file_name'] = $app_id . '_' .
date('Ymd_His') . '.' . (end(explode(".", $_FILES['foto']['name'])));
....
583.                          echo $tr_append;
```

**Reflected XSS All Clients\Path 11:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7395 |
| Status | New |

Method upload at line 547 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 562 | 590 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
562.                    $config['file_name'] = $app_id . '_' . $name .
'.' . (end(explode(".", $_FILES['foto']['name'])));
....
590.                          echo $label;
```

**Reflected XSS All Clients\Path 12:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7396 |
| Status | New |

Method upload at line 547 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 562 | 583 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
562.                    $config['file_name'] = $app_id . '_' . $name .
'.' . (end(explode(".", $_FILES['foto']['name'])));
....
583.                          echo $tr_append;
```

**Reflected XSS All Clients\Path 13:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7397 |
| Status | New |

Method upload at line 547 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 566 | 590 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
566.                    $config['file_name'] = $app_id . '_' . $name .
'.' . (end(explode(".", $_FILES['foto']['name'])));
....
590.                          echo $label;
```

**Reflected XSS All Clients\Path 14:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7398
Status New

Method upload at line 547 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 566 | 583 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
566.                    $config['file_name'] = $app_id . '_' . $name .
'.' . (end(explode(".", $_FILES['foto']['name'])));
....
583.                          echo $tr_append;
```

**Reflected XSS All Clients\Path 15:**

Severity High
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7399 |
| Status | New |

Method upload at line 547 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 578 | 583 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
578.                            $tr_append .= '<td><a href="' .
$lihat_path . '" class="foto">' . $_FILES['foto']['name'] . '</a>';
....
583.                            echo $tr_append;
```

**Reflected XSS All Clients\Path 16:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7400 |
| Status | New |

Method upload at line 547 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 587 | 590 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
587.                            $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
590.                            echo $label;
```

**Reflected XSS All Clients\Path 17:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7401 |
| Status | New |

Method upload_new at line 1197 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 1197 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 1209 | 1225 |
| Object | _FILES | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/aplikasi_merchant.php |
| Method | public function upload_new() { |

```
....
1209.                    $config['file_name'] = $app_id . '_' . $this-
>util->generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
1225.                    echo $label;
```

**Reflected XSS All Clients\Path 18:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7402 |
| Status | New |

Method upload_new at line 1197 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 1197 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 1213 | 1225 |
| Object | _FILES | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/aplikasi_merchant.php |
| Method | public function upload_new() { |

```
....
1213.                    $config['file_name'] = $app_id . '_' . $this-
>util->generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
1225.                    echo $label;
```

**Reflected XSS All Clients\Path 19:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7403 |
| Status | New |

Method upload_new at line 1197 of application/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 1197 of application/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 1222 | 1225 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function upload_new() {

```
....
1222.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
1225.                    echo $label;
```

**Reflected XSS All Clients\Path 20:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7404 |
| Status | New |

Method upload_new at line 100 of application/controllers/aplikasi_tambah_merchant/analisa.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 100 of application/controllers/aplikasi_tambah_merchant/analisa.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/analisa.php | application/controllers/aplikasi_tambah_merchant/analisa.php |
| Line | 111 | 122 |

| | | |
|---|---|---|
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/analisa.php
Method public function upload_new() {

```
....
111.                $config['file_name'] = $app_id . '_' . $this->util-
>generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
122.                    echo $label;
```

**Reflected XSS All Clients\Path 21:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7405 |
| Status | New |

Method upload_new at line 100 of application/controllers/aplikasi_tambah_merchant/analisa.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 100 of application/controllers/aplikasi_tambah_merchant/analisa.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/analisa.php | application/controllers/aplikasi_tambah_merchant/analisa.php |
| Line | 119 | 122 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/analisa.php
Method public function upload_new() {

```
....
119.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
122.                    echo $label;
```

**Reflected XSS All Clients\Path 22:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7406 |
| Status | New |

Method upload_new at line 643 of application/controllers/aplikasi_tambah_merchant/input_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 643 of application/controllers/aplikasi_tambah_merchant/input_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 655 | 666 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php
Method public function upload_new() {

```
....
655.                $config['file_name'] = $app_id . '_' . $this->util-
>generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
666.                    echo $label;
```

**Reflected XSS All Clients\Path 23:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7407 |
| Status | New |

Method upload_new at line 643 of application/controllers/aplikasi_tambah_merchant/input_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 643 of application/controllers/aplikasi_tambah_merchant/input_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 663 | 666 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php
Method public function upload_new() {

```
....
663.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
666.                    echo $label;
```

**Reflected XSS All Clients\Path 24:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7408 |

| | |
|---|---|
| Status | New |

Method upload_new at line 626 of application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 626 of application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php |
| Line | 638 | 649 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php
Method public function upload_new() {

```
....
638.                $config['file_name'] = $app_id . '_' . $this->util-
>generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
649.                    echo $label;
```

**Reflected XSS All Clients\Path 25:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7409 |
| Status | New |

Method upload_new at line 626 of application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 626 of application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php |
| Line | 646 | 649 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php

| | |
|---|---|
| Method | public function upload_new() { |

```
....
646.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
649.                    echo $label;
```

**Reflected XSS All Clients\Path 26:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7410 |
| Status | New |

Method upload_new at line 933 of application/controllers/pameran.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 933 of application/controllers/pameran.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/pameran.php | application/controllers/pameran.php |
| Line | 944 | 955 |
| Object | _FILES | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/pameran.php |
| Method | public function upload_new() { |

```
....
944.              $config['file_name'] = $app_id . '_' . $this->util-
>generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
955.                    echo $label;
```

**Reflected XSS All Clients\Path 27:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7411 |
| Status | New |

Method upload_new at line 933 of application/controllers/pameran.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 933 of application/controllers/pameran.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/pameran.php | application/controllers/pameran.php |
| Line | 952 | 955 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/pameran.php
Method public function upload_new() {

```
....
952.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
955.                    echo $label;
```

**Reflected XSS All Clients\Path 28:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7412 |
| Status | New |

Method upload_new at line 755 of application/controllers/qris.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 755 of application/controllers/qris.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/qris.php | application/controllers/qris.php |
| Line | 765 | 776 |
| Object | _FILES | echo |

Code Snippet
File Name application/controllers/qris.php
Method public function upload_new() {

```
....
765.              $config['file_name']            = $app_id . '_' .
$this->util->generateRandomString(5) . '_' . $name . '.' .
(end(explode(".", $_FILES['foto']['name'])));
....
776.                    echo $label;
```

**Reflected XSS All Clients\Path 29:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7413 |
| Status | New |

Method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php |
| Line | 558 | 590 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
558.                    $config['file_name'] = $app_id . '_' .
date('Ymd_His') . '.' . (end(explode(".", $_FILES['foto']['name'])));
....
590.                          echo $label;
```

**Reflected XSS All Clients\Path 30:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7414 |
| Status | New |

Method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php |
| Line | 558 | 583 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
558.                    $config['file_name'] = $app_id . '_' .
date('Ymd_His') . '.' . (end(explode(".", $_FILES['foto']['name'])));
....
583.                          echo $tr_append;
```

**Reflected XSS All Clients\Path 31:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7415 |

| | |
|---|---|
| Status | New |

Method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php |
| Line | 562 | 590 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
562.                    $config['file_name'] = $app_id . '_' . $name .
'.' . (end(explode(".", $_FILES['foto']['name'])));
....
590.                          echo $label;
```

**Reflected XSS All Clients\Path 32:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7416 |
| Status | New |

Method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php |
| Line | 562 | 583 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
562.                    $config['file_name'] = $app_id . '_' . $name .
'.' . (end(explode(".", $_FILES['foto']['name'])));
....
583.                          echo $tr_append;
```

**Reflected XSS All Clients\Path 33:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7417 |
| Status | New |

Method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php |
| Line | 566 | 590 |
| Object | _FILES | echo |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php

Method public function upload() {

```
....
566.                    $config['file_name'] = $app_id . '_' . $name .
'.' . (end(explode(".", $_FILES['foto']['name'])));
....
590.                          echo $label;
```

**Reflected XSS All Clients\Path 34:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7418 |
| Status | New |

Method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/contro | BACKUP_DEPLOY_FMS_20210407/contro |

| | | |
|---|---|---|
| | llers/controllers/aplikasi_merchant.php | llers/controllers/aplikasi_merchant.php |
| Line | 566 | 583 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
566.                    $config['file_name'] = $app_id . '_' . $name .
'.' . (end(explode(".", $_FILES['foto']['name'])));
....
583.                          echo $tr_append;
```

**Reflected XSS All Clients\Path 35:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7419 |
| Status | New |

Method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php |
| Line | 578 | 583 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
578.                          $tr_append .= '<td><a href="' .
$lihat_path . '" class="foto">' . $_FILES['foto']['name'] . '</a>';
....
583.                          echo $tr_append;
```

**Reflected XSS All Clients\Path 36:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7420 |
| Status | New |

Method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload at line 547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php |
| Line | 587 | 590 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php
Method public function upload() {

```
....
587.                            $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
590.                            echo $label;
```

**Reflected XSS All Clients\Path 37:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7421 |
| Status | New |

Method upload_new at line 1197 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 1197 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php |
| Line | 1209 | 1225 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php
Method public function upload_new() {

```
....
1209.                    $config['file_name'] = $app_id . '_' . $this-
>util->generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
1225.                    echo $label;
```

**Reflected XSS All Clients\Path 38:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7422 |
| Status | New |

Method upload_new at line 1197 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 1197 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php |
| Line | 1213 | 1225 |
| Object | _FILES | echo |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php

Method public function upload_new() {

```
....
1213.                    $config['file_name'] = $app_id . '_' . $this-
>util->generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
1225.                    echo $label;
```

**Reflected XSS All Clients\Path 39:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7423 |
| Status | New |

Method upload_new at line 1197 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 1197 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php |
| Line | 1222 | 1225 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_merchant.php
Method public function upload_new() {

```
....
1222.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
1225.                    echo $label;
```

**Reflected XSS All Clients\Path 40:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7424
Status New

Method upload_new at line 100 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/analisa.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 100 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/analisa.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/analisa.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/analisa.php |
| Line | 111 | 122 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/analisa.php
Method public function upload_new() {

```
....
111.                $config['file_name'] = $app_id . '_' . $this->util-
>generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
122.                    echo $label;
```

**Reflected XSS All Clients\Path 41:**

Severity High
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7425 |
| Status | New |

Method upload_new at line 100 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/analisa.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 100 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/analisa.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/analisa.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/analisa.php |
| Line | 119 | 122 |
| Object | _FILES | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/analisa.php |
| Method | public function upload_new() { |

```
....
119.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
122.                    echo $label;
```

**Reflected XSS All Clients\Path 42:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7426 |
| Status | New |

Method upload_new at line 603 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/input_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 603 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/input_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/input_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 614 | 625 |
| Object | _FILES | echo |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Method | public function upload_new() { |

```
....
614.                $config['file_name'] = $app_id . '_' . $this->util-
>generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
625.                    echo $label;
```

**Reflected XSS All Clients\Path 43:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7427 |
| Status | New |

Method upload_new at line 603 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/input_merchant.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 603 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/input_merchant.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/input_merchant.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 622 | 625 |
| Object | _FILES | echo |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Method | public function upload_new() { |

```
....
622.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
625.                    echo $label;
```

**Reflected XSS All Clients\Path 44:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7428 |
| Status | New |

Method upload_new at line 933 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 933 of

BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php |
| Line | 944 | 955 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php
Method public function upload_new() {

```
....
944.                $config['file_name'] = $app_id . '_' . $this->util-
>generateRandomString(5) . '_' . $name . '.' . (end(explode(".",
$_FILES['foto']['name'])));
....
955.                    echo $label;
```

**Reflected XSS All Clients\Path 45:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7429
Status New

Method upload_new at line 933 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php gets user input for the _FILES element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method upload_new at line 933 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php |
| Line | 952 | 955 |
| Object | _FILES | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php
Method public function upload_new() {

```
....
952.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
....
955.                    echo $label;
```

**Reflected XSS All Clients\Path 46:**

Severity High
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7430 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input for the _POST element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <script type="text/javascript" src="<?php echo base_url('javascript/jquery.validate.min.js')?>"></script> at line 1 of application/views/qris/cm_input.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/views/qris/cm_input.php |
| Line | 182 | 58 |
| Object | _POST | echo |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/views/qris/cm_input.php

Method <script type="text/javascript" src="<?php echo base_url('javascript/jquery.validate.min.js')?>"></script>

```
....
58.                             <tr><td>Nama PIC</td><td><input
type="text" name="pic_cm" value="<?=$this->input->post('pic');?>"
onkeyup="this.value=this.value.replace(/[^A-Za-z\s]*$/,'');"></td></tr>
```

**Reflected XSS All Clients\Path 47:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7431 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input for the _POST element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <script type="text/javascript" src="<?php echo base_url('javascript/jquery.validate.min.js')?>"></script> at line 1 of BACKUP_DEPLOY_FMS_20210407/views/views/maintenance/cm_input_bck20190114.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/views/views/maintenance/cm_input_bck20190114.php |
| Line | 182 | 169 |

| | | |
|---|---|---|
| Object | _POST | echo |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/views/views/maintenance/cm_input_bck20190114.php
Method <script type="text/javascript" src="<?php echo base_url('javascript/jquery.validate.min.js')?>"></script>

```
....
169.                                <tr><td>No Telp PIC</td><td><input
type="text" name="tlp_pic" value="<?=$this->input->post('telp_pic');?>"
onkeyup="this.value=this.value.replace(/[^\d]/,'');"></td></tr>
```

**Reflected XSS All Clients\Path 48:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7432 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input for the _POST element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <script type="text/javascript" src="<?php echo base_url('javascript/jquery.validate.min.js')?>"></script> at line 1 of BACKUP_DEPLOY_FMS_20210407/views/views/maintenance_bck07112017/cm_input.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/views/views/maintenance_bck07112017/cm_input.php |
| Line | 182 | 146 |
| Object | _POST | echo |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/maintenance_bck07112017/cm_input.php |
| Method | <script type="text/javascript" src="<?php echo base_url('javascript/jquery.validate.min.js')?>"></script> |

```
....
146.                                <tr><td>Penelpon</td><td><input
type="text" name="pic" value="<?=$this->input->post('pic');?>"
onkeyup="this.value=this.value.replace(/[^A-Za-z\s]*$/,'');"></td></tr>
```

**Reflected XSS All Clients\Path 49:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7433 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input for the _POST element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <script type="text/javascript" src="<?php echo base_url('javascript/jquery.validate.min.js')?>"></script> at line 1 of BACKUP_DEPLOY_FMS_20210407/views/views/maintenance_bck07112017/cm_input.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/views/views/maintenance_bck07112017/cm_input.php |
| Line | 182 | 147 |
| Object | _POST | echo |

Code Snippet

| | |
|---|---|
| File Name | system/core/Input.php |
| Method | function post($index = NULL, $xss_clean = FALSE) |

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/maintenance_bck07112017/cm_input.php |
| Method | <script type="text/javascript" src="<?php echo base_url('javascript/jquery.validate.min.js')?>"></script> |

```
....
147.                                <tr><td>No Telp PIC</td><td><input
type="text" name="tlp_pic" value="<?=$this->input->post('telp_pic');?>"
onkeyup="this.value=this.value.replace(/[^\d]/,'');"></td></tr>
```

**Reflected XSS All Clients\Path 50:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7434 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input for the _POST element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method <?php at line 1 of application/views/aplikasi_outlet/edit_outlet_form_batch.php. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/views/aplikasi_outlet/edit_outlet_form_batch.php |
| Line | 182 | 111 |
| Object | _POST | echo |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/views/aplikasi_outlet/edit_outlet_form_batch.php

Method <?php

```
....
111.        var tabel = "<?=$this->input->post('tabel')?>";
```

## SQL Injection

Query Path:

PHP\Cx\PHP High Risk\SQL Injection Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

*Description*

**SQL Injection\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=839 |
| Status | New |

Method cm_monitoring at line 3984 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 4004 | 453 |
| Object | get | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php

Method function cm_monitoring()

```
....
4004.                    $config['total_rows']  = $this->maintenance_model->get_cm_list_hist_done($list_param, $filter, $this->input->get('filter_tahun'), 1, $data['page'], $config['per_page'],1);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=840 |
| Status | New |

Method cm_monitoring at line 3984 of application/controllers/maintenance_20190524.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 4017 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance_20190524.php

Method function cm_monitoring()

```
....
4017.                    $data['list'] = $this->maintenance_model-
>get_cm_list_hist_done($list_param, $filter, $this->input-
>get('filter_tahun'), 0, $data['page']/15, $config['per_page']);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=841 |
| Status | New |

Method cm_monitoring at line 4043 of application/controllers/maintenance.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | system/database/DB_driver.php |
| Line | 4076 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance.php

Method function cm_monitoring()

```
....
4076.                    $data['list'] = $this->maintenance_model-
>get_cm_list_hist_done($list_param, $filter, $this->input-
>get('filter_tahun'), 0, $data['page']/15, $config['per_page']);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=842 |
| Status | New |

Method cm_monitoring at line 3984 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 4017 | 453 |
| Object | get | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php

Method function cm_monitoring()

```
....
4017.                    $data['list'] = $this->maintenance_model-
>get_cm_list_hist_done($list_param, $filter, $this->input-
>get('filter_tahun'), 0, $data['page']/15, $config['per_page']);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 5:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=843 |
| Status | New |

Method cm_monitoring at line 3989 of application/controllers/maintenance_20190610.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 4022 | 453 |
| Object | get | _execute |

Code Snippet
File Name application/controllers/maintenance_20190610.php
Method function cm_monitoring()

```
....
4022.                    $data['list'] = $this->maintenance_model-
>get_cm_list_hist_done($list_param, $filter, $this->input-
>get('filter_tahun'), 0, $data['page']/15, $config['per_page']);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 6:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=844 |
| Status | New |

Method cm_monitoring at line 4043 of application/controllers/maintenance.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | system/database/DB_driver.php |
| Line | 4063 | 453 |
| Object | get | _execute |

Code Snippet
File Name application/controllers/maintenance.php
Method function cm_monitoring()

```
....
4063.                    $config['total_rows']  = $this-
>maintenance_model->get_cm_list_hist_done($list_param, $filter, $this-
>input->get('filter_tahun'), 1, $data['page'], $config['per_page'],1);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 7:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=845 |
| Status | New |

Method cm_monitoring at line 3989 of application/controllers/maintenance_20190610.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 4009 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance_20190610.php

Method function cm_monitoring()

```
....
4009.                    $config['total_rows']  = $this-
>maintenance_model->get_cm_list_hist_done($list_param, $filter, $this-
>input->get('filter_tahun'), 1, $data['page'], $config['per_page'],1);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 8:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=846 |
| Status | New |

Method cm_monitoring at line 3989 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 4009 | 453 |

| | | |
|---|---|---|
| Object | get | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php
Method function cm_monitoring()

```
....
4009.                    $config['total_rows']  = $this->maintenance_model->get_cm_list_hist_done($list_param, $filter, $this->input->get('filter_tahun'), 1, $data['page'], $config['per_page'],1);
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 9:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=847 |
| Status | New |

Method cm_monitoring at line 4033 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php | system/database/DB_driver.php |
| Line | 4053 | 453 |
| Object | get | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php
Method function cm_monitoring()

```
....
4053.                    $config['total_rows']  = $this->maintenance_model->get_cm_list_hist_done($list_param, $filter, $this->input->get('filter_tahun'), 1, $data['page'], $config['per_page'],1);
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 10:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=848 |
| Status | New |

Method cm_monitoring at line 3984 of application/controllers/maintenance_20190524.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 4004 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance_20190524.php

Method function cm_monitoring()

```
....
4004.                    $config['total_rows']  = $this->maintenance_model->get_cm_list_hist_done($list_param, $filter, $this->input->get('filter_tahun'), 1, $data['page'], $config['per_page'],1);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 11:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=849 |
| Status | New |

Method cm_monitoring at line 4033 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php | system/database/DB_driver.php |
| Line | 4066 | 453 |
| Object | get | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php
Method function cm_monitoring()

```
....
4066.                    $data['list'] = $this->maintenance_model-
>get_cm_list_hist_done($list_param, $filter, $this->input-
>get('filter_tahun'), 0, $data['page']/15, $config['per_page']);
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.               return $this->_execute($sql);
```

**SQL Injection\Path 12:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=850 |
| Status | New |

Method cm_monitoring at line 3989 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 4022 | 453 |
| Object | get | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php
Method function cm_monitoring()

```
....
4022.                    $data['list'] = $this->maintenance_model-
>get_cm_list_hist_done($list_param, $filter, $this->input-
>get('filter_tahun'), 0, $data['page']/15, $config['per_page']);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.            return $this->_execute($sql);
```

**SQL Injection\Path 13:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=851 |
| Status | New |

Method ebor_gmail_start_csv at line 1920 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler.php gets user input from the _SERVER element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler.php | system/database/DB_driver.php |
| Line | 1922 | 453 |
| Object | _SERVER | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler.php

Method function ebor_gmail_start_csv($tgl_trx = '')

```
....
1922.           if(isset($_SERVER['argv'][3])) $tgl_trx =
$_SERVER['argv'][3];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.            return $this->_execute($sql);
```

**SQL Injection\Path 14:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=852 |
| Status | New |

Method ebor_gmail_start_csv at line 1927 of application/controllers/scheduler.php gets user input from the _SERVER element. This element's value then flows through the code without being properly sanitized or

validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/scheduler.php | system/database/DB_driver.php |
| Line | 1929 | 453 |
| Object | _SERVER | _execute |

Code Snippet

File Name application/controllers/scheduler.php

Method function ebor_gmail_start_csv($tgl_trx = '')

```
....
1929.             if(isset($_SERVER['argv'][3])) $tgl_trx =
$_SERVER['argv'][3];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 15:**

Severity High

Result State To Verify

Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=853

Status New

Method pemasangan_result_form at line 2235 of application/controllers/implementasi_new.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi_new.php | system/database/DB_driver.php |
| Line | 2293 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/implementasi_new.php

Method public function pemasangan_result_form()

```
....
2293.                   $vendor_list            = $this-
>implementasi_new_model->get_implementor($this->input->get('init_kota'),
$this->uker_branch, 1);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 16:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=854 |
| Status | New |

Method pemasangan_result_form at line 2235 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php | system/database/DB_driver.php |
| Line | 2293 | 453 |
| Object | get | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php

Method public function pemasangan_result_form()

```
....
2293.                    $vendor_list            = $this-
>implementasi_new_model->get_implementor($this->input->get('init_kota'),
$this->uker_branch, 1);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 17:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=855 |
| Status | New |

Method pemasangan_request_form at line 1638 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php | system/database/DB_driver.php |
| Line | 1674 | 453 |
| Object | get | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php

Method public function pemasangan_request_form()

```
....
1674.                    $vendor_list            = $this-
>implementasi_new_model->get_implementor($this->input->get('init_kota'),
$this->uker_branch, 1);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 18:**

Severity High

Result State To Verify

Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=856

Status New

Method pemasangan_request_form at line 1638 of application/controllers/implementasi_new.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi_new.php | system/database/DB_driver.php |
| Line | 1674 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/implementasi_new.php

Method public function pemasangan_request_form()

```
....
1674.                    $vendor_list            = $this-
>implementasi_new_model->get_implementor($this->input->get('init_kota'),
$this->uker_branch, 1);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 19:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=857 |
| Status | New |

Method cm_list_done at line 3990 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php | system/database/DB_driver.php |
| Line | 3999 | 453 |
| Object | get | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php

Method function cm_list_done()

```
....
3999.              $tahun = ($this->input->get('tahun'))?$this->input-
>get('tahun'):'';
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 20:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=858 |
| Status | New |

Method cm_list_done at line 3605 of application/controllers/maintenance_bck07112017.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck07112017.php | system/database/DB_driver.php |
| Line | 3614 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance_bck07112017.php

Method function cm_list_done()

```
....
3614.             $tahun = ($this->input->get('tahun'))?$this->input->get('tahun'):'';
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 21:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=859 |
| Status | New |

Method cm_list_done at line 4080 of application/controllers/maintenance_20190610.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 4089 | 453 |
| Object | get | _execute |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/maintenance_20190610.php |
| Method | function cm_list_done() |

```
....
4089.             $tahun = ($this->input->get('tahun'))?$this->input-
>get('tahun'):'';
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 22:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=860 |
| Status | New |

Method cm_list_done at line 4024 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php | system/database/DB_driver.php |
| Line | 4033 | 453 |
| Object | get | _execute |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php |
| Method | function cm_list_done() |

```
....
4033.             $tahun = ($this->input->get('tahun'))?$this->input-
>get('tahun'):'';
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 23:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=861 |
| Status | New |

Method cm_list_done at line 4075 of application/controllers/maintenance_20190524.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 4084 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance_20190524.php

Method function cm_list_done()

```
....
4084.             $tahun = ($this->input->get('tahun'))?$this->input->get('tahun'):'';
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 24:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=862 |
| Status | New |

Method cm_list_done at line 4006 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php | system/database/DB_driver.php |
| Line | 4015 | 453 |

| | | |
|---|---|---|
| Object | get | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php

Method function cm_list_done()

```
....
4015.            $tahun = ($this->input->get('tahun'))?$this->input->get('tahun'):'';
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**SQL Injection\Path 25:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=863 |
| Status | New |

Method cm_list_done at line 4080 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 4089 | 453 |
| Object | get | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php

Method function cm_list_done()

```
....
4089.            $tahun = ($this->input->get('tahun'))?$this->input->get('tahun'):'';
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 26:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=864 |
| Status | New |

Method cm_list_done at line 3990 of application/controllers/maintenance_bck20180906.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20180906.php | system/database/DB_driver.php |
| Line | 3999 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance_bck20180906.php

Method function cm_list_done()

```
....
3999.               $tahun = ($this->input->get('tahun'))?$this->input->get('tahun'):'';
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 27:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=865 |
| Status | New |

Method cm_list_done at line 4006 of application/controllers/maintenance_20181213.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_201 | system/database/DB_driver.php |

| | | |
|---|---|---|
| | 81213.php | |
| Line | 4015 | 453 |
| Object | get | _execute |

Code Snippet
File Name application/controllers/maintenance_20181213.php
Method function cm_list_done()

```
....
4015.             $tahun = ($this->input->get('tahun'))?$this->input->get('tahun'):'';
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 28:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=866
Status New

Method cm_list_done at line 4075 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 4084 | 453 |
| Object | get | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php
Method function cm_list_done()

```
....
4084.             $tahun = ($this->input->get('tahun'))?$this->input->get('tahun'):'';
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.            return $this->_execute($sql);
```

**SQL Injection\Path 29:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=867 |
| Status | New |

Method cm_list_done at line 3605 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php | system/database/DB_driver.php |
| Line | 3614 | 453 |
| Object | get | _execute |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php |
| Method | function cm_list_done() |

```
....
3614.           $tahun = ($this->input->get('tahun'))?$this->input->get('tahun'):'';
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.            return $this->_execute($sql);
```

**SQL Injection\Path 30:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=868 |
| Status | New |

Method cm_list_done at line 4024 of application/controllers/maintenance_bck20190114.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20190114.php | system/database/DB_driver.php |
| Line | 4033 | 453 |
| Object | get | _execute |

Code Snippet
File Name application/controllers/maintenance_bck20190114.php
Method function cm_list_done()

```
....
4033.             $tahun = ($this->input->get('tahun'))?$this->input->get('tahun'):'';
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**SQL Injection\Path 31:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=869
Status New

Method tarik_data at line 46 of application/controllers/maintenance_20190524.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/maintenance_20190524.php
Method function tarik_data()

```
....
49.                 $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 32:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=870 |
| Status | New |

Method tarik_data at line 46 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php

Method function tarik_data()

```
....
49.                 $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 33:**

| | |
|---|---|
| Severity | High |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=871 |
| Status | New |

Method tarik_data at line 46 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php

Method function tarik_data()

```
....
49.                 $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 34:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=872 |
| Status | New |

Method tarik_data at line 46 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php | system/database/DB_driver.php |

| | | |
|---|---|---|
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php
Method function tarik_data()

```
....
49.                 $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 35:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=873 |
| Status | New |

Method tarik_data at line 46 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php
Method function tarik_data()

```
....
49.                 $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 36:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=874 |
| Status | New |

Method tarik_data at line 46 of application/controllers/maintenance_20190610.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/maintenance_20190610.php

Method function tarik_data()

```
....
49.                $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 37:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=875 |
| Status | New |

Method tarik_data at line 46 of application/controllers/maintenance_bck20180906.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck | system/database/DB_driver.php |

| | | |
|---|---|---|
| | 20180906.php | |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/maintenance_bck20180906.php
Method function tarik_data()

```
....
49.                 $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 38:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=876
Status New

Method tarik_data at line 46 of application/controllers/maintenance.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/maintenance.php
Method function tarik_data()

```
....
49.                 $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 39:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=877 |
| Status | New |

Method tarik_data at line 46 of application/controllers/maintenance_20181213.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20181213.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/maintenance_20181213.php

Method function tarik_data()

```
....
49.                $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 40:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=878 |
| Status | New |

Method tarik_data at line 46 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php
Method function tarik_data()

```
....
49.                 $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 41:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=879
Status New

Method tarik_data at line 46 of application/controllers/maintenance_bck20190114.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20190114.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/maintenance_bck20190114.php
Method function tarik_data()

```
....
49.                 $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 42:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=880 |
| Status | New |

Method tarik_data at line 46 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | post | _execute |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php |
| Method | function tarik_data() |

```
....
49.                $this->dl_tarik_data($this->input->post('dari'),$this->input->post('sampai'));
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 43:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=881 |
| Status | New |

Method replace at line 17 of application/controllers/replace_edc.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/replace_edc.php | system/database/DB_driver.php |
| Line | 21 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/replace_edc.php
Method public function replace()

```
....
21.                 $data['edc'] = $this->replace_edc_model-
>get_edc_aktif($this->input->post('cmbPos'));
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**SQL Injection\Path 44:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=882 |
| Status | New |

Method replace at line 17 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/replace_edc.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/replace_edc.php | system/database/DB_driver.php |
| Line | 21 | 453 |
| Object | post | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/replace_edc.php
Method public function replace()

```
....
21.                 $data['edc'] = $this->replace_edc_model-
>get_edc_aktif($this->input->post('cmbPos'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.            return $this->_execute($sql);
```

**SQL Injection\Path 45:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=883 |
| Status | New |

Method cm_ubah_implementor_approval at line 3845 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php | system/database/DB_driver.php |
| Line | 3847 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php

Method function cm_ubah_implementor_approval()

```
....
3847.           $id_cm          = $this->input->post('id');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.            return $this->_execute($sql);
```

**SQL Injection\Path 46:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=884 |
| Status | New |

Method cm_ubah_implementor_approval at line 3887 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 3889 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php

Method function cm_ubah_implementor_approval()

```
....
3889.            $id_cm            = $this->input->post('id');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**SQL Injection\Path 47:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=885 |
| Status | New |

Method cm_ubah_implementor_approval at line 3862 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php | system/database/DB_driver.php |
| Line | 3864 | 453 |
| Object | post | _execute |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php |
| Method | function cm_ubah_implementor_approval() |

```
....
3864.            $id_cm            = $this->input->post('id');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.             return $this->_execute($sql);
```

**SQL Injection\Path 48:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=886 |
| Status | New |

Method cm_ubah_implementor_approval at line 3882 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 3884 | 453 |
| Object | post | _execute |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php |
| Method | function cm_ubah_implementor_approval() |

```
....
3884.            $id_cm            = $this->input->post('id');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.             return $this->_execute($sql);
```

**SQL Injection\Path 49:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=887 |
| Status | New |

Method cm_ubah_implementor_approval at line 3941 of application/controllers/maintenance.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | system/database/DB_driver.php |
| Line | 3943 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/maintenance.php

Method function cm_ubah_implementor_approval()

```
....
3943.            $id_cm            = $this->input->post('id');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**SQL Injection\Path 50:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=888 |
| Status | New |

Method cm_ubah_implementor_approval at line 3880 of application/controllers/maintenance_bck20190114.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20190114.php | system/database/DB_driver.php |
| Line | 3882 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/maintenance_bck20190114.php
Method function cm_ubah_implementor_approval()

```
....
3882.            $id_cm            = $this->input->post('id');
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

## Second Order SQL Injection

Query Path:
PHP\Cx\PHP High Risk\Second Order SQL Injection Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

*Description*

**Second Order SQL Injection\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=112 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets database data from the oci_fetch_assoc element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method deleteCacheData at line 157 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Line | 155 | 165 |
| Object | oci_fetch_assoc | queryExec |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php

Method public function deleteCacheData($pCoord) {

```
....
165.                if (!$this->_DBHandle->queryExec($query))
```

**Second Order SQL Injection\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=113 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets database data from the oci_fetch_assoc element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/database/DB_driver.php |
| Line | 155 | 453 |
| Object | oci_fetch_assoc | _execute |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=114 |
| Status | New |

Method getCacheData at line 139 of application/third_party/PHPExcel/CachedObjectStorage/Memcache.php gets database data from the ".cache" element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php | system/database/DB_driver.php |
| Line | 147 | 453 |
| Object | ".cache" | _execute |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/Memcache.php

Method public function getCacheData($pCoord) {

```
....
147.                    $obj = $this->_memcache->get($this-
>_cachePrefix.$pCoord.'.cache');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=115 |
| Status | New |

Method getCacheData at line 99 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php gets database data from the fetchSingle element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | system/database/DB_driver.php |
| Line | 117 | 453 |
| Object | fetchSingle | _execute |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php

Method public function getCacheData($pCoord) {

```
....
117.                $cellResult = $cellResultSet->fetchSingle();
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 5:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=116 |
| Status | New |

Method detail_sign_sik at line 2172 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_uker_branch element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2182 | 453 |
| Object | _SESSION_uker_branch | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2182.                    $org_surat = $_SESSION['uker_branch'].'/OJL/';
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 6:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=117 |
| Status | New |

Method detail_sign_sik at line 2172 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2242 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2242.                    $sufix =
$_SESSION['username'].'_'.date('Y_m_d_h_i_s');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 7:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=118 |
| Status | New |

Method detail_sign_sik at line 2172 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2344 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2344.                                $qrparams['data'] =
str_replace(array('
','/'),array('_','|'),$_SESSION["nama_lengkap"]).'_'.str_replace(array('
','/'),array('_','|'),$subdata['no_sp']);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 8:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=119 |
| Status | New |

Method detail_sign_sik at line 2172 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2522 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2522.                                $qrparams_pameran['data'] =
str_replace(array('
','/'),array('_','|'),$_SESSION["nama_lengkap"]).'_'.str_replace(array('
','/'),array('_','|'),$subdata['no_sp']);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 9:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=120 |
| Status | New |

Method detail_sign_sik at line 2172 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2584 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2584.                        $update['init_user_kirim_sik_kabag'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 10:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=121 |
| Status | New |

Method detail_sign_sik at line 2172 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2584 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php
Method public function detail_sign_sik()

```
....
2584.                        $update['init_user_kirim_sik_kabag'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 11:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=122 |
| Status | New |

Method detail_sign_sik at line 2172 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_uker_branch element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2181 | 453 |
| Object | _SESSION_uker_branch | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php
Method public function detail_sign_sik()

```
....
2181.                    $param['kanwil_tujuan'] =
$_SESSION['uker_branch'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 12:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=123 |
| Status | New |

Method detail_sign_sik at line 2172 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2407 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2407.                        $update['init_user_kirim_sik_kabag'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 13:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=124 |
| Status | New |

Method detail_sign_sik at line 2172 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2407 | 453 |

| | | |
|---|---|---|
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php
Method public function detail_sign_sik()

```
....
2407.                        $update['init_user_kirim_sik_kabag'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 14:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=125 |
| Status | New |

Method ver_outlet_process at line 678 of application/controllers/aplikasi_outlet_bck20190524.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet_bck20190524.php | system/database/DB_driver.php |
| Line | 821 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet
File Name application/controllers/aplikasi_outlet_bck20190524.php
Method function ver_outlet_process() {

```
....
821.                    $status['user_verifikasi'] =
$_SESSION['username'] . '|' . $_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 15:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=126 |
| Status | New |

Method ver_outlet_process at line 678 of application/controllers/aplikasi_outlet_bck20190524.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet_bck20190524.php | system/database/DB_driver.php |
| Line | 821 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet

File Name application/controllers/aplikasi_outlet_bck20190524.php

Method function ver_outlet_process() {

```
....
821.                    $status['user_verifikasi'] =
$_SESSION['username'] . '|' . $_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 16:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=127 |
| Status | New |

Method ver_outlet_process at line 678 of application/controllers/aplikasi_outlet_bck20190524.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet_bck20190524.php | system/database/DB_driver.php |
| Line | 694 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet
File Name application/controllers/aplikasi_outlet_bck20190524.php
Method function ver_outlet_process() {

```
....
694.                    $status['user_verifikasi'] =
$_SESSION['username'] . '|' . $_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 17:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=128 |
| Status | New |

Method ver_outlet_process at line 678 of application/controllers/aplikasi_outlet_bck20190524.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet_bck20190524.php | system/database/DB_driver.php |
| Line | 694 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet
File Name application/controllers/aplikasi_outlet_bck20190524.php
Method function ver_outlet_process() {

```
....
694.                    $status['user_verifikasi'] =
$_SESSION['username'] . '|' . $_SESSION['nama_lengkap'];
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 18:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=129 |
| Status | New |

Method distribusi_tms at line 17 of application/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 29 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/implementasi.php |
| Method | public function distribusi_tms() |

```
....
29.                     $update['init_user_distribusi_tms'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 19:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=130 |
| Status | New |

Method distribusi_tms at line 17 of application/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| Source | Destination |
|---|---|

| File | application/controllers/implementasi.php | system/database/DB_driver.php |
|---|---|---|
| Line | 29 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function distribusi_tms()

```
....
29.                     $update['init_user_distribusi_tms'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 20:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=131 |
| Status | New |

Method distribusi_tms at line 17 of application/controllers/implementasi.php gets database data from the _SESSION_distribusi_tms_id_terpilih element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 49 | 453 |
| Object | _SESSION_distribusi_tms_id_terpilih | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function distribusi_tms()

```
....
49.                           $where['collection'] =
isset($_SESSION['distribusi_tms_id_terpilih'])?$_SESSION['distribusi_tms
_id_terpilih']:array();
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 21:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=132 |
| Status | New |

Method registrasi_tms at line 115 of application/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 130 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function registrasi_tms()

```
....
130.                    $update['init_user_registrasi_tms'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 22:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=133 |
| Status | New |

Method registrasi_tms at line 115 of application/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |

| | | |
|---|---|---|
| Line | 130 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function registrasi_tms()

```
....
130.                    $update['init_user_registrasi_tms'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 23:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=134
Status New

Method registrasi_tms at line 115 of application/controllers/implementasi.php gets database data from the _SESSION_uker_branch element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 121 | 453 |
| Object | _SESSION_uker_branch | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function registrasi_tms()

```
....
121.                    $param['kanwil_tujuan'] =
$_SESSION['uker_branch'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 24:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=135 |
| Status | New |

Method registrasi_tms at line 115 of application/controllers/implementasi.php gets database data from the _SESSION_registrasi_tms_id_terpilih element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 149 | 453 |
| Object | _SESSION_registrasi_tms_id_terpilih | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function registrasi_tms()

```
....
149.                            $where['collection'] =
isset($_SESSION['registrasi_tms_id_terpilih'])?$_SESSION['registrasi_tms
_id_terpilih']:array();
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 25:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=136 |
| Status | New |

Method send at line 532 of application/controllers/implementasi.php gets database data from the _SESSION_sik element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |

| | | |
|---|---|---|
| Line | 561 | 453 |
| Object | _SESSION_sik | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function send()

```
....
561.                        $update = $_SESSION['sik']['update'];
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 26:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=137 |
| Status | New |

Method send at line 532 of application/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 740 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function send()

```
....
740.                        $update['init_user_kirim_sik_implementor']
= $_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 27:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=138 |
| Status | New |

Method send at line 532 of application/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 740 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function send()

```
....
740.                            $update['init_user_kirim_sik_implementor']
= $_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 28:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=139 |
| Status | New |

Method send at line 532 of application/controllers/implementasi.php gets database data from the _SESSION_sik element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 562 | 453 |
| Object | _SESSION_sik | _execute |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/implementasi.php |
| Method | public function send() |

```
....
562.                        $where = $_SESSION['sik']['where'];
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 29:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=140 |
| Status | New |

Method detail_check_sik at line 2056 of application/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2076 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/implementasi.php |
| Method | public function detail_check_sik() |

```
....
2076.                   $update['init_user_kirim_sik_spv'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 30:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=141 |

| | |
|---|---|
| Status | New |

Method detail_check_sik at line 2056 of application/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2076 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function detail_check_sik()

```
....
2076.                    $update['init_user_kirim_sik_spv'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 31:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=142 |
| Status | New |

Method detail_check_sik at line 2056 of application/controllers/implementasi.php gets database data from the _SESSION_uker_branch element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2065 | 453 |
| Object | _SESSION_uker_branch | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function detail_check_sik()

```
....
2065.                    $param['kanwil_tujuan'] =
$_SESSION['uker_branch'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 32:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=143 |
| Status | New |

Method detail_sign_sik at line 2172 of application/controllers/implementasi.php gets database data from the _SESSION_uker_branch element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2182 | 453 |
| Object | _SESSION_uker_branch | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2182.                    $org_surat = $_SESSION['uker_branch'].'/OJL/';
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 33:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=144 |
| Status | New |

Method detail_sign_sik at line 2172 of application/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2242 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2242.                    $sufix =
$_SESSION['username'].'_'.date('Y_m_d_h_i_s');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 34:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=145 |
| Status | New |

Method detail_sign_sik at line 2172 of application/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2344 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2344.                                $qrparams['data'] =
str_replace(array('
','/'),array('_','|'),$_SESSION["nama_lengkap"]).'_'.str_replace(array('
','/'),array('_','|'),$subdata['no_sp']);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 35:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=146 |
| Status | New |

Method detail_sign_sik at line 2172 of application/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2522 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2522.                                $qrparams_pameran['data'] =
str_replace(array('
','/'),array('_','|'),$_SESSION["nama_lengkap"]).'_'.str_replace(array('
','/'),array('_','|'),$subdata['no_sp']);
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 36:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=147 |
| Status | New |

Method detail_sign_sik at line 2172 of application/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2584 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2584.                          $update['init_user_kirim_sik_kabag'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 37:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=148 |
| Status | New |

Method detail_sign_sik at line 2172 of application/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2584 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2584.                        $update['init_user_kirim_sik_kabag'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 38:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=149 |
| Status | New |

Method detail_sign_sik at line 2172 of application/controllers/implementasi.php gets database data from the _SESSION_uker_branch element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2181 | 453 |
| Object | _SESSION_uker_branch | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function detail_sign_sik()

```
....
2181.                   $param['kanwil_tujuan'] =
$_SESSION['uker_branch'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 39:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=150 |
| Status | New |

Method detail_sign_sik at line 2172 of application/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2407 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function detail_sign_sik()

```
....
2407.                         $update['init_user_kirim_sik_kabag'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 40:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=151
Status New

Method detail_sign_sik at line 2172 of application/controllers/implementasi.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2407 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function detail_sign_sik()

```
....
2407.                         $update['init_user_kirim_sik_kabag'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.            return $this->_execute($sql);
```

**Second Order SQL Injection\Path 41:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=152 |
| Status | New |

Method detail_check_sik at line 2056 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2076 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php

Method public function detail_check_sik()

```
....
2076.                   $update['init_user_kirim_sik_spv'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.            return $this->_execute($sql);
```

**Second Order SQL Injection\Path 42:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=153 |
| Status | New |

Method detail_check_sik at line 2056 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the

_SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2076 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php
Method public function detail_check_sik()

```
....
2076.                    $update['init_user_kirim_sik_spv'] =
$_SESSION['username'].'|'.$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 43:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=154 |
| Status | New |

Method detail_check_sik at line 2056 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets database data from the _SESSION_uker_branch element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 2065 | 453 |
| Object | _SESSION_uker_branch | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php
Method public function detail_check_sik()

```
....
2065.                    $param['kanwil_tujuan'] =
$_SESSION['uker_branch'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 44:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=155 |
| Status | New |

Method ver_pameran_process at line 549 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php | system/database/DB_driver.php |
| Line | 562 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php

Method public function ver_pameran_process()

```
....
562.              $db_upd_status['user_verifikasi']   =
$_SESSION['username']."|".$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 45:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=156 |
| Status | New |

Method ver_pameran_process at line 549 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php | system/database/DB_driver.php |
| Line | 562 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php

Method public function ver_pameran_process()

```
....
562.                $db_upd_status['user_verifikasi']    =
$_SESSION['username']."|".$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 46:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=157 |
| Status | New |

Method edit_app_pameran_process at line 752 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php | system/database/DB_driver.php |
| Line | 771 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php

Method public function edit_app_pameran_process()

```
....
771.                $db_upd_status['user_edit']          =
$_SESSION['username']."|".$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 47:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=158 |
| Status | New |

Method edit_app_pameran_process at line 752 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php | system/database/DB_driver.php |
| Line | 771 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php

Method public function edit_app_pameran_process()

```
....
771.                $db_upd_status['user_edit']          =
$_SESSION['username']."|".$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Second Order SQL Injection\Path 48:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=159 |
| Status | New |

Method ver_mdr_pameran_process at line 1003 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php | system/database/DB_driver.php |
| Line | 1014 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php

Method function ver_mdr_pameran_process() {

```
....
1014.                    $status['user_mdr'] =
$_SESSION['username']."|".$_SESSION['nama_lengkap'];
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 49:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=160 |
| Status | New |

Method ver_mdr_pameran_process at line 1003 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php gets database data from the _SESSION_nama_lengkap element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php | system/database/DB_driver.php |
| Line | 1014 | 453 |
| Object | _SESSION_nama_lengkap | _execute |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/pameran.php |
| Method | function ver_mdr_pameran_process() { |

```
....
1014.                    $status['user_mdr'] =
$_SESSION['username']."|".$_SESSION['nama_lengkap'];
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.              return $this->_execute($sql);
```

**Second Order SQL Injection\Path 50:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=161 |
| Status | New |

Method input_merchant_process at line 708 of application/controllers/aplikasi_tambah_merchant/input_merchant.php gets database data from the _SESSION_username element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in a database query in method simple_query at line 446 of system/database/DB_driver.php. This may enable an Second-Order SQL Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant.php | system/database/DB_driver.php |
| Line | 738 | 453 |
| Object | _SESSION_username | _execute |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Method | public function input_merchant_process() { |

```
....
738.                          $status['user_entry'] =
$_SESSION['username'] . "|" . $_SESSION['nama_lengkap'];
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.              return $this->_execute($sql);
```

## File Manipulation

Query Path:

## Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.8 - Improper access control
FISMA 2014: Configuration Management
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A1-Broken Access Control

## Description

**File Manipulation\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=575 |
| Status | New |

The input obtained via <?php in the file system/helpers/dompdf/www/controller.php at line 1 is used to determine the location of a file to be written into by addLine in the file system/helpers/dompdf/lib/php-font-lib/classes/adobe_font_metrics.cls.php at line 181, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/controller.php | system/helpers/dompdf/lib/php-font-lib/classes/adobe_font_metrics.cls.php |
| Line | 22 | 182 |
| Object | _FILES | f |

Code Snippet

File Name system/helpers/dompdf/www/controller.php

Method <?php

```
....
22.      $data = $_FILES["file"];
```

File Name system/helpers/dompdf/lib/php-font-lib/classes/adobe_font_metrics.cls.php

Method function addLine($line) {

```
....
182.      fwrite($this->f, "$line\n");
```

**File Manipulation\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=576 |
| Status | New |

The input obtained via hapus_file_exist in the file application/controllers/aplikasi_edit.php at line 696 is used to determine the location of a file to be written into by hapus_file_exist in the file

application/controllers/aplikasi_edit.php at line 696, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_edit.php | application/controllers/aplikasi_edit.php |
| Line | 698 | 705 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/aplikasi_edit.php
Method public function hapus_file_exist()

```
....
698.                $path       = $this->input->post('path');
....
705.                echo unlink(FCPATH.$path);
```

**File Manipulation\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=577 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_file_exist in the file application/controllers/aplikasi_edit.php at line 696, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_edit.php |
| Line | 182 | 705 |
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_edit.php
Method public function hapus_file_exist()

```
....
705.                echo unlink(FCPATH.$path);
```

**File Manipulation\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=578 |
| Status | New |

The input obtained via hapus_file in the file application/controllers/aplikasi_edit.php at line 708 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_edit.php at line 708, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_edit.php | application/controllers/aplikasi_edit.php |
| Line | 709 | 711 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/aplikasi_edit.php
Method public function hapus_file() {

```
....
709.                $path = $this->input->post('path');
....
711.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 5:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=579 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_edit.php at line 708, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_edit.php |
| Line | 182 | 711 |
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_edit.php

Method public function hapus_file() {

```
....
711.            echo unlink(FCPATH . $path);
```

**File Manipulation\Path 6:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=580
Status New

The input obtained via hapus_foto in the file application/controllers/aplikasi_merchant.php at line 595 is used to determine the location of a file to be written into by hapus_foto in the file application/controllers/aplikasi_merchant.php at line 595, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 599 | 601 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function hapus_foto() {

```
....
599.            $link = $this->input->post('link');
....
601.            unlink(FCPATH . $link);
```

**File Manipulation\Path 7:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=581
Status New

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_foto in the file application/controllers/aplikasi_merchant.php at line 595, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_merchant.php |
| Line | 182 | 601 |

| | | |
|---|---|---|
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_merchant.php
Method public function hapus_foto() {

```
....
601.                unlink(FCPATH . $link);
```

**File Manipulation\Path 8:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=582
Status New

The input obtained via hapus_file in the file application/controllers/aplikasi_merchant.php at line 605 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_merchant.php at line 605, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 606 | 608 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method public function hapus_file() {

```
....
606.                $path = $this->input->post('path');
....
608.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 9:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=583
Status New

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_merchant.php at line 605, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_merchant.php |
| Line | 182 | 608 |
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_merchant.php
Method public function hapus_file() {

```
....
608.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 10:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=584
Status New

The input obtained via hapus_file in the file application/controllers/aplikasi_outlet.php at line 121 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_outlet.php at line 121, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet.php | application/controllers/aplikasi_outlet.php |
| Line | 122 | 124 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/aplikasi_outlet.php
Method public function hapus_file() {

```
....
122.                $path = $this->input->post('path');
....
124.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 11:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=585 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_outlet.php at line 121, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_outlet.php |
| Line | 182 | 124 |
| Object | _POST | BinaryExpr |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_outlet.php

Method public function hapus_file() {

```
....
124.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 12:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=586 |
| Status | New |

The input obtained via input_outlet_upload in the file application/controllers/aplikasi_outlet.php at line 347 is used to determine the location of a file to be written into by input_outlet_upload in the file application/controllers/aplikasi_outlet.php at line 347, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet.php | application/controllers/aplikasi_outlet.php |
| Line | 360 | 558 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/aplikasi_outlet.php
Method function input_outlet_upload() {

```
....
360.                    $handle =
fopen($_FILES['file_upload']['tmp_name'], "r");
....
558.                            fclose($handle);
```

**File Manipulation\Path 13:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=587 |
| Status | New |

The input obtained via upload_outlet in the file application/controllers/aplikasi_outlet.php at line 1124 is used to determine the location of a file to be written into by upload_outlet in the file application/controllers/aplikasi_outlet.php at line 1124, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet.php | application/controllers/aplikasi_outlet.php |
| Line | 1199 | 1467 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/aplikasi_outlet.php
Method function upload_outlet(){

```
....
1199.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
1467.             fclose($handle);
```

**File Manipulation\Path 14:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=588 |
| Status | New |

The input obtained via hapus_file in the file application/controllers/aplikasi_outlet_bck20190524.php at line 120 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_outlet_bck20190524.php at line 120, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet_bck20190524.php | application/controllers/aplikasi_outlet_bck20190524.php |
| Line | 121 | 123 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/aplikasi_outlet_bck20190524.php
Method public function hapus_file() {

```
....
121.                $path = $this->input->post('path');
....
123.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 15:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=589 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_outlet_bck20190524.php at line 120, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_outlet_bck20190524.php |
| Line | 182 | 123 |
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_outlet_bck20190524.php
Method public function hapus_file() {

```
....
123.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 16:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=590 |
| Status | New |

The input obtained via input_outlet_upload in the file application/controllers/aplikasi_outlet_bck20190524.php at line 346 is used to determine the location of a file to be written into by input_outlet_upload in the file application/controllers/aplikasi_outlet_bck20190524.php at line 346, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet_bck20190524.php | application/controllers/aplikasi_outlet_bck20190524.php |
| Line | 359 | 557 |
| Object | _FILES | handle |

Code Snippet

File Name application/controllers/aplikasi_outlet_bck20190524.php

Method function input_outlet_upload() {

```
....
359.                    $handle =
fopen($_FILES['file_upload']['tmp_name'], "r");
....
557.                            fclose($handle);
```

**File Manipulation\Path 17:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=591 |
| Status | New |

The input obtained via upload_outlet in the file application/controllers/aplikasi_outlet_bck20190524.php at line 1123 is used to determine the location of a file to be written into by upload_outlet in the file application/controllers/aplikasi_outlet_bck20190524.php at line 1123, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet_bck20190524.php | application/controllers/aplikasi_outlet_bck20190524.php |
| Line | 1198 | 1466 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/aplikasi_outlet_bck20190524.php
Method function upload_outlet(){

```
....
1198.            $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
1466.            fclose($handle);
```

**File Manipulation\Path 18:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=592
Status New

The input obtained via hapus_file in the file application/controllers/aplikasi_tambah_merchant/analisa.php at line 126 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_tambah_merchant/analisa.php at line 126, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/analisa.php | application/controllers/aplikasi_tambah_merchant/analisa.php |
| Line | 127 | 129 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/analisa.php
Method public function hapus_file() {

```
....
127.             $path = $this->input->post('path');
....
129.             echo unlink(FCPATH . $path);
```

**File Manipulation\Path 19:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=593
Status New

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_tambah_merchant/analisa.php at line 126, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_tambah_ |

| | | |
|---|---|---|
| | | merchant/analisa.php |
| Line | 182 | 129 |
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_tambah_merchant/analisa.php
Method public function hapus_file() {

```
....
129.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 20:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=594
Status New

The input obtained via hapus_file in the file application/controllers/aplikasi_tambah_merchant/input_merchant.php at line 670 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_tambah_merchant/input_merchant.php at line 670, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 671 | 673 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php
Method public function hapus_file() {

```
....
671.                $path = $this->input->post('path');
....
673.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 21:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=595 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_tambah_merchant/input_merchant.php at line 670, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 182 | 673 |
| Object | _POST | BinaryExpr |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php

Method public function hapus_file() {

```
....
673.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 22:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=596 |
| Status | New |

The input obtained via hapus_foto in the file application/controllers/aplikasi_tambah_merchant/input_merchant.php at line 676 is used to determine the location of a file to be written into by hapus_foto in the file application/controllers/aplikasi_tambah_merchant/input_merchant.php at line 676, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 680 | 682 |

| | | |
|---|---|---|
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php
Method public function hapus_foto() {

```
....
680.            $link = $this->input->post('link');
....
682.            unlink(FCPATH . $link);
```

**File Manipulation\Path 23:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=597 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_foto in the file application/controllers/aplikasi_tambah_merchant/input_merchant.php at line 676, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 182 | 682 |
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php
Method public function hapus_foto() {

```
....
682.            unlink(FCPATH . $link);
```

**File Manipulation\Path 24:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=598 |
| Status | New |

The input obtained via hapus_file in the file application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php at line 653 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php at line 653, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php |
| Line | 654 | 656 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php
Method public function hapus_file() {

```
....
654.                $path = $this->input->post('path');
....
656.                echo unlink(FCPATH . $path);
```

**File Manipulation\Path 25:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=599 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_file in the file application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php at line 653, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php |
| Line | 182 | 656 |
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php

Method public function hapus_file() {

```
....
656.            echo unlink(FCPATH . $path);
```

**File Manipulation\Path 26:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=600 |
| Status | New |

The input obtained via hapus_foto in the file application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php at line 659 is used to determine the location of a file to be written into by hapus_foto in the file application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php at line 659, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php |
| Line | 663 | 665 |
| Object | post | BinaryExpr |

Code Snippet

File Name application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php

Method public function hapus_foto() {

```
....
663.            $link = $this->input->post('link');
....
665.            unlink(FCPATH . $link);
```

**File Manipulation\Path 27:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=601 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by hapus_foto in the file application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php at line 659, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php |
| Line | 182 | 665 |
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php
Method public function hapus_foto() {

```
....
665.                unlink(FCPATH . $link);
```

**File Manipulation\Path 28:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=602
Status New

The input obtained via get in the file system/core/Input.php at line 144 is used to determine the location of a file to be written into by send_to_approval in the file application/controllers/ebor.php at line 24, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 154 | 59 |
| Object | _GET | filepath |

Code Snippet
File Name system/core/Input.php
Method function get($index = NULL, $xss_clean = FALSE)

```
....
154.                            $get[$key] = $this-
>_fetch_from_array($_GET, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method public function send_to_approval() {

```
....
59.                             unlink($filepath);
```

**File Manipulation\Path 29:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=603 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by send_to_approval in the file application/controllers/ebor.php at line 24, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 59 |
| Object | _POST | filepath |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method public function send_to_approval() {

```
....
59.                             unlink($filepath);
```

**File Manipulation\Path 30:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=604 |
| Status | New |

The input obtained via daftar_save in the file application/controllers/ebor.php at line 196 is used to determine the location of a file to be written into by daftar_save in the file application/controllers/ebor.php at line 196, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 199 | 243 |
| Object | post | filerk |

Code Snippet
File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
199.            $mid        = $this->input->post('mid');
....
243.                            unlink($filerk);
```

**File Manipulation\Path 31:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=605
Status New

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by daftar_save in the file application/controllers/ebor.php at line 196, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 243 |
| Object | _POST | filerk |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
243.                                unlink($filerk);
```

**File Manipulation\Path 32:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=606 |
| Status | New |

The input obtained via daftar_save in the file application/controllers/ebor.php at line 196 is used to determine the location of a file to be written into by daftar_save in the file application/controllers/ebor.php at line 196, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 201 | 243 |
| Object | post | filerk |

Code Snippet
File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
201.              $tgl        = $this->input->post('tgl');
....
243.                                unlink($filerk);
```

**File Manipulation\Path 33:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=607 |
| Status | New |

The input obtained via daftar_save in the file application/controllers/ebor.php at line 196 is used to determine the location of a file to be written into by daftar_save in the file application/controllers/ebor.php at line 196, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 199 | 244 |
| Object | post | filedetail |

Code Snippet
File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
199.                $mid        = $this->input->post('mid');
....
244.                                unlink($filedetail);
```

**File Manipulation\Path 34:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=608 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by daftar_save in the file application/controllers/ebor.php at line 196, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 244 |
| Object | _POST | filedetail |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method public function daftar_save()

```
....
244.                                unlink($filedetail);
```

**File Manipulation\Path 35:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=609 |
| Status | New |

The input obtained via daftar_save in the file application/controllers/ebor.php at line 196 is used to determine the location of a file to be written into by daftar_save in the file application/controllers/ebor.php at line 196, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 201 | 244 |
| Object | post | filedetail |

Code Snippet
File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
201.            $tgl        = $this->input->post('tgl');
....
244.                            unlink($filedetail);
```

**File Manipulation\Path 36:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=610 |
| Status | New |

The input obtained via daftar_save in the file application/controllers/ebor.php at line 196 is used to determine the location of a file to be written into by daftar_save in the file application/controllers/ebor.php at line 196, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 199 | 453 |
| Object | post | filepath |

Code Snippet
File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
199.            $mid        = $this->input->post('mid');
....
453.                                    unlink($filepath);
```

**File Manipulation\Path 37:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=611 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by daftar_save in the file application/controllers/ebor.php at line 196, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 453 |
| Object | _POST | filepath |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
453.                                    unlink($filepath);
```

**File Manipulation\Path 38:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=612
Status New

The input obtained via daftar_save in the file application/controllers/ebor.php at line 196 is used to determine the location of a file to be written into by daftar_save in the file application/controllers/ebor.php at line 196, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 201 | 453 |
| Object | post | filepath |

Code Snippet
File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
201.              $tgl        = $this->input->post('tgl');
....
453.                                    unlink($filepath);
```

**File Manipulation\Path 39:**

Severity High
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=613 |
| Status | New |

The input obtained via get in the file system/core/Input.php at line 144 is used to determine the location of a file to be written into by generate_file in the file application/controllers/ebor.php at line 931, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 154 | 972 |
| Object | _GET | filerk |

Code Snippet

File Name system/core/Input.php

Method function get($index = NULL, $xss_clean = FALSE)

```
....
154.                            $get[$key] = $this-
>_fetch_from_array($_GET, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method function generate_file($data) {

```
....
972.                            unlink($filerk);
```

**File Manipulation\Path 40:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=614 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by generate_file in the file application/controllers/ebor.php at line 931, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 972 |
| Object | _POST | filerk |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method function generate_file($data) {

```
....
972.                            unlink($filerk);
```

**File Manipulation\Path 41:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=615 |
| Status | New |

The input obtained via get in the file system/core/Input.php at line 144 is used to determine the location of a file to be written into by generate_file in the file application/controllers/ebor.php at line 931, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 154 | 973 |
| Object | _GET | filedetail |

Code Snippet

File Name system/core/Input.php

Method function get($index = NULL, $xss_clean = FALSE)

```
....
154.                            $get[$key] = $this-
>_fetch_from_array($_GET, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method function generate_file($data) {

```
....
973.                            unlink($filedetail);
```

**File Manipulation\Path 42:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=616 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by generate_file in the file application/controllers/ebor.php at line 931, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 973 |
| Object | _POST | filedetail |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php
Method function generate_file($data) {

```
....
973.                            unlink($filedetail);
```

**File Manipulation\Path 43:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=617 |
| Status | New |

The input obtained via edit in the file application/controllers/email_blast.php at line 117 is used to determine the location of a file to be written into by edit in the file application/controllers/email_blast.php at line 117, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/email_blast.php | application/controllers/email_blast.php |
| Line | 134 | 138 |
| Object | post | attdel |

Code Snippet
File Name application/controllers/email_blast.php
Method public function edit(){

```
....
134.                                        $att_old = explode(';',$this-
>input->post('attachment_old'));
....
138.
      unlink($attdel);
```

**File Manipulation\Path 44:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=618 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by edit in the file application/controllers/email_blast.php at line 117, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/email_blast.php |
| Line | 182 | 138 |
| Object | _POST | attdel |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                          $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/email_blast.php

Method public function edit(){

```
....
138.
      unlink($attdel);
```

**File Manipulation\Path 45:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=619 |
| Status | New |

The input obtained via edit in the file application/controllers/email_blast.php at line 117 is used to determine the location of a file to be written into by edit in the file application/controllers/email_blast.php at line 117, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/email_blast.php | application/controllers/email_blast.php |
| Line | 201 | 205 |
| Object | post | attdel |

Code Snippet
File Name application/controllers/email_blast.php
Method public function edit(){

```
....
201.                                $att_old = explode(';',$this->input-
>post('attachment_old'));
....
205.                                                    unlink($attdel);
```

**File Manipulation\Path 46:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=620 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by edit in the file application/controllers/email_blast.php at line 117, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/email_blast.php |
| Line | 182 | 205 |
| Object | _POST | attdel |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/email_blast.php
Method public function edit(){

```
....
205.                                                    unlink($attdel);
```

**File Manipulation\Path 47:**

| | |
|---|---|
| Severity | High |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=621 |
| Status | New |

The input obtained via sik_signer_save in the file application/controllers/implementasi_new.php at line 808 is used to determine the location of a file to be written into by sik_signer_save in the file application/controllers/implementasi_new.php at line 808, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi_new.php | application/controllers/implementasi_new.php |
| Line | 860 | 1077 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/implementasi_new.php
Method public function sik_signer_save()

```
....
860.              $kode_kirim_arr = $this->input-
>post('init_kode_kirim');
....
1077.                                unlink($folder.$filename);
```

**File Manipulation\Path 48:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=622 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by sik_signer_save in the file application/controllers/implementasi_new.php at line 808, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/implementasi_new.php |
| Line | 182 | 1077 |
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                          $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/implementasi_new.php

Method public function sik_signer_save()

```
....
1077.                                unlink($folder.$filename);
```

**File Manipulation\Path 49:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=623 |
| Status | New |

The input obtained via sik_signer_save in the file application/controllers/implementasi_new.php at line 808 is used to determine the location of a file to be written into by sik_signer_save in the file application/controllers/implementasi_new.php at line 808, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi_new.php | application/controllers/implementasi_new.php |
| Line | 860 | 1078 |
| Object | post | BinaryExpr |

Code Snippet

File Name application/controllers/implementasi_new.php

Method public function sik_signer_save()

```
....
860.              $kode_kirim_arr = $this->input-
>post('init_kode_kirim');
....
1078.                                unlink($folder.$pdfsp);
```

**File Manipulation\Path 50:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=624 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the location of a file to be written into by sik_signer_save in the file application/controllers/implementasi_new.php at line 808, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/implementasi_new.php |

| | | |
|---|---|---|
| Line | 182 | 1078 |
| Object | _POST | BinaryExpr |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/implementasi_new.php

Method public function sik_signer_save()

```
....
1078.                               unlink($folder.$pdfsp);
```

## File Disclosure

Query Path:
PHP\Cx\PHP High Risk\File Disclosure Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.8 - Improper access control
FISMA 2014: Configuration Management
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A1-Broken Access Control

*Description*

**File Disclosure\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=490 |
| Status | New |

The input obtained via input_outlet_upload in the file application/controllers/aplikasi_outlet.php at line 347 is used to determine the file to be read by input_outlet_upload in the file application/controllers/aplikasi_outlet.php at line 347, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet.php | application/controllers/aplikasi_outlet.php |
| Line | 360 | 376 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/aplikasi_outlet.php
Method function input_outlet_upload() {

```
....
360.                    $handle =
fopen($_FILES['file_upload']['tmp_name'], "r");
....
376.                        while (($data = fgetcsv($handle, 1000000,
","))  != FALSE)  {
```

**File Disclosure\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=491 |
| Status | New |

The input obtained via upload_outlet in the file application/controllers/aplikasi_outlet.php at line 1124 is used to determine the file to be read by upload_outlet in the file application/controllers/aplikasi_outlet.php at line 1124, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet.php | application/controllers/aplikasi_outlet.php |
| Line | 1199 | 1203 |
| Object | _FILES | handle |

Code Snippet

File Name application/controllers/aplikasi_outlet.php

Method function upload_outlet(){

```
....
1199.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
1203.                    while (($data = fgetcsv($handle, 1000000,
$separator))  != FALSE)  {
```

**File Disclosure\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=492 |
| Status | New |

The input obtained via input_outlet_upload in the file application/controllers/aplikasi_outlet_bck20190524.php at line 346 is used to determine the file to be read by input_outlet_upload in the file application/controllers/aplikasi_outlet_bck20190524.php at line 346, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet_bck20190524.php | application/controllers/aplikasi_outlet_bck20190524.php |

| | | |
|---|---|---|
| Line | 359 | 375 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/aplikasi_outlet_bck20190524.php
Method function input_outlet_upload() {

```
....
359.                    $handle =
fopen($_FILES['file_upload']['tmp_name'], "r");
....
375.                          while (($data = fgetcsv($handle, 1000000,
","))  != FALSE)  {
```

**File Disclosure\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=493 |
| Status | New |

The input obtained via upload_outlet in the file application/controllers/aplikasi_outlet_bck20190524.php at line 1123 is used to determine the file to be read by upload_outlet in the file application/controllers/aplikasi_outlet_bck20190524.php at line 1123, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_outlet_bck20190524.php | application/controllers/aplikasi_outlet_bck20190524.php |
| Line | 1198 | 1202 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/aplikasi_outlet_bck20190524.php
Method function upload_outlet(){

```
....
1198.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
1202.                    while (($data = fgetcsv($handle, 1000000,
$separator))  != FALSE)  {
```

**File Disclosure\Path 5:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=494 |
| Status | New |

The input obtained via cm_upload_save in the file application/controllers/maintenance.php at line 4741 is used to determine the file to be read by cm_upload_save in the file application/controllers/maintenance.php at line 4741, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | application/controllers/maintenance.php |
| Line | 4759 | 4763 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/maintenance.php
Method function cm_upload_save(){

```
....
4759.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4763.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 6:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=495 |
| Status | New |

The input obtained via cm_upload_save in the file application/controllers/maintenance_20181213.php at line 4588 is used to determine the file to be read by cm_upload_save in the file application/controllers/maintenance_20181213.php at line 4588, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20181213.php | application/controllers/maintenance_20181213.php |
| Line | 4606 | 4610 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/maintenance_20181213.php
Method function cm_upload_save(){

```
....
4606.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4610.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 7:**

| | |
|---|---|
| Severity | High |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=496 |
| Status | New |

The input obtained via cm_upload_save in the file application/controllers/maintenance_20190524.php at line 4658 is used to determine the file to be read by cm_upload_save in the file application/controllers/maintenance_20190524.php at line 4658, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | application/controllers/maintenance_20190524.php |
| Line | 4676 | 4680 |
| Object | _FILES | handle |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/maintenance_20190524.php |
| Method | function cm_upload_save(){ |

```
....
4676.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4680.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 8:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=497 |
| Status | New |

The input obtained via cm_upload_save in the file application/controllers/maintenance_20190610.php at line 4663 is used to determine the file to be read by cm_upload_save in the file application/controllers/maintenance_20190610.php at line 4663, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | application/controllers/maintenance_20190610.php |
| Line | 4681 | 4685 |
| Object | _FILES | handle |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/maintenance_20190610.php |
| Method | function cm_upload_save(){ |

```
....
4681.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4685.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 9:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=498 |
| Status | New |

The input obtained via cm_upload_save in the file application/controllers/maintenance_bck07112017.php at line 4145 is used to determine the file to be read by cm_upload_save in the file application/controllers/maintenance_bck07112017.php at line 4145, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck07112017.php | application/controllers/maintenance_bck07112017.php |
| Line | 4163 | 4167 |
| Object | _FILES | handle |

Code Snippet

File Name application/controllers/maintenance_bck07112017.php

Method function cm_upload_save(){

```
....
4163.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4167.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 10:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=499 |
| Status | New |

The input obtained via cm_upload_save in the file application/controllers/maintenance_bck20180906.php at line 4568 is used to determine the file to be read by cm_upload_save in the file application/controllers/maintenance_bck20180906.php at line 4568, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20180906.php | application/controllers/maintenance_bck20180906.php |

| | | |
|---|---|---|
| Line | 4586 | 4590 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/maintenance_bck20180906.php
Method function cm_upload_save(){

```
....
4586.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4590.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 11:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=500 |
| Status | New |

The input obtained via cm_upload_save in the file application/controllers/maintenance_bck20190114.php at line 4607 is used to determine the file to be read by cm_upload_save in the file application/controllers/maintenance_bck20190114.php at line 4607, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20190114.php | application/controllers/maintenance_bck20190114.php |
| Line | 4625 | 4629 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/maintenance_bck20190114.php
Method function cm_upload_save(){

```
....
4625.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4629.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 12:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=501 |
| Status | New |

The input obtained via add_clr_upload in the file application/controllers/stock_clr.php at line 98 is used to determine the file to be read by add_clr_upload in the file application/controllers/stock_clr.php at line 98, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/stock_clr.php | application/controllers/stock_clr.php |
| Line | 101 | 109 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/stock_clr.php
Method public function add_clr_upload()

```
....
101.                $handle = fopen($_FILES['upload_csv']['tmp_name'],
"r");
....
109.                      while (($data = fgetcsv($handle, 1000000, ","))
!= FALSE) {
```

**File Disclosure\Path 13:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=502
Status New

The input obtained via add_edc_upload in the file application/controllers/stock_edc.php at line 119 is used to determine the file to be read by add_edc_upload in the file application/controllers/stock_edc.php at line 119, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/stock_edc.php | application/controllers/stock_edc.php |
| Line | 122 | 130 |
| Object | _FILES | handle |

Code Snippet
File Name application/controllers/stock_edc.php
Method public function add_edc_upload()

```
....
122.                $handle = fopen($_FILES['upload_csv']['tmp_name'],
"r");
....
130.                      while (($data = fgetcsv($handle, 1000000, ","))
!= FALSE) {
```

**File Disclosure\Path 14:**

Severity High
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=503 |
| Status | New |

The input obtained via download_file_ in the file application/controllers/super_admin.php at line 78 is used to determine the file to be read by download_file_ in the file application/controllers/super_admin.php at line 78, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |
| Line | 80 | 85 |
| Object | post | dest_file |

Code Snippet
File Name application/controllers/super_admin.php
Method private function download_file_()

```
....
80.         $dest_file = $this->input->post('destination_file');
....
85.         readfile($dest_file);
```

**File Disclosure\Path 15:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=504 |
| Status | New |

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the file to be read by download_file_ in the file application/controllers/super_admin.php at line 78, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/super_admin.php |
| Line | 182 | 85 |
| Object | _POST | dest_file |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/super_admin.php
Method private function download_file_()

```
....
85.         readfile($dest_file);
```

**File Disclosure\Path 16:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=505 |
| Status | New |

The input obtained via <?php in the file application/third_party/dompdf/dompdf.php at line 1 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 197 | 502 |
| Object | _GET | file |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
197.      $file = rawurldecode($_GET["input_file"]);
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 17:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=506 |
| Status | New |

The input obtained via <?php in the file application/third_party/dompdf/dompdf.php at line 1 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 212 | 502 |
| Object | _GET | file |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
212.      $base_path = rawurldecode($_GET["base_path"]);
```

File Name application/third_party/dompdf/include/dompdf.cls.php
Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 18:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=507
Status New

The input obtained via getoptions in the file application/third_party/dompdf/dompdf.php at line 48 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 74 | 502 |
| Object | _SERVER | file |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
74.        $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php
Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this-
>_http_context);
```

**File Disclosure\Path 19:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=508 |
| Status | New |

The input obtained via getoptions in the file application/third_party/dompdf/dompdf.php at line 48 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 81 | 502 |
| Object | _SERVER | file |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
81.        $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this-
>_http_context);
```

**File Disclosure\Path 20:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=509 |
| Status | New |

The input obtained via getoptions in the file application/third_party/dompdf/dompdf.php at line 48 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 88 | 502 |
| Object | _SERVER | file |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
88.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php
Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 21:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=510 |
| Status | New |

The input obtained via getoptions in the file application/third_party/dompdf/dompdf.php at line 48 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 95 | 502 |
| Object | _SERVER | file |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
95.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

| | |
|---|---|
| Method | function load_html_file($file) { |

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 22:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=511 |
| Status | New |

The input obtained via getoptions in the file application/third_party/dompdf/dompdf.php at line 48 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 112 | 502 |
| Object | _SERVER | file |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
112.        $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 23:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=512 |
| Status | New |

The input obtained via getoptions in the file application/third_party/dompdf/dompdf.php at line 48 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 117 | 502 |
| Object | _SERVER | file |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
117.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name application/third_party/dompdf/include/dompdf.cls.php
Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 24:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=513
Status New

The input obtained via <?php in the file system/helpers/dompdf/dompdf.php at line 1 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 198 | 502 |
| Object | _GET | file |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
198.      $file = rawurldecode($_GET["input_file"]);
```

File Name application/third_party/dompdf/include/dompdf.cls.php

| | |
|---|---|
| Method | function load_html_file($file) { |

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 25:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=514 |
| Status | New |

The input obtained via <?php in the file system/helpers/dompdf/dompdf.php at line 1 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 213 | 502 |
| Object | _GET | file |

Code Snippet

| | |
|---|---|
| File Name | system/helpers/dompdf/dompdf.php |
| Method | <?php |

```
....
213.      $base_path = rawurldecode($_GET["base_path"]);
```

| | |
|---|---|
| File Name | application/third_party/dompdf/include/dompdf.cls.php |
| Method | function load_html_file($file) { |

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 26:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=515 |
| Status | New |

The input obtained via getoptions in the file system/helpers/dompdf/dompdf.php at line 49 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 75 | 502 |
| Object | _SERVER | file |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
75.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php
Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 27:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=516
Status New

The input obtained via getoptions in the file system/helpers/dompdf/dompdf.php at line 49 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 82 | 502 |
| Object | _SERVER | file |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
82.         $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

| | |
|---|---|
| Method | function load_html_file($file) { |

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 28:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=517 |
| Status | New |

The input obtained via getoptions in the file system/helpers/dompdf/dompdf.php at line 49 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 89 | 502 |
| Object | _SERVER | file |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
89.        $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 29:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=518 |
| Status | New |

The input obtained via getoptions in the file system/helpers/dompdf/dompdf.php at line 49 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 96 | 502 |
| Object | _SERVER | file |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
96.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php
Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 30:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=519 |
| Status | New |

The input obtained via getoptions in the file system/helpers/dompdf/dompdf.php at line 49 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 113 | 502 |
| Object | _SERVER | file |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
113.         $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

| | |
|---|---|
| Method | function load_html_file($file) { |

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 31:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=520 |
| Status | New |

The input obtained via getoptions in the file system/helpers/dompdf/dompdf.php at line 49 is used to determine the file to be read by load_html_file in the file application/third_party/dompdf/include/dompdf.cls.php at line 467, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 118 | 502 |
| Object | _SERVER | file |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
118.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

**File Disclosure\Path 32:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=521 |
| Status | New |

The input obtained via <?php in the file system/helpers/dompdf/www/controller.php at line 1 is used to determine the file to be read by register_font in the file application/third_party/dompdf/include/font_metrics.cls.php at line 309, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/controller.php | application/third_party/dompdf/include/font_metrics.cls.php |
| Line | 22 | 331 |
| Object | _FILES | remote_file |

Code Snippet
File Name system/helpers/dompdf/www/controller.php
Method <?php

```
....
22.      $data = $_FILES["file"];
```

File Name application/third_party/dompdf/include/font_metrics.cls.php
Method static function register_font($style, $remote_file) {

```
....
331.          file_put_contents($local_file,
file_get_contents($remote_file));
```

**File Disclosure\Path 33:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=522
Status New

The input obtained via explode_url in the file application/third_party/dompdf/include/functions.inc.php at line 179 is used to determine the file to be read by load_css_file in the file application/third_party/dompdf/include/stylesheet.cls.php at line 280, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/stylesheet.cls.php |
| Line | 254 | 310 |
| Object | _SERVER | file |

Code Snippet
File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
254.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

| | |
|---|---|
| File Name | application/third_party/dompdf/include/stylesheet.cls.php |
| Method | function load_css_file($file, $origin = self::ORIG_AUTHOR) { |

```
....
310.        $css = file_get_contents($file, null, $this->_dompdf-
>get_http_context());
```

**File Disclosure\Path 34:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=523 |
| Status | New |

The input obtained via explode_url in the file system/helpers/dompdf/include/functions.inc.php at line 163 is used to determine the file to be read by load_css_file in the file application/third_party/dompdf/include/stylesheet.cls.php at line 280, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/stylesheet.cls.php |
| Line | 231 | 310 |
| Object | _SERVER | file |

Code Snippet

| | |
|---|---|
| File Name | system/helpers/dompdf/include/functions.inc.php |
| Method | function explode_url($url) { |

```
....
231.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

| | |
|---|---|
| File Name | application/third_party/dompdf/include/stylesheet.cls.php |
| Method | function load_css_file($file, $origin = self::ORIG_AUTHOR) { |

```
....
310.        $css = file_get_contents($file, null, $this->_dompdf-
>get_http_context());
```

**File Disclosure\Path 35:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=524 |
| Status | New |

The input obtained via input_outlet_upload in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet.php at line 347 is used to

determine the file to be read by input_outlet_upload in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet.php at line 347, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet.php |
| Line | 360 | 376 |
| Object | _FILES | handle |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet.php
Method function input_outlet_upload() {

```
....
360.                    $handle =
fopen($_FILES['file_upload']['tmp_name'], "r");
....
376.                          while (($data = fgetcsv($handle, 1000000,
","))  != FALSE)  {
```

**File Disclosure\Path 36:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=525 |
| Status | New |

The input obtained via upload_outlet in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet.php at line 1124 is used to determine the file to be read by upload_outlet in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet.php at line 1124, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet.php |
| Line | 1199 | 1203 |
| Object | _FILES | handle |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet.php
Method function upload_outlet(){

```
....
1199.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
1203.                    while (($data = fgetcsv($handle, 1000000,
$separator))  != FALSE)  {
```

**File Disclosure\Path 37:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=526 |
| Status | New |

The input obtained via input_outlet_upload in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet_bck20190524.php at line 346 is used to determine the file to be read by input_outlet_upload in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet_bck20190524.php at line 346, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet_bck20190524.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet_bck20190524.php |
| Line | 359 | 375 |
| Object | _FILES | handle |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet_bck20190524.php

Method function input_outlet_upload() {

```
....
359.                    $handle =
fopen($_FILES['file_upload']['tmp_name'], "r");
....
375.                            while (($data = fgetcsv($handle, 1000000,
","))  != FALSE)  {
```

**File Disclosure\Path 38:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=527 |
| Status | New |

The input obtained via upload_outlet in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet_bck20190524.php at line 1123 is used to determine the file to be read by upload_outlet in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet_bck20190524.php at line 1123, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet_bck20190524.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet_bck20190524.php |
| Line | 1198 | 1202 |

| | | |
|---|---|---|
| Object | _FILES | handle |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/aplikasi_outlet_bck20190524.php
Method function upload_outlet(){

```
....
1198.            $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
1202.                 while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 39:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=528
Status New

The input obtained via cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php at line 4731 is used to determine the file to be read by cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php at line 4731, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php |
| Line | 4749 | 4753 |
| Object | _FILES | handle |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php
Method function cm_upload_save(){

```
....
4749.            $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4753.                 while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 40:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=529
Status New

The input obtained via cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php at line 4588 is used to determine the file to be read by cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php at line 4588, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php |
| Line | 4606 | 4610 |
| Object | _FILES | handle |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php
Method function cm_upload_save(){

```
....
4606.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4610.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 41:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=530
Status New

The input obtained via cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php at line 4658 is used to determine the file to be read by cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php at line 4658, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php |
| Line | 4676 | 4680 |
| Object | _FILES | handle |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php
Method function cm_upload_save(){

```
....
4676.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4680.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 42:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=531 |
| Status | New |

The input obtained via cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php at line 4663 is used to determine the file to be read by cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php at line 4663, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php |
| Line | 4681 | 4685 |
| Object | _FILES | handle |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php

Method function cm_upload_save(){

```
....
4681.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4685.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 43:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=532 |
| Status | New |

The input obtained via cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php at line 4145 is used to determine the file to be read by cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php at line 4145, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php |
| Line | 4163 | 4167 |
| Object | _FILES | handle |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php
Method function cm_upload_save(){

```
....
4163.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4167.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 44:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=533 |
| Status | New |

The input obtained via cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php at line 4568 is used to determine the file to be read by cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php at line 4568, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php |
| Line | 4586 | 4590 |
| Object | _FILES | handle |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php
Method function cm_upload_save(){

```
....
4586.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4590.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 45:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=534 |
| Status | New |

The input obtained via cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php at line 4607 is used to determine the file to be read by cm_upload_save in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php at line 4607, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php |
| Line | 4625 | 4629 |
| Object | _FILES | handle |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php

Method function cm_upload_save(){

```
....
4625.             $handle = fopen($_FILES['file_upload']['tmp_name'],
"r");
....
4629.                   while (($data = fgetcsv($handle, 1000000,
$separator)) != FALSE) {
```

**File Disclosure\Path 46:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=535 |
| Status | New |

The input obtained via add_clr_upload in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock_clr.php at line 98 is used to determine the file to be read by add_clr_upload in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock_clr.php at line 98, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock_clr.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock_clr.php |
| Line | 101 | 109 |
| Object | _FILES | handle |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock_clr.php |
| Method | public function add_clr_upload() |

```
....
101.                $handle = fopen($_FILES['upload_csv']['tmp_name'],
"r");
....
109.                      while (($data = fgetcsv($handle, 1000000, ","))
!= FALSE) {
```

**File Disclosure\Path 47:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=536 |
| Status | New |

The input obtained via add_edc_upload in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock_edc.php at line 119 is used to determine the file to be read by add_edc_upload in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock_edc.php at line 119, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock_edc.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock_edc.php |
| Line | 122 | 130 |
| Object | _FILES | handle |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock_edc.php |
| Method | public function add_edc_upload() |

```
....
122.                $handle = fopen($_FILES['upload_csv']['tmp_name'],
"r");
....
130.                      while (($data = fgetcsv($handle, 1000000, ","))
!= FALSE) {
```

**File Disclosure\Path 48:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=537 |
| Status | New |

The input obtained via download_file_ in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php at line 78 is used to determine the file to be read by download_file_ in the file

BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php at line 78, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 80 | 85 |
| Object | post | dest_file |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php
Method private function download_file_()

```
....
80.         $dest_file = $this->input->post('destination_file');
....
85.         readfile($dest_file);
```

**File Disclosure\Path 49:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=538
Status New

The input obtained via post in the file system/core/Input.php at line 172 is used to determine the file to be read by download_file_ in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php at line 78, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 182 | 85 |
| Object | _POST | dest_file |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php
Method private function download_file_()

```
....
85.         readfile($dest_file);
```

**File Disclosure\Path 50:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=539 |
| Status | New |

The input obtained via <?php in the file application/third_party/dompdf/dompdf.php at line 1 is used to determine the file to be read by load_html_file in the file system/helpers/dompdf/include/dompdf.cls.php at line 335, potentially disclosing the contents of that file.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 197 | 364 |
| Object | _GET | file |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
197.      $file = rawurldecode($_GET["input_file"]);
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html_file($file) {

```
....
364.      $contents = file_get_contents($file, null, $this->_http_context);
```

## Command Injection

Query Path:

PHP\Cx\PHP High Risk\Command Injection Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

*Description*

**Command Injection\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=1 |
| Status | New |

The application's pks method calls an OS (shell) command with exec, at line 33 of application/controllers/cetak.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the pks method, at line 33 of application/controllers/cetak.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/cetak.php | application/controllers/cetak.php |
| Line | 40 | 103 |
| Object | post | exec |

Code Snippet
File Name application/controllers/cetak.php
Method public function pks()

```
....
40.                 $appId = $this->input->post('appid');
....
103.                                  exec('wkhtmltopdf -T 1cm -R 1cm -L
1cm -B 1cm --disable-smart-shrinking  --page-size A4
http://172.18.44.66/index.php/cetak_process/pks/'.$appId.'
/var/www/template_formulir/pks/'.$filename.' 2>&1');
```

**Command Injection\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=2 |
| Status | New |

The application's pks method calls an OS (shell) command with exec, at line 33 of application/controllers/cetak.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/cetak.php |
| Line | 182 | 103 |
| Object | _POST | exec |

Code Snippet
File Name system/core/Input.php

| | |
|---|---|
| Method | function post($index = NULL, $xss_clean = FALSE) |

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

| | |
|---|---|
| File Name | application/controllers/cetak.php |
| Method | public function pks() |

```
....
103.                                exec('wkhtmltopdf -T 1cm -R 1cm -L
1cm -B 1cm --disable-smart-shrinking  --page-size A4
http://172.18.44.66/index.php/cetak_process/pks/'.$appId.'
/var/www/template_formulir/pks/'.$filename.' 2>&1');
```

**Command Injection\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=3 |
| Status | New |

The application's addendum method calls an OS (shell) command with exec, at line 149 of application/controllers/cetak.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/cetak.php |
| Line | 182 | 200 |
| Object | _POST | exec |

| | |
|---|---|
| Code Snippet | |
| File Name | system/core/Input.php |
| Method | function post($index = NULL, $xss_clean = FALSE) |

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

| | |
|---|---|
| File Name | application/controllers/cetak.php |
| Method | public function addendum() |

```
....
200.                            exec('wkhtmltopdf -T 1cm -R 1cm -L 1cm -B
1cm --disable-smart-shrinking  --page-size A4
http://172.18.44.66/index.php/cetak_process/addendum/'.$app_id.'
/var/www/template_formulir/addendum/'.$filename.' 2>&1');
```

**Command Injection\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=4 |
| Status | New |

The application's daftar_save method calls an OS (shell) command with exec, at line 196 of application/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 237 |
| Object | _POST | exec |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method public function daftar_save()

```
....
237.                                exec('wkhtmltopdf -T 10 -R 10 -L 10
-B 35 -O landscape --footer-spacing 5 --footer-html ' . $footer_html . '
--disable-smart-shrinking --page-size legal ' . $filerk . ' ' .
$result_file[0] . ' 2>&1');
```

**Command Injection\Path 5:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=5 |
| Status | New |

The application's daftar_save method calls an OS (shell) command with exec, at line 196 of application/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 238 |
| Object | _POST | exec |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method public function daftar_save()

```
....
238.                                exec('wkhtmltopdf -T 10 -R 10 -L 5 -
B 35 -O landscape --footer-spacing 5 --footer-html ' . $footer_html . '
--disable-smart-shrinking --page-size legal ' . $filedetail . ' ' .
$result_file[1] . ' 2>&1');
```

**Command Injection\Path 6:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=6 |
| Status | New |

The application's generate_file method calls an OS (shell) command with exec, at line 931 of application/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 966 |
| Object | _POST | exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method function generate_file($data) {

```
....
966.                            exec('wkhtmltopdf -T 10 -R 10 -L 10 -B 35
-O landscape --footer-spacing 5 --footer-html ' . $footer_html . ' --
disable-smart-shrinking --page-size legal ' . $filerk . ' ' .
$result_file[0] . ' 2>&1');
```

**Command Injection\Path 7:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7
Status New

The application's generate_file method calls an OS (shell) command with exec, at line 931 of application/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 967 |
| Object | _POST | exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method function generate_file($data) {

```
....
967.                            exec('wkhtmltopdf -T 10 -R 10 -L 5 -B 35 -
O landscape --footer-spacing 5 --footer-html ' . $footer_html . ' --
disable-smart-shrinking --page-size legal ' . $filedetail . ' ' .
$result_file[1] . ' 2>&1');
```

**Command Injection\Path 8:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=8 |
| Status | New |

The application's detail method calls an OS (shell) command with shell_exec, at line 257 of application/controllers/email_blast.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/email_blast.php |
| Line | 182 | 269 |
| Object | _POST | shell_exec |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/email_blast.php

Method public function detail(){

```
....
269.                                        shell_exec('php
/var/www/mms/index.php scheduler email_blast_approved_proccess '.$this-
>input->post('id').' >>
/home/administrator/mms_logs/email_blast_approved_process_'.$this-
>input->post('id').'.log');
```

**Command Injection\Path 9:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=9 |
| Status | New |

The application's write_file_ method calls an OS (shell) command with shell_exec, at line 48 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/super_admin.php |
| Line | 182 | 61 |
| Object | _POST | shell_exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/super_admin.php
Method private function write_file_($is_redirect_explore = '0')

```
....
61.         $chmod_get_dir = trim(shell_exec('sudo stat -c %a
'.$get_dir.' 2>&1'));
```

**Command Injection\Path 10:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10 |
| Status | New |

The application's write_file_ method calls an OS (shell) command with shell_exec, at line 48 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/super_admin.php |
| Line | 182 | 63 |
| Object | _POST | shell_exec |

Code Snippet
File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/super_admin.php

Method private function write_file_($is_redirect_explore = '0')

```
....
63.         shell_exec('sudo chmod -R 777 '.$get_dir.' 2>&1');
```

**Command Injection\Path 11:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11 |
| Status | New |

The application's write_file_ method calls an OS (shell) command with shell_exec, at line 48 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/super_admin.php |
| Line | 182 | 73 |
| Object | _POST | shell_exec |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/super_admin.php

Method private function write_file_($is_redirect_explore = '0')

```
....
73.         shell_exec('sudo chmod -R '.$chmod_get_dir.' '.$get_dir.'
2>&1');
```

**Command Injection\Path 12:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=12 |
| Status | New |

The application's syntax_file_ method calls an OS (shell) command with shell_exec, at line 89 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/super_admin.php |
| Line | 182 | 92 |
| Object | _POST | shell_exec |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/super_admin.php

Method private function syntax_file_()

```
....
92.         return "<pre>".shell_exec($cm)."</pre>";
```

**Command Injection\Path 13:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13 |
| Status | New |

The application's query_file_ method calls an OS (shell) command with shell_exec, at line 95 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/super_admin.php |
| Line | 182 | 104 |

| | | |
|---|---|---|
| Object | _POST | shell_exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/super_admin.php

Method private function query_file_()

```
....
104.              $result_exec = shell_exec($shell_exec." 2>&1");
```

**Command Injection\Path 14:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14
Status New

The application's explore_file_ method calls an OS (shell) command with shell_exec, at line 114 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/super_admin.php |
| Line | 182 | 143 |
| Object | _POST | shell_exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/super_admin.php

Method public function explore_file_($is_redirect_from_write = '0')

```
....
143.                $get_all = shell_exec('sudo ls -a '.$data['path'].'
');
```

**Command Injection\Path 15:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=15 |
| Status | New |

The application's explore_file_ method calls an OS (shell) command with shell_exec, at line 114 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/super_admin.php |
| Line | 182 | 146 |
| Object | _POST | shell_exec |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/super_admin.php

Method public function explore_file_($is_redirect_from_write = '0')

```
....
146.                $get_file = shell_exec('sudo ls -p '.$data['path'].' |
grep -v /');
```

**Command Injection\Path 16:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=16 |
| Status | New |

The application's pks method calls an OS (shell) command with exec, at line 33 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php |
| Line | 182 | 103 |
| Object | _POST | exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php
Method public function pks()

```
....
103.                                exec('wkhtmltopdf -T 1cm -R 1cm -L
1cm -B 1cm --disable-smart-shrinking  --page-size A4
http://172.18.44.66/index.php/cetak_process/pks/'.$appId.'
/var/www/template_formulir/pks/'.$filename.' 2>&1');
```

**Command Injection\Path 17:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17
Status New

The application's addendum method calls an OS (shell) command with exec, at line 149 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php |
| Line | 182 | 200 |
| Object | _POST | exec |

Code Snippet

| | |
|---|---|
| File Name | system/core/Input.php |
| Method | function post($index = NULL, $xss_clean = FALSE) |

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php |
| Method | public function addendum() |

```
....
200.                            exec('wkhtmltopdf -T 1cm -R 1cm -L 1cm -B
1cm --disable-smart-shrinking  --page-size A4
http://172.18.44.66/index.php/cetak_process/addendum/'.$app_id.'
/var/www/template_formulir/addendum/'.$filename.' 2>&1');
```

**Command Injection\Path 18:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18 |
| Status | New |

The application's daftar_save method calls an OS (shell) command with exec, at line 193 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php |
| Line | 182 | 233 |
| Object | _POST | exec |

Code Snippet

| | |
|---|---|
| File Name | system/core/Input.php |
| Method | function post($index = NULL, $xss_clean = FALSE) |

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php |
| Method | public function daftar_save() |

```
....
233.                                exec('wkhtmltopdf -T 10 -R 10 -L 10
-B 35 -O landscape --footer-spacing 5 --footer-html '.$footer_html.' --
disable-smart-shrinking --page-size A4 '.$filerk.' '.$result_file[0].'
2>&1');
```

**Command Injection\Path 19:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=19 |
| Status | New |

The application's daftar_save method calls an OS (shell) command with exec, at line 193 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php |
| Line | 182 | 234 |
| Object | _POST | exec |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php

Method public function daftar_save()

```
....
234.                                exec('wkhtmltopdf -T 10 -R 10 -L 10
-B 35 -O landscape --footer-spacing 5 --footer-html '.$footer_html.' --
disable-smart-shrinking --page-size A4 '.$filedetail.'
'.$result_file[1].' 2>&1');
```

**Command Injection\Path 20:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=20 |

| Status | New |
|---|---|

The application's generate_file method calls an OS (shell) command with exec, at line 890 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php |
| Line | 182 | 924 |
| Object | _POST | exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php
Method function generate_file($data) {

```
....
924.                            exec('wkhtmltopdf -T 10 -R 10 -L 10 -B 35 -O landscape --footer-spacing 5 --footer-html ' . $footer_html . ' --disable-smart-shrinking --page-size A4 ' . $filerk . ' ' . $result_file[0] . ' 2>&1');
```

**Command Injection\Path 21:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=21 |
| Status | New |

The application's generate_file method calls an OS (shell) command with exec, at line 890 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/contro |

| | | |
|---|---|---|
| | | llers/controllers/ebor.php |
| Line | 182 | 925 |
| Object | _POST | exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php
Method function generate_file($data) {

```
....
925.                            exec('wkhtmltopdf -T 10 -R 10 -L 10 -B 35
-O landscape --footer-spacing 5 --footer-html ' . $footer_html . ' --
disable-smart-shrinking --page-size A4 ' . $filedetail . ' ' .
$result_file[1] . ' 2>&1');
```

**Command Injection\Path 22:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22 |
| Status | New |

The application's detail method calls an OS (shell) command with shell_exec, at line 257 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/email_blast.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/email_blast.php |
| Line | 182 | 269 |
| Object | _POST | shell_exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/email_blast.php

Method public function detail(){

```
....
269.                                        shell_exec('php
/var/www/mms/index.php scheduler email_blast_approved_proccess '.$this-
>input->post('id').' >>
/home/administrator/mms_logs/email_blast_approved_process_'.$this-
>input->post('id').'.log');
```

**Command Injection\Path 23:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23 |
| Status | New |

The application's write_file_ method calls an OS (shell) command with shell_exec, at line 48 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 182 | 61 |
| Object | _POST | shell_exec |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php

Method private function write_file_($is_redirect_explore = '0')

```
....
61.         $chmod_get_dir = trim(shell_exec('sudo stat -c %a
'.$get_dir.' 2>&1'));
```

**Command Injection\Path 24:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=24 |
| Status | New |

The application's write_file_ method calls an OS (shell) command with shell_exec, at line 48 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 182 | 63 |
| Object | _POST | shell_exec |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php

Method private function write_file_($is_redirect_explore = '0')

```
....
63.         shell_exec('sudo chmod -R 777 '.$get_dir.' 2>&1');
```

**Command Injection\Path 25:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=25 |
| Status | New |

The application's write_file_ method calls an OS (shell) command with shell_exec, at line 48 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 182 | 73 |
| Object | _POST | shell_exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php
Method private function write_file_($is_redirect_explore = '0')

```
....
73.         shell_exec('sudo chmod -R '.$chmod_get_dir.' '.$get_dir.'
2>&1');
```

**Command Injection\Path 26:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=26 |
| Status | New |

The application's syntax_file_ method calls an OS (shell) command with shell_exec, at line 89 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 182 | 92 |

| | | |
|---|---|---|
| Object | _POST | shell_exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php
Method private function syntax_file_()

```
....
92.         return "<pre>".shell_exec($cm)."</pre>";
```

**Command Injection\Path 27:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=27
Status New

The application's query_file_ method calls an OS (shell) command with shell_exec, at line 95 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 182 | 104 |
| Object | _POST | shell_exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php
Method private function query_file_()

```
....
104.                $result_exec = shell_exec($shell_exec." 2>&1");
```

**Command Injection\Path 28:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=28 |
| Status | New |

The application's explore_file_ method calls an OS (shell) command with shell_exec, at line 114 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 182 | 143 |
| Object | _POST | shell_exec |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php

Method public function explore_file_($is_redirect_from_write = '0')

```
....
143.                $get_all = shell_exec('sudo ls -a '.$data['path'].'
');
```

**Command Injection\Path 29:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=29 |
| Status | New |

The application's explore_file_ method calls an OS (shell) command with shell_exec, at line 114 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _POST, which is retrieved by the application in the post method, at line 172 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 182 | 146 |
| Object | _POST | shell_exec |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php
Method public function explore_file_($is_redirect_from_write = '0')

```
....
146.                $get_file = shell_exec('sudo ls -p '.$data['path'].' | grep -v /');
```

**Command Injection\Path 30:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=30 |
| Status | New |

The application's addendum method calls an OS (shell) command with exec, at line 149 of application/controllers/cetak.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the addendum method, at line 149 of application/controllers/cetak.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/cetak.php | application/controllers/cetak.php |
| Line | 156 | 200 |
| Object | post | exec |

Code Snippet
File Name application/controllers/cetak.php
Method public function addendum()

```
....
156.                    $app_id     = $this->input->post('app_id');
....
200.                          exec('wkhtmltopdf -T 1cm -R 1cm -L 1cm -B
1cm --disable-smart-shrinking  --page-size A4
http://172.18.44.66/index.php/cetak_process/addendum/'.$app_id.'
/var/www/template_formulir/addendum/'.$filename.' 2>&1');
```

**Command Injection\Path 31:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=31
Status New

The application's daftar_save method calls an OS (shell) command with exec, at line 196 of application/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the daftar_save method, at line 196 of application/controllers/ebor.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 199 | 237 |
| Object | post | exec |

Code Snippet
File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
199.              $mid        = $this->input->post('mid');
....
237.                                exec('wkhtmltopdf -T 10 -R 10 -L 10
-B 35 -O landscape --footer-spacing 5 --footer-html ' . $footer_html . '
--disable-smart-shrinking --page-size legal ' . $filerk . ' ' .
$result_file[0] . ' 2>&1');
```

**Command Injection\Path 32:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=32
Status New

The application's daftar_save method calls an OS (shell) command with exec, at line 196 of application/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the daftar_save method, at line 196 of application/controllers/ebor.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 199 | 238 |
| Object | post | exec |

Code Snippet
File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
199.              $mid        = $this->input->post('mid');
....
238.                                exec('wkhtmltopdf -T 10 -R 10 -L 5 -
B 35 -O landscape --footer-spacing 5 --footer-html ' . $footer_html . '
--disable-smart-shrinking --page-size legal ' . $filedetail . ' ' .
$result_file[1] . ' 2>&1');
```

**Command Injection\Path 33:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=33
Status New

The application's daftar_save method calls an OS (shell) command with exec, at line 196 of application/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the daftar_save method, at line 196 of application/controllers/ebor.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 201 | 237 |
| Object | post | exec |

Code Snippet
File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
201.              $tgl        = $this->input->post('tgl');
....
237.                                exec('wkhtmltopdf -T 10 -R 10 -L 10
-B 35 -O landscape --footer-spacing 5 --footer-html ' . $footer_html . '
--disable-smart-shrinking --page-size legal ' . $filerk . ' ' .
$result_file[0] . ' 2>&1');
```

**Command Injection\Path 34:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=34 |
| Status | New |

The application's daftar_save method calls an OS (shell) command with exec, at line 196 of application/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the daftar_save method, at line 196 of application/controllers/ebor.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 201 | 238 |
| Object | post | exec |

Code Snippet
File Name application/controllers/ebor.php
Method public function daftar_save()

```
....
201.              $tgl        = $this->input->post('tgl');
....
238.                                exec('wkhtmltopdf -T 10 -R 10 -L 5 -
B 35 -O landscape --footer-spacing 5 --footer-html ' . $footer_html . '
--disable-smart-shrinking --page-size legal ' . $filedetail . ' ' .
$result_file[1] . ' 2>&1');
```

**Command Injection\Path 35:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=35 |
| Status | New |

The application's generate_file method calls an OS (shell) command with exec, at line 931 of application/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _GET, which is retrieved by the application in the get method, at line 144 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 154 | 966 |
| Object | _GET | exec |

Code Snippet

File Name system/core/Input.php
Method function get($index = NULL, $xss_clean = FALSE)

```
....
154.                            $get[$key] = $this-
>_fetch_from_array($_GET, $key, $xss_clean);
```

File Name application/controllers/ebor.php
Method function generate_file($data) {

```
....
966.                            exec('wkhtmltopdf -T 10 -R 10 -L 10 -B 35
-O landscape --footer-spacing 5 --footer-html ' . $footer_html . ' --
disable-smart-shrinking --page-size legal ' . $filerk . ' ' .
$result_file[0] . ' 2>&1');
```

**Command Injection\Path 36:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=36 |
| Status | New |

The application's generate_file method calls an OS (shell) command with exec, at line 931 of application/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _GET, which is retrieved by the application in the get method, at line 144 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 154 | 967 |
| Object | _GET | exec |

Code Snippet
File Name system/core/Input.php
Method function get($index = NULL, $xss_clean = FALSE)

```
....
154.                            $get[$key] = $this-
>_fetch_from_array($_GET, $key, $xss_clean);
```

File Name application/controllers/ebor.php
Method function generate_file($data) {

```
....
967.                            exec('wkhtmltopdf -T 10 -R 10 -L 5 -B 35 -
O landscape --footer-spacing 5 --footer-html ' . $footer_html . ' --
disable-smart-shrinking --page-size legal ' . $filedetail . ' ' .
$result_file[1] . ' 2>&1');
```

**Command Injection\Path 37:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=37 |
| Status | New |

The application's generate_file method calls an OS (shell) command with exec, at line 890 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _GET, which is retrieved by the application in the get method, at line 144 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php |
| Line | 154 | 924 |
| Object | _GET | exec |

Code Snippet

File Name system/core/Input.php

Method function get($index = NULL, $xss_clean = FALSE)

```
....
154.                            $get[$key] = $this-
>_fetch_from_array($_GET, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php

Method function generate_file($data) {

```
....
924.                            exec('wkhtmltopdf -T 10 -R 10 -L 10 -B 35
-O landscape --footer-spacing 5 --footer-html ' . $footer_html . ' --
disable-smart-shrinking --page-size A4 ' . $filerk . ' ' .
$result_file[0] . ' 2>&1');
```

**Command Injection\Path 38:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=38 |

| Status | New |
|---|---|

The application's generate_file method calls an OS (shell) command with exec, at line 890 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _GET, which is retrieved by the application in the get method, at line 144 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php |
| Line | 154 | 925 |
| Object | _GET | exec |

Code Snippet
File Name system/core/Input.php
Method function get($index = NULL, $xss_clean = FALSE)

```
....
154.                            $get[$key] = $this-
>_fetch_from_array($_GET, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php
Method function generate_file($data) {

```
....
925.                            exec('wkhtmltopdf -T 10 -R 10 -L 10 -B 35
-O landscape --footer-spacing 5 --footer-html ' . $footer_html . ' --
disable-smart-shrinking --page-size A4 ' . $filedetail . ' ' .
$result_file[1] . ' 2>&1');
```

**Command Injection\Path 39:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=39 |
| Status | New |

The application's detail method calls an OS (shell) command with shell_exec, at line 257 of application/controllers/email_blast.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the detail method, at line 257 of application/controllers/email_blast.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/email_blast.php | application/controllers/email_blast.php |

| | | |
|---|---|---|
| Line | 269 | 269 |
| Object | post | shell_exec |

Code Snippet
File Name application/controllers/email_blast.php
Method public function detail(){

```
....
269.                                        shell_exec('php
/var/www/mms/index.php scheduler email_blast_approved_proccess '.$this-
>input->post('id').' >>
/home/administrator/mms_logs/email_blast_approved_process_'.$this-
>input->post('id').'.log');
```

**Command Injection\Path 40:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=40 |
| Status | New |

The application's detail method calls an OS (shell) command with shell_exec, at line 257 of application/controllers/email_blast.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the detail method, at line 257 of application/controllers/email_blast.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/email_blast.php | application/controllers/email_blast.php |
| Line | 269 | 269 |
| Object | post | shell_exec |

Code Snippet
File Name application/controllers/email_blast.php
Method public function detail(){

```
....
269.                                        shell_exec('php
/var/www/mms/index.php scheduler email_blast_approved_proccess '.$this-
>input->post('id').' >>
/home/administrator/mms_logs/email_blast_approved_process_'.$this-
>input->post('id').'.log');
```

**Command Injection\Path 41:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=41 |
| Status | New |

The application's ebor_gmail_start_csv method calls an OS (shell) command with shell_exec, at line 1927 of application/controllers/scheduler.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, _SERVER, which is retrieved by the application in the ebor_gmail_start_csv method, at line 1927 of application/controllers/scheduler.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/scheduler.php | application/controllers/scheduler.php |
| Line | 1929 | 1964 |
| Object | _SERVER | shell_exec |

Code Snippet
File Name application/controllers/scheduler.php
Method function ebor_gmail_start_csv($tgl_trx = '')

```
....
1929.             if(isset($_SERVER['argv'][3])) $tgl_trx =
$_SERVER['argv'][3];
....
1964.                          shell_exec('nohup php
/var/www/mms/index.php scheduler ebor_gmail_run_csv '.$tgl_trx.' 1 100 0
>> /home/administrator/mms/log/ebor_gmail_run_csv_'.$tgl_trx.'.log');
```

**Command Injection\Path 42:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=42
Status New

The application's write_file_ method calls an OS (shell) command with shell_exec, at line 48 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the write_file_ method, at line 48 of application/controllers/super_admin.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |
| Line | 50 | 61 |
| Object | post | shell_exec |

Code Snippet
File Name application/controllers/super_admin.php
Method private function write_file_($is_redirect_explore = '0')

```
....
50.         $dest_file = $this->input->post('destination_file');
....
61.         $chmod_get_dir = trim(shell_exec('sudo stat -c %a
'.$get_dir.' 2>&1'));
```

**Command Injection\Path 43:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=43 |
| Status | New |

The application's write_file_ method calls an OS (shell) command with shell_exec, at line 48 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the write_file_ method, at line 48 of application/controllers/super_admin.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |
| Line | 50 | 63 |
| Object | post | shell_exec |

Code Snippet

File Name application/controllers/super_admin.php

Method private function write_file_($is_redirect_explore = '0')

```
....
50.         $dest_file = $this->input->post('destination_file');
....
63.         shell_exec('sudo chmod -R 777 '.$get_dir.' 2>&1');
```

**Command Injection\Path 44:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=44 |
| Status | New |

The application's write_file_ method calls an OS (shell) command with shell_exec, at line 48 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the write_file_ method, at line 48 of application/controllers/super_admin.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |

| | | |
|---|---|---|
| Line | 50 | 73 |
| Object | post | shell_exec |

Code Snippet
File Name application/controllers/super_admin.php
Method private function write_file_($is_redirect_explore = '0')

```
....
50.         $dest_file = $this->input->post('destination_file');
....
73.         shell_exec('sudo chmod -R '.$chmod_get_dir.' '.$get_dir.'
2>&1');
```

**Command Injection\Path 45:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=45 |
| Status | New |

The application's syntax_file_ method calls an OS (shell) command with shell_exec, at line 89 of application/controllers/super_admin.php, using an untrusted string with the command to execute. This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the syntax_file_ method, at line 89 of application/controllers/super_admin.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |
| Line | 91 | 92 |
| Object | post | shell_exec |

Code Snippet
File Name application/controllers/super_admin.php
Method private function syntax_file_()

```
....
91.         $cm = $this->input->post('syntax_file')." 2>&1";
92.         return "<pre>".shell_exec($cm)."</pre>";
```

**Command Injection\Path 46:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=46 |
| Status | New |

The application's query_file_ method calls an OS (shell) command with shell_exec, at line 95 of application/controllers/super_admin.php, using an untrusted string with the command to execute. This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the query_file_ method, at line 95 of application/controllers/super_admin.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |
| Line | 97 | 104 |
| Object | post | shell_exec |

Code Snippet
File Name application/controllers/super_admin.php
Method private function query_file_()

```
....
97.         $ip = $this->input->post('ip_host');
....
104.              $result_exec = shell_exec($shell_exec." 2>&1");
```

**Command Injection\Path 47:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=47
Status New

The application's query_file_ method calls an OS (shell) command with shell_exec, at line 95 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the query_file_ method, at line 95 of application/controllers/super_admin.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |
| Line | 98 | 104 |
| Object | post | shell_exec |

Code Snippet
File Name application/controllers/super_admin.php
Method private function query_file_()

```
....
98.         $user = $this->input->post('user_host');
....
104.              $result_exec = shell_exec($shell_exec." 2>&1");
```

**Command Injection\Path 48:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=48

| | |
|---|---|
| Status | New |

The application's query_file_ method calls an OS (shell) command with shell_exec, at line 95 of application/controllers/super_admin.php, using an untrusted string with the command to execute. This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the query_file_ method, at line 95 of application/controllers/super_admin.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |
| Line | 99 | 104 |
| Object | post | shell_exec |

Code Snippet
File Name application/controllers/super_admin.php
Method private function query_file_()

```
....
99.         $pass = $this->input->post('pass_host');
....
104.              $result_exec = shell_exec($shell_exec." 2>&1");
```

**Command Injection\Path 49:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=49 |
| Status | New |

The application's query_file_ method calls an OS (shell) command with shell_exec, at line 95 of application/controllers/super_admin.php, using an untrusted string with the command to execute. This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the query_file_ method, at line 95 of application/controllers/super_admin.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |
| Line | 100 | 104 |
| Object | post | shell_exec |

Code Snippet
File Name application/controllers/super_admin.php
Method private function query_file_()

```
....
100.              $qry = $this->input->post('syntax_file');
....
104.              $result_exec = shell_exec($shell_exec." 2>&1");
```

**Command Injection\Path 50:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=50 |
| Status | New |

The application's explore_file_ method calls an OS (shell) command with shell_exec, at line 114 of application/controllers/super_admin.php, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, post, which is retrieved by the application in the explore_file_ method, at line 114 of application/controllers/super_admin.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |
| Line | 123 | 143 |
| Object | post | shell_exec |

Code Snippet
File Name application/controllers/super_admin.php
Method public function explore_file_($is_redirect_from_write = '0')

```
....
123.                    $dest_file = $this->input-
>post('destination_file');
....
143.              $get_all = shell_exec('sudo ls -a '.$data['path'].'
');
```

## Code Injection

Query Path:
PHP\Cx\PHP High Risk\Code Injection Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

*Description*

**Code Injection\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=74 |
| Status | New |

The application's invoke_method method receives and dynamically executes user-controlled code using call_arg, at line 493 of application/libraries/nusoap/class.soap_server.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the parse_http_headers method, at line 320 of application/libraries/nusoap/class.soap_server.php.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soap_server.php | application/libraries/nusoap/class.soap_server.php |
| Line | 352 | 629 |
| Object | _SERVER | call_arg |

Code Snippet

File Name application/libraries/nusoap/class.soap_server.php

Method function parse_http_headers() {

```
....
352.                    foreach ($_SERVER as $k => $v) {
```

File Name application/libraries/nusoap/class.soap_server.php

Method function invoke_method() {

```
....
629.                            $this->methodreturn =
call_user_func_array($call_arg, array_values($this->methodparams));
```

**Code Injection\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=75 |
| Status | New |

The application's invoke_method method receives and dynamically executes user-controlled code using call_arg, at line 493 of application/libraries/nusoap/class.soap_server.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the parse_http_headers method, at line 320 of application/libraries/nusoap/class.soap_server.php.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soap_server.php | application/libraries/nusoap/class.soap_server.php |
| Line | 352 | 631 |
| Object | _SERVER | call_arg |

Code Snippet

| | |
|---|---|
| File Name | application/libraries/nusoap/class.soap_server.php |
| Method | function parse_http_headers() { |

```
....
352.                    foreach ($_SERVER as $k => $v) {
```

| | |
|---|---|
| File Name | application/libraries/nusoap/class.soap_server.php |
| Method | function invoke_method() { |

```
....
631.                        $this->methodreturn =
call_user_func_array($call_arg, array());
```

**Code Injection\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=76 |
| Status | New |

The application's invoke_method method receives and dynamically executes user-controlled code using eval, at line 493 of application/libraries/nusoap/class.soap_server.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the parse_http_headers method, at line 320 of application/libraries/nusoap/class.soap_server.php.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soap_server.php | application/libraries/nusoap/class.soap_server.php |
| Line | 352 | 615 |
| Object | _SERVER | eval |

Code Snippet

| | |
|---|---|
| File Name | application/libraries/nusoap/class.soap_server.php |
| Method | function parse_http_headers() { |

```
....
352.                    foreach ($_SERVER as $k => $v) {
```

| | |
|---|---|
| File Name | application/libraries/nusoap/class.soap_server.php |
| Method | function invoke_method() { |

```
....
615.                    @eval($funcCall);
```

**Code Injection\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | Proposed Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=77 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _GET, which is retrieved by the application in the <?php method, at line 1 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 197 | 586 |
| Object | _GET | eval |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
197.      $file = rawurldecode($_GET["input_file"]);
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.        eval("?" . ">$str");
```

**Code Injection\Path 5:**

| | |
|---|---|
| Severity | High |
| Result State | Proposed Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=78 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _GET, which is retrieved by the application in the <?php method, at line 1 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |

| | | |
|---|---|---|
| Line | 197 | 443 |
| Object | _GET | eval |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
197.      $file = rawurldecode($_GET["input_file"]);
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.        eval("?" . ">$str");
```

**Code Injection\Path 6:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=79
Status New

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _GET, which is retrieved by the application in the <?php method, at line 1 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 212 | 586 |
| Object | _GET | eval |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
212.      $base_path = rawurldecode($_GET["base_path"]);
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.        eval("?" . ">$str");
```

**Code Injection\Path 7:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=80 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _GET, which is retrieved by the application in the <?php method, at line 1 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 212 | 443 |
| Object | _GET | eval |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
212.      $base_path = rawurldecode($_GET["base_path"]);
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.        eval("?" . ">$str");
```

**Code Injection\Path 8:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=81 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 74 | 586 |
| Object | _SERVER | eval |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
74.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php
Method function load_html($str, $encoding = null) {

```
....
586.         eval("?" . ">$str");
```

**Code Injection\Path 9:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=82 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 74 | 443 |
| Object | _SERVER | eval |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
74.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.         eval("?" . ">$str");
```

**Code Injection\Path 10:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=83 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 81 | 586 |
| Object | _SERVER | eval |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
81.         $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.         eval("?" . ">$str");
```

**Code Injection\Path 11:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=84 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 81 | 443 |
| Object | _SERVER | eval |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
81.         $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.         eval("?" . ">$str");
```

**Code Injection\Path 12:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=85 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 88 | 586 |
| Object | _SERVER | eval |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
88.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.         eval("?" . ">$str");
```

**Code Injection\Path 13:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=86 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 88 | 443 |
| Object | _SERVER | eval |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
88.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.         eval("?" . ">$str");
```

**Code Injection\Path 14:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=87 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 95 | 586 |
| Object | _SERVER | eval |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
95.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.         eval("?" . ">$str");
```

**Code Injection\Path 15:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=88 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf. | system/helpers/dompdf/include/dompdf. |

| | | |
|---|---|---|
| | php | cls.php |
| Line | 95 | 443 |
| Object | _SERVER | eval |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
95.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.         eval("?" . ">$str");
```

**Code Injection\Path 16:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=89
Status New

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 112 | 586 |
| Object | _SERVER | eval |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
112.         $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.        eval("?" . ">$str");
```

**Code Injection\Path 17:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=90 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 112 | 443 |
| Object | _SERVER | eval |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
112.        $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.        eval("?" . ">$str");
```

**Code Injection\Path 18:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=91 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 117 | 586 |
| Object | _SERVER | eval |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
117.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name application/third_party/dompdf/include/dompdf.cls.php
Method function load_html($str, $encoding = null) {

```
....
586.        eval("?" . ">$str");
```

**Code Injection\Path 19:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=92 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 48 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 117 | 443 |
| Object | _SERVER | eval |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
117.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.        eval("?" . ">$str");
```

**Code Injection\Path 20:**

| | |
|---|---|
| Severity | High |
| Result State | Proposed Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=93 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _GET, which is retrieved by the application in the <?php method, at line 1 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 198 | 586 |
| Object | _GET | eval |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
198.      $file = rawurldecode($_GET["input_file"]);
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.        eval("?" . ">$str");
```

**Code Injection\Path 21:**

| | |
|---|---|
| Severity | High |
| Result State | Proposed Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=94 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _GET, which is retrieved by the application in the <?php method, at line 1 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 198 | 443 |
| Object | _GET | eval |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
198.      $file = rawurldecode($_GET["input_file"]);
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.        eval("?" . ">$str");
```

**Code Injection\Path 22:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=95 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _GET, which is retrieved by the application in the <?php method, at line 1 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 213 | 586 |
| Object | _GET | eval |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
213.      $base_path = rawurldecode($_GET["base_path"]);
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.        eval("?" . ">$str");
```

**Code Injection\Path 23:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=96 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _GET, which is retrieved by the application in the <?php method, at line 1 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 213 | 443 |
| Object | _GET | eval |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
213.      $base_path = rawurldecode($_GET["base_path"]);
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.        eval("?" . ">$str");
```

**Code Injection\Path 24:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=97 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 75 | 586 |
| Object | _SERVER | eval |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
75.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.         eval("?" . ">$str");
```

**Code Injection\Path 25:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=98 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf. |

| | | |
|---|---|---|
| | | cls.php |
| Line | 75 | 443 |
| Object | _SERVER | eval |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
75.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/include/dompdf.cls.php
Method function load_html($str, $encoding = null) {

```
....
443.         eval("?" . ">$str");
```

**Code Injection\Path 26:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=99
Status New

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 82 | 586 |
| Object | _SERVER | eval |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
82.         $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php
Method function load_html($str, $encoding = null) {

```
....
586.        eval("?" . ">$str");
```

**Code Injection\Path 27:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=100 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 82 | 443 |
| Object | _SERVER | eval |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
82.        $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.        eval("?" . ">$str");
```

**Code Injection\Path 28:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=101 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 89 | 586 |
| Object | _SERVER | eval |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
89.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php
Method function load_html($str, $encoding = null) {

```
....
586.         eval("?" . ">$str");
```

**Code Injection\Path 29:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=102
Status New

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 89 | 443 |
| Object | _SERVER | eval |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
89.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.         eval("?" . ">$str");
```

**Code Injection\Path 30:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=103 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 96 | 586 |
| Object | _SERVER | eval |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
96.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.         eval("?" . ">$str");
```

**Code Injection\Path 31:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=104 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 96 | 443 |
| Object | _SERVER | eval |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
96.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.         eval("?" . ">$str");
```

**Code Injection\Path 32:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=105 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 113 | 586 |
| Object | _SERVER | eval |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
113.        $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.        eval("?" . ">$str");
```

**Code Injection\Path 33:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=106 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 113 | 443 |
| Object | _SERVER | eval |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
113.        $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name system/helpers/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
443.        eval("?" . ">$str");
```

**Code Injection\Path 34:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=107 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 118 | 586 |
| Object | _SERVER | eval |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
118.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.        eval("?" . ">$str");
```

**Code Injection\Path 35:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=108 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using eval, at line 390 of system/helpers/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _SERVER, which is retrieved by the application in the getoptions method, at line 49 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/include/dompdf. |

| | | |
|---|---|---|
| | | cls.php |
| Line | 118 | 443 |
| Object | _SERVER | eval |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
118.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name system/helpers/dompdf/include/dompdf.cls.php
Method function load_html($str, $encoding = null) {

```
....
443.        eval("?" . ">$str");
```

**Code Injection\Path 36:**

Severity High
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=109
Status New

The application's _sanitize_globals method receives and dynamically executes user-controlled code using $_Variable, at line 565 of system/core/Input.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _GET, which is retrieved by the application in the _sanitize_globals method, at line 565 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/core/Input.php |
| Line | 575 | 582 |
| Object | _GET | $_Variable |

Code Snippet
File Name system/core/Input.php
Method function _sanitize_globals()

```
....
575.            foreach (array($_GET, $_POST, $_COOKIE) as $global)
....
582.                                $$global = NULL;
```

**Code Injection\Path 37:**

Severity High

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=110 |
| Status | New |

The application's _sanitize_globals method receives and dynamically executes user-controlled code using $_Variable, at line 565 of system/core/Input.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _COOKIE, which is retrieved by the application in the _sanitize_globals method, at line 565 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/core/Input.php |
| Line | 575 | 582 |
| Object | _COOKIE | $_Variable |

Code Snippet
File Name system/core/Input.php
Method function _sanitize_globals()

```
....
575.            foreach (array($_GET, $_POST, $_COOKIE) as $global)
....
582.                                $$global = NULL;
```

**Code Injection\Path 38:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=111 |
| Status | New |

The application's _sanitize_globals method receives and dynamically executes user-controlled code using $_Variable, at line 565 of system/core/Input.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code via user input, _POST, which is retrieved by the application in the _sanitize_globals method, at line 565 of system/core/Input.php.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/core/Input.php |
| Line | 575 | 582 |
| Object | _POST | $_Variable |

Code Snippet
File Name system/core/Input.php
Method function _sanitize_globals()

```
....
575.                foreach (array($_GET, $_POST, $_COOKIE) as $global)
....
582.                                $$global = NULL;
```

## Trust Boundary Violation

Query Path:
PHP\Cx\PHP Medium Threat\Trust Boundary Violation Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.8 - Improper access control
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A5-Broken Access Control
OWASP Top 10 2021: A4-Insecure Design

### *Description*

**Trust Boundary Violation\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14199 |
| Status | New |

Method bismod_process at line 251 of application/controllers/admin.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in bismod_process at line 251 of application/controllers/admin.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin.php | application/controllers/admin.php |
| Line | 255 | 380 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin.php
Method public function bismod_process($nama_paket = null)

```
....
255.                $data['nama_paket'] = trim($this->input-
>post('nama_paket'));;
....
380.                        $_SESSION['info_success'] = $nama_paket ?
$data['nama_paket'].' berhasil update' : $data['nama_paket'] . '
berhasil diupdate.';
```

**Trust Boundary Violation\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14200 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in bismod_process at line 251 of application/controllers/admin.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin.php |
| Line | 182 | 380 |
| Object | _POST | _SESSION_info_success |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin.php
Method public function bismod_process($nama_paket = null)

```
....
380.                     $_SESSION['info_success'] = $nama_paket ?
$data['nama_paket'].' berhasil update' : $data['nama_paket'] . '
berhasil diupdate.';
```

**Trust Boundary Violation\Path 3:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14201
Status New

Method getCacheData at line 111 of application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php gets user input from element _fileHandle. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in manage_target_marketing_form_upload at line 5601 of application/controllers/admin.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php | application/controllers/admin.php |
| Line | 126 | 5796 |
| Object | _fileHandle | _SESSION_info_error |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php
Method public function getCacheData($pCoord) {

```
....
126.                $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/controllers/admin.php

Method public function manage_target_marketing_form_upload()

```
....
5796.                    $_SESSION['info_error'] = "Upload Gagal!
".$error_valid;
```

**Trust Boundary Violation\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14202 |
| Status | New |

Method getCacheData at line 103 of application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php gets user input from element _fileHandle. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in manage_target_marketing_form_upload at line 5601 of application/controllers/admin.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php | application/controllers/admin.php |
| Line | 118 | 5796 |
| Object | _fileHandle | _SESSION_info_error |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php

Method public function getCacheData($pCoord) {

```
....
118.                $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/controllers/admin.php

Method public function manage_target_marketing_form_upload()

```
....
5796.                    $_SESSION['info_error'] = "Upload Gagal!
".$error_valid;
```

**Trust Boundary Violation\Path 5:**

| | |
|---|---|
| Severity | Medium |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14203 |
| Status | New |

Method add_grup at line 2019 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in add_grup at line 2019 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2025 | 2036 |
| Object | post | _SESSION_info_success |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/admin_bck20190114.php |
| Method | public function add_grup() |

```
....
2025.             $namagrup = strtoupper(trim($this->input-
>post('nama_grup')));
....
2036.                         $_SESSION['info_success'] = "Tambah Grup
".$namagrup." Berhasil";
```

**Trust Boundary Violation\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14204 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in add_grup at line 2019 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2036 |
| Object | _POST | _SESSION_info_success |

| | |
|---|---|
| Code Snippet | |
| File Name | system/core/Input.php |
| Method | function post($index = NULL, $xss_clean = FALSE) |

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php

Method public function add_grup()

```
....
2036.                           $_SESSION['info_success'] = "Tambah Grup
".$namagrup." Berhasil";
```

**Trust Boundary Violation\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14205 |
| Status | New |

Method edit_grup at line 2049 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in edit_grup at line 2049 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2061 | 2066 |
| Object | post | _SESSION_info_success |

Code Snippet

File Name application/controllers/admin_bck20190114.php

Method public function edit_grup()

```
....
2061.                   $namagrup = strtoupper($this->input-
>post('nama_grup'));
....
2066.                           $_SESSION['info_success'] = "Edit Grup
".$namagrup." Berhasil";
```

**Trust Boundary Violation\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14206 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side

Session object, in edit_grup at line 2049 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2066 |
| Object | _POST | _SESSION_info_success |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method public function edit_grup()

```
....
2066.                           $_SESSION['info_success'] = "Edit Grup ".$namagrup." Berhasil";
```

**Trust Boundary Violation\Path 9:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14207
Status New

Method merk_edc at line 2148 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_edc at line 2148 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2154 | 2158 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function merk_edc()

```
....
2154.                    $nama = trim($this->input->post('nama'));
....
2158.                          $_SESSION['info_success'] = 'Sukses tambah
merk EDC '.$nama;
```

**Trust Boundary Violation\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14208 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_edc at line 2148 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2158 |
| Object | _POST | _SESSION_info_success |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                          $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php

Method function merk_edc()

```
....
2158.                          $_SESSION['info_success'] = 'Sukses tambah
merk EDC '.$nama;
```

**Trust Boundary Violation\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14209 |
| Status | New |

Method merk_edc at line 2148 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_edc at line 2148 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2154 | 2160 |
| Object | post | _SESSION_info_error |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function merk_edc()

```
....
2154.                    $nama = trim($this->input->post('nama'));
....
2160.                          $_SESSION['info_error'] = 'Gagal tambah
merk EDC '.$nama;
```

**Trust Boundary Violation\Path 12:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14210
Status New

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_edc at line 2148 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2160 |
| Object | _POST | _SESSION_info_error |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                           $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function merk_edc()

```
....
2160.                          $_SESSION['info_error'] = 'Gagal tambah
merk EDC '.$nama;
```

**Trust Boundary Violation\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14211 |
| Status | New |

Method merk_edc at line 2148 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_edc at line 2148 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2167 | 2177 |
| Object | post | _SESSION_info_success |

Code Snippet

File Name application/controllers/admin_bck20190114.php

Method function merk_edc()

```
....
2167.                    $nama_lama = trim($this->input-
>post('nama_lama'));
....
2177.                                $_SESSION['info_success'] = 'Sukses
edit merk EDC '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14212 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_edc at line 2148 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2177 |
| Object | _POST | _SESSION_info_success |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php

Method function merk_edc()

```
....
2177.                                $_SESSION['info_success'] = 'Sukses
edit merk EDC '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14213 |
| Status | New |

Method merk_edc at line 2148 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_edc at line 2148 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2168 | 2177 |
| Object | post | _SESSION_info_success |

Code Snippet

File Name application/controllers/admin_bck20190114.php

Method function merk_edc()

```
....
2168.                    $nama_baru = trim($this->input-
>post('nama_baru'));
....
2177.                                $_SESSION['info_success'] = 'Sukses
edit merk EDC '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14214 |
| Status | New |

Method merk_edc at line 2148 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is

eventually stored in the server-side Session object, in merk_edc at line 2148 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2167 | 2179 |
| Object | post | _SESSION_info_error |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function merk_edc()

```
....
2167.                    $nama_lama = trim($this->input-
>post('nama_lama'));
....
2179.                                $_SESSION['info_error'] = 'Gagal
edit merk EDC '.$nama_lama;
```

**Trust Boundary Violation\Path 17:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14215
Status New

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_edc at line 2148 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2179 |
| Object | _POST | _SESSION_info_error |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                         $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function merk_edc()

```
....
2179.                                $_SESSION['info_error'] = 'Gagal
edit merk EDC '.$nama_lama;
```

**Trust Boundary Violation\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14216 |
| Status | New |

Method vendor_edc at line 2192 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edc at line 2192 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2198 | 2202 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_edc()

```
....
2198.                    $nama = trim($this->input->post('nama'));
....
2202.                          $_SESSION['info_success'] = 'Sukses tambah
vendor EDC '.$nama;
```

**Trust Boundary Violation\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14217 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edc at line 2192 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2202 |
| Object | _POST | _SESSION_info_success |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function vendor_edc()

```
....
2202.                           $_SESSION['info_success'] = 'Sukses tambah
vendor EDC '.$nama;
```

**Trust Boundary Violation\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14218 |
| Status | New |

Method vendor_edc at line 2192 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edc at line 2192 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2198 | 2204 |
| Object | post | _SESSION_info_error |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_edc()

```
....
2198.                   $nama = trim($this->input->post('nama'));
....
2204.                           $_SESSION['info_error'] = 'Gagal tambah
vendor EDC '.$nama;
```

**Trust Boundary Violation\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14219 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edc at line 2192 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2204 |
| Object | _POST | _SESSION_info_error |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function vendor_edc()

```
....
2204.                           $_SESSION['info_error'] = 'Gagal tambah vendor EDC '.$nama;
```

**Trust Boundary Violation\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14220 |
| Status | New |

Method vendor_edc at line 2192 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edc at line 2192 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2211 | 2221 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_edc()

```
....
2211.                    $nama_lama = trim($this->input-
>post('nama_lama'));
....
2221.                                $_SESSION['info_success'] = 'Sukses
edit vendor EDC '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14221 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edc at line 2192 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2221 |
| Object | _POST | _SESSION_info_success |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                         $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php

Method function vendor_edc()

```
....
2221.                                $_SESSION['info_success'] = 'Sukses
edit vendor EDC '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14222 |
| Status | New |

Method vendor_edc at line 2192 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is

eventually stored in the server-side Session object, in vendor_edc at line 2192 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2212 | 2221 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_edc()

```
....
2212.                    $nama_baru = trim($this->input->post('nama_baru'));
....
2221.                                $_SESSION['info_success'] = 'Sukses edit vendor EDC '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 25:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14223
Status New

Method vendor_edc at line 2192 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edc at line 2192 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2211 | 2223 |
| Object | post | _SESSION_info_error |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_edc()

```
....
2211.                    $nama_lama = trim($this->input->post('nama_lama'));
....
2223.                                $_SESSION['info_error'] = 'Gagal edit vendor EDC '.$nama_lama;
```

**Trust Boundary Violation\Path 26:**

Severity Medium
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14224 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edc at line 2192 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2223 |
| Object | _POST | _SESSION_info_error |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php

Method function vendor_edc()

```
....
2223.                                $_SESSION['info_error'] = 'Gagal edit vendor EDC '.$nama_lama;
```

**Trust Boundary Violation\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14225 |
| Status | New |

Method merk_clr at line 2236 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_clr at line 2236 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2242 | 2246 |
| Object | post | _SESSION_info_success |

Code Snippet

File Name application/controllers/admin_bck20190114.php

Method function merk_clr()

```
....
2242.                    $nama = trim($this->input->post('nama'));
....
2246.                          $_SESSION['info_success'] = 'Sukses tambah
merk CLR '.$nama;
```

**Trust Boundary Violation\Path 28:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14226
Status New

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_clr at line 2236 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2246 |
| Object | _POST | _SESSION_info_success |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                          $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function merk_clr()

```
....
2246.                          $_SESSION['info_success'] = 'Sukses tambah
merk CLR '.$nama;
```

**Trust Boundary Violation\Path 29:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14227
Status New

Method merk_clr at line 2236 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is

eventually stored in the server-side Session object, in merk_clr at line 2236 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2242 | 2248 |
| Object | post | _SESSION_info_error |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function merk_clr()

```
....
2242.                    $nama = trim($this->input->post('nama'));
....
2248.                          $_SESSION['info_error'] = 'Gagal tambah
merk CLR '.$nama;
```

**Trust Boundary Violation\Path 30:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14228
Status New

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_clr at line 2236 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2248 |
| Object | _POST | _SESSION_info_error |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                          $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function merk_clr()

```
....
2248.                          $_SESSION['info_error'] = 'Gagal tambah
merk CLR '.$nama;
```

**Trust Boundary Violation\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14229 |
| Status | New |

Method merk_clr at line 2236 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_clr at line 2236 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2255 | 2265 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function merk_clr()

```
....
2255.                    $nama_lama = trim($this->input-
>post('nama_lama'));
....
2265.                                $_SESSION['info_success'] = 'Sukses
edit merk CLR '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14230 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_clr at line 2236 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2265 |
| Object | _POST | _SESSION_info_success |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function merk_clr()

```
....
2265.                                $_SESSION['info_success'] = 'Sukses
edit merk CLR '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 33:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14231
Status New

Method merk_clr at line 2236 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_clr at line 2236 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2256 | 2265 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function merk_clr()

```
....
2256.                    $nama_baru = trim($this->input-
>post('nama_baru'));
....
2265.                                $_SESSION['info_success'] = 'Sukses
edit merk CLR '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 34:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14232
Status New

Method merk_clr at line 2236 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_clr at line 2236 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2255 | 2267 |
| Object | post | _SESSION_info_error |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function merk_clr()

```
....
2255.                    $nama_lama = trim($this->input->post('nama_lama'));
....
2267.                                $_SESSION['info_error'] = 'Gagal edit merk CLR '.$nama_lama;
```

**Trust Boundary Violation\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14233 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in merk_clr at line 2236 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2267 |
| Object | _POST | _SESSION_info_error |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                         $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function merk_clr()

```
....
2267.                                $_SESSION['info_error'] = 'Gagal
edit merk CLR '.$nama_lama;
```

**Trust Boundary Violation\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14234 |
| Status | New |

Method vendor_clr at line 2280 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_clr at line 2280 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2286 | 2290 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_clr()

```
....
2286.                    $nama = trim($this->input->post('nama'));
....
2290.                          $_SESSION['info_success'] = 'Sukses tambah
vendor CLR '.$nama;
```

**Trust Boundary Violation\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14235 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_clr at line 2280 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2290 |
| Object | _POST | _SESSION_info_success |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function vendor_clr()

```
....
2290.                           $_SESSION['info_success'] = 'Sukses tambah
vendor CLR '.$nama;
```

**Trust Boundary Violation\Path 38:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14236
Status New

Method vendor_clr at line 2280 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_clr at line 2280 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2286 | 2292 |
| Object | post | _SESSION_info_error |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_clr()

```
....
2286.                   $nama = trim($this->input->post('nama'));
....
2292.                           $_SESSION['info_error'] = 'Gagal tambah
vendor CLR '.$nama;
```

**Trust Boundary Violation\Path 39:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14237
Status New

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_clr at line 2280 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2292 |
| Object | _POST | _SESSION_info_error |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function vendor_clr()

```
....
2292.                           $_SESSION['info_error'] = 'Gagal tambah vendor CLR '.$nama;
```

**Trust Boundary Violation\Path 40:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14238
Status New

Method vendor_clr at line 2280 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_clr at line 2280 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2299 | 2309 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_clr()

```
....
2299.                    $nama_lama = trim($this->input-
>post('nama_lama'));
....
2309.                                $_SESSION['info_success'] = 'Sukses
edit vendor CLR '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14239 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_clr at line 2280 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2309 |
| Object | _POST | _SESSION_info_success |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                         $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php

Method function vendor_clr()

```
....
2309.                                $_SESSION['info_success'] = 'Sukses
edit vendor CLR '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14240 |
| Status | New |

Method vendor_clr at line 2280 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is

eventually stored in the server-side Session object, in vendor_clr at line 2280 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2300 | 2309 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_clr()

```
....
2300.                    $nama_baru = trim($this->input-
>post('nama_baru'));
....
2309.                                $_SESSION['info_success'] = 'Sukses
edit vendor CLR '.$nama_lama.' menjadi '.$nama_baru;
```

**Trust Boundary Violation\Path 43:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14241
Status New

Method vendor_clr at line 2280 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_clr at line 2280 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2299 | 2311 |
| Object | post | _SESSION_info_error |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_clr()

```
....
2299.                    $nama_lama = trim($this->input-
>post('nama_lama'));
....
2311.                                $_SESSION['info_error'] = 'Gagal
edit vendor CLR '.$nama_lama;
```

**Trust Boundary Violation\Path 44:**

Severity Medium
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14242 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_clr at line 2280 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2311 |
| Object | _POST | _SESSION_info_error |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php

Method function vendor_clr()

```
....
2311.                                $_SESSION['info_error'] = 'Gagal edit vendor CLR '.$nama_lama;
```

**Trust Boundary Violation\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14243 |
| Status | New |

Method vendor_add at line 2339 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_add at line 2339 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2351 | 2360 |
| Object | post | _SESSION_info_success |

Code Snippet

File Name application/controllers/admin_bck20190114.php

Method function vendor_add()

```
....
2351.                    $datadb['kode']    = strtoupper($this->input-
>post('kode'));
....
2360.                          $_SESSION['info_success'] = "Tambah vendor
".$datadb['kode']." berhasil";
```

**Trust Boundary Violation\Path 46:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14244
Status New

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_add at line 2339 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2360 |
| Object | _POST | _SESSION_info_success |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                          $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function vendor_add()

```
....
2360.                          $_SESSION['info_success'] = "Tambah vendor
".$datadb['kode']." berhasil";
```

**Trust Boundary Violation\Path 47:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14245
Status New

Method vendor_edit at line 2368 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is

eventually stored in the server-side Session object, in vendor_edit at line 2368 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2383 | 2390 |
| Object | post | _SESSION_info_error |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_edit()

```
....
2383.                    $kode              = $this->input->post('kode');
....
2390.                          $_SESSION['info_error'] = "Update vendor
".$kode." gagal (data tidak berubah)";
```

**Trust Boundary Violation\Path 48:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14246
Status New

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edit at line 2368 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2390 |
| Object | _POST | _SESSION_info_error |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                          $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function vendor_edit()

```
....
2390.                        $_SESSION['info_error'] = "Update vendor
".$kode." gagal (data tidak berubah)";
```

**Trust Boundary Violation\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14247 |
| Status | New |

Method vendor_edit at line 2368 of application/controllers/admin_bck20190114.php gets user input from element post. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edit at line 2368 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 2383 | 2392 |
| Object | post | _SESSION_info_success |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method function vendor_edit()

```
....
2383.                   $kode             = $this->input->post('kode');
....
2392.                        $_SESSION['info_success'] = "Update vendor
".$kode." berhasil";
```

**Trust Boundary Violation\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14248 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from element _POST. This element's value flows through the code without being properly sanitized or validated and is eventually stored in the server-side Session object, in vendor_edit at line 2368 of application/controllers/admin_bck20190114.php. This constitutes a Trust Boundary Violation.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 2392 |
| Object | _POST | _SESSION_info_success |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method function vendor_edit()

```
....
2392.                       $_SESSION['info_success'] = "Update vendor
".$kode." berhasil";
```

## XSRF

Query Path:
PHP\Cx\PHP Medium Threat\XSRF Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.9 - Cross-site request forgery
OWASP Top 10 2013: A8-Cross-Site Request Forgery (CSRF)
NIST SP 800-53: SC-23 Session Authenticity (P1)
OWASP Top 10 2021: A1-Broken Access Control

*Description*

**XSRF\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11712 |
| Status | New |

Method pasang_edc at line 1186 of application/controllers/implementasi.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 1191 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function pasang_edc()

```
....
1191.                       $init_id = trim($this->input->post('id'));
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11713 |
| Status | New |

Method post at line 172 of system/core/Input.php gets a parameter from a user request from _POST. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/database/DB_driver.php |
| Line | 182 | 453 |
| Object | _POST | _execute |

Code Snippet

| | |
|---|---|
| File Name | system/core/Input.php |
| Method | function post($index = NULL, $xss_clean = FALSE) |

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11714 |
| Status | New |

Method pasang_edc at line 1186 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 1191 | 453 |
| Object | post | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php
Method public function pasang_edc()

```
....
1191.                        $init_id = trim($this->input->post('id'));
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11715 |
| Status | New |

Method report_pasang_edc at line 1877 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 1921 | 453 |
| Object | post | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php
Method public function report_pasang_edc()

```
....
1921.                                $tgl_pemasangan = trim($this->input-
>post('tgl_pemasangan'));
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11716 |
| Status | New |

Method pasang_edc at line 1186 of application/controllers/implementasi.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 1195 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/implementasi.php

Method public function pasang_edc()

```
....
1195.                        $tgl_pasang = trim($this->input-
>post('tgl_pasang'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11717 |
| Status | New |

Method report_pasang_edc at line 1877 of application/controllers/implementasi.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 1921 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/implementasi.php
Method public function report_pasang_edc()

```
....
1921.                                $tgl_pemasangan = trim($this->input-
>post('tgl_pemasangan'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11718 |
| Status | New |

Method pasang_edc at line 1186 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php | system/database/DB_driver.php |
| Line | 1195 | 453 |
| Object | post | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi.php
Method public function pasang_edc()

```
....
1195.                          $tgl_pasang = trim($this->input-
>post('tgl_pasang'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11719 |
| Status | New |

Method form_submit at line 30 of application/controllers/remark_merchant.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/remark_merchant.php | system/database/DB_driver.php |
| Line | 36 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/remark_merchant.php

Method public function form_submit()

```
....
36.         $remark_3_arr     = $this->input->post('remark_3');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11720 |
| Status | New |

Method form_submit at line 30 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php | system/database/DB_driver.php |
| Line | 36 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php

| | |
|---|---|
| Method | public function form_submit() |

```
....
36.         $remark_3_arr     = $this->input->post('remark_3');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11721 |
| Status | New |

Method form_submit at line 30 of application/controllers/remark_merchant.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/remark_merchant.php | system/database/DB_driver.php |
| Line | 35 | 453 |
| Object | post | _execute |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/remark_merchant.php |
| Method | public function form_submit() |

```
....
35.         $remark_2_arr     = $this->input->post('remark_2');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11722 |
| Status | New |

Method form_submit at line 30 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php | system/database/DB_driver.php |
| Line | 35 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php

Method public function form_submit()

```
....
35.         $remark_2_arr     = $this->input->post('remark_2');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11723 |
| Status | New |

Method form_submit at line 30 of application/controllers/remark_merchant.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/remark_merchant.php | system/database/DB_driver.php |
| Line | 34 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/remark_merchant.php

Method public function form_submit()

```
....
34.         $remark_1_arr     = $this->input->post('remark_1');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.            return $this->_execute($sql);
```

**XSRF\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11724 |
| Status | New |

Method form_submit at line 30 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php | system/database/DB_driver.php |
| Line | 34 | 453 |
| Object | post | _execute |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php |
| Method | public function form_submit() |

```
....
34.         $remark_1_arr     = $this->input->post('remark_1');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.            return $this->_execute($sql);
```

**XSRF\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11725 |
| Status | New |

Method form_submit at line 30 of application/controllers/remark_merchant.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/controllers/remark_merchant.php | system/database/DB_driver.php |
| Line | 32 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/remark_merchant.php
Method public function form_submit()

```
....
32.         $tid_arr          = $this->input->post('tid');
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11726 |
| Status | New |

Method form_submit at line 30 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php | system/database/DB_driver.php |
| Line | 32 | 453 |
| Object | post | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php
Method public function form_submit()

```
....
32.         $tid_arr          = $this->input->post('tid');
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11727 |
| Status | New |

Method form_submit at line 30 of application/controllers/remark_merchant.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/remark_merchant.php | system/database/DB_driver.php |
| Line | 33 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/remark_merchant.php

Method public function form_submit()

```
....
33.         $mid_arr          = $this->input->post('mid');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11728 |
| Status | New |

Method form_submit at line 30 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php | system/database/DB_driver.php |

| | | |
|---|---|---|
| Line | 33 | 453 |
| Object | post | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/remark_merchant.php
Method public function form_submit()

```
....
33.         $mid_arr          = $this->input->post('mid');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11729 |
| Status | New |

Method cm_form_all at line 1485 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php | system/database/DB_driver.php |
| Line | 1488 | 453 |
| Object | get | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php
Method function cm_form_all()

```
....
1488.             $post             = $this->input->get();
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11730 |
| Status | New |

Method cm_form_all at line 1501 of application/controllers/maintenance_20190610.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 1504 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance_20190610.php

Method function cm_form_all()

```
....
1504.               $post               = $this->input->get();
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11731 |
| Status | New |

Method cm_form_all at line 1485 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php | system/database/DB_driver.php |

| | | |
|---|---|---|
| Line | 1488 | 453 |
| Object | get | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php
Method function cm_form_all()

```
....
1488.            $post            = $this->input->get();
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11732 |
| Status | New |

Method cm_form_all at line 1499 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php | system/database/DB_driver.php |
| Line | 1502 | 453 |
| Object | get | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php
Method function cm_form_all()

```
....
1502.            $post            = $this->input->get();
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11733 |
| Status | New |

Method cm_form_all at line 1485 of application/controllers/maintenance_bck20180906.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20180906.php | system/database/DB_driver.php |
| Line | 1488 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance_bck20180906.php

Method function cm_form_all()

```
....
1488.               $post               = $this->input->get();
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**XSRF\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11734 |
| Status | New |

Method cm_form_all at line 1532 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php | system/database/DB_driver.php |

| | | |
|---|---|---|
| Line | 1535 | 453 |
| Object | get | _execute |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php
Method function cm_form_all()

```
....
1535.            $post            = $this->input->get();
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11735 |
| Status | New |

Method cm_form_all at line 1499 of application/controllers/maintenance_bck20190114.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20190114.php | system/database/DB_driver.php |
| Line | 1502 | 453 |
| Object | get | _execute |

Code Snippet
File Name application/controllers/maintenance_bck20190114.php
Method function cm_form_all()

```
....
1502.            $post            = $this->input->get();
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11736 |
| Status | New |

Method cm_form_all at line 1532 of application/controllers/maintenance.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | system/database/DB_driver.php |
| Line | 1535 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance.php

Method function cm_form_all()

```
....
1535.             $post             = $this->input->get();
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11737 |
| Status | New |

Method cm_form_all at line 1501 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 1504 | 453 |
| Object | get | _execute |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php |
| Method | function cm_form_all() |

```
....
1504.            $post            = $this->input->get();
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11738 |
| Status | New |

Method cm_form_all at line 1485 of application/controllers/maintenance_20181213.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20181213.php | system/database/DB_driver.php |
| Line | 1488 | 453 |
| Object | get | _execute |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/maintenance_20181213.php |
| Method | function cm_form_all() |

```
....
1488.            $post            = $this->input->get();
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11739 |

| | |
|---|---|
| Status | New |

Method cm_form_all at line 1501 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 1504 | 453 |
| Object | get | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php

Method function cm_form_all()

```
....
1504.            $post            = $this->input->get();
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11740 |
| Status | New |

Method cm_form_all at line 1501 of application/controllers/maintenance_20190524.php gets a parameter from a user request from get. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 1504 | 453 |
| Object | get | _execute |

Code Snippet

File Name application/controllers/maintenance_20190524.php

Method function cm_form_all()

```
....
1504.            $post            = $this->input->get();
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11741 |
| Status | New |

Method get_data_merchant at line 4414 of application/controllers/maintenance_bck20190114.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20190114.php | system/database/DB_driver.php |
| Line | 4417 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/maintenance_bck20190114.php

Method function get_data_merchant()

```
....
4417.            $mid = $this->input->post('mid');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11742 |
| Status | New |

Method get_data_merchant at line 4520 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php | system/database/DB_driver.php |
| Line | 4523 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php

Method function get_data_merchant()

```
....
4523.             $mid = $this->input->post('mid');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11743 |
| Status | New |

Method get_data_merchant at line 4395 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php | system/database/DB_driver.php |
| Line | 4398 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php

Method function get_data_merchant()

```
....
4398.             $mid = $this->input->post('mid');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11744 |
| Status | New |

Method get_data_merchant at line 4465 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 4468 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php

Method function get_data_merchant()

```
....
4468.             $mid = $this->input->post('mid');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11745 |

| | |
|---|---|
| Status | New |

Method get_data_merchant at line 4470 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 4473 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php

Method function get_data_merchant()

```
....
4473.             $mid = $this->input->post('mid');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11746 |
| Status | New |

Method get_data_merchant at line 3994 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php | system/database/DB_driver.php |
| Line | 3997 | 453 |
| Object | post | _execute |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php |
| Method | function get_data_merchant() |

```
....
3997.            $mid = $this->input->post('mid');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11747 |
| Status | New |

Method get_data_merchant at line 4379 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php | system/database/DB_driver.php |
| Line | 4382 | 453 |
| Object | post | _execute |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php |
| Method | function get_data_merchant() |

```
....
4382.            $mid = $this->input->post('mid');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 37:**

| | |
|---|---|
| Severity | Medium |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11748 |
| Status | New |

Method get_data_merchant at line 4414 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php | system/database/DB_driver.php |
| Line | 4417 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php

Method function get_data_merchant()

```
....
4417.             $mid = $this->input->post('mid');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11749 |
| Status | New |

Method get_data_merchant at line 4379 of application/controllers/maintenance_bck20180906.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20180906.php | system/database/DB_driver.php |
| Line | 4382 | 453 |
| Object | post | _execute |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/maintenance_bck20180906.php |
| Method | function get_data_merchant() |

```
....
4382.            $mid = $this->input->post('mid');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11750 |
| Status | New |

Method get_data_merchant at line 3994 of application/controllers/maintenance_bck07112017.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck07112017.php | system/database/DB_driver.php |
| Line | 3997 | 453 |
| Object | post | _execute |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/maintenance_bck07112017.php |
| Method | function get_data_merchant() |

```
....
3997.            $mid = $this->input->post('mid');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11751 |
| Status | New |

Method get_data_merchant at line 4470 of application/controllers/maintenance_20190610.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 4473 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/maintenance_20190610.php
Method function get_data_merchant()

```
....
4473.             $mid = $this->input->post('mid');
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11752 |
| Status | New |

Method get_data_merchant at line 4465 of application/controllers/maintenance_20190524.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 4468 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/maintenance_20190524.php
Method function get_data_merchant()

```
....
4468.             $mid = $this->input->post('mid');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.            return $this->_execute($sql);
```

**XSRF\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11753 |
| Status | New |

Method get_data_merchant at line 4395 of application/controllers/maintenance_20181213.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20181213.php | system/database/DB_driver.php |
| Line | 4398 | 453 |
| Object | post | _execute |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/maintenance_20181213.php |
| Method | function get_data_merchant() |

```
....
4398.           $mid = $this->input->post('mid');
```

| | |
|---|---|
| File Name | system/database/DB_driver.php |
| Method | function simple_query($sql) |

```
....
453.            return $this->_execute($sql);
```

**XSRF\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11754 |
| Status | New |

Method get_data_merchant at line 4530 of application/controllers/maintenance.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | system/database/DB_driver.php |

| | | |
|---|---|---|
| Line | 4533 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/maintenance.php
Method function get_data_merchant()

```
....
4533.            $mid = $this->input->post('mid');
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11755 |
| Status | New |

Method cm_penarikan_approve at line 2241 of application/controllers/maintenance_20190524.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 2245 | 453 |
| Object | post | _execute |

Code Snippet
File Name application/controllers/maintenance_20190524.php
Method function cm_penarikan_approve()

```
....
2245.            $mid        = $this->input->post('mid');
```

File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11756 |
| Status | New |

Method input_cm_settlement_pilih at line 26 of application/controllers/settlement.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/settlement.php | system/database/DB_driver.php |
| Line | 27 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/settlement.php

Method function input_cm_settlement_pilih() {

```
....
27.         $where['mid']                    = trim($this->input-
>post('mid'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11757 |
| Status | New |

Method input_cm_settlement_pilih at line 26 of application/controllers/settlement.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/settlement.php | system/database/DB_driver.php |
| Line | 28 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/settlement.php

Method function input_cm_settlement_pilih() {

```
....
28.         $where['tid']                 = trim($this->input-
>post('tid'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11758 |
| Status | New |

Method input_cm_settlement_pilih at line 26 of application/controllers/settlement.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/settlement.php | system/database/DB_driver.php |
| Line | 29 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/settlement.php

Method function input_cm_settlement_pilih() {

```
....
29.         $where['nama_merchant'] = trim($this->input-
>post('nama_merchant'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.              return $this->_execute($sql);
```

**XSRF\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11759 |
| Status | New |

Method input_cm_merchant_pilih at line 4562 of application/controllers/maintenance_20190524.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | system/database/DB_driver.php |
| Line | 4563 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/maintenance_20190524.php

Method function input_cm_merchant_pilih() {

```
....
4563.            $mid              = trim($this->input->post('mid'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11760 |
| Status | New |

Method input_cm_merchant_pilih at line 4083 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php | system/database/DB_driver.php |
| Line | 4084 | 453 |
| Object | post | _execute |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php

Method function input_cm_merchant_pilih() {

```
....
4084.            $mid              = trim($this->input->post('mid'));
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

**XSRF\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11761 |
| Status | New |

Method cm_penarikan_approve at line 2246 of application/controllers/maintenance_20190610.php gets a parameter from a user request from post. This parameter value flows through the code and is eventually used to access application state altering functionality. This may enable Cross-Site Request Forgery (XSRF).

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | system/database/DB_driver.php |
| Line | 2250 | 453 |
| Object | post | _execute |

Code Snippet

File Name application/controllers/maintenance_20190610.php

Method function cm_penarikan_approve()

```
....
2250.            $mid        = $this->input->post('mid');
```

File Name system/database/DB_driver.php

Method function simple_query($sql)

```
....
453.             return $this->_execute($sql);
```

## Path Traversal

Query Path:

PHP\Cx\PHP Medium Threat\Path Traversal Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.8 - Improper access control
OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

OWASP Top 10 2021: A1-Broken Access Control

*Description*

**Path Traversal\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10537 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 74 | 274 |
| Object | _SERVER | outfile |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
74.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
274.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10538 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |

| | | |
|---|---|---|
| Line | 81 | 274 |
| Object | _SERVER | outfile |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
81.         $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
274.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 3:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10539
Status New

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 88 | 274 |
| Object | _SERVER | outfile |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
88.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
274.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10540 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 95 | 274 |
| Object | _SERVER | outfile |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
95.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
274.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10541 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 112 | 274 |
| Object | _SERVER | outfile |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
112.        $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
274.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10542 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 117 | 274 |
| Object | _SERVER | outfile |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
117.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
274.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10543 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/dompdf.php |
| Line | 254 | 274 |
| Object | _SERVER | outfile |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
254.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
274.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10544 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 74 | 279 |
| Object | _SERVER | outfile |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
74.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
279.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10545 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 81 | 279 |
| Object | _SERVER | outfile |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
81.         $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
279.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10546 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 88 | 279 |
| Object | _SERVER | outfile |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
88.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
279.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10547 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 95 | 279 |
| Object | _SERVER | outfile |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
95.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
279.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10548 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 112 | 279 |
| Object | _SERVER | outfile |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
112.         $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
279.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10549 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 117 | 279 |
| Object | _SERVER | outfile |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
117.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
279.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10550 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of application/third_party/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/dompdf.php |
| Line | 254 | 279 |
| Object | _SERVER | outfile |

Code Snippet
File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
254.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
279.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10551 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 75 | 275 |
| Object | _SERVER | outfile |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
75.        $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
275.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10552 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 82 | 275 |
| Object | _SERVER | outfile |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
82.         $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
275.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10553 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |

| | | |
|---|---|---|
| Line | 89 | 275 |
| Object | _SERVER | outfile |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
89.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
275.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10554 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 96 | 275 |
| Object | _SERVER | outfile |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
96.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
275.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10555 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 113 | 275 |
| Object | _SERVER | outfile |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
113.        $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
275.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10556 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |

| | | |
|---|---|---|
| Line | 118 | 275 |
| Object | _SERVER | outfile |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
118.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
275.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10557 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | system/helpers/dompdf/dompdf.php |
| Line | 231 | 275 |
| Object | _SERVER | outfile |

Code Snippet
File Name system/helpers/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
231.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
275.    $outfile = realpath(dirname($outfile)) . DIRECTORY_SEPARATOR .
basename($outfile);
```

**Path Traversal\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10558 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 75 | 280 |
| Object | _SERVER | outfile |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
75.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
280.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10559 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |

| | | |
|---|---|---|
| Line | 82 | 280 |
| Object | _SERVER | outfile |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
82.         $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
280.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10560 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 89 | 280 |
| Object | _SERVER | outfile |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
89.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
280.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10561 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 96 | 280 |
| Object | _SERVER | outfile |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
96.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
280.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10562 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |

| | | |
|---|---|---|
| Line | 113 | 280 |
| Object | _SERVER | outfile |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
113.        $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
280.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10563 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 118 | 280 |
| Object | _SERVER | outfile |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
118.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
280.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10564 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/dompdf.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | system/helpers/dompdf/dompdf.php |
| Line | 231 | 280 |
| Object | _SERVER | outfile |

Code Snippet

File Name system/helpers/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
231.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
280.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Path Traversal\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10565 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/www/examples.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in <?php at line 1 of system/helpers/dompdf/www/examples.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | system/helpers/dompdf/www/examples.php | system/helpers/dompdf/www/examples.php |
| Line | 57 | 57 |
| Object | _SERVER | dirname |

Code Snippet
File Name system/helpers/dompdf/www/examples.php
Method <?php

```
....
57.  $dompdf = dirname(dirname($_SERVER["PHP_SELF"]));
```

**Path Traversal\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10566 |
| Status | New |

Method <?php at line 1 of application/third_party/dompdf/dompdf.php gets dynamic data from the _GET element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 197 | 216 |
| Object | _GET | path |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
197.      $file = rawurldecode($_GET["input_file"]);
```

File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10567 |

| | |
|---|---|
| Status | New |

Method <?php at line 1 of application/third_party/dompdf/dompdf.php gets dynamic data from the _GET element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 212 | 216 |
| Object | _GET | path |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
212.      $base_path = rawurldecode($_GET["base_path"]);
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10568 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 74 | 216 |
| Object | _SERVER | path |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
74.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10569 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 81 | 216 |
| Object | _SERVER | path |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
81.         $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10570 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 88 | 216 |
| Object | _SERVER | path |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
88.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10571 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 95 | 216 |
| Object | _SERVER | path |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
95.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10572 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 112 | 216 |
| Object | _SERVER | path |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
112.        $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10573 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 117 | 216 |
| Object | _SERVER | path |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method function getoptions() {

```
....
117.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10574 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/dompdf.php gets dynamic data from the _GET element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 198 | 216 |
| Object | _GET | path |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
198.      $file = rawurldecode($_GET["input_file"]);
```

File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10575 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/dompdf.php gets dynamic data from the _GET element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 213 | 216 |
| Object | _GET | path |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
213.      $base_path = rawurldecode($_GET["base_path"]);
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10576 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |

| | | |
|---|---|---|
| Line | 75 | 216 |
| Object | _SERVER | path |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
75.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.            $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10577 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 82 | 216 |
| Object | _SERVER | path |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
82.         $opts["o"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.            $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10578 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 89 | 216 |
| Object | _SERVER | path |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
89.         $opts["b"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.            $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10579 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 96 | 216 |
| Object | _SERVER | path |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
96.         $opts["f"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10580 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 113 | 216 |
| Object | _SERVER | path |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method function getoptions() {

```
....
113.         $opts["t"] = $_SERVER['argv'][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10581 |
| Status | New |

Method getoptions at line 49 of system/helpers/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 118 | 216 |
| Object | _SERVER | path |

Code Snippet

File Name system/helpers/dompdf/dompdf.php

Method function getoptions() {

```
....
118.        $opts["filename"] = $_SERVER["argv"][$i];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10582 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 254 | 216 |
| Object | _SERVER | path |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
254.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10583 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 231 | 216 |
| Object | _SERVER | path |

Code Snippet

File Name system/helpers/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
231.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
216.          $path = rtrim(dirname($arr["path"]), '/\\') . "/";
```

**Path Traversal\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10584 |
| Status | New |

Method <?php at line 1 of application/third_party/dompdf/dompdf.php gets dynamic data from the _GET element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 197 | 243 |
| Object | _GET | url |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
197.      $file = rawurldecode($_GET["input_file"]);
```

File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
243.      $path = dirname($url);
```

**Path Traversal\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10585 |
| Status | New |

Method <?php at line 1 of application/third_party/dompdf/dompdf.php gets dynamic data from the _GET element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 212 | 243 |
| Object | _GET | url |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
212.      $base_path = rawurldecode($_GET["base_path"]);
```

File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
243.        $path = dirname($url);
```

**Path Traversal\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10586 |
| Status | New |

Method getoptions at line 48 of application/third_party/dompdf/dompdf.php gets dynamic data from the _SERVER element. This element's value then flows through the code and is eventually used in a file path for local disk access in explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php. This may cause a Path Traversal vulnerability.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 74 | 243 |
| Object | _SERVER | url |

Code Snippet

File Name application/third_party/dompdf/dompdf.php

Method function getoptions() {

```
....
74.         $opts["p"] = $_SERVER["argv"][$i+1];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
243.        $path = dirname($url);
```

## Stored File Manipulation

Query Path:

PHP\Cx\PHP Medium Threat\Stored File Manipulation Version:1

### Categories

FISMA 2014: Configuration Management
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A1-Broken Access Control

*Description*

**Stored File Manipulation\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=11343 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by delete_uploads in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_temp.php at line 164, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_temp.php |
| Line | 155 | 237 |
| Object | oci_fetch_assoc | BinaryExpr |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_temp.php

Method public function delete_uploads($maxdate)

```
....
237.
      unlink(FCPATH.'uploads/ba_implementasi/'.$init->init_ba);
```

**Stored File Manipulation\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11344 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by delete_uploads in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_temp.php at line 164, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_temp.php |
| Line | 155 | 234 |
| Object | oci_fetch_assoc | BinaryExpr |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

| | |
|---|---|
| Method | protected function _fetch_assoc() |

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_temp.php |
| Method | public function delete_uploads($maxdate) |

```
....
234.                                unlink(FCPATH.'dokumen_sik/'.$init-
>init_attachment);
```

**Stored File Manipulation\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11345 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by delete_uploads in the file application/controllers/script_temp.php at line 164, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/script_temp.php |
| Line | 155 | 237 |
| Object | oci_fetch_assoc | BinaryExpr |

| | |
|---|---|
| Code Snippet | |
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | application/controllers/script_temp.php |
| Method | public function delete_uploads($maxdate) |

```
....
237.
      unlink(FCPATH.'uploads/ba_implementasi/'.$init->init_ba);
```

**Stored File Manipulation\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11346 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by delete_uploads in the file application/controllers/script_temp.php at line 164, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/script_temp.php |
| Line | 155 | 234 |
| Object | oci_fetch_assoc | BinaryExpr |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/script_temp.php

Method public function delete_uploads($maxdate)

```
....
234.                                unlink(FCPATH.'dokumen_sik/'.$init->init_attachment);
```

**Stored File Manipulation\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11347 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by interface_ubah_data in the file application/controllers/maintenance_scheduler.php at line 16, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 498 |
| Object | oci_fetch_assoc | cl_upd |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | application/controllers/maintenance_scheduler.php |
| Method | public function interface_ubah_data($pass = '') |

```
....
498.                            $fwrite_result = fwrite($handle, $cl_upd);
```

**Stored File Manipulation\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11348 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by interface_ubah_data in the file application/controllers/maintenance_scheduler.php at line 16, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 458 |
| Object | oci_fetch_assoc | psw_upd_tid |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | application/controllers/maintenance_scheduler.php |
| Method | public function interface_ubah_data($pass = '') |

```
....
458.                            $fwrite_result = fwrite($handle,
$psw_upd_tid);
```

**Stored File Manipulation\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11349 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by interface_ubah_data in the file application/controllers/maintenance_scheduler.php at line 16, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 421 |
| Object | oci_fetch_assoc | psw_upd_mid |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
421.                            $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Stored File Manipulation\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11350 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by interface_ubah_data in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php at line 16, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php |
| Line | 155 | 498 |
| Object | oci_fetch_assoc | cl_upd |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php
Method public function interface_ubah_data($pass = '')

```
....
498.                            $fwrite_result = fwrite($handle, $cl_upd);
```

**Stored File Manipulation\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11351 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by interface_ubah_data in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php at line 16, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php |
| Line | 155 | 458 |
| Object | oci_fetch_assoc | psw_upd_tid |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php
Method public function interface_ubah_data($pass = '')

```
....
458.                            $fwrite_result = fwrite($handle,
$psw_upd_tid);
```

**Stored File Manipulation\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11352 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by interface_ubah_data in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php at line 16, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php |
| Line | 155 | 421 |
| Object | oci_fetch_assoc | psw_upd_mid |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
421.                            $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Stored File Manipulation\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11353 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php at line 103 is used to determine the location of a file to be written into by save in the file application/third_party/PHPExcel/Writer/HTML.php at line 151, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php | application/third_party/PHPExcel/Writer/HTML.php |
| Line | 118 | 178 |
| Object | _fileHandle | generateSheetData |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php
Method public function getCacheData($pCoord) {

```
....
118.             $this->_currentObject = unserialize(fread($this->_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/third_party/PHPExcel/Writer/HTML.php
Method public function save($pFilename = null) {

```
....
178.             fwrite($fileHandle, $this->generateSheetData());
```

**Stored File Manipulation\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11354 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php at line 111 is used to determine the location of a file to be written into by save in the file application/third_party/PHPExcel/Writer/HTML.php at line 151, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php | application/third_party/PHPExcel/Writer/HTML.php |
| Line | 126 | 178 |
| Object | _fileHandle | generateSheetData |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php
Method public function getCacheData($pCoord) {

```
....
126.             $this->_currentObject = unserialize(fread($this->_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Writer/HTML.php |
| Method | public function save($pFilename = null) { |

```
....
178.            fwrite($fileHandle, $this->generateSheetData());
```

**Stored File Manipulation\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11355 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/SQLite.php at line 99 is used to determine the location of a file to be written into by save in the file application/third_party/PHPExcel/Writer/HTML.php at line 151, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/Writer/HTML.php |
| Line | 117 | 178 |
| Object | fetchSingle | generateSheetData |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Method | public function getCacheData($pCoord) { |

```
....
117.            $cellResult = $cellResultSet->fetchSingle();
```

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Writer/HTML.php |
| Method | public function save($pFilename = null) { |

```
....
178.            fwrite($fileHandle, $this->generateSheetData());
```

**Stored File Manipulation\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11356 |
| Status | New |

The input obtained via _writeChartInCell in the file application/third_party/PHPExcel/Writer/HTML.php at line 629 is used to determine the location of a file to be written into by save in the file

application/third_party/PHPExcel/Writer/HTML.php at line 151, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Writer/HTML.php | application/third_party/PHPExcel/Writer/HTML.php |
| Line | 646 | 178 |
| Object | fp | generateSheetData |

Code Snippet
File Name application/third_party/PHPExcel/Writer/HTML.php
Method private function _writeChartInCell(PHPExcel_Worksheet $pSheet, $coordinates) {

```
....
646.                                        $picture =
fread($fp,filesize($chartFileName));
```

File Name application/third_party/PHPExcel/Writer/HTML.php
Method public function save($pFilename = null) {

```
....
178.                fwrite($fileHandle, $this->generateSheetData());
```

**Stored File Manipulation\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11357 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/Memcache.php at line 139 is used to determine the location of a file to be written into by save in the file application/third_party/PHPExcel/Writer/HTML.php at line 151, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php | application/third_party/PHPExcel/Writer/HTML.php |
| Line | 147 | 178 |
| Object | ".cache" | generateSheetData |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/Memcache.php
Method public function getCacheData($pCoord) {

```
....
147.                    $obj = $this->_memcache->get($this-
>_cachePrefix.$pCoord.'.cache');
```

File Name application/third_party/PHPExcel/Writer/HTML.php

Method public function save($pFilename = null) {

```
....
178.              fwrite($fileHandle, $this->generateSheetData());
```

**Stored File Manipulation\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11358 |
| Status | New |

The input obtained via _writeImageInCell in the file application/third_party/PHPExcel/Writer/HTML.php at line 567 is used to determine the location of a file to be written into by save in the file application/third_party/PHPExcel/Writer/HTML.php at line 151, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Writer/HTML.php | application/third_party/PHPExcel/Writer/HTML.php |
| Line | 599 | 178 |
| Object | fp | generateSheetData |

Code Snippet

File Name application/third_party/PHPExcel/Writer/HTML.php

Method private function _writeImageInCell(PHPExcel_Worksheet $pSheet, $coordinates) {

```
....
599.                                        $picture =
fread($fp,filesize($filename));
```

File Name application/third_party/PHPExcel/Writer/HTML.php

Method public function save($pFilename = null) {

```
....
178.              fwrite($fileHandle, $this->generateSheetData());
```

**Stored File Manipulation\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11359 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php at line 111 is used to determine the location of a file to be written into by _writeLine in the file application/third_party/PHPExcel/Writer/CSV.php at line 276, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php | application/third_party/PHPExcel/Writer/CSV.php |
| Line | 126 | 304 |
| Object | _fileHandle | mb_convert_encoding |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php

Method public function getCacheData($pCoord) {

```
....
126.                $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/third_party/PHPExcel/Writer/CSV.php

Method private function _writeLine($pFileHandle = null, $pValues = null) {

```
....
304.                            fwrite($pFileHandle,
mb_convert_encoding($line,"UTF-16LE","UTF-8"));
```

**Stored File Manipulation\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11360 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php at line 103 is used to determine the location of a file to be written into by _writeLine in the file application/third_party/PHPExcel/Writer/CSV.php at line 276, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php | application/third_party/PHPExcel/Writer/CSV.php |
| Line | 118 | 304 |

| | | |
|---|---|---|
| Object | _fileHandle | mb_convert_encoding |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php
Method public function getCacheData($pCoord) {

```
....
118.                $this->_currentObject = unserialize(fread($this->_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/third_party/PHPExcel/Writer/CSV.php
Method private function _writeLine($pFileHandle = null, $pValues = null) {

```
....
304.                            fwrite($pFileHandle, mb_convert_encoding($line,"UTF-16LE","UTF-8"));
```

**Stored File Manipulation\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11361 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/SQLite.php at line 99 is used to determine the location of a file to be written into by _writeLine in the file application/third_party/PHPExcel/Writer/CSV.php at line 276, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/Writer/CSV.php |
| Line | 117 | 304 |
| Object | fetchSingle | mb_convert_encoding |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php
Method public function getCacheData($pCoord) {

```
....
117.                $cellResult = $cellResultSet->fetchSingle();
```

File Name application/third_party/PHPExcel/Writer/CSV.php
Method private function _writeLine($pFileHandle = null, $pValues = null) {

```
....
304.                            fwrite($pFileHandle,
mb_convert_encoding($line,"UTF-16LE","UTF-8"));
```

**Stored File Manipulation\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11362 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/Memcache.php at line 139 is used to determine the location of a file to be written into by _writeLine in the file application/third_party/PHPExcel/Writer/CSV.php at line 276, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php | application/third_party/PHPExcel/Writer/CSV.php |
| Line | 147 | 304 |
| Object | ".cache" | mb_convert_encoding |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/Memcache.php

Method public function getCacheData($pCoord) {

```
....
147.                    $obj = $this->_memcache->get($this-
>_cachePrefix.$pCoord.'.cache');
```

File Name application/third_party/PHPExcel/Writer/CSV.php

Method private function _writeLine($pFileHandle = null, $pValues = null) {

```
....
304.                            fwrite($pFileHandle,
mb_convert_encoding($line,"UTF-16LE","UTF-8"));
```

**Stored File Manipulation\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11363 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php at line 111 is used to determine the location of a file to be written into by _writeLine in the file application/third_party/PHPExcel/Writer/CSV.php

at line 276, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php | application/third_party/PHPExcel/Writer/CSV.php |
| Line | 126 | 306 |
| Object | _fileHandle | line |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php
Method public function getCacheData($pCoord) {

```
....
126.                $this->_currentObject = unserialize(fread($this->_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/third_party/PHPExcel/Writer/CSV.php
Method private function _writeLine($pFileHandle = null, $pValues = null) {

```
....
306.                            fwrite($pFileHandle, $line);
```

**Stored File Manipulation\Path 22:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11364
Status New

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php at line 103 is used to determine the location of a file to be written into by _writeLine in the file application/third_party/PHPExcel/Writer/CSV.php at line 276, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php | application/third_party/PHPExcel/Writer/CSV.php |
| Line | 118 | 306 |
| Object | _fileHandle | line |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php
Method public function getCacheData($pCoord) {

```
....
118.                $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/third_party/PHPExcel/Writer/CSV.php

Method private function _writeLine($pFileHandle = null, $pValues = null) {

```
....
306.                            fwrite($pFileHandle, $line);
```

**Stored File Manipulation\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11365 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/SQLite.php at line 99 is used to determine the location of a file to be written into by _writeLine in the file application/third_party/PHPExcel/Writer/CSV.php at line 276, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/Writer/CSV.php |
| Line | 117 | 306 |
| Object | fetchSingle | line |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php

Method public function getCacheData($pCoord) {

```
....
117.                $cellResult = $cellResultSet->fetchSingle();
```

File Name application/third_party/PHPExcel/Writer/CSV.php

Method private function _writeLine($pFileHandle = null, $pValues = null) {

```
....
306.                            fwrite($pFileHandle, $line);
```

**Stored File Manipulation\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=11366 |
| Status | New |

The input obtained via getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/Memcache.php at line 139 is used to determine the location of a file to be written into by _writeLine in the file application/third_party/PHPExcel/Writer/CSV.php at line 276, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php | application/third_party/PHPExcel/Writer/CSV.php |
| Line | 147 | 306 |
| Object | ".cache" | line |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/Memcache.php

Method public function getCacheData($pCoord) {

```
....
147.                    $obj = $this->_memcache->get($this-
>_cachePrefix.$pCoord.'.cache');
```

File Name application/third_party/PHPExcel/Writer/CSV.php

Method private function _writeLine($pFileHandle = null, $pValues = null) {

```
....
306.                        fwrite($pFileHandle, $line);
```

**Stored File Manipulation\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11367 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by qc_interface_send in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php at line 705, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php |
| Line | 155 | 1133 |
| Object | oci_fetch_assoc | cl_upd |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php
Method public function qc_interface_send($pass = '')

```
....
1133.                        $fwrite_result = fwrite($handle, $cl_upd);
```

**Stored File Manipulation\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11368 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by qc_interface_send in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php at line 705, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php |
| Line | 155 | 1094 |
| Object | oci_fetch_assoc | psw_upd_tid |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php
Method public function qc_interface_send($pass = '')

```
....
1094.                        $fwrite_result = fwrite($handle,
$psw_upd_tid);
```

**Stored File Manipulation\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11369 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by qc_interface_send in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php at line 705, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php |
| Line | 155 | 1057 |
| Object | oci_fetch_assoc | psw_upd_mid |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php

Method public function qc_interface_send($pass = '')

```
....
1057.                           $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Stored File Manipulation\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11370 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by qc_interface_send in the file application/controllers/maintenance_scheduler.php at line 705, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_resul | application/controllers/maintenance_sch |

| | t.php | eduler.php |
|---|---|---|
| Line | 155 | 1133 |
| Object | oci_fetch_assoc | cl_upd |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php
Method public function qc_interface_send($pass = '')

```
....
1133.                       $fwrite_result = fwrite($handle, $cl_upd);
```

**Stored File Manipulation\Path 29:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11371
Status New

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by qc_interface_send in the file application/controllers/maintenance_scheduler.php at line 705, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 1094 |
| Object | oci_fetch_assoc | psw_upd_tid |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php
Method public function qc_interface_send($pass = '')

```
....
1094.                          $fwrite_result = fwrite($handle,
$psw_upd_tid);
```

**Stored File Manipulation\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11372 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by qc_interface_send in the file application/controllers/maintenance_scheduler.php at line 705, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 1057 |
| Object | oci_fetch_assoc | psw_upd_mid |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function qc_interface_send($pass = '')

```
....
1057.                          $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Stored File Manipulation\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11373 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_tid_psw in the file application/libraries/file_interface_lib.php at line 2368, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/libraries/file_interface_lib.php |
| Line | 155 | 2391 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/libraries/file_interface_lib.php
Method function checking_tid_psw($tid, $ymd, $type)

```
....
2391.                                fclose($handle);
```

**Stored File Manipulation\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11374 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_tid_psw in the file application/libraries/file_interface_lib.php at line 2368, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/libraries/file_interface_lib.php |
| Line | 155 | 2396 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/libraries/file_interface_lib.php

| | |
|---|---|
| Method | function checking_tid_psw($tid, $ymd, $type) |

```
....
2396.                                   fclose($handle);
```

**Stored File Manipulation\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11375 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_tid_psw in the file application/libraries/file_interface_lib.php at line 2368, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/libraries/file_interface_lib.php |
| Line | 155 | 2404 |
| Object | oci_fetch_assoc | handle |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                 return oci_fetch_assoc($id);
```

File Name application/libraries/file_interface_lib.php

Method function checking_tid_psw($tid, $ymd, $type)

```
....
2404.                fclose($handle);
```

**Stored File Manipulation\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11376 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_tid_psw in the file application/views/aplikasi_merchant/file_interface_lib.php at line 2310, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2333 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/views/aplikasi_merchant/file_interface_lib.php

Method function checking_tid_psw($tid, $ymd, $type)

```
....
2333.                                fclose($handle);
```

**Stored File Manipulation\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11377 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_tid_psw in the file application/views/aplikasi_merchant/file_interface_lib.php at line 2310, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2338 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/views/aplikasi_merchant/file_interface_lib.php

| | |
|---|---|
| Method | function checking_tid_psw($tid, $ymd, $type) |

```
....
2338.                                   fclose($handle);
```

**Stored File Manipulation\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11378 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_tid_psw in the file application/views/aplikasi_merchant/file_interface_lib.php at line 2310, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2346 |
| Object | oci_fetch_assoc | handle |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.                 return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | application/views/aplikasi_merchant/file_interface_lib.php |
| Method | function checking_tid_psw($tid, $ymd, $type) |

```
....
2346.                fclose($handle);
```

**Stored File Manipulation\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11379 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_tid_psw in the file BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php at line 2310, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2333 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php
Method function checking_tid_psw($tid, $ymd, $type)

```
....
2333.                                fclose($handle);
```

**Stored File Manipulation\Path 38:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11380
Status New

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_tid_psw in the file BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php at line 2310, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2338 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php

Method function checking_tid_psw($tid, $ymd, $type)

```
....
2338.                                   fclose($handle);
```

**Stored File Manipulation\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11381 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_tid_psw in the file BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php at line 2310, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2346 |
| Object | oci_fetch_assoc | handle |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                    return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php

Method function checking_tid_psw($tid, $ymd, $type)

```
....
2346.                   fclose($handle);
```

**Stored File Manipulation\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11382 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_mid_psw in the file application/libraries/file_interface_lib.php at line 2191, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/libraries/file_interface_lib.php |
| Line | 155 | 2214 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/libraries/file_interface_lib.php
Method function checking_mid_psw($mid, $ymd, $type)

```
....
2214.                                fclose($handle);
```

**Stored File Manipulation\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11383 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_mid_psw in the file application/libraries/file_interface_lib.php at line 2191, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/libraries/file_interface_lib.php |
| Line | 155 | 2219 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/libraries/file_interface_lib.php

Method function checking_mid_psw($mid, $ymd, $type)

```
....
2219.                               fclose($handle);
```

**Stored File Manipulation\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11384 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_mid_psw in the file application/libraries/file_interface_lib.php at line 2191, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/libraries/file_interface_lib.php |
| Line | 155 | 2227 |
| Object | oci_fetch_assoc | handle |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/libraries/file_interface_lib.php

Method function checking_mid_psw($mid, $ymd, $type)

```
....
2227.               fclose($handle);
```

**Stored File Manipulation\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11385 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_mid_psw in the file application/views/aplikasi_merchant/file_interface_lib.php at line 2133, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2156 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/views/aplikasi_merchant/file_interface_lib.php

Method function checking_mid_psw($mid, $ymd, $type)

```
....
2156.                                fclose($handle);
```

**Stored File Manipulation\Path 44:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11386
Status New

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_mid_psw in the file application/views/aplikasi_merchant/file_interface_lib.php at line 2133, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2161 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/views/aplikasi_merchant/file_interface_lib.php

Method function checking_mid_psw($mid, $ymd, $type)

```
....
2161.                               fclose($handle);
```

**Stored File Manipulation\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11387 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_mid_psw in the file application/views/aplikasi_merchant/file_interface_lib.php at line 2133, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2169 |
| Object | oci_fetch_assoc | handle |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/views/aplikasi_merchant/file_interface_lib.php

Method function checking_mid_psw($mid, $ymd, $type)

```
....
2169.               fclose($handle);
```

**Stored File Manipulation\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11388 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_mid_psw in the file BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php at line 2133, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2156 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php
Method function checking_mid_psw($mid, $ymd, $type)

```
....
2156.                                fclose($handle);
```

**Stored File Manipulation\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11389 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_mid_psw in the file BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php at line 2133, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2161 |
| Object | oci_fetch_assoc | handle |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php

| | |
|---|---|
| Method | protected function _fetch_assoc() |

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php |
| Method | function checking_mid_psw($mid, $ymd, $type) |

```
....
2161.                               fclose($handle);
```

**Stored File Manipulation\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11390 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by checking_mid_psw in the file BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php at line 2133, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php |
| Line | 155 | 2169 |
| Object | oci_fetch_assoc | handle |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_merchant/file_interface_lib.php |
| Method | function checking_mid_psw($mid, $ymd, $type) |

```
....
2169.               fclose($handle);
```

**Stored File Manipulation\Path 49:**

| | |
|---|---|
| Severity | Medium |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11391 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by merchant_excel_generate in the file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php at line 1999, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php |
| Line | 155 | 2020 |
| Object | oci_fetch_assoc | m |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php

Method public function merchant_excel_generate()

```
....
2020.                    fputcsv($output, $m);
```

**Stored File Manipulation\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11392 |
| Status | New |

The input obtained via _fetch_assoc in the file system/database/drivers/oci8/oci8_result.php at line 152 is used to determine the location of a file to be written into by merchant_excel_generate in the file application/controllers/admin.php at line 2403, potentially allowing an attacker to alter or corrupt the contents of that file, or create a new file altogether.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/admin.php |
| Line | 155 | 2424 |
| Object | oci_fetch_assoc | m |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.            return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | application/controllers/admin.php |
| Method | public function merchant_excel_generate() |

```
....
2424.                fputcsv($output, $m);
```

## Use of Hard coded Cryptographic Key

Query Path:
PHP\Cx\PHP Medium Threat\Use of Hard coded Cryptographic Key Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage
OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A2-Cryptographic Failures

*Description*

**Use of Hard coded Cryptographic Key\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11622 |
| Status | New |

The variable encryption_key at line 1 of application/config/config.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | application/config/config.php | application/config/config.php |
| Line | 231 | 231 |
| Object | encryption_key | encryption_key |

| | |
|---|---|
| Code Snippet | |
| File Name | application/config/config.php |
| Method | <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed'); |

```
....
231.  $config['encryption_key'] = 'mms12345';
```

**Use of Hard coded Cryptographic Key\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11623 |
| Status | New |

The variable encryption_key at line 1 of application/config/config_20210615.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | application/config/config_20210615.php | application/config/config_20210615.php |
| Line | 231 | 231 |
| Object | encryption_key | encryption_key |

Code Snippet
File Name application/config/config_20210615.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
231.  $config['encryption_key'] = 'mms12345';
```

**Use of Hard coded Cryptographic Key\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11624 |
| Status | New |

The variable "user" at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1827 | 253 |
| Object | "user" | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1827.        $this->o_encryption($this->numObj, 'new',
array('user'=>$userPass, 'owner'=>$ownerPass, 'p'=>$p));
```

File Name system/helpers/dompdf/lib/class.pdf.php
Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11625 |
| Status | New |

The variable "11000000" at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1807 | 253 |
| Object | "11000000" | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1807.      $p = bindec("11000000");
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11626 |
| Status | New |

The variable "print" at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1809 | 253 |
| Object | "print" | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1809.      $options =  array('print'=>4, 'modify'=>8, 'copy'=>16,
'add'=>32);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11627 |
| Status | New |

The variable 32 at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1809 | 253 |
| Object | 32 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1809.      $options =  array('print'=>4, 'modify'=>8, 'copy'=>16,
'add'=>32);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11628 |
| Status | New |

The variable "add" at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |

| | | |
|---|---|---|
| Line | 1809 | 253 |
| Object | "add" | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1809.      $options =  array('print'=>4, 'modify'=>8, 'copy'=>16,
'add'=>32);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11629 |
| Status | New |

The variable 16 at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1809 | 253 |
| Object | 16 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1809.      $options =  array('print'=>4, 'modify'=>8, 'copy'=>16,
'add'=>32);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11630 |
| Status | New |

The variable "copy" at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1809 | 253 |
| Object | "copy" | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1809.      $options =  array('print'=>4, 'modify'=>8, 'copy'=>16,
'add'=>32);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11631 |
| Status | New |

The variable 8 at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1809 | 253 |
| Object | 8 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1809.      $options =  array('print'=>4, 'modify'=>8, 'copy'=>16,
'add'=>32);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11632 |
| Status | New |

The variable "modify" at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1809 | 253 |
| Object | "modify" | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1809.      $options =  array('print'=>4, 'modify'=>8, 'copy'=>16,
'add'=>32);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11633 |
| Status | New |

The variable 4 at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1809 | 253 |
| Object | 4 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1809.      $options =  array('print'=>4, 'modify'=>8, 'copy'=>16,
'add'=>32);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11634 |
| Status | New |

The variable "p" at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1827 | 253 |
| Object | "p" | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1827.        $this->o_encryption($this->numObj, 'new',
array('user'=>$userPass, 'owner'=>$ownerPass, 'p'=>$p));
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11635 |
| Status | New |

The variable "owner" at line 1806 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1827 | 253 |
| Object | "owner" | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1827.        $this->o_encryption($this->numObj, 'new',
array('user'=>$userPass, 'owner'=>$ownerPass, 'p'=>$p));
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11636 |
| Status | New |

The variable 32 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1655 | 253 |
| Object | 32 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1655.          $user =  substr($options['user'], 0, 32);
```

File Name system/helpers/dompdf/lib/class.pdf.php
Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11637 |
| Status | New |

The variable 0 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1655 | 253 |
| Object | 0 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1655.          $user =  substr($options['user'], 0, 32);
```

File Name system/helpers/dompdf/lib/class.pdf.php
Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11638 |
| Status | New |

The variable 250 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1639 | 253 |
| Object | 250 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method protected function o_encryption($id, $action, $options = '') {

```
....
1639.                .chr(0x64) .chr(0x00) .chr(0x4E) .chr(0x56)
.chr(0xFF) .chr(0xFA) .chr(0x01) .chr(0x08)
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11639 |
| Status | New |

The variable 1 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1639 | 253 |
| Object | 1 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method protected function o_encryption($id, $action, $options = '') {

```
....
1639.                .chr(0x64) .chr(0x00) .chr(0x4E) .chr(0x56)
.chr(0xFF) .chr(0xFA) .chr(0x01) .chr(0x08)
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11640 |
| Status | New |

The variable 8 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1639 | 253 |
| Object | 8 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method protected function o_encryption($id, $action, $options = '') {

```
....
1639.                .chr(0x64) .chr(0x00) .chr(0x4E) .chr(0x56)
.chr(0xFF) .chr(0xFA) .chr(0x01) .chr(0x08)
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11641 |
| Status | New |

The variable 46 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1640 | 253 |
| Object | 46 | encryptionKey |

Code Snippet

| | |
|---|---|
| File Name | system/helpers/dompdf/lib/class.pdf.php |
| Method | protected function o_encryption($id, $action, $options = '') { |

```
....
1640.                .chr(0x2E) .chr(0x2E) .chr(0x00) .chr(0xB6)
.chr(0xD0) .chr(0x68) .chr(0x3E) .chr(0x80)
```

| | |
|---|---|
| File Name | system/helpers/dompdf/lib/class.pdf.php |
| Method | public $encryptionKey = ''; |

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11642 |
| Status | New |

The variable 46 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1640 | 253 |
| Object | 46 | encryptionKey |

Code Snippet

| | |
|---|---|
| File Name | system/helpers/dompdf/lib/class.pdf.php |
| Method | protected function o_encryption($id, $action, $options = '') { |

```
....
1640.                .chr(0x2E) .chr(0x2E) .chr(0x00) .chr(0xB6)
.chr(0xD0) .chr(0x68) .chr(0x3E) .chr(0x80)
```

| | |
|---|---|
| File Name | system/helpers/dompdf/lib/class.pdf.php |
| Method | public $encryptionKey = ''; |

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11643 |
| Status | New |

The variable 0 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1640 | 253 |
| Object | 0 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1640.                .chr(0x2E) .chr(0x2E) .chr(0x00) .chr(0xB6)
.chr(0xD0) .chr(0x68) .chr(0x3E) .chr(0x80)
```

File Name system/helpers/dompdf/lib/class.pdf.php
Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11644 |
| Status | New |

The variable 182 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1640 | 253 |
| Object | 182 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1640.                .chr(0x2E) .chr(0x2E) .chr(0x00) .chr(0xB6)
.chr(0xD0) .chr(0x68) .chr(0x3E) .chr(0x80)
```

File Name system/helpers/dompdf/lib/class.pdf.php

| | |
|---|---|
| Method | public $encryptionKey = ''; |

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11645 |
| Status | New |

The variable 208 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1640 | 253 |
| Object | 208 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method protected function o_encryption($id, $action, $options = '') {

```
....
1640.                .chr(0x2E) .chr(0x2E) .chr(0x00) .chr(0xB6)
.chr(0xD0) .chr(0x68) .chr(0x3E) .chr(0x80)
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11646 |
| Status | New |

The variable 104 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1640 | 253 |
| Object | 104 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1640.                .chr(0x2E) .chr(0x2E) .chr(0x00) .chr(0xB6)
.chr(0xD0) .chr(0x68) .chr(0x3E) .chr(0x80)
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 26:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11647
Status New

The variable 62 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1640 | 253 |
| Object | 62 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1640.                .chr(0x2E) .chr(0x2E) .chr(0x00) .chr(0xB6)
.chr(0xD0) .chr(0x68) .chr(0x3E) .chr(0x80)
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 27:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti

| | |
|---|---|
| | d=4881&pathid=11648 |
| Status | New |

The variable 128 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1640 | 253 |
| Object | 128 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1640.                .chr(0x2E) .chr(0x2E) .chr(0x00) .chr(0xB6)
.chr(0xD0) .chr(0x68) .chr(0x3E) .chr(0x80)
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11649 |
| Status | New |

The variable 2 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1641 | 253 |
| Object | 2 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1641.                .chr(0x2F) .chr(0x0C) .chr(0xA9) .chr(0xFE)
.chr(0x64) .chr(0x53) .chr(0x69) .chr(0x7A);
```

| | |
|---|---|
| File Name | system/helpers/dompdf/lib/class.pdf.php |
| Method | public $encryptionKey = ''; |

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11650 |
| Status | New |

The variable 12 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1641 | 253 |
| Object | 12 | encryptionKey |

Code Snippet

| | |
|---|---|
| File Name | system/helpers/dompdf/lib/class.pdf.php |
| Method | protected function o_encryption($id, $action, $options = '') { |

```
....
1641.                .chr(0x2F) .chr(0x0C) .chr(0xA9) .chr(0xFE)
.chr(0x64) .chr(0x53) .chr(0x69) .chr(0x7A);
```

| | |
|---|---|
| File Name | system/helpers/dompdf/lib/class.pdf.php |
| Method | public $encryptionKey = ''; |

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11651 |
| Status | New |

The variable 169 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1641 | 253 |

| | | |
|---|---|---|
| Object | 169 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1641.                .chr(0x2F) .chr(0x0C) .chr(0xA9) .chr(0xFE)
.chr(0x64) .chr(0x53) .chr(0x69) .chr(0x7A);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11652 |
| Status | New |

The variable 254 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1641 | 253 |
| Object | 254 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1641.                .chr(0x2F) .chr(0x0C) .chr(0xA9) .chr(0xFE)
.chr(0x64) .chr(0x53) .chr(0x69) .chr(0x7A);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 32:**

| | |
|---|---|
| Severity | Medium |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11653 |
| Status | New |

The variable 100 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1641 | 253 |
| Object | 100 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method protected function o_encryption($id, $action, $options = '') {

```
....
1641.                .chr(0x2F) .chr(0x0C) .chr(0xA9) .chr(0xFE)
.chr(0x64) .chr(0x53) .chr(0x69) .chr(0x7A);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11654 |
| Status | New |

The variable 83 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1641 | 253 |
| Object | 83 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method protected function o_encryption($id, $action, $options = '') {

```
....
1641.                .chr(0x2F) .chr(0x0C) .chr(0xA9) .chr(0xFE)
.chr(0x64) .chr(0x53) .chr(0x69) .chr(0x7A);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11655 |
| Status | New |

The variable 105 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1641 | 253 |
| Object | 105 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method protected function o_encryption($id, $action, $options = '') {

```
....
1641.                .chr(0x2F) .chr(0x0C) .chr(0xA9) .chr(0xFE)
.chr(0x64) .chr(0x53) .chr(0x69) .chr(0x7A);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11656 |
| Status | New |

The variable 122 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |

| | | |
|---|---|---|
| Line | 1641 | 253 |
| Object | 122 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1641.                .chr(0x2F) .chr(0x0C) .chr(0xA9) .chr(0xFE)
.chr(0x64) .chr(0x53) .chr(0x69) .chr(0x7A);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11657 |
| Status | New |

The variable 32 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1657 | 253 |
| Object | 32 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1657.          $user =  $options['user'].substr($pad, 0, 32-$len);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11658 |
| Status | New |

The variable "8bit" at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1653 | 253 |
| Object | "8bit" | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method protected function o_encryption($id, $action, $options = '') {

```
....
1653.        $len =  mb_strlen($options['user'], '8bit');
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11659 |
| Status | New |

The variable 0 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1657 | 253 |
| Object | 0 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method protected function o_encryption($id, $action, $options = '') {

```
....
1657.          $user =  $options['user'].substr($pad, 0, 32-$len);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11660 |
| Status | New |

The variable 255 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1669 | 253 |
| Object | 255 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method protected function o_encryption($id, $action, $options = '') {

```
....
1669.        $tmp =  $this->md5_16($user.$ovalue.chr($options['p'])
.chr(255) .chr(255) .chr(255) .$this->fileIdentifier);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11661 |
| Status | New |

The variable 255 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |

| | | |
|---|---|---|
| Line | 1669 | 253 |
| Object | 255 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1669.        $tmp =  $this->md5_16($user.$ovalue.chr($options['p'])
.chr(255) .chr(255) .chr(255) .$this->fileIdentifier);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11662 |
| Status | New |

The variable 255 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1669 | 253 |
| Object | 255 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1669.        $tmp =  $this->md5_16($user.$ovalue.chr($options['p'])
.chr(255) .chr(255) .chr(255) .$this->fileIdentifier);
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11663 |
| Status | New |

The variable 2 at line 1704 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1708 | 253 |
| Object | 2 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function md5_16($string) {

```
....
1708.        $out.= chr(hexdec(substr($tmp, $i, 2)));
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11664 |
| Status | New |

The variable 0 at line 1704 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1707 | 253 |
| Object | 0 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function md5_16($string) {

```
....
1707.      for  ($i = 0;$i <= 30;$i = $i+2) {
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11665 |
| Status | New |

The variable 2 at line 1704 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1707 | 253 |
| Object | 2 | encryptionKey |

Code Snippet

File Name system/helpers/dompdf/lib/class.pdf.php

Method function md5_16($string) {

```
....
1707.      for  ($i = 0;$i <= 30;$i = $i+2) {
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11666 |
| Status | New |

The variable 5 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1671 | 253 |
| Object | 5 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1671.        $ukey =  substr($tmp, 0, 5);
```

File Name system/helpers/dompdf/lib/class.pdf.php
Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11667 |
| Status | New |

The variable 0 at line 1626 of system/helpers/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1671 | 253 |
| Object | 0 | encryptionKey |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method protected function o_encryption($id, $action, $options = '') {

```
....
1671.        $ukey =  substr($tmp, 0, 5);
```

File Name system/helpers/dompdf/lib/class.pdf.php
Method public $encryptionKey = '';

```
....
253.    public  $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11668 |
| Status | New |

The variable "user" at line 1812 of application/third_party/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/lib/class.pdf.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 1833 | 252 |
| Object | "user" | encryptionKey |

Code Snippet

File Name application/third_party/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1833.        $this->o_encryption($this->numObj, 'new', array('user' =>
$userPass, 'owner' => $ownerPass, 'p' => $p));
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
252.    public $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11669 |
| Status | New |

The variable "11000000" at line 1812 of application/third_party/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/lib/class.pdf.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 1813 | 252 |
| Object | "11000000" | encryptionKey |

Code Snippet

File Name application/third_party/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1813.      $p = bindec("11000000");
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
252.    public $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11670 |
| Status | New |

The variable "print" at line 1812 of application/third_party/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/lib/class.pdf.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 1815 | 252 |
| Object | "print" | encryptionKey |

Code Snippet

File Name application/third_party/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1815.      $options = array('print' => 4, 'modify' => 8, 'copy' => 16,
'add' => 32);
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
252.    public $encryptionKey = '';
```

**Use of Hard coded Cryptographic Key\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11671 |
| Status | New |

The variable 32 at line 1812 of application/third_party/dompdf/lib/class.pdf.php is assigned a hardcoded, literal value. This static value is used as an encryption key.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/lib/class.pdf.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 1815 | 252 |
| Object | 32 | encryptionKey |

Code Snippet

File Name application/third_party/dompdf/lib/class.pdf.php

Method function setEncryption($userPass = '', $ownerPass = '', $pc = array()) {

```
....
1815.      $options = array('print' => 4, 'modify' => 8, 'copy' => 16,
'add' => 32);
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method public $encryptionKey = '';

```
....
252.    public $encryptionKey = '';
```

## Header Injection

Query Path:

PHP\Cx\PHP Medium Threat\Header Injection Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
FISMA 2014: Configuration Management
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

*Description*

**Header Injection\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11254 |
| Status | New |

Method data_upload at line 15 of application/controllers/restore.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in data_upload at line 15 of application/controllers/restore.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/restore.php | application/controllers/restore.php |

| | | |
|---|---|---|
| Line | 30 | 129 |
| Object | post | local_file |

Code Snippet
File Name application/controllers/restore.php
Method public function data_upload()

```
....
30.                 $jenis = $this->input->post('jenis');
....
129.                                $is_get = ftp_get($conn,
$local_file, $remote_file, FTP_BINARY);
```

**Header Injection\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11255 |
| Status | New |

Method post at line 172 of system/core/Input.php receives a user input from the _POST element. This element's value then copied into the request header without being properly sanitized or validated in data_upload at line 15 of application/controllers/restore.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/restore.php |
| Line | 182 | 129 |
| Object | _POST | local_file |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/restore.php
Method public function data_upload()

```
....
129.                                $is_get = ftp_get($conn,
$local_file, $remote_file, FTP_BINARY);
```

**Header Injection\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11256 |
| Status | New |

Method data_upload at line 15 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in data_upload at line 15 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php |
| Line | 30 | 129 |
| Object | post | local_file |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php |
| Method | public function data_upload() |

```
....
30.                 $jenis = $this->input->post('jenis');
....
129.                                  $is_get = ftp_get($conn,
$local_file, $remote_file, FTP_BINARY);
```

**Header Injection\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11257 |
| Status | New |

Method post at line 172 of system/core/Input.php receives a user input from the _POST element. This element's value then copied into the request header without being properly sanitized or validated in data_upload at line 15 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php |
| Line | 182 | 129 |
| Object | _POST | local_file |

| | |
|---|---|
| Code Snippet | |
| File Name | system/core/Input.php |
| Method | function post($index = NULL, $xss_clean = FALSE) |

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php

Method public function data_upload()

```
....
129.                                $is_get = ftp_get($conn,
$local_file, $remote_file, FTP_BINARY);
```

**Header Injection\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11258 |
| Status | New |

Method getnik at line 1573 of application/controllers/aplikasi_tambah_merchant/input_merchant.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in getnik at line 1573 of application/controllers/aplikasi_tambah_merchant/input_merchant.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 1589 | 1598 |
| Object | post | json_encode |

Code Snippet

File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php

Method public function getnik(){

```
....
1589.                               "NAMA_LENGKAP"    =>
strtoupper(trim($this->input->post('nama'))),
....
1598.                     curl_setopt($ch, CURLOPT_POSTFIELDS,
json_encode($data));
```

**Header Injection\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11259 |
| Status | New |

Method post at line 172 of system/core/Input.php receives a user input from the _POST element. This element's value then copied into the request header without being properly sanitized or validated in getnik at line 1573 of application/controllers/aplikasi_tambah_merchant/input_merchant.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 182 | 1598 |
| Object | _POST | json_encode |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php
Method public function getnik(){

```
....
1598.                   curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($data));
```

**Header Injection\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11260 |
| Status | New |

Method getnik at line 1573 of application/controllers/aplikasi_tambah_merchant/input_merchant.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in getnik at line 1573 of application/controllers/aplikasi_tambah_merchant/input_merchant.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 1588 | 1598 |
| Object | post | json_encode |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php

| | |
|---|---|
| Method | public function getnik(){ |

```
....
1588.                                "NIK"                    =>
strtoupper(trim($this->input->post('nik'))),
....
1598.                    curl_setopt($ch, CURLOPT_POSTFIELDS,
json_encode($data));
```

**Header Injection\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11261 |
| Status | New |

Method cm_penarikan_approve at line 2241 of application/controllers/maintenance_20190524.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | application/controllers/patching.php |
| Line | 2246 | 956 |
| Object | post | array |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/maintenance_20190524.php |
| Method | function cm_penarikan_approve() |

```
....
2246.             $tid        = $this->input->post('tid');
```

| | |
|---|---|
| File Name | application/controllers/patching.php |
| Method | function delete_tid_brilink($tid) { |

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11262 |
| Status | New |

Method post at line 172 of system/core/Input.php receives a user input from the _POST element. This element's value then copied into the request header without being properly sanitized or validated in

delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/patching.php |
| Line | 182 | 956 |
| Object | _POST | array |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.            curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 10:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11263
Status New

Method cm_penarikan_approve at line 2246 of application/controllers/maintenance_20190610.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | application/controllers/patching.php |
| Line | 2251 | 956 |
| Object | post | array |

Code Snippet
File Name application/controllers/maintenance_20190610.php
Method function cm_penarikan_approve()

```
....
2251.             $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11264 |
| Status | New |

Method cm_penarikan_approve at line 2213 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php | application/controllers/patching.php |
| Line | 2218 | 956 |
| Object | post | array |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php

Method function cm_penarikan_approve()

```
....
2218.             $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11265 |
| Status | New |

Method cm_penarikan_approve at line 2239 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php | application/controllers/patching.php |
| Line | 2244 | 956 |
| Object | post | array |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php

Method function cm_penarikan_approve()

```
....
2244.             $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11266 |
| Status | New |

Method cm_penarikan_approve at line 2073 of application/controllers/maintenance_bck07112017.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck07112017.php | application/controllers/patching.php |

| | | |
|---|---|---|
| Line | 2078 | 956 |
| Object | post | array |

Code Snippet
File Name application/controllers/maintenance_bck07112017.php
Method function cm_penarikan_approve()

```
....
2078.            $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11267 |
| Status | New |

Method cm_penarikan_approve at line 2073 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php | application/controllers/patching.php |
| Line | 2078 | 956 |
| Object | post | array |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php
Method function cm_penarikan_approve()

```
....
2078.            $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php

| | |
|---|---|
| Method | function delete_tid_brilink($tid) { |

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11268 |
| Status | New |

Method cm_penarikan_approve at line 2213 of application/controllers/maintenance_bck20180906.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20180906.php | application/controllers/patching.php |
| Line | 2218 | 956 |
| Object | post | array |

Code Snippet

File Name application/controllers/maintenance_bck20180906.php

Method function cm_penarikan_approve()

```
....
2218.             $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11269 |
| Status | New |

Method cm_penarikan_approve at line 2284 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or

validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php | application/controllers/patching.php |
| Line | 2289 | 956 |
| Object | post | array |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php
Method function cm_penarikan_approve()

```
....
2289.             $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11270 |
| Status | New |

Method cm_penarikan_approve at line 2239 of application/controllers/maintenance_bck20190114.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20190114.php | application/controllers/patching.php |
| Line | 2244 | 956 |
| Object | post | array |

Code Snippet
File Name application/controllers/maintenance_bck20190114.php
Method function cm_penarikan_approve()

```
....
2244.             $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11271 |
| Status | New |

Method cm_penarikan_approve at line 2225 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php | application/controllers/patching.php |
| Line | 2230 | 956 |
| Object | post | array |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php

Method function cm_penarikan_approve()

```
....
2230.             $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11272 |
| Status | New |

Method cm_penarikan_approve at line 2284 of application/controllers/maintenance.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | application/controllers/patching.php |
| Line | 2289 | 956 |
| Object | post | array |

Code Snippet

File Name application/controllers/maintenance.php

Method function cm_penarikan_approve()

```
....
2289.             $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11273 |
| Status | New |

Method cm_penarikan_approve at line 2241 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php | application/controllers/patching.php |
| Line | 2246 | 956 |

| | | |
|---|---|---|
| Object | post | array |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php
Method function cm_penarikan_approve()

```
....
2246.            $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11274 |
| Status | New |

Method cm_penarikan_approve at line 2225 of application/controllers/maintenance_20181213.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20181213.php | application/controllers/patching.php |
| Line | 2230 | 956 |
| Object | post | array |

Code Snippet
File Name application/controllers/maintenance_20181213.php
Method function cm_penarikan_approve()

```
....
2230.            $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11275 |
| Status | New |

Method cm_penarikan_approve at line 2246 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of application/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php | application/controllers/patching.php |
| Line | 2251 | 956 |
| Object | post | array |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php

Method function cm_penarikan_approve()

```
....
2251.             $tid        = $this->input->post('tid');
```

File Name application/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11276 |
| Status | New |

Method data_upload at line 15 of application/controllers/restore.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated

in data_upload at line 15 of application/controllers/restore.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/restore.php | application/controllers/restore.php |
| Line | 30 | 129 |
| Object | post | remote_file |

Code Snippet
File Name application/controllers/restore.php
Method public function data_upload()

```
....
30.                 $jenis = $this->input->post('jenis');
....
129.                                $is_get = ftp_get($conn,
$local_file, $remote_file, FTP_BINARY);
```

**Header Injection\Path 24:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11277
Status New

Method post at line 172 of system/core/Input.php receives a user input from the _POST element. This element's value then copied into the request header without being properly sanitized or validated in data_upload at line 15 of application/controllers/restore.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/restore.php |
| Line | 182 | 129 |
| Object | _POST | remote_file |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/restore.php
Method public function data_upload()

```
....
129.                                $is_get = ftp_get($conn,
$local_file, $remote_file, FTP_BINARY);
```

**Header Injection\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11278 |
| Status | New |

Method cekkartu at line 442 of application/controllers/settlement.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in cek_no_kartu at line 369 of application/controllers/settlement.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/settlement.php | application/controllers/settlement.php |
| Line | 444 | 377 |
| Object | post | postString |

Code Snippet

File Name application/controllers/settlement.php

Method function cekkartu(){

```
....
444.              $no_kartu = $this->input->post('nokartu');
```

File Name application/controllers/settlement.php

Method public function cek_no_kartu($data){

```
....
377.              curl_setopt($ch, CURLOPT_POSTFIELDS, $postString);
```

**Header Injection\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11279 |
| Status | New |

Method post at line 172 of system/core/Input.php receives a user input from the _POST element. This element's value then copied into the request header without being properly sanitized or validated in cek_no_kartu at line 369 of application/controllers/settlement.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | system/core/Input.php | application/controllers/settlement.php |
| Line | 182 | 377 |
| Object | _POST | postString |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/settlement.php
Method public function cek_no_kartu($data){

```
....
377.                curl_setopt($ch, CURLOPT_POSTFIELDS, $postString);
```

**Header Injection\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11280 |
| Status | New |

Method sales_person_pilih at line 829 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/msrp.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in inquiry_ektp at line 3 of application/helpers/ektp_helper.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/msrp.php | application/helpers/ektp_helper.php |
| Line | 833 | 7 |
| Object | post | BinaryExpr |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/msrp.php
Method public function sales_person_pilih() {

```
....
833.                $term = $data['is_msrp_internal'] == '1' ? trim($this->input->post('term_internal')) : trim($this->input->post('term_eksternal'));
```

| | |
|---|---|
| File Name | application/helpers/ektp_helper.php |
| Method | function inquiry_ektp($no_ktp, $userws) { |

```
....
7.          curl_setopt($ch,CURLOPT_URL,$url.'?'.$request);
```

**Header Injection\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11281 |
| Status | New |

Method post at line 172 of system/core/Input.php receives a user input from the _POST element. This element's value then copied into the request header without being properly sanitized or validated in inquiry_ektp at line 3 of application/helpers/ektp_helper.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/helpers/ektp_helper.php |
| Line | 182 | 7 |
| Object | _POST | BinaryExpr |

Code Snippet

| | |
|---|---|
| File Name | system/core/Input.php |
| Method | function post($index = NULL, $xss_clean = FALSE) |

```
....
182.                        $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

| | |
|---|---|
| File Name | application/helpers/ektp_helper.php |
| Method | function inquiry_ektp($no_ktp, $userws) { |

```
....
7.          curl_setopt($ch,CURLOPT_URL,$url.'?'.$request);
```

**Header Injection\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11282 |
| Status | New |

Method sales_person_pilih at line 829 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/msrp.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated

in inquiry_ektp at line 3 of application/helpers/ektp_helper.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/msrp.php | application/helpers/ektp_helper.php |
| Line | 833 | 7 |
| Object | post | BinaryExpr |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/msrp.php
Method public function sales_person_pilih() {

```
....
833.              $term = $data['is_msrp_internal'] == '1' ? trim($this->input->post('term_internal')) : trim($this->input->post('term_eksternal'));
```

File Name application/helpers/ektp_helper.php
Method function inquiry_ektp($no_ktp, $userws) {

```
....
7.          curl_setopt($ch,CURLOPT_URL,$url.'?'.$request);
```

**Header Injection\Path 30:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11283
Status New

Method sales_person_pilih at line 829 of application/controllers/msrp.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in inquiry_ektp at line 3 of application/helpers/ektp_helper.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/msrp.php | application/helpers/ektp_helper.php |
| Line | 833 | 7 |
| Object | post | BinaryExpr |

Code Snippet
File Name application/controllers/msrp.php
Method public function sales_person_pilih() {

```
....
833.                $term = $data['is_msrp_internal'] == '1' ? trim($this->input->post('term_internal')) : trim($this->input->post('term_eksternal'));
```

File Name application/helpers/ektp_helper.php

Method function inquiry_ektp($no_ktp, $userws) {

```
....
7.          curl_setopt($ch,CURLOPT_URL,$url.'?'.$request);
```

**Header Injection\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11284 |
| Status | New |

Method sales_person_pilih at line 829 of application/controllers/msrp.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in inquiry_ektp at line 3 of application/helpers/ektp_helper.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/msrp.php | application/helpers/ektp_helper.php |
| Line | 833 | 7 |
| Object | post | BinaryExpr |

Code Snippet

File Name application/controllers/msrp.php

Method public function sales_person_pilih() {

```
....
833.                $term = $data['is_msrp_internal'] == '1' ? trim($this->input->post('term_internal')) : trim($this->input->post('term_eksternal'));
```

File Name application/helpers/ektp_helper.php

Method function inquiry_ektp($no_ktp, $userws) {

```
....
7.          curl_setopt($ch,CURLOPT_URL,$url.'?'.$request);
```

**Header Injection\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11285 |
| Status | New |

Method get_nama_ektp at line 325 of application/controllers/user.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in inquiry_ektp at line 3 of application/helpers/ektp_helper.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/user.php | application/helpers/ektp_helper.php |
| Line | 327 | 7 |
| Object | post | BinaryExpr |

Code Snippet

File Name application/controllers/user.php

Method public function get_nama_ektp(){

```
....
327.            $nik = $this->input->post('nik');
```

File Name application/helpers/ektp_helper.php

Method function inquiry_ektp($no_ktp, $userws) {

```
....
7.          curl_setopt($ch,CURLOPT_URL,$url.'?'.$request);
```

**Header Injection\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11286 |
| Status | New |

Method get_nama_ektp at line 325 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in inquiry_ektp at line 3 of application/helpers/ektp_helper.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php | application/helpers/ektp_helper.php |
| Line | 327 | 7 |
| Object | post | BinaryExpr |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php

| | |
|---|---|
| Method | public function get_nama_ektp(){ |

```
....
327.            $nik = $this->input->post('nik');
```

| | |
|---|---|
| File Name | application/helpers/ektp_helper.php |
| Method | function inquiry_ektp($no_ktp, $userws) { |

```
....
7.          curl_setopt($ch,CURLOPT_URL,$url.'?'.$request);
```

**Header Injection\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11287 |
| Status | New |

Method cm_penarikan_approve at line 2241 of application/controllers/maintenance_20190524.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2246 | 956 |
| Object | post | array |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/maintenance_20190524.php |
| Method | function cm_penarikan_approve() |

```
....
2246.            $tid        = $this->input->post('tid');
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Method | function delete_tid_brilink($tid) { |

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11288 |
| Status | New |

Method post at line 172 of system/core/Input.php receives a user input from the _POST element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 182 | 956 |
| Object | _POST | array |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11289 |
| Status | New |

Method cm_penarikan_approve at line 2246 of application/controllers/maintenance_20190610.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2251 | 956 |
| Object | post | array |

Code Snippet
File Name application/controllers/maintenance_20190610.php
Method function cm_penarikan_approve()

```
....
2251.             $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 37:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11290
Status New

Method cm_penarikan_approve at line 2213 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2218 | 956 |
| Object | post | array |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20180906.php
Method function cm_penarikan_approve()

```
....
2218.             $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11291 |
| Status | New |

Method cm_penarikan_approve at line 2239 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2244 | 956 |
| Object | post | array |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck20190114.php

Method function cm_penarikan_approve()

```
....
2244.             $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11292 |
| Status | New |

Method cm_penarikan_approve at line 2073 of application/controllers/maintenance_bck07112017.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck07112017.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2078 | 956 |
| Object | post | array |

Code Snippet

File Name application/controllers/maintenance_bck07112017.php

Method function cm_penarikan_approve()

```
....
2078.             $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11293 |
| Status | New |

Method cm_penarikan_approve at line 2073 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2078 | 956 |
| Object | post | array |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_bck07112017.php
Method function cm_penarikan_approve()

```
....
2078.             $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11294 |
| Status | New |

Method cm_penarikan_approve at line 2213 of application/controllers/maintenance_bck20180906.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20180906.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2218 | 956 |
| Object | post | array |

Code Snippet
File Name application/controllers/maintenance_bck20180906.php
Method function cm_penarikan_approve()

```
....
2218.             $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11295 |
| Status | New |

Method cm_penarikan_approve at line 2284 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2289 | 956 |
| Object | post | array |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance.php

Method function cm_penarikan_approve()

```
....
2289.            $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11296 |
| Status | New |

Method cm_penarikan_approve at line 2239 of application/controllers/maintenance_bck20190114.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/controllers/maintenance_bck20190114.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2244 | 956 |
| Object | post | array |

Code Snippet
File Name application/controllers/maintenance_bck20190114.php
Method function cm_penarikan_approve()

```
....
2244.            $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11297 |
| Status | New |

Method cm_penarikan_approve at line 2225 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2230 | 956 |
| Object | post | array |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20181213.php
Method function cm_penarikan_approve()

```
....
2230.            $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11298 |
| Status | New |

Method cm_penarikan_approve at line 2284 of application/controllers/maintenance.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2289 | 956 |
| Object | post | array |

Code Snippet

File Name application/controllers/maintenance.php

Method function cm_penarikan_approve()

```
....
2289.             $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11299 |
| Status | New |

Method cm_penarikan_approve at line 2241 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2246 | 956 |
| Object | post | array |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190524.php

Method function cm_penarikan_approve()

```
....
2246.             $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11300 |
| Status | New |

Method cm_penarikan_approve at line 2225 of application/controllers/maintenance_20181213.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20181213.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2230 | 956 |
| Object | post | array |

Code Snippet
File Name application/controllers/maintenance_20181213.php
Method function cm_penarikan_approve()

```
....
2230.             $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11301 |
| Status | New |

Method cm_penarikan_approve at line 2246 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in delete_tid_brilink at line 950 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 2251 | 956 |
| Object | post | array |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_20190610.php
Method function cm_penarikan_approve()

```
....
2251.             $tid        = $this->input->post('tid');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Header Injection\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11302 |
| Status | New |

Method data_upload at line 15 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php receives a user input from the post element. This element's value then copied into the request header without being properly sanitized or validated in data_upload at line 15 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php |
| Line | 30 | 129 |
| Object | post | remote_file |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php

Method public function data_upload()

```
....
30.               $jenis = $this->input->post('jenis');
....
129.                                $is_get = ftp_get($conn,
$local_file, $remote_file, FTP_BINARY);
```

**Header Injection\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11303 |
| Status | New |

Method post at line 172 of system/core/Input.php receives a user input from the _POST element. This element's value then copied into the request header without being properly sanitized or validated in data_upload at line 15 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php. If a 3rd party can influence this value it may enable an HTTP Header Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php |
| Line | 182 | 129 |

| Object | _POST | remote_file |
|---|---|---|

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php

Method public function data_upload()

```
....
129.                                $is_get = ftp_get($conn,
$local_file, $remote_file, FTP_BINARY);
```

## Stored Code Injection

Query Path:
PHP\Cx\PHP Medium Threat\Stored Code Injection Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

*Description*

**Stored Code Injection\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10467 |
| Status | New |

The application's _processTokenStack method receives and dynamically executes user-controlled code using call_user_func_array, at line 3089 of application/third_party/PHPExcel/Calculation.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using _fileHandle, at line 111 of application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php | application/third_party/PHPExcel/Calculation.php |
| Line | 126 | 3436 |

| | | |
|---|---|---|
| Object | _fileHandle | call_user_func_array |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php
Method public function getCacheData($pCoord) {

```
....
126.             $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/third_party/PHPExcel/Calculation.php

Method private function _processTokenStack($tokens, $cellID = NULL, PHPExcel_Cell $pCell = NULL) {

```
....
3436.                                           $result =
call_user_func_array(explode('::',$functionCall),$args);
```

**Stored Code Injection\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10468 |
| Status | New |

The application's _processTokenStack method receives and dynamically executes user-controlled code using call_user_func_array, at line 3089 of application/third_party/PHPExcel/Calculation.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using _fileHandle, at line 111 of application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php | application/third_party/PHPExcel/Calculation.php |
| Line | 126 | 3442 |
| Object | _fileHandle | call_user_func_array |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php
Method public function getCacheData($pCoord) {

```
....
126.             $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Calculation.php |
| Method | private function _processTokenStack($tokens, $cellID = NULL, PHPExcel_Cell $pCell = NULL) { |

```
....
3442.                                                $result =
call_user_func_array($functionCall,$args);
```

**Stored Code Injection\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10469 |
| Status | New |

The application's showHideRows method receives and dynamically executes user-controlled code using array, at line 602 of application/third_party/PHPExcel/Worksheet/AutoFilter.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using _fileHandle, at line 111 of application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php | application/third_party/PHPExcel/Worksheet/AutoFilter.php |
| Line | 126 | 803 |
| Object | _fileHandle | array |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php |
| Method | public function getCacheData($pCoord) { |

```
....
126.              $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Worksheet/AutoFilter.php |
| Method | public function showHideRows() |

```
....
803.
      array('PHPExcel_Worksheet_AutoFilter',$columnFilterTest['method'])
,
```

**Stored Code Injection\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10470 |
| Status | New |

The application's _processTokenStack method receives and dynamically executes user-controlled code using call_user_func_array, at line 3089 of application/third_party/PHPExcel/Calculation.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using ".cache", at line 139 of application/third_party/PHPExcel/CachedObjectStorage/Memcache.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php | application/third_party/PHPExcel/Calculation.php |
| Line | 147 | 3442 |
| Object | ".cache" | call_user_func_array |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/Memcache.php

Method public function getCacheData($pCoord) {

```
....
147.                    $obj = $this->_memcache->get($this-
>_cachePrefix.$pCoord.'.cache');
```

File Name application/third_party/PHPExcel/Calculation.php

Method private function _processTokenStack($tokens, $cellID = NULL, PHPExcel_Cell $pCell = NULL) {

```
....
3442.                                           $result =
call_user_func_array($functionCall,$args);
```

**Stored Code Injection\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10471 |
| Status | New |

The application's _processTokenStack method receives and dynamically executes user-controlled code using call_user_func_array, at line 3089 of application/third_party/PHPExcel/Calculation.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using ".cache", at line 139 of application/third_party/PHPExcel/CachedObjectStorage/Memcache.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php | application/third_party/PHPExcel/Calculation.php |
| Line | 147 | 3436 |
| Object | ".cache" | call_user_func_array |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/Memcache.php
Method public function getCacheData($pCoord) {

```
....
147.                    $obj = $this->_memcache->get($this->_cachePrefix.$pCoord.'.cache');
```

File Name application/third_party/PHPExcel/Calculation.php

Method private function _processTokenStack($tokens, $cellID = NULL, PHPExcel_Cell $pCell = NULL) {

```
....
3436.                                                $result = call_user_func_array(explode('::',$functionCall),$args);
```

**Stored Code Injection\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10472 |
| Status | New |

The application's showHideRows method receives and dynamically executes user-controlled code using array, at line 602 of application/third_party/PHPExcel/Worksheet/AutoFilter.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using ".cache", at line 139 of application/third_party/PHPExcel/CachedObjectStorage/Memcache.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php | application/third_party/PHPExcel/Worksheet/AutoFilter.php |
| Line | 147 | 803 |
| Object | ".cache" | array |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/Memcache.php
Method public function getCacheData($pCoord) {

```
....
147.                    $obj = $this->_memcache->get($this-
>_cachePrefix.$pCoord.'.cache');
```

File Name application/third_party/PHPExcel/Worksheet/AutoFilter.php

Method public function showHideRows()

```
....
803.
      array('PHPExcel_Worksheet_AutoFilter',$columnFilterTest['method'])
,
```

**Stored Code Injection\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10473 |
| Status | New |

The application's _processTokenStack method receives and dynamically executes user-controlled code using call_user_func_array, at line 3089 of application/third_party/PHPExcel/Calculation.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using _fileHandle, at line 103 of application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php | application/third_party/PHPExcel/Calculation.php |
| Line | 118 | 3442 |
| Object | _fileHandle | call_user_func_array |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php

Method public function getCacheData($pCoord) {

```
....
118.                $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/third_party/PHPExcel/Calculation.php

Method private function _processTokenStack($tokens, $cellID = NULL, PHPExcel_Cell $pCell = NULL) {

```
....
3442.                                                $result =
call_user_func_array($functionCall,$args);
```

**Stored Code Injection\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10474 |
| Status | New |

The application's _processTokenStack method receives and dynamically executes user-controlled code using call_user_func_array, at line 3089 of application/third_party/PHPExcel/Calculation.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using _fileHandle, at line 103 of application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php | application/third_party/PHPExcel/Calculation.php |
| Line | 118 | 3436 |
| Object | _fileHandle | call_user_func_array |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php

Method public function getCacheData($pCoord) {

```
....
118.              $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/third_party/PHPExcel/Calculation.php

Method private function _processTokenStack($tokens, $cellID = NULL, PHPExcel_Cell $pCell = NULL) {

```
....
3436.                                                $result =
call_user_func_array(explode('::',$functionCall),$args);
```

**Stored Code Injection\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10475 |
| Status | New |

The application's showHideRows method receives and dynamically executes user-controlled code using array, at line 602 of application/third_party/PHPExcel/Worksheet/AutoFilter.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using _fileHandle, at line 103 of application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php | application/third_party/PHPExcel/Worksheet/AutoFilter.php |
| Line | 118 | 803 |
| Object | _fileHandle | array |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php

Method public function getCacheData($pCoord) {

```
....
118.             $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

File Name application/third_party/PHPExcel/Worksheet/AutoFilter.php

Method public function showHideRows()

```
....
803.
      array('PHPExcel_Worksheet_AutoFilter',$columnFilterTest['method'])
,
```

**Stored Code Injection\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10476 |
| Status | New |

The application's _processTokenStack method receives and dynamically executes user-controlled code using call_user_func_array, at line 3089 of application/third_party/PHPExcel/Calculation.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using fetchSingle, at line 99 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/Calculation.php |

| | | |
|---|---|---|
| Line | 117 | 3442 |
| Object | fetchSingle | call_user_func_array |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php
Method public function getCacheData($pCoord) {

```
....
117.            $cellResult = $cellResultSet->fetchSingle();
```

File Name application/third_party/PHPExcel/Calculation.php

Method private function _processTokenStack($tokens, $cellID = NULL, PHPExcel_Cell $pCell = NULL) {

```
....
3442.                                           $result =
call_user_func_array($functionCall,$args);
```

**Stored Code Injection\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10477 |
| Status | New |

The application's _processTokenStack method receives and dynamically executes user-controlled code using call_user_func_array, at line 3089 of application/third_party/PHPExcel/Calculation.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using fetchSingle, at line 99 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/Calculation.php |
| Line | 117 | 3436 |
| Object | fetchSingle | call_user_func_array |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php
Method public function getCacheData($pCoord) {

```
....
117.            $cellResult = $cellResultSet->fetchSingle();
```

File Name application/third_party/PHPExcel/Calculation.php

| | |
|---|---|
| Method | private function _processTokenStack($tokens, $cellID = NULL, PHPExcel_Cell $pCell = NULL) { |

```
....
3436.                                                $result =
call_user_func_array(explode('::',$functionCall),$args);
```

**Stored Code Injection\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10478 |
| Status | New |

The application's showHideRows method receives and dynamically executes user-controlled code using array, at line 602 of application/third_party/PHPExcel/Worksheet/AutoFilter.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the getCacheData method, using fetchSingle, at line 99 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/Worksheet/AutoFilter.php |
| Line | 117 | 803 |
| Object | fetchSingle | array |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Method | public function getCacheData($pCoord) { |

```
....
117.              $cellResult = $cellResultSet->fetchSingle();
```

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Worksheet/AutoFilter.php |
| Method | public function showHideRows() |

```
....
803.
      array('PHPExcel_Worksheet_AutoFilter',$columnFilterTest['method'])
,
```

**Stored Code Injection\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10479 |
| Status | New |

The application's restoreSerializedObject method receives and dynamically executes user-controlled code using BinaryExpr, at line 4135 of system/helpers/dompdf/lib/class.pdf.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the insert_cached_document method, using pg_fetch_assoc, at line 96 of application/third_party/dompdf/include/page_cache.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/page_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 110 | 4137 |
| Object | pg_fetch_assoc | BinaryExpr |

Code Snippet

File Name application/third_party/dompdf/include/page_cache.cls.php

Method static function insert_cached_document(CPDF_Adapter $pdf, $id, $new_page = true) {

```
....
110.      while ($row = pg_fetch_assoc($res)) {
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function restoreSerializedObject($obj) {

```
....
4137.      eval('$this->objects[$obj_id] = ' . $obj . ';');
```

**Stored Code Injection\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10480 |
| Status | New |

The application's restoreSerializedObject method receives and dynamically executes user-controlled code using BinaryExpr, at line 4135 of system/helpers/dompdf/lib/class.pdf.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the insert_cached_document method, using pg_fetch_assoc, at line 97 of system/helpers/dompdf/include/page_cache.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/page_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 111 | 4137 |

| | | |
|---|---|---|
| Object | pg_fetch_assoc | BinaryExpr |

Code Snippet

File Name system/helpers/dompdf/include/page_cache.cls.php

Method static function insert_cached_document(CPDF_Adapter $pdf, $id, $new_page = true) {

```
....
111.      while ($row = pg_fetch_assoc($res)) {
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function restoreSerializedObject($obj) {

```
....
4137.      eval('$this->objects[$obj_id] = ' . $obj . ';');
```

**Stored Code Injection\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10481 |
| Status | New |

The application's load_html method receives and dynamically executes user-controlled code using BinaryExpr, at line 528 of application/third_party/dompdf/include/dompdf.cls.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the load_html_file method, using file, at line 467 of application/third_party/dompdf/include/dompdf.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/dompdf.cls.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 502 | 586 |
| Object | file | BinaryExpr |

Code Snippet

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html_file($file) {

```
....
502.      $contents = file_get_contents($file, null, $this->_http_context);
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function load_html($str, $encoding = null) {

```
....
586.        eval("?" . ">$str");
```

**Stored Code Injection\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10482 |
| Status | New |

The application's privAddFile method receives and dynamically executes user-controlled code using $_Function, at line 2525 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the read method, using f, at line 142 of system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 144 | 2777 |
| Object | f | $_Function |

Code Snippet

File Name system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php

Method public function read($n) {

```
....
144.      return fread($this->f, $n);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privAddFile($p_filedescr, &$p_header, &$p_options)

```
....
2777.        $v_result =
$p_options[PCLZIP_CB_POST_ADD](PCLZIP_CB_POST_ADD, $v_local_header);
```

**Stored Code Injection\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10483 |
| Status | New |

The application's privAddFile method receives and dynamically executes user-controlled code using $_Function, at line 2525 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the read method, using f, at line 142 of system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 144 | 2623 |
| Object | f | $_Function |

Code Snippet
File Name system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php
Method public function read($n) {

```
....
144.      return fread($this->f, $n);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privAddFile($p_filedescr, &$p_header, &$p_options)

```
....
2623.        $v_result =
$p_options[PCLZIP_CB_PRE_ADD](PCLZIP_CB_PRE_ADD, $v_local_header);
```

**Stored Code Injection\Path 18:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10484
Status New

The application's privExtractFile method receives and dynamically executes user-controlled code using $_Function, at line 3615 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the read method, using f, at line 142 of system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 144 | 3700 |
| Object | f | $_Function |

Code Snippet
File Name system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php
Method public function read($n) {

```
....
144.      return fread($this->f, $n);
```

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Method | function privExtractFile(&$p_entry, $p_path, $p_remove_path, $p_remove_all_path, &$p_options) |

```
....
3700.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10485 |
| Status | New |

The application's privExtractFile method receives and dynamically executes user-controlled code using $_Function, at line 3615 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the read method, using f, at line 142 of system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 144 | 3947 |
| Object | f | $_Function |

Code Snippet

| | |
|---|---|
| File Name | system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php |
| Method | public function read($n) { |

```
....
144.      return fread($this->f, $n);
```

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Method | function privExtractFile(&$p_entry, $p_path, $p_remove_path, $p_remove_all_path, &$p_options) |

```
....
3947.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10486 |
| Status | New |

The application's privExtractFileInOutput method receives and dynamically executes user-controlled code using $_Function, at line 4042 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the read method, using f, at line 142 of system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 144 | 4068 |
| Object | f | $_Function |

Code Snippet

File Name system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php

Method public function read($n) {

```
....
144.      return fread($this->f, $n);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileInOutput(&$p_entry, &$p_options)

```
....
4068.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10487 |
| Status | New |

The application's privExtractFileInOutput method receives and dynamically executes user-controlled code using $_Function, at line 4042 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the read method, using f, at line 142 of system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 144 | 4136 |
| Object | f | $_Function |

Code Snippet

File Name system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php

Method public function read($n) {

```
....
144.      return fread($this->f, $n);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileInOutput(&$p_entry, &$p_options)

```
....
4136.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10488 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the read method, using f, at line 142 of system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 144 | 4183 |

| | | |
|---|---|---|
| Object | f | $_Function |

Code Snippet
File Name system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php
Method public function read($n) {

```
....
144.      return fread($this->f, $n);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileAsString(&$p_entry, &$p_string, &$p_options)

```
....
4183.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10489 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the read method, using f, at line 142 of system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 144 | 4254 |
| Object | f | $_Function |

Code Snippet
File Name system/helpers/dompdf/lib/php-font-lib/classes/font_binary_stream.cls.php
Method public function read($n) {

```
....
144.      return fread($this->f, $n);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileAsString(&$p_entry, &$p_string, &$p_options)

```
....
4254.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10490 |
| Status | New |

The application's privAddFile method receives and dynamically executes user-controlled code using $_Function, at line 2525 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privAddFileUsingTempFile method, using v_file_compressed, at line 2798 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 2855 | 2777 |
| Object | v_file_compressed | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privAddFileUsingTempFile($p_filedescr, &$p_header, &$p_options)

```
....
2855.      $v_binary_data = @fread($v_file_compressed, 8);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privAddFile($p_filedescr, &$p_header, &$p_options)

```
....
2777.        $v_result =
$p_options[PCLZIP_CB_POST_ADD](PCLZIP_CB_POST_ADD, $v_local_header);
```

**Stored Code Injection\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10491 |
| Status | New |

The application's privExtractFile method receives and dynamically executes user-controlled code using $_Function, at line 3615 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4426 | 3700 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4426.        $p_header['extra'] = fread($this->zip_fd,
$p_header['extra_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFile(&$p_entry, $p_path, $p_remove_path, $p_remove_all_path, &$p_options)

```
....
3700.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10492 |
| Status | New |

The application's privExtractFile method receives and dynamically executes user-controlled code using $_Function, at line 3615 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |

| | | |
|---|---|---|
| Line | 4426 | 3947 |
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4426.        $p_header['extra'] = fread($this->zip_fd,
$p_header['extra_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFile(&$p_entry, $p_path, $p_remove_path, $p_remove_all_path, &$p_options)

```
....
3947.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10493 |
| Status | New |

The application's privExtractFileInOutput method receives and dynamically executes user-controlled code using $_Function, at line 4042 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4426 | 4068 |
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4426.        $p_header['extra'] = fread($this->zip_fd,
$p_header['extra_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileInOutput(&$p_entry, &$p_options)

```
....
4068.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10494 |
| Status | New |

The application's privExtractFileInOutput method receives and dynamically executes user-controlled code using $_Function, at line 4042 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4426 | 4136 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4426.        $p_header['extra'] = fread($this->zip_fd,
$p_header['extra_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileInOutput(&$p_entry, &$p_options)

```
....
4136.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10495 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4426 | 4183 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4426.        $p_header['extra'] = fread($this->zip_fd,
$p_header['extra_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileAsString(&$p_entry, &$p_string, &$p_options)

```
....
4183.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10496 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4426 | 4254 |
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4426.        $p_header['extra'] = fread($this->zip_fd,
$p_header['extra_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privExtractFileAsString(&$p_entry, &$p_string, &$p_options)

```
....
4254.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10497 |
| Status | New |

The application's privExtractFile method receives and dynamically executes user-controlled code using $_Function, at line 3615 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4420 | 3947 |
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4420.        $p_header['filename'] = fread($this->zip_fd,
$p_header['filename_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFile(&$p_entry, $p_path, $p_remove_path, $p_remove_all_path, &$p_options)

```
....
3947.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10498 |
| Status | New |

The application's privExtractFileInOutput method receives and dynamically executes user-controlled code using $_Function, at line 4042 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4420 | 4068 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4420.        $p_header['filename'] = fread($this->zip_fd,
$p_header['filename_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileInOutput(&$p_entry, &$p_options)

```
....
4068.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10499 |
| Status | New |

The application's privExtractFile method receives and dynamically executes user-controlled code using $_Function, at line 3615 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4420 | 3700 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4420.        $p_header['filename'] = fread($this->zip_fd,
$p_header['filename_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFile(&$p_entry, $p_path, $p_remove_path, $p_remove_all_path, &$p_options)

```
....
3700.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10500 |
| Status | New |

The application's privExtractFileInOutput method receives and dynamically executes user-controlled code using $_Function, at line 4042 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4420 | 4136 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4420.        $p_header['filename'] = fread($this->zip_fd,
$p_header['filename_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileInOutput(&$p_entry, &$p_options)

```
....
4136.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10501 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |

| | | |
|---|---|---|
| Line | 4420 | 4183 |
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4420.        $p_header['filename'] = fread($this->zip_fd,
$p_header['filename_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileAsString(&$p_entry, &$p_string, &$p_options)

```
....
4183.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10502 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4420 | 4254 |
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4420.        $p_header['filename'] = fread($this->zip_fd,
$p_header['filename_len']);
```

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Method | function privExtractFileAsString(&$p_entry, &$p_string, &$p_options) |

```
....
4254.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10503 |
| Status | New |

The application's privExtractFileInOutput method receives and dynamically executes user-controlled code using $_Function, at line 4042 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4432 | 4136 |
| Object | zip_fd | $_Function |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Method | function privReadCentralFileHeader(&$p_header) |

```
....
4432.        $p_header['comment'] = fread($this->zip_fd,
$p_header['comment_len']);
```

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Method | function privExtractFileInOutput(&$p_entry, &$p_options) |

```
....
4136.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=10504 |
| Status | New |

The application's privExtractFile method receives and dynamically executes user-controlled code using $_Function, at line 3615 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4432 | 3947 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4432.        $p_header['comment'] = fread($this->zip_fd,
$p_header['comment_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFile(&$p_entry, $p_path, $p_remove_path, $p_remove_all_path, &$p_options)

```
....
3947.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10505 |
| Status | New |

The application's privExtractFile method receives and dynamically executes user-controlled code using $_Function, at line 3615 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4432 | 3700 |
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4432.        $p_header['comment'] = fread($this->zip_fd,
$p_header['comment_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privExtractFile(&$p_entry, $p_path, $p_remove_path, $p_remove_all_path, &$p_options)

```
....
3700.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10506 |
| Status | New |

The application's privExtractFileInOutput method receives and dynamically executes user-controlled code using $_Function, at line 4042 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4432 | 4068 |
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4432.        $p_header['comment'] = fread($this->zip_fd,
$p_header['comment_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileInOutput(&$p_entry, &$p_options)

```
....
4068.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10507 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4432 | 4254 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4432.        $p_header['comment'] = fread($this->zip_fd,
$p_header['comment_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileAsString(&$p_entry, &$p_string, &$p_options)

```
....
4254.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10508 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4432 | 4183 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4432.        $p_header['comment'] = fread($this->zip_fd,
$p_header['comment_len']);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileAsString(&$p_entry, &$p_string, &$p_options)

```
....
4183.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10509 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4400 | 4183 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4400.      $v_binary_data = fread($this->zip_fd, 42);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileAsString(&$p_entry, &$p_string, &$p_options)

```
....
4183.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10510 |
| Status | New |

The application's privExtractFileInOutput method receives and dynamically executes user-controlled code using $_Function, at line 4042 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4400 | 4136 |

| | | |
|---|---|---|
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4400.      $v_binary_data = fread($this->zip_fd, 42);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileInOutput(&$p_entry, &$p_options)

```
....
4136.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10511 |
| Status | New |

The application's privExtractFileInOutput method receives and dynamically executes user-controlled code using $_Function, at line 4042 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4400 | 4068 |
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4400.      $v_binary_data = fread($this->zip_fd, 42);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileInOutput(&$p_entry, &$p_options)

```
....
4068.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10512 |
| Status | New |

The application's privExtractFile method receives and dynamically executes user-controlled code using $_Function, at line 3615 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4400 | 3947 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4400.      $v_binary_data = fread($this->zip_fd, 42);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFile(&$p_entry, $p_path, $p_remove_path, $p_remove_all_path, &$p_options)

```
....
3947.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10513 |
| Status | New |

The application's privExtractFile method receives and dynamically executes user-controlled code using $_Function, at line 3615 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4400 | 3700 |
| Object | zip_fd | $_Function |

Code Snippet

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privReadCentralFileHeader(&$p_header)

```
....
4400.      $v_binary_data = fread($this->zip_fd, 42);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFile(&$p_entry, $p_path, $p_remove_path, $p_remove_all_path, &$p_options)

```
....
3700.        $v_result =
$p_options[PCLZIP_CB_PRE_EXTRACT](PCLZIP_CB_PRE_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10514 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privReadCentralFileHeader method, using zip_fd, at line 4380 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4400 | 4254 |

| | | |
|---|---|---|
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privReadCentralFileHeader(&$p_header)

```
....
4400.      $v_binary_data = fread($this->zip_fd, 42);
```

File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php

Method function privExtractFileAsString(&$p_entry, &$p_string, &$p_options)

```
....
4254.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10515 |
| Status | New |

The application's privExtractFileAsString method receives and dynamically executes user-controlled code using $_Function, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the privExtractFileAsString method, using zip_fd, at line 4154 of application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php | application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php |
| Line | 4213 | 4254 |
| Object | zip_fd | $_Function |

Code Snippet
File Name application/third_party/PHPExcel/Shared/PCLZip/pclzip.lib.php
Method function privExtractFileAsString(&$p_entry, &$p_string, &$p_options)

```
....
4213.            $p_string = @fread($this->zip_fd,
$p_entry['compressed_size']);
....
4254.        $v_result =
$p_options[PCLZIP_CB_POST_EXTRACT](PCLZIP_CB_POST_EXTRACT,
$v_local_header);
```

**Stored Code Injection\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=10516 |
| Status | New |

The application's _ci_load method receives and dynamically executes user-controlled code using BinaryExpr, at line 741 of system/core/Loader.php. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the executed code by inserting the payload in standard text fields in the database or a local file. This text is retrieved by the _ci_load method, using _ci_path, at line 741 of system/core/Loader.php, and then sent to the executing method.

| | Source | Destination |
|---|---|---|
| File | system/core/Loader.php | system/core/Loader.php |
| Line | 829 | 829 |
| Object | _ci_path | BinaryExpr |

Code Snippet
File Name system/core/Loader.php
Method protected function _ci_load($_ci_data)

```
....
829.                    echo eval('?>'.preg_replace("/;*\s*\?>/", ";
?>", str_replace('<?=', '<?php echo ', file_get_contents($_ci_path))));
```

## Privacy Violation

Query Path:
PHP\Cx\PHP Medium Threat\Privacy Violation Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.8 - Improper access control
OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A1-Broken Access Control

*Description*

**Privacy Violation\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11143 |
| Status | New |

Method inisiasi_check_process at line 1061 of application/controllers/interface_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/controllers/interface_scheduler.php | application/controllers/interface_scheduler.php |
| Line | 1091 | 1441 |
| Object | checking_mid_psw | echo |

Code Snippet
File Name application/controllers/interface_scheduler.php
Method public function inisiasi_check_process()

```
....
1091.                                $result = $this->file_interface_lib->checking_mid_psw($iface_row->mid, $ymd, 'insert');
```

File Name application/controllers/interface_scheduler.php

Method private function logging($ket)

```
....
1441.             echo date("H:i:s").' '.$ket."\r\n";
```

**Privacy Violation\Path 2:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11144
Status New

Method inisiasi_check_process at line 1061 of application/controllers/interface_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/interface_scheduler.php | application/controllers/interface_scheduler.php |
| Line | 1137 | 1441 |
| Object | checking_tid_psw | echo |

Code Snippet
File Name application/controllers/interface_scheduler.php
Method public function inisiasi_check_process()

```
....
1137.                                $result = $this->file_interface_lib->checking_tid_psw($iface_row->tid, $ymd, 'insert');
```

File Name application/controllers/interface_scheduler.php

Method private function logging($ket)

```
....
1441.             echo date("H:i:s").' '.$ket."\r\n";
```

**Privacy Violation\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11145 |
| Status | New |

Method qc_interface_process at line 888 of application/controllers/quality_control.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/quality_control.php | application/controllers/quality_control.php |
| Line | 1040 | 1238 |
| Object | data_psw | psw_upd_mid |

Code Snippet

File Name application/controllers/quality_control.php

Method public function qc_interface_process()

```
....
1040.                                         $data_psw = array(
....
1238.                                 fwrite($handle, $psw_upd_mid);
```

**Privacy Violation\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11146 |
| Status | New |

Method qc_interface_process at line 888 of application/controllers/quality_control.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/quality_control.php | application/controllers/quality_control.php |
| Line | 1080 | 1251 |
| Object | data_psw | psw_upd_tid |

Code Snippet

File Name application/controllers/quality_control.php

Method public function qc_interface_process()

```
....
1080.                                        $data_psw    = array(
....
1251.                                fwrite($handle, $psw_upd_tid);
```

**Privacy Violation\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11147 |
| Status | New |

Method interface_merchant_existing at line 129 of application/controllers/script_migrasi.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/script_migrasi.php | application/controllers/script_migrasi.php |
| Line | 152 | 183 |
| Object | data_psw | string |

Code Snippet
File Name application/controllers/script_migrasi.php
Method public function interface_merchant_existing($kirim_csap = false)

```
....
152.                                 $data_psw = array(
....
183.                                       $fwrite_result =
fwrite($handle, $string);
```

**Privacy Violation\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11148 |
| Status | New |

Method interface_merchant_existing at line 129 of application/controllers/script_migrasi.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/script_migrasi.php | application/controllers/script_migrasi.php |
| Line | 152 | 214 |
| Object | data_psw | psw_upd_mid |

Code Snippet
File Name application/controllers/script_migrasi.php
Method public function interface_merchant_existing($kirim_csap = false)

```
....
152.                                $data_psw = array(
....
214.                                $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Privacy Violation\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11149 |
| Status | New |

Method inisiasi_check_process at line 1053 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_scheduler.php |
| Line | 1083 | 1433 |
| Object | checking_mid_psw | echo |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_scheduler.php

Method public function inisiasi_check_process()

```
....
1083.                               $result = $this->file_interface_lib-
>checking_mid_psw($iface_row->mid, $ymd, 'insert');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_scheduler.php

Method private function logging($ket)

```
....
1433.             echo date("H:i:s").' '.$ket."\r\n";
```

**Privacy Violation\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11150 |
| Status | New |

Method inisiasi_check_process at line 1053 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_scheduler.php |
| Line | 1129 | 1433 |
| Object | checking_tid_psw | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_scheduler.php
Method public function inisiasi_check_process()

```
....
1129.                                $result = $this->file_interface_lib->checking_tid_psw($iface_row->tid, $ymd, 'insert');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_scheduler.php
Method private function logging($ket)

```
....
1433.             echo date("H:i:s").' '.$ket."\r\n";
```

**Privacy Violation\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11151 |
| Status | New |

Method qc_interface_process at line 888 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php |
| Line | 1040 | 1238 |
| Object | data_psw | psw_upd_mid |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php
Method public function qc_interface_process()

```
....
1040.                                        $data_psw = array(
....
1238.                                fwrite($handle, $psw_upd_mid);
```

**Privacy Violation\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11152 |
| Status | New |

Method qc_interface_process at line 888 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php |
| Line | 1080 | 1251 |
| Object | data_psw | psw_upd_tid |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php
Method public function qc_interface_process()

```
....
1080.                                          $data_psw    = array(
....
1251.                                fwrite($handle, $psw_upd_tid);
```

**Privacy Violation\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11153 |
| Status | New |

Method interface_merchant_existing at line 129 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_migrasi.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_migrasi.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_migrasi.php |
| Line | 152 | 183 |
| Object | data_psw | string |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_migrasi.php
Method public function interface_merchant_existing($kirim_csap = false)

```
....
152.                                 $data_psw = array(
....
183.                                       $fwrite_result =
fwrite($handle, $string);
```

**Privacy Violation\Path 12:**

| | |
|---|---|
| Severity | Medium |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11154 |
| Status | New |

Method interface_merchant_existing at line 129 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_migrasi.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_migrasi.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_migrasi.php |
| Line | 152 | 214 |
| Object | data_psw | psw_upd_mid |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/script_migrasi.php
Method public function interface_merchant_existing($kirim_csap = false)

```
....
152.                                $data_psw = array(
....
214.                                $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Privacy Violation\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11155 |
| Status | New |

Method inisiasi_report_process at line 50 of application/controllers/interface_report.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/interface_report.php | application/controllers/interface_report.php |
| Line | 209 | 503 |
| Object | psw_tid | psw_tid |

Code Snippet
File Name application/controllers/interface_report.php
Method public function inisiasi_report_process()

```
....
209.                                                $psw_tid .=
$result['msg'];
....
503.                                fwrite($handle, $psw_tid);
```

**Privacy Violation\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11156 |
| Status | New |

Method inisiasi_patch_process at line 576 of application/controllers/interface_report.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/interface_report.php | application/controllers/interface_report.php |
| Line | 662 | 783 |
| Object | psw_tid | psw_tid |

Code Snippet
File Name application/controllers/interface_report.php
Method public function inisiasi_patch_process()

```
....
662.                                                    $psw_tid .=
$result['msg'];
....
783.                                fwrite($handle, $psw_tid);
```

**Privacy Violation\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11157 |
| Status | New |

Method interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_scheduler.php | application/controllers/maintenance_scheduler.php |
| Line | 219 | 421 |
| Object | psw_upd_mid | psw_upd_mid |

Code Snippet
File Name application/controllers/maintenance_scheduler.php
Method public function interface_ubah_data($pass = '')

```
....
219.                                        $psw_upd_mid .=
$result_psw_mid;
....
421.                            $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Privacy Violation\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11158 |
| Status | New |

Method interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_scheduler.php | application/controllers/maintenance_scheduler.php |
| Line | 246 | 458 |
| Object | psw_upd_tid | psw_upd_tid |

Code Snippet
File Name application/controllers/maintenance_scheduler.php
Method public function interface_ubah_data($pass = '')

```
....
246.                                        $psw_upd_tid      .=
$result_psw_tid;
....
458.                            $fwrite_result = fwrite($handle,
$psw_upd_tid);
```

**Privacy Violation\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11159 |
| Status | New |

Method qc_interface_send at line 705 of application/controllers/maintenance_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_scheduler.php | application/controllers/maintenance_scheduler.php |
| Line | 887 | 1057 |
| Object | psw_upd_mid | psw_upd_mid |

Code Snippet
File Name application/controllers/maintenance_scheduler.php
Method public function qc_interface_send($pass = '')

```
....
887.                                        $psw_upd_mid .=
$result_psw_mid;
....
1057.                           $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Privacy Violation\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11160 |
| Status | New |

Method qc_interface_send at line 705 of application/controllers/maintenance_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_scheduler.php | application/controllers/maintenance_scheduler.php |
| Line | 914 | 1094 |
| Object | psw_upd_tid | psw_upd_tid |

Code Snippet
File Name application/controllers/maintenance_scheduler.php
Method public function qc_interface_send($pass = '')

```
....
914.                                        $psw_upd_tid .=
$result_psw_tid;
....
1094.                           $fwrite_result = fwrite($handle,
$psw_upd_tid);
```

**Privacy Violation\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11161 |
| Status | New |

Method inisiasi_report_process at line 50 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php |
| Line | 209 | 503 |
| Object | psw_tid | psw_tid |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php
Method public function inisiasi_report_process()

```
....
209.                                                    $psw_tid .=
$result['msg'];
....
503.                                fwrite($handle, $psw_tid);
```

**Privacy Violation\Path 20:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11162
Status New

Method inisiasi_patch_process at line 576 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php |
| Line | 662 | 783 |
| Object | psw_tid | psw_tid |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php
Method public function inisiasi_patch_process()

```
....
662.                                                    $psw_tid .=
$result['msg'];
....
783.                                fwrite($handle, $psw_tid);
```

**Privacy Violation\Path 21:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11163
Status New

Method interface_ubah_data at line 16 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php |

| | | |
|---|---|---|
| Line | 219 | 421 |
| Object | psw_upd_mid | psw_upd_mid |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php
Method public function interface_ubah_data($pass = '')

```
....
219.                                        $psw_upd_mid .=
$result_psw_mid;
....
421.                            $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Privacy Violation\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11164 |
| Status | New |

Method interface_ubah_data at line 16 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php |
| Line | 246 | 458 |
| Object | psw_upd_tid | psw_upd_tid |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php
Method public function interface_ubah_data($pass = '')

```
....
246.                                        $psw_upd_tid      .=
$result_psw_tid;
....
458.                            $fwrite_result = fwrite($handle,
$psw_upd_tid);
```

**Privacy Violation\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11165 |
| Status | New |

Method qc_interface_send at line 705 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php |
| Line | 887 | 1057 |
| Object | psw_upd_mid | psw_upd_mid |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php
Method public function qc_interface_send($pass = '')

```
....
887.                                        $psw_upd_mid .=
$result_psw_mid;
....
1057.                           $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Privacy Violation\Path 24:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11166
Status New

Method qc_interface_send at line 705 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php |
| Line | 914 | 1094 |
| Object | psw_upd_tid | psw_upd_tid |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/maintenance_scheduler.php
Method public function qc_interface_send($pass = '')

```
....
914.                                        $psw_upd_tid .=
$result_psw_tid;
....
1094.                           $fwrite_result = fwrite($handle,
$psw_upd_tid);
```

**Privacy Violation\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11167 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 195 | 835 |
| Object | pass | echo |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function record_warnings($errno, $errstr, $errfile, $errline) {

```
....
835.      echo $errstr . "\n";
```

**Privacy Violation\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11168 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/functions.inc.php |
| Line | 181 | 835 |
| Object | pass | echo |

Code Snippet

File Name system/helpers/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name application/third_party/dompdf/include/functions.inc.php

Method function record_warnings($errno, $errstr, $errfile, $errline) {

```
....
835.      echo $errstr . "\n";
```

**Privacy Violation\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11169 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | system/helpers/dompdf/include/functions.inc.php |
| Line | 195 | 771 |
| Object | pass | echo |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name system/helpers/dompdf/include/functions.inc.php

Method function record_warnings($errno, $errstr, $errfile, $errline) {

```
....
771.      echo $errstr . "\n";
```

**Privacy Violation\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11170 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | system/helpers/dompdf/include/functions.inc.php |
| Line | 181 | 771 |
| Object | pass | echo |

Code Snippet
File Name system/helpers/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name system/helpers/dompdf/include/functions.inc.php
Method function record_warnings($errno, $errstr, $errfile, $errline) {

```
....
771.      echo $errstr . "\n";
```

**Privacy Violation\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11171 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/stylesheet.cls.php |
| Line | 181 | 1336 |
| Object | pass | print |

Code Snippet
File Name system/helpers/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name application/third_party/dompdf/include/stylesheet.cls.php
Method private function _parse_properties($str) {

```
....
1336.          if (DEBUGCSS) print 'novalue'.$prop.')';
```

**Privacy Violation\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11172 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/stylesheet.cls.php |
| Line | 195 | 1336 |
| Object | pass | print |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name application/third_party/dompdf/include/stylesheet.cls.php

Method private function _parse_properties($str) {

```
....
1336.          if (DEBUGCSS) print 'novalue'.$prop.')';
```

**Privacy Violation\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11173 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/stylesheet.cls.php |
| Line | 181 | 1172 |
| Object | pass | print |

Code Snippet
File Name system/helpers/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name application/third_party/dompdf/include/stylesheet.cls.php

Method protected function _image($val) {

```
....
1172.        print $this->get_protocol()."\n".$this-
>get_base_path()."\n".$path."\n";
```

**Privacy Violation\Path 32:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11174
Status New

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/stylesheet.cls.php |
| Line | 195 | 1172 |
| Object | pass | print |

Code Snippet
File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name application/third_party/dompdf/include/stylesheet.cls.php

Method protected function _image($val) {

```
....
1172.        print $this->get_protocol()."\n".$this-
>get_base_path()."\n".$path."\n";
```

**Privacy Violation\Path 33:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti

| | |
|---|---|
| | d=4881&pathid=11175 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/stylesheet.cls.php |
| Line | 195 | 1171 |
| Object | pass | print_r |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
195.            $host .= ":" . $arr["pass"];
```

File Name application/third_party/dompdf/include/stylesheet.cls.php

Method protected function _image($val) {

```
....
1171.         print_r($parsed_url);
```

**Privacy Violation\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11176 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/stylesheet.cls.php |
| Line | 181 | 1171 |
| Object | pass | print_r |

Code Snippet

File Name system/helpers/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
181.            $host .= "@" . $arr["pass"];
```

| | |
|---|---|
| File Name | application/third_party/dompdf/include/stylesheet.cls.php |
| Method | protected function _image($val) { |

```
....
1171.        print_r($parsed_url);
```

**Privacy Violation\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11177 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | system/helpers/dompdf/include/stylesheet.cls.php |
| Line | 195 | 1115 |
| Object | pass | print |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/dompdf/include/functions.inc.php |
| Method | function explode_url($url) { |

```
....
195.          $host .= ":" . $arr["pass"];
```

| | |
|---|---|
| File Name | system/helpers/dompdf/include/stylesheet.cls.php |
| Method | protected function _image($val) { |

```
....
1115.        print $this->get_protocol()."\n".$this-
>get_base_path()."\n".$path."\n";
```

**Privacy Violation\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11178 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | system/helpers/dompdf/include/stylesheet.cls.php |

| | | |
|---|---|---|
| Line | 181 | 1115 |
| Object | pass | print |

Code Snippet
File Name system/helpers/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name system/helpers/dompdf/include/stylesheet.cls.php

Method protected function _image($val) {

```
....
1115.        print $this->get_protocol()."\n".$this-
>get_base_path()."\n".$path."\n";
```

**Privacy Violation\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11179 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | system/helpers/dompdf/include/stylesheet.cls.php |
| Line | 195 | 1114 |
| Object | pass | print_r |

Code Snippet
File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name system/helpers/dompdf/include/stylesheet.cls.php

Method protected function _image($val) {

```
....
1114.        print_r($parsed_url);
```

**Privacy Violation\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11180 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | system/helpers/dompdf/include/stylesheet.cls.php |
| Line | 181 | 1114 |
| Object | pass | print_r |

Code Snippet

File Name system/helpers/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name system/helpers/dompdf/include/stylesheet.cls.php

Method protected function _image($val) {

```
....
1114.        print_r($parsed_url);
```

**Privacy Violation\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11181 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 181 | 945 |
| Object | pass | echo |

Code Snippet

File Name system/helpers/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function render() {

```
....
945.        echo $this->get_canvas()->get_cpdf()->messages;
```

**Privacy Violation\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11182 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 195 | 945 |
| Object | pass | echo |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name application/third_party/dompdf/include/dompdf.cls.php

Method function render() {

```
....
945.        echo $this->get_canvas()->get_cpdf()->messages;
```

**Privacy Violation\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11183 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/style.cls.php |
| Line | 181 | 1518 |
| Object | pass | print_r |

Code Snippet
File Name system/helpers/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name application/third_party/dompdf/include/style.cls.php
Method protected function _image($val) {

```
....
1518.        print_r($parsed_url);
```

**Privacy Violation\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11184 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/style.cls.php |
| Line | 195 | 1518 |
| Object | pass | print_r |

Code Snippet
File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name application/third_party/dompdf/include/style.cls.php
Method protected function _image($val) {

```
....
1518.        print_r($parsed_url);
```

**Privacy Violation\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11185 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/style.cls.php |
| Line | 195 | 1519 |
| Object | pass | print |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name application/third_party/dompdf/include/style.cls.php

Method protected function _image($val) {

```
....
1519.        print $this->_stylesheet->get_protocol()."\n".$this->_stylesheet->get_base_path()."\n".$path."\n";
```

**Privacy Violation\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11186 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/style.cls.php |
| Line | 181 | 1519 |
| Object | pass | print |

Code Snippet
File Name system/helpers/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name application/third_party/dompdf/include/style.cls.php

Method protected function _image($val) {

```
....
1519.        print $this->_stylesheet->get_protocol()."\n".$this-
>_stylesheet->get_base_path()."\n".$path."\n";
```

**Privacy Violation\Path 45:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11187
Status New

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/dompdf.php |
| Line | 195 | 279 |
| Object | pass | outfile |

Code Snippet
File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name application/third_party/dompdf/dompdf.php

Method <?php

```
....
279.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

**Privacy Violation\Path 46:**

Severity Medium
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11188 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | system/helpers/dompdf/include/style.cls.php |
| Line | 181 | 1393 |
| Object | pass | print_r |

Code Snippet

File Name system/helpers/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name system/helpers/dompdf/include/style.cls.php

Method protected function _image($val) {

```
....
1393.        print_r($parsed_url);
```

**Privacy Violation\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11189 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | system/helpers/dompdf/include/style.cls.php |
| Line | 195 | 1393 |
| Object | pass | print_r |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name system/helpers/dompdf/include/style.cls.php

Method protected function _image($val) {

```
....
1393.        print_r($parsed_url);
```

**Privacy Violation\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11190 |
| Status | New |

Method explode_url at line 179 of application/third_party/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | system/helpers/dompdf/include/style.cls.php |
| Line | 195 | 1394 |
| Object | pass | print |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
195.          $host .= ":" . $arr["pass"];
```

File Name system/helpers/dompdf/include/style.cls.php

Method protected function _image($val) {

```
....
1394.        print $this->_stylesheet->get_protocol()."\n".$this->_stylesheet->get_base_path()."\n".$path."\n";
```

**Privacy Violation\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11191 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/function | system/helpers/dompdf/include/style.cls. |

| | | |
|---|---|---|
| | s.inc.php | php |
| Line | 181 | 1394 |
| Object | pass | print |

Code Snippet
File Name system/helpers/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name system/helpers/dompdf/include/style.cls.php

Method protected function _image($val) {

```
....
1394.        print $this->_stylesheet->get_protocol()."\n".$this-
>_stylesheet->get_base_path()."\n".$path."\n";
```

**Privacy Violation\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11192 |
| Status | New |

Method explode_url at line 163 of system/helpers/dompdf/include/functions.inc.php sends user information outside the application. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | system/helpers/dompdf/dompdf.php |
| Line | 181 | 280 |
| Object | pass | outfile |

Code Snippet
File Name system/helpers/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
181.          $host .= "@" . $arr["pass"];
```

File Name system/helpers/dompdf/dompdf.php

Method <?php

```
....
280.    file_put_contents($outfile, $dompdf->output( array("compress" =>
0) ));
```

## Insecure Randomness

Query Path:
PHP\Cx\PHP Medium Threat\Insecure Randomness Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage
FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2021: A2-Cryptographic Failures

*Description*

**Insecure Randomness\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11095 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/www/examples.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/examples.php | system/helpers/dompdf/www/examples.php |
| Line | 84 | 84 |
| Object | rand | rand |

Code Snippet
File Name system/helpers/dompdf/www/examples.php
Method <?php

```
....
84.     $arrow = "images/arrow_0" . rand(1, 6) . ".gif";
```

**Insecure Randomness\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11096 |
| Status | New |

Method li_arrow at line 8 of system/helpers/dompdf/www/head.inc uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | system/helpers/dompdf/www/head.inc | system/helpers/dompdf/www/head.inc |
| Line | 9 | 9 |
| Object | rand | rand |

Code Snippet
File Name system/helpers/dompdf/www/head.inc
Method function li_arrow() {

```
....
9.    return '<li style="list-style-image: url(\'images/arrow_0' .
rand(1,6) . '.gif\');">';
```

**Insecure Randomness\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11097 |
| Status | New |

Method li_star at line 12 of system/helpers/dompdf/www/head.inc uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/head.inc | system/helpers/dompdf/www/head.inc |
| Line | 13 | 13 |
| Object | rand | rand |

Code Snippet
File Name system/helpers/dompdf/www/head.inc
Method function li_star() {

```
....
13.    return '<li style="list-style-image: url(\'images/star_0' .
rand(1,5) . '.gif\');">';
```

**Insecure Randomness\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11098 |
| Status | New |

Method ebor_gmail_start at line 1691 of application/controllers/scheduler.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/controllers/scheduler.php | application/controllers/scheduler.php |
| Line | 1695 | 1695 |

| | | |
|---|---|---|
| Object | rand | rand |

Code Snippet
File Name application/controllers/scheduler.php
Method function ebor_gmail_start($job_id='',$tgl_trx = '')

```
....
1695.            if($job_id == '') $job_id = rand(100,999);
```

**Insecure Randomness\Path 5:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11099
Status New

Method distribusi_stock_download at line 863 of application/controllers/stock.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/controllers/stock.php | application/controllers/stock.php |
| Line | 902 | 902 |
| Object | rand | rand |

Code Snippet
File Name application/controllers/stock.php
Method public function distribusi_stock_download()

```
....
902.            $skrg = date('mdHi').rand(0, 9);
```

**Insecure Randomness\Path 6:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11100
Status New

Method get_userws_ektp at line 13 of application/helpers/ektp_helper.php uses a weak method array_rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/helpers/ektp_helper.php | application/helpers/ektp_helper.php |
| Line | 16 | 16 |
| Object | array_rand | array_rand |

Code Snippet
File Name application/helpers/ektp_helper.php

| | |
|---|---|
| Method | function get_userws_ektp() |

```
....
16.   $key = array_rand($all_user);
```

**Insecure Randomness\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11101 |
| Status | New |

Method serialize_val at line 407 of application/libraries/nusoap/class.nusoap_base.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.nusoap_base.php | application/libraries/nusoap/class.nusoap_base.php |
| Line | 429 | 429 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/class.nusoap_base.php |
| Method | function serialize_val($val,$name=false,$type=false,$name_ns=false,$type_ns=false,$attributes=false,$use='encoded',$soapval=false) { |

```
....
429.                    $prefix = 'nu'.rand(1000,9999);
```

**Insecure Randomness\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11102 |
| Status | New |

Method serialize_val at line 407 of application/libraries/nusoap/class.nusoap_base.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.nusoap_base.php | application/libraries/nusoap/class.nusoap_base.php |
| Line | 439 | 439 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/class.nusoap_base.php |

| | |
|---|---|
| Method | function serialize_val($val,$name=false,$type=false,$name_ns=false,$type_ns=false,$attributes=false,$use='encoded',$soapval=false) { |

```
....
439.                    $type_prefix = 'ns'.rand(1000,9999);
```

**Insecure Randomness\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11103 |
| Status | New |

Method serialize_val at line 407 of application/libraries/nusoap/class.nusoap_base.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.nusoap_base.php | application/libraries/nusoap/class.nusoap_base.php |
| Line | 598 | 598 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/class.nusoap_base.php |
| Method | function serialize_val($val,$name=false,$type=false,$name_ns=false,$type_ns=false,$attributes=false,$use='encoded',$soapval=false) { |

```
....
598.                                                    $tt_prefix = 'ns'
. rand(1000, 9999);
```

**Insecure Randomness\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11104 |
| Status | New |

Method call at line 157 of application/libraries/nusoap/class.soapclient.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soapclient.php | application/libraries/nusoap/class.soapclient.php |
| Line | 198 | 198 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/class.soapclient.php |
| Method | function call($operation,$params=array(),$namespace='http://tempuri.org',$soapAction='',$headers=false,$rpcParams=null,$style='rpc',$use='encoded'){ |

```
....
198.                        $nsPrefix = 'ns' . rand(1000, 9999);
```

**Insecure Randomness\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11105 |
| Status | New |

Method call at line 157 of application/libraries/nusoap/class.soapclient.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soapclient.php | application/libraries/nusoap/class.soapclient.php |
| Line | 237 | 237 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/class.soapclient.php |
| Method | function call($operation,$params=array(),$namespace='http://tempuri.org',$soapAction='',$headers=false,$rpcParams=null,$style='rpc',$use='encoded'){ |

```
....
237.                    $nsPrefix = 'ns' . rand(1000, 9999);
```

**Insecure Randomness\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11106 |
| Status | New |

Method getProxy at line 701 of application/libraries/nusoap/class.soapclient.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soapclient.php | application/libraries/nusoap/class.soapclient.php |
| Line | 702 | 702 |
| Object | rand | rand |

Code Snippet
File Name application/libraries/nusoap/class.soapclient.php
Method function getProxy() {

```
....
702.            $r = rand();
```

**Insecure Randomness\Path 13:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11107
Status New

Method getProxyClassCode at line 808 of application/libraries/nusoap/class.soapclient.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soapclient.php | application/libraries/nusoap/class.soapclient.php |
| Line | 809 | 809 |
| Object | rand | rand |

Code Snippet
File Name application/libraries/nusoap/class.soapclient.php
Method function getProxyClassCode() {

```
....
809.            $r = rand();
```

**Insecure Randomness\Path 14:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11108
Status New

Method serializeType at line 1292 of application/libraries/nusoap/class.wsdl.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.wsdl.php | application/libraries/nusoap/class.wsdl.php |
| Line | 1398 | 1398 |
| Object | rand | rand |

Code Snippet
File Name application/libraries/nusoap/class.wsdl.php

| | |
|---|---|
| Method | function serializeType($name, $type, $value, $use='encoded', $encodingStyle=false, $unqualified=false) |

```
....
1398.                                    $tt_prefix = 'ns' . rand(1000,
9999);
```

**Insecure Randomness\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11109 |
| Status | New |

Method serialize_val at line 407 of application/libraries/nusoap/nusoap.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 429 | 429 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/nusoap.php |
| Method | function serialize_val($val,$name=false,$type=false,$name_ns=false,$type_ns=false,$attributes=false,$use='encoded',$soapval=false) { |

```
....
429.                    $prefix = 'nu'.rand(1000,9999);
```

**Insecure Randomness\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11110 |
| Status | New |

Method serialize_val at line 407 of application/libraries/nusoap/nusoap.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 439 | 439 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/nusoap.php |

| | |
|---|---|
| Method | function serialize_val($val,$name=false,$type=false,$name_ns=false,$type_ns=false,$attributes=false,$use='encoded',$soapval=false) { |

```
....
439.                    $type_prefix = 'ns'.rand(1000,9999);
```

**Insecure Randomness\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11111 |
| Status | New |

Method serialize_val at line 407 of application/libraries/nusoap/nusoap.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 598 | 598 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/nusoap.php |
| Method | function serialize_val($val,$name=false,$type=false,$name_ns=false,$type_ns=false,$attributes=false,$use='encoded',$soapval=false) { |

```
....
598.                                                    $tt_prefix = 'ns'
. rand(1000, 9999);
```

**Insecure Randomness\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11112 |
| Status | New |

Method serializeType at line 5874 of application/libraries/nusoap/nusoap.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 5980 | 5980 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/nusoap.php |

| | |
|---|---|
| Method | function serializeType($name, $type, $value, $use='encoded', $encodingStyle=false, $unqualified=false) |

```
....
5980.                                    $tt_prefix = 'ns' . rand(1000,
9999);
```

**Insecure Randomness\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11113 |
| Status | New |

Method call at line 7314 of application/libraries/nusoap/nusoap.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 7355 | 7355 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/nusoap.php |
| Method | function call($operation,$params=array(),$namespace='http://tempuri.org',$soapAction='',$headers=false,$rpcParams=null,$style='rpc',$use='encoded'){ |

```
....
7355.                          $nsPrefix = 'ns' . rand(1000, 9999);
```

**Insecure Randomness\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11114 |
| Status | New |

Method call at line 7314 of application/libraries/nusoap/nusoap.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 7394 | 7394 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/nusoap.php |

| | |
|---|---|
| Method | function call($operation,$params=array(),$namespace='http://tempuri.org',$soapAction='',$headers=false,$rpcParams=null,$style='rpc',$use='encoded'){ |

```
....
7394.                    $nsPrefix = 'ns' . rand(1000, 9999);
```

**Insecure Randomness\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11115 |
| Status | New |

Method getProxy at line 7858 of application/libraries/nusoap/nusoap.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 7859 | 7859 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/nusoap.php |
| Method | function getProxy() { |

```
....
7859.             $r = rand();
```

**Insecure Randomness\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11116 |
| Status | New |

Method getProxyClassCode at line 7965 of application/libraries/nusoap/nusoap.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 7966 | 7966 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/nusoap.php |
| Method | function getProxyClassCode() { |

```
....
7966.            $r = rand();
```

**Insecure Randomness\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11117 |
| Status | New |

Method generateRandomString at line 451 of application/libraries/util.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/util.php | application/libraries/util.php |
| Line | 456 | 456 |
| Object | rand | rand |

Code Snippet
File Name application/libraries/util.php
Method function generateRandomString($length = 10) {

```
....
456.                $randomString .= $characters[rand(0,
$charactersLength - 1)];
```

**Insecure Randomness\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11118 |
| Status | New |

Method generateRandomString at line 451 of application/libraries/util_20181213.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/libraries/util_20181213.php | application/libraries/util_20181213.php |
| Line | 456 | 456 |
| Object | rand | rand |

Code Snippet
File Name application/libraries/util_20181213.php
Method function generateRandomString($length = 10) {

```
....
456.                $randomString .= $characters[rand(0,
$charactersLength - 1)];
```

**Insecure Randomness\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11119 |
| Status | New |

Method set_batch_ebor at line 144 of application/models/scheduler_model.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/models/scheduler_model.php | application/models/scheduler_model.php |
| Line | 146 | 146 |
| Object | rand | rand |

Code Snippet
File Name application/models/scheduler_model.php
Method function set_batch_ebor($limit, $offset, $tgl_trx, $ebor_mode)

```
....
146.              $batch = rand(100000,999999);
```

**Insecure Randomness\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11120 |
| Status | New |

Method set_batch_ebor at line 143 of application/models/scheduler_model_20190610.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/models/scheduler_model_20190610.php | application/models/scheduler_model_20190610.php |
| Line | 145 | 145 |
| Object | rand | rand |

Code Snippet
File Name application/models/scheduler_model_20190610.php
Method function set_batch_ebor($limit, $offset, $tgl_trx, $ebor_mode)

```
....
145.            $batch = rand(100000,999999);
```

**Insecure Randomness\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11121 |
| Status | New |

Method set_batch_ebor at line 143 of application/models/scheduler_model_20220113.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/models/scheduler_model_20220113.php | application/models/scheduler_model_20220113.php |
| Line | 145 | 145 |
| Object | rand | rand |

Code Snippet

File Name application/models/scheduler_model_20220113.php

Method function set_batch_ebor($limit, $offset, $tgl_trx, $ebor_mode)

```
....
145.            $batch = rand(100000,999999);
```

**Insecure Randomness\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11122 |
| Status | New |

Method _getUniqueID at line 282 of application/third_party/PHPExcel/CachedObjectStorage/CacheBase.php uses a weak method mt_rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/CacheBase.php | application/third_party/PHPExcel/CachedObjectStorage/CacheBase.php |
| Line | 286 | 286 |
| Object | mt_rand | mt_rand |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/CacheBase.php

Method protected function _getUniqueID() {

```
....
286.                    $baseUnique = mt_rand();
```

**Insecure Randomness\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11123 |
| Status | New |

Method RAND at line 878 of application/third_party/PHPExcel/Calculation/MathTrig.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Calculation/MathTrig.php | application/third_party/PHPExcel/Calculation/MathTrig.php |
| Line | 883 | 883 |
| Object | rand | rand |

Code Snippet
File Name application/third_party/PHPExcel/Calculation/MathTrig.php
Method public static function RAND($min = 0, $max = 0) {

```
....
883.                    return (rand(0,10000000)) / 10000000;
```

**Insecure Randomness\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11124 |
| Status | New |

Method RAND at line 878 of application/third_party/PHPExcel/Calculation/MathTrig.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Calculation/MathTrig.php | application/third_party/PHPExcel/Calculation/MathTrig.php |
| Line | 885 | 885 |
| Object | rand | rand |

Code Snippet
File Name application/third_party/PHPExcel/Calculation/MathTrig.php
Method public static function RAND($min = 0, $max = 0) {

```
....
885.                    return rand($min, $max);
```

**Insecure Randomness\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11125 |
| Status | New |

Method __construct at line 81 of application/third_party/PHPExcel/Worksheet/MemoryDrawing.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Worksheet/MemoryDrawing.php | application/third_party/PHPExcel/Worksheet/MemoryDrawing.php |
| Line | 87 | 87 |
| Object | rand | rand |

Code Snippet
File Name application/third_party/PHPExcel/Worksheet/MemoryDrawing.php
Method public function __construct()

```
....
87.         $this->_uniqueName                  = md5(rand(0, 9999).
time() . rand(0, 9999));
```

**Insecure Randomness\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11126 |
| Status | New |

Method __construct at line 81 of application/third_party/PHPExcel/Worksheet/MemoryDrawing.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Worksheet/MemoryDrawing.php | application/third_party/PHPExcel/Worksheet/MemoryDrawing.php |
| Line | 87 | 87 |
| Object | rand | rand |

Code Snippet
File Name application/third_party/PHPExcel/Worksheet/MemoryDrawing.php
Method public function __construct()

```
....
87.         $this->_uniqueName                  = md5(rand(0, 9999).
time() . rand(0, 9999));
```

**Insecure Randomness\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11127 |
| Status | New |

Method ebor_gmail_start at line 1684 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler.php |
| Line | 1688 | 1688 |
| Object | rand | rand |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/scheduler.php

Method function ebor_gmail_start($job_id='',$tgl_trx = '')

```
....
1688.             if($job_id == '') $job_id = rand(100,999);
```

**Insecure Randomness\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11128 |
| Status | New |

Method distribusi_stock_download at line 863 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php |
| Line | 902 | 902 |
| Object | rand | rand |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php

Method public function distribusi_stock_download()

```
....
902.                $skrg = date('mdHi').rand(0, 9);
```

**Insecure Randomness\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11129 |
| Status | New |

Method set_batch_ebor at line 143 of BACKUP_DEPLOY_FMS_20210407/models/models/scheduler_model.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/models/models/scheduler_model.php | BACKUP_DEPLOY_FMS_20210407/models/models/scheduler_model.php |
| Line | 145 | 145 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/models/models/scheduler_model.php |
| Method | function set_batch_ebor($limit, $offset, $tgl_trx, $ebor_mode) |

```
....
145.                $batch = rand(100000,999999);
```

**Insecure Randomness\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11130 |
| Status | New |

Method set_batch_ebor at line 143 of BACKUP_DEPLOY_FMS_20210407/models/models/scheduler_model_20190610.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/models/models/scheduler_model_20190610.php | BACKUP_DEPLOY_FMS_20210407/models/models/scheduler_model_20190610.php |
| Line | 145 | 145 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/models/models/scheduler_model_20190610.php |

| | |
|---|---|
| Method | function set_batch_ebor($limit, $offset, $tgl_trx, $ebor_mode) |

```
....
145.                $batch = rand(100000,999999);
```

**Insecure Randomness\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11131 |
| Status | New |

Method xss_hash at line 476 of system/core/Security.php uses a weak method mt_srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/core/Security.php | system/core/Security.php |
| Line | 480 | 480 |
| Object | mt_srand | mt_srand |

| | |
|---|---|
| Code Snippet | |
| File Name | system/core/Security.php |
| Method | public function xss_hash() |

```
....
480.                    mt_srand();
```

**Insecure Randomness\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11132 |
| Status | New |

Method xss_hash at line 476 of system/core/Security.php uses a weak method mt_rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/core/Security.php | system/core/Security.php |
| Line | 481 | 481 |
| Object | mt_rand | mt_rand |

| | |
|---|---|
| Code Snippet | |
| File Name | system/core/Security.php |
| Method | public function xss_hash() |

```
....
481.                    $this->_xss_hash = md5(time() + mt_rand(0,
1999999999));
```

**Insecure Randomness\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11133 |
| Status | New |

Method _csrf_set_hash at line 853 of system/core/Security.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/core/Security.php | system/core/Security.php |
| Line | 867 | 867 |
| Object | rand | rand |

Code Snippet
File Name system/core/Security.php
Method protected function _csrf_set_hash()

```
....
867.                    return $this->_csrf_hash = md5(uniqid(rand(),
TRUE));
```

**Insecure Randomness\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11134 |
| Status | New |

Method <?php at line 1 of system/helpers/MPDF/examples/example14_page_numbers_ToC_Index_Bookmarks.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/helpers/MPDF/examples/example14_page_numbers_ToC_Index_Bookmarks.php | system/helpers/MPDF/examples/example14_page_numbers_ToC_Index_Bookmarks.php |
| Line | 179 | 179 |
| Object | rand | rand |

Code Snippet
File Name system/helpers/MPDF/examples/example14_page_numbers_ToC_Index_Bookmarks.php

| | |
|---|---|
| Method | <?php |

```
....
179.            $y =  rand(1,10);       // every tenth word
```

**Insecure Randomness\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11135 |
| Status | New |

Method print_graph at line 49 of system/helpers/MPDF/graph.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/helpers/MPDF/graph.php | system/helpers/MPDF/graph.php |
| Line | 232 | 232 |
| Object | rand | rand |

| | |
|---|---|
| Code Snippet | |
| File Name | system/helpers/MPDF/graph.php |
| Method | function print_graph($g,$pgwidth) { |

```
....
232.        $figure_file =
"graph_cache/".rand(11111,999999999)."."$img_type;
```

**Insecure Randomness\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11136 |
| Status | New |

Method _xor_encode at line 238 of system/libraries/Encrypt.php uses a weak method mt_rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/libraries/Encrypt.php | system/libraries/Encrypt.php |
| Line | 243 | 243 |
| Object | mt_rand | mt_rand |

| | |
|---|---|
| Code Snippet | |
| File Name | system/libraries/Encrypt.php |
| Method | function _xor_encode($string, $key) |

```
....
243.                    $rand .= mt_rand(0, mt_getrandmax());
```

**Insecure Randomness\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11137 |
| Status | New |

Method sess_create at line 305 of system/libraries/Session.php uses a weak method mt_rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/libraries/Session.php | system/libraries/Session.php |
| Line | 310 | 310 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name system/libraries/Session.php
Method function sess_create()

```
....
310.                    $sessid .= mt_rand(0, mt_getrandmax());
```

**Insecure Randomness\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11138 |
| Status | New |

Method sess_update at line 343 of system/libraries/Session.php uses a weak method mt_rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/libraries/Session.php | system/libraries/Session.php |
| Line | 357 | 357 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name system/libraries/Session.php
Method function sess_update()

```
....
357.                    $new_sessid .= mt_rand(0, mt_getrandmax());
```

**Insecure Randomness\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11139 |
| Status | New |

Method _sess_gc at line 753 of system/libraries/Session.php uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/libraries/Session.php | system/libraries/Session.php |
| Line | 760 | 760 |
| Object | srand | srand |

Code Snippet
File Name system/libraries/Session.php
Method function _sess_gc()

```
....
760.            srand(time());
```

**Insecure Randomness\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11140 |
| Status | New |

Method _sess_gc at line 753 of system/libraries/Session.php uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/libraries/Session.php | system/libraries/Session.php |
| Line | 761 | 761 |
| Object | rand | rand |

Code Snippet
File Name system/libraries/Session.php
Method function _sess_gc()

```
....
761.            if ((rand() % 100) < $this->gc_probability)
```

**Insecure Randomness\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11141 |

| Status | New |
|---|---|

Method set_filename at line 390 of system/libraries/Upload.php uses a weak method mt_srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/libraries/Upload.php | system/libraries/Upload.php |
| Line | 394 | 394 |
| Object | mt_srand | mt_srand |

Code Snippet
File Name system/libraries/Upload.php
Method public function set_filename($path, $filename)

```
....
394.                    mt_srand();
```

**Insecure Randomness\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11142 |
| Status | New |

Method set_filename at line 390 of system/libraries/Upload.php uses a weak method mt_rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

| | Source | Destination |
|---|---|---|
| File | system/libraries/Upload.php | system/libraries/Upload.php |
| Line | 395 | 395 |
| Object | mt_rand | mt_rand |

Code Snippet
File Name system/libraries/Upload.php
Method public function set_filename($path, $filename)

```
....
395.                    $filename = md5(uniqid(mt_rand())).$this-
>file_ext;
```

## Client Use Of JQuery Outdated Version

Query Path:
JavaScript\Cx\JavaScript Medium Threat\Client Use Of JQuery Outdated Version Version:1

### Categories

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2021: A6-Vulnerable and Outdated Components

*Description*

**Client Use Of JQuery Outdated Version\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11226 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in application/views/super_admin/explore_super_admin.php, at line 1, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/super_admin/explore_super_admin.php | application/views/super_admin/explore_super_admin.php |
| Line | 1 | 1 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet

File Name application/views/super_admin/explore_super_admin.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script>

```
....
1.  <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11227 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in application/views/super_admin/home_super_admin.php, at line 1, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/super_admin/home_super_admin.php | application/views/super_admin/home_super_admin.php |
| Line | 1 | 1 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet

File Name application/views/super_admin/home_super_admin.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script>

```
....
1.  <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11228 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/template/cetak_header.php, at line 21, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/cetak_header.php | application/views/template/cetak_header.php |
| Line | 21 | 21 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet

File Name application/views/template/cetak_header.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
21.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11229 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/template/header.php, at line 22, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/header.php | application/views/template/header.php |
| Line | 22 | 22 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet

File Name application/views/template/header.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
22.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11230 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/template/header_backup_28072020.php, at line 22, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/header_backup_28072020.php | application/views/template/header_backup_28072020.php |
| Line | 22 | 22 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet

File Name application/views/template/header_backup_28072020.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
22.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11231 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in application/views/template/header_new.php, at line 17, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/header_new.php | application/views/template/header_new.php |
| Line | 17 | 17 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet

File Name application/views/template/header_new.php

| | |
|---|---|
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> |

```
....
17.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11232 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in application/views/template/header_new_backup_28072020.php, at line 15, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/header_new_backup_28072020.php | application/views/template/header_new_backup_28072020.php |
| Line | 15 | 15 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/template/header_new_backup_28072020.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> |

```
....
15.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11233 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/template/popup_header.php, at line 16, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/popup_header.php | application/views/template/popup_header.php |
| Line | 16 | 16 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet

| | |
|---|---|
| File Name | application/views/template/popup_header.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
16.      <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11234 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/user/choose_level.php, at line 19, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/user/choose_level.php | application/views/user/choose_level.php |
| Line | 19 | 19 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/user/choose_level.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
19.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11235 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/user/login.php, at line 19, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/user/login.php | application/views/user/login.php |
| Line | 19 | 19 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/user/login.php |

| | |
|---|---|
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
19.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11236 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/explore_super_admin.php, at line 1, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/explore_super_admin.php | BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/explore_super_admin.php |
| Line | 1 | 1 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/explore_super_admin.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> |

```
....
1.  <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11237 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/home_super_admin.php, at line 1, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/home_super_admin.php | BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/home_super_admin.php |

| | | |
|---|---|---|
| Line | 1 | 1 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/home_super_admin.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script>

```
....
1.  <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 13:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11238
Status New

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/cetak_header.php, at line 21, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/cetak_header.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/cetak_header.php |
| Line | 21 | 21 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/template/cetak_header.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
21.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 14:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11239
Status New

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/header.php, at line 22, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/header.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/header.php |
| Line | 22 | 22 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/template/header.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
22.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 15:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11240
Status New

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/header_backup_28072020.php, at line 22, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_backup_28072020.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_backup_28072020.php |
| Line | 22 | 22 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/template/header_backup_28072020.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
22.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 16:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11241
Status New

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new.php, at line 17, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new.php |
| Line | 17 | 17 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script>

```
....
17.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11242 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new_backup_28072020.php, at line 15, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new_backup_28072020.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new_backup_28072020.php |
| Line | 15 | 15 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new_backup_28072020.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script>

```
....
15.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11243 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/popup_header.php, at line 16, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/popup_header.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/popup_header.php |
| Line | 16 | 16 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/template/popup_header.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
16.      <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11244 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/user/choose_level.php, at line 19, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/user/choose_level.php | BACKUP_DEPLOY_FMS_20210407/views/views/user/choose_level.php |
| Line | 19 | 19 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/user/choose_level.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
19.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11245 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/user/login.php, at line 19, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/user/login.php | BACKUP_DEPLOY_FMS_20210407/views/views/user/login.php |
| Line | 19 | 19 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/user/login.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
19.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11246 |
| Status | New |

Method in javascript/colorbox/index.html, at line 12, calls an obsolete API, jquery/1.9.0. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | javascript/colorbox/index.html | javascript/colorbox/index.html |
| Line | 12 | 12 |
| Object | jquery/1.9.0 | jquery/1.9.0 |

Code Snippet

File Name javascript/colorbox/index.html

Method <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"></script>

```
....
12.         <script
src="https://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"><
/script>
```

**Client Use Of JQuery Outdated Version\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11247 |
| Status | New |

Method in system/helpers/dompdf/www/debugger.php, at line 9, calls an obsolete API, jquery-1.4.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/debugger.php | system/helpers/dompdf/www/debugger.php |
| Line | 9 | 9 |
| Object | jquery-1.4.2 | jquery-1.4.2 |

Code Snippet
File Name system/helpers/dompdf/www/debugger.php
Method <script type="text/javascript" src="jquery-1.4.2.js"></script>

```
....
9.    <script type="text/javascript" src="jquery-1.4.2.js"></script>
```

**Client Use Of JQuery Outdated Version\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11248 |
| Status | New |

Method in system/helpers/dompdf/www/head.inc, at line 25, calls an obsolete API, jquery-1.4.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/head.inc | system/helpers/dompdf/www/head.inc |
| Line | 25 | 25 |
| Object | jquery-1.4.2 | jquery-1.4.2 |

Code Snippet
File Name system/helpers/dompdf/www/head.inc
Method <script type="text/javascript" src="jquery-1.4.2.js"></script>

```
....
25.    <script type="text/javascript" src="jquery-1.4.2.js"></script>
```

# Client Use Of JQuery Outdated Version

Query Path:
Typescript\Cx\Typescript Medium Threat\Client Use Of JQuery Outdated Version Version:1

*Description*

**Client Use Of JQuery Outdated Version\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11586 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in application/views/super_admin/explore_super_admin.php, at line 1, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/super_admin/explore_super_admin.php | application/views/super_admin/explore_super_admin.php |
| Line | 1 | 1 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet

File Name application/views/super_admin/explore_super_admin.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script>

```
....
1.  <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11587 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in application/views/super_admin/home_super_admin.php, at line 1, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/super_admin/home_super_admin.php | application/views/super_admin/home_super_admin.php |
| Line | 1 | 1 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet

File Name application/views/super_admin/home_super_admin.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script>

```
....
1.  <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11588 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/template/cetak_header.php, at line 21, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/cetak_header.php | application/views/template/cetak_header.php |
| Line | 21 | 21 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet

File Name application/views/template/cetak_header.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
21.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11589 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/template/header.php, at line 22, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/header.php | application/views/template/header.php |
| Line | 22 | 22 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet

File Name application/views/template/header.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
22.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11590 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/template/header_backup_28072020.php, at line 22, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/header_backup_28072020.php | application/views/template/header_backup_28072020.php |
| Line | 22 | 22 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet

File Name application/views/template/header_backup_28072020.php

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
22.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11591 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in application/views/template/header_new.php, at line 17, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/header_new.php | application/views/template/header_new.php |
| Line | 17 | 17 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet

File Name application/views/template/header_new.php

| | |
|---|---|
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> |

```
....
17.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11592 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in application/views/template/header_new_backup_28072020.php, at line 15, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/header_new_backup_28072020.php | application/views/template/header_new_backup_28072020.php |
| Line | 15 | 15 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/template/header_new_backup_28072020.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> |

```
....
15.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11593 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/template/popup_header.php, at line 16, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/template/popup_header.php | application/views/template/popup_header.php |
| Line | 16 | 16 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet

| | |
|---|---|
| File Name | application/views/template/popup_header.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
16.      <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11594 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/user/choose_level.php, at line 19, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/user/choose_level.php | application/views/user/choose_level.php |
| Line | 19 | 19 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/user/choose_level.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
19.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11595 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in application/views/user/login.php, at line 19, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/user/login.php | application/views/user/login.php |
| Line | 19 | 19 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/user/login.php |

| | |
|---|---|
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
19.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11596 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/explore_super_admin.php, at line 1, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/explore_super_admin.php | BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/explore_super_admin.php |
| Line | 1 | 1 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/explore_super_admin.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> |

```
....
1.  <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11597 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/home_super_admin.php, at line 1, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/home_super_admin.php | BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/home_super_admin.php |

| | | |
|---|---|---|
| Line | 1 | 1 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/super_admin/home_super_admin.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script>

```
....
1.  <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 13:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11598
Status New

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/cetak_header.php, at line 21, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/cetak_header.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/cetak_header.php |
| Line | 21 | 21 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/template/cetak_header.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
21.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 14:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11599
Status New

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/header.php, at line 22, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/header.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/header.php |
| Line | 22 | 22 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/template/header.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
22.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 15:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11600
Status New

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/header_backup_28072020.php, at line 22, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_backup_28072020.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_backup_28072020.php |
| Line | 22 | 22 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/template/header_backup_28072020.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script>

```
....
22.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 16:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11601
Status New

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new.php, at line 17, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new.php |
| Line | 17 | 17 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script>

```
....
17.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11602 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new_backup_28072020.php, at line 15, calls an obsolete API, jquery-1.10.1. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new_backup_28072020.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new_backup_28072020.php |
| Line | 15 | 15 |
| Object | jquery-1.10.1 | jquery-1.10.1 |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/template/header_new_backup_28072020.php
Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.10.1.min.js")?>"></script>

```
....
15.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.10.1.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11603 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/template/popup_header.php, at line 16, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/template/popup_header.php | BACKUP_DEPLOY_FMS_20210407/views/views/template/popup_header.php |
| Line | 16 | 16 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/template/popup_header.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
16.      <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11604 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/user/choose_level.php, at line 19, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/user/choose_level.php | BACKUP_DEPLOY_FMS_20210407/views/views/user/choose_level.php |
| Line | 19 | 19 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/user/choose_level.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
19.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11605 |
| Status | New |

Method <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> in BACKUP_DEPLOY_FMS_20210407/views/views/user/login.php, at line 19, calls an obsolete API, jquery-1.8.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/user/login.php | BACKUP_DEPLOY_FMS_20210407/views/views/user/login.php |
| Line | 19 | 19 |
| Object | jquery-1.8.2 | jquery-1.8.2 |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/user/login.php |
| Method | <script type="text/javascript" src="<?php echo base_url("javascript/jquery-1.8.2.min.js")?>"></script> |

```
....
19.   <script type="text/javascript" src="<?php echo
base_url("javascript/jquery-1.8.2.min.js")?>"></script>
```

**Client Use Of JQuery Outdated Version\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11606 |
| Status | New |

Method in javascript/colorbox/index.html, at line 12, calls an obsolete API, jquery/1.9.0. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | javascript/colorbox/index.html | javascript/colorbox/index.html |
| Line | 12 | 12 |
| Object | jquery/1.9.0 | jquery/1.9.0 |

Code Snippet

| | |
|---|---|
| File Name | javascript/colorbox/index.html |
| Method | <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"></script> |

```
....
12.         <script
src="https://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"><
/script>
```

**Client Use Of JQuery Outdated Version\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11607 |
| Status | New |

Method in system/helpers/dompdf/www/debugger.php, at line 9, calls an obsolete API, jquery-1.4.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/debugger.php | system/helpers/dompdf/www/debugger.php |
| Line | 9 | 9 |
| Object | jquery-1.4.2 | jquery-1.4.2 |

Code Snippet
File Name system/helpers/dompdf/www/debugger.php
Method <script type="text/javascript" src="jquery-1.4.2.js"></script>

```
....
9.    <script type="text/javascript" src="jquery-1.4.2.js"></script>
```

**Client Use Of JQuery Outdated Version\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11608 |
| Status | New |

Method in system/helpers/dompdf/www/head.inc, at line 25, calls an obsolete API, jquery-1.4.2. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/head.inc | system/helpers/dompdf/www/head.inc |
| Line | 25 | 25 |
| Object | jquery-1.4.2 | jquery-1.4.2 |

Code Snippet
File Name system/helpers/dompdf/www/head.inc
Method <script type="text/javascript" src="jquery-1.4.2.js"></script>

```
....
25.    <script type="text/javascript" src="jquery-1.4.2.js"></script>
```

# HTTP Response Splitting

Query Path:
PHP\Cx\PHP Medium Threat\HTTP Response Splitting Version:0

## Categories

FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

## *Description*

**HTTP Response Splitting\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11194 |
| Status | New |

Method merchant_excel_generate_old at line 1891 of application/controllers/admin_bck20190114.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in merchant_excel_generate_old at line 1891 of application/controllers/admin_bck20190114.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 1894 | 1988 |
| Object | post | header |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method public function merchant_excel_generate_old()

```
....
1894.             $tgl_awal   = $this->input->post('tgl_awal');
....
1988.             header('Content-Disposition:
attachment;filename="'.$filename.'"'); //tell browser what's the file
name
```

**HTTP Response Splitting\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11195 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from the _POST element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in merchant_excel_generate_old at line 1891 of application/controllers/admin_bck20190114.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_bck20190114.php |
| Line | 182 | 1988 |
| Object | _POST | header |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_bck20190114.php
Method public function merchant_excel_generate_old()

```
....
1988.             header('Content-Disposition: attachment;filename="'.$filename.'"'); //tell browser what's the file name
```

**HTTP Response Splitting\Path 3:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11196
Status New

Method merchant_excel_generate_old at line 1891 of application/controllers/admin_bck20190114.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in merchant_excel_generate_old at line 1891 of application/controllers/admin_bck20190114.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_bck20190114.php | application/controllers/admin_bck20190114.php |
| Line | 1895 | 1988 |
| Object | post | header |

Code Snippet
File Name application/controllers/admin_bck20190114.php
Method public function merchant_excel_generate_old()

```
....
1895.             $tgl_akhir  = $this->input->post('tgl_akhir');
....
1988.             header('Content-Disposition:
attachment;filename="'.$filename.'"'); //tell browser what's the file
name
```

**HTTP Response Splitting\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11197 |
| Status | New |

Method penerimaan_stock_download at line 1297 of application/controllers/stock.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in penerimaan_stock_download at line 1297 of application/controllers/stock.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/stock.php | application/controllers/stock.php |
| Line | 1299 | 1393 |
| Object | get | header |

Code Snippet
File Name application/controllers/stock.php
Method public function penerimaan_stock_download()

```
....
1299.             $id_dist    = $this->input->get('no_sp');
....
1393.                   header('Content-Disposition:
attachment;filename='.$filename); //tell browser what's the file name
```

**HTTP Response Splitting\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11198 |
| Status | New |

Method view_stock_clr_simcard at line 1632 of application/controllers/stock.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in generate_excel_stock at line 2143 of application/controllers/stock.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/stock.php | application/controllers/stock.php |
| Line | 1702 | 2252 |

| | | |
|---|---|---|
| Object | get | header |

Code Snippet
File Name application/controllers/stock.php
Method public function view_stock_clr_simcard()

```
....
1702.                    $wheres['jenis_barang']        = $this->input-
>get('jenis_barang');
```

File Name application/controllers/stock.php

Method public function generate_excel_stock($list, $jenis_barang)

```
....
2252.              header('Content-Disposition:
attachment;filename="'.$filename.'"'); //tell browser what's the file
name
```

**HTTP Response Splitting\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11199 |
| Status | New |

Method download_file_ at line 78 of application/controllers/super_admin.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in download_file_ at line 78 of application/controllers/super_admin.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | application/controllers/super_admin.php | application/controllers/super_admin.php |
| Line | 80 | 84 |
| Object | post | header |

Code Snippet
File Name application/controllers/super_admin.php
Method private function download_file_()

```
....
80.         $dest_file = $this->input->post('destination_file');
....
84.         header('Content-Disposition: attachment;
filename='.$filename);
```

**HTTP Response Splitting\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=11200 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from the _POST element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in download_file_ at line 78 of application/controllers/super_admin.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/super_admin.php |
| Line | 182 | 84 |
| Object | _POST | header |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/super_admin.php

Method private function download_file_()

```
....
84.         header('Content-Disposition: attachment;
filename='.$filename);
```

**HTTP Response Splitting\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11201 |
| Status | New |

Method report at line 536 of BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in generate_csv at line 647 of BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php | BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php |
| Line | 616 | 700 |
| Object | get | header |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php |
| Method | public function report() |

```
....
616.                $paramprint .= $this->input->get('init_id_cb').'_'.
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php |
| Method | public function generate_csv($list,$paramprint) |

```
....
700.                header('Content-Disposition: attachment;filename="MMS
Report Chargeback '.date('Ymd').'_'.$paramprint.'.csv');
```

**HTTP Response Splitting\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11202 |
| Status | New |

Method report at line 536 of BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in generate_csv at line 647 of BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php | BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php |
| Line | 617 | 700 |
| Object | get | header |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php |
| Method | public function report() |

```
....
617.                                $this->input->get('init_ticket_no');
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_CHARGEBACK_20210426/application/controllers/chargeback.php |
| Method | public function generate_csv($list,$paramprint) |

```
....
700.                header('Content-Disposition: attachment;filename="MMS
Report Chargeback '.date('Ymd').'_'.$paramprint.'.csv');
```

**HTTP Response Splitting\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11203 |
| Status | New |

Method merchant_excel_generate_old at line 1891 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in merchant_excel_generate_old at line 1891 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php |
| Line | 1894 | 1988 |
| Object | post | header |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php |
| Method | public function merchant_excel_generate_old() |

```
....
1894.               $tgl_awal   = $this->input->post('tgl_awal');
....
1988.               header('Content-Disposition:
attachment;filename="'.$filename.'"'); //tell browser what's the file
name
```

**HTTP Response Splitting\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11204 |
| Status | New |

Method post at line 172 of system/core/Input.php gets user input from the _POST element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in merchant_excel_generate_old at line 1891 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/contro |

| | | |
|---|---|---|
| | | llers/controllers/admin_bck20190114.php |
| Line | 182 | 1988 |
| Object | _POST | header |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php
Method public function merchant_excel_generate_old()

```
....
1988.             header('Content-Disposition: attachment;filename="'.$filename.'"'); //tell browser what's the file name
```

**HTTP Response Splitting\Path 12:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11205
Status New

Method merchant_excel_generate_old at line 1891 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in merchant_excel_generate_old at line 1891 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php |
| Line | 1895 | 1988 |
| Object | post | header |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin_bck20190114.php
Method public function merchant_excel_generate_old()

```
....
1895.             $tgl_akhir  = $this->input->post('tgl_akhir');
....
1988.             header('Content-Disposition:
attachment;filename="'.$filename.'"'); //tell browser what's the file
name
```

**HTTP Response Splitting\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11206 |
| Status | New |

Method report at line 536 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in generate_csv at line 647 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php |
| Line | 616 | 700 |
| Object | get | header |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php

Method public function report()

```
....
616.              $paramprint .= $this->input->get('init_id_cb').'_'.
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php

Method public function generate_csv($list,$paramprint)

```
....
700.              header('Content-Disposition: attachment;filename="MMS
Report Chargeback '.date('Ymd').'_'.$paramprint.'.csv');
```

**HTTP Response Splitting\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11207 |
| Status | New |

Method report at line 536 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in generate_csv at line 647 of

BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php |
| Line | 617 | 700 |
| Object | get | header |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php
Method public function report()

```
....
617.                                $this->input->get('init_ticket_no');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/chargeback.php
Method public function generate_csv($list,$paramprint)

```
....
700.                header('Content-Disposition: attachment;filename="MMS
Report Chargeback '.date('Ymd').'_'.$paramprint.'.csv');
```

**HTTP Response Splitting\Path 15:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11208
Status New

Method penerimaan_stock_download at line 1297 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in penerimaan_stock_download at line 1297 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php |
| Line | 1299 | 1393 |
| Object | get | header |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php
Method public function penerimaan_stock_download()

```
....
1299.             $id_dist    = $this->input->get('no_sp');
....
1393.                   header('Content-Disposition:
attachment;filename='.$filename); //tell browser what's the file name
```

**HTTP Response Splitting\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11209 |
| Status | New |

Method view_stock_clr_simcard at line 1632 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php gets user input from the get element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in generate_excel_stock at line 2143 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php |
| Line | 1702 | 2252 |
| Object | get | header |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php

Method public function view_stock_clr_simcard()

```
....
1702.                   $wheres['jenis_barang']       = $this->input-
>get('jenis_barang');
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/stock.php

Method public function generate_excel_stock($list, $jenis_barang)

```
....
2252.             header('Content-Disposition:
attachment;filename="'.$filename.'"'); //tell browser what's the file
name
```

**HTTP Response Splitting\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11210 |
| Status | New |

Method download_file_ at line 78 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php gets user input from the post element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in download_file_ at line 78 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 80 | 84 |
| Object | post | header |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php
Method private function download_file_()

```
....
80.         $dest_file = $this->input->post('destination_file');
....
84.         header('Content-Disposition: attachment;
filename='.$filename);
```

**HTTP Response Splitting\Path 18:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11211
Status New

Method post at line 172 of system/core/Input.php gets user input from the _POST element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in download_file_ at line 78 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Line | 182 | 84 |
| Object | _POST | header |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/super_admin.php |
| Method | private function download_file_() |

```
....
84.         header('Content-Disposition: attachment;
filename='.$filename);
```

**HTTP Response Splitting\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11212 |
| Status | New |

Method _csrf_set_hash at line 853 of system/core/Security.php gets user input from the _COOKIE element. This element's value then flows through the code without being properly sanitized or validated, and is eventually used in an HTTP response header in csrf_set_cookie at line 174 of system/core/Security.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Security.php | system/core/Security.php |
| Line | 864 | 189 |
| Object | _COOKIE | setcookie |

Code Snippet

| | |
|---|---|
| File Name | system/core/Security.php |
| Method | protected function _csrf_set_hash() |

```
....
864.                        return $this->_csrf_hash = $_COOKIE[$this-
>_csrf_cookie_name];
```

| | |
|---|---|
| File Name | system/core/Security.php |
| Method | public function csrf_set_cookie() |

```
....
189.             setcookie($this->_csrf_cookie_name, $this->_csrf_hash,
$expire, config_item('cookie_path'), config_item('cookie_domain'),
$secure_cookie);
```

**HTTP Response Splitting\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11213 |
| Status | New |

Method user_agent at line 537 of system/core/Input.php gets user input from the _SERVER element. This element's value then flows through the code without being properly sanitized or validated, and is eventually

used in an HTTP response header in _set_cookie at line 642 of system/libraries/Session.php. This may enable an HTTP Response Splitting attack, in certain older versions that do not mitigate this attack.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/libraries/Session.php |
| Line | 544 | 665 |
| Object | _SERVER | setcookie |

Code Snippet

File Name system/core/Input.php

Method function user_agent()

```
....
544.                $this->user_agent = ( !
isset($_SERVER['HTTP_USER_AGENT'])) ? FALSE :
$_SERVER['HTTP_USER_AGENT'];
```

File Name system/libraries/Session.php

Method function _set_cookie($cookie_data = NULL)

```
....
665.                setcookie(
```

## Deserialization of Untrusted Data

Query Path:

PHP\Cx\PHP Medium Threat\Deserialization of Untrusted Data Version:1

### Categories

OWASP Top 10 2021: A8-Software and Data Integrity Failures

### *Description*

**Deserialization of Untrusted Data\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11609 |
| Status | New |

The serialized object BinaryExpr processed in getNamedCharacterReferences in the file application/third_party/dompdf/lib/html5lib/Data.php at line 63 is deserialized by unserialize in the file application/third_party/dompdf/lib/html5lib/Data.php at line 63.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/lib/html5lib/Data.php | application/third_party/dompdf/lib/html5lib/Data.php |
| Line | 66 | 65 |
| Object | BinaryExpr | unserialize |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/dompdf/lib/html5lib/Data.php |
| Method | public static function getNamedCharacterReferences() { |

```
....
66.                 file_get_contents(dirname(__FILE__) . '/named-
character-references.ser'));
....
65.             self::$namedCharacterReferences = unserialize(
```

**Deserialization of Untrusted Data\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11610 |
| Status | New |

The serialized object BinaryExpr processed in getNamedCharacterReferences in the file system/helpers/dompdf/lib/html5lib/Data.php at line 63 is deserialized by unserialize in the file system/helpers/dompdf/lib/html5lib/Data.php at line 63.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/html5lib/Data.php | system/helpers/dompdf/lib/html5lib/Data.php |
| Line | 66 | 65 |
| Object | BinaryExpr | unserialize |

Code Snippet

| | |
|---|---|
| File Name | system/helpers/dompdf/lib/html5lib/Data.php |
| Method | public static function getNamedCharacterReferences() { |

```
....
66.                 file_get_contents(dirname(__FILE__) . '/named-
character-references.ser'));
....
65.             self::$namedCharacterReferences = unserialize(
```

**Deserialization of Untrusted Data\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11611 |
| Status | New |

The serialized object pFilename processed in loadIntoExisting in the file application/third_party/PHPExcel/Reader/Excel2003XML.php at line 293 is deserialized by unserialize in the file application/third_party/PHPExcel/CachedObjectStorage/APC.php at line 135.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Reader/Excel2003XML.php | application/third_party/PHPExcel/CachedObjectStorage/APC.php |
| Line | 333 | 156 |

| | | |
|---|---|---|
| Object | pFilename | unserialize |

Code Snippet
File Name application/third_party/PHPExcel/Reader/Excel2003XML.php
Method public function loadIntoExisting($pFilename, PHPExcel $objPHPExcel)

```
....
333.            $xml = simplexml_load_file($pFilename);
```

File Name application/third_party/PHPExcel/CachedObjectStorage/APC.php

Method public function getCacheData($pCoord) {

```
....
156.        $this->_currentObject = unserialize($obj);
```

**Deserialization of Untrusted Data\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11612 |
| Status | New |

The serialized object pFilename processed in loadIntoExisting in the file application/third_party/PHPExcel/Reader/Excel2003XML.php at line 293 is deserialized by unserialize in the file application/third_party/PHPExcel/CachedObjectStorage/Memcache.php at line 139.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Reader/Excel2003XML.php | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php |
| Line | 333 | 160 |
| Object | pFilename | unserialize |

Code Snippet
File Name application/third_party/PHPExcel/Reader/Excel2003XML.php
Method public function loadIntoExisting($pFilename, PHPExcel $objPHPExcel)

```
....
333.            $xml = simplexml_load_file($pFilename);
```

File Name application/third_party/PHPExcel/CachedObjectStorage/Memcache.php

Method public function getCacheData($pCoord) {

```
....
160.            $this->_currentObject = unserialize($obj);
```

**Deserialization of Untrusted Data\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11613 |
| Status | New |

The serialized object pFilename processed in loadIntoExisting in the file application/third_party/PHPExcel/Reader/Excel2003XML.php at line 293 is deserialized by unserialize in the file application/third_party/PHPExcel/CachedObjectStorage/SQLite.php at line 99.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Reader/Excel2003XML.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Line | 333 | 118 |
| Object | pFilename | unserialize |

Code Snippet

File Name application/third_party/PHPExcel/Reader/Excel2003XML.php

Method public function loadIntoExisting($pFilename, PHPExcel $objPHPExcel)

```
....
333.            $xml = simplexml_load_file($pFilename);
```

File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php

Method public function getCacheData($pCoord) {

```
....
118.            $this->_currentObject = unserialize($cellResult);
```

**Deserialization of Untrusted Data\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11614 |
| Status | New |

The serialized object pFilename processed in loadIntoExisting in the file application/third_party/PHPExcel/Reader/Excel2003XML.php at line 293 is deserialized by unserialize in the file application/third_party/PHPExcel/CachedObjectStorage/Wincache.php at line 137.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Reader/Excel2003XML.php | application/third_party/PHPExcel/CachedObjectStorage/Wincache.php |
| Line | 333 | 160 |
| Object | pFilename | unserialize |

Code Snippet

File Name application/third_party/PHPExcel/Reader/Excel2003XML.php

Method public function loadIntoExisting($pFilename, PHPExcel $objPHPExcel)

```
....
333.            $xml = simplexml_load_file($pFilename);
```

File Name application/third_party/PHPExcel/CachedObjectStorage/Wincache.php

Method public function getCacheData($pCoord) {

```
....
160.            $this->_currentObject = unserialize($obj);
```

**Deserialization of Untrusted Data\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11615 |
| Status | New |

The serialized object fileHandle processed in loadIntoExisting in the file application/third_party/PHPExcel/Reader/SYLK.php at line 221 is deserialized by unserialize in the file application/third_party/PHPExcel/CachedObjectStorage/APC.php at line 135.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Reader/SYLK.php | application/third_party/PHPExcel/CachedObjectStorage/APC.php |
| Line | 246 | 156 |
| Object | fileHandle | unserialize |

Code Snippet

File Name application/third_party/PHPExcel/Reader/SYLK.php

Method public function loadIntoExisting($pFilename, PHPExcel $objPHPExcel)

```
....
246.            while (($rowData = fgets($fileHandle)) !== FALSE) {
```

File Name application/third_party/PHPExcel/CachedObjectStorage/APC.php

Method public function getCacheData($pCoord) {

```
....
156.        $this->_currentObject = unserialize($obj);
```

**Deserialization of Untrusted Data\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11616 |
| Status | New |

The serialized object fileHandle processed in loadIntoExisting in the file application/third_party/PHPExcel/Reader/SYLK.php at line 221 is deserialized by unserialize in the file application/third_party/PHPExcel/CachedObjectStorage/Memcache.php at line 139.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Reader/SYLK.php | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php |
| Line | 246 | 160 |
| Object | fileHandle | unserialize |

Code Snippet
File Name application/third_party/PHPExcel/Reader/SYLK.php
Method public function loadIntoExisting($pFilename, PHPExcel $objPHPExcel)

```
....
246.            while (($rowData = fgets($fileHandle)) !== FALSE) {
```

File Name application/third_party/PHPExcel/CachedObjectStorage/Memcache.php
Method public function getCacheData($pCoord) {

```
....
160.            $this->_currentObject = unserialize($obj);
```

**Deserialization of Untrusted Data\Path 9:**

Severity Medium
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11617
Status New

The serialized object fileHandle processed in loadIntoExisting in the file application/third_party/PHPExcel/Reader/SYLK.php at line 221 is deserialized by unserialize in the file application/third_party/PHPExcel/CachedObjectStorage/SQLite.php at line 99.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Reader/SYLK.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Line | 246 | 118 |
| Object | fileHandle | unserialize |

Code Snippet
File Name application/third_party/PHPExcel/Reader/SYLK.php
Method public function loadIntoExisting($pFilename, PHPExcel $objPHPExcel)

```
....
246.            while (($rowData = fgets($fileHandle)) !== FALSE) {
```

File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php

Method public function getCacheData($pCoord) {

```
....
118.            $this->_currentObject = unserialize($cellResult);
```

**Deserialization of Untrusted Data\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11618 |
| Status | New |

The serialized object fileHandle processed in loadIntoExisting in the file application/third_party/PHPExcel/Reader/SYLK.php at line 221 is deserialized by unserialize in the file application/third_party/PHPExcel/CachedObjectStorage/Wincache.php at line 137.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Reader/SYLK.php | application/third_party/PHPExcel/CachedObjectStorage/Wincache.php |
| Line | 246 | 160 |
| Object | fileHandle | unserialize |

Code Snippet

File Name application/third_party/PHPExcel/Reader/SYLK.php

Method public function loadIntoExisting($pFilename, PHPExcel $objPHPExcel)

```
....
246.            while (($rowData = fgets($fileHandle)) !== FALSE) {
```

File Name application/third_party/PHPExcel/CachedObjectStorage/Wincache.php

Method public function getCacheData($pCoord) {

```
....
160.            $this->_currentObject = unserialize($obj);
```

**Deserialization of Untrusted Data\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11619 |
| Status | New |

The serialized object _fileHandle processed in getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php at line 111 is deserialized by unserialize in the file application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php at line 111.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php | application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php |
| Line | 126 | 126 |
| Object | _fileHandle | unserialize |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/DiscISAM.php
Method public function getCacheData($pCoord) {

```
....
126.             $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

**Deserialization of Untrusted Data\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11620 |
| Status | New |

The serialized object _fileHandle processed in getCacheData in the file application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php at line 103 is deserialized by unserialize in the file application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php at line 103.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php | application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php |
| Line | 118 | 118 |
| Object | _fileHandle | unserialize |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/PHPTemp.php
Method public function getCacheData($pCoord) {

```
....
118.             $this->_currentObject = unserialize(fread($this-
>_fileHandle,$this->_cellCache[$pCoord]['sz']));
```

**Deserialization of Untrusted Data\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11621 |
| Status | New |

The serialized object _COOKIE processed in cookie in the file system/core/Input.php at line 223 is deserialized by unserialize in the file system/libraries/Session.php at line 722.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/libraries/Session.php |
| Line | 225 | 724 |
| Object | _COOKIE | unserialize |

Code Snippet

File Name system/core/Input.php

Method function cookie($index = '', $xss_clean = FALSE)

```
....
225.            return $this->_fetch_from_array($_COOKIE, $index,
$xss_clean);
```

File Name system/libraries/Session.php

Method function _unserialize($data)

```
....
724.            $data = @unserialize(strip_slashes($data));
```

## Stored XPath Injection

Query Path:
PHP\Cx\PHP Medium Threat\Stored XPath Injection Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

*Description*

**Stored XPath Injection\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18419 |
| Status | New |

The application's get_cell_list method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 280 of application/third_party/dompdf/include/attribute_translator.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/third_party/dompdf/include/attribute_translator.cls.php |
| Line | 155 | 300 |
| Object | oci_fetch_assoc | query |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/third_party/dompdf/include/attribute_translator.cls.php
Method static protected function get_cell_list(DOMNode $node) {

```
....
300.      return $xpath->query($query, $node);
```

**Stored XPath Injection\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18420 |
| Status | New |

The application's _process_html method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 677 of application/third_party/dompdf/include/dompdf.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/third_party/dompdf/include/dompdf.cls.php |
| Line | 155 | 698 |
| Object | oci_fetch_assoc | query |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | application/third_party/dompdf/include/dompdf.cls.php |
| Method | protected function _process_html() { |

```
....
698.      $stylesheets = $xpath->query("//*[name() = 'link' or name() =
'style']");
```

**Stored XPath Injection\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18421 |
| Status | New |

The application's decorate_frame method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 47 of application/third_party/dompdf/include/frame_factory.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/third_party/dompdf/include/frame_factory.cls.php |
| Line | 155 | 222 |
| Object | oci_fetch_assoc | query |

| | |
|---|---|
| Code Snippet | |
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.              return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | application/third_party/dompdf/include/frame_factory.cls.php |
| Method | static function decorate_frame(Frame $frame, DOMPDF $dompdf, Frame $root = null) { |

```
....
222.            $count = $xpath->query("li", $parent_node)->length;
```

**Stored XPath Injection\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18422 |
| Status | New |

The application's fix_tables method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 133 of application/third_party/dompdf/include/frame_tree.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/third_party/dompdf/include/frame_tree.cls.php |
| Line | 155 | 138 |
| Object | oci_fetch_assoc | query |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name application/third_party/dompdf/include/frame_tree.cls.php

Method protected function fix_tables(){

```
....
138.      $captions = $xp->query("//table/caption");
```

**Stored XPath Injection\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18423 |
| Status | New |

The application's fix_tables method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 133 of application/third_party/dompdf/include/frame_tree.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/third_party/dompdf/include/frame_tree.cls.php |
| Line | 155 | 144 |
| Object | oci_fetch_assoc | query |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/third_party/dompdf/include/frame_tree.cls.php

Method protected function fix_tables(){

```
....
144.      $rows = $xp->query("//table/tr");
```

**Stored XPath Injection\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18424 |
| Status | New |

The application's apply_styles method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 795 of application/third_party/dompdf/include/stylesheet.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/third_party/dompdf/include/stylesheet.cls.php |
| Line | 155 | 820 |
| Object | oci_fetch_assoc | query |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/third_party/dompdf/include/stylesheet.cls.php

Method function apply_styles(Frame_Tree $tree) {

```
....
820.        $nodes = @$xp->query($query["query"]);
```

**Stored XPath Injection\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18425 |
| Status | New |

The application's apply_styles method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 795 of application/third_party/dompdf/include/stylesheet.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/third_party/dompdf/include/stylesheet.cls.php |
| Line | 155 | 854 |
| Object | oci_fetch_assoc | query |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/third_party/dompdf/include/stylesheet.cls.php

Method function apply_styles(Frame_Tree $tree) {

```
....
854.        $nodes = @$xp->query($query["query"]);
```

**Stored XPath Injection\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18426 |
| Status | New |

The application's get_cell_list method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 261 of system/helpers/dompdf/include/attribute_translator.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/helpers/dompdf/include/attribute_translator.cls.php |
| Line | 155 | 280 |
| Object | oci_fetch_assoc | query |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name system/helpers/dompdf/include/attribute_translator.cls.php
Method static protected function get_cell_list($node) {

```
....
280.      return $xpath->query($query, $node);
```

**Stored XPath Injection\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18427 |
| Status | New |

The application's render method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 682 of system/helpers/dompdf/include/dompdf.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/helpers/dompdf/include/dompdf.cls.php |
| Line | 155 | 762 |
| Object | oci_fetch_assoc | query |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | system/helpers/dompdf/include/dompdf.cls.php |
| Method | function render() { |

```
....
762.            $count = $xpath->query("li", $parent_node)->length;
```

**Stored XPath Injection\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18428 |
| Status | New |

The application's fix_tables method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 125 of system/helpers/dompdf/include/frame_tree.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/helpers/dompdf/include/frame_tree.cls.php |
| Line | 155 | 130 |
| Object | oci_fetch_assoc | query |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.             return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | system/helpers/dompdf/include/frame_tree.cls.php |
| Method | protected function fix_tables(){ |

```
....
130.      $captions = $xp->query("//table/caption");
```

**Stored XPath Injection\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18429 |
| Status | New |

The application's fix_tables method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 125 of system/helpers/dompdf/include/frame_tree.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/helpers/dompdf/include/frame_tree.cls.php |
| Line | 155 | 136 |
| Object | oci_fetch_assoc | query |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name system/helpers/dompdf/include/frame_tree.cls.php

Method protected function fix_tables(){

```
....
136.      $rows = $xp->query("//table/tr");
```

**Stored XPath Injection\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18430 |
| Status | New |

The application's apply_styles method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 751 of system/helpers/dompdf/include/stylesheet.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/helpers/dompdf/include/stylesheet.cls.php |
| Line | 155 | 775 |
| Object | oci_fetch_assoc | query |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name system/helpers/dompdf/include/stylesheet.cls.php

Method function apply_styles(Frame_Tree $tree) {

```
....
775.        $nodes = @$xp->query($query["query"]);
```

**Stored XPath Injection\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18431 |
| Status | New |

The application's apply_styles method constructs an XPath query, for navigating an XML document. The XPath query is created with query, at line 751 of system/helpers/dompdf/include/stylesheet.cls.php, using an untrusted string embedded in the expression.

This may enable an attacker to modify the XPath expression, leading to an XPath Injection attack.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/helpers/dompdf/include/stylesheet.cls.php |
| Line | 155 | 810 |
| Object | oci_fetch_assoc | query |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name system/helpers/dompdf/include/stylesheet.cls.php

Method function apply_styles(Frame_Tree $tree) {

```
....
810.        $nodes = @$xp->query($query["query"]);
```

# Inappropriate Encoding for Output Context

Query Path:
PHP\Cx\PHP Medium Threat\Inappropriate Encoding for Output Context Version:1

## Categories

OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 2021: A4-Insecure Design

## *Description*

**Inappropriate Encoding for Output Context\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11218 |
| Status | New |

The application uses htmlspecialchars function, at line 1 of javascript/ckeditor/samples/old/assets/posteddata.php, to encode user input which was received earlier. However, encoding function is faulty and does not encode all input properly. The application then sends the partially encoded input, to the response web page that is output back to the client. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/samples/old/assets/posteddata.php | javascript/ckeditor/samples/old/assets/posteddata.php |
| Line | 36 | 42 |
| Object | htmlspecialchars | echo |

Code Snippet
File Name javascript/ckeditor/samples/old/assets/posteddata.php
Method <!DOCTYPE html>

```
....
36.                 $value = htmlspecialchars(
stripslashes((string)$value) );
....
42.                 <td><pre class="samples"><?php echo $value;
?></pre></td>
```

**Inappropriate Encoding for Output Context\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11219 |
| Status | New |

The application uses htmlspecialchars function, at line 1 of javascript/ckeditor/samples/old/assets/posteddata.php, to encode user input which was received earlier. However, encoding function is faulty and does not encode all input properly. The application then sends the partially encoded input, to the response web page that is output back to the client. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/samples/old/assets/p | javascript/ckeditor/samples/old/assets/p |

| | | |
|---|---|---|
| | osteddata.php | osteddata.php |
| Line | 38 | 42 |
| Object | htmlspecialchars | echo |

Code Snippet
File Name javascript/ckeditor/samples/old/assets/posteddata.php
Method <!DOCTYPE html>

```
....
38.                 $value = htmlspecialchars( (string)$value );
....
42.                 <td><pre class="samples"><?php echo $value;
?></pre></td>
```

**Inappropriate Encoding for Output Context\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11220 |
| Status | New |

The application uses htmlspecialchars function, at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, to encode user input which was received earlier. However, encoding function is faulty and does not encode all input properly. The application then sends the partially encoded input, to the response web page that is output back to the client. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 927 | 928 |
| Object | htmlspecialchars | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
927.  $url = htmlspecialchars($_SERVER['HTTP_REFERER']);
928.        echo "<a href='$url' class='button' id='back'>Kembali</a>";
```

**Inappropriate Encoding for Output Context\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11221 |
| Status | New |

The application uses htmlspecialchars function, at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, to encode user input which was received earlier. However, encoding function is faulty and does not encode all input properly. The application then

sends the partially encoded input, to the response web page that is output back to the client. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 1726 | 1727 |
| Object | htmlspecialchars | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
1726.                    $url = htmlspecialchars($http_referer);
1727.                    echo "<a href='$url' id='back'><button
class='button'><< Kembali</button></a>  ";
```

**Inappropriate Encoding for Output Context\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11222 |
| Status | New |

The application uses htmlspecialchars function, at line 1 of application/views/pameran/detail_merchant_view.php, to encode user input which was received earlier. However, encoding function is faulty and does not encode all input properly. The application then sends the partially encoded input, to the response web page that is output back to the client. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | application/views/pameran/detail_merchant_view.php | application/views/pameran/detail_merchant_view.php |
| Line | 611 | 612 |
| Object | htmlspecialchars | echo |

Code Snippet
File Name application/views/pameran/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
611.          $url = htmlspecialchars($_SERVER['HTTP_REFERER']);
612.          echo "<a href='$url' class='button'
id='back'>Kembali</a>";
```

**Inappropriate Encoding for Output Context\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11223 |

| | |
|---|---|
| Status | New |

The application uses htmlspecialchars function, at line 1 of BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_daftar/detail_merchant_view.php, to encode user input which was received earlier. However, encoding function is faulty and does not encode all input properly. The application then sends the partially encoded input, to the response web page that is output back to the client. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_daftar/detail_merchant_view.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 927 | 928 |
| Object | htmlspecialchars | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_daftar/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
927.  $url = htmlspecialchars($_SERVER['HTTP_REFERER']);
928.        echo "<a href='$url' class='button' id='back'>Kembali</a>";
```

**Inappropriate Encoding for Output Context\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11224 |
| Status | New |

The application uses htmlspecialchars function, at line 1 of BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_daftar/detail_merchant_view_new.php, to encode user input which was received earlier. However, encoding function is faulty and does not encode all input properly. The application then sends the partially encoded input, to the response web page that is output back to the client. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_daftar/detail_merchant_view_new.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 1656 | 1657 |
| Object | htmlspecialchars | echo |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
1656.                    $url = htmlspecialchars($http_referer);
1657.                    echo "<a href='$url' id='back'><button
class='button'><< Kembali</button></a>  ";
```

**Inappropriate Encoding for Output Context\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11225 |
| Status | New |

The application uses htmlspecialchars function, at line 1 of BACKUP_DEPLOY_FMS_20210407/views/views/pameran/detail_merchant_view.php, to encode user input which was received earlier. However, encoding function is faulty and does not encode all input properly. The application then sends the partially encoded input, to the response web page that is output back to the client. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/pameran/detail_merchant_view.php | BACKUP_DEPLOY_FMS_20210407/views/views/pameran/detail_merchant_view.php |
| Line | 611 | 612 |
| Object | htmlspecialchars | echo |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/pameran/detail_merchant_view.php

Method <?php $m = $merchant->row();?>

```
....
611.          $url = htmlspecialchars($_SERVER['HTTP_REFERER']);
612.          echo "<a href='$url' class='button'
id='back'>Kembali</a>";
```

## Reflected File Download

Query Path:

PHP\Cx\PHP Medium Threat\Reflected File Download Version:1

### Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A1-Broken Access Control

*Description*

**Reflected File Download\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11577 |
| Status | New |

An explicit filename is not defined for the Content-Disposition header in line 172 at file system/core/Input.php. Filename attribute is required in order to prevent the browser from assuming the resource is an executable and download a possibly malicious file.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/patching.php |
| Line | 182 | 956 |
| Object | _POST | curl_setopt |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/patching.php
Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Reflected File Download\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11578 |
| Status | New |

An explicit filename is not defined for the Content-Disposition header in line 172 at file system/core/Input.php. Filename attribute is required in order to prevent the browser from assuming the resource is an executable and download a possibly malicious file.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php |
| Line | 182 | 956 |
| Object | _POST | curl_setopt |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/patching.php

Method function delete_tid_brilink($tid) {

```
....
956.          curl_setopt($curl, CURLOPT_POSTFIELDS,
array('request'=>json_encode($curl_post_data)));
```

**Reflected File Download\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11579 |
| Status | New |

An explicit filename is not defined for the Content-Disposition header in line 172 at file system/core/Input.php. Filename attribute is required in order to prevent the browser from assuming the resource is an executable and download a possibly malicious file.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/libraries/Zip.php |
| Line | 182 | 249 |
| Object | _POST | file_get_contents |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                          $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name system/libraries/Zip.php

Method function read_file($path, $preserve_filepath = FALSE)

```
....
249.              if (FALSE !== ($data = file_get_contents($path)))
```

**Reflected File Download\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11580 |
| Status | New |

An explicit filename is not defined for the Content-Disposition header in line 172 at file system/core/Input.php. Filename attribute is required in order to prevent the browser from assuming the resource is an executable and download a possibly malicious file.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_api.php |
| Line | 182 | 81 |
| Object | _POST | curl_setopt |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_api.php
Method function app_integration_add($del = 0)

```
....
81.                     curl_setopt($curl, CURLOPT_POSTFIELDS,
json_encode($data));
```

**Reflected File Download\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11581 |
| Status | New |

An explicit filename is not defined for the Content-Disposition header in line 172 at file system/core/Input.php. Filename attribute is required in order to prevent the browser from assuming the resource is an executable and download a possibly malicious file.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/helpers/ektp_helper.php |
| Line | 182 | 7 |
| Object | _POST | curl_setopt |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/helpers/ektp_helper.php
Method function inquiry_ektp($no_ktp, $userws) {

```
....
7.          curl_setopt($ch,CURLOPT_URL,$url.'?'.$request);
```

**Reflected File Download\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11582 |
| Status | New |

An explicit filename is not defined for the Content-Disposition header in line 172 at file system/core/Input.php. Filename attribute is required in order to prevent the browser from assuming the resource is an executable and download a possibly malicious file.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 182 | 1598 |
| Object | _POST | curl_setopt |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php

Method public function getnik(){

```
....
1598.                   curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($data));
```

**Reflected File Download\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11583 |
| Status | New |

An explicit filename is not defined for the Content-Disposition header in line 172 at file system/core/Input.php. Filename attribute is required in order to prevent the browser from assuming the resource is an executable and download a possibly malicious file.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/qris.php |

| | | |
|---|---|---|
| Line | 182 | 310 |
| Object | _POST | curl_setopt |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/qris.php
Method public function getnik(){

```
....
310.                    curl_setopt($ch, CURLOPT_POSTFIELDS,
json_encode($data));
```

## HttpOnlyCookies

Query Path:
PHP\Cx\PHP Medium Threat\HttpOnlyCookies Version:1

### Categories

OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
OWASP Top 10 2021: A5-Security Misconfiguration

*Description*
**HttpOnlyCookies\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11214 |
| Status | New |

The web application's set_cookie method creates a cookie setcookie, at line 246 of system/core/Input.php, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/core/Input.php |
| Line | 286 | 286 |
| Object | setcookie | setcookie |

Code Snippet
File Name system/core/Input.php
Method function set_cookie($name = '', $value = '', $expire = '', $domain = '', $path = '/', $prefix = '', $secure = FALSE)

```
....
286.                setcookie($prefix.$name, $value, $expire, $path,
$domain, $secure);
```

**HttpOnlyCookies\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11215 |
| Status | New |

The web application's csrf_set_cookie method creates a cookie setcookie, at line 174 of system/core/Security.php, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | system/core/Security.php | system/core/Security.php |
| Line | 189 | 189 |
| Object | setcookie | setcookie |

Code Snippet

File Name system/core/Security.php

Method public function csrf_set_cookie()

```
....
189.                setcookie($this->_csrf_cookie_name, $this->_csrf_hash,
$expire, config_item('cookie_path'), config_item('cookie_domain'),
$secure_cookie);
```

**HttpOnlyCookies\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11216 |
| Status | New |

The web application's sess_destroy method creates a cookie setcookie, at line 399 of system/libraries/Session.php, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | system/libraries/Session.php | system/libraries/Session.php |
| Line | 409 | 409 |
| Object | setcookie | setcookie |

Code Snippet

| | |
|---|---|
| File Name | system/libraries/Session.php |
| Method | function sess_destroy() |

```
....
409.                setcookie(
```

**HttpOnlyCookies\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11217 |
| Status | New |

The web application's _set_cookie method creates a cookie setcookie, at line 642 of system/libraries/Session.php, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | system/libraries/Session.php | system/libraries/Session.php |
| Line | 665 | 665 |
| Object | setcookie | setcookie |

| | |
|---|---|
| Code Snippet | |
| File Name | system/libraries/Session.php |
| Method | function _set_cookie($cookie_data = NULL) |

```
....
665.                setcookie(
```

## Client Potential XSS

Query Path:
JavaScript\Cx\JavaScript Medium Threat\Client Potential XSS Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: Access Control
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
OWASP Top 10 2021: A3-Injection

*Description*

**Client Potential XSS\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11249 |
| Status | New |

Method addEvent at line 3024 of javascript/highcharts/modules/canvas-tools.src.js gets user input for the text element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method addEvent at line 3024 of javascript/highcharts/modules/canvas-tools.src.js. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | javascript/highcharts/modules/canvas-tools.src.js | javascript/highcharts/modules/canvas-tools.src.js |
| Line | 3031 | 3031 |
| Object | text | innerHTML |

Code Snippet
File Name javascript/highcharts/modules/canvas-tools.src.js
Method addEvent(chart, 'tooltipRefresh', function (args) {

```
....
3031.                        tooltipDiv.innerHTML = args.text;
```

**Client Potential XSS\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11250 |
| Status | New |

Method f at line 1845 of javascript/highcharts/modules/canvas-tools.js gets user input for the text element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method f at line 1845 of javascript/highcharts/modules/canvas-tools.js. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | javascript/highcharts/modules/canvas-tools.js | javascript/highcharts/modules/canvas-tools.js |
| Line | 1850 | 1850 |
| Object | text | innerHTML |

Code Snippet
File Name javascript/highcharts/modules/canvas-tools.js
Method f(a, "tooltipRefresh", function(d) {

```
....
1850.                  h.innerHTML = d.text;
```

**Client Potential XSS\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11251 |
| Status | New |

Method Qd at line 476 of javascript/ckeditor/samples/toolbarconfigurator/lib/codemirror/codemirror.js gets user input for the text element. This element's value then flows through the code without being properly sanitized or validated and is eventually displayed to the user in method t at line 3320 of javascript/ckeditor/samples/toolbarconfigurator/lib/codemirror/codemirror.js. This may enable a Cross-Site-Scripting attack.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/samples/toolbarconfigurator/lib/codemirror/codemirror.js | javascript/ckeditor/samples/toolbarconfigurator/lib/codemirror/codemirror.js |
| Line | 483 | 3325 |
| Object | text | appendChild |

Code Snippet

File Name javascript/ckeditor/samples/toolbarconfigurator/lib/codemirror/codemirror.js

Method function Qd(a, b, c, d) {

```
....
483.                f.insertBefore(g, b.text);
```

File Name javascript/ckeditor/samples/toolbarconfigurator/lib/codemirror/codemirror.js

Method function t(a, b, c, d) {

```
....
3325.           else if (b) for (c = 0; c < b.length; ++c)
a.appendChild(b[c]);
```

## Cross Site History Manipulation

Query Path:

PHP\Cx\PHP Medium Threat\Cross Site History Manipulation Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.8 - Improper access control
OWASP Top 10 2013: A8-Cross-Site Request Forgery (CSRF)

### *Description*

**Cross Site History Manipulation\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | Not Exploitable |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7383 |
| Status | New |

Method service at line 236 of application/libraries/nusoap/class.soap_server.php may leak server-side conditional values, enabling user tracking from another website. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soap_server.php | application/libraries/nusoap/class.soap_server.php |
| Line | 269 | 269 |
| Object | if | if |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/class.soap_server.php |
| Method | function service($data){ |

```
....
269.                if (strpos($this->externalWSDLURL, "http://") !==
false) { // assume URL
```

**Cross Site History Manipulation\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=7384 |
| Status | New |

Method service at line 3694 of application/libraries/nusoap/nusoap.php may leak server-side conditional values, enabling user tracking from another website. This may constitute a Privacy Violation.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 3727 | 3727 |
| Object | if | if |

| | |
|---|---|
| Code Snippet | |
| File Name | application/libraries/nusoap/nusoap.php |
| Method | function service($data){ |

```
....
3727.                if (strpos($this->externalWSDLURL, "http://") !==
false) { // assume URL
```

## Client Reflected File Download

Query Path:
JavaScript\Cx\JavaScript Medium Threat\Client Reflected File Download Version:1

### Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A1-Broken Access Control

*Description*

**Client Reflected File Download\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11584 |
| Status | New |

An explicit filename is not defined for the Content-Disposition header in line 282 at file javascript/highcharts/modules/data.src.js.

Filename attribute is required in order to prevent the browser from assuming the resource is an executable and download a possibly malicious file.

| | Source | Destination |
|---|---|---|
| File | javascript/highcharts/modules/data.src.js | javascript/highcharts/modules/data.src.js |
| Line | 286 | 282 |
| Object | ""/public/values?alt=json-in-script&callback=?"" | ajax |

Code Snippet
File Name javascript/highcharts/modules/data.src.js
Method jQuery.ajax({

```
....
286.                                    '/public/values?alt=json-in-
script&callback=?',
```

File Name javascript/highcharts/modules/data.src.js
Method parseGoogleSpreadsheet: function () {

```
....
282.                            jQuery.ajax({
```

**Client Reflected File Download\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11585 |
| Status | New |

An explicit filename is not defined for the Content-Disposition header in line 117 at file javascript/highcharts/modules/data.js.
Filename attribute is required in order to prevent the browser from assuming the resource is an executable and download a possibly malicious file.

| | Source | Destination |
|---|---|---|
| File | javascript/highcharts/modules/data.js | javascript/highcharts/modules/data.js |
| Line | 119 | 117 |
| Object | ""/public/values?alt=json-in-script&callback=?"" | ajax |

Code Snippet
File Name javascript/highcharts/modules/data.js
Method e && jQuery.ajax({

```
....
119.                    url:
"https://spreadsheets.google.com/feeds/cells/" + e + "/" +
(a.googleSpreadsheetWorksheet || "od6") + "/public/values?alt=json-in-
script&callback=?",
```

| | |
|---|---|
| File Name | javascript/highcharts/modules/data.js |
| Method | parseGoogleSpreadsheet: function() { |

```
....
117.                e && jQuery.ajax({
```

## Client Potential Code Injection

Query Path:
JavaScript\Cx\JavaScript Medium Threat\Client Potential Code Injection Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: Configuration Management
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

*Description*

**Client Potential Code Injection\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11252 |
| Status | New |

The application's addEvent method receives and dynamically executes user-controlled code using eval, at line 441 of javascript/ajaxupload_3_5.js. This could enable an attacker to inject and run arbitrary code.

The attacker can inject the malicious payload into the victim's browser, via external input nodeValue. This is read by the browser in the addEvent method, at line 441 of javascript/ajaxupload_3_5.js. The browser then executes this code itself.

| | Source | Destination |
|---|---|---|
| File | javascript/ajaxupload_3_5.js | javascript/ajaxupload_3_5.js |
| Line | 492 | 495 |
| Object | nodeValue | eval |

Code Snippet

| | |
|---|---|
| File Name | javascript/ajaxupload_3_5.js |
| Method | addEvent(iframe, 'load', function(e){ |

```
....
492.                                                    response =
doc.body.firstChild.firstChild.nodeValue;
....
495.                                                    response =
window["eval"]("(" + response + ")");
```

## Object Injection

Query Path:
PHP\Cx\PHP Medium Threat\Object Injection Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A8-Software and Data Integrity Failures

*Description*

**Object Injection\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=11253 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/libraries/Session.php |
| Line | 225 | 724 |
| Object | _COOKIE | unserialize |

Code Snippet

File Name system/core/Input.php
Method function cookie($index = '', $xss_clean = FALSE)

```
....
225.                return $this->_fetch_from_array($_COOKIE, $index,
$xss_clean);
```

File Name system/libraries/Session.php
Method function _unserialize($data)

```
....
724.                $data = @unserialize(strip_slashes($data));
```

## Possible Flow Control

Query Path:
PHP\Cx\Php Low Visibility\Possible Flow Control Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.8 - Improper access control

*Description*

**Possible Flow Control\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18432 |
| Status | New |

Possible flow control was found in line 1 in file system/helpers/dompdf/www/controller.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/controller.php | system/helpers/dompdf/www/controller.php |
| Line | 5 | 10 |
| Object | _GET | cmd |

Code Snippet
File Name system/helpers/dompdf/www/controller.php
Method <?php

```
....
5.  $cmd = isset($_GET["cmd"]) ? $_GET["cmd"] : null;
....
10.  switch ($cmd) {
```

**Possible Flow Control\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18433 |
| Status | New |

Possible flow control was found in line 1 in file system/helpers/dompdf/www/controller.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/controller.php | system/helpers/dompdf/www/controller.php |
| Line | 22 | 26 |
| Object | _FILES | error |

Code Snippet
File Name system/helpers/dompdf/www/controller.php
Method <?php

```
....
22.      $data = $_FILES["file"];
....
26.          switch($error) {
```

**Possible Flow Control\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18434 |
| Status | New |

Possible flow control was found in line 330 in file application/controllers/dashboard.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/dashboard.php | application/controllers/dashboard.php |
| Line | 333 | 335 |
| Object | get | param_jenis |

Code Snippet
File Name application/controllers/dashboard.php
Method function autocomplete_param_input()

```
....
333.              $param_jenis = trim($this->input->get('param_jenis'));
....
335.              switch ($param_jenis) {
```

**Possible Flow Control\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18435 |
| Status | New |

Possible flow control was found in line 328 in file application/controllers/dashboard_20190610.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/dashboard_20190610.php | application/controllers/dashboard_20190610.php |
| Line | 331 | 333 |
| Object | get | param_jenis |

Code Snippet
File Name application/controllers/dashboard_20190610.php
Method function autocomplete_param_input()

```
....
331.            $param_jenis = trim($this->input->get('param_jenis'));
....
333.            switch ($param_jenis) {
```

**Possible Flow Control\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18436 |
| Status | New |

Possible flow control was found in line 682 in file application/controllers/ebor.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/ebor.php | application/controllers/ebor.php |
| Line | 685 | 734 |
| Object | post | strtolower |

Code Snippet
File Name application/controllers/ebor.php
Method function email_approval_detail() {

```
....
685.            $keterangan = $this->input->post('keterangan');
....
734.
      switch(strtolower(str_replace('EBOR','',$keterangan))){
```

**Possible Flow Control\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18437 |
| Status | New |

Possible flow control was found in line 682 in file application/controllers/ebor.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/ebor.php |
| Line | 182 | 734 |
| Object | _POST | strtolower |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/ebor.php

Method function email_approval_detail() {

```
....
734.
      switch(strtolower(str_replace('EBOR','',$keterangan))){
```

**Possible Flow Control\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18438 |
| Status | New |

Possible flow control was found in line 1272 in file application/controllers/implementasi_new.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi_new.php | application/controllers/implementasi_new.php |
| Line | 1281 | 1282 |
| Object | get | tipe_edc |

Code Snippet

File Name application/controllers/implementasi_new.php

Method public function cari_sn()

```
....
1281.                   $tipe_edc = $this->input->get('tipe_edc');
1282.                   switch ($tipe_edc) {
```

**Possible Flow Control\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18439 |
| Status | New |

Possible flow control was found in line 1865 in file application/controllers/implementasi_simple.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi_sim | application/controllers/implementasi_sim |

| | | |
|---|---|---|
| | ple.php | ple.php |
| Line | 1874 | 1875 |
| Object | get | tipe_edc |

Code Snippet
File Name application/controllers/implementasi_simple.php
Method public function cari_sn()

```
....
1874.                   $tipe_edc = $this->input->get('tipe_edc');
1875.                   switch ($tipe_edc) {
```

**Possible Flow Control\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18440 |
| Status | New |

Possible flow control was found in line 50 in file application/controllers/interface_report.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/interface_report.php | application/controllers/interface_report.php |
| Line | 53 | 100 |
| Object | post | tl |

Code Snippet
File Name application/controllers/interface_report.php
Method public function inisiasi_report_process()

```
....
53.         $tl = $this->input->post('tl');
....
100.                            switch ($tl) {
```

**Possible Flow Control\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18441 |
| Status | New |

Possible flow control was found in line 50 in file application/controllers/interface_report.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/interface_report.p |

| | | |
|---|---|---|
| | | hp |
| Line | 182 | 100 |
| Object | _POST | tl |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/interface_report.php

Method public function inisiasi_report_process()

```
....
100.                            switch ($tl) {
```

**Possible Flow Control\Path 11:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18442
Status New

Possible flow control was found in line 888 in file application/controllers/quality_control.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/quality_control.php | application/controllers/quality_control.php |
| Line | 891 | 949 |
| Object | post | tl |

Code Snippet
File Name application/controllers/quality_control.php
Method public function qc_interface_process()

```
....
891.                $tl    = $this->input->post('tl');
....
949.                            switch ($tl) {
```

**Possible Flow Control\Path 12:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18443

| Status | New |
|---|---|

Possible flow control was found in line 888 in file application/controllers/quality_control.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/quality_control.php |
| Line | 182 | 949 |
| Object | _POST | tl |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/quality_control.php

Method public function qc_interface_process()

```
....
949.                            switch ($tl) {
```

**Possible Flow Control\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18444 |
| Status | New |

Possible flow control was found in line 15 in file application/controllers/restore.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/restore.php | application/controllers/restore.php |
| Line | 30 | 34 |
| Object | post | jenis |

Code Snippet

File Name application/controllers/restore.php

Method public function data_upload()

```
....
30.                 $jenis = $this->input->post('jenis');
....
34.                 switch ($jenis) {
```

**Possible Flow Control\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18445 |
| Status | New |

Possible flow control was found in line 15 in file application/controllers/restore.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/restore.php |
| Line | 182 | 34 |
| Object | _POST | jenis |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/restore.php

Method public function data_upload()

```
....
34.                 switch ($jenis) {
```

**Possible Flow Control\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18446 |
| Status | New |

Possible flow control was found in line 27 in file application/libraries/util_indonesia.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php | application/libraries/util_indonesia.php |

| | | |
|---|---|---|
| Line | 2123 | 28 |
| Object | post | month |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php
Method public function sik_ganti_signer_save()

```
....
2123.             $kode_kirim_arr = $this->input-
>post('init_kode_kirim_tmp');
```

File Name application/libraries/util_indonesia.php

Method function get_bulan($month) {

```
....
28.         switch($month) {
```

**Possible Flow Control\Path 16:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18447
Status New

Possible flow control was found in line 27 in file application/libraries/util_indonesia.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/libraries/util_indonesia.php |
| Line | 182 | 28 |
| Object | _POST | month |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/libraries/util_indonesia.php

Method function get_bulan($month) {

```
....
28.         switch($month) {
```

**Possible Flow Control\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18448 |
| Status | New |

Possible flow control was found in line 27 in file application/libraries/util_indonesia.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/implementasi_new.php | application/libraries/util_indonesia.php |
| Line | 2123 | 28 |
| Object | post | month |

Code Snippet

File Name application/controllers/implementasi_new.php

Method public function sik_ganti_signer_save()

```
....
2123.             $kode_kirim_arr = $this->input-
>post('init_kode_kirim_tmp');
```

File Name application/libraries/util_indonesia.php

Method function get_bulan($month) {

```
....
28.         switch($month) {
```

**Possible Flow Control\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18449 |
| Status | New |

Possible flow control was found in line 5 in file application/models/report_model.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/report.php | application/models/report_model.php |
| Line | 86 | 86 |
| Object | get | status |

Code Snippet

File Name application/controllers/report.php

Method public function get_report_app_inisiasi()

```
....
86.                 $wheres    = $this->input->get();
```

File Name application/models/report_model.php

Method public function get_report_app_inisiasi($is_count, $limit, $page, $wheres, $order_by, $is_full = 0)

```
....
86.         switch ($status) {
```

**Possible Flow Control\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18450 |
| Status | New |

Possible flow control was found in line 5 in file application/models/report_model.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/report.php | application/models/report_model.php |
| Line | 86 | 86 |
| Object | get | status |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/report.php

Method public function get_report_app_inisiasi()

```
....
86.                 $wheres    = $this->input->get();
```

File Name application/models/report_model.php

Method public function get_report_app_inisiasi($is_count, $limit, $page, $wheres, $order_by, $is_full = 0)

```
....
86.         switch ($status) {
```

**Possible Flow Control\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18451 |
| Status | New |

Possible flow control was found in line 47 in file application/third_party/dompdf/include/frame_factory.cls.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/frame_factory.cls.php |
| Line | 254 | 62 |
| Object | _SERVER | display |

Code Snippet

File Name application/third_party/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
254.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name application/third_party/dompdf/include/frame_factory.cls.php

Method static function decorate_frame(Frame $frame, DOMPDF $dompdf, Frame $root = null) {

```
....
62.      switch ($display) {
```

**Possible Flow Control\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18452 |
| Status | New |

Possible flow control was found in line 47 in file application/third_party/dompdf/include/frame_factory.cls.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/frame_factory.cls.php |
| Line | 231 | 62 |
| Object | _SERVER | display |

Code Snippet

File Name system/helpers/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
231.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name application/third_party/dompdf/include/frame_factory.cls.php

Method static function decorate_frame(Frame $frame, DOMPDF $dompdf, Frame $root = null) {

```
....
62.      switch ($display) {
```

**Possible Flow Control\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18453 |
| Status | New |

Possible flow control was found in line 221 in file application/third_party/PHPExcel/IOFactory.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/settlement.php | application/third_party/PHPExcel/IOFactory.php |
| Line | 184 | 228 |
| Object | _FILES | strtolower |

Code Snippet

File Name application/controllers/settlement.php

Method function upload_settlement_excel(){

```
....
184.                    $form_extf =
pathinfo($_FILES['file_upload']['name'], PATHINFO_EXTENSION);
```

File Name application/third_party/PHPExcel/IOFactory.php

Method public static function createReaderForFile($pFilename) {

```
....
228.                    switch (strtolower($pathinfo['extension'])) {
```

**Possible Flow Control\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18454 |

| Status | New |
|---|---|

Possible flow control was found in line 221 in file application/third_party/PHPExcel/IOFactory.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/settlement.php | application/third_party/PHPExcel/IOFactory.php |
| Line | 184 | 228 |
| Object | _FILES | strtolower |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/settlement.php
Method function upload_settlement_excel(){

```
....
184.                    $form_extf =
pathinfo($_FILES['file_upload']['name'], PATHINFO_EXTENSION);
```

File Name application/third_party/PHPExcel/IOFactory.php
Method public static function createReaderForFile($pFilename) {

```
....
228.                    switch (strtolower($pathinfo['extension'])) {
```

**Possible Flow Control\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18455 |
| Status | New |

Possible flow control was found in line 328 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard.php |
| Line | 331 | 333 |
| Object | get | param_jenis |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard.php
Method function autocomplete_param_input()

```
....
331.                $param_jenis = trim($this->input->get('param_jenis'));
....
333.                switch ($param_jenis) {
```

**Possible Flow Control\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18456 |
| Status | New |

Possible flow control was found in line 328 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard_20190610.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard_20190610.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard_20190610.php |
| Line | 331 | 333 |
| Object | get | param_jenis |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/dashboard_20190610.php |
| Method | function autocomplete_param_input() |

```
....
331.                $param_jenis = trim($this->input->get('param_jenis'));
....
333.                switch ($param_jenis) {
```

**Possible Flow Control\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18457 |
| Status | New |

Possible flow control was found in line 641 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php |
| Line | 644 | 693 |
| Object | post | strtolower |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php
Method function email_approval_detail() {

```
....
644.              $keterangan = $this->input->post('keterangan');
....
693.
      switch(strtolower(str_replace('EBOR','',$keterangan))){
```

**Possible Flow Control\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18458 |
| Status | New |

Possible flow control was found in line 641 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php |
| Line | 182 | 693 |
| Object | _POST | strtolower |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                          $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/ebor.php
Method function email_approval_detail() {

```
....
693.
      switch(strtolower(str_replace('EBOR','',$keterangan))){
```

**Possible Flow Control\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18459 |
| Status | New |

Possible flow control was found in line 1272 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php |
| Line | 1281 | 1282 |
| Object | get | tipe_edc |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_new.php
Method public function cari_sn()

```
....
1281.                   $tipe_edc = $this->input->get('tipe_edc');
1282.                   switch ($tipe_edc) {
```

**Possible Flow Control\Path 29:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18460
Status New

Possible flow control was found in line 1828 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_simple.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_simple.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_simple.php |
| Line | 1837 | 1838 |
| Object | get | tipe_edc |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/implementasi_simple.php
Method public function cari_sn()

```
....
1837.                   $tipe_edc = $this->input->get('tipe_edc');
1838.                   switch ($tipe_edc) {
```

**Possible Flow Control\Path 30:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti

| | |
|---|---|
| | d=4881&pathid=18461 |
| Status | New |

Possible flow control was found in line 50 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php |
| Line | 53 | 100 |
| Object | post | tl |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php
Method public function inisiasi_report_process()

```
....
53.         $tl = $this->input->post('tl');
....
100.                        switch ($tl) {
```

**Possible Flow Control\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18462 |
| Status | New |

Possible flow control was found in line 50 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php |
| Line | 182 | 100 |
| Object | _POST | tl |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/interface_report.php

| | |
|---|---|
| Method | public function inisiasi_report_process() |

```
....
100.                        switch ($tl) {
```

**Possible Flow Control\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18463 |
| Status | New |

Possible flow control was found in line 888 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php |
| Line | 891 | 949 |
| Object | post | tl |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php |
| Method | public function qc_interface_process() |

```
....
891.              $tl   = $this->input->post('tl');
....
949.                        switch ($tl) {
```

**Possible Flow Control\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18464 |
| Status | New |

Possible flow control was found in line 888 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php |
| Line | 182 | 949 |
| Object | _POST | tl |

Code Snippet

| | |
|---|---|
| File Name | system/core/Input.php |
| Method | function post($index = NULL, $xss_clean = FALSE) |

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/quality_control.php |
| Method | public function qc_interface_process() |

```
....
949.                            switch ($tl) {
```

**Possible Flow Control\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18465 |
| Status | New |

Possible flow control was found in line 15 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php |
| Line | 30 | 34 |
| Object | post | jenis |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php |
| Method | public function data_upload() |

```
....
30.                 $jenis = $this->input->post('jenis');
....
34.                 switch ($jenis) {
```

**Possible Flow Control\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18466 |
| Status | New |

Possible flow control was found in line 15 in file BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php |
| Line | 182 | 34 |
| Object | _POST | jenis |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                        $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php
Method public function data_upload()

```
....
34.                 switch ($jenis) {
```

**Possible Flow Control\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18467 |
| Status | New |

Possible flow control was found in line 5 in file BACKUP_DEPLOY_FMS_20210407/models/models/report_model.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/report.php | BACKUP_DEPLOY_FMS_20210407/models/models/report_model.php |
| Line | 86 | 85 |
| Object | get | status |

Code Snippet
File Name application/controllers/report.php
Method public function get_report_app_inisiasi()

```
....
86.                 $wheres    = $this->input->get();
```

File Name BACKUP_DEPLOY_FMS_20210407/models/models/report_model.php

| | |
|---|---|
| Method | public function get_report_app_inisiasi($is_count, $limit, $page, $wheres, $order_by, $is_full = 0) |

```
....
85.         switch ($status) {
```

**Possible Flow Control\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18468 |
| Status | New |

Possible flow control was found in line 5 in file BACKUP_DEPLOY_FMS_20210407/models/models/report_model.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/report.php | BACKUP_DEPLOY_FMS_20210407/models/models/report_model.php |
| Line | 86 | 85 |
| Object | get | status |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/report.php

Method public function get_report_app_inisiasi()

```
....
86.             $wheres    = $this->input->get();
```

File Name BACKUP_DEPLOY_FMS_20210407/models/models/report_model.php

Method public function get_report_app_inisiasi($is_count, $limit, $page, $wheres, $order_by, $is_full = 0)

```
....
85.         switch ($status) {
```

**Possible Flow Control\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18469 |
| Status | New |

Possible flow control was found in line 143 in file system/libraries/Upload.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | system/libraries/Upload.php | system/libraries/Upload.php |
| Line | 163 | 165 |
| Object | _FILES | error |

Code Snippet
File Name system/libraries/Upload.php
Method public function do_upload($field = 'userfile')

```
....
163.                    $error = ( ! isset($_FILES[$field]['error'])) ?
4 : $_FILES[$field]['error'];
....
165.                    switch($error)
```

**Possible Flow Control\Path 39:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18470
Status New

Possible flow control was found in line 343 in file application/third_party/dompdf/include/frame_decorator.cls.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | application/third_party/dompdf/include/frame_decorator.cls.php |
| Line | 254 | 344 |
| Object | _SERVER | is |

Code Snippet
File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
254.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name application/third_party/dompdf/include/frame_decorator.cls.php
Method function remove_child(Frame $child, $update_node = true) {

```
....
344.      while  ( $child instanceof Frame_Decorator ) {
```

**Possible Flow Control\Path 40:**

Severity Low
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18471 |
| Status | New |

Possible flow control was found in line 343 in file application/third_party/dompdf/include/frame_decorator.cls.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | application/third_party/dompdf/include/frame_decorator.cls.php |
| Line | 231 | 344 |
| Object | _SERVER | is |

Code Snippet
File Name system/helpers/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
231.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name application/third_party/dompdf/include/frame_decorator.cls.php

Method function remove_child(Frame $child, $update_node = true) {

```
....
344.      while  ( $child instanceof Frame_Decorator ) {
```

**Possible Flow Control\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18472 |
| Status | New |

Possible flow control was found in line 235 in file system/helpers/dompdf/include/frame_decorator.cls.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/functions.inc.php | system/helpers/dompdf/include/frame_decorator.cls.php |
| Line | 254 | 236 |
| Object | _SERVER | is |

Code Snippet
File Name application/third_party/dompdf/include/functions.inc.php
Method function explode_url($url) {

```
....
254.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name system/helpers/dompdf/include/frame_decorator.cls.php

Method function remove_child(Frame $child, $update_node = true) {

```
....
236.      while  ( $child instanceof Frame_Decorator )
```

**Possible Flow Control\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18473 |
| Status | New |

Possible flow control was found in line 235 in file system/helpers/dompdf/include/frame_decorator.cls.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/functions.inc.php | system/helpers/dompdf/include/frame_decorator.cls.php |
| Line | 231 | 236 |
| Object | _SERVER | is |

Code Snippet

File Name system/helpers/dompdf/include/functions.inc.php

Method function explode_url($url) {

```
....
231.        $host = isset($_SERVER["HTTP_HOST"]) ? $_SERVER["HTTP_HOST"]
: php_uname("n");
```

File Name system/helpers/dompdf/include/frame_decorator.cls.php

Method function remove_child(Frame $child, $update_node = true) {

```
....
236.      while  ( $child instanceof Frame_Decorator )
```

**Possible Flow Control\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18474 |
| Status | New |

Possible flow control was found in line 1 in file system/helpers/dompdf/www/controller.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/controller.php | system/helpers/dompdf/www/controller.php |
| Line | 22 | 25 |
| Object | _FILES | error |

Code Snippet
File Name system/helpers/dompdf/www/controller.php
Method <?php

```
....
22.      $data = $_FILES["file"];
....
25.        if ($error) {
```

**Possible Flow Control\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18475 |
| Status | New |

Possible flow control was found in line 309 in file application/controllers/admin_super.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/admin_super.php |
| Line | 182 | 410 |
| Object | _POST | post |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                          $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/admin_super.php

Method public function regenerate_mid_tid($appid=null)

```
....
410.                                                    if ($this->input-
>post('cetak_pks'))
```

**Possible Flow Control\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18476 |
| Status | New |

Possible flow control was found in line 517 in file application/controllers/aplikasi_merchant.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 520 | 523 |
| Object | post | all |

Code Snippet

File Name application/controllers/aplikasi_merchant.php

Method public function get_uker($kode_kanwil) {

```
....
520.                $all = $this->input->post('all') ? $this->input-
>post('all') : 0;
....
523.                if ($all) {
```

**Possible Flow Control\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18477 |
| Status | New |

Possible flow control was found in line 517 in file application/controllers/aplikasi_merchant.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_merchant.php |
| Line | 182 | 523 |
| Object | _POST | all |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_merchant.php

Method public function get_uker($kode_kanwil) {

```
....
523.                if ($all) {
```

**Possible Flow Control\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18478 |
| Status | New |

Possible flow control was found in line 679 in file application/controllers/aplikasi_outlet.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_outlet.php |
| Line | 182 | 691 |
| Object | _POST | post |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_outlet.php

Method function ver_outlet_process() {

```
....
691.                if($this->input->post('check_gelondong')){
```

**Possible Flow Control\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18479 |
| Status | New |

Possible flow control was found in line 948 in file application/controllers/aplikasi_outlet.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_outlet.php |
| Line | 182 | 972 |
| Object | _POST | post |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this->_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_outlet.php
Method function app_analis_outlet_process() {

```
....
972.                            else if($this->input->post('flag_gelondong')){
```

**Possible Flow Control\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18480 |
| Status | New |

Possible flow control was found in line 1038 in file application/controllers/aplikasi_outlet.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_outlet.php |
| Line | 182 | 1048 |
| Object | _POST | post |

Code Snippet
File Name system/core/Input.php
Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_outlet.php

Method function app_outlet_process() {

```
....
1048.                    if ($this->input->post('approve')) {
```

**Possible Flow Control\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18481 |
| Status | New |

Possible flow control was found in line 1038 in file application/controllers/aplikasi_outlet.php. This may be used by an attacker to control program's flow and have unexpected behavior.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | application/controllers/aplikasi_outlet.php |
| Line | 182 | 1105 |
| Object | _POST | post |

Code Snippet

File Name system/core/Input.php

Method function post($index = NULL, $xss_clean = FALSE)

```
....
182.                            $post[$key] = $this-
>_fetch_from_array($_POST, $key, $xss_clean);
```

File Name application/controllers/aplikasi_outlet.php

Method function app_outlet_process() {

```
....
1105.                    } elseif ($this->input->post('reject')) {
```

## Client JQuery Deprecated Symbols

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client JQuery Deprecated Symbols Version:1

### Categories

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities

OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2021: A6-Vulnerable and Outdated Components

*Description*

**Client JQuery Deprecated Symbols\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17083 |
| Status | New |

Method $ in application/views/report_msrp/sales_person_search.php, at line 2, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | application/views/report_msrp/sales_person_search.php | application/views/report_msrp/sales_person_search.php |
| Line | 3 | 3 |
| Object | die | die |

Code Snippet
File Name application/views/report_msrp/sales_person_search.php
Method $(document).ready(function(){

```
....
3.    $('.rdinternal').die();
```

**Client JQuery Deprecated Symbols\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17084 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/implementasi_simple/distribusi_tms_form.php, at line 2, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/implementasi_simple/distribusi_tms_form.php | BACKUP_DEPLOY_FMS_20210407/views/views/implementasi_simple/distribusi_tms_form.php |
| Line | 7 | 7 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/implementasi_simple/distribusi_tms_form.php
Method $(document).ready(function(){

```
....
7.    $('#init_provincy').die();
```

**Client JQuery Deprecated Symbols\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17085 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 185 | 185 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
185.        $('.required_ket').die();
```

**Client JQuery Deprecated Symbols\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17086 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 191 | 191 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

| | |
|---|---|
| Method | $(document).ready(function(){ |

```
....
191.        $('.required_foto').die();
```

**Client JQuery Deprecated Symbols\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17087 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 196 | 196 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
196.        $('.tabs-menu a').die();
```

**Client JQuery Deprecated Symbols\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17088 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 223 | 223 |
| Object | die | die |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
223.        $('#btn_next').die();
```

**Client JQuery Deprecated Symbols\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17089 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 250 | 250 |
| Object | die | die |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
250.        $('#btn_previous').die();
```

**Client JQuery Deprecated Symbols\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17090 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 277 | 277 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
277.        $('#btn_draft').die();
```

**Client JQuery Deprecated Symbols\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17091 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 305 | 305 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
305.        $('.checkbox_msrp').die();
```

**Client JQuery Deprecated Symbols\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17092 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 395 | 395 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
395.        $('.tahun').die();
```

**Client JQuery Deprecated Symbols\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17093 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 409 | 409 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
409.        $('.asumsi_pembayaran_auto').die();
```

**Client JQuery Deprecated Symbols\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17094 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 427 | 427 |

| | | |
|---|---|---|
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
427.        $('.trx_kartu_auto').die();
```

**Client JQuery Deprecated Symbols\Path 13:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17095
Status New

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 440 | 440 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
440.        $('.prosentase_off_auto').die();
```

**Client JQuery Deprecated Symbols\Path 14:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17096
Status New

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |

| | | |
|---|---|---|
| Line | 453 | 453 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
453.        $('.trx_bri_auto').die();
```

**Client JQuery Deprecated Symbols\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17097 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 495 | 495 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
495.        $('.datepicker').die('focus');
```

**Client JQuery Deprecated Symbols\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17098 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_t | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_t |

| | | |
|---|---|---|
| | ambah_merchant.php | ambah_merchant.php |
| Line | 511 | 511 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
511.        $('.datepickerymd').die('focus');
```

**Client JQuery Deprecated Symbols\Path 17:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17099
Status New

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 521 | 521 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
521.        $('.currency').die();
```

**Client JQuery Deprecated Symbols\Path 18:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17100
Status New

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 586 | 586 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
586.        $('.hapus_mdr').die();
```

**Client JQuery Deprecated Symbols\Path 19:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17101
Status New

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 608 | 608 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
608.        $('.hapusbank_btn').die();
```

**Client JQuery Deprecated Symbols\Path 20:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17102
Status New

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 631 | 631 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
631.        $('.btn_hapus_edc').die();
```

**Client JQuery Deprecated Symbols\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17103 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 637 | 637 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
637.        $('.edc_tipe').die();
```

**Client JQuery Deprecated Symbols\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17104 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 649 | 649 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
649.        $('#merchant_channel').die();
```

**Client JQuery Deprecated Symbols\Path 23:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17105
Status New

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 697 | 697 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
697.        $('#sub_dsa').die();
```

**Client JQuery Deprecated Symbols\Path 24:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17106
Status New

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 724 | 724 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
724.        $('#sub_channel').die();
```

**Client JQuery Deprecated Symbols\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17107 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 792 | 792 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
792.        $('#kode_kanwil').die();
```

**Client JQuery Deprecated Symbols\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17108 |

| | |
|---|---|
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 997 | 997 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
997.        $('#rek_no').die();
```

**Client JQuery Deprecated Symbols\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17109 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1007 | 1007 |
| Object | die | die |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php
Method $(document).ready(function(){

```
....
1007.       $('.upload').die();
```

**Client JQuery Deprecated Symbols\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=17110 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1063 | 1063 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1063.        $('.photo_upload').die();
```

**Client JQuery Deprecated Symbols\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17111 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1140 | 1140 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1140.        $('.hapus_dokumen_btn').die();
```

**Client JQuery Deprecated Symbols\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17112 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1400 | 1400 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1400.        $('.popup').die();
```

**Client JQuery Deprecated Symbols\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17113 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1437 | 1437 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1437.        $('.datepicker').die('focus');
```

**Client JQuery Deprecated Symbols\Path 32:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17114 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1497 | 1497 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1497.        $('.autocom').die();
```

**Client JQuery Deprecated Symbols\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17115 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1553 | 1553 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1553.        $('#mcc_visa_auto').die('focus');
```

**Client JQuery Deprecated Symbols\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17116 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1560 | 1560 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1560.        $('#mcc_master_auto').die('focus');
```

**Client JQuery Deprecated Symbols\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17117 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1567 | 1567 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1567.        $('#merchant_grouping').die('focus');
```

**Client JQuery Deprecated Symbols\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17118 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1574 | 1574 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1574.        $('#merchant_grouping').die('blur');
```

**Client JQuery Deprecated Symbols\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17119 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1603 | 1603 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1603.        $('#mcc_visa_auto').die('change');
```

**Client JQuery Deprecated Symbols\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17120 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1643 | 1643 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1643.        $('#mcc_master_auto').die('change');
```

**Client JQuery Deprecated Symbols\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17121 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1706 | 1706 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1706.        $('#mcc_npg_auto').die('focus');
```

**Client JQuery Deprecated Symbols\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17122 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1713 | 1713 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method $(document).ready(function(){

```
....
1713.        $('#mcc_unik_auto').die('focus');
```

**Client JQuery Deprecated Symbols\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17123 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1720 | 1720 |
| Object | die | die |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php

| | |
|---|---|
| Method | $(document).ready(function(){ |

```
....
1720.        $('#mcc_npg_auto').die('change');
```

**Client JQuery Deprecated Symbols\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17124 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1762 | 1762 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
1762.        $('#mcc_unik_auto').die('change');
```

**Client JQuery Deprecated Symbols\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17125 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1798 | 1798 |
| Object | die | die |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
1798.        $('.avg_trans').die();
```

**Client JQuery Deprecated Symbols\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17126 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1803 | 1803 |
| Object | die | die |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
1803.        $('.required_style').die();
```

**Client JQuery Deprecated Symbols\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17127 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1816 | 1816 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
1816.        $('.callnumb').die();
```

**Client JQuery Deprecated Symbols\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17128 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 2109 | 2109 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
2109.        $('#exist').die('focus');
```

**Client JQuery Deprecated Symbols\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17129 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 2281 | 2281 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
2281.        $('#redeem_jenis_kartu').die();
```

**Client JQuery Deprecated Symbols\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17130 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 2298 | 2298 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
2298.        $('.opt_redemption').die();
```

**Client JQuery Deprecated Symbols\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17131 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 2344 | 2344 |

| | | |
|---|---|---|
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
2344.        $('.mdr_plan').die();
```

**Client JQuery Deprecated Symbols\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17132 |
| Status | New |

Method $ in BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php, at line 184, calls an obsolete API, die. This has been deprecated, and should not be used in a modern codebase.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 2352 | 2352 |
| Object | die | die |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | $(document).ready(function(){ |

```
....
2352.        $('.mdr_term').die();
```

## XSS Evasion Attack

Query Path:
PHP\Cx\Php Low Visibility\XSS Evasion Attack Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: Access Control
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
OWASP Top 10 2021: A3-Injection

*Description*

**XSS Evasion Attack\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13633 |
| Status | New |

Method <?php at line 1 of application/third_party/dompdf/dompdf.php gets a client-side controlled data for the rawurldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <?php at line 1 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 202 | 260 |
| Object | rawurldecode | echo |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
202.      $paper = rawurldecode($_GET["paper"]);
....
260.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**XSS Evasion Attack\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13634 |
| Status | New |

Method <?php at line 1 of application/third_party/dompdf/dompdf.php gets a client-side controlled data for the rawurldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <?php at line 1 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 207 | 260 |
| Object | rawurldecode | echo |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
207.      $orientation = rawurldecode($_GET["orientation"]);
....
260.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**XSS Evasion Attack\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13635 |
| Status | New |

Method <?php at line 1 of application/third_party/dompdf/dompdf.php gets a client-side controlled data for the rawurldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <?php at line 1 of application/third_party/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/dompdf.php | application/third_party/dompdf/dompdf.php |
| Line | 212 | 260 |
| Object | rawurldecode | echo |

Code Snippet
File Name application/third_party/dompdf/dompdf.php
Method <?php

```
....
212.      $base_path = rawurldecode($_GET["base_path"]);
....
260.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**XSS Evasion Attack\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13636 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/dompdf.php gets a client-side controlled data for the rawurldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <?php at line 1 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 203 | 261 |
| Object | rawurldecode | echo |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
203.      $paper = rawurldecode($_GET["paper"]);
....
261.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**XSS Evasion Attack\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13637 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/dompdf.php gets a client-side controlled data for the rawurldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <?php at line 1 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 208 | 261 |
| Object | rawurldecode | echo |

Code Snippet
File Name system/helpers/dompdf/dompdf.php
Method <?php

```
....
208.      $orientation = rawurldecode($_GET["orientation"]);
....
261.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**XSS Evasion Attack\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13638 |
| Status | New |

Method <?php at line 1 of system/helpers/dompdf/dompdf.php gets a client-side controlled data for the rawurldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <?php at line 1 of system/helpers/dompdf/dompdf.php.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/dompdf.php | system/helpers/dompdf/dompdf.php |
| Line | 213 | 261 |
| Object | rawurldecode | echo |

Code Snippet
File Name system/helpers/dompdf/dompdf.php

| | |
|---|---|
| Method | <?php |

```
....
213.      $base_path = rawurldecode($_GET["base_path"]);
....
261.    echo $dompdf->get_canvas()->get_cpdf()->messages;
```

**XSS Evasion Attack\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13639 |
| Status | New |

Method update_signer_settle_debit at line 452 of application/controllers/dashboard_settlement.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in update_signer_settle_debit at line 452 of application/controllers/dashboard_settlement.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/dashboard_settlement.php | application/controllers/dashboard_settlement.php |
| Line | 490 | 561 |
| Object | json_decode | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/dashboard_settlement.php |
| Method | public function update_signer_settle_debit(){ |

```
....
490.                                        $arr_out_inq =
json_decode($out_inq);
....
561.                                        echo '0|Push settle gagal
'.$msg_aksi.'. Gagal settle : '.$msg_settle.'.';
```

**XSS Evasion Attack\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13640 |
| Status | New |

Method update_signer_settle_debit at line 452 of application/controllers/dashboard_settlement.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in update_signer_settle_debit at line 452 of application/controllers/dashboard_settlement.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/dashboard_settlement.php | application/controllers/dashboard_settlement.php |
| Line | 508 | 561 |

| | | |
|---|---|---|
| Object | json_decode | echo |

Code Snippet
File Name application/controllers/dashboard_settlement.php
Method public function update_signer_settle_debit(){

```
....
508.                                                    $arr_out_psw
= json_decode($out_psw);
....
561.                                        echo '0|Push settle gagal
'.$msg_aksi.'. Gagal settle : '.$msg_settle.'.';
```

**XSS Evasion Attack\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13641 |
| Status | New |

Method pilotsettledebit at line 617 of application/controllers/dashboard_settlement.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in pilotsettledebit at line 617 of application/controllers/dashboard_settlement.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/dashboard_settlement.php | application/controllers/dashboard_settlement.php |
| Line | 629 | 663 |
| Object | json_decode | echo |

Code Snippet
File Name application/controllers/dashboard_settlement.php
Method public function pilotsettledebit(){

```
....
629.            $arr_out_inq = json_decode($out_inq);
....
663.            echo $msg_settle;
```

**XSS Evasion Attack\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13642 |
| Status | New |

Method pilotsettledebit at line 617 of application/controllers/dashboard_settlement.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in pilotsettledebit at line 617 of application/controllers/dashboard_settlement.php.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/controllers/dashboard_settlement.php | application/controllers/dashboard_settlement.php |
| Line | 646 | 663 |
| Object | json_decode | echo |

Code Snippet
File Name application/controllers/dashboard_settlement.php
Method public function pilotsettledebit(){

```
....
646.                                $arr_out_psw =
json_decode($out_psw);
....
663.                echo $msg_settle;
```

**XSS Evasion Attack\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13643 |
| Status | New |

Method get_subchannel at line 1221 of application/controllers/maintenance.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1221 of application/controllers/maintenance.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | application/controllers/maintenance.php |
| Line | 1225 | 1262 |
| Object | urldecode | echo |

Code Snippet
File Name application/controllers/maintenance.php
Method function get_subchannel()

```
....
1225.              $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1262.                    echo form_dropdown('sub_channel',
$opt_subchannel, $sub_channel, 'class="required"');
```

**XSS Evasion Attack\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13644 |
| Status | New |

Method get_subchannel at line 1221 of application/controllers/maintenance.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1221 of application/controllers/maintenance.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance.php | application/controllers/maintenance.php |
| Line | 1225 | 1264 |
| Object | urldecode | echo |

Code Snippet
File Name application/controllers/maintenance.php
Method function get_subchannel()

```
....
1225.             $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1264.                   echo form_dropdown('', $opt_subchannel,
$sub_channel, 'class="required" id="sub_dsa"');
```

**XSS Evasion Attack\Path 13:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13645
Status New

Method get_subchannel at line 1188 of application/controllers/maintenance_20181213.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1188 of application/controllers/maintenance_20181213.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20181213.php | application/controllers/maintenance_20181213.php |
| Line | 1192 | 1215 |
| Object | urldecode | echo |

Code Snippet
File Name application/controllers/maintenance_20181213.php
Method function get_subchannel()

```
....
1192.             $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1215.                   echo form_dropdown('sub_channel',
$opt_subchannel, $sub_channel, 'class="required"');
```

**XSS Evasion Attack\Path 14:**

Severity Low

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13646 |
| Status | New |

Method get_subchannel at line 1188 of application/controllers/maintenance_20181213.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1188 of application/controllers/maintenance_20181213.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20181213.php | application/controllers/maintenance_20181213.php |
| Line | 1192 | 1217 |
| Object | urldecode | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/maintenance_20181213.php |
| Method | function get_subchannel() |

```
....
1192.             $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1217.                   echo form_dropdown('', $opt_subchannel,
$sub_channel, 'class="required" id="sub_dsa"');
```

**XSS Evasion Attack\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13647 |
| Status | New |

Method get_subchannel at line 1190 of application/controllers/maintenance_20190524.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1190 of application/controllers/maintenance_20190524.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | application/controllers/maintenance_20190524.php |
| Line | 1194 | 1231 |
| Object | urldecode | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/maintenance_20190524.php |
| Method | function get_subchannel() |

```
....
1194.              $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1231.                    echo form_dropdown('sub_channel',
$opt_subchannel, $sub_channel, 'class="required"');
```

**XSS Evasion Attack\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13648 |
| Status | New |

Method get_subchannel at line 1190 of application/controllers/maintenance_20190524.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1190 of application/controllers/maintenance_20190524.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190524.php | application/controllers/maintenance_20190524.php |
| Line | 1194 | 1233 |
| Object | urldecode | echo |

Code Snippet

File Name application/controllers/maintenance_20190524.php

Method function get_subchannel()

```
....
1194.              $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1233.                    echo form_dropdown('', $opt_subchannel,
$sub_channel, 'class="required" id="sub_dsa"');
```

**XSS Evasion Attack\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13649 |
| Status | New |

Method get_subchannel at line 1190 of application/controllers/maintenance_20190610.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1190 of application/controllers/maintenance_20190610.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | application/controllers/maintenance_20190610.php |
| Line | 1194 | 1231 |

| | | |
|---|---|---|
| Object | urldecode | echo |

Code Snippet
File Name application/controllers/maintenance_20190610.php
Method function get_subchannel()

```
....
1194.             $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1231.                   echo form_dropdown('sub_channel',
$opt_subchannel, $sub_channel, 'class="required"');
```

**XSS Evasion Attack\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13650 |
| Status | New |

Method get_subchannel at line 1190 of application/controllers/maintenance_20190610.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1190 of application/controllers/maintenance_20190610.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_20190610.php | application/controllers/maintenance_20190610.php |
| Line | 1194 | 1233 |
| Object | urldecode | echo |

Code Snippet
File Name application/controllers/maintenance_20190610.php
Method function get_subchannel()

```
....
1194.             $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1233.                   echo form_dropdown('', $opt_subchannel,
$sub_channel, 'class="required" id="sub_dsa"');
```

**XSS Evasion Attack\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13651 |
| Status | New |

Method get_subchannel at line 1109 of application/controllers/maintenance_bck07112017.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1109 of application/controllers/maintenance_bck07112017.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck07112017.php | application/controllers/maintenance_bck07112017.php |
| Line | 1113 | 1133 |
| Object | urldecode | echo |

Code Snippet
File Name application/controllers/maintenance_bck07112017.php
Method function get_subchannel()

```
....
1113.             $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1133.             echo form_dropdown('sub_channel', $opt_subchannel,
$sub_channel, 'class="required"');
```

**XSS Evasion Attack\Path 20:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13652
Status New

Method get_subchannel at line 1188 of application/controllers/maintenance_bck20180906.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1188 of application/controllers/maintenance_bck20180906.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20180906.php | application/controllers/maintenance_bck20180906.php |
| Line | 1192 | 1215 |
| Object | urldecode | echo |

Code Snippet
File Name application/controllers/maintenance_bck20180906.php
Method function get_subchannel()

```
....
1192.             $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1215.                   echo form_dropdown('sub_channel',
$opt_subchannel, $sub_channel, 'class="required"');
```

**XSS Evasion Attack\Path 21:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13653

| | |
|---|---|
| Status | New |

Method get_subchannel at line 1188 of application/controllers/maintenance_bck20180906.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1188 of application/controllers/maintenance_bck20180906.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20180906.php | application/controllers/maintenance_bck20180906.php |
| Line | 1192 | 1217 |
| Object | urldecode | echo |

Code Snippet
File Name application/controllers/maintenance_bck20180906.php
Method function get_subchannel()

```
....
1192.             $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1217.                   echo form_dropdown('', $opt_subchannel,
$sub_channel, 'class="required" id="sub_dsa"');
```

**XSS Evasion Attack\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13654 |
| Status | New |

Method get_subchannel at line 1188 of application/controllers/maintenance_bck20190114.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1188 of application/controllers/maintenance_bck20190114.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20190114.php | application/controllers/maintenance_bck20190114.php |
| Line | 1192 | 1229 |
| Object | urldecode | echo |

Code Snippet
File Name application/controllers/maintenance_bck20190114.php
Method function get_subchannel()

```
....
1192.             $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1229.                   echo form_dropdown('sub_channel',
$opt_subchannel, $sub_channel, 'class="required"');
```

**XSS Evasion Attack\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13655 |
| Status | New |

Method get_subchannel at line 1188 of application/controllers/maintenance_bck20190114.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 1188 of application/controllers/maintenance_bck20190114.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/maintenance_bck20190114.php | application/controllers/maintenance_bck20190114.php |
| Line | 1192 | 1231 |
| Object | urldecode | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/maintenance_bck20190114.php |
| Method | function get_subchannel() |

```
....
1192.             $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
1231.                   echo form_dropdown('', $opt_subchannel,
$sub_channel, 'class="required" id="sub_dsa"');
```

**XSS Evasion Attack\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13656 |
| Status | New |

Method delete_tid_brilink at line 950 of application/controllers/patching.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in delete_tid_brilink at line 950 of application/controllers/patching.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/patching.php | application/controllers/patching.php |
| Line | 962 | 970 |
| Object | json_decode | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/patching.php |
| Method | function delete_tid_brilink($tid) { |

```
....
962.            $response = json_decode($curl_response);
....
970.        echo $response;
```

**XSS Evasion Attack\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13657 |
| Status | New |

Method get_jenis_masalah at line 420 of application/controllers/settlement.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_jenis_masalah at line 420 of application/controllers/settlement.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/settlement.php | application/controllers/settlement.php |
| Line | 433 | 435 |
| Object | urldecode | echo |

Code Snippet
File Name application/controllers/settlement.php
Method function get_jenis_masalah()

```
....
433.                                    $jenis = urldecode($this->uri->segment(3));
....
435.                            echo form_dropdown('jenis', $opt_sub_jenis, $jenis, 'class="required" id="jenis"');
```

**XSS Evasion Attack\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13658 |
| Status | New |

Method get_subchannel at line 504 of application/controllers/settlement.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 504 of application/controllers/settlement.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/settlement.php | application/controllers/settlement.php |
| Line | 508 | 531 |
| Object | urldecode | echo |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/settlement.php |
| Method | function get_subchannel() |

```
....
508.                $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
531.                      echo form_dropdown('sub_channel',
$opt_subchannel, $sub_channel, 'class="required"');
```

**XSS Evasion Attack\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13659 |
| Status | New |

Method get_subchannel at line 504 of application/controllers/settlement.php gets a client-side controlled data for the urldecode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in get_subchannel at line 504 of application/controllers/settlement.php.

| | Source | Destination |
|---|---|---|
| File | application/controllers/settlement.php | application/controllers/settlement.php |
| Line | 508 | 533 |
| Object | urldecode | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/settlement.php |
| Method | function get_subchannel() |

```
....
508.                $sub_channel      = urldecode($this->input-
>post('sub_channel'));
....
533.                      echo form_dropdown('', $opt_subchannel,
$sub_channel, 'class="required" id="sub_dsa"');
```

**XSS Evasion Attack\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13660 |
| Status | New |

Method read_param_blacklist at line 265 of application/helpers/view_helper.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in read_param_blacklist at line 265 of application/helpers/view_helper.php.

| | Source | Destination |
|---|---|---|
| File | application/helpers/view_helper.php | application/helpers/view_helper.php |
| Line | 274 | 325 |

| | | |
|---|---|---|
| Object | json_decode | echo |

Code Snippet
File Name application/helpers/view_helper.php
Method function read_param_blacklist($id_blacklist_param='', $mid="")

```
....
274.        $data = (json_decode($id_blacklist_param));
....
325.                                echo $param[1];
```

**XSS Evasion Attack\Path 29:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13661
Status New

Method read_param_blacklist at line 265 of application/helpers/view_helper.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in read_param_blacklist at line 265 of application/helpers/view_helper.php.

| | Source | Destination |
|---|---|---|
| File | application/helpers/view_helper.php | application/helpers/view_helper.php |
| Line | 274 | 381 |
| Object | json_decode | echo |

Code Snippet
File Name application/helpers/view_helper.php
Method function read_param_blacklist($id_blacklist_param='', $mid="")

```
....
274.        $data = (json_decode($id_blacklist_param));
....
381.                                        echo $param[0];
```

**XSS Evasion Attack\Path 30:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13662
Status New

Method read_param_blacklist at line 265 of application/helpers/view_helper.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in read_param_blacklist at line 265 of application/helpers/view_helper.php.

| | Source | Destination |
|---|---|---|
| File | application/helpers/view_helper.php | application/helpers/view_helper.php |

| | | |
|---|---|---|
| Line | 274 | 283 |
| Object | json_decode | echo |

Code Snippet
File Name application/helpers/view_helper.php
Method function read_param_blacklist($id_blacklist_param='', $mid="")

```
....
274.        $data = (json_decode($id_blacklist_param));
....
283.                        echo $arr_param[$x]."<br>";
```

**XSS Evasion Attack\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13663 |
| Status | New |

Method read_param_blacklist at line 265 of application/helpers/view_helper.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in read_param_blacklist at line 265 of application/helpers/view_helper.php.

| | Source | Destination |
|---|---|---|
| File | application/helpers/view_helper.php | application/helpers/view_helper.php |
| Line | 274 | 277 |
| Object | json_decode | echo |

Code Snippet
File Name application/helpers/view_helper.php
Method function read_param_blacklist($id_blacklist_param='', $mid="")

```
....
274.        $data = (json_decode($id_blacklist_param));
....
277.              echo "<td><a class='lihat'
href='".site_url('admin/detail_merchant_blacklist')."?id=".key($data[$i]
)."'>".key($data[$i])."</a></td>";
```

**XSS Evasion Attack\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13664 |
| Status | New |

Method read_more_param_blacklist at line 393 of application/helpers/view_helper.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in read_more_param_blacklist at line 393 of application/helpers/view_helper.php.

| | Source | Destination |
|---|---|---|
| File | application/helpers/view_helper.php | application/helpers/view_helper.php |
| Line | 402 | 409 |
| Object | json_decode | echo |

Code Snippet
File Name application/helpers/view_helper.php
Method function read_more_param_blacklist($id_blacklist_param='', $mid="", $id="")

```
....
402.        $data = (json_decode($id_blacklist_param));
....
409.                                echo $arr_param[$x]."<br>";
```

**XSS Evasion Attack\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13665 |
| Status | New |

Method read_more_param_blacklist at line 393 of application/helpers/view_helper.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in read_more_param_blacklist at line 393 of application/helpers/view_helper.php.

| | Source | Destination |
|---|---|---|
| File | application/helpers/view_helper.php | application/helpers/view_helper.php |
| Line | 402 | 405 |
| Object | json_decode | echo |

Code Snippet
File Name application/helpers/view_helper.php
Method function read_more_param_blacklist($id_blacklist_param='', $mid="", $id="")

```
....
402.        $data = (json_decode($id_blacklist_param));
....
405.                    echo "ID Blacklist ".key($data[$i])." : </br>";
```

**XSS Evasion Attack\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13666 |
| Status | New |

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code

without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_high_risk.php | application/views/admin/v_detail_mcs_mcc_high_risk.php |
| Line | 59 | 97 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_high_risk.php
Method <script type="text/javascript">

```
....
59.   $mcc = json_decode($data_mcs->data_mcc);
....
97.   <td align="center"><?=$_mcc->risk?></td>
```

**XSS Evasion Attack\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13667 |
| Status | New |

Method <script type="text/javascript">> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_high_risk.php | application/views/admin/v_detail_mcs_mcc_high_risk.php |
| Line | 59 | 96 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_high_risk.php
Method <script type="text/javascript">

```
....
59.   $mcc = json_decode($data_mcs->data_mcc);
....
96.   <td align="center"><?=$_mcc->fee_type?></td>
```

**XSS Evasion Attack\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13668 |
| Status | New |

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_high_risk.php | application/views/admin/v_detail_mcs_mcc_high_risk.php |
| Line | 59 | 92 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_high_risk.php
Method <script type="text/javascript">

```
....
59.   $mcc = json_decode($data_mcs->data_mcc);
....
92.   <td align="center"><?=$_mcc->fee_unik != '' ? $_mcc->fee_unik : '-
'?></td>
```

**XSS Evasion Attack\Path 37:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13669
Status New

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_high_risk.php | application/views/admin/v_detail_mcs_mcc_high_risk.php |
| Line | 59 | 91 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_high_risk.php
Method <script type="text/javascript">

```
....
59.   $mcc = json_decode($data_mcs->data_mcc);
....
91.   <td align="center"><?=$_mcc->fee_off_us != '' ? $_mcc->fee_off_us
: '-'?></td>
```

**XSS Evasion Attack\Path 38:**

Severity Low

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13670 |
| Status | New |

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_high_risk.php | application/views/admin/v_detail_mcs_mcc_high_risk.php |
| Line | 59 | 90 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_high_risk.php
Method <script type="text/javascript">

```
....
59.   $mcc = json_decode($data_mcs->data_mcc);
....
90.   <td align="center"><?=$_mcc->fee_on_us != '' ? $_mcc->fee_on_us :
'-'?></td>
```

**XSS Evasion Attack\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13671 |
| Status | New |

Method <script type="text/javascript">> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_high_risk.php | application/views/admin/v_detail_mcs_mcc_high_risk.php |
| Line | 59 | 94 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_high_risk.php
Method <script type="text/javascript">

```
....
59.   $mcc = json_decode($data_mcs->data_mcc);
....
94.   <td align="center"><?=$_mcc->fee?></td>
```

**XSS Evasion Attack\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13672 |
| Status | New |

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_high_risk.php | application/views/admin/v_detail_mcs_mcc_high_risk.php |
| Line | 59 | 88 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_high_risk.php
Method <script type="text/javascript">

```
....
59.   $mcc = json_decode($data_mcs->data_mcc);
....
88.   <td align="center">><?=$_mcc->deskripsi?></td>
```

**XSS Evasion Attack\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13673 |
| Status | New |

Method <script type="text/javascript">> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript">> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_high_risk.php | application/views/admin/v_detail_mcs_mcc_high_risk.php |
| Line | 59 | 87 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_high_risk.php
Method <script type="text/javascript">

```
....
59.   $mcc = json_decode($data_mcs->data_mcc);
....
87.   <?php if ($data_mcs->jenis_mcc != 'NPG') { ?><td
align="center"><?=$_mcc->tcc?></td><?php } ?>
```

**XSS Evasion Attack\Path 42:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13674
Status New

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_high_risk.php | application/views/admin/v_detail_mcs_mcc_high_risk.php |
| Line | 59 | 86 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_high_risk.php
Method <script type="text/javascript">

```
....
59.   $mcc = json_decode($data_mcs->data_mcc);
....
86.   <td align="center"><?=$_mcc->grup == 'UNIK' ? 'UANG ELEKTRONIK' :
$_mcc->grup?></td>
```

**XSS Evasion Attack\Path 43:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13675
Status New

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_high_risk.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_high_risk.php | application/views/admin/v_detail_mcs_mcc_high_risk.php |

| | | |
|---|---|---|
| Line | 59 | 84 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_high_risk.php
Method <script type="text/javascript">

```
....
59.   $mcc = json_decode($data_mcs->data_mcc);
....
84.   <td align="center"><b><?=$_mcc->kode?></b></td>
```

**XSS Evasion Attack\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13676 |
| Status | New |

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_jcb.php | application/views/admin/v_detail_mcs_mcc_jcb.php |
| Line | 89 | 131 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_jcb.php
Method <script type="text/javascript">

```
....
89.   $mcc = json_decode($data_mcs->data_mcc);
....
131.                    <input type="hidden" value="<?= $mcc->risk?>"
name="risk"/>
```

**XSS Evasion Attack\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13677 |
| Status | New |

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_jcb.php | application/views/admin/v_detail_mcs_mcc_jcb.php |
| Line | 89 | 130 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_jcb.php
Method <script type="text/javascript">

```
....
89.   $mcc = json_decode($data_mcs->data_mcc);
....
130.                    <td><?= $mcc->risk?>
```

**XSS Evasion Attack\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13678 |
| Status | New |

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_jcb.php | application/views/admin/v_detail_mcs_mcc_jcb.php |
| Line | 89 | 125 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_jcb.php
Method <script type="text/javascript">

```
....
89.   $mcc = json_decode($data_mcs->data_mcc);
....
125.                    <input type="hidden" value="<?= $mcc-
>fee_type?>" name="fee_type"/>
```

**XSS Evasion Attack\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13679 |
| Status | New |

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_jcb.php | application/views/admin/v_detail_mcs_mcc_jcb.php |
| Line | 89 | 124 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_jcb.php
Method <script type="text/javascript">

```
....
89.   $mcc = json_decode($data_mcs->data_mcc);
....
124.                    <td><?= $mcc->fee_type?>
```

**XSS Evasion Attack\Path 48:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13680
Status New

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_jcb.php | application/views/admin/v_detail_mcs_mcc_jcb.php |
| Line | 89 | 119 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_jcb.php
Method <script type="text/javascript">

```
....
89.   $mcc = json_decode($data_mcs->data_mcc);
....
119.                    <input type="hidden" value="<?= $mcc->fee?>"
name="fee"/>
```

**XSS Evasion Attack\Path 49:**

Severity Low
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13681 |
| Status | New |

Method <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_jcb.php | application/views/admin/v_detail_mcs_mcc_jcb.php |
| Line | 89 | 118 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_jcb.php
Method <script type="text/javascript">

```
....
89.   $mcc = json_decode($data_mcs->data_mcc);
....
118.                    <td><?= $mcc->fee?>
```

**XSS Evasion Attack\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13682 |
| Status | New |

Method <script type="text/javascript">> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php gets a client-side controlled data for the json_decode element. This element's value is used in client-side code without being properly sanitized or validated and is eventually integrated into the HTML code in <script type="text/javascript"> at line 1 of application/views/admin/v_detail_mcs_mcc_jcb.php.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_detail_mcs_mcc_jcb.php | application/views/admin/v_detail_mcs_mcc_jcb.php |
| Line | 89 | 113 |
| Object | json_decode | echo |

Code Snippet
File Name application/views/admin/v_detail_mcs_mcc_jcb.php
Method <script type="text/javascript">

```
....
89.   $mcc = json_decode($data_mcs->data_mcc);
....
113.                    <input type="hidden" value="<?= $mcc-
>deskripsi?>" name="deskripsi"/>
```

# Unsafe Use Of Target blank

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Unsafe Use Of Target blank Version:1

## Categories

FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

## *Description*

**Unsafe Use Of Target blank\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22471 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank"> at line 587 of application/controllers/aplikasi_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 587 | 587 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

Code Snippet

File Name application/controllers/aplikasi_merchant.php

Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';

```
....
587.                            $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22472 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank"> at line 1222 of application/controllers/aplikasi_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |

| | | |
|---|---|---|
| Line | 1222 | 1222 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';

```
....
1222.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22473 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank">> at line 119 of application/controllers/aplikasi_tambah_merchant/analisa.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/analisa.php | application/controllers/aplikasi_tambah_merchant/analisa.php |
| Line | 119 | 119 |
| Object | <a href="' . $lihat_path . '" target="_blank">> | <a href="' . $lihat_path . '" target="_blank">> |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/analisa.php
Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';

```
....
119.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22474 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank">> at line 663 of application/controllers/aplikasi_tambah_merchant/input_merchant.php, without correctly setting the

"rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 663 | 663 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php
Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';

```
....
663.                    $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22475 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank">> at line 646 of application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php |
| Line | 646 | 646 |
| Object | <a href="' . $lihat_path . '" target="_blank">> | <a href="' . $lihat_path . '" target="_blank">> |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php
Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';

```
....
646.                    $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22476 |
| Status | New |

Using <a href="'.$filename.'" target="_blank"> at line 77 of application/controllers/inisiasi_checker.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_checker.php | application/controllers/inisiasi_checker.php |
| Line | 77 | 77 |
| Object | <a href="'.$filename.'" target="_blank"> | <a href="'.$filename.'" target="_blank"> |

Code Snippet

File Name application/controllers/inisiasi_checker.php

Method $data_insert['cl_mid_log'] .= 'See the report from Cardlink <a href="'.$filename.'" target="_blank">here</a>';

```
....
77.                                 $data_insert['cl_mid_log'] .= 'See
the report from Cardlink <a href="'.$filename.'"
target="_blank">here</a>';
```

**Unsafe Use Of Target blank\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22477 |
| Status | New |

Using <a href="'.$filename.'" target="_blank"> at line 118 of application/controllers/inisiasi_checker.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_checker.php | application/controllers/inisiasi_checker.php |
| Line | 118 | 118 |
| Object | <a href="'.$filename.'" target="_blank"> | <a href="'.$filename.'" target="_blank"> |

Code Snippet

File Name application/controllers/inisiasi_checker.php

Method $data_insert['cl_tid_log'] .= 'See the report from Cardlink <a href="'.$filename.'" target="_blank">here</a><br>';

```
....
118.                                $data_insert['cl_tid_log'] .= 'See
the report from Cardlink <a href="'.$filename.'"
target="_blank">here</a><br>';
```

**Unsafe Use Of Target blank\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22478 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank"> at line 952 of application/controllers/pameran.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/pameran.php | application/controllers/pameran.php |
| Line | 952 | 952 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

Code Snippet

File Name application/controllers/pameran.php

Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';

```
....
952.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22479 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank"> at line 773 of application/controllers/qris.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/qris.php | application/controllers/qris.php |
| Line | 773 | 773 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/qris.php |
| Method | $label = '<a href="' . $lihat_path . '" target="_blank">' . $config['file_name'] . '</a>  '; |

```
....
773.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $config['file_name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22480 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> at line 111 of application/views/admin/v_admin_paket_bismod.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_admin_paket_bismod.php | application/views/admin/v_admin_paket_bismod.php |
| Line | 111 | 111 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/admin/v_admin_paket_bismod.php |
| Method | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank">Download Form MCC JCB High Risk </a>    |

```
....
111.                <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>"
target="_blank">Download Form MCC JCB High Risk </a>   
```

**Unsafe Use Of Target blank\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22481 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> at line 162 of application/views/admin/v_admin_paket_bismod.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_admin_paket_bismod.php | application/views/admin/v_admin_paket_bismod.php |
| Line | 162 | 162 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> |

Code Snippet

File Name application/views/admin/v_admin_paket_bismod.php

Method <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank">Download Form MCC JCB High Risk </a>   

```
....
162.              <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>"
target="_blank">Download Form MCC JCB High Risk </a>   
```

**Unsafe Use Of Target blank\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22482 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> at line 145 of application/views/admin/v_manage_mcc_jcb.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_mcc_jcb.php | application/views/admin/v_manage_mcc_jcb.php |
| Line | 145 | 145 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/admin/v_manage_mcc_jcb.php |
| Method | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank">Download Form MCC JCB High Risk </a>    |

```
....
145.              <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>"
target="_blank">Download Form MCC JCB High Risk </a>   
```

**Unsafe Use Of Target blank\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22483 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_master_high_risk'?>" target="_blank"> at line 145 of application/views/admin/v_manage_mcc_master.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_mcc_master.php | application/views/admin/v_manage_mcc_master.php |
| Line | 145 | 145 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_master_high_risk'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_master_high_risk'?>" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/admin/v_manage_mcc_master.php |
| Method | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_master_high_risk'?>" target="_blank">Download Form MCC Master High Risk </a>    |

```
....
145.              <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_mcc_master_high_risk'?>"
target="_blank">Download Form MCC Master High Risk
</a>   
```

**Unsafe Use Of Target blank\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=22484 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank"> at line 152 of application/views/admin/v_manage_mcc_npg.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_mcc_npg.php | application/views/admin/v_manage_mcc_npg.php |
| Line | 152 | 152 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank"> |

Code Snippet

File Name application/views/admin/v_manage_mcc_npg.php

Method <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank">Download Form MCC NPG & Unik High Risk </a> 

```
....
152.                    <a id="download" style="color:#FFF;text-
decoration: none" class="button"
href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>"
target="_blank">Download Form MCC NPG & Unik High Risk </a> 
```

**Unsafe Use Of Target blank\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22485 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank"> at line 173 of application/views/admin/v_manage_mcc_npg.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_mcc_npg.php | application/views/admin/v_manage_mcc_npg.php |
| Line | 173 | 173 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_f | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_f |

| | | |
|---|---|---|
| | orm_mcc_npg_high_risk'?>" target="_blank"> | orm_mcc_npg_high_risk'?>" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/admin/v_manage_mcc_npg.php |
| Method | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank">Download Form MCC NPG & Unik High Risk </a>  |

```
....
173.                    <a id="download" style="color:#FFF;text-
decoration: none" class="button"
href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>"
target="_blank">Download Form MCC NPG & Unik High Risk </a> 
```

**Unsafe Use Of Target blank\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22486 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_visa_high_risk'?>" target="_blank"> at line 145 of application/views/admin/v_manage_mcc_visa.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_mcc_visa.php | application/views/admin/v_manage_mcc_visa.php |
| Line | 145 | 145 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_visa_high_risk'?>" target="_blank">> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_visa_high_risk'?>" target="_blank">> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/admin/v_manage_mcc_visa.php |
| Method | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_visa_high_risk'?>" target="_blank">Download Form MCC Visa High Risk </a>    |

```
....
145.                <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_mcc_visa_high_risk'?>"
target="_blank">Download Form MCC Visa High Risk </a>   
```

**Unsafe Use Of Target blank\Path 17:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22487 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_blacklist'?>" target="_blank"> at line 159 of application/views/admin/v_manage_merchant_blacklist.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_merchant_blacklist.php | application/views/admin/v_manage_merchant_blacklist.php |
| Line | 159 | 159 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_blacklist'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_blacklist'?>" target="_blank"> |

Code Snippet

File Name application/views/admin/v_manage_merchant_blacklist.php

Method <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_blacklist'?>" target="_blank">Download Form Pengisian </a>   

```
....
159.              <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_blacklist'?>"
target="_blank">Download Form Pengisian </a>   
```

**Unsafe Use Of Target blank\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22488 |
| Status | New |

Using <a href="<?=site_url('admin/manage_target_marketing_form_download');?>" target="_blank" id="download_target"> at line 47 of application/views/admin/v_manage_target_marketing_form.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_target_marketing_form.php | application/views/admin/v_manage_target_marketing_form.php |
| Line | 47 | 47 |
| Object | <a href="<?=site_url('admin/manage_targe | <a href="<?=site_url('admin/manage_targe |

| | | |
|---|---|---|
| | t_marketing_form_download');?>" target="_blank" id="download_target"> | t_marketing_form_download');?>" target="_blank" id="download_target"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/admin/v_manage_target_marketing_form.php |
| Method | <td><a href="<?=site_url('admin/manage_target_marketing_form_download');?>" target="_blank" id="download_target">Download</a></td> |

```
....
47.         <td><a
href="<?=site_url('admin/manage_target_marketing_form_download');?>"
target="_blank" id="download_target">Download</a></td>
```

**Unsafe Use Of Target blank\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22489 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> at line 1056 of application/views/aplikasi_edit/edit_merchant_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant_new.php | application/views/aplikasi_edit/edit_merchant_new.php |
| Line | 1056 | 1056 |
| Object | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_edit/edit_merchant_new.php |
| Method | tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">'+arr_data['photo_name']+'</a>'; |

```
....
1056.                                   tr_foto_append += '<td><canvas
id="'+canvas_id+'" height="0" width="0"
style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="'+arr_data['lihat_path']+'"
target="_blank">'+arr_data['photo_name']+'</a>';
```

**Unsafe Use Of Target blank\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22490 |

| | |
|---|---|
| Status | New |

Using <a class="foto" id="'+link_href_foto_id+'" href="" target="_blank"> at line 2369 of application/views/aplikasi_edit/edit_merchant_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant_new.php | application/views/aplikasi_edit/edit_merchant_new.php |
| Line | 2369 | 2369 |
| Object | <a class="foto" id="'+link_href_foto_id+'" href="" target="_blank"> | <a class="foto" id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_edit/edit_merchant_new.php
Method // tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a class="foto" id="'+link_href_foto_id+'" href="" target="_blank">Foto '+counter+'</a>';

```
....
2369.  //          tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a class="foto" id="'+link_href_foto_id+'" href="" target="_blank">Foto '+counter+'</a>';
```

**Unsafe Use Of Target blank\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22491 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 2385 of application/views/aplikasi_edit/edit_merchant_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant_new.php | application/views/aplikasi_edit/edit_merchant_new.php |
| Line | 2385 | 2385 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank">  | <a id="'+link_href_foto_id+'" href="" target="_blank">  |

Code Snippet
File Name application/views/aplikasi_edit/edit_merchant_new.php
Method // dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';

```
....
2385.  //         dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';
```

**Unsafe Use Of Target blank\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22492 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 458 of application/views/aplikasi_edit/edit_outlet.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_outlet.php | application/views/aplikasi_edit/edit_outlet.php |
| Line | 458 | 458 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_edit/edit_outlet.php

Method tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank">Foto '+counter+'</a>';

```
....
458.        tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank">Foto '+counter+'</a>';
```

**Unsafe Use Of Target blank\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22493 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank">> at line 217 of application/views/aplikasi_merchant/analisa_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/analisa_view.php | application/views/aplikasi_merchant/analisa_view.php |
| Line | 217 | 217 |
| Object | <a id="'+link_href_foto_id+'" href="" | <a id="'+link_href_foto_id+'" href="" |

| | | |
|---|---|---|
| | target="_blank"> | target="_blank"> |

Code Snippet
File Name application/views/aplikasi_merchant/analisa_view.php
Method // dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';

```
....
217.  //    dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';
```

**Unsafe Use Of Target blank\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22494 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 796 of application/views/aplikasi_merchant/analisa_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/analisa_view_new.php | application/views/aplikasi_merchant/analisa_view_new.php |
| Line | 796 | 796 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank">> | <a id="'+link_href_foto_id+'" href="" target="_blank">> |

Code Snippet
File Name application/views/aplikasi_merchant/analisa_view_new.php
Method dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';

```
....
796.        dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';
```

**Unsafe Use Of Target blank\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22495 |
| Status | New |

Using <a class="dokumen" href="'.base_url($img['link']).'" target="_blank" id="'.base_url($img['link']).'"> at line 118 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 118 | 118 |
| Object | <a class="dokumen" href="'.base_url($img['link']).'" target="_blank" id="'.base_url($img['link']).'"> | <a class="dokumen" href="'.base_url($img['link']).'" target="_blank" id="'.base_url($img['link']).'"> |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <td><?='<a class="dokumen" href="'.base_url($img['link']).'" target="_blank" id="'.base_url($img['link']).'">Foto '.$count_foto.'</a>';?>

```
....
118.                    <td><?='<a class="dokumen"
href="'.base_url($img['link']).'" target="_blank"
id="'.base_url($img['link']).'">Foto '.$count_foto.'</a>';?>
```

**Unsafe Use Of Target blank\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22496 |
| Status | New |

Using <a href="'.base_url($dok['ktp_link']).'" class="dokumen" target="_blank"> at line 236 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 236 | 236 |
| Object | <a href="'.base_url($dok['ktp_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['ktp_link']).'" class="dokumen" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <td><?=$dok['ktp_link']=='' ? '-' : '<a href="'.base_url($dok['ktp_link']).'" class="dokumen" target="_blank">KTP</a>';?></td>

```
....
236.                    <td><?=$dok['ktp_link']=='' ? '-' : '<a
href="'.base_url($dok['ktp_link']).'" class="dokumen"
target="_blank">KTP</a>';?></td>
```

**Unsafe Use Of Target blank\Path 27:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22497 |
| Status | New |

Using <a href="'.base_url($dok['npwp_link']).'" class="dokumen" target="_blank"> at line 244 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 244 | 244 |
| Object | <a href="'.base_url($dok['npwp_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['npwp_link']).'" class="dokumen" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php

Method <td><?=$dok['npwp_link']=='' ? '-' : '<a href="'.base_url($dok['npwp_link']).'" class="dokumen" target="_blank">NPWP</a>';?></td>

```
....
244.                    <td><?=$dok['npwp_link']=='' ? '-' : '<a
href="'.base_url($dok['npwp_link']).'" class="dokumen"
target="_blank">NPWP</a>';?></td>
```

**Unsafe Use Of Target blank\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22498 |
| Status | New |

Using <a href="'.base_url($dok['tdp_link']).'" class="dokumen" target="_blank">> at line 252 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 252 | 252 |
| Object | <a href="'.base_url($dok['tdp_link']).'" class="dokumen" target="_blank">> | <a href="'.base_url($dok['tdp_link']).'" class="dokumen" target="_blank">> |

Code Snippet

File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php

| | |
|---|---|
| Method | <td><?=$dok['tdp_link']=='' ? '-' : '<a href="'.base_url($dok['tdp_link']).'" class="dokumen" target="_blank">TDP</a>';?></td> |

```
....
252.                    <td><?=$dok['tdp_link']=='' ? '-' : '<a
href="'.base_url($dok['tdp_link']).'" class="dokumen"
target="_blank">TDP</a>';?></td>
```

**Unsafe Use Of Target blank\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22499 |
| Status | New |

Using <a href="'.base_url($dok['siup_link']).'" class="dokumen" target="_blank"> at line 260 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 260 | 260 |
| Object | <a href="'.base_url($dok['siup_link']).'" class="dokumen" target="_blank">> | <a href="'.base_url($dok['siup_link']).'" class="dokumen" target="_blank">> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Method | <td><?=$dok['siup_link']=='' ? '-' : '<a href="'.base_url($dok['siup_link']).'" class="dokumen" target="_blank">SIUP</a>';?></td> |

```
....
260.                    <td><?=$dok['siup_link']=='' ? '-' : '<a
href="'.base_url($dok['siup_link']).'" class="dokumen"
target="_blank">SIUP</a>';?></td>
```

**Unsafe Use Of Target blank\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22500 |
| Status | New |

Using <a href="'.base_url($dok['situ_link']).'" class="dokumen" target="_blank">> at line 268 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/pop | application/views/aplikasi_merchant/pop |

| | | |
|---|---|---|
| | up_detail_app_merchant.php | up_detail_app_merchant.php |
| Line | 268 | 268 |
| Object | <a href="'.base_url($dok['situ_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['situ_link']).'" class="dokumen" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <td><?=$dok['situ_link']=='' ? '-' : '<a href="'.base_url($dok['situ_link']).'" class="dokumen" target="_blank">SITU</a>';?></td>

```
....
268.                    <td><?=$dok['situ_link']=='' ? '-' : '<a
href="'.base_url($dok['situ_link']).'" class="dokumen"
target="_blank">SITU</a>';?></td>
```

**Unsafe Use Of Target blank\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22501 |
| Status | New |

Using <a href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen" target="_blank"> at line 276 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 276 | 276 |
| Object | <a href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <td><?=$dok['surat_kuasa_link']=='' ? '-' : '<a href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen" target="_blank">Surat Kuasa</a>';?></td>

```
....
276.                    <td><?=$dok['surat_kuasa_link']=='' ? '-' : '<a
href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen"
target="_blank">Surat Kuasa</a>';?></td>
```

**Unsafe Use Of Target blank\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=22502 |
| Status | New |

Using <a href="'.base_url($dok['akta_jbs_link']).'" class="dokumen" target="_blank"> at line 284 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 284 | 284 |
| Object | <a href="'.base_url($dok['akta_jbs_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['akta_jbs_link']).'" class="dokumen" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Method | <td><?=$dok['akta_jbs_link']=='' ? '-' : '<a href="'.base_url($dok['akta_jbs_link']).'" class="dokumen" target="_blank">Akta Jual Beli / Sewa</a>';?></td> |

```
....
284.                    <td><?=$dok['akta_jbs_link']=='' ? '-' : '<a
href="'.base_url($dok['akta_jbs_link']).'" class="dokumen"
target="_blank">Akta Jual Beli / Sewa</a>';?></td>
```

**Unsafe Use Of Target blank\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22503 |
| Status | New |

Using <a href="'.base_url($dok['lainnya_link']).'" class="dokumen" target="_blank"> at line 292 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 292 | 292 |
| Object | <a href="'.base_url($dok['lainnya_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['lainnya_link']).'" class="dokumen" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_merchant/popup_detail_app_merchant.php |

| | |
|---|---|
| Method | <td><?=$dok['lainnya_link']=='' ? '-' : '<a href="'.base_url($dok['lainnya_link']).'" class="dokumen" target="_blank">Lainnya</a>';?></td> |

```
....
292.                    <td><?=$dok['lainnya_link']=='' ? '-' : '<a
href="'.base_url($dok['lainnya_link']).'" class="dokumen"
target="_blank">Lainnya</a>';?></td>
```

**Unsafe Use Of Target blank\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22504 |
| Status | New |

Using <a href="'.base_url($dok['business_model_link']).'" target="_blank"> at line 318 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 318 | 318 |
| Object | <a href="'.base_url($dok['business_model_link']).'" target="_blank"> | <a href="'.base_url($dok['business_model_link']).'" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Method | <td><?=$dok['business_model_link']=='' ? '-' : '<a href="'.base_url($dok['business_model_link']).'" target="_blank">Business Model (download)</a>';?></td> |

```
....
318.                    <td><?=$dok['business_model_link']=='' ? '-' :
'<a href="'.base_url($dok['business_model_link']).'"
target="_blank">Business Model (download)</a>';?></td>
```

**Unsafe Use Of Target blank\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22505 |
| Status | New |

Using <a href="'.base_url($dok['lkm_link']).'" class="dokumen" target="_blank">> at line 324 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 324 | 324 |
| Object | <a href="'.base_url($dok['lkm_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['lkm_link']).'" class="dokumen" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php

Method <td><?php echo $dok['lkm_link']=='' ? '-' : '<a href="'.base_url($dok['lkm_link']).'" class="dokumen" target="_blank">LKM</a>';?></td>

```
....
324.                    <td><?php echo $dok['lkm_link']=='' ? '-' : '<a
href="'.base_url($dok['lkm_link']).'" class="dokumen"
target="_blank">LKM</a>';?></td>
```

**Unsafe Use Of Target blank\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22506 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 154 of application/views/aplikasi_outlet/edit_outlet_form_batch.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/edit_outlet_form_batch.php | application/views/aplikasi_outlet/edit_outlet_form_batch.php |
| Line | 154 | 154 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank">  | <a id="'+link_href_foto_id+'" href="" target="_blank">  |

Code Snippet

File Name application/views/aplikasi_outlet/edit_outlet_form_batch.php

Method tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>';

```
....
154.        tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0"
width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 37:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22507 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> at line 304 of application/views/aplikasi_outlet/input_outlet_form.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/input_outlet_form.php | application/views/aplikasi_outlet/input_outlet_form.php |
| Line | 304 | 304 |
| Object | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_outlet/input_outlet_form.php

Method tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">'+arr_data['photo_name']+'</a>';

```
....
304.                                tr_foto_append += '<td><canvas
id="'+canvas_id+'" height="0" width="0"
style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="'+arr_data['lihat_path']+'"
target="_blank">'+arr_data['photo_name']+'</a>';
```

**Unsafe Use Of Target blank\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22508 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 518 of application/views/aplikasi_outlet/input_outlet_form.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/input_outlet_form.php | application/views/aplikasi_outlet/input_outlet_form.php |
| Line | 518 | 518 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_outlet/input_outlet_form.php

| | |
|---|---|
| Method | // tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>'; |

```
....
518.  //    tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0"
width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22509 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 373 of application/views/aplikasi_outlet/input_outlet_form_bck07112017.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/input_outlet_form_bck07112017.php | application/views/aplikasi_outlet/input_outlet_form_bck07112017.php |
| Line | 373 | 373 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_outlet/input_outlet_form_bck07112017.php |
| Method | tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>'; |

```
....
373.        tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0"
width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22510 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> at line 337 of application/views/aplikasi_outlet/ver_outlet.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | application/views/aplikasi_outlet/ver_outlet.php | application/views/aplikasi_outlet/ver_outlet.php |
| Line | 337 | 337 |
| Object | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_outlet/ver_outlet.php

Method tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">'+arr_data['photo_name']+'</a>';

```
....
337.                                tr_foto_append += '<td><canvas
id="'+canvas_id+'" height="0" width="0"
style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="'+arr_data['lihat_path']+'"
target="_blank">'+arr_data['photo_name']+'</a>';
```

**Unsafe Use Of Target blank\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22511 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 572 of application/views/aplikasi_outlet/ver_outlet.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/ver_outlet.php | application/views/aplikasi_outlet/ver_outlet.php |
| Line | 572 | 572 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_outlet/ver_outlet.php

Method // tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>';

```
....
572.  //    tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0"
width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22512 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> at line 1235 of application/views/aplikasi_tambah_merchant/form_tambah_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1235 | 1235 |
| Object | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">'+arr_data['photo_name']+'</a>';

```
....
1235.                                tr_foto_append += '<td><canvas
id="'+canvas_id+'" height="0" width="0"
style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="'+arr_data['lihat_path']+'"
target="_blank">'+arr_data['photo_name']+'</a>';
```

**Unsafe Use Of Target blank\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22513 |
| Status | New |

Using <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> at line 1487 of application/views/aplikasi_tambah_merchant/form_tambah_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |

| | | |
|---|---|---|
| Line | 1487 | 1487 |
| Object | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> |

Code Snippet

File Name application/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method tr_dupl += '<td><a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] + '</a></td>';

```
....
1487.                                                    tr_dupl +=
'<td><a target="_blank"
href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail'
);?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+
dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] +
'</a></td>';
```

**Unsafe Use Of Target blank\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22514 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 2712 of application/views/aplikasi_tambah_merchant/form_tambah_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 2712 | 2712 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method // tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>';

```
....
2712.  //          tr_foto_append += '<td><canvas id="'+canvas_id+'"
height="0" width="0" style="display:none;"></canvas><a
id="'+link_href_foto_id+'" href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22515 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 2729 of application/views/aplikasi_tambah_merchant/form_tambah_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 2729 | 2729 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method // dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';

```
....
2729.  //          dok_append += '<a id="'+link_href_foto_id+'" href="" 
target="_blank">'+dok_name+'</a>  ';
```

**Unsafe Use Of Target blank\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22516 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> at line 1127 of application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |

| | | |
|---|---|---|
| Line | 1127 | 1127 |
| Object | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Method | tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">'+arr_data['photo_name']+'</a>'; |

```
....
1127.                                tr_foto_append += '<td><canvas
id="'+canvas_id+'" height="0" width="0"
style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="'+arr_data['lihat_path']+'"
target="_blank">'+arr_data['photo_name']+'</a>';
```

**Unsafe Use Of Target blank\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22517 |
| Status | New |

Using <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> at line 1379 of application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Line | 1379 | 1379 |
| Object | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |

| | |
|---|---|
| Method | tr_dupl += '<td><a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] + '</a></td>'; |

```
....
1379.                                                    tr_dupl +=
'<td><a target="_blank"
href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail'
);?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+
dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] +
'</a></td>';
```

**Unsafe Use Of Target blank\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22518 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 2502 of application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Line | 2502 | 2502 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Method | //  tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>'; |

```
....
2502.  //         tr_foto_append += '<td><canvas id="'+canvas_id+'"
height="0" width="0" style="display:none;"></canvas><a
id="'+link_href_foto_id+'" href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22519 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 2519 of application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Line | 2519 | 2519 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php
Method // dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';

```
....
2519.  //          dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';
```

**Unsafe Use Of Target blank\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22520 |
| Status | New |

Using <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> at line 184 of application/views/aplikasi_tambah_merchant/input_form_2.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/input_form_2.php | application/views/aplikasi_tambah_merchant/input_form_2.php |
| Line | 184 | 184 |
| Object | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> |

Code Snippet
File Name application/views/aplikasi_tambah_merchant/input_form_2.php

| | |
|---|---|
| Method | tr_dupl += '<td><a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] + '</a></td>'; |

```
....
184.
      tr_dupl += '<td><a target="_blank"
href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail'
);?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+
dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] +
'</a></td>';
```

## Unsafe Use Of Target blank

Query Path:
Typescript\Cx\Typescript Low Visibility\Unsafe Use Of Target blank Version:1

*Description*

**Unsafe Use Of Target blank\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22922 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank"> at line 587 of application/controllers/aplikasi_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 587 | 587 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/aplikasi_merchant.php |
| Method | $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  '; |

```
....
587.                          $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22923 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank"> at line 1222 of application/controllers/aplikasi_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_merchant.php | application/controllers/aplikasi_merchant.php |
| Line | 1222 | 1222 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

Code Snippet
File Name application/controllers/aplikasi_merchant.php
Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';

```
....
1222.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22924 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank"> at line 119 of application/controllers/aplikasi_tambah_merchant/analisa.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/analisa.php | application/controllers/aplikasi_tambah_merchant/analisa.php |
| Line | 119 | 119 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

Code Snippet
File Name application/controllers/aplikasi_tambah_merchant/analisa.php
Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';

```
....
119.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22925 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank"> at line 663 of application/controllers/aplikasi_tambah_merchant/input_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant.php | application/controllers/aplikasi_tambah_merchant/input_merchant.php |
| Line | 663 | 663 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

Code Snippet

File Name application/controllers/aplikasi_tambah_merchant/input_merchant.php

Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';

```
....
663.                    $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22926 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank"> at line 646 of application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php | application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php |
| Line | 646 | 646 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

Code Snippet

File Name application/controllers/aplikasi_tambah_merchant/input_merchant_20210615.php

| | |
|---|---|
| Method | $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  '; |

```
....
646.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22927 |
| Status | New |

Using <a href="'.$filename.'" target="_blank"> at line 77 of application/controllers/inisiasi_checker.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_checker.php | application/controllers/inisiasi_checker.php |
| Line | 77 | 77 |
| Object | <a href="'.$filename.'" target="_blank">> | <a href="'.$filename.'" target="_blank">> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/inisiasi_checker.php |
| Method | $data_insert['cl_mid_log'] .= 'See the report from Cardlink <a href="'.$filename.'" target="_blank">here</a>'; |

```
....
77.                                 $data_insert['cl_mid_log'] .= 'See
the report from Cardlink <a href="'.$filename.'"
target="_blank">here</a>';
```

**Unsafe Use Of Target blank\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22928 |
| Status | New |

Using <a href="'.$filename.'" target="_blank">> at line 118 of application/controllers/inisiasi_checker.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_checker.php | application/controllers/inisiasi_checker.php |
| Line | 118 | 118 |

| | | |
|---|---|---|
| Object | <a href="'.$filename.'" target="_blank"> | <a href="'.$filename.'" target="_blank">> |

Code Snippet
File Name application/controllers/inisiasi_checker.php
Method $data_insert['cl_tid_log'] .= 'See the report from Cardlink <a href="'.$filename.'" target="_blank">here</a><br>';

```
....
118.                                $data_insert['cl_tid_log'] .= 'See
the report from Cardlink <a href="'.$filename.'"
target="_blank">here</a><br>';
```

**Unsafe Use Of Target blank\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22929 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank">> at line 952 of application/controllers/pameran.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/pameran.php | application/controllers/pameran.php |
| Line | 952 | 952 |
| Object | <a href="' . $lihat_path . '" target="_blank">> | <a href="' . $lihat_path . '" target="_blank">> |

Code Snippet
File Name application/controllers/pameran.php
Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $_FILES['foto']['name'] . '</a>  ';

```
....
952.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $_FILES['foto']['name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22930 |
| Status | New |

Using <a href="' . $lihat_path . '" target="_blank">> at line 773 of application/controllers/qris.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/controllers/qris.php | application/controllers/qris.php |
| Line | 773 | 773 |
| Object | <a href="' . $lihat_path . '" target="_blank"> | <a href="' . $lihat_path . '" target="_blank"> |

Code Snippet
File Name application/controllers/qris.php
Method $label = '<a href="' . $lihat_path . '" target="_blank">' . $config['file_name'] . '</a>  ';

```
....
773.                    $label = '<a href="' . $lihat_path . '"
target="_blank">' . $config['file_name'] . '</a>  ';
```

**Unsafe Use Of Target blank\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22931 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> at line 111 of application/views/admin/v_admin_paket_bismod.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_admin_paket_bismod.php | application/views/admin/v_admin_paket_bismod.php |
| Line | 111 | 111 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> |

Code Snippet
File Name application/views/admin/v_admin_paket_bismod.php
Method <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank">Download Form MCC JCB High Risk </a>   

```
....
111.                <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>"
target="_blank">Download Form MCC JCB High Risk </a>   
```

**Unsafe Use Of Target blank\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22932 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> at line 162 of application/views/admin/v_admin_paket_bismod.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_admin_paket_bismod.php | application/views/admin/v_admin_paket_bismod.php |
| Line | 162 | 162 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> |

Code Snippet

File Name application/views/admin/v_admin_paket_bismod.php

Method <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank">Download Form MCC JCB High Risk </a>   

```
....
162.                <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>"
target="_blank">Download Form MCC JCB High Risk </a>   
```

**Unsafe Use Of Target blank\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22933 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> at line 145 of application/views/admin/v_manage_mcc_jcb.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_mcc_jcb.php | application/views/admin/v_manage_mcc_jcb.php |
| Line | 145 | 145 |

| | | |
|---|---|---|
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank"> |

Code Snippet
File Name application/views/admin/v_manage_mcc_jcb.php
Method <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>" target="_blank">Download Form MCC JCB High Risk </a>   

```
....
145.              <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_mcc_jcb_high_risk'?>"
target="_blank">Download Form MCC JCB High Risk </a>   
```

**Unsafe Use Of Target blank\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22934 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_master_high_risk'?>" target="_blank"> at line 145 of application/views/admin/v_manage_mcc_master.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_mcc_master.php | application/views/admin/v_manage_mcc_master.php |
| Line | 145 | 145 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_master_high_risk'?>" target="_blank">> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_master_high_risk'?>" target="_blank">> |

Code Snippet
File Name application/views/admin/v_manage_mcc_master.php
Method <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_master_high_risk'?>" target="_blank">Download Form MCC Master High Risk </a>   

```
....
145.                <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_mcc_master_high_risk'?>"
target="_blank">Download Form MCC Master High Risk
</a>   
```

**Unsafe Use Of Target blank\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22935 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank"> at line 152 of application/views/admin/v_manage_mcc_npg.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_mcc_npg.php | application/views/admin/v_manage_mcc_npg.php |
| Line | 152 | 152 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank"> |

Code Snippet

File Name application/views/admin/v_manage_mcc_npg.php

Method <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank">Download Form MCC NPG & Unik High Risk </a> 

```
....
152.                    <a id="download" style="color:#FFF;text-
decoration: none" class="button"
href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>"
target="_blank">Download Form MCC NPG & Unik High Risk </a> 
```

**Unsafe Use Of Target blank\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22936 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank"> at line 173 of

application/views/admin/v_manage_mcc_npg.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_mcc_npg.php | application/views/admin/v_manage_mcc_npg.php |
| Line | 173 | 173 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank"> |

Code Snippet
File Name application/views/admin/v_manage_mcc_npg.php
Method <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>" target="_blank">Download Form MCC NPG & Unik High Risk </a> 

```
....
173.                    <a id="download" style="color:#FFF;text-
decoration: none" class="button"
href="<?=site_url().'/admin/download_form_mcc_npg_high_risk'?>"
target="_blank">Download Form MCC NPG & Unik High Risk </a> 
```

**Unsafe Use Of Target blank\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22937 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_visa_high_risk'?>" target="_blank"> at line 145 of application/views/admin/v_manage_mcc_visa.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_mcc_visa.php | application/views/admin/v_manage_mcc_visa.php |
| Line | 145 | 145 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_visa_high_risk'?>" target="_blank">  | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_visa_high_risk'?>" target="_blank">  |

Code Snippet
File Name application/views/admin/v_manage_mcc_visa.php

| | |
|---|---|
| Method | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_mcc_visa_high_risk'?>" target="_blank">Download Form MCC Visa High Risk </a>    |

```
....
145.              <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_mcc_visa_high_risk'?>"
target="_blank">Download Form MCC Visa High Risk </a>   
```

**Unsafe Use Of Target blank\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22938 |
| Status | New |

Using <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_blacklist'?>" target="_blank"> at line 159 of application/views/admin/v_manage_merchant_blacklist.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_merchant_blacklist.php | application/views/admin/v_manage_merchant_blacklist.php |
| Line | 159 | 159 |
| Object | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_blacklist'?>" target="_blank"> | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_blacklist'?>" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/admin/v_manage_merchant_blacklist.php |
| Method | <a id="download" style="color:#FFF;text-decoration: none" class="button" href="<?=site_url().'/admin/download_form_blacklist'?>" target="_blank">Download Form Pengisian </a>    |

```
....
159.              <a id="download" style="color:#FFF;text-decoration:
none" class="button"
href="<?=site_url().'/admin/download_form_blacklist'?>"
target="_blank">Download Form Pengisian </a>   
```

**Unsafe Use Of Target blank\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22939 |
| Status | New |

Using <a href="<?=site_url('admin/manage_target_marketing_form_download');?>" target="_blank" id="download_target"> at line 47 of application/views/admin/v_manage_target_marketing_form.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/admin/v_manage_target_marketing_form.php | application/views/admin/v_manage_target_marketing_form.php |
| Line | 47 | 47 |
| Object | <a href="<?=site_url('admin/manage_target_marketing_form_download');?>" target="_blank" id="download_target"> | <a href="<?=site_url('admin/manage_target_marketing_form_download');?>" target="_blank" id="download_target"> |

Code Snippet

File Name application/views/admin/v_manage_target_marketing_form.php

Method <td><a href="<?=site_url('admin/manage_target_marketing_form_download');?>" target="_blank" id="download_target">Download</a></td>

```
....
47.         <td><a
href="<?=site_url('admin/manage_target_marketing_form_download');?>"
target="_blank" id="download_target">Download</a></td>
```

**Unsafe Use Of Target blank\Path 19:**

Severity Low

Result State To Verify

Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22940

Status New

Using <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> at line 1056 of application/views/aplikasi_edit/edit_merchant_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant_new.php | application/views/aplikasi_edit/edit_merchant_new.php |
| Line | 1056 | 1056 |
| Object | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_edit/edit_merchant_new.php

Method tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">'+arr_data['photo_name']+'</a>';

```
....
1056.                                    tr_foto_append += '<td><canvas
id="'+canvas_id+'" height="0" width="0"
style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="'+arr_data['lihat_path']+'"
target="_blank">'+arr_data['photo_name']+'</a>';
```

**Unsafe Use Of Target blank\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22941 |
| Status | New |

Using <a class="foto" id="'+link_href_foto_id+'" href="" target="_blank"> at line 2369 of application/views/aplikasi_edit/edit_merchant_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant_new.php | application/views/aplikasi_edit/edit_merchant_new.php |
| Line | 2369 | 2369 |
| Object | <a class="foto" id="'+link_href_foto_id+'" href="" target="_blank"> | <a class="foto" id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_edit/edit_merchant_new.php

Method // tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a class="foto" id="'+link_href_foto_id+'" href="" target="_blank">Foto '+counter+'</a>';

```
....
2369.  //         tr_foto_append += '<td><canvas id="'+canvas_id+'"
height="0" width="0" style="display:none;"></canvas><a class="foto"
id="'+link_href_foto_id+'" href="" target="_blank">Foto
'+counter+'</a>';
```

**Unsafe Use Of Target blank\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22942 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 2385 of application/views/aplikasi_edit/edit_merchant_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant_new.php | application/views/aplikasi_edit/edit_merchant_new.php |
| Line | 2385 | 2385 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_edit/edit_merchant_new.php
Method // dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';

```
....
2385.  //          dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';
```

**Unsafe Use Of Target blank\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22943 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 458 of application/views/aplikasi_edit/edit_outlet.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_outlet.php | application/views/aplikasi_edit/edit_outlet.php |
| Line | 458 | 458 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_edit/edit_outlet.php
Method tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank">Foto '+counter+'</a>';

```
....
458.        tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank">Foto '+counter+'</a>';
```

**Unsafe Use Of Target blank\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22944 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 217 of application/views/aplikasi_merchant/analisa_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/analisa_view.php | application/views/aplikasi_merchant/analisa_view.php |
| Line | 217 | 217 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_merchant/analisa_view.php
Method // dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';

```
....
217.  //    dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';
```

**Unsafe Use Of Target blank\Path 24:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22945
Status New

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 796 of application/views/aplikasi_merchant/analisa_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/analisa_view_new.php | application/views/aplikasi_merchant/analisa_view_new.php |
| Line | 796 | 796 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_merchant/analisa_view_new.php
Method dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';

```
....
796.        dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';
```

**Unsafe Use Of Target blank\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22946 |
| Status | New |

Using <a class="dokumen" href="'.base_url($img['link']).'" target="_blank" id="'.base_url($img['link']).'"> at line 118 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 118 | 118 |
| Object | <a class="dokumen" href="'.base_url($img['link']).'" target="_blank" id="'.base_url($img['link']).'"> | <a class="dokumen" href="'.base_url($img['link']).'" target="_blank" id="'.base_url($img['link']).'"> |

Code Snippet

File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php

Method <td><?='<a class="dokumen" href="'.base_url($img['link']).'" target="_blank" id="'.base_url($img['link']).'">Foto '.$count_foto.'</a>';?>

```
....
118.                    <td><?='<a class="dokumen"
href="'.base_url($img['link']).'" target="_blank"
id="'.base_url($img['link']).'">Foto '.$count_foto.'</a>';?>
```

**Unsafe Use Of Target blank\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22947 |
| Status | New |

Using <a href="'.base_url($dok['ktp_link']).'" class="dokumen" target="_blank"> at line 236 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 236 | 236 |
| Object | <a href="'.base_url($dok['ktp_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['ktp_link']).'" class="dokumen" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Method | <td><?=$dok['ktp_link']=='' ? '-' : '<a href="'.base_url($dok['ktp_link']).'" class="dokumen" target="_blank">KTP</a>';?></td> |

```
....
236.                    <td><?=$dok['ktp_link']=='' ? '-' : '<a
href="'.base_url($dok['ktp_link']).'" class="dokumen"
target="_blank">KTP</a>';?></td>
```

**Unsafe Use Of Target blank\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22948 |
| Status | New |

Using <a href="'.base_url($dok['npwp_link']).'" class="dokumen" target="_blank"> at line 244 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 244 | 244 |
| Object | <a href="'.base_url($dok['npwp_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['npwp_link']).'" class="dokumen" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Method | <td><?=$dok['npwp_link']=='' ? '-' : '<a href="'.base_url($dok['npwp_link']).'" class="dokumen" target="_blank">NPWP</a>';?></td> |

```
....
244.                    <td><?=$dok['npwp_link']=='' ? '-' : '<a
href="'.base_url($dok['npwp_link']).'" class="dokumen"
target="_blank">NPWP</a>';?></td>
```

**Unsafe Use Of Target blank\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22949 |
| Status | New |

Using <a href="'.base_url($dok['tdp_link']).'" class="dokumen" target="_blank"> at line 252 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 252 | 252 |
| Object | <a href="'.base_url($dok['tdp_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['tdp_link']).'" class="dokumen" target="_blank">> |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <td><?=$dok['tdp_link']=='' ? '-' : '<a href="'.base_url($dok['tdp_link']).'" class="dokumen" target="_blank">TDP</a>';?></td>

```
....
252.                    <td><?=$dok['tdp_link']=='' ? '-' : '<a
href="'.base_url($dok['tdp_link']).'" class="dokumen"
target="_blank">TDP</a>';?></td>
```

**Unsafe Use Of Target blank\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22950 |
| Status | New |

Using <a href="'.base_url($dok['siup_link']).'" class="dokumen" target="_blank"> at line 260 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 260 | 260 |
| Object | <a href="'.base_url($dok['siup_link']).'" class="dokumen" target="_blank">> | <a href="'.base_url($dok['siup_link']).'" class="dokumen" target="_blank">> |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <td><?=$dok['siup_link']=='' ? '-' : '<a href="'.base_url($dok['siup_link']).'" class="dokumen" target="_blank">SIUP</a>';?></td>

```
....
260.                    <td><?=$dok['siup_link']=='' ? '-' : '<a
href="'.base_url($dok['siup_link']).'" class="dokumen"
target="_blank">SIUP</a>';?></td>
```

**Unsafe Use Of Target blank\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=22951 |
| Status | New |

Using <a href="'.base_url($dok['situ_link']).'" class="dokumen" target="_blank"> at line 268 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 268 | 268 |
| Object | <a href="'.base_url($dok['situ_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['situ_link']).'" class="dokumen" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php

Method <td><?=$dok['situ_link']=='' ? '-' : '<a href="'.base_url($dok['situ_link']).'" class="dokumen" target="_blank">SITU</a>';?></td>

```
....
268.                    <td><?=$dok['situ_link']=='' ? '-' : '<a
href="'.base_url($dok['situ_link']).'" class="dokumen"
target="_blank">SITU</a>';?></td>
```

**Unsafe Use Of Target blank\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22952 |
| Status | New |

Using <a href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen" target="_blank"> at line 276 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 276 | 276 |
| Object | <a href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php

Method <td><?=$dok['surat_kuasa_link']=='' ? '-' : '<a href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen" target="_blank">Surat Kuasa</a>';?></td>

```
....
276.                    <td><?=$dok['surat_kuasa_link']=='' ? '-' : '<a
href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen"
target="_blank">Surat Kuasa</a>';?></td>
```

**Unsafe Use Of Target blank\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22953 |
| Status | New |

Using <a href="'.base_url($dok['akta_jbs_link']).'" class="dokumen" target="_blank"> at line 284 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 284 | 284 |
| Object | <a href="'.base_url($dok['akta_jbs_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['akta_jbs_link']).'" class="dokumen" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php

Method <td><?=$dok['akta_jbs_link']=='' ? '-' : '<a href="'.base_url($dok['akta_jbs_link']).'" class="dokumen" target="_blank">Akta Jual Beli / Sewa</a>';?></td>

```
....
284.                    <td><?=$dok['akta_jbs_link']=='' ? '-' : '<a
href="'.base_url($dok['akta_jbs_link']).'" class="dokumen"
target="_blank">Akta Jual Beli / Sewa</a>';?></td>
```

**Unsafe Use Of Target blank\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22954 |
| Status | New |

Using <a href="'.base_url($dok['lainnya_link']).'" class="dokumen" target="_blank"> at line 292 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/pop | application/views/aplikasi_merchant/pop |

| | | |
|---|---|---|
| | up_detail_app_merchant.php | up_detail_app_merchant.php |
| Line | 292 | 292 |
| Object | <a href="'.base_url($dok['lainnya_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['lainnya_link']).'" class="dokumen" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <td><?=$dok['lainnya_link']=='' ? '-' : '<a href="'.base_url($dok['lainnya_link']).'" class="dokumen" target="_blank">Lainnya</a>';?></td>

```
....
292.                    <td><?=$dok['lainnya_link']=='' ? '-' : '<a
href="'.base_url($dok['lainnya_link']).'" class="dokumen"
target="_blank">Lainnya</a>';?></td>
```

**Unsafe Use Of Target blank\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22955 |
| Status | New |

Using <a href="'.base_url($dok['business_model_link']).'" target="_blank"> at line 318 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 318 | 318 |
| Object | <a href="'.base_url($dok['business_model_link']).'" target="_blank">> | <a href="'.base_url($dok['business_model_link']).'" target="_blank">> |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <td><?=$dok['business_model_link']=='' ? '-' : '<a href="'.base_url($dok['business_model_link']).'" target="_blank">Business Model (download)</a>';?></td>

```
....
318.                    <td><?=$dok['business_model_link']=='' ? '-' :
'<a href="'.base_url($dok['business_model_link']).'"
target="_blank">Business Model (download)</a>';?></td>
```

**Unsafe Use Of Target blank\Path 35:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22956 |
| Status | New |

Using <a href="'.base_url($dok['lkm_link']).'" class="dokumen" target="_blank"> at line 324 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 324 | 324 |
| Object | <a href="'.base_url($dok['lkm_link']).'" class="dokumen" target="_blank"> | <a href="'.base_url($dok['lkm_link']).'" class="dokumen" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Method | <td><?php echo $dok['lkm_link']=='' ? '-' : '<a href="'.base_url($dok['lkm_link']).'" class="dokumen" target="_blank">LKM</a>';?></td> |

```
....
324.                    <td><?php echo $dok['lkm_link']=='' ? '-' : '<a
href="'.base_url($dok['lkm_link']).'" class="dokumen"
target="_blank">LKM</a>';?></td>
```

**Unsafe Use Of Target blank\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22957 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 154 of application/views/aplikasi_outlet/edit_outlet_form_batch.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/edit_outlet_form_batch.php | application/views/aplikasi_outlet/edit_outlet_form_batch.php |
| Line | 154 | 154 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank">> | <a id="'+link_href_foto_id+'" href="" target="_blank">> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_outlet/edit_outlet_form_batch.php |

| | |
|---|---|
| Method | tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>'; |

```
....
154.        tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0"
width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22958 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> at line 304 of application/views/aplikasi_outlet/input_outlet_form.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/input_outlet_form.php | application/views/aplikasi_outlet/input_outlet_form.php |
| Line | 304 | 304 |
| Object | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_outlet/input_outlet_form.php |
| Method | tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">'+arr_data['photo_name']+'</a>'; |

```
....
304.                                tr_foto_append += '<td><canvas
id="'+canvas_id+'" height="0" width="0"
style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="'+arr_data['lihat_path']+'"
target="_blank">'+arr_data['photo_name']+'</a>';
```

**Unsafe Use Of Target blank\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22959 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank">> at line 518 of application/views/aplikasi_outlet/input_outlet_form.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/input_outlet_form.php | application/views/aplikasi_outlet/input_outlet_form.php |
| Line | 518 | 518 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_outlet/input_outlet_form.php
Method // tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>';

```
....
518.  //    tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0"
width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22960 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 373 of application/views/aplikasi_outlet/input_outlet_form_bck07112017.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/input_outlet_form_bck07112017.php | application/views/aplikasi_outlet/input_outlet_form_bck07112017.php |
| Line | 373 | 373 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_outlet/input_outlet_form_bck07112017.php
Method tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>';

```
....
373.        tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0"
width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 40:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22961 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> at line 337 of application/views/aplikasi_outlet/ver_outlet.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/ver_outlet.php | application/views/aplikasi_outlet/ver_outlet.php |
| Line | 337 | 337 |
| Object | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> |

Code Snippet
File Name application/views/aplikasi_outlet/ver_outlet.php
Method tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">'+arr_data['photo_name']+'</a>';

```
....
337.                                tr_foto_append += '<td><canvas
id="'+canvas_id+'" height="0" width="0"
style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="'+arr_data['lihat_path']+'"
target="_blank">'+arr_data['photo_name']+'</a>';
```

**Unsafe Use Of Target blank\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22962 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 572 of application/views/aplikasi_outlet/ver_outlet.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_outlet/ver_outlet.php | application/views/aplikasi_outlet/ver_outlet.php |
| Line | 572 | 572 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank">  | <a id="'+link_href_foto_id+'" href="" target="_blank">  |

Code Snippet
File Name application/views/aplikasi_outlet/ver_outlet.php

| | |
|---|---|
| Method | // tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>'; |

```
....
572.  //    tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0"
width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22963 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> at line 1235 of application/views/aplikasi_tambah_merchant/form_tambah_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1235 | 1235 |
| Object | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">'+arr_data['photo_name']+'</a>'; |

```
....
1235.                                tr_foto_append += '<td><canvas
id="'+canvas_id+'" height="0" width="0"
style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="'+arr_data['lihat_path']+'"
target="_blank">'+arr_data['photo_name']+'</a>';
```

**Unsafe Use Of Target blank\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22964 |
| Status | New |

Using <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+

dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> at line 1487 of application/views/aplikasi_tambah_merchant/form_tambah_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 1487 | 1487 |
| Object | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> |

Code Snippet

File Name application/views/aplikasi_tambah_merchant/form_tambah_merchant.php

Method tr_dupl += '<td><a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] + '</a></td>';

```
....
1487.                                                    tr_dupl +=
'<td><a target="_blank"
href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail'
);?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+
dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] +
'</a></td>';
```

**Unsafe Use Of Target blank\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22965 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 2712 of application/views/aplikasi_tambah_merchant/form_tambah_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 2712 | 2712 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet

| | |
|---|---|
| File Name | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | // tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>'; |

```
....
2712.  //          tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22966 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 2729 of application/views/aplikasi_tambah_merchant/form_tambah_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Line | 2729 | 2729 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_tambah_merchant/form_tambah_merchant.php |
| Method | // dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  '; |

```
....
2729.  //          dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';
```

**Unsafe Use Of Target blank\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22967 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">> at line 1127 of application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Line | 1127 | 1127 |
| Object | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> | <a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php

Method tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="'+arr_data['lihat_path']+'" target="_blank">'+arr_data['photo_name']+'</a>';

```
....
1127.                                tr_foto_append += '<td><canvas
id="'+canvas_id+'" height="0" width="0"
style="display:none;"></canvas><a id="'+link_href_foto_id+'"
href="'+arr_data['lihat_path']+'"
target="_blank">'+arr_data['photo_name']+'</a>';
```

**Unsafe Use Of Target blank\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22968 |
| Status | New |

Using <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> at line 1379 of application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Line | 1379 | 1379 |
| Object | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> |

Code Snippet

| | |
|---|---|
| File Name | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Method | tr_dupl += '<td><a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] + '</a></td>'; |

```
....
1379.                                                    tr_dupl +=
'<td><a target="_blank"
href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail'
);?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+
dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] +
'</a></td>';
```

**Unsafe Use Of Target blank\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22969 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 2502 of application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Line | 2502 | 2502 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet

| | |
|---|---|
| File Name | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Method | // tr_foto_append += '<td><canvas id="'+canvas_id+'" height="0" width="0" style="display:none;"></canvas><a id="'+link_href_foto_id+'" href="" target="_blank"></a>'; |

```
....
2502.  //          tr_foto_append += '<td><canvas id="'+canvas_id+'"
height="0" width="0" style="display:none;"></canvas><a
id="'+link_href_foto_id+'" href="" target="_blank"></a>';
```

**Unsafe Use Of Target blank\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22970 |
| Status | New |

Using <a id="'+link_href_foto_id+'" href="" target="_blank"> at line 2519 of application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php | application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php |
| Line | 2519 | 2519 |
| Object | <a id="'+link_href_foto_id+'" href="" target="_blank"> | <a id="'+link_href_foto_id+'" href="" target="_blank"> |

Code Snippet

File Name application/views/aplikasi_tambah_merchant/form_tambah_merchant_20210615.php

Method // dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';

```
....
2519.  //          dok_append += '<a id="'+link_href_foto_id+'" href="" target="_blank">'+dok_name+'</a>  ';
```

**Unsafe Use Of Target blank\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22971 |
| Status | New |

Using <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> at line 184 of application/views/aplikasi_tambah_merchant/input_form_2.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_tambah_merchant/input_form_2.php | application/views/aplikasi_tambah_merchant/input_form_2.php |
| Line | 184 | 184 |
| Object | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> | <a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'"> |

Code Snippet

| | |
|---|---|
| File Name | application/views/aplikasi_tambah_merchant/input_form_2.php |
| Method | tr_dupl += '<td><a target="_blank" href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail');?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+ dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] + '</a></td>'; |

```
....
184.
      tr_dupl += '<td><a target="_blank"
href="<?=site_url('aplikasi_tambah_merchant/input_merchant/popup_detail'
);?>?mid='+ dupl_arr['mid'] +'&app_id='+ dupl_arr['app_id'] +'&tabel='+
dupl_arr['tabel'] +'">'+ dupl_arr['mid'] +' / '+ dupl_arr['app_id'] +
'</a></td>';
```

## Improper Exception Handling

Query Path:
PHP\Cx\Php Low Visibility\Improper Exception Handling Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.5 - Improper error handling
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2021: A4-Insecure Design

*Description*

**Improper Exception Handling\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13378 |
| Status | New |

Method db_set_charset at line 136 of system/database/drivers/mysql/mysql_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysql/mysql_driver.php | system/database/drivers/mysql/mysql_driver.php |
| Line | 146 | 146 |
| Object | mysql_query | mysql_query |

| | |
|---|---|
| Code Snippet | |
| File Name | system/database/drivers/mysql/mysql_driver.php |
| Method | function db_set_charset($charset, $collation) |

```
....
146.                    return @mysql_query("SET NAMES '".$this-
>escape_str($charset)."' COLLATE '".$this->escape_str($collation)."'",
$this->conn_id);
```

**Improper Exception Handling\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13379 |
| Status | New |

Method _execute at line 176 of system/database/drivers/mysql/mysql_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysql/mysql_driver.php | system/database/drivers/mysql/mysql_driver.php |
| Line | 179 | 179 |
| Object | mysql_query | mysql_query |

Code Snippet
File Name system/database/drivers/mysql/mysql_driver.php
Method function _execute($sql)

```
....
179.                return @mysql_query($sql, $this->conn_id);
```

**Improper Exception Handling\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13380 |
| Status | New |

Method _db_set_charset at line 136 of system/database/drivers/mysqli/mysqli_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysqli/mysqli_driver.php | system/database/drivers/mysqli/mysqli_driver.php |
| Line | 146 | 146 |
| Object | mysqli_query | mysqli_query |

Code Snippet
File Name system/database/drivers/mysqli/mysqli_driver.php
Method function _db_set_charset($charset, $collation)

```
....
146.                    return @mysqli_query($this->conn_id, "SET NAMES
'".$this->escape_str($charset)."' COLLATE '".$this-
>escape_str($collation)."'");
```

**Improper Exception Handling\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=13381 |
| Status | New |

Method _execute at line 176 of system/database/drivers/mysqli/mysqli_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysqli/mysqli_driver.php | system/database/drivers/mysqli/mysqli_driver.php |
| Line | 179 | 179 |
| Object | mysqli_query | mysqli_query |

Code Snippet
File Name system/database/drivers/mysqli/mysqli_driver.php
Method function _execute($sql)

```
....
179.            $result = @mysqli_query($this->conn_id, $sql);
```

**Improper Exception Handling\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13382 |
| Status | New |

Method _execute at line 140 of system/database/drivers/mssql/mssql_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mssql/mssql_driver.php | system/database/drivers/mssql/mssql_driver.php |
| Line | 143 | 143 |
| Object | mssql_query | mssql_query |

Code Snippet
File Name system/database/drivers/mssql/mssql_driver.php
Method function _execute($sql)

```
....
143.            return @mssql_query($sql, $this->conn_id);
```

**Improper Exception Handling\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13383 |
| Status | New |

Method _execute at line 150 of system/database/drivers/odbc/odbc_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/odbc/odbc_driver.php | system/database/drivers/odbc/odbc_driver.php |
| Line | 153 | 153 |
| Object | odbc_exec | odbc_exec |

Code Snippet
File Name system/database/drivers/odbc/odbc_driver.php
Method function _execute($sql)

```
....
153.            return @odbc_exec($this->conn_id, $sql);
```

**Improper Exception Handling\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13384 |
| Status | New |

Method _execute at line 165 of system/database/drivers/oci8/oci8_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_driver.php | system/database/drivers/oci8/oci8_driver.php |
| Line | 172 | 172 |
| Object | oci_execute | oci_execute |

Code Snippet
File Name system/database/drivers/oci8/oci8_driver.php
Method protected function _execute($sql)

```
....
172.            return @oci_execute($this->stmt_id, $this->_commit);
```

**Improper Exception Handling\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13385 |
| Status | New |

Method num_rows at line 43 of system/database/drivers/oci8/oci8_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/database/drivers/oci8/oci8_result.php |
| Line | 48 | 48 |
| Object | oci_execute | oci_execute |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method public function num_rows()

```
....
48.                 @oci_execute($this->stmt_id);
```

**Improper Exception Handling\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13386 |
| Status | New |

Method num_rows at line 43 of system/database/drivers/oci8/oci8_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/database/drivers/oci8/oci8_result.php |
| Line | 52 | 52 |
| Object | oci_execute | oci_execute |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method public function num_rows()

```
....
52.                     @oci_execute($this->curs_id);
```

**Improper Exception Handling\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13387 |
| Status | New |

Method __query at line 40 of application/third_party/dompdf/include/page_cache.cls.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/third_party/dompdf/include/page_cache.cls.php | application/third_party/dompdf/include/page_cache.cls.php |
| Line | 41 | 41 |
| Object | pg_query | pg_query |

Code Snippet
File Name application/third_party/dompdf/include/page_cache.cls.php
Method private static function __query($sql) {

```
....
41.      if ( !($res = pg_query(self::$__connection, $sql)) )
```

**Improper Exception Handling\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13388 |
| Status | New |

Method _execute at line 173 of system/database/drivers/postgre/postgre_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/postgre/postgre_driver.php | system/database/drivers/postgre/postgre_driver.php |
| Line | 176 | 176 |
| Object | pg_query | pg_query |

Code Snippet
File Name system/database/drivers/postgre/postgre_driver.php
Method function _execute($sql)

```
....
176.              return @pg_query($this->conn_id, $sql);
```

**Improper Exception Handling\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13389 |
| Status | New |

Method trans_begin at line 203 of system/database/drivers/postgre/postgre_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/postgre/postgre_driver.php | system/database/drivers/postgre/postgre_driver.php |

| | | |
|---|---|---|
| Line | 221 | 221 |
| Object | pg_exec | pg_exec |

Code Snippet
File Name system/database/drivers/postgre/postgre_driver.php
Method function trans_begin($test_mode = FALSE)

```
....
221.            return @pg_exec($this->conn_id, "begin");
```

**Improper Exception Handling\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13390 |
| Status | New |

Method trans_commit at line 232 of system/database/drivers/postgre/postgre_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/postgre/postgre_driver.php | system/database/drivers/postgre/postgre_driver.php |
| Line | 245 | 245 |
| Object | pg_exec | pg_exec |

Code Snippet
File Name system/database/drivers/postgre/postgre_driver.php
Method function trans_commit()

```
....
245.            return @pg_exec($this->conn_id, "commit");
```

**Improper Exception Handling\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13391 |
| Status | New |

Method trans_rollback at line 256 of system/database/drivers/postgre/postgre_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/postgre/postgre_driver.php | system/database/drivers/postgre/postgre_driver.php |
| Line | 269 | 269 |

| | | |
|---|---|---|
| Object | pg_exec | pg_exec |

Code Snippet
File Name system/database/drivers/postgre/postgre_driver.php
Method function trans_rollback()

```
....
269.            return @pg_exec($this->conn_id, "rollback");
```

**Improper Exception Handling\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13392 |
| Status | New |

Method __query at line 41 of system/helpers/dompdf/include/page_cache.cls.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/page_cache.cls.php | system/helpers/dompdf/include/page_cache.cls.php |
| Line | 42 | 42 |
| Object | pg_query | pg_query |

Code Snippet
File Name system/helpers/dompdf/include/page_cache.cls.php
Method private static function __query($sql) {

```
....
42.     if ( !($res = pg_query(self::$__connection, $sql)) )
```

**Improper Exception Handling\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13393 |
| Status | New |

Method _execute at line 167 of system/database/drivers/sqlite/sqlite_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/sqlite/sqlite_driver.php | system/database/drivers/sqlite/sqlite_driver.php |
| Line | 170 | 170 |
| Object | sqlite_query | sqlite_query |

| | |
|---|---|
| Code Snippet | |
| File Name | system/database/drivers/sqlite/sqlite_driver.php |
| Method | function _execute($sql) |

```
....
170.                return @sqlite_query($this->conn_id, $sql);
```

**Improper Exception Handling\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13394 |
| Status | New |

Method __construct at line 299 of application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |
| Line | 315 | 315 |
| Object | prepare | prepare |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |
| Method | public function __construct(PHPExcel_Worksheet $parent) { |

```
....
315.                $this->_deleteQuery = $this->_DBHandle-
>prepare("DELETE FROM kvp_".$this->_TableName." WHERE id = :id");
```

**Improper Exception Handling\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13395 |
| Status | New |

Method __construct at line 299 of application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |
| Line | 314 | 314 |
| Object | prepare | prepare |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |

| | |
|---|---|
| Method | public function __construct(PHPExcel_Worksheet $parent) { |

```
....
314.                $this->_updateQuery = $this->_DBHandle-
>prepare("UPDATE kvp_".$this->_TableName." SET id=:toId WHERE
id=:fromId");
```

**Improper Exception Handling\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13396 |
| Status | New |

Method __construct at line 299 of application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |
| Line | 313 | 313 |
| Object | prepare | prepare |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |
| Method | public function __construct(PHPExcel_Worksheet $parent) { |

```
....
313.                $this->_insertQuery = $this->_DBHandle-
>prepare("INSERT OR REPLACE INTO kvp_".$this->_TableName."
VALUES(:id,:data)");
```

**Improper Exception Handling\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13397 |
| Status | New |

Method __construct at line 299 of application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |
| Line | 312 | 312 |
| Object | prepare | prepare |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |
| Method | public function __construct(PHPExcel_Worksheet $parent) { |

```
....
312.                $this->_selectQuery = $this->_DBHandle-
>prepare("SELECT value FROM kvp_".$this->_TableName." WHERE id = :id");
```

**Improper Exception Handling\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13398 |
| Status | New |

Method __construct at line 299 of application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |
| Line | 308 | 308 |
| Object | exec | exec |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |
| Method | public function __construct(PHPExcel_Worksheet $parent) { |

```
....
308.                    if (!$this->_DBHandle->exec('CREATE TABLE
kvp_'.$this->_TableName.' (id VARCHAR(12) PRIMARY KEY, value BLOB)'))
```

**Improper Exception Handling\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13399 |
| Status | New |

Method _execute at line 189 of system/database/drivers/pdo/pdo_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/pdo/pdo_driver.php | system/database/drivers/pdo/pdo_driver.php |
| Line | 200 | 200 |
| Object | execute | execute |

| | |
|---|---|
| Code Snippet | |
| File Name | system/database/drivers/pdo/pdo_driver.php |

| | |
|---|---|
| Method | function _execute($sql) |

```
....
200.                        $result_id->execute();
```

**Improper Exception Handling\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13400 |
| Status | New |

Method _execute at line 189 of system/database/drivers/pdo/pdo_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/pdo/pdo_driver.php | system/database/drivers/pdo/pdo_driver.php |
| Line | 193 | 193 |
| Object | execute | execute |

| | |
|---|---|
| Code Snippet | |
| File Name | system/database/drivers/pdo/pdo_driver.php |
| Method | function _execute($sql) |

```
....
193.              $result_id->execute();
```

**Improper Exception Handling\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13401 |
| Status | New |

Method _storeData at line 59 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Line | 63 | 63 |
| Object | queryExec | queryExec |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Method | protected function _storeData() { |

```
....
63.                 if (!$this->_DBHandle->queryExec("INSERT OR REPLACE
INTO kvp_".$this->_TableName." VALUES('".$this-
>_currentObjectID."','".sqlite_escape_string(serialize($this-
>_currentObject))."')"))
```

**Improper Exception Handling\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13402 |
| Status | New |

Method deleteCacheData at line 157 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Line | 165 | 165 |
| Object | queryExec | queryExec |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php

Method public function deleteCacheData($pCoord) {

```
....
165.                 if (!$this->_DBHandle->queryExec($query))
```

**Improper Exception Handling\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13403 |
| Status | New |

Method getCellList at line 203 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Line | 209 | 209 |
| Object | unbufferedQuery | unbufferedQuery |

Code Snippet

File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php

Method public function getCellList() {

```
....
209.                $cellIdsResult = $this->_DBHandle-
>unbufferedQuery($query,SQLITE_ASSOC);
```

**Improper Exception Handling\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13404 |
| Status | New |

Method copyCellCollection at line 228 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Line | 234 | 234 |
| Object | queryExec | queryExec |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php
Method public function copyCellCollection(PHPExcel_Worksheet $parent) {

```
....
234.                if (!$this->_DBHandle->queryExec('CREATE TABLE
kvp_'.$tableName.' (id VARCHAR(12) PRIMARY KEY, value BLOB)
```

**Improper Exception Handling\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13405 |
| Status | New |

Method __construct at line 266 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Line | 275 | 275 |
| Object | queryExec | queryExec |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php
Method public function __construct(PHPExcel_Worksheet $parent) {

```
....
275.                    if (!$this->_DBHandle->queryExec('CREATE TABLE
kvp_'.$this->_TableName.' (id VARCHAR(12) PRIMARY KEY, value BLOB)'))
```

**Improper Exception Handling\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13406 |
| Status | New |

Method simple_query at line 446 of system/database/DB_driver.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/DB_driver.php | system/database/DB_driver.php |
| Line | 453 | 453 |
| Object | _execute | _execute |

Code Snippet
File Name system/database/DB_driver.php
Method function simple_query($sql)

```
....
453.                return $this->_execute($sql);
```

**Improper Exception Handling\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13407 |
| Status | New |

Method moveCell at line 179 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Line | 185 | 185 |
| Object | exec | exec |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php
Method public function moveCell($fromAddress, $toAddress) {

```
....
185.            $result = $this->_DBHandle->exec($query);
```

**Improper Exception Handling\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13408 |
| Status | New |

Method moveCell at line 179 of application/third_party/PHPExcel/CachedObjectStorage/SQLite.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite.php |
| Line | 190 | 190 |
| Object | exec | exec |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite.php
Method public function moveCell($fromAddress, $toAddress) {

```
....
190.            $result = $this->_DBHandle->exec($query);
```

**Improper Exception Handling\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13409 |
| Status | New |

Method copyCellCollection at line 261 of application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php | application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php |
| Line | 267 | 267 |
| Object | exec | exec |

Code Snippet
File Name application/third_party/PHPExcel/CachedObjectStorage/SQLite3.php
Method public function copyCellCollection(PHPExcel_Worksheet $parent) {

```
....
267.                if (!$this->_DBHandle->exec('CREATE TABLE
kvp_'.$tableName.' (id VARCHAR(12) PRIMARY KEY, value BLOB)
```

**Improper Exception Handling\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13410 |
| Status | New |

Method _fetch_assoc at line 145 of system/database/drivers/mssql/mssql_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mssql/mssql_result.php | system/database/drivers/mssql/mssql_result.php |
| Line | 147 | 147 |
| Object | mssql_fetch_assoc | mssql_fetch_assoc |

Code Snippet
File Name system/database/drivers/mssql/mssql_result.php
Method function _fetch_assoc()

```
....
147.                return mssql_fetch_assoc($this->result_id);
```

**Improper Exception Handling\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13411 |
| Status | New |

Method _fetch_assoc at line 150 of system/database/drivers/mysql/mysql_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysql/mysql_result.php | system/database/drivers/mysql/mysql_result.php |
| Line | 152 | 152 |
| Object | mysql_fetch_assoc | mysql_fetch_assoc |

Code Snippet
File Name system/database/drivers/mysql/mysql_result.php
Method function _fetch_assoc()

```
....
152.                return mysql_fetch_assoc($this->result_id);
```

**Improper Exception Handling\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13412 |
| Status | New |

Method _fetch_assoc at line 150 of system/database/drivers/mysqli/mysqli_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysqli/mysqli_result.php | system/database/drivers/mysqli/mysqli_result.php |
| Line | 152 | 152 |
| Object | mysqli_fetch_assoc | mysqli_fetch_assoc |

Code Snippet
File Name system/database/drivers/mysqli/mysqli_result.php
Method function _fetch_assoc()

```
....
152.                return mysqli_fetch_assoc($this->result_id);
```

**Improper Exception Handling\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13413 |
| Status | New |

Method list_fields at line 63 of system/database/drivers/mysql/mysql_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysql/mysql_result.php | system/database/drivers/mysql/mysql_result.php |
| Line | 66 | 66 |
| Object | mysql_fetch_field | mysql_fetch_field |

Code Snippet
File Name system/database/drivers/mysql/mysql_result.php
Method function list_fields()

```
....
66.         while ($field = mysql_fetch_field($this->result_id))
```

**Improper Exception Handling\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13414 |
| Status | New |

Method _backup at line 78 of system/database/drivers/mysql/mysql_utility.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysql/mysql_utility.php | system/database/drivers/mysql/mysql_utility.php |
| Line | 146 | 146 |
| Object | mysql_fetch_field | mysql_fetch_field |

Code Snippet
File Name system/database/drivers/mysql/mysql_utility.php
Method function _backup($params = array())

```
....
146.                    while ($field = mysql_fetch_field($query->result_id))
```

**Improper Exception Handling\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13415 |
| Status | New |

Method list_fields at line 63 of system/database/drivers/mysqli/mysqli_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysqli/mysqli_result.php | system/database/drivers/mysqli/mysqli_result.php |
| Line | 66 | 66 |
| Object | mysqli_fetch_field | mysqli_fetch_field |

Code Snippet
File Name system/database/drivers/mysqli/mysqli_result.php
Method function list_fields()

```
....
66.         while ($field = mysqli_fetch_field($this->result_id))
```

**Improper Exception Handling\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13416 |
| Status | New |

Method field_data at line 84 of system/database/drivers/mysql/mysql_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysql/mysql_result.php | system/database/drivers/mysql/mysql_result.php |
| Line | 87 | 87 |
| Object | mysql_fetch_object | mysql_fetch_object |

| | |
|---|---|
| Code Snippet | |
| File Name | system/database/drivers/mysql/mysql_result.php |
| Method | function field_data() |

```
....
87.         while ($field = mysql_fetch_object($this->result_id))
```

**Improper Exception Handling\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13417 |
| Status | New |

Method _fetch_object at line 165 of system/database/drivers/mysql/mysql_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysql/mysql_result.php | system/database/drivers/mysql/mysql_result.php |
| Line | 167 | 167 |
| Object | mysql_fetch_object | mysql_fetch_object |

| | |
|---|---|
| Code Snippet | |
| File Name | system/database/drivers/mysql/mysql_result.php |
| Method | function _fetch_object() |

```
....
167.            return mysql_fetch_object($this->result_id);
```

**Improper Exception Handling\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13418 |
| Status | New |

Method field_data at line 84 of system/database/drivers/mysqli/mysqli_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysqli/mysqli_result.php | system/database/drivers/mysqli/mysqli_result.php |
| Line | 87 | 87 |
| Object | mysqli_fetch_object | mysqli_fetch_object |

Code Snippet
File Name system/database/drivers/mysqli/mysqli_result.php
Method function field_data()

```
....
87.         while ($field = mysqli_fetch_object($this->result_id))
```

**Improper Exception Handling\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13419 |
| Status | New |

Method _fetch_object at line 165 of system/database/drivers/mysqli/mysqli_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysqli/mysqli_result.php | system/database/drivers/mysqli/mysqli_result.php |
| Line | 167 | 167 |
| Object | mysqli_fetch_object | mysqli_fetch_object |

Code Snippet
File Name system/database/drivers/mysqli/mysqli_result.php
Method function _fetch_object()

```
....
167.                return mysqli_fetch_object($this->result_id);
```

**Improper Exception Handling\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13420 |
| Status | New |

Method _fetch_assoc at line 145 of system/database/drivers/odbc/odbc_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/odbc/odbc_result.php | system/database/drivers/odbc/odbc_result.php |
| Line | 149 | 149 |
| Object | odbc_fetch_array | odbc_fetch_array |

Code Snippet
File Name system/database/drivers/odbc/odbc_result.php
Method function _fetch_assoc()

```
....
149.                    return odbc_fetch_array($this->result_id);
```

**Improper Exception Handling\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13421 |
| Status | New |

Method _fetch_object at line 167 of system/database/drivers/odbc/odbc_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/odbc/odbc_result.php | system/database/drivers/odbc/odbc_result.php |
| Line | 171 | 171 |
| Object | odbc_fetch_object | odbc_fetch_object |

Code Snippet
File Name system/database/drivers/odbc/odbc_result.php
Method function _fetch_object()

```
....
171.                    return odbc_fetch_object($this->result_id);
```

**Improper Exception Handling\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13422 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/database/drivers/oci8/oci8_result.php |
| Line | 155 | 155 |
| Object | oci_fetch_assoc | oci_fetch_assoc |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

**Improper Exception Handling\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13423 |
| Status | New |

Method _fetch_object at line 168 of system/database/drivers/oci8/oci8_result.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | system/database/drivers/oci8/oci8_result.php |
| Line | 171 | 171 |
| Object | oci_fetch_object | oci_fetch_object |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_object()

```
....
171.                return @oci_fetch_object($id);
```

**Improper Exception Handling\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13424 |
| Status | New |

Method store_page at line 46 of application/third_party/dompdf/include/page_cache.cls.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/page_cache.cls.php | application/third_party/dompdf/include/page_cache.cls.php |
| Line | 52 | 52 |
| Object | pg_fetch_assoc | pg_fetch_assoc |

Code Snippet
File Name application/third_party/dompdf/include/page_cache.cls.php
Method static function store_page($id, $page_num, $data) {

```
....
52.       $row = pg_fetch_assoc($res);
```

**Improper Exception Handling\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13425 |
| Status | New |

Method get_page_timestamp at line 85 of application/third_party/dompdf/include/page_cache.cls.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/page_cache.cls.php | application/third_party/dompdf/include/page_cache.cls.php |
| Line | 89 | 89 |
| Object | pg_fetch_assoc | pg_fetch_assoc |

Code Snippet
File Name application/third_party/dompdf/include/page_cache.cls.php
Method static function get_page_timestamp($id, $page_num) {

```
....
89.      $row = pg_fetch_assoc($res);
```

**Improper Exception Handling\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13426 |
| Status | New |

Method insert_cached_document at line 96 of application/third_party/dompdf/include/page_cache.cls.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/page_cache.cls.php | application/third_party/dompdf/include/page_cache.cls.php |
| Line | 101 | 101 |
| Object | pg_fetch_assoc | pg_fetch_assoc |

Code Snippet

File Name application/third_party/dompdf/include/page_cache.cls.php

Method static function insert_cached_document(CPDF_Adapter $pdf, $id, $new_page = true) {

```
....
101.      while ($row = pg_fetch_assoc($res))
```

**Improper Exception Handling\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13427 |
| Status | New |

Method insert_cached_document at line 96 of application/third_party/dompdf/include/page_cache.cls.php performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/page_cache.cls.php | application/third_party/dompdf/include/page_cache.cls.php |
| Line | 110 | 110 |
| Object | pg_fetch_assoc | pg_fetch_assoc |

Code Snippet

File Name application/third_party/dompdf/include/page_cache.cls.php

Method static function insert_cached_document(CPDF_Adapter $pdf, $id, $new_page = true) {

```
....
110.      while ($row = pg_fetch_assoc($res)) {
```

## Unsafe Use Of Target Blank

Query Path:
PHP\Cx\Php Low Visibility\Unsafe Use Of Target Blank Version:1

### Categories

FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

### *Description*

**Unsafe Use Of Target Blank\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22738 |
| Status | New |

Using "" target="_blank" id="" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 200 | 200 |
| Object | "" target="_blank" id="" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
200.                    <td><?='<a class="dokumen" href="' .
base_url($img->link) . '" target="_blank" id="' . base_url($img->link) .
'">Foto ' . $count_foto . '</a>';?>
```

**Unsafe Use Of Target Blank\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22739 |
| Status | New |

Using "" class="dokumen" target="_blank">KTP</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 321 | 321 |
| Object | "" class="dokumen" target="_blank">KTP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
321.                    <td><?=$dok->ktp_link == '' ? '-' : '<a href="'
. base_url($dok->ktp_link) . '" class="dokumen"
target="_blank">KTP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22740 |
| Status | New |

Using "" class="dokumen" target="_blank">NPWP</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 329 | 329 |
| Object | "" class="dokumen" target="_blank">NPWP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
329.                    <td><?=$dok->npwp_link == '' ? '-' : '<a href="'
. base_url($dok->npwp_link) . '" class="dokumen"
target="_blank">NPWP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22741 |
| Status | New |

Using "" class="dokumen" target="_blank">TDP</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 337 | 337 |
| Object | "" class="dokumen" target="_blank">TDP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
337.                    <td><?=$dok->tdp_link == '' ? '-' : '<a href="'
. base_url($dok->tdp_link) . '" class="dokumen"
target="_blank">TDP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 5:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22742
Status New

Using "" class="dokumen" target="_blank">SIUP</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 345 | 345 |
| Object | "" class="dokumen" target="_blank">SIUP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
345.                    <td><?=$dok->siup_link == '' ? '-' : '<a href="'
. base_url($dok->siup_link) . '" class="dokumen"
target="_blank">SIUP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22743 |
| Status | New |

Using "" class="dokumen" target="_blank">SITU</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 353 | 353 |
| Object | "" class="dokumen" target="_blank">SITU</a>" | echo |

Code Snippet

File Name application/views/aplikasi_daftar/detail_merchant_view.php

Method <?php $m = $merchant->row();?>

```
....
353.                    <td><?=$dok->situ_link == '' ? '-' : '<a href="'
. base_url($dok->situ_link) . '" class="dokumen"
target="_blank">SITU</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22744 |
| Status | New |

Using "" class="dokumen" target="_blank">Surat Kuasa</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 361 | 361 |
| Object | "" class="dokumen" target="_blank">Surat Kuasa</a>" | echo |

Code Snippet

File Name application/views/aplikasi_daftar/detail_merchant_view.php

Method <?php $m = $merchant->row();?>

```
....
361.                    <td><?=$dok->surat_kuasa_link == '' ? '-' : '<a
href="' . base_url($dok->surat_kuasa_link) . '" class="dokumen"
target="_blank">Surat Kuasa</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22745 |
| Status | New |

Using "" class="dokumen" target="_blank">Akta Jual Beli / Sewa</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 369 | 369 |
| Object | "" class="dokumen" target="_blank">Akta Jual Beli / Sewa</a>" | echo |

Code Snippet

File Name application/views/aplikasi_daftar/detail_merchant_view.php

Method <?php $m = $merchant->row();?>

```
....
369.                    <td><?=$dok->akta_jbs_link == '' ? '-' : '<a
href="' . base_url($dok->akta_jbs_link) . '" class="dokumen"
target="_blank">Akta Jual Beli / Sewa</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22746 |
| Status | New |

Using "" class="dokumen" target="_blank">Lainnya</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |

| | | |
|---|---|---|
| Line | 377 | 377 |
| Object | "" class="dokumen" target="_blank">Lainnya</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
377.                    <td><?=$dok->lainnya_link == '' ? '-' : '<a
href="' . base_url($dok->lainnya_link) . '" class="dokumen"
target="_blank">Lainnya</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22747 |
| Status | New |

Using "" target="_blank">Business Model (download)</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 403 | 403 |
| Object | "" target="_blank">Business Model (download)</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
403.                    <td><?=$dok->business_model_link == '0' ? '-' :
'<a href="' . base_url($dok->business_model_link) . '"
target="_blank">Business Model (download)</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22748 |
| Status | New |

Using "" class="dokumen" target="_blank">LKM</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view.php, without correctly setting the "rel"

attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view.php | application/views/aplikasi_daftar/detail_merchant_view.php |
| Line | 409 | 409 |
| Object | "" class="dokumen" target="_blank">LKM</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view.php
Method <?php $m = $merchant->row();?>

```
....
409.                    <td><?php echo $dok->lkm_link == '' ? '-' : '<a
href="' . base_url($dok->lkm_link) . '" class="dokumen"
target="_blank">LKM</a>'; ?></td>
```

**Unsafe Use Of Target Blank\Path 12:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22749
Status New

Using "" target="_blank" id="" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 667 | 667 |
| Object | "" target="_blank" id="" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
667.                                <td><?='<a class="dokumen" href="' .
base_url($img->link) . '" target="_blank" id="' . base_url($img->link) .
'">'.substr($img->link, (strrpos($img->link,'/') + 1)).'</a>';?>
```

**Unsafe Use Of Target Blank\Path 13:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti

| | |
|---|---|
| | d=4881&pathid=22750 |
| Status | New |

Using "" class="dokumen" target="_blank">KTP</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 696 | 696 |
| Object | "" class="dokumen" target="_blank">KTP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
696.                                <td><?=$dok->ktp_link == '' ? '-' :
'<a href="' . base_url($dok->ktp_link) . '" class="dokumen"
target="_blank">KTP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22751 |
| Status | New |

Using "" class="dokumen" target="_blank">NPWP</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 704 | 704 |
| Object | "" class="dokumen" target="_blank">NPWP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
704.                                <td><?=$dok->npwp_link == '' ? '-' :
'<a href="' . base_url($dok->npwp_link) . '" class="dokumen"
target="_blank">NPWP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22752 |
| Status | New |

Using "" class="dokumen" target="_blank">TDP</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 712 | 712 |
| Object | "" class="dokumen" target="_blank">TDP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
712.                                <td><?=$dok->tdp_link == '' ? '-' :
'<a href="' . base_url($dok->tdp_link) . '" class="dokumen"
target="_blank">TDP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22753 |
| Status | New |

Using "" class="dokumen" target="_blank">SIUP</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 720 | 720 |

| | | |
|---|---|---|
| Object | "" class="dokumen" target="_blank">SIUP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
720.                                <td><?=$dok->siup_link == '' ? '-' :
'<a href="' . base_url($dok->siup_link) . '" class="dokumen"
target="_blank">SIUP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22754 |
| Status | New |

Using "" class="dokumen" target="_blank">SITU</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 728 | 728 |
| Object | "" class="dokumen" target="_blank">SITU</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
728.                                <td><?=$dok->situ_link == '' ? '-' :
'<a href="' . base_url($dok->situ_link) . '" class="dokumen"
target="_blank">SITU</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22755 |
| Status | New |

Using "" class="dokumen" target="_blank">Surat Kuasa</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 736 | 736 |
| Object | "" class="dokumen" target="_blank">Surat Kuasa</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
736.                                <td><?=$dok->surat_kuasa_link == ''
? '-' : '<a href="' . base_url($dok->surat_kuasa_link) . '"
class="dokumen" target="_blank">Surat Kuasa</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 19:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22756
Status New

Using "" class="dokumen" target="_blank">Akta Jual Beli / Sewa</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 744 | 744 |
| Object | "" class="dokumen" target="_blank">Akta Jual Beli / Sewa</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
744.                                <td><?=$dok->akta_jbs_link == '' ?
'-' : '<a href="' . base_url($dok->akta_jbs_link) . '" class="dokumen"
target="_blank">Akta Jual Beli / Sewa</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 20:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22757

| | |
|---|---|
| Status | New |

Using "" class="dokumen" target="_blank">Lainnya</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 752 | 752 |
| Object | "" class="dokumen" target="_blank">Lainnya</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
752.                                <td><?=$dok->lainnya_link == '' ? '-
' : '<a href="' . base_url($dok->lainnya_link) . '" class="dokumen"
target="_blank">Lainnya</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22758 |
| Status | New |

Using "" class="dokumen" target="_blank">LKM</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 786 | 786 |
| Object | "" class="dokumen" target="_blank">LKM</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
786.                                <td><?php echo $dok->lkm_link == ''
? '-' : '<a href="' . base_url($dok->lkm_link) . '" class="dokumen"
target="_blank">LKM</a>'; ?></td>
```

**Unsafe Use Of Target Blank\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22759 |
| Status | New |

Using "" class="dokumen" target="_blank">PKS</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 792 | 792 |
| Object | "" class="dokumen" target="_blank">PKS</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
792.                                <td><?php echo $dok->pks_link == ''
? '-' : '<a href="' . base_url($dok->pks_link) . '" class="dokumen"
target="_blank">PKS</a>'; ?></td>
```

**Unsafe Use Of Target Blank\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22760 |
| Status | New |

Using "" class="dokumen" target="_blank">FPM</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 798 | 798 |
| Object | "" class="dokumen" target="_blank">FPM</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php

Method <style>

```
....
798.                                <td><?php echo $dok->fpm_link == ''
? '-' : '<a href="' . base_url($dok->fpm_link) . '" class="dokumen"
target="_blank">FPM</a>'; ?></td>
```

**Unsafe Use Of Target Blank\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22761 |
| Status | New |

Using "" class="dokumen" target="_blank">Bisnis Model</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_new.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_new.php | application/views/aplikasi_daftar/detail_merchant_view_new.php |
| Line | 804 | 804 |
| Object | "" class="dokumen" target="_blank">Bisnis Model</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_new.php
Method <style>

```
....
804.                                <td><?php echo $dok->bismod_link ==
'' ? '-' : '<a href="' . base_url($dok->bismod_link) . '"
class="dokumen" target="_blank">Bisnis Model</a>'; ?></td>
```

**Unsafe Use Of Target Blank\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22762 |
| Status | New |

Using "" class="dokumen" target="_blank">Lihat Hasil Field Verification</a>" at line 1 of application/views/aplikasi_daftar/detail_merchant_view_old.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_merchant_view_old.php | application/views/aplikasi_daftar/detail_merchant_view_old.php |

| | | |
|---|---|---|
| Line | 694 | 694 |
| Object | "" class="dokumen" target="_blank">Lihat Hasil Field Verification</a>" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_merchant_view_old.php
Method <script>

```
....
694.                            <?php echo $dok->field_ver_link==='' ?
'Hasil Field Verification belum diupload' : '<a href="'.base_url($dok-
>field_ver_link).'" class="dokumen" target="_blank">Lihat Hasil Field
Verification</a>';?>
```

**Unsafe Use Of Target Blank\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22763 |
| Status | New |

Using "" target="_blank" id="" at line 1 of application/views/aplikasi_daftar/detail_outlet_view.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_daftar/detail_outlet_view.php | application/views/aplikasi_daftar/detail_outlet_view.php |
| Line | 186 | 186 |
| Object | "" target="_blank" id="" | echo |

Code Snippet
File Name application/views/aplikasi_daftar/detail_outlet_view.php
Method <script type="text/javascript">

```
....
186.                    <td><?='<a class="dokumen" href="' .
base_url($img->link) . '" target="_blank" id="' . base_url($img->link) .
'">Foto ' . $count_foto . '</a>';?>
```

**Unsafe Use Of Target Blank\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22764 |
| Status | New |

Using "" target="_blank">KTP</a> <button class="redbutton hapus_dokumen_btn" rel="" at line 1 of application/views/aplikasi_edit/edit_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant.php | application/views/aplikasi_edit/edit_merchant.php |
| Line | 841 | 840 |
| Object | "" target="_blank">KTP</a>   <button class="redbutton hapus_dokumen_btn" rel="" | echo |

Code Snippet
File Name application/views/aplikasi_edit/edit_merchant.php
Method <?php

```
....
841.                                                    '<a
href="'.base_url($dok->ktp_link).'"
target="_blank">KTP</a>  <button class="redbutton
hapus_dokumen_btn" rel="'.$dok->ktp_link.'" name="ktp_link"
app_id="'.$dok->app_id.'">Hapus</button>';?></td>
....
840.                     <td class="dok_td"><?php echo $dok->ktp_link=='' 
? '<div class="button"
style="position:absolute;background:#F7941D;margin-left:6%">Upload
File</div><input id="ktp_link" class="upload" type="file"
style="opacity:0;z-index:1;cursor:pointer;width:100%" accept="image/*"
name="ktp_link">' :
```

**Unsafe Use Of Target Blank\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22765 |
| Status | New |

Using "" target="_blank">NPWP</a>  <button class="redbutton hapus_dokumen_btn" rel="" at line 1 of application/views/aplikasi_edit/edit_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant.php | application/views/aplikasi_edit/edit_merchant.php |
| Line | 856 | 855 |
| Object | "" target="_blank">NPWP</a>  <button class="redbutton hapus_dokumen_btn" rel="" | echo |

Code Snippet
File Name application/views/aplikasi_edit/edit_merchant.php
Method <?php

```
....
856.                                                    '<a
href="'.base_url($dok->npwp_link).'"
target="_blank">NPWP</a>  <button class="redbutton
hapus_dokumen_btn" rel="'.$dok->npwp_link.'" name="npwp_link"
app_id="'.$dok->app_id.'">Hapus</button>';?></td>
....
855.                    <td class="dok_td"><?php echo $dok-
>npwp_link=='' ? '<div class="button"
style="position:absolute;background:#F7941D;margin-left:6%">Upload
File</div><input id="npwp_link" class="upload" type="file"
style="opacity:0;z-index:1;cursor:pointer;width:100%" accept="image/*"
name="npwp_link">' :
```

**Unsafe Use Of Target Blank\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22766 |
| Status | New |

Using "" target="_blank">TDP</a>  <button class="redbutton hapus_dokumen_btn" rel="" at line 1 of application/views/aplikasi_edit/edit_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant.php | application/views/aplikasi_edit/edit_merchant.php |
| Line | 871 | 870 |
| Object | "" target="_blank">TDP</a>   <button class="redbutton hapus_dokumen_btn" rel="" | echo |

Code Snippet

File Name application/views/aplikasi_edit/edit_merchant.php

Method <?php

```
....
871.                                                    '<a
href="'.base_url($dok->tdp_link).'"
target="_blank">TDP</a>  <button class="redbutton
hapus_dokumen_btn" rel="'.$dok->tdp_link.'" name="tdp_link"
app_id="'.$dok->app_id.'">Hapus</button>';?></td>
....
870.                    <td class="dok_td"><?php echo $dok->tdp_link=''
? '<div class="button"
style="position:absolute;background:#F7941D;margin-left:6%">Upload
File</div><input id="tdp_link" class="upload" type="file"
style="opacity:0;z-index:1;cursor:pointer;width:100%" accept="image/*"
name="tdp_link">' :
```

**Unsafe Use Of Target Blank\Path 30:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22767 |
| Status | New |

Using "" target="_blank">SIUP</a>  <button class="redbutton hapus_dokumen_btn" rel="" at line 1 of application/views/aplikasi_edit/edit_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant.php | application/views/aplikasi_edit/edit_merchant.php |
| Line | 886 | 885 |
| Object | "" target="_blank">SIUP</a>  <button class="redbutton hapus_dokumen_btn" rel="" | echo |

Code Snippet
File Name application/views/aplikasi_edit/edit_merchant.php
Method <?php

```
....
886.                                                    '<a
href="'.base_url($dok->siup_link).'"
target="_blank">SIUP</a>  <button class="redbutton
hapus_dokumen_btn" rel="'.$dok->siup_link.'" name="siup_link"
app_id="'.$dok->app_id.'">Hapus</button>';?></td>
....
885.                    <td class="dok_td"><?php echo $dok-
>siup_link=='' ? '<div class="button"
style="position:absolute;background:#F7941D;margin-left:6%">Upload
File</div><input id="siup_link" class="upload" type="file"
style="opacity:0;z-index:1;cursor:pointer;width:100%" accept="image/*"
name="siup_link">' :
```

**Unsafe Use Of Target Blank\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22768 |
| Status | New |

Using "" target="_blank">SITU</a>  <button class="redbutton hapus_dokumen_btn" rel="" at line 1 of application/views/aplikasi_edit/edit_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant.php | application/views/aplikasi_edit/edit_merchant.php |
| Line | 901 | 900 |
| Object | "" | echo |

| | | |
|---|---|---|
| | target="_blank">SITU</a>  <button class="redbutton hapus_dokumen_btn" rel="" | |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_edit/edit_merchant.php |
| Method | <?php |

```
....
901.                                                    '<a
href="'.base_url($dok->situ_link).'"
target="_blank">SITU</a>  <button class="redbutton
hapus_dokumen_btn" rel="'.$dok->situ_link.'" name="situ_link"
app_id="'.$dok->app_id.'">Hapus</button>';?></td>
....
900.                    <td class="dok_td"><?php echo $dok-
>situ_link=='' ? '<div class="button"
style="position:absolute;background:#F7941D;margin-left:6%">Upload
File</div><input id="situ_link" class="upload" type="file"
style="opacity:0;z-index:1;cursor:pointer;width:100%" accept="image/*"
name="situ_link">' :
```

**Unsafe Use Of Target Blank\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22769 |
| Status | New |

Using "" target="_blank">Surat Kuasa</a>  <button class="redbutton hapus_dokumen_btn" rel="" at line 1 of application/views/aplikasi_edit/edit_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant.php | application/views/aplikasi_edit/edit_merchant.php |
| Line | 916 | 915 |
| Object | "" target="_blank">Surat Kuasa</a>  <button class="redbutton hapus_dokumen_btn" rel="" | echo |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/aplikasi_edit/edit_merchant.php |
| Method | <?php |

```
....
916.                                        '<a href="'.base_url($dok-
>surat_kuasa_link).'" target="_blank">Surat Kuasa</a>  <button
class="redbutton hapus_dokumen_btn" rel="'.$dok->surat_kuasa_link.'"
name="surat_kuasa_link" app_id="'.$dok-
>app_id.'">Hapus</button>';?></td>
....
915.                    <td class="dok_td"><?php echo $dok-
>surat_kuasa_link=='' ? '<div class="button"
style="position:absolute;background:#F7941D;margin-left:6%">Upload
File</div><input id="surat_kuasa_link" class="upload" type="file"
style="opacity:0;z-index:1;cursor:pointer;width:100%" accept="image/*"
name="surat_kuasa_link">' :
```

**Unsafe Use Of Target Blank\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22770 |
| Status | New |

Using "" target="_blank">Akta Jual Beli / Sewa</a>  <button class="redbutton hapus_dokumen_btn" rel="" at line 1 of application/views/aplikasi_edit/edit_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant.php | application/views/aplikasi_edit/edit_merchant.php |
| Line | 931 | 930 |
| Object | "" target="_blank">Akta Jual Beli / Sewa</a>  <button class="redbutton hapus_dokumen_btn" rel="" | echo |

Code Snippet

File Name application/views/aplikasi_edit/edit_merchant.php

Method <?php

```
....
931.                                                    '<a
href="'.base_url($dok->akta_jbs_link).'" target="_blank">Akta Jual Beli
/ Sewa</a>  <button class="redbutton hapus_dokumen_btn"
rel="'.$dok->akta_jbs_link.'" name="akta_jbs_link" app_id="'.$dok-
>app_id.'">Hapus</button>';?></td>
....
930.                    <td class="dok_td"><?php echo $dok-
>akta_jbs_link=='' ? '<div class="button"
style="position:absolute;background:#F7941D;margin-left:6%">Upload
File</div><input id="akta_jbs_link" class="upload" type="file"
style="opacity:0;z-index:1;cursor:pointer;width:100%" accept="image/*"
name="akta_jbs_link">' :
```

**Unsafe Use Of Target Blank\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22771 |
| Status | New |

Using "" target="_blank">Lainnya</a>  <button class="redbutton hapus_dokumen_btn" rel="" at line 1 of application/views/aplikasi_edit/edit_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_edit/edit_merchant.php | application/views/aplikasi_edit/edit_merchant.php |
| Line | 946 | 945 |
| Object | "" target="_blank">Lainnya</a>  <button class="redbutton hapus_dokumen_btn" rel="" | echo |

Code Snippet
File Name application/views/aplikasi_edit/edit_merchant.php
Method <?php

```
....
946.                                                    '<a
href="'.base_url($dok->lainnya_link).'"
target="_blank">Lainnya</a>  <button class="redbutton
hapus_dokumen_btn" rel="'.$dok->lainnya_link.'" name="lainnya_link"
app_id="'.$dok->app_id.'">Hapus</button>';?></td>
....
945.                    <td class="dok_td"><?php echo $dok-
>lainnya_link==='' ? '<div class="button"
style="position:absolute;background:#F7941D;margin-left:6%">Upload
File</div><input id="lainnya_link" class="upload" type="file"
style="opacity:0;z-index:1;cursor:pointer;width:100%" accept="image/*"
name="lainnya_link">' :
```

**Unsafe Use Of Target Blank\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22772 |
| Status | New |

Using "" target="_blank" id="" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 118 | 118 |

| | | |
|---|---|---|
| Object | "" target="_blank" id="" | echo |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <?php

```
....
118.                    <td><?='<a class="dokumen"
href="'.base_url($img['link']).'" target="_blank"
id="'.base_url($img['link']).'">Foto '.$count_foto.'</a>';?>
```

**Unsafe Use Of Target Blank\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22773 |
| Status | New |

Using "" class="dokumen" target="_blank">KTP</a>" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 236 | 236 |
| Object | "" class="dokumen" target="_blank">KTP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <?php

```
....
236.                    <td><?=$dok['ktp_link']=='' ? '-' : '<a
href="'.base_url($dok['ktp_link']).'" class="dokumen"
target="_blank">KTP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22774 |
| Status | New |

Using "" class="dokumen" target="_blank">NPWP</a>" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 244 | 244 |
| Object | "" class="dokumen" target="_blank">NPWP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <?php

```
....
244.                    <td><?=$dok['npwp_link']=='' ? '-' : '<a
href="'.base_url($dok['npwp_link']).'" class="dokumen"
target="_blank">NPWP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22775 |
| Status | New |

Using "" class="dokumen" target="_blank">TDP</a>" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 252 | 252 |
| Object | "" class="dokumen" target="_blank">TDP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <?php

```
....
252.                    <td><?=$dok['tdp_link']=='' ? '-' : '<a
href="'.base_url($dok['tdp_link']).'" class="dokumen"
target="_blank">TDP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22776 |
| Status | New |

Using "" class="dokumen" target="_blank">SIUP</a>" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 260 | 260 |
| Object | "" class="dokumen" target="_blank">SIUP</a>" | echo |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <?php

```
....
260.                    <td><?=$dok['siup_link']=='' ? '-' : '<a
href="'.base_url($dok['siup_link']).'" class="dokumen"
target="_blank">SIUP</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22777 |
| Status | New |

Using "" class="dokumen" target="_blank">SITU</a>" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 268 | 268 |
| Object | "" class="dokumen" target="_blank">SITU</a>" | echo |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <?php

```
....
268.                    <td><?=$dok['situ_link']=='' ? '-' : '<a
href="'.base_url($dok['situ_link']).'" class="dokumen"
target="_blank">SITU</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22778 |
| Status | New |

Using "" class="dokumen" target="_blank">Surat Kuasa</a>" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 276 | 276 |
| Object | "" class="dokumen" target="_blank">Surat Kuasa</a>" | echo |

Code Snippet

File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php

Method <?php

```
....
276.                    <td><?=$dok['surat_kuasa_link']=='' ? '-' : '<a
href="'.base_url($dok['surat_kuasa_link']).'" class="dokumen"
target="_blank">Surat Kuasa</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22779 |
| Status | New |

Using "" class="dokumen" target="_blank">Akta Jual Beli / Sewa</a>" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 284 | 284 |
| Object | "" class="dokumen" target="_blank">Akta Jual Beli / Sewa</a>" | echo |

Code Snippet

File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php

Method <?php

```
....
284.                    <td><?=$dok['akta_jbs_link']=='' ? '-' : '<a
href="'.base_url($dok['akta_jbs_link']).'" class="dokumen"
target="_blank">Akta Jual Beli / Sewa</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22780 |
| Status | New |

Using "" class="dokumen" target="_blank">Lainnya</a>" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 292 | 292 |
| Object | "" class="dokumen" target="_blank">Lainnya</a>" | echo |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <?php

```
....
292.                    <td><?=$dok['lainnya_link']=='' ? '-' : '<a
href="'.base_url($dok['lainnya_link']).'" class="dokumen"
target="_blank">Lainnya</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22781 |
| Status | New |

Using "" target="_blank">Business Model (download)</a>" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |

| | | |
|---|---|---|
| Line | 318 | 318 |
| Object | "" target="_blank">Business Model (download)</a>" | echo |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <?php

```
....
318.                    <td><?=$dok['business_model_link']=='' ? '-' :
'<a href="'.base_url($dok['business_model_link']).'"
target="_blank">Business Model (download)</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22782 |
| Status | New |

Using "" class="dokumen" target="_blank">LKM</a>" at line 1 of application/views/aplikasi_merchant/popup_detail_app_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/aplikasi_merchant/popup_detail_app_merchant.php | application/views/aplikasi_merchant/popup_detail_app_merchant.php |
| Line | 324 | 324 |
| Object | "" class="dokumen" target="_blank">LKM</a>" | echo |

Code Snippet
File Name application/views/aplikasi_merchant/popup_detail_app_merchant.php
Method <?php

```
....
324.                    <td><?php echo $dok['lkm_link']=='' ? '-' : '<a
href="'.base_url($dok['lkm_link']).'" class="dokumen"
target="_blank">LKM</a>';?></td>
```

**Unsafe Use Of Target Blank\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22783 |
| Status | New |

Using "" class="dokumen" target="_blank">PKS</a>" at line 1 of application/views/cetak/detail_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/cetak/detail_merchant.php | application/views/cetak/detail_merchant.php |
| Line | 424 | 424 |
| Object | "" class="dokumen" target="_blank">PKS</a>" | echo |

Code Snippet
File Name application/views/cetak/detail_merchant.php
Method <style type="text/css">

```
....
424.                    <td><?php echo $dok->pks_link == '' ? '-' : '<a
href="' . base_url($dok->pks_link) . '" class="dokumen"
target="_blank">PKS</a>'; ?></td>
```

**Unsafe Use Of Target Blank\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22784 |
| Status | New |

Using "" class="dokumen" target="_blank">FPM</a>" at line 1 of application/views/cetak/detail_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/cetak/detail_merchant.php | application/views/cetak/detail_merchant.php |
| Line | 430 | 430 |
| Object | "" class="dokumen" target="_blank">FPM</a>" | echo |

Code Snippet
File Name application/views/cetak/detail_merchant.php
Method <style type="text/css">

```
....
430.                    <td><?php echo $dok->fpm_link == '' ? '-' : '<a
href="' . base_url($dok->fpm_link) . '" class="dokumen"
target="_blank">FPM</a>'; ?></td>
```

**Unsafe Use Of Target Blank\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22785 |
| Status | New |

Using "" class="dokumen" target="_blank">Bisnis Model</a>" at line 1 of application/views/cetak/detail_merchant.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/cetak/detail_merchant.php | application/views/cetak/detail_merchant.php |
| Line | 436 | 436 |
| Object | "" class="dokumen" target="_blank">Bisnis Model</a>" | echo |

Code Snippet
File Name application/views/cetak/detail_merchant.php
Method <style type="text/css">

```
....
436.                    <td><?php echo $dok->bismod_link == '' ? '-' :
'<a href="' . base_url($dok->bismod_link) . '" class="dokumen"
target="_blank">Bisnis Model</a>'; ?></td>
```

**Unsafe Use Of Target Blank\Path 49:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22786
Status New

Using "" class="dokumen" target="_blank">doc IPM</a><br>" at line 1 of application/views/chargeback/chargeback_confirm.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/chargeback/chargeback_confirm.php | application/views/chargeback/chargeback_confirm.php |
| Line | 154 | 154 |
| Object | "" class="dokumen" target="_blank">doc IPM</a><br>" | echo |

Code Snippet
File Name application/views/chargeback/chargeback_confirm.php
Method <style type="text/css">

```
....
154.                        <?=$list->dok == '' ? '-' : '<a href="' .
base_url($list->dok) . '" class="dokumen" target="_blank"><i>doc
IPM</i></a><br>';?>
```

**Unsafe Use Of Target Blank\Path 50:**

Severity Low

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22787 |
| Status | New |

Using "" class="dokumen" target="_blank">doc OPK</a><br>" at line 1 of application/views/chargeback/chargeback_confirm.php, without correctly setting the "rel" attribute, or disassociating the new window from its parent, is an unsafe way of opening a new window.

| | Source | Destination |
|---|---|---|
| File | application/views/chargeback/chargeback_confirm.php | application/views/chargeback/chargeback_confirm.php |
| Line | 155 | 155 |
| Object | "" class="dokumen" target="_blank">doc OPK</a><br>" | echo |

Code Snippet
File Name application/views/chargeback/chargeback_confirm.php
Method <style type="text/css">

```
....
155.                          <?=$list->dok_opk == '' ? '-' : '<a
href="' . base_url($list->dok_opk) . '" class="dokumen"
target="_blank"><i>doc OPK</i></a><br>';?>
```

## Insufficiently Protected Credentials

Query Path:
PHP\Cx\Php Low Visibility\Insufficiently Protected Credentials Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage
OWASP Top 10 2013: A2-Broken Authentication and Session Management
FISMA 2014: Media Protection
NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity (P1)
OWASP Top 10 2017: A2-Broken Authentication
OWASP Top 10 2021: A4-Insecure Design

*Description*

**Insufficiently Protected Credentials\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14061 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of application/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_resul | application/controllers/inisiasi_scheduler. |

| | | |
|---|---|---|
| | t.php | php |
| Line | 155 | 1653 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1653.                                          $log_temp['psw_tid_log']
= $init->init_tid." on Report PSW: ";
```

**Insufficiently Protected Credentials\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14062 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of application/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler.php |
| Line | 155 | 1656 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1656.
      $log_temp['psw_tid_log'] .= $tid_psw_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14063 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of application/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler.php |
| Line | 155 | 1663 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1663.
      $log_temp['psw_tid_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14064 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of application/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler.php |
| Line | 155 | 1607 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1607.
      $log_temp['psw_jcb_log'] = $init->init_mid." on Report JCB: ";
```

**Insufficiently Protected Credentials\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14065 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of application/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler.php |
| Line | 155 | 1610 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1610.
      $log_temp['psw_jcb_log'] .= $mid_jcb_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14066 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of application/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler.php |
| Line | 155 | 1616 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1616.
      $log_temp['psw_jcb_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14067 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of application/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler.php |
| Line | 155 | 1588 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1588.
      $log_temp['psw_mid_log'] = $init->init_mid." on Report PSW: ";
```

**Insufficiently Protected Credentials\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14068 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of application/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler.php |
| Line | 155 | 1591 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1591.
      $log_temp['psw_mid_log'] .= $mid_psw_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14069 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of application/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler.php |
| Line | 155 | 1597 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1597.
      $log_temp['psw_mid_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14070 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 155 | 1653 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1653.                                                $log_temp['psw_tid_log']
= $init->init_tid." on Report PSW: ";
```

**Insufficiently Protected Credentials\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14071 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 155 | 1656 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1656.
      $log_temp['psw_tid_log'] .= $tid_psw_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14072 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 155 | 1663 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1663.
      $log_temp['psw_tid_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14073 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 155 | 1607 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1607.
      $log_temp['psw_jcb_log'] = $init->init_mid." on Report JCB: ";
```

**Insufficiently Protected Credentials\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14074 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 155 | 1610 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1610.
      $log_temp['psw_jcb_log'] .= $mid_jcb_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14075 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 155 | 1616 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1616.
      $log_temp['psw_jcb_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14076 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of

BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 155 | 1588 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1588.
      $log_temp['psw_mid_log'] = $init->init_mid." on Report PSW: ";
```

**Insufficiently Protected Credentials\Path 17:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14077
Status New

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 155 | 1591 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1591.
      $log_temp['psw_mid_log'] .= $mid_psw_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14078 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 155 | 1597 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1597.
      $log_temp['psw_mid_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14079 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1522 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1522.                                                $log_temp['psw_tid_log']
= $init->init_tid." on Report PSW: ";
```

**Insufficiently Protected Credentials\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14080 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1525 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

| | |
|---|---|
| Method | protected function _fetch_assoc() |

```
....
155.            return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Method | function check_inisiasi_new() |

```
....
1525.
      $log_temp['psw_tid_log'] .= $tid_psw_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14081 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1532 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.            return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Method | function check_inisiasi_new() |

```
....
1532.
      $log_temp['psw_tid_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14082 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1475 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1475.
      $log_temp['psw_jcb_log'] = $init->init_mid." on Report JCB: ";
```

**Insufficiently Protected Credentials\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14083 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_2016 |

| | | |
|---|---|---|
| | | 1206.php |
| Line | 155 | 1478 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php
Method function check_inisiasi_new()

```
....
1478.
      $log_temp['psw_jcb_log'] .= $mid_jcb_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14084 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1484 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Method | function check_inisiasi_new() |

```
....
1484.
      $log_temp['psw_jcb_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14085 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1455 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.              return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Method | function check_inisiasi_new() |

```
....
1455.
      $log_temp['psw_mid_log'] = $init->init_mid." on Report PSW: ";
```

**Insufficiently Protected Credentials\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14086 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1458 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1458.
      $log_temp['psw_mid_log'] .= $mid_psw_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14087 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1464 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

| | |
|---|---|
| Method | protected function _fetch_assoc() |

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Method | function check_inisiasi_new() |

```
....
1464.
      $log_temp['psw_mid_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14088 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 943 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_not_yet_used.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_not_yet_used.php |
| Line | 155 | 1099 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet

| | |
|---|---|
| File Name | system/database/drivers/oci8/oci8_result.php |
| Method | protected function _fetch_assoc() |

```
....
155.                return oci_fetch_assoc($id);
```

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_not_yet_used.php |
| Method | function check_inisiasi_new() |

```
....
1099.                                          $log_temp['psw_tid_log']
= $init->init_tid."on Report PSW: ".(int)$is_tid_psw;
```

**Insufficiently Protected Credentials\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14089 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 943 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_not_yet_used.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_not_yet_used.php |
| Line | 155 | 1061 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_not_yet_used.php

Method function check_inisiasi_new()

```
....
1061.
      $log_temp['psw_mid_log'] = $init->init_mid." on Report PSW:
".(int)$is_mid_psw;
```

**Insufficiently Protected Credentials\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14090 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of application/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_resul | application/controllers/inisiasi_scheduler |

| | | |
|---|---|---|
| | t.php | _20161206.php |
| Line | 155 | 1522 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1522.                                          $log_temp['psw_tid_log']
= $init->init_tid." on Report PSW: ";
```

**Insufficiently Protected Credentials\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14091 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of application/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1525 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1525.
      $log_temp['psw_tid_log'] .= $tid_psw_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14092 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of application/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1532 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1532.
      $log_temp['psw_tid_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14093 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of application/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1475 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_20161206.php
Method function check_inisiasi_new()

```
....
1475.
      $log_temp['psw_jcb_log'] = $init->init_mid." on Report JCB: ";
```

**Insufficiently Protected Credentials\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14094 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of application/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1478 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1478.
      $log_temp['psw_jcb_log'] .= $mid_jcb_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14095 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of application/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1484 |
| Object | oci_fetch_assoc | psw_jcb_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1484.
      $log_temp['psw_jcb_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14096 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of

application/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1455 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_20161206.php
Method function check_inisiasi_new()

```
....
1455.
      $log_temp['psw_mid_log'] = $init->init_mid." on Report PSW: ";
```

**Insufficiently Protected Credentials\Path 37:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14097
Status New

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of application/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1458 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.            return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1458.
      $log_temp['psw_mid_log'] .= $mid_psw_status[$idx_found];
```

**Insufficiently Protected Credentials\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14098 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 1317 of application/controllers/inisiasi_scheduler_20161206.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 155 | 1464 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.              return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1464.
      $log_temp['psw_mid_log'] .= 'NOT FOUND';
```

**Insufficiently Protected Credentials\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14099 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 943 of application/controllers/inisiasi_scheduler_not_yet_used.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler_not_yet_used.php |
| Line | 155 | 1099 |
| Object | oci_fetch_assoc | psw_tid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.             return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_not_yet_used.php

Method function check_inisiasi_new()

```
....
1099.                                          $log_temp['psw_tid_log']
= $init->init_tid."on Report PSW: ".(int)$is_tid_psw;
```

**Insufficiently Protected Credentials\Path 40:**

Severity Low

Result State To Verify

Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14100

Status New

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in check_inisiasi_new at line 943 of application/controllers/inisiasi_scheduler_not_yet_used.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/inisiasi_scheduler_not_yet_used.php |
| Line | 155 | 1061 |
| Object | oci_fetch_assoc | psw_mid_log |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/inisiasi_scheduler_not_yet_used.php

Method function check_inisiasi_new()

```
....
1061.
      $log_temp['psw_mid_log'] = $init->init_mid." on Report PSW:
".(int)$is_mid_psw;
```

**Insufficiently Protected Credentials\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14101 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 229 |
| Object | oci_fetch_assoc | data_psw |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
229.                                $data_psw    = array(
```

**Insufficiently Protected Credentials\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14102 |

| | |
|---|---|
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 238 |
| Object | oci_fetch_assoc | data_psw |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
238.                                        $result_psw_tid .= $this-
>file_interface_lib->generate_interface_psw_tid($data_psw);
```

**Insufficiently Protected Credentials\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14103 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 246 |
| Object | oci_fetch_assoc | psw_upd_tid |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
246.                                        $psw_upd_tid       .=
$result_psw_tid;
```

**Insufficiently Protected Credentials\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14104 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 458 |
| Object | oci_fetch_assoc | psw_upd_tid |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
458.                            $fwrite_result = fwrite($handle,
$psw_upd_tid);
```

**Insufficiently Protected Credentials\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14105 |

| | |
|---|---|
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 449 |
| Object | oci_fetch_assoc | psw_upd_tid |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
449.                    if ($psw_upd_tid != '') {
```

**Insufficiently Protected Credentials\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14106 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 189 |
| Object | oci_fetch_assoc | data_psw |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
189.                                $data_psw          = array(
```

**Insufficiently Protected Credentials\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14107 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 213 |
| Object | oci_fetch_assoc | data_psw |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
213.                                $result_psw_mid = $this->file_interface_lib->generate_interface_psw_mid($data_psw);
```

**Insufficiently Protected Credentials\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14108 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 219 |
| Object | oci_fetch_assoc | psw_upd_mid |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
219.                                        $psw_upd_mid .=
$result_psw_mid;
```

**Insufficiently Protected Credentials\Path 49:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14109
Status New

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 421 |
| Object | oci_fetch_assoc | psw_upd_mid |

Code Snippet
File Name system/database/drivers/oci8/oci8_result.php
Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
421.                        $fwrite_result = fwrite($handle,
$psw_upd_mid);
```

**Insufficiently Protected Credentials\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14110 |
| Status | New |

Method _fetch_assoc at line 152 of system/database/drivers/oci8/oci8_result.php gets a user password from the oci_fetch_assoc element. This element's value then flows through the code without being encrypted and is written to the database in interface_ubah_data at line 16 of application/controllers/maintenance_scheduler.php. This may enable passwords to be stolen by an attacker.

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/oci8/oci8_result.php | application/controllers/maintenance_scheduler.php |
| Line | 155 | 412 |
| Object | oci_fetch_assoc | psw_upd_mid |

Code Snippet

File Name system/database/drivers/oci8/oci8_result.php

Method protected function _fetch_assoc()

```
....
155.                return oci_fetch_assoc($id);
```

File Name application/controllers/maintenance_scheduler.php

Method public function interface_ubah_data($pass = '')

```
....
412.                    if ($psw_upd_mid != '') {
```

## Use of Broken or Risky Cryptographic Algorithm

Query Path:

PHP\Cx\Php Low Visibility\Use of Broken or Risky Cryptographic Algorithm Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Configuration Management
NIST SP 800-53: SC-13 Cryptographic Protection (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A2-Cryptographic Failures

*Description*

**Use of Broken or Risky Cryptographic Algorithm\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17003 |
| Status | New |

In md5_16, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in system/helpers/dompdf/lib/class.pdf.php at line 1704.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/lib/class.pdf.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 1705 | 1705 |
| Object | md5 | md5 |

Code Snippet
File Name system/helpers/dompdf/lib/class.pdf.php
Method function md5_16($string) {

```
....
1705.      $tmp =  md5($string);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17004 |
| Status | New |

In edit_user, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/controllers/user.php at line 506.

| | Source | Destination |
|---|---|---|
| File | application/controllers/user.php | application/controllers/user.php |
| Line | 528 | 528 |
| Object | md5 | md5 |

Code Snippet
File Name application/controllers/user.php
Method public function edit_user()

```
....
528.                    $datadb['password'] = md5($password);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17005 |
| Status | New |

In ubah_password, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/controllers/user.php at line 631.

| | Source | Destination |
|---|---|---|
| File | application/controllers/user.php | application/controllers/user.php |
| Line | 636 | 636 |
| Object | md5 | md5 |

Code Snippet
File Name application/controllers/user.php
Method public function ubah_password()

```
....
636.                    $pass_old = md5($this->input->post('pass_old'));
```

**Use of Broken or Risky Cryptographic Algorithm\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17006 |
| Status | New |

In ubah_password, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/controllers/user.php at line 631.

| | Source | Destination |
|---|---|---|
| File | application/controllers/user.php | application/controllers/user.php |
| Line | 637 | 637 |
| Object | md5 | md5 |

Code Snippet
File Name application/controllers/user.php
Method public function ubah_password()

```
....
637.                    $password = md5($this->input->post('password'));
```

**Use of Broken or Risky Cryptographic Algorithm\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17007 |
| Status | New |

In setCredentials, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.soap_transport_http.php at line 468.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soap_transport_http.php | application/libraries/nusoap/class.soap_transport_http.php |
| Line | 486 | 486 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.soap_transport_http.php
Method function setCredentials($username, $password, $authtype = 'basic', $digestRequest = array(), $certRequest = array()) {

```
....
486.                            $HA1 = md5($A1);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17008 |
| Status | New |

In setCredentials, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.soap_transport_http.php at line 468.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soap_transport_http.php | application/libraries/nusoap/class.soap_transport_http.php |
| Line | 492 | 492 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.soap_transport_http.php
Method function setCredentials($username, $password, $authtype = 'basic', $digestRequest = array(), $certRequest = array()) {

```
....
492.                            $HA2 =  md5($A2);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17009 |
| Status | New |

In setCredentials, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.soap_transport_http.php at line 468.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.soap_transport_http.php | application/libraries/nusoap/class.soap_transport_http.php |
| Line | 514 | 514 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.soap_transport_http.php
Method function setCredentials($username, $password, $authtype = 'basic', $digestRequest = array(), $certRequest = array()) {

```
....
514.                            $hashedDigest = md5($unhashedDigest);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17010 |
| Status | New |

In createFilename, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.wsdlcache.php at line 60.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.wsdlcache.php | application/libraries/nusoap/class.wsdlcache.php |
| Line | 61 | 61 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.wsdlcache.php
Method function createFilename($wsdl) {

```
....
61.         return $this->cache_dir.'/wsdlcache-' . md5($wsdl);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17011 |
| Status | New |

In obtainMutex, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.wsdlcache.php at line 124.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.wsdlcache.php | application/libraries/nusoap/class.wsdlcache.php |
| Line | 125 | 125 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.wsdlcache.php
Method function obtainMutex($filename, $mode) {

```
....
125.                if (isset($this->fplock[md5($filename)])) {
```

**Use of Broken or Risky Cryptographic Algorithm\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17012 |
| Status | New |

In obtainMutex, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.wsdlcache.php at line 124.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.wsdlcache.php | application/libraries/nusoap/class.wsdlcache.php |
| Line | 129 | 129 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.wsdlcache.php
Method function obtainMutex($filename, $mode) {

```
....
129.                $this->fplock[md5($filename)] =
fopen($filename.".lock", "w");
```

**Use of Broken or Risky Cryptographic Algorithm\Path 11:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17013 |
| Status | New |

In obtainMutex, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.wsdlcache.php at line 124.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.wsdlcache.php | application/libraries/nusoap/class.wsdlcache.php |
| Line | 131 | 131 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.wsdlcache.php
Method function obtainMutex($filename, $mode) {

```
....
131.                    return flock($this->fplock[md5($filename)],
LOCK_SH);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17014 |
| Status | New |

In obtainMutex, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.wsdlcache.php at line 124.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.wsdlcache.php | application/libraries/nusoap/class.wsdlcache.php |
| Line | 133 | 133 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.wsdlcache.php
Method function obtainMutex($filename, $mode) {

```
....
133.                    return flock($this->fplock[md5($filename)],
LOCK_EX);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17015 |
| Status | New |

In releaseMutex, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.wsdlcache.php at line 172.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.wsdlcache.php | application/libraries/nusoap/class.wsdlcache.php |
| Line | 173 | 173 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.wsdlcache.php
Method function releaseMutex($filename) {

```
....
173.            $ret = flock($this->fplock[md5($filename)], LOCK_UN);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17016 |
| Status | New |

In releaseMutex, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.wsdlcache.php at line 172.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.wsdlcache.php | application/libraries/nusoap/class.wsdlcache.php |
| Line | 174 | 174 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.wsdlcache.php
Method function releaseMutex($filename) {

```
....
174.            fclose($this->fplock[md5($filename)]);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17017 |
| Status | New |

In releaseMutex, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/class.wsdlcache.php at line 172.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/class.wsdlcache.php | application/libraries/nusoap/class.wsdlcache.php |
| Line | 175 | 175 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/class.wsdlcache.php
Method function releaseMutex($filename) {

```
....
175.                unset($this->fplock[md5($filename)]);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17018 |
| Status | New |

In setCredentials, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/nusoap.php at line 2622.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 2640 | 2640 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/nusoap.php
Method function setCredentials($username, $password, $authtype = 'basic', $digestRequest = array(), $certRequest = array()) {

```
....
2640.                        $HA1 = md5($A1);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17019 |
| Status | New |

In setCredentials, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/nusoap.php at line 2622.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 2646 | 2646 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/nusoap.php
Method function setCredentials($username, $password, $authtype = 'basic', $digestRequest = array(), $certRequest = array()) {

```
....
2646.                        $HA2 =  md5($A2);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17020 |
| Status | New |

In setCredentials, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/nusoap.php at line 2622.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoap.php | application/libraries/nusoap/nusoap.php |
| Line | 2668 | 2668 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/nusoap.php
Method function setCredentials($username, $password, $authtype = 'basic', $digestRequest = array(), $certRequest = array()) {

```
....
2668.                        $hashedDigest = md5($unhashedDigest);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17021 |
| Status | New |

In addAttachment, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/nusoapmime.php at line 88.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoapmime | application/libraries/nusoap/nusoapmime |

| | | |
|---|---|---|
| | .php | .php |
| Line | 90 | 90 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/nusoapmime.php
Method function addAttachment($data, $filename = '', $contenttype = 'application/octet-stream', $cid = false) {

```
....
90.                 $cid = md5(uniqid(time()));
```

**Use of Broken or Risky Cryptographic Algorithm\Path 20:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17022
Status New

In addAttachment, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/libraries/nusoap/nusoapmime.php at line 318.

| | Source | Destination |
|---|---|---|
| File | application/libraries/nusoap/nusoapmime.php | application/libraries/nusoap/nusoapmime.php |
| Line | 320 | 320 |
| Object | md5 | md5 |

Code Snippet
File Name application/libraries/nusoap/nusoapmime.php
Method function addAttachment($data, $filename = '', $contenttype = 'application/octet-stream', $cid = false) {

```
....
320.                    $cid = md5(uniqid(time()));
```

**Use of Broken or Risky Cryptographic Algorithm\Path 21:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17023
Status New

In userCheck, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/models/user_model.php at line 10.

| | Source | Destination |
|---|---|---|
| File | application/models/user_model.php | application/models/user_model.php |

| | | |
|---|---|---|
| Line | 12 | 12 |
| Object | md5 | md5 |

Code Snippet
File Name application/models/user_model.php
Method public function userCheck($username, $password)

```
....
12.         $query = "SELECT * FROM user_data WHERE active_status = 1
and username='".$username."' and password='".md5($password)."'";
```

**Use of Broken or Risky Cryptographic Algorithm\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17024 |
| Status | New |

In get_user_non_bri, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/models/user_model.php at line 34.

| | Source | Destination |
|---|---|---|
| File | application/models/user_model.php | application/models/user_model.php |
| Line | 43 | 43 |
| Object | md5 | md5 |

Code Snippet
File Name application/models/user_model.php
Method public function get_user_non_bri($username, $password)

```
....
43.         $this->db->where('password', md5($password));
```

**Use of Broken or Risky Cryptographic Algorithm\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17025 |
| Status | New |

In register_font, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/dompdf/include/font_metrics.cls.php at line 309.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/font_metrics.cls.php | application/third_party/dompdf/include/font_metrics.cls.php |
| Line | 318 | 318 |
| Object | md5 | md5 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/dompdf/include/font_metrics.cls.php |
| Method | static function register_font($style, $remote_file) { |

```
....
318.      $local_file = DOMPDF_FONT_DIR . md5($remote_file);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17026 |
| Status | New |

In md5_16, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/dompdf/lib/class.pdf.php at line 1710.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/lib/class.pdf.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 1711 | 1711 |
| Object | md5 | md5 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/dompdf/lib/class.pdf.php |
| Method | function md5_16($string) { |

```
....
1711.      $tmp = md5($string);
```

**Use of Broken or Risky Cryptographic Algorithm\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17027 |
| Status | New |

In copyCellCollection, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/CachedObjectStorage/APC.php at line 203.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/APC.php | application/third_party/PHPExcel/CachedObjectStorage/APC.php |
| Line | 207 | 207 |
| Object | md5 | md5 |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/PHPExcel/CachedObjectStorage/APC.php |
| Method | public function copyCellCollection(PHPExcel_Worksheet $parent) { |

```
....
207.          $newCachePrefix = substr(md5($baseUnique),0,8).'.';
```

**Use of Broken or Risky Cryptographic Algorithm\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17028 |
| Status | New |

In __construct, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/CachedObjectStorage/APC.php at line 254.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/APC.php | application/third_party/PHPExcel/CachedObjectStorage/APC.php |
| Line | 259 | 259 |
| Object | md5 | md5 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/PHPExcel/CachedObjectStorage/APC.php |
| Method | public function __construct(PHPExcel_Worksheet $parent, $arguments) { |

```
....
259.              $this->_cachePrefix =
substr(md5($baseUnique),0,8).'.';
```

**Use of Broken or Risky Cryptographic Algorithm\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17029 |
| Status | New |

In copyCellCollection, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/CachedObjectStorage/Memcache.php at line 204.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php |
| Line | 208 | 208 |
| Object | md5 | md5 |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php |
| Method | public function copyCellCollection(PHPExcel_Worksheet $parent) { |

```
....
208.                $newCachePrefix = substr(md5($baseUnique),0,8).'.';
```

**Use of Broken or Risky Cryptographic Algorithm\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17030 |
| Status | New |

In __construct, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/CachedObjectStorage/Memcache.php at line 255.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php |
| Line | 262 | 262 |
| Object | md5 | md5 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/PHPExcel/CachedObjectStorage/Memcache.php |
| Method | public function __construct(PHPExcel_Worksheet $parent, $arguments) { |

```
....
262.                    $this->_cachePrefix =
substr(md5($baseUnique),0,8).'.';
```

**Use of Broken or Risky Cryptographic Algorithm\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17031 |
| Status | New |

In copyCellCollection, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/CachedObjectStorage/Wincache.php at line 204.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Wincache.php | application/third_party/PHPExcel/CachedObjectStorage/Wincache.php |
| Line | 208 | 208 |
| Object | md5 | md5 |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/PHPExcel/CachedObjectStorage/Wincache.php |
| Method | public function copyCellCollection(PHPExcel_Worksheet $parent) { |

```
....
208.                $newCachePrefix = substr(md5($baseUnique),0,8).'.';
```

**Use of Broken or Risky Cryptographic Algorithm\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17032 |
| Status | New |

In __construct, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/CachedObjectStorage/Wincache.php at line 256.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/CachedObjectStorage/Wincache.php | application/third_party/PHPExcel/CachedObjectStorage/Wincache.php |
| Line | 261 | 261 |
| Object | md5 | md5 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/PHPExcel/CachedObjectStorage/Wincache.php |
| Method | public function __construct(PHPExcel_Worksheet $parent, $arguments) { |

```
....
261.                    $this->_cachePrefix =
substr(md5($baseUnique),0,8).'.';
```

**Use of Broken or Risky Cryptographic Algorithm\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17033 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Cell/DataValidation.php at line 440.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Cell/DataValidation.php | application/third_party/PHPExcel/Cell/DataValidation.php |
| Line | 441 | 441 |
| Object | md5 | md5 |

Code Snippet

| | |
|---|---|
| File Name | application/third_party/PHPExcel/Cell/DataValidation.php |
| Method | public function getHashCode() { |

```
....
441.            return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17034 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Cell/Hyperlink.php at line 119.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Cell/Hyperlink.php | application/third_party/PHPExcel/Cell/Hyperlink.php |
| Line | 120 | 120 |
| Object | md5 | md5 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/PHPExcel/Cell/Hyperlink.php |
| Method | public function getHashCode() { |

```
....
120.            return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17035 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Comment.php at line 289.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Comment.php | application/third_party/PHPExcel/Comment.php |
| Line | 290 | 290 |
| Object | md5 | md5 |

| | |
|---|---|
| Code Snippet | |
| File Name | application/third_party/PHPExcel/Comment.php |
| Method | public function getHashCode() { |

```
....
290.            return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17036 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/RichText.php at line 172.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/RichText.php | application/third_party/PHPExcel/RichText.php |
| Line | 179 | 179 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/RichText.php

Method public function getHashCode()

```
....
179.            return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17037 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/RichText/Run.php at line 81.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/RichText/Run.php | application/third_party/PHPExcel/RichText/Run.php |
| Line | 82 | 82 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/RichText/Run.php

Method public function getHashCode() {

```
....
82.         return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17038 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/RichText/TextElement.php at line 88.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/RichText/TextElement.php | application/third_party/PHPExcel/RichText/TextElement.php |
| Line | 89 | 89 |
| Object | md5 | md5 |

Code Snippet
File Name application/third_party/PHPExcel/RichText/TextElement.php
Method public function getHashCode() {

```
....
89.         return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17039 |
| Status | New |

In calculate, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Shared/trend/trendClass.php at line 87.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Shared/trend/trendClass.php | application/third_party/PHPExcel/Shared/trend/trendClass.php |
| Line | 101 | 101 |
| Object | md5 | md5 |

Code Snippet
File Name application/third_party/PHPExcel/Shared/trend/trendClass.php
Method public static function calculate($trendType=self::TREND_BEST_FIT, $yValues, $xValues=array(), $const=True) {

```
....
101.                $key =
md5($trendType.$const.serialize($yValues).serialize($xValues));
```

**Use of Broken or Risky Cryptographic Algorithm\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17040 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Style.php at line 574.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Style.php | application/third_party/PHPExcel/Style.php |
| Line | 581 | 581 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/Style.php

Method public function getHashCode()

```
....
581.            return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17041 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Style/Alignment.php at line 394.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Style/Alignment.php | application/third_party/PHPExcel/Style/Alignment.php |
| Line | 398 | 398 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/Style/Alignment.php

Method public function getHashCode() {

```
....
398.                return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17042 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Style/Border.php at line 283.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Style/Border.php | application/third_party/PHPExcel/Style/Border.php |
| Line | 287 | 287 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/Style/Border.php

Method public function getHashCode() {

```
....
287.                return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17043 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Style/Borders.php at line 409.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Style/Borders.php | application/third_party/PHPExcel/Style/Borders.php |
| Line | 413 | 413 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/Style/Borders.php

Method public function getHashCode() {

```
....
413.        return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17044 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Style/Color.php at line 419.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Style/Color.php | application/third_party/PHPExcel/Style/Color.php |
| Line | 423 | 423 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/Style/Color.php

Method public function getHashCode() {

```
....
423.            return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17045 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Style/Conditional.php at line 254.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Style/Conditional.php | application/third_party/PHPExcel/Style/Conditional.php |
| Line | 255 | 255 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/Style/Conditional.php

Method public function getHashCode() {

```
....
255.        return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17046 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Style/Fill.php at line 308.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Style/Fill.php | application/third_party/PHPExcel/Style/Fill.php |
| Line | 312 | 312 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/Style/Fill.php

Method public function getHashCode() {

```
....
312.            return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17047 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Style/Font.php at line 514.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Style/Font.php | application/third_party/PHPExcel/Style/Font.php |
| Line | 518 | 518 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/Style/Font.php

Method public function getHashCode() {

```
....
518.                return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17048 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Style/NumberFormat.php at line 360.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Style/NumberFormat.php | application/third_party/PHPExcel/Style/NumberFormat.php |
| Line | 365 | 365 |
| Object | md5 | md5 |

Code Snippet
File Name application/third_party/PHPExcel/Style/NumberFormat.php
Method public function getHashCode()

```
....
365.                return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17049 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Style/Protection.php at line 196.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Style/Protection.php | application/third_party/PHPExcel/Style/Protection.php |
| Line | 200 | 200 |
| Object | md5 | md5 |

Code Snippet
File Name application/third_party/PHPExcel/Style/Protection.php
Method public function getHashCode() {

```
....
200.        return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17050 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Worksheet.php at line 2570.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Worksheet.php | application/third_party/PHPExcel/Worksheet.php |
| Line | 2572 | 2572 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/Worksheet.php

Method public function getHashCode() {

```
....
2572.              $this->_hash = md5( $this->_title .
```

**Use of Broken or Risky Cryptographic Algorithm\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17051 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Worksheet/BaseDrawing.php at line 456.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Worksheet/BaseDrawing.php | application/third_party/PHPExcel/Worksheet/BaseDrawing.php |
| Line | 457 | 457 |
| Object | md5 | md5 |

Code Snippet

File Name application/third_party/PHPExcel/Worksheet/BaseDrawing.php

Method public function getHashCode() {

```
....
457.        return md5(
```

**Use of Broken or Risky Cryptographic Algorithm\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=17052 |
| Status | New |

In getHashCode, the application protects sensitive data using a cryptographic algorithm, md5, that is considered weak or even trivially broken, in application/third_party/PHPExcel/Worksheet/Drawing.php at line 127.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Worksheet/Drawing.php | application/third_party/PHPExcel/Worksheet/Drawing.php |
| Line | 128 | 128 |
| Object | md5 | md5 |

Code Snippet
File Name application/third_party/PHPExcel/Worksheet/Drawing.php
Method public function getHashCode() {

```
....
128.        return md5(
```

## Use Of Hardcoded Password

Query Path:
PHP\Cx\Php Low Visibility\Use Of Hardcoded Password Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage
OWASP Top 10 2013: A2-Broken Authentication and Session Management
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A2-Broken Authentication
OWASP Top 10 2021: A7-Identification and Authentication Failures

*Description*

**Use Of Hardcoded Password\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13308 |
| Status | New |

The application uses a single, hard-coded password "dbMMSPSB123" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of

application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 52 | 52 |
| Object | "dbMMSPSB123" | "dbMMSPSB123" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
52.  $db['default']['password'] = 'dbMMSPSB123';
```

**Use Of Hardcoded Password\Path 2:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13309
Status New

The application uses a single, hard-coded password "mms" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 106 | 106 |
| Object | "mms" | "mms" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
106.  $db['dwh']['password'] = 'mms';
```

**Use Of Hardcoded Password\Path 3:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13310
Status New

The application uses a single, hard-coded password "officelinux123" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 122 | 122 |
| Object | "officelinux123" | "officelinux123" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
122.  $db['portalsdm']['password'] = 'officelinux123';
```

**Use Of Hardcoded Password\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13311 |
| Status | New |

The application uses a single, hard-coded password "P@ssw0rd" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 154 | 154 |
| Object | "P@ssw0rd" | "P@ssw0rd" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
154.  $db['antasena']['password'] = 'P@ssw0rd';
```

**Use Of Hardcoded Password\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13312 |
| Status | New |

The application uses a single, hard-coded password "P@ssw0rd" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |

| | | |
|---|---|---|
| Line | 171 | 171 |
| Object | "P@ssw0rd" | "P@ssw0rd" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
171.  $db['cl']['password'] = 'P@ssw0rd';
```

**Use Of Hardcoded Password\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13313 |
| Status | New |

The application uses a single, hard-coded password "P@ssw0rd" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 188 | 188 |
| Object | "P@ssw0rd" | "P@ssw0rd" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
188.  $db['cl_mirror']['password'] = 'P@ssw0rd';
```

**Use Of Hardcoded Password\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13314 |
| Status | New |

The application uses a single, hard-coded password "SIMATDB123" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 205 | 205 |

| | | |
|---|---|---|
| Object | "SIMATDB123" | "SIMATDB123" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
205.  $db['dbsimat']['password'] = 'SIMATDB123';
```

**Use Of Hardcoded Password\Path 8:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13315
Status New

The application uses a single, hard-coded password "P@ssw0rd" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 221 | 221 |
| Object | "P@ssw0rd" | "P@ssw0rd" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
221.  $db['eform']['password'] = 'P@ssw0rd';
```

**Use Of Hardcoded Password\Path 9:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13316
Status New

The application uses a single, hard-coded password "P@ssw0rd" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 254 | 254 |
| Object | "P@ssw0rd" | "P@ssw0rd" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
254.  $db['rekon_visa']['password'] = "P@ssw0rd";
```

**Use Of Hardcoded Password\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13317 |
| Status | New |

The application uses a single, hard-coded password "P@ssw0rd" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 288 | 288 |
| Object | "P@ssw0rd" | "P@ssw0rd" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
288.  $db['ebor']['password'] = 'P@ssw0rd';
```

**Use Of Hardcoded Password\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13318 |
| Status | New |

The application uses a single, hard-coded password "P@ssw0rd" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 304 | 304 |
| Object | "P@ssw0rd" | "P@ssw0rd" |

Code Snippet
File Name application/config/database.php

| | |
|---|---|
| Method | <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed'); |

```
....
304.  $db['rekon']['password'] = 'P@ssw0rd';
```

**Use Of Hardcoded Password\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13319 |
| Status | New |

The application uses a single, hard-coded password "brisa12" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 320 | 320 |
| Object | "brisa12" | "brisa12" |

| | |
|---|---|
| Code Snippet | |
| File Name | application/config/database.php |
| Method | <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed'); |

```
....
320.  $db['sv']['password'] = 'brisa12';
```

**Use Of Hardcoded Password\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13320 |
| Status | New |

The application uses a single, hard-coded password "dbMMSPSB123" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 352 | 352 |
| Object | "dbMMSPSB123" | "dbMMSPSB123" |

| | |
|---|---|
| Code Snippet | |
| File Name | application/config/database.php |
| Method | <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed'); |

```
....
352.  $db['edcpro']['password'] = 'dbMMSPSB123';
```

**Use Of Hardcoded Password\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13321 |
| Status | New |

The application uses a single, hard-coded password "P@ssw0rd321" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 384 | 384 |
| Object | "P@ssw0rd321" | "P@ssw0rd321" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
384.  $db['riskalert']['password'] = 'P@ssw0rd321';
```

**Use Of Hardcoded Password\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13322 |
| Status | New |

The application uses a single, hard-coded password "P@ssw0rd" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 400 | 400 |
| Object | "P@ssw0rd" | "P@ssw0rd" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
400.  $db['msb_par']['password'] = 'P@ssw0rd';
```

**Use Of Hardcoded Password\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13323 |
| Status | New |

The application uses a single, hard-coded password "P@ssw0rd" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 419 | 419 |
| Object | "P@ssw0rd" | "P@ssw0rd" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
419.  $db['crm']['password'] = 'P@ssw0rd';
```

**Use Of Hardcoded Password\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13324 |
| Status | New |

The application uses a single, hard-coded password "mms" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 435 | 435 |
| Object | "mms" | "mms" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
435.  $db['crm_new']['password'] = 'mms';
```

**Use Of Hardcoded Password\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13325 |
| Status | New |

The application uses a single, hard-coded password "P@ssw0rd" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 452 | 452 |
| Object | "P@ssw0rd" | "P@ssw0rd" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
452.  $db['echannel']['password'] = 'P@ssw0rd';
```

**Use Of Hardcoded Password\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13326 |
| Status | New |

The application uses a single, hard-coded password "P@ssw0rd4145" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/database.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/database.php | application/config/database.php |
| Line | 469 | 469 |
| Object | "P@ssw0rd4145" | "P@ssw0rd4145" |

Code Snippet
File Name application/config/database.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
469.  $db['email']['password'] = 'P@ssw0rd4145';
```

**Use Of Hardcoded Password\Path 20:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13327 |
| Status | New |

The application uses a single, hard-coded password "pswaix" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 144 of application/controllers/inisiasi.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi.php | application/controllers/inisiasi.php |
| Line | 182 | 182 |
| Object | "pswaix" | "pswaix" |

Code Snippet
File Name application/controllers/inisiasi.php
Method public function export_approve_process()

```
....
182.                    $conn['password'] = 'pswaix';
```

**Use Of Hardcoded Password\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13328 |
| Status | New |

The application uses a single, hard-coded password "pptpsb" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 143 of application/controllers/restore.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/restore.php | application/controllers/restore.php |
| Line | 149 | 149 |
| Object | "pptpsb" | "pptpsb" |

Code Snippet
File Name application/controllers/restore.php
Method public function backup_file()

```
....
149.                $config['password'] = 'pptpsb';
```

**Use Of Hardcoded Password\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13329 |

| | |
|---|---|
| Status | New |

The application uses a single, hard-coded password "25d55ad283aa400af464c76d713c07ad" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 257 of application/controllers/user.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/user.php | application/controllers/user.php |
| Line | 290 | 290 |
| Object | "25d55ad283aa400af464c76d713c07ad" | "25d55ad283aa400af464c76d713c07ad" |

Code Snippet
File Name application/controllers/user.php
Method public function add_user()

```
....
290.                                $datadb['password'] =
'25d55ad283aa400af464c76d713c07ad';
```

**Use Of Hardcoded Password\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13330 |
| Status | New |

The application uses a single, hard-coded password "25d55ad283aa400af464c76d713c07ad" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 648 of application/controllers/user.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/user.php | application/controllers/user.php |
| Line | 694 | 694 |
| Object | "25d55ad283aa400af464c76d713c07ad" | "25d55ad283aa400af464c76d713c07ad" |

Code Snippet
File Name application/controllers/user.php
Method public function add_user_upload()

```
....
694.                                $data_user['password']        =
'25d55ad283aa400af464c76d713c07ad';
```

**Use Of Hardcoded Password\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13331 |
| Status | New |

The application uses a single, hard-coded password "pswaix" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 144 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi.php |
| Line | 182 | 182 |
| Object | "pswaix" | "pswaix" |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi.php
Method public function export_approve_process()

```
....
182.                    $conn['password'] = 'pswaix';
```

**Use Of Hardcoded Password\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13332 |
| Status | New |

The application uses a single, hard-coded password "pptpsb" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 143 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php |
| Line | 149 | 149 |
| Object | "pptpsb" | "pptpsb" |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/restore.php
Method public function backup_file()

```
....
149.                $config['password'] = 'pptpsb';
```

**Use Of Hardcoded Password\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13333 |
| Status | New |

The application uses a single, hard-coded password "25d55ad283aa400af464c76d713c07ad" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 257 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php |
| Line | 290 | 290 |
| Object | "25d55ad283aa400af464c76d713c07ad" | "25d55ad283aa400af464c76d713c07ad" |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php
Method public function add_user()

```
....
290.                                $datadb['password'] =
'25d55ad283aa400af464c76d713c07ad';
```

**Use Of Hardcoded Password\Path 27:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13334
Status New

The application uses a single, hard-coded password "25d55ad283aa400af464c76d713c07ad" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 644 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php |
| Line | 690 | 690 |
| Object | "25d55ad283aa400af464c76d713c07ad" | "25d55ad283aa400af464c76d713c07ad" |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/user.php
Method public function add_user_upload()

```
....
690.                                $data_user['password']        =
'25d55ad283aa400af464c76d713c07ad';
```

**Use Of Hardcoded Password\Path 28:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13335
Status New

The application uses a single, hard-coded password "pswaix" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/config.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/config.php | application/config/config.php |
| Line | 371 | 371 |
| Object | "pswaix" | "pswaix" |

Code Snippet
File Name application/config/config.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
371.  $config['psw_user'] = 'pswaix';
```

**Use Of Hardcoded Password\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13336 |
| Status | New |

The application uses a single, hard-coded password "pswaix" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1 of application/config/config_20210615.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/config/config_20210615.php | application/config/config_20210615.php |
| Line | 371 | 371 |
| Object | "pswaix" | "pswaix" |

Code Snippet
File Name application/config/config_20210615.php
Method <?php if ( ! defined('BASEPATH')) exit('No direct script access allowed');

```
....
371.  $config['psw_user'] = 'pswaix';
```

**Use Of Hardcoded Password\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13337 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1450 of

application/controllers/inisiasi_scheduler.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler.php | application/controllers/inisiasi_scheduler.php |
| Line | 1602 | 1602 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1602.
      $log_temp['psw_mid_log'] = "---";
```

**Use Of Hardcoded Password\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13338 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1450 of application/controllers/inisiasi_scheduler.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler.php | application/controllers/inisiasi_scheduler.php |
| Line | 1621 | 1621 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1621.
      $log_temp['psw_jcb_log'] = "---";
```

**Use Of Hardcoded Password\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13339 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1450 of application/controllers/inisiasi_scheduler.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler.php | application/controllers/inisiasi_scheduler.php |
| Line | 1628 | 1628 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1628.                                          $log_temp['psw_mid_log']
      = "---";
```

**Use Of Hardcoded Password\Path 33:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13340
Status New

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1450 of application/controllers/inisiasi_scheduler.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler.php | application/controllers/inisiasi_scheduler.php |
| Line | 1629 | 1629 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1629.                                          $log_temp['psw_jcb_log']
      = "---";
```

**Use Of Hardcoded Password\Path 34:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13341
Status New

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1450 of application/controllers/inisiasi_scheduler.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler.php | application/controllers/inisiasi_scheduler.php |
| Line | 1668 | 1668 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler.php
Method function check_inisiasi_new()

```
....
1668.                                                $log_temp['psw_tid_log']
= "---";
```

**Use Of Hardcoded Password\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13342 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1317 of application/controllers/inisiasi_scheduler_20161206.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler_20161206.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 1469 | 1469 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler_20161206.php
Method function check_inisiasi_new()

```
....
1469.
      $log_temp['psw_mid_log'] = "---";
```

**Use Of Hardcoded Password\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13343 |

| | |
|---|---|
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1317 of application/controllers/inisiasi_scheduler_20161206.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler_20161206.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 1489 | 1489 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler_20161206.php
Method function check_inisiasi_new()

```
....
1489.
      $log_temp['psw_jcb_log'] = "---";
```

**Use Of Hardcoded Password\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13344 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1317 of application/controllers/inisiasi_scheduler_20161206.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler_20161206.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 1491 | 1491 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler_20161206.php
Method function check_inisiasi_new()

```
....
1491.
$log_temp['psw_jcb_log'] = "---";
```

**Use Of Hardcoded Password\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=13345 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1317 of application/controllers/inisiasi_scheduler_20161206.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler_20161206.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 1497 | 1497 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler_20161206.php
Method function check_inisiasi_new()

```
....
1497.                                        $log_temp['psw_mid_log']
      = "---";
```

**Use Of Hardcoded Password\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13346 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1317 of application/controllers/inisiasi_scheduler_20161206.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler_20161206.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 1498 | 1498 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler_20161206.php
Method function check_inisiasi_new()

```
....
1498.                                        $log_temp['psw_jcb_log']
      = "---";
```

**Use Of Hardcoded Password\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13347 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1317 of application/controllers/inisiasi_scheduler_20161206.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler_20161206.php | application/controllers/inisiasi_scheduler_20161206.php |
| Line | 1537 | 1537 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler_20161206.php
Method function check_inisiasi_new()

```
....
1537.                                                $log_temp['psw_tid_log']
= "---";
```

**Use Of Hardcoded Password\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13348 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 943 of application/controllers/inisiasi_scheduler_not_yet_used.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler_not_yet_used.php | application/controllers/inisiasi_scheduler_not_yet_used.php |
| Line | 1064 | 1064 |
| Object | "---" | "---" |

Code Snippet
File Name application/controllers/inisiasi_scheduler_not_yet_used.php
Method function check_inisiasi_new()

```
....
1064.
      $log_temp['psw_mid_log'] = "---";
```

**Use Of Hardcoded Password\Path 42:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13349 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 943 of application/controllers/inisiasi_scheduler_not_yet_used.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler_not_yet_used.php | application/controllers/inisiasi_scheduler_not_yet_used.php |
| Line | 1070 | 1070 |
| Object | "---" | "---" |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/inisiasi_scheduler_not_yet_used.php |
| Method | function check_inisiasi_new() |

```
....
1070.                                          $log_temp['psw_mid_log']
      = "---";
```

**Use Of Hardcoded Password\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13350 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 943 of application/controllers/inisiasi_scheduler_not_yet_used.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/controllers/inisiasi_scheduler_not_yet_used.php | application/controllers/inisiasi_scheduler_not_yet_used.php |
| Line | 1102 | 1102 |
| Object | "---" | "---" |

| | |
|---|---|
| Code Snippet | |
| File Name | application/controllers/inisiasi_scheduler_not_yet_used.php |
| Method | function check_inisiasi_new() |

```
....
1102.                                          $log_temp['psw_tid_log']
= "---";
```

**Use Of Hardcoded Password\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13351 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 1602 | 1602 |
| Object | "---" | "---" |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1602.
      $log_temp['psw_mid_log'] = "---";
```

**Use Of Hardcoded Password\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13352 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 1621 | 1621 |
| Object | "---" | "---" |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1621.
      $log_temp['psw_jcb_log'] = "---";
```

**Use Of Hardcoded Password\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13353 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 1628 | 1628 |
| Object | "---" | "---" |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1628.                                          $log_temp['psw_mid_log']
      = "---";
```

**Use Of Hardcoded Password\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13354 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 1629 | 1629 |
| Object | "---" | "---" |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1629.                                          $log_temp['psw_jcb_log']
      = "---";
```

**Use Of Hardcoded Password\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13355 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1450 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php |
| Line | 1668 | 1668 |
| Object | "---" | "---" |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler.php

Method function check_inisiasi_new()

```
....
1668.                                        $log_temp['psw_tid_log']
= "---";
```

**Use Of Hardcoded Password\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13356 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Line | 1469 | 1469 |
| Object | "---" | "---" |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php

Method function check_inisiasi_new()

```
....
1469.
      $log_temp['psw_mid_log'] = "---";
```

**Use Of Hardcoded Password\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13357 |
| Status | New |

The application uses a single, hard-coded password "---" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 1317 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Line | 1489 | 1489 |
| Object | "---" | "---" |

Code Snippet

| | |
|---|---|
| File Name | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/inisiasi_scheduler_20161206.php |
| Method | function check_inisiasi_new() |

```
....
1489.
      $log_temp['psw_jcb_log'] = "---";
```

## Information Exposure Through an Error Message

Query Path:
PHP\Cx\Php Low Visibility\Information Exposure Through an Error Message Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.5 - Improper error handling
OWASP Top 10 2013: A5-Security Misconfiguration
FISMA 2014: Configuration Management
NIST SP 800-53: SI-11 Error Handling (P2)
OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 2021: A4-Insecure Design

*Description*

**Information Exposure Through an Error Message\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13582 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 141 | 4548 |
| Object | e | print |

Code Snippet
File Name application/third_party/dompdf/include/image_cache.cls.php
Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php
Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4548.                if (DEBUGPNG) print '[addPngFromFile unsupported
filter method '.$file.']';
```

**Information Exposure Through an Error Message\Path 2:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13583
Status New

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 137 | 4548 |
| Object | e | print |

Code Snippet
File Name system/helpers/dompdf/include/image_cache.cls.php
Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4548.                if (DEBUGPNG) print '[addPngFromFile unsupported
filter method '.$file.']';
```

**Information Exposure Through an Error Message\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13584 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 141 | 4539 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4539.                if (DEBUGPNG) print '[addPngFromFile unsupported
compression method '.$file.']';
```

**Information Exposure Through an Error Message\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13585 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 137 | 4539 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4539.                if (DEBUGPNG) print '[addPngFromFile unsupported
compression method '.$file.']';
```

**Information Exposure Through an Error Message\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13586 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 141 | 4620 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4620.                   if (DEBUGPNG) print '[addPngFromFile unsupported
transparency type '.$file.']';
```

**Information Exposure Through an Error Message\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13587 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 137 | 4620 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4620.                   if (DEBUGPNG) print '[addPngFromFile unsupported
transparency type '.$file.']';
```

**Information Exposure Through an Error Message\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=13588 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 141 | 4683 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4683.            if (DEBUGPNG) print '[addPngFromFile alpha channel not
supported: '.$info['colorType']].' '.$file.']';
```

**Information Exposure Through an Error Message\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13589 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 137 | 4683 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4683.            if (DEBUGPNG) print '[addPngFromFile alpha channel not
supported: '.$info['colorType']].' '.$file.']';
```

**Information Exposure Through an Error Message\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13590 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 141 | 4657 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4657.            if (DEBUGPNG) print '[addPngFromFile bit depth of 8 or
less is supported '.$file.']';
```

**Information Exposure Through an Error Message\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13591 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 137 | 4657 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4657.          if (DEBUGPNG) print '[addPngFromFile bit depth of 8 or
less is supported '.$file.']';
```

**Information Exposure Through an Error Message\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13592 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 141 | 4647 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4647.            if (DEBUGPNG) print '[addPngFromFile no support for interlaced images in pdf '.$file.']';
```

**Information Exposure Through an Error Message\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13593 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 137 | 4647 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4647.            if (DEBUGPNG) print '[addPngFromFile no support for interlaced images in pdf '.$file.']';
```

**Information Exposure Through an Error Message\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=13594 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 141 | 4638 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4638.            if (DEBUGPNG) print '[addPngFromFile information header
is missing '.$file.']';
```

**Information Exposure Through an Error Message\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13595 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 137 | 4638 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4638.            if (DEBUGPNG) print '[addPngFromFile information header
is missing '.$file.']';
```

**Information Exposure Through an Error Message\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13596 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 141 | 4501 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4501.            if (DEBUGPNG) print '[addPngFromFile this file does not
have a valid header '.$file.']';
```

**Information Exposure Through an Error Message\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13597 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of system/helpers/dompdf/lib/class.pdf.php, line 4479.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 137 | 4501 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0, $h = 0, &$data, $is_mask = false, $mask = null) {

```
....
4501.            if (DEBUGPNG) print '[addPngFromFile this file does not
have a valid header '.$file.']';
```

**Information Exposure Through an Error Message\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13598 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addImagePng of system/helpers/dompdf/lib/class.pdf.php, line 4210.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 141 | 4233 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addImagePng($file, $x, $y, $w = 0, $h = 0, &$img, $is_mask = false, $mask = null) {

```
....
4233.        if (DEBUGPNG) print '[addImagePng '.$file.']';
```

**Information Exposure Through an Error Message\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13599 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addImagePng of system/helpers/dompdf/lib/class.pdf.php, line 4210.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | system/helpers/dompdf/lib/class.pdf.php |
| Line | 137 | 4233 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name system/helpers/dompdf/lib/class.pdf.php

Method function addImagePng($file, $x, $y, $w = 0, $h = 0, &$img, $is_mask = false, $mask = null) {

```
....
4233.        if (DEBUGPNG) print '[addImagePng '.$file.']';
```

**Information Exposure Through an Error Message\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13600 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 141 | 4191 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4191.                if (DEBUGPNG) print '[addPngFromFile unsupported
filter method '.$file.']';
```

**Information Exposure Through an Error Message\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13601 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 137 | 4191 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4191.                if (DEBUGPNG) print '[addPngFromFile unsupported
filter method '.$file.']';
```

**Information Exposure Through an Error Message\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13602 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 141 | 4182 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4182.                if (DEBUGPNG) print '[addPngFromFile unsupported
compression method '.$file.']';
```

**Information Exposure Through an Error Message\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13603 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 137 | 4182 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4182.                if (DEBUGPNG) print '[addPngFromFile unsupported
compression method '.$file.']';
```

**Information Exposure Through an Error Message\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13604 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 141 | 4261 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4261.                   if (DEBUGPNG) print '[addPngFromFile unsupported
transparency type '.$file.']';
```

**Information Exposure Through an Error Message\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13605 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 137 | 4261 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4261.                   if (DEBUGPNG) print '[addPngFromFile unsupported
transparency type '.$file.']';
```

**Information Exposure Through an Error Message\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=13606 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 141 | 4324 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4324.            if (DEBUGPNG) print '[addPngFromFile alpha channel not
supported: '.$info['colorType'].' '.$file.']';
```

**Information Exposure Through an Error Message\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13607 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 137 | 4324 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4324.            if (DEBUGPNG) print '[addPngFromFile alpha channel not supported: '.$info['colorType'].' '.$file.']';
```

**Information Exposure Through an Error Message\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13608 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 141 | 4298 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4298.          if (DEBUGPNG) print '[addPngFromFile bit depth of 8 or less is supported '.$file.']';
```

**Information Exposure Through an Error Message\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13609 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 137 | 4298 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4298.          if (DEBUGPNG) print '[addPngFromFile bit depth of 8 or
less is supported '.$file.']';
```

**Information Exposure Through an Error Message\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13610 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 141 | 4288 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4288.            if (DEBUGPNG) print '[addPngFromFile no support for interlaced images in pdf '.$file.']';
```

**Information Exposure Through an Error Message\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13611 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 137 | 4288 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4288.            if (DEBUGPNG) print '[addPngFromFile no support for interlaced images in pdf '.$file.']';
```

**Information Exposure Through an Error Message\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=13612 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 141 | 4279 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4279.            if (DEBUGPNG) print '[addPngFromFile information header
is missing '.$file.']';
```

**Information Exposure Through an Error Message\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13613 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 137 | 4279 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4279.            if (DEBUGPNG) print '[addPngFromFile information header is missing '.$file.']';
```

**Information Exposure Through an Error Message\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13614 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 141 | 4144 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4144.            if (DEBUGPNG) print '[addPngFromFile this file does not have a valid header '.$file.']';
```

**Information Exposure Through an Error Message\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13615 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addPngFromBuf of application/third_party/dompdf/lib/class.pdf.php, line 4122.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 137 | 4144 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addPngFromBuf($file, $x, $y, $w = 0.0, $h = 0.0, &$data, $is_mask = false, $mask = null) {

```
....
4144.            if (DEBUGPNG) print '[addPngFromFile this file does not
have a valid header '.$file.']';
```

**Information Exposure Through an Error Message\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13616 |
| Status | New |

Method resolve_url, at line 47 of application/third_party/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addImagePng of application/third_party/dompdf/lib/class.pdf.php, line 3838.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 141 | 3865 |
| Object | e | print |

Code Snippet

File Name application/third_party/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $protocol, $host, $base_path, DOMPDF $dompdf) {

```
....
141.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addImagePng($file, $x, $y, $w = 0.0, $h = 0.0, &$img, $is_mask = false, $mask = null) {

```
....
3865.        if (DEBUGPNG) print '[addImagePng '.$file.']';
```

**Information Exposure Through an Error Message\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13617 |
| Status | New |

Method resolve_url, at line 45 of system/helpers/dompdf/include/image_cache.cls.php, handles an Exception or runtime Error e. During the exception handling code, the application exposes the exception details to print, in method addImagePng of application/third_party/dompdf/lib/class.pdf.php, line 3838.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/image_cache.cls.php | application/third_party/dompdf/lib/class.pdf.php |
| Line | 137 | 3865 |
| Object | e | print |

Code Snippet

File Name system/helpers/dompdf/include/image_cache.cls.php

Method static function resolve_url($url, $proto, $host, $base_path) {

```
....
137.        $message = $e->getMessage()." \n $url";
```

File Name application/third_party/dompdf/lib/class.pdf.php

Method function addImagePng($file, $x, $y, $w = 0.0, $h = 0.0, &$img, $is_mask = false, $mask = null) {

```
....
3865.        if (DEBUGPNG) print '[addImagePng '.$file.']';
```

**Information Exposure Through an Error Message\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13618 |
| Status | New |

Method _processTokenStack, at line 3089 of application/third_party/PHPExcel/Calculation.php, handles an Exception or runtime Error ex. During the exception handling code, the application exposes the exception details to echo, in method writeDebugLog of application/third_party/PHPExcel/CalcEngine/Logger.php, line 119.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Calculation.php | application/third_party/PHPExcel/CalcEngine/Logger.php |
| Line | 3219 | 125 |
| Object | ex | echo |

Code Snippet

File Name application/third_party/PHPExcel/Calculation.php

Method private function _processTokenStack($tokens, $cellID = NULL, PHPExcel_Cell $pCell = NULL) {

```
....
3219.                                                    $this->_debugLog-
>writeDebugLog('JAMA Matrix Exception: ', $ex->getMessage());
```

File Name application/third_party/PHPExcel/CalcEngine/Logger.php

Method public function writeDebugLog() {

```
....
125.                            echo $cellReference,
```

**Information Exposure Through an Error Message\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13619 |
| Status | New |

Method _processTokenStack, at line 3089 of application/third_party/PHPExcel/Calculation.php, handles an Exception or runtime Error ex. During the exception handling code, the application exposes the exception details to echo, in method writeDebugLog of application/third_party/PHPExcel/CalcEngine/Logger.php, line 119.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Calculation.php | application/third_party/PHPExcel/CalcEngine/Logger.php |
| Line | 3265 | 125 |
| Object | ex | echo |

Code Snippet

File Name application/third_party/PHPExcel/Calculation.php

Method private function _processTokenStack($tokens, $cellID = NULL, PHPExcel_Cell $pCell = NULL) {

```
....
3265.                                        $this->_debugLog-
>writeDebugLog('JAMA Matrix Exception: ', $ex->getMessage());
```

File Name application/third_party/PHPExcel/CalcEngine/Logger.php

Method public function writeDebugLog() {

```
....
125.                            echo $cellReference,
```

**Information Exposure Through an Error Message\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13620 |
| Status | New |

Method _executeNumericBinaryOperation, at line 3589 of application/third_party/PHPExcel/Calculation.php, handles an Exception or runtime Error ex. During the exception handling code, the application exposes the exception details to echo, in method writeDebugLog of application/third_party/PHPExcel/CalcEngine/Logger.php, line 119.

| | Source | Destination |
|---|---|---|
| File | application/third_party/PHPExcel/Calculation.php | application/third_party/PHPExcel/CalcEngine/Logger.php |
| Line | 3620 | 125 |
| Object | ex | echo |

Code Snippet

File Name application/third_party/PHPExcel/Calculation.php

Method private function _executeNumericBinaryOperation($cellID,$operand1,$operand2,$operation,$matrixFunction,&$stack) {

```
....
3620.                           $this->_debugLog->writeDebugLog('JAMA
Matrix Exception: ', $ex->getMessage());
```

File Name application/third_party/PHPExcel/CalcEngine/Logger.php

Method public function writeDebugLog() {

```
....
125.                            echo $cellReference,
```

**Information Exposure Through an Error Message\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13621 |
| Status | New |

Method <?php, at line 1 of index.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method <?php of index.php, line 1.

| | Source | Destination |
|---|---|---|
| File | index.php | index.php |
| Line | 12 | 12 |
| Object | error_reporting | error_reporting |

Code Snippet
File Name index.php
Method <?php

```
....
12.     error_reporting(E_ALL);
```

**Information Exposure Through an Error Message\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13622 |
| Status | New |

Method <?php, at line 1 of index.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method <?php of index.php, line 1.

| | Source | Destination |
|---|---|---|
| File | index.php | index.php |
| Line | 61 | 61 |
| Object | error_reporting | error_reporting |

Code Snippet
File Name index.php
Method <?php

```
....
61.             error_reporting(E_ALL);
```

**Information Exposure Through an Error Message\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13623 |
| Status | New |

Method bismod_list, at line 201 of application/controllers/admin.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method bismod_list of application/controllers/admin.php, line 201.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin.php | application/controllers/admin.php |
| Line | 205 | 205 |
| Object | error_reporting | error_reporting |

Code Snippet
File Name application/controllers/admin.php
Method public function bismod_list()

```
....
205.            error_reporting(E_ALL);
```

**Information Exposure Through an Error Message\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13624 |
| Status | New |

Method merchant_excel_generate, at line 2403 of application/controllers/admin.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method merchant_excel_generate of application/controllers/admin.php, line 2403.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin.php | application/controllers/admin.php |
| Line | 2406 | 2406 |
| Object | error_reporting | error_reporting |

Code Snippet
File Name application/controllers/admin.php
Method public function merchant_excel_generate()

```
....
2406.           error_reporting(E_ALL);
```

**Information Exposure Through an Error Message\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13625 |
| Status | New |

Method manage_pn_rm_merchant, at line 4951 of application/controllers/admin.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method manage_pn_rm_merchant of application/controllers/admin.php, line 4951.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | application/controllers/admin.php | application/controllers/admin.php |
| Line | 4960 | 4960 |
| Object | error_reporting | error_reporting |

Code Snippet
File Name application/controllers/admin.php
Method public function manage_pn_rm_merchant()

```
....
4960.             error_reporting(E_ALL);
```

**Information Exposure Through an Error Message\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13626 |
| Status | New |

Method merchant_excel_generate, at line 2105 of application/controllers/admin_paket_bismod.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method merchant_excel_generate of application/controllers/admin_paket_bismod.php, line 2105.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_paket_bismod.php | application/controllers/admin_paket_bismod.php |
| Line | 2108 | 2108 |
| Object | error_reporting | error_reporting |

Code Snippet
File Name application/controllers/admin_paket_bismod.php
Method public function merchant_excel_generate()

```
....
2108.             error_reporting(E_ALL);
```

**Information Exposure Through an Error Message\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13627 |
| Status | New |

Method manage_pn_rm_merchant, at line 4653 of application/controllers/admin_paket_bismod.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method manage_pn_rm_merchant of application/controllers/admin_paket_bismod.php, line 4653.

| | Source | Destination |
|---|---|---|
| File | application/controllers/admin_paket_bis | application/controllers/admin_paket_bis |

| | | |
|---|---|---|
| | mod.php | mod.php |
| Line | 4662 | 4662 |
| Object | error_reporting | error_reporting |

Code Snippet
File Name application/controllers/admin_paket_bismod.php
Method public function manage_pn_rm_merchant()

```
....
4662.            error_reporting(E_ALL);
```

**Information Exposure Through an Error Message\Path 47:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13628
Status New

Method __construct, at line 5 of application/controllers/automatic_deploy.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method __construct of application/controllers/automatic_deploy.php, line 5.

| | Source | Destination |
|---|---|---|
| File | application/controllers/automatic_deploy.php | application/controllers/automatic_deploy.php |
| Line | 12 | 12 |
| Object | error_reporting | error_reporting |

Code Snippet
File Name application/controllers/automatic_deploy.php
Method public function __construct()

```
....
12.         error_reporting(E_ALL);
```

**Information Exposure Through an Error Message\Path 48:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13629
Status New

Method __construct, at line 5 of application/controllers/scheduler.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method __construct of application/controllers/scheduler.php, line 5.

| | Source | Destination |
|---|---|---|
| File | application/controllers/scheduler.php | application/controllers/scheduler.php |
| Line | 14 | 14 |

| | | |
|---|---|---|
| Object | error_reporting | error_reporting |

Code Snippet
File Name application/controllers/scheduler.php
Method public function __construct()

```
....
14.         error_reporting(E_ALL);
```

**Information Exposure Through an Error Message\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13630 |
| Status | New |

Method merchant_excel_generate, at line 1999 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method merchant_excel_generate of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php, line 1999.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php |
| Line | 2002 | 2002 |
| Object | error_reporting | error_reporting |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php
Method public function merchant_excel_generate()

```
....
2002.             error_reporting(E_ALL);
```

**Information Exposure Through an Error Message\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13631 |
| Status | New |

Method manage_pn_rm_merchant, at line 4547 of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php, handles an Exception or runtime Error error_reporting. During the exception handling code, the application exposes the exception details to error_reporting, in method manage_pn_rm_merchant of BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php, line 4547.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php |

| | | |
|---|---|---|
| Line | 4556 | 4556 |
| Object | error_reporting | error_reporting |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/admin.php
Method public function manage_pn_rm_merchant()

```
....
4556.            error_reporting(E_ALL);
```

## Reliance on Cookies in a Decision

Query Path:
PHP\Cx\Php Low Visibility\Reliance on Cookies in a Decision Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.10 - Broken authentication and session management
OWASP Top 10 2017: A2-Broken Authentication
OWASP Top 10 2021: A8-Software and Data Integrity Failures

*Description*

**Reliance on Cookies in a Decision\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14185 |
| Status | New |

The cookie _COOKIE obtained by cookie at system/core/Input.php in line 223 uses its value in making a decision in _unserialize at system/libraries/Session.php in line 722, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/libraries/Session.php |
| Line | 225 | 730 |
| Object | _COOKIE | val |

Code Snippet
File Name system/core/Input.php
Method function cookie($index = '', $xss_clean = FALSE)

```
....
225.            return $this->_fetch_from_array($_COOKIE, $index,
$xss_clean);
```

File Name system/libraries/Session.php
Method function _unserialize($data)

```
....
730.                        if (is_string($val))
```

**Reliance on Cookies in a Decision\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14186 |
| Status | New |

The cookie _COOKIE obtained by cookie at system/core/Input.php in line 223 uses its value in making a decision in _unserialize at system/libraries/Session.php in line 722, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/libraries/Session.php |
| Line | 225 | 726 |
| Object | _COOKIE | data |

Code Snippet

File Name system/core/Input.php

Method function cookie($index = '', $xss_clean = FALSE)

```
....
225.                return $this->_fetch_from_array($_COOKIE, $index,
$xss_clean);
```

File Name system/libraries/Session.php

Method function _unserialize($data)

```
....
726.                if (is_array($data))
```

**Reliance on Cookies in a Decision\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14187 |
| Status | New |

The cookie _COOKIE obtained by cookie at system/core/Input.php in line 223 uses its value in making a decision in sess_read at system/libraries/Session.php in line 135, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/libraries/Session.php |
| Line | 225 | 159 |
| Object | _COOKIE | session |

Code Snippet

File Name system/core/Input.php

Method function cookie($index = '', $xss_clean = FALSE)

```
....
225.                return $this->_fetch_from_array($_COOKIE, $index,
$xss_clean);
```

File Name system/libraries/Session.php

Method function sess_read()

```
....
159.                    if ($hash !==  md5($session.$this-
>encryption_key))
```

**Reliance on Cookies in a Decision\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14188 |
| Status | New |

The cookie _COOKIE obtained by cookie at system/core/Input.php in line 223 uses its value in making a decision in sess_read at system/libraries/Session.php in line 135, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/libraries/Session.php |
| Line | 225 | 159 |
| Object | _COOKIE | hash |

Code Snippet

File Name system/core/Input.php

Method function cookie($index = '', $xss_clean = FALSE)

```
....
225.                return $this->_fetch_from_array($_COOKIE, $index,
$xss_clean);
```

File Name system/libraries/Session.php

Method function sess_read()

```
....
159.                    if ($hash !==  md5($session.$this-
>encryption_key))
```

**Reliance on Cookies in a Decision\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14189 |

| Status | New |
|---|---|

The cookie _COOKIE obtained by cookie at system/core/Input.php in line 223 uses its value in making a decision in sess_read at system/libraries/Session.php in line 135, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/libraries/Session.php |
| Line | 225 | 141 |
| Object | _COOKIE | session |

Code Snippet
File Name system/core/Input.php
Method function cookie($index = '', $xss_clean = FALSE)

```
....
225.                return $this->_fetch_from_array($_COOKIE, $index,
$xss_clean);
```

File Name system/libraries/Session.php
Method function sess_read()

```
....
141.                if ($session === FALSE)
```

**Reliance on Cookies in a Decision\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14190 |
| Status | New |

The cookie _COOKIE obtained by cookie at system/core/Input.php in line 223 uses its value in making a decision in _fetch_from_array at system/core/Input.php in line 119, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/core/Input.php |
| Line | 225 | 121 |
| Object | _COOKIE | array |

Code Snippet
File Name system/core/Input.php
Method function cookie($index = '', $xss_clean = FALSE)

```
....
225.                return $this->_fetch_from_array($_COOKIE, $index,
$xss_clean);
```

File Name system/core/Input.php

Method function _fetch_from_array(&$array, $index = '', $xss_clean = FALSE)

```
....
121.            if ( ! isset($array[$index]))
```

**Reliance on Cookies in a Decision\Path 7:**

Severity Low
Result State Confirmed
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14191
Status New

The cookie _COOKIE obtained by _sanitize_globals at system/core/Input.php in line 565 uses its value in making a decision in _sanitize_globals at system/core/Input.php in line 565, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/core/Input.php |
| Line | 575 | 579 |
| Object | _COOKIE | global |

Code Snippet
File Name system/core/Input.php
Method function _sanitize_globals()

```
....
575.            foreach (array($_GET, $_POST, $_COOKIE) as $global)
....
579.                        if ( ! in_array($global, $protected))
```

**Reliance on Cookies in a Decision\Path 8:**

Severity Low
Result State Confirmed
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14192
Status New

The cookie _COOKIE obtained by _sanitize_globals at system/core/Input.php in line 565 uses its value in making a decision in _sanitize_globals at system/core/Input.php in line 565, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/core/Input.php |
| Line | 575 | 577 |
| Object | _COOKIE | global |

Code Snippet
File Name system/core/Input.php
Method function _sanitize_globals()

```
....
575.            foreach (array($_GET, $_POST, $_COOKIE) as $global)
....
577.                  if ( ! is_array($global))
```

**Reliance on Cookies in a Decision\Path 9:**

Severity Low
Result State Confirmed
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14193
Status New

The cookie _COOKIE obtained by _sanitize_globals at system/core/Input.php in line 565 uses its value in making a decision in _clean_input_data at system/core/Input.php in line 666, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/core/Input.php |
| Line | 635 | 706 |
| Object | _COOKIE | str |

Code Snippet
File Name system/core/Input.php
Method function _sanitize_globals()

```
....
635.                  foreach ($_COOKIE as $key => $val)
```

File Name system/core/Input.php
Method function _clean_input_data($str)

```
....
706.                  if (strpos($str, "\r") !== FALSE)
```

**Reliance on Cookies in a Decision\Path 10:**

Severity Low
Result State Confirmed
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14194
Status New

The cookie _COOKIE obtained by _sanitize_globals at system/core/Input.php in line 565 uses its value in making a decision in clean_string at system/core/Utf8.php in line 85, without properly validating its contents.

| | Source | Destination |
|---|---|---|

| File | system/core/Input.php | system/core/Utf8.php |
|---|---|---|
| Line | 635 | 87 |
| Object | _COOKIE | str |

Code Snippet
File Name system/core/Input.php
Method function _sanitize_globals()

```
....
635.                    foreach ($_COOKIE as $key => $val)
```

File Name system/core/Utf8.php

Method function clean_string($str)

```
....
87.         if ($this->_is_ascii($str) === FALSE)
```

**Reliance on Cookies in a Decision\Path 11:**

Severity Low
Result State Confirmed
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14195
Status New

The cookie _COOKIE obtained by _sanitize_globals at system/core/Input.php in line 565 uses its value in making a decision in _clean_input_data at system/core/Input.php in line 666, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Input.php | system/core/Input.php |
| Line | 635 | 668 |
| Object | _COOKIE | str |

Code Snippet
File Name system/core/Input.php
Method function _sanitize_globals()

```
....
635.                    foreach ($_COOKIE as $key => $val)
```

File Name system/core/Input.php

Method function _clean_input_data($str)

```
....
668.                if (is_array($str))
```

**Reliance on Cookies in a Decision\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14196 |
| Status | New |

The cookie _COOKIE obtained by csrf_verify at system/core/Security.php in line 132 uses its value in making a decision in csrf_verify at system/core/Security.php in line 132, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Security.php | system/core/Security.php |
| Line | 148 | 148 |
| Object | _COOKIE | != |

Code Snippet
File Name system/core/Security.php
Method public function csrf_verify()

```
....
148.                if ($_POST[$this->_csrf_token_name] != $_COOKIE[$this-
>_csrf_cookie_name])
```

**Reliance on Cookies in a Decision\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14197 |
| Status | New |

The cookie _COOKIE obtained by _csrf_set_hash at system/core/Security.php in line 853 uses its value in making a decision in _csrf_set_hash at system/core/Security.php in line 853, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Security.php | system/core/Security.php |
| Line | 861 | 861 |
| Object | _COOKIE | isset |

Code Snippet
File Name system/core/Security.php
Method protected function _csrf_set_hash()

```
....
861.                    if (isset($_COOKIE[$this->_csrf_cookie_name]) &&
```

**Reliance on Cookies in a Decision\Path 14:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=14198 |
| Status | New |

The cookie _COOKIE obtained by _csrf_set_hash at system/core/Security.php in line 853 uses its value in making a decision in _csrf_set_hash at system/core/Security.php in line 853, without properly validating its contents.

| | Source | Destination |
|---|---|---|
| File | system/core/Security.php | system/core/Security.php |
| Line | 862 | 862 |
| Object | _COOKIE | preg_match |

Code Snippet
File Name system/core/Security.php
Method protected function _csrf_set_hash()

```
....
862.                          preg_match('#^[0-9a-f]{32}$#iS',
$_COOKIE[$this->_csrf_cookie_name]) === 1)
```

## Use Of Hardcoded Password

Query Path:
JavaScript\Cx\JavaScript Server Side Vulnerabilities\Use Of Hardcoded Password Version:1

### Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A7-Identification and Authentication Failures

*Description*

**Use Of Hardcoded Password\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22453 |
| Status | New |

The application uses a single, hard-coded password ""123456"" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 38 of application/views/rekon_settlement/edit_trouble_ticket.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/views/rekon_settlement/edit_trouble_ticket.php | application/views/rekon_settlement/edit_trouble_ticket.php |
| Line | 39 | 39 |
| Object | ""123456"" | Password |

| | |
|---|---|
| Code Snippet | |
| File Name | application/views/rekon_settlement/edit_trouble_ticket.php |
| Method | {'ChannelID' : 'CS', |

```
....
39.                     'Password' : '123456',
```

**Use Of Hardcoded Password\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22454 |
| Status | New |

The application uses a single, hard-coded password ""123456"" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 48 of BACKUP_DEPLOY_FMS_20210407/views/views/rekon_settlement/cm_input.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/rekon_settlement/cm_input.php | BACKUP_DEPLOY_FMS_20210407/views/views/rekon_settlement/cm_input.php |
| Line | 49 | 49 |
| Object | ""123456"" | Password |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/rekon_settlement/cm_input.php |
| Method | {'ChannelID' : 'CS', |

```
....
49.                     'Password' : '123456',
```

**Use Of Hardcoded Password\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22455 |
| Status | New |

The application uses a single, hard-coded password ""123456"" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 48 of application/views/rekon_settlement/cm_input.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/views/rekon_settlement/cm_input.php | application/views/rekon_settlement/cm_input.php |
| Line | 49 | 49 |
| Object | ""123456"" | Password |

Code Snippet

| | |
|---|---|
| File Name | application/views/rekon_settlement/cm_input.php |
| Method | {'ChannelID' : 'CS', |

```
....
49.                     'Password' : '123456',
```

**Use Of Hardcoded Password\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22456 |
| Status | New |

The application uses a single, hard-coded password ""123456"" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 38 of BACKUP_DEPLOY_FMS_20210407/views/views/rekon_settlement/edit_trouble_ticket.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/rekon_settlement/edit_trouble_ticket.php | BACKUP_DEPLOY_FMS_20210407/views/views/rekon_settlement/edit_trouble_ticket.php |
| Line | 39 | 39 |
| Object | ""123456"" | Password |

| | |
|---|---|
| Code Snippet | |
| File Name | BACKUP_DEPLOY_FMS_20210407/views/views/rekon_settlement/edit_trouble_ticket.php |
| Method | {'ChannelID' : 'CS', |

```
....
39.                     'Password' : '123456',
```

**Use Of Hardcoded Password\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22457 |
| Status | New |

The application uses a single, hard-coded password ""#password"" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 10 of application/views/user/change_password.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/views/user/change_password.php | application/views/user/change_password.php |
| Line | 10 | 10 |
| Object | ""#password"" | pass_ver |

Code Snippet
File Name application/views/user/change_password.php
Method pass_ver: { equalTo: "#password" }

```
....
10.             pass_ver: { equalTo: "#password" }
```

File Name application/views/user/change_password.php
Method rules: {

```
....
10.             pass_ver: { equalTo: "#password" }
```

**Use Of Hardcoded Password\Path 6:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22458
Status New

The application uses a single, hard-coded password ""#password"" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 10 of application/views/user/change_password.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | application/views/user/change_password.php | application/views/user/change_password.php |
| Line | 10 | 10 |
| Object | ""#password"" | pass_ver |

Code Snippet
File Name application/views/user/change_password.php
Method pass_ver: { equalTo: "#password" }

```
....
10.             pass_ver: { equalTo: "#password" }
```

File Name application/views/user/change_password.php
Method rules: {

```
....
10.             pass_ver: { equalTo: "#password" }
```

**Use Of Hardcoded Password\Path 7:**

Severity Low
Result State To Verify

| | |
|---|---|
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22459 |
| Status | New |

The application uses a single, hard-coded password ""#password"" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 10 of BACKUP_DEPLOY_FMS_20210407/views/views/user/change_password.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/user/change_password.php | BACKUP_DEPLOY_FMS_20210407/views/views/user/change_password.php |
| Line | 10 | 10 |
| Object | ""#password"" | pass_ver |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/user/change_password.php

Method pass_ver: { equalTo: "#password" }

```
....
10.             pass_ver: { equalTo: "#password" }
```

File Name BACKUP_DEPLOY_FMS_20210407/views/views/user/change_password.php

Method rules: {

```
....
10.             pass_ver: { equalTo: "#password" }
```

**Use Of Hardcoded Password\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22460 |
| Status | New |

The application uses a single, hard-coded password ""#password"" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 10 of BACKUP_DEPLOY_FMS_20210407/views/views/user/change_password.php appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/views/views/user/change_password.php | BACKUP_DEPLOY_FMS_20210407/views/views/user/change_password.php |
| Line | 10 | 10 |
| Object | ""#password"" | pass_ver |

Code Snippet

File Name BACKUP_DEPLOY_FMS_20210407/views/views/user/change_password.php

Method pass_ver: { equalTo: "#password" }

```
....
10.             pass_ver: { equalTo: "#password" }
```

File Name BACKUP_DEPLOY_FMS_20210407/views/views/user/change_password.php

Method rules: {

```
....
10.             pass_ver: { equalTo: "#password" }
```

**Use Of Hardcoded Password\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22461 |
| Status | New |

The application uses a single, hard-coded password ""Password"" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 342 of javascript/ckeditor/lang/en.js appears in the code as plaintext, and cannot be changed without rebuilding the application.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/lang/en.js | javascript/ckeditor/lang/en.js |
| Line | 351 | 351 |
| Object | ""Password"" | typePass |

Code Snippet

File Name javascript/ckeditor/lang/en.js

Method "textfield": {

```
....
351.             "typePass": "Password",
```

## Unprotected Cookie

Query Path:
JavaScript\Cx\JavaScript Server Side Vulnerabilities\Unprotected Cookie Version:1

### Categories

FISMA 2014: System And Communications Protection
NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity (P1)
OWASP Top 10 2021: A5-Security Misconfiguration

*Description*

**Unprotected Cookie\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22462 |
| Status | New |

The web application's function method creates a cookie setCookie, at line 703 of javascript/ckeditor/ckeditor.js, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/ckeditor.js | javascript/ckeditor/ckeditor.js |
| Line | 713 | 713 |
| Object | setCookie | setCookie |

Code Snippet
File Name javascript/ckeditor/ckeditor.js
Method getCsrfToken: function() {

```
....
713.                    CKEDITOR.tools.setCookie("ckCsrfToken", a)
```

**Unprotected Cookie\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22463 |
| Status | New |

The web application's function method creates a cookie setCookie, at line 825 of javascript/ckeditor/plugins/wsc/dialogs/wsc.js, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/plugins/wsc/dialogs/wsc.js | javascript/ckeditor/plugins/wsc/dialogs/wsc.js |
| Line | 827 | 827 |
| Object | setCookie | setCookie |

Code Snippet
File Name javascript/ckeditor/plugins/wsc/dialogs/wsc.js
Method set: function(a, c) {

```
....
827.                        this.setCookie(a, d, {
```

**Unprotected Cookie\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22464 |
| Status | New |

The web application's function method creates a cookie setCookie, at line 852 of javascript/ckeditor/plugins/wsc/dialogs/wsc.js, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/plugins/wsc/dialogs/wsc.js | javascript/ckeditor/plugins/wsc/dialogs/wsc.js |
| Line | 853 | 853 |
| Object | setCookie | setCookie |

Code Snippet
File Name javascript/ckeditor/plugins/wsc/dialogs/wsc.js
Method deleteCookie: function(a) {

```
....
853.                            this.setCookie(a, null, {
```

**Unprotected Cookie\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22465 |
| Status | New |

The web application's $ method creates a cookie setCookie, at line 248 of javascript/ddaccordion.js, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | javascript/ddaccordion.js | javascript/ddaccordion.js |
| Line | 256 | 256 |
| Object | setCookie | setCookie |

Code Snippet
File Name javascript/ddaccordion.js
Method $(window).bind('unload', function(){ //clean up and persist on page unload

```
....
256.                            ddaccordion.setCookie(config.headerclass,
expandedindices)
```

**Unprotected Cookie\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22466 |
| Status | New |

The web application's { method creates a cookie cookie, at line 53 of javascript/ckeditor/plugins/wsc/dialogs/wsc.js, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/plugins/wsc/dialogs/wsc.js | javascript/ckeditor/plugins/wsc/dialogs/wsc.js |
| Line | 78 | 78 |
| Object | cookie | cookie |

Code Snippet
File Name javascript/ckeditor/plugins/wsc/dialogs/wsc.js
Method return {

```
....
78.             cookie: {
```

**Unprotected Cookie\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22467 |
| Status | New |

The web application's function method creates a cookie cookie, at line 700 of javascript/ckeditor/ckeditor.js, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/ckeditor.js | javascript/ckeditor/ckeditor.js |
| Line | 701 | 701 |
| Object | cookie | cookie |

Code Snippet
File Name javascript/ckeditor/ckeditor.js
Method setCookie: function(a, b) {

```
....
701.                 document.cookie = encodeURIComponent(a) + "\x3d" +
encodeURIComponent(b) + ";path\x3d/"
```

**Unprotected Cookie\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22468 |
| Status | New |

The web application's function method creates a cookie cookie, at line 838 of javascript/ckeditor/plugins/wsc/dialogs/wsc.js, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/plugins/wsc/dialogs/wsc.js | javascript/ckeditor/plugins/wsc/dialogs/wsc.js |
| Line | 850 | 850 |
| Object | cookie | cookie |

Code Snippet
File Name javascript/ckeditor/plugins/wsc/dialogs/wsc.js
Method setCookie: function(a, b, c) {

```
....
850.                            document.cookie = a
```

**Unprotected Cookie\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22469 |
| Status | New |

The web application's function method creates a cookie cookie, at line 39 of javascript/ckeditor/plugins/wsc/dialogs/wsc.js, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/plugins/wsc/dialogs/wsc.js | javascript/ckeditor/plugins/wsc/dialogs/wsc.js |
| Line | 51 | 51 |
| Object | cookie | cookie |

Code Snippet
File Name javascript/ckeditor/plugins/wsc/dialogs/wsc.js
Method var a = function(a, b, d) {

```
....
51.               document.cookie = a
```

**Unprotected Cookie\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22470 |

| | |
|---|---|
| Status | New |

The web application's setCookie:function method creates a cookie cookie, at line 154 of javascript/ddaccordion.js, and returns it in the response. However, the application is not configured to automatically set the cookie with the "httpOnly" attribute, and the code does not explicitly add this to the cookie.

| | Source | Destination |
|---|---|---|
| File | javascript/ddaccordion.js | javascript/ddaccordion.js |
| Line | 155 | 155 |
| Object | cookie | cookie |

Code Snippet
File Name javascript/ddaccordion.js
Method setCookie:function(name, value){

```
....
155.            document.cookie = name + "=" + value + "; path=/"
```

## Hardcoded Absolute Path

Query Path:
PHP\Cx\Php Low Visibility\Hardcoded Absolute Path Version:1

### Categories

OWASP Top 10 2021: A8-Software and Data Integrity Failures

*Description*

**Hardcoded Absolute Path\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13300 |
| Status | New |

The injeksi method references external files using a hard-coded, absolute path ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking --page-size A4 " in application/controllers/cetak.php at line 333.

| | Source | Destination |
|---|---|---|
| File | application/controllers/cetak.php | application/controllers/cetak.php |
| Line | 355 | 355 |
| Object | ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking --page-size A4 " | ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking --page-size A4 " |

Code Snippet
File Name application/controllers/cetak.php
Method public function injeksi($nametemp='', $page=0)

```
....
355.                            exec('"C:/Program Files
(x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --
disable-smart-shrinking  --page-size A4
'.site_url('/cetak/injeksi').'/'.$nametemp.'/1
C:/xampp/htdocs/mms/template_formulir/pengajuan_injeksi/'.$filename.'.pd
f 2>&1');
```

**Hardcoded Absolute Path\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13301 |
| Status | New |

The injeksi method references external files using a hard-coded, absolute path ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking --page-size A4 -O Landscape " in application/controllers/cetak.php at line 333.

| | Source | Destination |
|---|---|---|
| File | application/controllers/cetak.php | application/controllers/cetak.php |
| Line | 356 | 356 |
| Object | ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking  --page-size A4 -O Landscape " | ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking  --page-size A4 -O Landscape " |

Code Snippet

| | |
|---|---|
| File Name | application/controllers/cetak.php |
| Method | public function injeksi($nametemp='', $page=0) |

```
....
356.                            exec('"C:/Program Files
(x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --
disable-smart-shrinking  --page-size A4 -O Landscape
'.site_url('/cetak/injeksi').'/'.$nametemp.'/2
C:/xampp/htdocs/mms/template_formulir/pengajuan_injeksi/'.$filename.'_la
mpiran.pdf 2>&1');
```

**Hardcoded Absolute Path\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13302 |
| Status | New |

The get_system_fonts method references external files using a hard-coded, absolute path ttf" in application/third_party/dompdf/include/font_metrics.cls.php at line 285.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | application/third_party/dompdf/include/font_metrics.cls.php | application/third_party/dompdf/include/font_metrics.cls.php |
| Line | 289 | 289 |
| Object | ttf" | ttf" |

Code Snippet
File Name application/third_party/dompdf/include/font_metrics.cls.php
Method static function get_system_fonts() {

```
....
289.                glob("C:\\Windows\\fonts\\*.ttf") +
```

**Hardcoded Absolute Path\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13303 |
| Status | New |

The get_system_fonts method references external files using a hard-coded, absolute path ttf" in application/third_party/dompdf/include/font_metrics.cls.php at line 285.

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/font_metrics.cls.php | application/third_party/dompdf/include/font_metrics.cls.php |
| Line | 290 | 290 |
| Object | ttf" | ttf" |

Code Snippet
File Name application/third_party/dompdf/include/font_metrics.cls.php
Method static function get_system_fonts() {

```
....
290.                glob("C:\\WinNT\\fonts\\*.ttf") +
```

**Hardcoded Absolute Path\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13304 |
| Status | New |

The injeksi method references external files using a hard-coded, absolute path ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking --page-size A4 " in BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php at line 333.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/contro | BACKUP_DEPLOY_FMS_20210407/contro |

| | | |
|---|---|---|
| | llers/controllers/cetak.php | llers/controllers/cetak.php |
| Line | 355 | 355 |
| Object | ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking --page-size A4 " | ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking --page-size A4 " |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php
Method public function injeksi($nametemp='', $page=0)

```
....
355.                            exec('"C:/Program Files
(x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --
disable-smart-shrinking  --page-size A4
'.site_url('/cetak/injeksi').'/'.$nametemp.'/1
C:/xampp/htdocs/mms/template_formulir/pengajuan_injeksi/'.$filename.'.pd
f 2>&1');
```

**Hardcoded Absolute Path\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13305 |
| Status | New |

The injeksi method references external files using a hard-coded, absolute path ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking --page-size A4 -O Landscape " in BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php at line 333.

| | Source | Destination |
|---|---|---|
| File | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php | BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php |
| Line | 356 | 356 |
| Object | ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking --page-size A4 -O Landscape " | ""C:/Program Files (x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --disable-smart-shrinking --page-size A4 -O Landscape " |

Code Snippet
File Name BACKUP_DEPLOY_FMS_20210407/controllers/controllers/cetak.php
Method public function injeksi($nametemp='', $page=0)

```
....
356.                            exec('"C:/Program Files
(x86)/wkhtmltopdf/wkhtmltopdf.exe" -T 1.5cm -R 1.5cm -L 2cm -B 1.5cm --
disable-smart-shrinking  --page-size A4 -O Landscape
'.site_url('/cetak/injeksi').'/'.$nametemp.'/2
C:/xampp/htdocs/mms/template_formulir/pengajuan_injeksi/'.$filename.'_la
mpiran.pdf 2>&1');
```

**Hardcoded Absolute Path\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13306 |
| Status | New |

The get_system_fonts method references external files using a hard-coded, absolute path ttf" in system/helpers/dompdf/include/font_metrics.cls.php at line 268.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/font_metrics.cls.php | system/helpers/dompdf/include/font_metrics.cls.php |
| Line | 272 | 272 |
| Object | ttf" | ttf" |

Code Snippet
File Name system/helpers/dompdf/include/font_metrics.cls.php
Method static function get_system_fonts() {

```
....
272.                glob("C:\\Windows\\fonts\\*.ttf") +
```

**Hardcoded Absolute Path\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=13307 |
| Status | New |

The get_system_fonts method references external files using a hard-coded, absolute path ttf" in system/helpers/dompdf/include/font_metrics.cls.php at line 268.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/font_metrics.cls.php | system/helpers/dompdf/include/font_metrics.cls.php |
| Line | 273 | 273 |
| Object | ttf" | ttf" |

Code Snippet
File Name system/helpers/dompdf/include/font_metrics.cls.php
Method static function get_system_fonts() {

```
....
273.                glob("C:\\WinNT\\fonts\\*.ttf") +
```

## Client DOM Open Redirect

Query Path:

## Categories

OWASP Top 10 2013: A10-Unvalidated Redirects and Forwards
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2021: A1-Broken Access Control

## *Description*

**Client DOM Open Redirect\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18410 |
| Status | New |

A possible open redirect has been found at line 8716 in javascript/ckeditor/ckeditor.js file. This might lead to an untrusted site which mainly used for phishing.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/ckeditor.js | javascript/ckeditor/ckeditor.js |
| Line | 229 | 6471 |
| Object | location | c |

Code Snippet

File Name javascript/ckeditor/ckeditor.js

Method var b = function(b, c) {

```
....
229.            b = {
```

File Name javascript/ckeditor/ckeditor.js

Method function x(a,

```
....
6471.         CKEDITOR.replace = function(b, d) {
```

**Client DOM Open Redirect\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18411 |
| Status | New |

A possible open redirect has been found at line 8716 in javascript/ckeditor/ckeditor.js file. This might lead to an untrusted site which mainly used for phishing.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/ckeditor.js | javascript/ckeditor/ckeditor.js |
| Line | 229 | 6471 |

| | | |
|---|---|---|
| Object | location | c |

Code Snippet
File Name javascript/ckeditor/ckeditor.js
Method var b = function(b, c) {

```
....
229.            b = {
```

File Name javascript/ckeditor/ckeditor.js

Method function x(a,

```
....
6471.         CKEDITOR.replace = function(b, d) {
```

**Client DOM Open Redirect\Path 3:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18412
Status New

A possible open redirect has been found at line 8716 in javascript/ckeditor/ckeditor.js file. This might lead to an untrusted site which mainly used for phishing.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/ckeditor.js | javascript/ckeditor/ckeditor.js |
| Line | 229 | 6471 |
| Object | location | c |

Code Snippet
File Name javascript/ckeditor/ckeditor.js
Method var b = function(b, c) {

```
....
229.            b = {
```

File Name javascript/ckeditor/ckeditor.js

Method function x(a,

```
....
6471.         CKEDITOR.replace = function(b, d) {
```

**Client DOM Open Redirect\Path 4:**

Severity Low
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti

| | |
|---|---|
| | d=4881&pathid=18413 |
| Status | New |

A possible open redirect has been found at line 8716 in javascript/ckeditor/ckeditor.js file. This might lead to an untrusted site which mainly used for phishing.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/ckeditor.js | javascript/ckeditor/ckeditor.js |
| Line | 229 | 6471 |
| Object | location | c |

Code Snippet

File Name javascript/ckeditor/ckeditor.js

Method var b = function(b, c) {

```
....
229.            b = {
```

File Name javascript/ckeditor/ckeditor.js

Method function x(a,

```
....
6471.        CKEDITOR.replace = function(b, d) {
```

## Client Use Of Iframe Without Sandbox

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client Use Of Iframe Without Sandbox Version:1

### Categories

NIST SP 800-53: SC-18 Mobile Code (P2)
OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 2021: A8-Software and Data Integrity Failures

*Description*

**Client Use Of Iframe Without Sandbox\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18416 |
| Status | New |

The application loads an external library or source code file using iframe____1466810155, at line 159 of system/helpers/dompdf/www/debugger.php. An attacker might be able to exploit this and cause the application to load arbitrary code.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/debugger.php | system/helpers/dompdf/www/debugger.php |
| Line | 159 | 159 |

| | | |
|---|---|---|
| Object | iframe____1466810155 | iframe____1466810155 |

Code Snippet
File Name system/helpers/dompdf/www/debugger.php
Method <iframe id="preview_html" name="preview_html" src="about:blank" frameborder="0" marginheight="0" marginwidth="0"></iframe>

```
....
159.        <iframe id="preview_html" name="preview_html"
src="about:blank" frameborder="0" marginheight="0"
marginwidth="0"></iframe>
```

**Client Use Of Iframe Without Sandbox\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18417 |
| Status | New |

The application loads an external library or source code file using iframe____1466810155, at line 162 of system/helpers/dompdf/www/debugger.php. An attacker might be able to exploit this and cause the application to load arbitrary code.

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/www/debugger.php | system/helpers/dompdf/www/debugger.php |
| Line | 162 | 162 |
| Object | iframe____1466810155 | iframe____1466810155 |

Code Snippet
File Name system/helpers/dompdf/www/debugger.php
Method <iframe id="preview" name="preview" src="about:blank" frameborder="0" marginheight="0" marginwidth="0"></iframe>

```
....
162.        <iframe id="preview" name="preview" src="about:blank"
frameborder="0" marginheight="0" marginwidth="0"></iframe>
```

**Client Use Of Iframe Without Sandbox\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18418 |
| Status | New |

The application loads an external library or source code file using iframe____1466810155, at line 26 of system/helpers/dompdf/www/examples.php. An attacker might be able to exploit this and cause the application to load arbitrary code.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | system/helpers/dompdf/www/examples.php | system/helpers/dompdf/www/examples.php |
| Line | 26 | 26 |
| Object | iframe____1466810155 | iframe____1466810155 |

Code Snippet
File Name system/helpers/dompdf/www/examples.php
Method <iframe id="preview" name="preview" src="about:blank" frameborder="0" marginheight="0" marginwidth="0"></iframe>

```
....
26.  <iframe id="preview" name="preview" src="about:blank"
frameborder="0" marginheight="0" marginwidth="0"></iframe>
```

## Client Potential ReDoS In Match

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client Potential ReDoS In Match Version:0

### Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A3-Injection

*Description*

**Client Potential ReDoS In Match\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18408 |
| Status | New |

The application uses a dangerous regex pattern "/edge[ \/](\d+.?\d*)/", at line 224 of javascript/ckeditor/ckeditor.js, to search and compare user input with match, at line 224 of javascript/ckeditor/ckeditor.js.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/ckeditor.js | javascript/ckeditor/ckeditor.js |
| Line | 226 | 226 |
| Object | "/edge[ \/](\d+.?\d*)/" | match |

Code Snippet
File Name javascript/ckeditor/ckeditor.js
Method CKEDITOR.env || (CKEDITOR.env = function() {

```
....
226.            d = a.match(/edge[ \/](\d+.?\d*)/),
```

**Client Potential ReDoS In Match\Path 2:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18409 |
| Status | New |

The application uses a dangerous regex pattern "/edge[ \/](\d+.?\d*)/", at line 224 of javascript/ckeditor/ckeditor.js, to search and compare user input with split, at line 224 of javascript/ckeditor/ckeditor.js.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/ckeditor.js | javascript/ckeditor/ckeditor.js |
| Line | 226 | 250 |
| Object | "/edge[ \/](\d+.?\d*)/" | split |

Code Snippet
File Name javascript/ckeditor/ckeditor.js
Method CKEDITOR.env || (CKEDITOR.env = function() {

```
....
226.                d = a.match(/edge[ \/](\d+.?\d*)/),
....
250.            b.gecko && (d = a.match(/rv:([\d\.]+)/)) && (d =
d[1].split("."), c = 1E4 * d[0] + 100 * (d[1] || 0) + 1 * (d[2] || 0));
```

## Client Potential DOM Open Redirect

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client Potential DOM Open Redirect Version:0

### Categories

OWASP Top 10 2013: A10-Unvalidated Redirects and Forwards
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2021: A1-Broken Access Control

### *Description*

**Client Potential DOM Open Redirect\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22450 |
| Status | New |

A possible open redirect has been found at line 8716 in javascript/ckeditor/ckeditor.js file. This might lead to an untrusted site which mainly used for phishing.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/ckeditor.js | javascript/ckeditor/ckeditor.js |
| Line | 8117 | 6471 |
| Object | text | c |

Code Snippet
File Name javascript/ckeditor/ckeditor.js

Method var b = function(b, c) {

```
....
8117.                                    h = h.text.replace(/(\r\n|\r)/g,
"\n").length;
```

File Name javascript/ckeditor/ckeditor.js

Method function x(a,

```
....
6471.          CKEDITOR.replace = function(b, d) {
```

**Client Potential DOM Open Redirect\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22451 |
| Status | New |

A possible open redirect has been found at line 8716 in javascript/ckeditor/ckeditor.js file. This might lead to an untrusted site which mainly used for phishing.

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/ckeditor.js | javascript/ckeditor/ckeditor.js |
| Line | 8134 | 6471 |
| Object | text | c |

Code Snippet

File Name javascript/ckeditor/ckeditor.js

Method var b = function(b, c) {

```
....
8134.                                h = h.text.replace(/(\r\n|\r)/g,
"\n").length;
```

File Name javascript/ckeditor/ckeditor.js

Method function x(a,

```
....
6471.          CKEDITOR.replace = function(b, d) {
```

## Client Insufficient ClickJacking Protection

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client Insufficient ClickJacking Protection Version:1

### Categories

FISMA 2014: Configuration Management
NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity (P1)

*Description*

**Client Insufficient ClickJacking Protection\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18414 |
| Status | New |

The application does not protect the web page 400.html from clickjacking attacks in legacy browsers, by using framebusting scripts.

| | Source | Destination |
|---|---|---|
| File | 400.html | 400.html |
| Line | 1 | 1 |
| Object | CxJSNS_500908525 | CxJSNS_500908525 |

Code Snippet
File Name 400.html
Method <html>

```
....
1.  <html>
```

## Client Overly Permissive Message Posting

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client Overly Permissive Message Posting Version:0

Categories

OWASP Top 10 2021: A5-Security Misconfiguration

*Description*

**Client Overly Permissive Message Posting\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=18415 |
| Status | New |

The web page uses the HTML5 Web Messaging technology to communicate with another web page in the browser, in javascript/ckeditor/plugins/wsc/dialogs/wsc.js at line 58. However, the application does not restrict communication to a specific domain ""*"".

| | Source | Destination |
|---|---|---|
| File | javascript/ckeditor/plugins/wsc/dialogs/wsc.js | javascript/ckeditor/plugins/wsc/dialogs/wsc.js |
| Line | 68 | 68 |
| Object | ""*"" | ""*"" |

Code Snippet
File Name javascript/ckeditor/plugins/wsc/dialogs/wsc.js

| | |
|---|---|
| Method | send: function(a) { |

```
....
68.                     h.postMessage(a, "*")
```

## Client Hardcoded Domain

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client Hardcoded Domain Version:1

### Categories

NIST SP 800-53: SC-18 Mobile Code (P2)
OWASP Top 10 2021: A8-Software and Data Integrity Failures

*Description*

**Client Hardcoded Domain\Path 1:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=22452 |
| Status | New |

The JavaScript file imported in ""https://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"" in javascript/colorbox/index.html at line 12 is from a remote domain, which may allow attackers to replace its contents with malicious code.

| | Source | Destination |
|---|---|---|
| File | javascript/colorbox/index.html | javascript/colorbox/index.html |
| Line | 12 | 12 |
| Object | ""https://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"" | ""https://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"" |

| | |
|---|---|
| Code Snippet | |
| File Name | javascript/colorbox/index.html |
| Method | <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"></script> |

```
....
12.         <script
src="https://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"><
/script>
```

## Possible Global Variable Overwrite

Query Path:
PHP\Cx\Php Best Coding Practice\Possible Global Variable Overwrite Version:1

*Description*

**Possible Global Variable Overwrite\Path 1:**

| | |
|---|---|
| Severity | Information |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23189 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/block_frame_reflower.cls.php | application/third_party/dompdf/include/block_frame_reflower.cls.php |
| Line | 182 | 182 |
| Object | extract | extract |

Code Snippet
File Name application/third_party/dompdf/include/block_frame_reflower.cls.php
Method protected function _calculate_restricted_width() {

```
....
182.      extract($this->_calculate_width($width));
```

**Possible Global Variable Overwrite\Path 2:**

Severity Information
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23190
Status New

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/block_frame_reflower.cls.php | application/third_party/dompdf/include/block_frame_reflower.cls.php |
| Line | 193 | 193 |
| Object | extract | extract |

Code Snippet
File Name application/third_party/dompdf/include/block_frame_reflower.cls.php
Method protected function _calculate_restricted_width() {

```
....
193.        extract($this->_calculate_width($max_width));
```

**Possible Global Variable Overwrite\Path 3:**

Severity Information
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23191
Status New

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/block_frame_reflower.cls.php | application/third_party/dompdf/include/block_frame_reflower.cls.php |
| Line | 197 | 197 |
| Object | extract | extract |

Code Snippet
File Name application/third_party/dompdf/include/block_frame_reflower.cls.php
Method protected function _calculate_restricted_width() {

```
....
197.        extract($this->_calculate_width($min_width));
```

**Possible Global Variable Overwrite\Path 4:**

Severity Information
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23192
Status New

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/cpdf_adapter.cls.php | application/third_party/dompdf/include/cpdf_adapter.cls.php |
| Line | 818 | 818 |
| Object | extract | extract |

Code Snippet
File Name application/third_party/dompdf/include/cpdf_adapter.cls.php
Method protected function _add_page_text() {

```
....
818.          extract($pt);
```

**Possible Global Variable Overwrite\Path 5:**

Severity Information
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23193
Status New

| | Source | Destination |
|---|---|---|
| File | application/third_party/dompdf/include/pdflib_adapter.cls.php | application/third_party/dompdf/include/pdflib_adapter.cls.php |
| Line | 966 | 966 |
| Object | extract | extract |

Code Snippet
File Name application/third_party/dompdf/include/pdflib_adapter.cls.php
Method protected function _add_page_text() {

```
....
966.          extract($pt);
```

**Possible Global Variable Overwrite\Path 6:**

| | |
|---|---|
| Severity | Information |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23194 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | system/core/Loader.php | system/core/Loader.php |
| Line | 807 | 807 |
| Object | extract | extract |

Code Snippet
File Name system/core/Loader.php
Method protected function _ci_load($_ci_data)

```
....
807.            extract($this->_ci_cached_vars);
```

**Possible Global Variable Overwrite\Path 7:**

| | |
|---|---|
| Severity | Information |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23195 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | system/database/DB_utility.php | system/database/DB_utility.php |
| Line | 260 | 260 |
| Object | extract | extract |

Code Snippet
File Name system/database/DB_utility.php
Method function xml_from_result($query, $params = array())

```
....
260.            extract($params);
```

**Possible Global Variable Overwrite\Path 8:**

| | |
|---|---|
| Severity | Information |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23196 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | system/database/drivers/mysql/mysql_utility.php | system/database/drivers/mysql/mysql_utility.php |

| | | |
|---|---|---|
| Line | 86 | 86 |
| Object | extract | extract |

Code Snippet
File Name system/database/drivers/mysql/mysql_utility.php
Method function _backup($params = array())

```
....
86.         extract($params);
```

**Possible Global Variable Overwrite\Path 9:**

Severity Information
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23197
Status New

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/block_frame_decorator.cls.php | system/helpers/dompdf/include/block_frame_decorator.cls.php |
| Line | 94 | 94 |
| Object | extract | extract |

Code Snippet
File Name system/helpers/dompdf/include/block_frame_decorator.cls.php
Method function set_line($lineno, $y = null, $w = null, $h = null, $tallest_frame = null, $left = null, $right = null) {

```
....
94.         extract($y);
```

**Possible Global Variable Overwrite\Path 10:**

Severity Information
Result State To Verify
Online Results https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23198
Status New

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/block_frame_reflower.cls.php | system/helpers/dompdf/include/block_frame_reflower.cls.php |
| Line | 180 | 180 |
| Object | extract | extract |

Code Snippet
File Name system/helpers/dompdf/include/block_frame_reflower.cls.php
Method protected function _calculate_restricted_width() {

```
....
180.      extract($this->_calculate_width($width));
```

**Possible Global Variable Overwrite\Path 11:**

| | |
|---|---|
| Severity | Information |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23199 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/block_frame_reflower.cls.php | system/helpers/dompdf/include/block_frame_reflower.cls.php |
| Line | 191 | 191 |
| Object | extract | extract |

Code Snippet
File Name system/helpers/dompdf/include/block_frame_reflower.cls.php
Method protected function _calculate_restricted_width() {

```
....
191.        extract($this->_calculate_width($max_width));
```

**Possible Global Variable Overwrite\Path 12:**

| | |
|---|---|
| Severity | Information |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23200 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/block_frame_reflower.cls.php | system/helpers/dompdf/include/block_frame_reflower.cls.php |
| Line | 194 | 194 |
| Object | extract | extract |

Code Snippet
File Name system/helpers/dompdf/include/block_frame_reflower.cls.php
Method protected function _calculate_restricted_width() {

```
....
194.        extract($this->_calculate_width($min_width));
```

**Possible Global Variable Overwrite\Path 13:**

| | |
|---|---|
| Severity | Information |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projecti |

| | |
|---|---|
| | d=4881&pathid=23201 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/cpdf_adapter.cls.php | system/helpers/dompdf/include/cpdf_adapter.cls.php |
| Line | 786 | 786 |
| Object | extract | extract |

Code Snippet
File Name system/helpers/dompdf/include/cpdf_adapter.cls.php
Method protected function _add_page_text() {

```
....
786.            extract($pt);
```

**Possible Global Variable Overwrite\Path 14:**

| | |
|---|---|
| Severity | Information |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23202 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/frame.cls.php | system/helpers/dompdf/include/frame.cls.php |
| Line | 597 | 597 |
| Object | extract | extract |

Code Snippet
File Name system/helpers/dompdf/include/frame.cls.php
Method function set_position($x = null, $y = null) {

```
....
597.         extract($x);
```

**Possible Global Variable Overwrite\Path 15:**

| | |
|---|---|
| Severity | Information |
| Result State | To Verify |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23203 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | system/helpers/dompdf/include/pdflib_adapter.cls.php | system/helpers/dompdf/include/pdflib_adapter.cls.php |
| Line | 913 | 913 |

| | | |
|---|---|---|
| Object | extract | extract |

Code Snippet
File Name system/helpers/dompdf/include/pdflib_adapter.cls.php
Method protected function _add_page_text() {

```
....
913.          extract($pt);
```

**Possible Global Variable Overwrite\Path 16:**

| | |
|---|---|
| Severity | Information |
| Result State | Confirmed |
| Online Results | https://sast.bri.co.id/CxWebClient/ViewerMain.aspx?scanid=1047116&projectid=4881&pathid=23204 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | system/libraries/Javascript.php | system/libraries/Javascript.php |
| Line | 43 | 43 |
| Object | extract | extract |

Code Snippet
File Name system/libraries/Javascript.php
Method public function __construct($params = array())

```
....
43.         extract($defaults);
```

# Command Injection

## Risk

### What might happen

An attacker could run arbitrary system-level OS commands on the application server host. Depending on the application's OS permissions, these could include:

- File actions (read / create / modify / delete)
- Open a network connection to the attacker's server
- Start and stop system services
- Modify the running application
- Complete server takeover

---

## Cause

### How does it happen

The application runs an OS system-level command to complete it's task, rather than via the application code. The command includes untrusted data, that may be controllable by an attacker. This untrusted string may contain malicious system-level commands engineered by an attacker, which could be executed as though the attacker were running commands directly on the application server.

In this case, the application receives data from the user input, and passes it as a string to the Operating System. This unvalidated data is then executed by the OS as a system command, running with the same system privileges as the application.

---

## General Recommendations

**How to avoid it**

- Refactor the code to avoid any direct shell command execution. Instead, use platform provided APIs or library calls.
- If it is impossible to remove the command execution, execute only static commands that do not include dynamic, user-controlled data.
- Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified format, rather than rejecting bad patterns (blacklist). Parameters should be limited to an allowed character set, and non-validated input should be dropped. In addition to characters, check for:
  - Data type
  - Size
  - Range
  - Format
  - Expected values
- In order to minimize damage as a measure of defense in depth, configure the application to run using a restricted user account that has no unnecessary OS privileges.
- If possible, isolate all OS commands to use a separate dedicated user account that has minimal privileges only for the specific commands and files used by the application, according to the Principle of Least Privilege.
- If absolutely necessary to call a system command or execute external program with user input, do not concatenate the user input with the command without sanitization. Use methods designed for this purpose, such as `escapeshellarg` and `escapeshellcmd`, where appropriate.

---

## Source Code Examples

**PHP**

**PHP Ping Script Vulnerable to Command Injection via String Concatenation**

```
<?php
      if (isset($_GET['host']) {
             $host = $_GET['host'];
             passthru("ping -c 1 ".$host); // host=www.google.com | cat /etc/passwd will print
the contents of /etc/passwd
    }
?>
```

**Sanitized PHP Ping Script**

```php
<?php
      if (isset($_GET['host']) {
             $host = $_GET['host'];
             passthru("ping -c 1 ".escapeshellarg($host));
     }
?>
```

# Code Injection

## Risk

### What might happen

An attacker could run arbitrary code on the application server host. Depending on the application's OS permissions,these could include:

- Database access, such as reading or modifying sensitive data;
- File actions (read / create / modify / delete);
- Changing the website;
- Open a network connection to the attacker's server;
- Decrypt secret data using the application's encryption keys;
- Start and stop system services;
- Complete server takeover.

---

## Cause

### How does it happen

The application performs some action by creating and running code that includes untrusted data, which might be under control of a malicious user. If the data contains malicious code, the executed code could contain system-level activities engineered by an attacker, as though the attacker were running code directly on the application server.

---

## General Recommendations

### How to avoid it

- The application should not compile, execute, or evaluate any untrusted code from any external source, including user input, uploaded files, or a database.
- If it is absolutely necessary to include external data in dynamic execution, it is permissible to pass the data as parameters to the code, but do not execute user data directly.
- If it is necessary to pass untrusted data to dynamic execution, enforce very strict data validation. For example, accept only integers between certain values.
- Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Parameters should be limited to an allowed character set, and non-validated input should be dropped. In addition to characters, check for:
  - Data type
  - Size
  - Range
  - Format
  - Expected values
- If possible, always prefer to whitelist known and trusted input instead of comparing to a blacklist.
- Configure the application to run using a restricted user account that has no unnecessary privileges.
- If possible, isolate all dynamic execution to use a separate, dedicated user account that has privileges only for the specific operations and files used by dynamic execution, according to the Principle of Least Privilege.

---

## Source Code Examples

**PHP**

**Dynamically Execute Arbitrary Code**

```
if (isset($_GET['code'])) {
      $code = $_GET['code'];
      eval($code);
}
```

**Call to Static Class from User Input**

```
$method = $_GET[method];
switch ($method) {
  case "methodOne":
    methodOne();
    break;
  case "methodTwo":
    methodTwo();
    break;
  //...
}
```

# Second Order SQL Injection

## Risk

### What might happen

An attacker could directly access all of the system's data. The attacker would be able to steal any sensitive information stored by the system (such as personal user details or credit cards), and possibly change or erase existing data.

---

## Cause

### How does it happen

The application communicates with its database by sending a textual SQL query. The application creates the query by simply concatenating strings including data obtained from the database. Since that data may have been previously obtained from user input, and is neither checked for data type validity nor subsequently sanitized, the data could contain SQL commands that would be interpreted as such by the database.

---

## General Recommendations

### How to avoid it

1. Validate all data, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
2. Instead of concatenating strings: a. Use secure database components such as stored procedures, parameterized queries, and object bindings (for commands and parameters). b. An even better solution is to use an ORM library, such as EntityFramework, Hibernate, or iBatis.
3. Restrict access to database objects and functionality, according to the Principle of Least Privilege.

---

## Source Code Examples

### CSharp

#### The application creates an SQL query using data obtained from a database

```
public class SecondOrderSQLInjection
{
        public void foo(SqlConnection connection, SqlDataAdapter DA)

    {

                DataSet DS = new DataSet();
                DA.Fill(ref DS, "UserName");
                SqlCommand command = new SqlCommand("SELECT * FROM Customers " + "WHERE
UserName = " + DS[0]["UserName"].ToString(), connection);
                command.ExecuteNonQuery();
        }
```

```
}
```

**The data obtained from the database is checked for potentially malicious characters**

```
class SecondOrderSQLInjectionFixed
{
        public void foo(SqlConnection connection, SqlDataAdapter DA)
    {
                DataSet DS = new DataSet();
                DA.Fill(ref DS, "UserName");
                string userName = DS[0]["UserName"].ToString().Replace("'", "");
                SqlCommand command = new SqlCommand("SELECT * FROM Customers " + "WHERE
UserName = " + userName, connection);
                command.ExecuteNonQuery();
        }
}
```

**Java**

**The application creates an SQL query using data obtained from a database**

```
public class Second_Order_SQL_Injection {
      public static void sql(Connection con, String sqlStm) {
            try {
                  Statement stmt = con.createStatement();
                  ResultSet rs = stmt.executeQuery(sqlStm);
                  String userName = rs.getString("USER_NAME");
                  String newSqlStm = "Update USER set PASSWORD = '1234' where userName like
" + userName;
                  stmt.executeUpdate(newSqlStm);
            } catch (Exception e) {
                  e.printStackTrace();
            }
      }
}
```

**The data obtained from the database is checked for potentially malicious characters**

```
public class Second_Order_SQL_Injection_Fixed {
      public static void sql(Connection con, String sqlStm) {
            try {
                  Statement stmt = con.createStatement();
                  ResultSet rs = stmt.executeQuery(sqlStm);
                  String userName = rs.getString("USER_NAME");
                  userName = userName.replaceAll("'", "");
                  String newSqlStm = "Update USER set PASSWORD = '1234' where userName like
" + userName;
                  stmt.executeUpdate(newSqlStm);
            } catch (Exception e) {
                  e.printStackTrace();
            }
```

```
        }
}
```

# File Disclosure

## Risk

### What might happen

If an attacker can disclose arbitrary files of their choice, they may disclose sensitive files that contain user or system credentials, personal or financial information and other sensitive files that the server may contain. They may also disclose application source code for further analysis, which may allow them to research, improve and escalate their attack against the application.

---

## Cause

### How does it happen

If an attacker can provide inputs to determine which files to read, and these inputs are not sanitized for file-system metacharacters (such as slashes), then the attacker may choose to read arbitrary files beyond those intended, disclosing these files' contents.

---

## General Recommendations

### How to avoid it

Consider using a static solution for reading files, such as a list of allowed files to read from, or a different file storage solution, such as a database. If reading local files from disk is absolutely required, ensure files being read from a specific folder, and restrict code access to this folder only; additionally, when a user provides the file name to be read, sanitize the file name for any file-system metacharacters, such as slashes, to prevent them from manipulating the path to access an unintended directory.

---

## Source Code Examples

### PHP

#### PHP Code Allows Reading Arbitrary OS Files

```
if (isset($_GET['imagename'])) {
      $filename = $_GET['imagename']; // Attacker can provide absolute path to file, such as
"/etc/passwd"
      readfile($filename);
}
```

#### Safely Reading A File, Removing Any Path, From A Specific Directory

```
if (isset($_GET['imagename'])) {
      $filename = getcwd()."/images/".basename($_GET['imagename']);
      readfile($filename);
}
```

# File Manipulation

## Risk

### What might happen

If an attacker can affect arbitrary files of their choice, they may overwrite or corrupt sensitive files, potentially resulting in denial of service. If an attacker is also able to choose the content being written, they may be able to inject code into arbitrary files, potentially resulting in malicious code execution.

## Cause

### How does it happen

A user provided input is used to determine which file is to be written into, potentially allowing them to affect or manipulate arbitrary files' contents.

## General Recommendations

### How to avoid it

Consider using a static solution for files to whom writing is allowed, such as a list of verified writable files or a different file storage solution, such as a database. If absolutely required, limit writing destination to a single folder by correctly sanitizing user provided inputs to set a filename, and programmatically set the destination folder. Consider supplementing this with a check to ensure whether a file exists or not, per business requirements of application code.

## Source Code Examples

### PHP

#### File Write Location Determined Solely By User Inputs, Potentially Leading to Remote Code Execution

```
if (isset($_GET['logname']) && isset($_GET['action'])) {
    $action = str_replace(array("\n", "\r"), '',$_GET['action']); // Remove line breaks
      $filename = $_GET['logname']; // An attacker can provide a 'logname' that is under the
webroot, creating a file that would be served by the server
      $file = fopen($filename,'a');
      fwrite($file, $action." was performed successfully.".PHP_EOL); // An attacker can set
$action to "<?php passthru($_GET['c']); ?>", resulting in a basic shell
}
```

#### File Write Location Determined Restricted by Code

```
if (isset($_GET['logname']) && isset($_GET['action'])) {
    $action = str_replace(array("\n", "\r"), '',$_GET['action']); // Remove line breaks
      $filename = "/var/log/application/".basename($_GET['logname']); // Can create arbitrary
log files, but restricted to a particular folder on the system.
      $file = fopen($filename,'a');
      fwrite($file, $action." was performed successfully.".PHP_EOL);
```

```
}
```

# SQL Injection

## Risk

### What might happen

An attacker could directly access all of the system's data. Using simple tools and text editing, the attacker would be able to steal any sensitive information stored by the system (such as personal user details or credit cards), and possibly change or erase existing data.

---

## Cause

### How does it happen

The application communicates with its database by sending a textual SQL query. The application creates the query by simply concatenating strings including the user's input. Since the user input is neither checked for data type validity nor subsequently sanitized, the input could contain SQL commands that would be interpreted as such by the database.

---

## General Recommendations

### How to avoid it

1. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values.
2. Instead of concatenating strings: a. Use secure database components such as stored procedures, parameterized queries, and object bindings (for commands and parameters). b. An even better solution is to use an ORM library, such as EntityFramework, Hibernate, or iBatis.
3. Restrict access to database objects and functionality, according to the Principle of Least Privilege.

---

## Source Code Examples

### CSharp

#### The application creates an SQL query using string obtained from the user

```
public class SQLInjection
{
        public void foo(TextBox tbUserName, SqliteConnection connection)
    {
                string user = tbUserName.Text;
                string sql = "insert into users(name) VALUES ('"+ user + "')";
                MySqlCommand cmd = new MySqlCommand(sql, connection);
                connection.Open();
                SqlDataReader reader = cmd.ExecuteReader();
        }
```

```
}
```

**The string obtained from the user is checked for potentially malicious characters**

```
class SqlInjectionFixed
{
        public void foo(TextBox tbUserName, SqliteConnection connection)
    {
                string user = tbUserName.Text;
                string sql = "insert into users(name) VALUES (@param1)";
                MySqlCommand cmd = new MySqlCommand(sql, connection);
                cmd.Parameters.AddWithValue(@param1, user);
                connection.Open();
                SqlDataReader reader = cmd.ExecuteReader();
        }
}
```

**Java**

**The application creates an SQL query using string obtained from the user**

```
public class SQL_Injection {
      public static void getUserId(Connection con) {
            System.out.println("enter user name");
            Scanner in = new Scanner(System.in);
            String user = in.nextLine();
            String query = "select user_id from User where user = " + user;
            Statement stmt = con.createStatement();
            ResultSet rs = stmt.executeQuery(query);
      }
}
```

**The string obtained from the user is checked for potentially malicious characters**

```
public class SQL_Injection_Fixed {
      public static void getUserId(Connection con) {
            System.out.println("enter user name");
            Scanner in = new Scanner(System.in);
            String user = in.nextLine();
            String query = "select user_id from User where user = ?";
            PreparedStatement stmt = con.createStatement(query);
            stmt.setString(1, user);
            ResultSet rs = stmt.executeQuery(query);
      }
}
```

# Stored XSS

## Risk

### What might happen

An attacker could use legitimate access to the application to submit engineered data to the application's database. When another user subsequently accesses this data, web pages may be rewritten and malicious scripts may be activated.

---

## Cause

### How does it happen

The application creates web pages that include data from the application's database. The data is embedded directly in the page's HTML, causing the browser to display it as part of the web page. This data may have originated in input from another user. If the data includes HTML fragments or Javascript, these are displayed too, and the user cannot tell that this is not the intended page. The vulnerability is the result of embedding arbitrary database data without first encoding it in a format that would prevent the browser from treating it like HTML instead of plain text.

---

## General Recommendations

### How to avoid it

1. Validate all dynamic data, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
2. Validation is not a replacement for encoding. Fully encode all dynamic data, regardless of source, before embedding it in output. Encoding should be context-sensitive. For example:
    - HTML encoding for HTML content
    - HTML attribute encoding for data output to attribute values
    - Javascript encoding for server-generated Javascript.
3. Consider using either the ESAPI encoding library, or its built-in functions. For earlier versions of ASP.NET, consider using the AntiXSS library.
4. In the Content-Type HTTP response header, explicitly define character encoding (charset) for the entire page.
5. Set the httpOnly flag on the session cookie, to prevent XSS exploits from stealing the cookie.

---

## Source Code Examples

### CSharp

**Data obtained from the execution of an SQL command is output to a label**

```
public class StoredXss
{
        public string foo(Label lblOutput, SqlConnection connection, int id)
```

```
    {
                string sql = "select email from CustomerLogin where customerNumber = @id";
                SqlCommand cmd = new SqlCommand(sql, connection);
                cmd.Prepare();
                cmd.Parameters.AddWithValue("@id", id);
                string output = (string)cmd.ExecuteScalar();
                lblOutput.Text = String.IsNullOrEmpty(output) ? "Customer Number does not
exist" : output;
        }
}
```

**The outputed string is Html encoded before it is displayed in the label**

```
public class StoredXssFixed
{
        public string foo(Label lblOutput, SqlConnection connection, HttpServerUtility
Server, int id)
    {
                string sql = "select email from CustomerLogin where customerNumber = @id";
                SqlCommand cmd = new SqlCommand(sql, connection);
                cmd.Prepare();
                cmd.Parameters.AddWithValue("@id", id);
                string output = (string)cmd.ExecuteScalar()
                lblOutput.Text = String.IsNullOrEmpty(output) ? "Customer Number does not
exist" : Server.HtmlEncode(output);
        }
}
```

**Java**

**Data obtained from the excecution of an SQL command is output to a label**

```
public class Stored_XSS {
      public static void XSSExample(Statement stmt) throws SQLException {
            Label label = new Label();
            ResultSet rs;
            rs = stmt.executeQuery("SELECT * FROM Customers WHERE UserName = Mickey");
            String lastNames = "";
            while (rs.next()) {
                  lastNames += rs.getString("Lname") + ", ";
            }
            label.setText("Mickey last names are: " + lastNames + " ");
      }
}
```

**The outputed string is encoded to hard-coded string before it is displayed in the label**

```
public class Stored_XSS_Fix {
      public static void XSSExample(Statement stmt) throws SQLException {
            Label label = new Label();
            ResultSet rs;
```

```
            HashMap<String, String> sanitize = new HashMap<String, String>();
            sanitize.put("A", "Cohen");
            sanitize.put("B", "Smith");
            sanitize.put("C", "Bond");
            rs = stmt.executeQuery("SELECT * FROM Customers WHERE UserName = Mickey");
            String lastNames = "";
            while (rs.next()) {
                  lastNames += sanitize.get(rs.getString("Lname")) + ", ";
            }
            label.setText("Mickey last names are: " + lastNames + " ");
      }
}
```

**JavaScript**

**Data obtained from the execution of an SQL command is rendered to a web-page template**

```
function renderUserProfileTable(res, connection, user_id) {
      connection.query('SELECT id,name,description from user WHERE id= ?',
[user_id],function(err, results) {
            var table = "<table>"
            table += "<table class='profile-html-table'>"
            table += "<tr><td>" + results[0].name + "</td></tr>"
            table += "<tr><td>" + results[0].description + "</td></tr>"
            table += "</table>"
            res.render("profile", table)
      });
}
```

**Data obtained from the execution of an SQL command is encoded and then rendered to a web-page template**

```
var htmlencoder = require('htmlencode');

function renderUserProfileTable(res, connection, user_id) {
      connection.query('SELECT id,name,description from user WHERE id= ?',
[user_id],function(err, results) {
            var table = "<table>"
            table += "<table class='profile-html-table'>"
            table += "<tr><td>" + htmlencoder.htmlEncode(results[0].name) + "</td></tr>"
            table += "<tr><td>" + htmlencoder.htmlEncode(results[0].description) +
"</td></tr>"
            table += "</table>"
            res.render("profile", table)
      });
}
```

# Reflected XSS All Clients

## Risk

### What might happen

An attacker could use social engineering to cause a user to send the website engineered input, rewriting web pages and inserting malicious scripts. The attacker can then pretend to be the original website, which would enable the attacker to steal the user's password, request the user's credit card information, provide false information, or run malware. From the victim's point of view, this is the original website, and the victim would blame the site for incurred damage.

---

## Cause

### How does it happen

The application creates web pages that include data from previous user input. The user input is embedded directly in the page's HTML, causing the browser to display it as part of the web page. If the input includes HTML fragments or JavaScript, these are displayed too, and the user cannot tell that this is not the intended page. The vulnerability is the result of embedding arbitrary user input without first encoding it in a format that would prevent the browser from treating it like HTML instead of plain text.

---

## General Recommendations

### How to avoid it

1. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
2. Fully encode all dynamic data before embedding it in output.
3. Encoding should be context-sensitive. For example:
    - HTML encoding for HTML content
    - HTML Attribute encoding for data output to attribute values
    - JavaScript encoding for server-generated JavaScript.
4. Consider using either the ESAPI encoding library, or the built-in platform functions. For earlier versions of ASP.NET, consider using the AntiXSS library.
5. In the Content-Type HTTP response header, explicitly define character encoding (charset) for the entire page.
6. Set the httpOnly flag on the session cookie, to prevent XSS exploits from stealing the cookie.

---

## Source Code Examples

### CSharp

**Bad - The application uses the "Referer" field string to construct the HttpResponse**

```
public class ReflectedXssAllClients
{
```

```
        public static void foo(HttpRequest Request, HttpResponse Response)
    {
                string Referer = Request.QueryString["Referer"];
                Response.BinaryWrite(Referer);
        }
}
```

**Good - The "Referer" field string is HTML encoded before use**

```
public class ReflectedXssAllClientsFixed
{
        public static void foo(HttpRequest Request, HttpResponse Response,
AntiXss.AntiXssEncoder encoder)
    {
                string Referer = Request.QueryString["Referer"];
                Response.BinaryWrite(encoder.HtmlEncode(Referer, true));
        }
}
```

**Bad - User input is written to a TextBox displayed on the screen enabling a user to inject a script**

```
public class ReflectedXSSSpecificClients
{
        public void foo(TextBox tb)
    {
                string input = Console.ReadLine();
                tb.Text = input;
        }
}
```

**Good - The user input is HTML encoded before being displayed on the screen**

```
public class ReflectedXSSSpecificClientsFixed
{
        public void foo(TextBox tb, AntiXssEncoder encode)
    {
                string input = Console.ReadLine();
                tb.Text = encode.HtmlEncode(input);
        }
}
```

**Bad - The application uses the "filename" field string from an HttpRequest construct an HttpResponse**

```
public class UTF7XSS
{
        public void foo(HttpRequest Request, HttpResponse Response
```

```
    {
        Response.Charset("UTF-7");
                string filename = Request.QueryString["filename"];
                Response.BinaryWrite(AntiXss.HtmlEncode(filename));
        }
}
```

**Good - The "filename" string is converted to an int and using a switch case the new "filename" string is constructed**

```
public class UTF7XSSFixed
{
        public static void foo(HttpRequest Request, HttpResponse Response)
    {
                Response.Charset("UTF-7");
                string filename = Request.QueryString["fileNum"];
                int fileNum = Convert.ToInt32(filename);

                switch(fileNum)
                {
                        case 1:
                                filename = "File1.txt";
                                break;
                        default:
                                filename = "File2.txt";
                                break;
                }

                Response.BinaryWrite(AntiXss.HtmlEncode(filename));
        }
}
```

**Java**

**User input is written to a label displayed on the screen enabling a user to inject a script**

```
public class ReflectedXSSAllClients {
      public static void XSSExample(TextArea name) {
            Label label = new Label();
            label.setText("Hello " + name.getText());
      }
}
```

**Switch case is used in order to assemble the label's text value and manage wrong user input**

```
public class ReflectedXSSAllClientsFixed {
      public static void XSSExample(TextArea name) {
            Label label = new Label();
            switch (name) {
            case "Joan":
                  label.setText("Hello Joan");
                  break;
            case "Jim":
                  label.setText("Hello Jim");
```

```
                break;
            case "James":
                label.setText("Hello James");
                break;
            default:
                System.out.println("Wrong Input");
            }
        }
    }
```

# Cross Site History Manipulation

## Risk

### What might happen

An attacker could compromise the browser's Same Origin Policy and violate a user's privacy, by manipulating the browser's History object in JavaScript. This could allow the attacker in certain situations to detect whether the user is logged in, track the user's activity, or infer the state of other conditional values. This may also enhance Cross Site Request Forgery (XSRF) attacks, by leaking the result of the initial attack.

---

## Cause

### How does it happen

Modern browsers expose the user's browsing history to local JavaScript as a stack of previously visited URLs. While the browsers enforce a strict Same Origin Policy (SOP) to prevent pages from one website from reading visited URLs on other websites, the History object does leak the size of the history stack. Using only this information, in some situations the attacker can discover the results of certain checks the application performs on the server-side. For example, if the application redirects an unauthenticated user to the login page, a script on another website can detect that whether or not the user is logged in, by checking the length of the History object.
This information leakage is enabled when the application redirects the user's browser based on the value of some condition, the state of the user's server-side session. E.g. whether the user is authenticated to the application, if the user has visited a certain page with specific parameters, or the value of some application data. For more information, see https://www.checkmarx.com/wp-content/uploads/2012/07/XSHM-Cross-site-history-manipulation.pdf .

---

## General Recommendations

### How to avoid it

Generic Guidance:

- Add the response header "X-Frame-Options: DENY" to all sensitive pages in the application, to protect against the IFrame version of XSHM in modern browser versions.

Specific Recommendations:

- Add a random value to all targeted URLs as a parameter.

---

## Source Code Examples

#### Java

#### Example of code that leaks the variable state via browser history

```
If (!isAuthenticated)
    response.sendRedirect("Login.jsp");
```

### Example code that prevents history leakage via random token

```
if (request.getParameter("r") == null)
    response.sendRedirect("Login.jsp?r=" + (new Random()).nextInt());

If (!isAuthenticated)
    response.sendRedirect("Login.jsp?r=" + (new Random()).nextInt());
```

# Stored Code Injection

## Risk

### What might happen

An attacker could run arbitrary code on the application server host. Depending on the application's OS permissions,these could include:

- Database access, such as reading or modifying sensitive data;
- File actions (read / create / modify / delete);
- Changing the website;
- Open a network connection to the attacker's server;
- Decrypt secret data using the application's encryption keys;
- Start and stop system services;
- Complete server takeover.

---

## Cause

### How does it happen

The application performs some action by creating and running code that includes untrusted data, which might be under control of a malicious user. If the data contains malicious code, the executed code could contain system-level activities engineered by an attacker, as though the attacker were running code directly on the application server.

---

## General Recommendations

### How to avoid it

- The application should not compile, execute, or evaluate any untrusted code from any external source, including user input, uploaded files, or a database.
- If it is absolutely necessary to include external data in dynamic execution, it is permissible to pass the data as parameters to the code, but do not execute user data directly.
- If it is necessary to pass untrusted data to dynamic execution, enforce very strict data validation. For example, accept only integers between certain values.
- Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Parameters should be limited to an allowed character set, and non-validated input should be dropped. In addition to characters, check for:
  - Data type
  - Size
  - Range
  - Format
  - Expected values
- If possible, always prefer to whitelist known and trusted input instead of comparing to a blacklist.
- Configure the application to run using a restricted user account that has no unnecessary privileges.
- If possible, isolate all dynamic execution to use a separate, dedicated user account that has privileges only for the specific operations and files used by dynamic execution, according to the Principle of Least Privilege.

---

## Source Code Examples

## PHP

### Dynamically Load and Execute Arbitrary Code

```
$result = mysql_query($conn, $sql);
if (mysql_num_rows($result) > 0) {
  $row = mysql_fetch_assoc($result);
  $code = $row["code"];
  eval($code);
}
```

### Call to Static Class from User Input

```
$result = mysql_query($conn, $sql);
if (mysql_num_rows($result) > 0) {
  $row = mysql_fetch_assoc($result);;
  $method = $row["method"];
  switch ($method) {
    case "methodOne":
      methodOne();
      break;
    case "methodTwo":
      methodTwo();
      break;
    //...
}
```

# Path Traversal

## Risk

### What might happen

An attacker could define arbitrary file path for the application to use, potentially leading to:

- Stealing sensitive files, such as configuration or system files
- Overwriting files such as program binaries, configuration files, or system files
- Deleting critical files, causing denial of service (DoS).

---

## Cause

### How does it happen

The application uses user input in the file path for accessing files on the application server's local disk.

---

## General Recommendations

### How to avoid it

1. Ideally, avoid depending on dynamic data for file selection.
2. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
   - Data type
   - Size
   - Range
   - Format
   - Expected values
3. Accept dynamic data only for the filename, not for the path and folders.
4. Ensure that file path is fully canonicalized.
5. Explicitly limit the application to use a designated folder that is separate from the applications binary folder.
6. Restrict the privileges of the application's OS user to necessary files and folders. The application should not be able to write to the application binary folder, and should not read anything outside of the application folder and data folder.

---

## Source Code Examples

### PHP

**Absolute Path Traversal in "filename" Parameter**

```
if (isset($_GET['filename'])) {
      $filename = $_GET['filename'];
      echo $filename;
      if (is_readable($filename)) {
             $fp = fopen($filename, 'rb');
             fpassthru ($fp);
      }
      else {
```

```
            // return 404
        }
    } else {
        // return 404
    }
```

### Relative Path Traversal in "filename" Parameter

```
if (isset($_GET['filename'])) {
        $filename = "public_files/".$_GET['filename'];
        echo $filename;
        if (is_readable($filename)) {
                $fp = fopen($filename, 'rb');
                fpassthru ($fp);
        }
        else {
                // return 404
        }
} else {
        // return 404
}
```

### Path Traversal Mitigated by Utilizing Basename

```
if (isset($_GET['filename'])) {
        $filename = "public_files/".basename($_GET['filename']);
        echo $filename;
        if (is_readable($filename)) {
                $fp = fopen($filename, 'rb');
                fpassthru ($fp);
        }
        else {
                // return 404
        }
} else {
        // return 404
}
```

# Insecure Randomness

## Risk

### What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

---

## Cause

### How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.
Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

---

## General Recommendations

### How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

---

## Source Code Examples

### Java

#### Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();
```

```
String sessionId = sessNum.toString();
```

**Cryptographically secure random number generator**

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

**Objc**

**Use of a weak pseudo-random number generator**

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

**Cryptographically secure random number generator**

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

**Swift**

**Use of a weak pseudo-random number generator**

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

**Cryptographically secure random number generator**

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

# Privacy Violation

## Risk

### What might happen

A user's personal information could be stolen by a malicious programmer, or an attacker that intercepts the data.

## Cause

### How does it happen

The application sends user information, such as passwords, account information, or credit card numbers, outside the application, such as writing it to a local text or log file or sending it to an external web service.

## General Recommendations

### How to avoid it

1. Personal data should be removed before writing to logs or other files.
2. Review the need and justification of sending personal data to remote web services.

## Source Code Examples

### CSharp

#### The user's password is written to the screen

```
class PrivacyViolation
{
        static void CreateUser(string username, string password)
    {
                AddUser(username, password);
                System.Console.WriteLine(password);
        }
}
```

# HTTP Response Splitting

## Risk

### What might happen

If the header setting code is of a vulnerable version, an attacker could:

- Arbitrarily change the application server's response header to a victim's HTTP request by manipulating headers
- Arbitrarily change the application server's response body by injecting two consecutive line breaks, which may result in Cross-Site Scripting (XSS) attacks
- Cause cache poisoning, potentially controlling any site's HTTP responses going through the same proxy as this application.

---

## Cause

### How does it happen

Since user input is being used in an HTTP response header, an attacker could include NewLine characters to make the header look like multiple headers with engineered content, potentially making the response look like multiple responses (for example, by engineering duplicate content-length headers). This can cause an organizational proxy server to provide the second, engineered response to a victim's subsequent request; or, if the proxy server also performs response caching, the attacker can send an immediate subsequent request to another site, causing the proxy server to cache the engineered response as a response from this second site and to later serve the response to other users.

Many modern web frameworks mitigate this issue, by offering sanitization for new line characters in strings inserted into headers by default. However, since many older versions of web frameworks fail to automatically mitigate this issue, manual sanitization of input may be required.

---

## General Recommendations

### How to avoid it

1. Validate all input, regardless of source (including cookies). Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
2. Additionally, remove or URL-encode all special (non-alphanumeric) user input before including it in the response header.

---

## Source Code Examples

### CSharp

**User input is being used in an HTTP response header, enabling an attacker to add a newline character and multiple headers**

```
public class HTTPResponseSplitting
{
        public void foo(HttpRequest Request, HttpResponse Response)
    {
                string author = Request.Params["author"];
                Response.AppendHeader("Author", author);
        }
}
```

**The user input is both excluded if it contains a newline character and the input is also URL encoded**

```
public class HTTPResponseSplittingFixed
{
        public void foo(HttpRequest Request, HttpResponse Response)
    {
                string author = Request.Params["author"];

                if (!author.Contains('\n'))
                {
                        author = HttpUtility.UrlEncode(author);
                        Response.AppendHeader("Author", author);
                }
        }
}
```

# HttpOnlyCookies

## Risk

### What might happen

Cookies that contain the user's session identifier, and other sensitive application cookies, are typically accessible by client-side scripts, such as JavaScript. Unless the web application explicitly prevents this using the "httpOnly" cookie flag, these cookies could be read and accessed by malicious client scripts, such as Cross-Site Scripting (XSS). This flag would mitigate the damage done in case XSS vulnerabilities are discovered, according to Defense in Depth.

---

## Cause

### How does it happen

The web application framework, by default, does not set the "httpOnly" flag for the application's sessionid cookie and other sensitive application cookies. Likewise, the application does not explicitly use the "httpOnly" cookie flag, thus allowing client scripts to access the cookies by default.

---

## General Recommendations

### How to avoid it

- Always set the "httpOnly" flag for any sensitive server-side cookie.

- It is highly recommended to implement HTTP Strict Transport Security (HSTS) in order to ensure that the cookie will be sent over a secured channel.

- Explicitly set the "httpOnly" flag for each cookie set by the application.

- In particular, explicitly set the `$httponly` parameter to true, any time a cookie is added to the response with `setcookie()` or `setrawcookie()`.

- Preferably, configure PHP to automatically set httpOnly on all cookies by adding `session.cookie_httponly = true` to `php.ini`, or by calling `ini_set('session.cookie_httponly', true);`

- Alternatively, enforce strong defaults by setting the session parameters for each session, using `session_set_cookie_params()` with `$httpOnly` set to `true`.

- If the cookie is being written directly to the response headers, e.g. via the `header()` method with the "`Set-Cookie:`" header name, append "`;httpOnly;`" to the end of the cookie value.

---

## Source Code Examples

### PHP

### Creating Cookie in Code

```
<?php
$cookievalue = getUserPreference();
```

```
setcookie("Preference", $cookievalue);
?>
```

### Explicitly setting the HttpOnly flag on Cookies

```
<?php
$cookievalue = getUserPreference();

setcookie("Preference", $cookievalue, time()+3600, $APPROOTDIR, $DOMAIN, true, true);
?>
```

### Configuring Default HttpOnly

```
<?php
ini_set('session.cookie_httponly', true);
?>
```

# Inappropriate Encoding for Output Context

## Risk

### What might happen

In some situations, using the faulty encoding functions can lead to Cross-Site Scripting (XSS). This would enable an attacker to steal the user's password, request the user's credit card information, provide false information, or run malware. From the victim's point of view, this is the original website, and the victim would blame the site for incurred damage.

---

## Cause

### How does it happen

The application creates web pages that include data from previous user input. The user input is embedded directly in the page's HTML, causing the browser to display it as part of the web page. This input is first encoded into HTML before being embedded.

However, the encoding function does not include the "ENT_QUOTES" and "ENT_HTML5" flags, and thus embedded apostrophes, backticks (`) and backslashes are not properly encoded. If the input is output in a context where apostrophes or backticks are significant, such as HTML attribute values or JavaScript, the encoding would not suffice and the unencoded input would be treated identically to the context. If two parameters are reflected in the same line, and that line is Javascript, the first parameter can be ended with backslash, escaping the quoted enclosure, and the following parameter could contain an XSS payload. Thus, and attacker would be able to embed content in the page as if it were the original source page.

---

## General Recommendations

### How to avoid it

Generic Guidance:

- Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns.
- Check for:
  - Data type
  - Size
  - Range
  - Format
  - Expected values
- Fully encode all dynamic data before embedding it in output.
- Encoding should be context-sensitive. For example:
  - HTML encoding for HTML content
  - HTML Attribute encoding for data output to attribute values
  - JavaScript encoding for server-generated JavaScript
- Prefer using functions built-in to the language or platform.
- In the Content-Type HTTP response header, explicitly define character encoding (charset) for the entire page.
- Set the httpOnly flag on the session cookie, to prevent XSS exploits from stealing the cookie.

Specific Recommendations:

- When calling `htmlentities()` or `htmlspecialchars()`, always set the `$flags` parameter to `ENT_HTML5 | ENT_QUOTES`

## Source Code Examples

### PHP

#### Unencoded Quotes in Attribute Value

```
<?php

$item = htmlEntities($_GET['item']);

print "<input value='$item'>";

?>
```

#### Quotes Encoded for Attributes

```
<?php

$item = htmlEntities($_GET['item'], ENT_HTML5 | ENT_QUOTES);

print "<input value='$item'>";

?>
```

# Client Use Of JQuery Outdated Version

## Risk

### What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions. However, even if deprecated code is used in a way that is completely secure, its very use and inclusion in the code base would encourage developers to re-use the deprecated element in the future, potentially leaving the application vulnerable to attack, which is why deprecated code should be eliminated from the code-base as a matter of practice.
Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.

---

## Cause

### How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

---

## General Recommendations

### How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

---

## Source Code Examples

### Java

#### Using Deprecated Methods for Security Checks

```
private void checkPermissions(InetAddress address) {

    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        secManager.checkMulticast(address, 0)
    }

}
```

#### A Replacement Security Check

```
private void checkPermissions(InetAddress address) {
```

```
    SecurityManager secManager = System.getSecurityManager();

    if (secManager != null) {
        SocketPermission permission = new SocketPermission(address.getHostAddress(),
"accept,connect");

        secManager.checkPermission(permission)
    }

}
```

# Client Potential XSS

## Risk

### What might happen

An attacker could use social engineering to cause a user to send the website engineered input, rewriting web pages and inserting malicious scripts. The attacker can then pretend to be the original website, which would enable the attacker to steal the user's password, request the user's credit card information, provide false information, or run malware. From the victim's point of view, this is the original website, and the victim would blame the site for incurred damage.

---

## Cause

### How does it happen

The application creates web pages that include data from previous user input. The user input is embedded directly in the page's HTML, causing the browser to display it as part of the web page. If the input includes HTML fragments or JavaScript, these are displayed too, and the user cannot tell that this is not the intended page. The vulnerability is the result of embedding arbitrary user input without first encoding it in a format that would prevent the browser from treating it like HTML instead of plain text.

---

## General Recommendations

### How to avoid it

1. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
2. Fully encode all dynamic data before embedding it in output.
3. Encoding should be context-sensitive. For example:
    - HTML encoding for HTML content
    - HTML Attribute encoding for data output to attribute values
    - JavaScript encoding for server-generated JavaScript.
4. Consider using either the ESAPI encoding library, or the built-in platform functions. For earlier versions of ASP.NET, consider using the AntiXSS library.
5. In the Content-Type HTTP response header, explicitly define character encoding (charset) for the entire page.
6. Set the httpOnly flag on the session cookie, to prevent XSS exploits from stealing the cookie.

---

## Source Code Examples

# Client Potential Code Injection

## Risk

### What might happen

An attacker could run arbitrary code on the application server host. Depending on the application's OS permissions,these could include:

- Database access, such as reading or modifying sensitive data;
- File actions (read / create / modify / delete);
- Changing the website;
- Open a network connection to the attacker's server;
- Decrypt secret data using the application's encryption keys;
- Start and stop system services;
- Complete server takeover.

The attacker would use social engineering techniques to convince the victim to use the attacker's code, either via a malformed link or otherwise. This will enable the attacker to gain control of the user's experience with the web application, hijacking the browser to alter the displayed web pages, mount phishing attacks, and execute arbitrary scripts.

---

## Cause

### How does it happen

The application performs some action by creating and running code that includes untrusted data, which might be under control of a malicious user. If the data contains malicious code, the executed code could contain system-level activities engineered by an attacker, as though the attacker were running code directly on the application server.

In this case, the untrusted code is read by the browser, and executed on the client side.

In this case, the payload executed is derived from dynamic page content, which may be dynamically affected by user inputs.

---

## General Recommendations

### How to avoid it

- The application should not compile, execute, or evaluate any untrusted code from any external source, including user input, uploaded files, or a database.
- If it is absolutely necessary to include external data in dynamic execution, it is permissible to pass the data as parameters to the code, but do not execute user data directly.
- If it is necessary to pass untrusted data to dynamic execution, enforce very strict data validation. For example, accept only integers between certain values.
- Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Parameters should be limited to an allowed character set, and non-validated input should be dropped. In addition to characters, check for:
  - Data type
  - Size
  - Range
  - Format
  - Expected values
- If possible, always prefer to whitelist known and trusted input instead of comparing to a blacklist.

- Configure the application to run using a restricted user account that has no unnecessary privileges.
- If possible, isolate all dynamic execution to use a separate, dedicated user account that has privileges only for the specific operations and files used by dynamic execution, according to the Principle of Least Privilege.

- On the client-side, do not use any form of dynamic code evaluation with any untrusted data. Dynamic evaluation is only allowed with hard-coded commands.

---

## Source Code Examples

**JavaScript**
**Dynamic evaluation of untrusted input**

```
eval(location.hash);
```

**Dynamically Invoking a Safe Function**

```
window.setTimeout(hardcodedFunction(), 1000);
```

**Evaluation of Code From Dynamic Page Element**

```
<div id="divElem" ></div>

<script>
eval(document.getElementById("divElem").innerText); // The contents of divElem will be
executed as a script
</script>
```

**Passing Parameters to Trusted Pre-Built Methods**

```
<div id="divElem" ></div>

<script>
var divElemText = document.getElementById("divElem").innerText;
trustedFunction(divElemText);
</script>
```

# Object Injection

## Risk

### What might happen

An attacker could prepare serialized data which when de-serialized would cause execution of the attacker python code on the server.

Arbitrary code execution on the server might lead to data loss, denial of service, or data security compromise.

---

## Cause

### How does it happen

The Pickle module implements generic and powerful serialization and de-serialization of arbitrary Python objects. Pickle supports serialization of acyclic and cyclic object graphs. If an object is referenced several times, only one master copy is serialized, and the other references are preserved as the references to the master copy.

The Pickle module is not intended to be used in untrusted environment, and it is not secure against invalid of maliciously constructed data.

The Pickle module supports several versions of serialization protocols, version 0 being a backward-compatible ASCII-only representation.

The Pickle allows arbitrary objects to declare serialization routine by defining a __reduce__ method. It should return either a string or a tuple describing how to reconstruct this object on de-serialization. This tuple should contain a callable and a tuple of arguments to be passed to this callable.

We can construct a pickle, that when de-serialized, will execute /bin/sh, as follows:

```
import cPickle

import subprocess
import base64

class RunBinSh(object):
 def __reduce__(self):
    return (subprocess.Popen, (('/bin/sh',),))

print base64.b64encode(cPickle.dumps(RunBinSh()))
```

---

## General Recommendations

### How to avoid it

- **Trust boundaries** - Do not use Pickle module for de-serialization of the data received from an untrusted or a user-controlled source.

Only unpickle data the application pickled itself. Normally the application could trust the data that come from its own server (DB, cache, etc).

However, if someone has access to manipulate the data, he/she can also exploit the pickle vulnerability.

- **Safer alternatives** - Consider using JSON formats.

- **Data signing** - Hash or sign the data with a secret key.
- **Secure communication** - If an application receives pickled data from a trusted application in a trusted environment, ensure that an encrypted network connection is used.

---

## Source Code Examples

**Python**

**Bad - The application receives the data from ZeroMQ and unpickles it without validation**

```
import zmq
import cPickle as pickle

class Server(object):
    def __init__(self):
        context = zmq.Context()

        self.receiver = context.socket(zmq.PULL)
        self.receiver.bind("tcp://*:1234")

        self.sender = context.socket(zmq.PUSH)
        self.sender.bind("tcp://*:1235")

    def send(self, data):
        self.sender.send(pickle.dumps(data))

    def recv(self):
        data = self.receiver.recv()
        return pickle.loads(data) # bad

s = Server()
print s.recv()
```

**Good - The application checks if SHA256 hash of the data and the secret key K is unchanged. The secret key K must not be revealed to an entrusted party**

```
import zmq
import cPickle as pickle

class Server(object):
    def __init__(self):
        context = zmq.Context()

        self.receiver = context.socket(zmq.PULL)
        self.receiver.bind("tcp://*:1234")

        self.sender = context.socket(zmq.PUSH)
        self.sender.bind("tcp://*:1235")

    def send(self, data):
        pickled = pickle.dumps(data)
        digest = hmac.new('K', pickled, hashlib.sha256).hexdigest()
        self.sender.send(digest + ' ' + pickled)

    def recv(self):
        data = self.receiver.recv()
        recv_digest, picked = data.split(' ');
        new_digest = hmac.new('K', pickled, hashlib.sha256).hexdigest()
        if recv_digest != new_digest: # good
```

```
            raise Exception('Integrity check failed')

s = Server()
print s.recv()
```

# Header Injection

## Risk

### What might happen

An attacker could:

- Hijack session, performing session fixation in which a cookie or other authenticated header is injected into the request.
- Cause web cache poisoning, via a Response Splitting attack or by tricking the cache server into unintentionally associating a URL with another URL's page (content), and caching this content for the URL.
- Bypass CSRF protection which relies on the referrer header.
- Bypass Firewall/IPS/IDS protection, via a Request smuggling attack, by sending a second, unnoticed request.
- Executing arbitrary Javascript code, via Cross-Site Scripting (XSS), by changing headers like Content-Type or overriding headers like x-xss-protection.

---

## Cause

### How does it happen

HTTP header injection vulnerabilities occur when an HTTP request header is influenced by an input received from the client without being validated. This attack usually occurs by injecting CRLF (newline) characters (i.e. \r, \n, %0a, %0d) into a HTTP request header, breaking out of the headers into the message body and writing a second arbitrary request. Alternatively, it is possible to perform other attacks by influencing the request authentication headers, security header and bypass. This attack makes it possible to exploit other attacks, like Cache Poisoning, Session Hijacking, Cross-site Scripting (XSS) and the ability to bypass web application firewall protection.

---

## General Recommendations

### How to avoid it

Perform URL encoding on all inputs before adding them to the request, such as CRLF characters, to avoid dealing with malicious data.

#### Secure Code Approach

Validate all input, regardless of source on the server side. Validation should be based on a whitelist. Accept only data fitting a specified structure, rather than reject bad patterns. Check for:

- Data type
- Size
- Range
- Format
- Expected values

---

## Source Code Examples

**JavaScript**

**User input is being used in a HTTP request header, enabling an attacker to add a newline character and multiple headers:**

```
var xmlhttp = new XmlHttpRequest();
xmlhttp.open("GET", url, true);
var username = location.search.split('user=')[1];
xmlhttp.setRequestHeader("x-user:", username);
xmlhttp.send();
```

**The user input is examined to contain and newline character and the input is also URL encoded:**

```
var xmlhttp = new XmlHttpRequest();
xmlhttp.open("GET", url, true);
var username = location.search.split('user=')[1];
var safeUsername = encodeURIComponent(username).replace(/[\n\r]/g, '');
xmlhttp.setRequestHeader("x-user:", safeUsername);
xmlhttp.send();
```

# Stored File Manipulation

## Risk

### What might happen

If an attacker can affect arbitrary files of their choice, they may overwrite or corrupt sensitive files, potentially resulting in denial of service. If an attacker is also able to choose the content being written, they may be able to inject code into arbitrary files, potentially resulting in malicious code execution.

---

## Cause

### How does it happen

A user provided input is used to determine which file is to be written into, potentially allowing them to affect or manipulate arbitrary files' contents.

---

## General Recommendations

### How to avoid it

Consider using a static solution for files to whom writing is allowed, such as a list of verified writable files or a different file storage solution, such as a database. If absolutely required, limit writing destination to a single folder by correctly sanitizing user provided inputs to set a filename, and programmatically set the destination folder. Consider supplementing this with a check to ensure whether a file exists or not, per business requirements of application code.

---

## Source Code Examples

# Reflected File Download

## Risk

### What might happen

Reflected File Download (RFD) is a vulnerability that allows attackers to gain RCE (Remote Code Execution) through the web on victim's machine.

In a RFD attack, the victim browses to a malicious URI which downloads a file to the computer and executes OS code, results with RCE.

---

## Cause

### How does it happen

There are 3 requirements for a successful RFD attack:

1) Reflection – User's input should be reflected in the response from the server.

2) Permissive URL – URL or API too permissive that allows an attacker to build a legitimate URI with an executable file extension.

3) Download Response – Download the response instead of rendering it, the browser will set the file with the file extension that was in the URI from (2).

---

## General Recommendations

### How to avoid it

- Use Encoding – Escaping the characters will not help since the problematic characters still exist, hence encoding is required instead.
- Content-Disposition with Filename attribute for API – Content-Disposition response header defines how to process the response and used to attach additional metadata, such as the filename. Setting the filename attribute will spare from the browser to guess the type of the resource and prevent of adding unnecessary executable extensions.
- CSRF Token – If possible, use a CSRF token in order to prevent attackers from creating a valid link to send to victims.
- Custom Headers – By requiring a custom HTTP header for the API calls, it's possible to use Same-Origin-Policy on the client side. This will make RFD unexploitable, unless there is an additional vulnerability involved.
- Remove support for path parameters – If not needed, support for path parameters should be removed.
- Add X-Content-Type-Options header – Adding X-Content-Type-Options: nosniff will prevent attackers from making the browsers "guess" that the file's intended content is executable and download it.

---

## Source Code Examples

**Java**
**Setting the filename attribute**

```
response.setHeader("Content-Disposition", "attachment; filename=" + filename);
```

**CSharp**
**Setting the filename attribute**

```
Response.AddHeader("Content-Disposition", "attachment; filename=" +filename);
```

**JavaScript**
**Setting the filename attribute**

```
res.setHeader('Content-disposition', 'attachment; filename=' + filename);
```

# Client Reflected File Download

## Risk

### What might happen

Reflected File Download (RFD) is a vulnerability that allows attackers to gain RCE (Remote Code Execution) through the web on victim's machine.

In a RFD attack, the victim browses to a malicious URI which downloads a file to the computer and executes OS code, results with RCE.

---

## Cause

### How does it happen

There are 3 requirements for a successful RFD attack:

1) Reflection – User's input should be reflected in the response from the server.

2) Permissive URL – URL or API too permissive that allows an attacker to build a legitimate URI with an executable file extension.

3) Download Response – Download the response instead of rendering it, the browser will set the file with the file extension that was in the URI from (2).

---

## General Recommendations

### How to avoid it

- Use Encoding – Escaping the characters will not help since the problematic characters still exist, hence encoding is required instead.
- Content-Disposition with Filename attribute for API – Content-Disposition response header defines how to process the response and used to attach additional metadata, such as the filename. Setting the filename attribute will spare from the browser to guess the type of the resource and prevent of adding unnecessary executable extensions.
- CSRF Token – If possible, use a CSRF token in order to prevent attackers from creating a valid link to send to victims.
- Custom Headers – By requiring a custom HTTP header for the API calls, it's possible to use Same-Origin-Policy on the client side. This will make RFD unexploitable, unless there is an additional vulnerability involved.
- Remove support for path parameters – If not needed, support for path parameters should be removed.
- Add X-Content-Type-Options header – Adding X-Content-Type-Options: nosniff will prevent attackers from making the browsers "guess" that the file's intended content is executable and download it.

---

## Source Code Examples

# Client Use Of JQuery Outdated Version

## Risk

### What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions. However, even if deprecated code is used in a way that is completely secure, its very use and inclusion in the code base would encourage developers to re-use the deprecated element in the future, potentially leaving the application vulnerable to attack, which is why deprecated code should be eliminated from the code-base as a matter of practice.
Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.

---

## Cause

### How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

---

## General Recommendations

### How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

---

## Source Code Examples

# Deserialization of Untrusted Data

## Risk

### What might happen

Deserialization of untrusted data may allow attackers to craft and provide a malicious object to the deserializing code. If a dangerous object is unsecurely deserialized, it may result in execution of code or operating system commands, by invoking classes or methods potentially available to the object during the deserialization process.

Additionally, deserialization may bypass logical object validation. Since deserialization often uses its own means of constructing a new object from the serialized data, it may bypass checks enforced in constructors or setters, which would allow attackers to deserialize an object whose properties are not validated, incorrect or outright malicious. This may lead to unexpected behavior, affecting logic in ways that are entirely dependent on implementation.

In PHP, deserialization will only affect objects in scope, and will only trigger their __construct() and __destruct() methods; this is because many "dangerous" methods in PHP are actually language constructs, and may not be invoked via serialization. This means that deserialization may still enable logic bypasses or exploitation of existing objects, but only if they employ a constructor or destructor whose implementation would pose a threat to the application. For example - a destructor that creates a file based on instance variables, which can be manipulated via deserialization, could allow attackers to use this class destructor to write a file with malicious code.

---

## Cause

### How does it happen

Object serialization and deserialization is integral to the process of remoting, wherein objects are passed between code instances over an intermediary medium, such as over a network. During deserialization, a new object is constructed from a serialized object provided over the medium; however, if the object being deserialized is untrusted, an unexpected and potentially dangerous object can be provided.

---

## General Recommendations

### How to avoid it

- Where possible, do not pass serialized object between remote instances. Instead, consider passing value primitives between instances and use these values to populate a newly constructed object.
- If required, use a whitelist approach to passed objects. Always ensure the passed object is known, trusted and expected. Do not dynamically construct an object from any source unless the object has been verified and is of a trusted, known type, and may not contain untrusted objects within it.

---

## Source Code Examples

### PHP

#### Create New User with unserialize()

```
//.. JSON Validity Checks ..//
$user_params = json_decode($HTTP_RAW_POST_DATA);
$user = unserialize($user_params);
```

**Create New User from JSON using Parameters**

```
//.. JSON Validity Checks ..//
$user_params = json_decode($HTTP_RAW_POST_DATA);
//.. Parameter Checks ..//
$name = $user_params['Name'];
$email = $user_params['Email'];
$phone = $user_params['Phone'];
$user = new User($name, $email, $phone);
```

# Use of Hard coded Cryptographic Key

## Risk

### What might happen

Static, unchangeable encryption keys in the source code can be stolen by an attacker with access to the source code or the application binaries. Once the attacker has the encryption key, this can be used to gain access to any encrypted secret data, thus violating the confidentiality of the data. Furthermore, it would be impossible to replace the encryption key once stolen. Note that if this is a product that can be installed numerous times, the encryption key will always be the same, allowing an attacker to break all instances at the same cost.

---

## Cause

### How does it happen

The application code uses an encryption key to encrypt and decrypt sensitive data. While it is important to create this encryption key randomly and keep it secret, the application has a single, static key embedded in plain text in the source code.
An attacker could gain access to the source code - whether in the source control system, developer workstations, or the server filesystem or product binaries themselves. Once the attacker has gained access to the source code, it is trivial to retrieve the plain text encryption key and use it to decrypt the sensitive data that the application was protecting.

---

## General Recommendations

### How to avoid it

Generic Guidance:

- Do not store any sensitive information, such as encryption keys, in plain text.
- Never hardcode encryption keys in the application source code.
- Implement proper key management, including dynamically generating random keys, protecting keys, and replacing keys as necessary.

Specific Recommendations:

- Remove the hardcoded encryption key from the application source code. Instead, retrieve the key from an external, protected store.

---

## Source Code Examples

### Java

#### Common example of hardcoded encryption key

```
//Generate a key
string encryptionKey = "EncryptionKey123"

//Encrypt the data
SecretKeySpec keySpec = new SecretKeySpec(encryptionKey.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
cipher.init(Cipher.ENCRYPT_MODE, keySpec);
output = cipher.doFinal(input)
```

# XSRF

## Risk

### What might happen

An attacker could cause the victim to perform any action for which the victim is authorized, such as transferring funds from the victim's account to the attacker's. The action will be logged as being performed by the victim, in the context of their account, and potentially without their knowledge that this action has occurred.

## Cause

### How does it happen

The application performs some action that modifies database contents, based purely on HTTP request content, and does not require per-request renewed authentication (such as transaction authentication or a synchronizer token), instead relying solely on session authentication. This means that an attacker could use social engineering to cause a victim to browse to a link which contains a transaction request to the vulnerable application, submitting that request from the user's browser. Once the application receives the request, it would trust the victim's session, and would perform the action. This type of attack is known as Cross-Site Request Forgery (XSRF or CSRF).

A Cross-Site Request Forgery attack relies on the trust between a server and an authenticated client. By only validating the session, the server ensures that a request has emerged from a client's web-browser. However, any website may submit GET and POST requests to other websites, to which the browser will automatically add the session token if it is in a cookie. This cross-site request can then be trusted as arriving from the user's browser, but does not validate that it was their intent was to make this request.

## General Recommendations

### How to avoid it

Mitigating XSRF requires an additional layer of authentication that is built into the request validation mechanism. This mechanism would attach an additional token that only applies to the given user; this token would be available within the user's web-page, but will not be attached automatically to a request from a different website (e.g. not stored in a cookie). Since the token is not automatically attached to the request, and is not available to the attacker, and is required by the server to process the request, it would be completely impossible for the attacker to fill in a valid cross-site form that contains this token.

Many platforms offer built-in XSRF mitigation functionality which should be used, and perform this type of token management under the hood. Alternatively, use a known or trusted library which adds this functionality.

If implementing XSRF protection is required, this protection should adhere to the following rules:

- Any state altering form (Create, Update, Delete operations) should enforce XSRF protection, by adding an XSRF token to every state altering form submission on the client.
- An XSRF token should be generated, and be unique per-user per-session (and, preferably, per request).
- The XSRF token should be inserted into the client side form, and be submitted to the server as part of the form request. For example, it could be a hidden field in an HTML form, or a custom header added by a Javascript request.
- The XSRF token in the request body or custom header must then be verified as belonging to the current user by the server, before a request is authorized and processed as valid.

# Source Code Examples

## CSharp

### HttpRequest content is used in a database query without any validation of that content

```
public class XSRF
{
        public void foo(SqliteConnection connection, HttpRequest Request)
    {
                string input = Request.QueryString["user"];
                string sql = "insert into Comments(comment) values (@user)";
                MySqlCommand cmd = new MySqlCommand(sql, connection);
            cmd.Parameters.AddwithValue(@user, input);
            connection.Open();
            SqlDataReader reader = cmd.ExecuteReader();
        }
}
```

### The HttpRequest content is validated using AntiXsrfTokenKey

```
public class XSRFFixed
{
        public void foo(SqliteConnection connection, AntiXsrf AntiXsrfTokenKey, HttpRequest
Request)
    {
                string input = AntiXsrfTokenKey.Validate(Request.QueryString["user"]);
                string sql = "insert into Comments(comment) values (@user)";
                MySqlCommand cmd = new MySqlCommand(sql, connection);
            cmd.Parameters.AddwithValue(@user, input);
            connection.Open();
            SqlDataReader reader = cmd.ExecuteReader();
        }

}
```

# Trust Boundary Violation

## Risk

### What might happen

Application developers may treat user input as trusted data, potentially creating an input-based vulnerability such as SQL Injection or Cross-Site Scripting.

## Cause

### How does it happen

The application places user input, which is untrusted data, in the server-side Session folder, which is considered a trusted location. This could lead developers to treat untrusted data as trusted.

## General Recommendations

### How to avoid it

1. Validate and sanitize all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
2. Don't mix untrusted user input with trusted data.

## Source Code Examples

### CSharp

#### Input from the user is added to the current session without sanitizing it

```
public class TrustBoundaryViolation
{
        public void foo()
    {
                string input = Console.ReadLine();
                HttpContext.Current.Session[□val□] = input;
        }
}
```

**The numbers are extracted from the user inputed data before use**

```
public class TrustBoundaryViolationFixed
{
        public void foo()
    {
                string input = Console.ReadLine();
                string inputValue = int.Parse(input).ToString();
                HttpContext.Current.Session[□val□] = inputValue;
        }
}
```

# Stored XPath Injection

## Risk

### What might happen

An attacker that can modify the XPath query with an arbitrary expression will be able to control which nodes in the XML document will be selected, and thus what data the application will process. This can have various effects depending on the type of XML document and its usage, including retrieval of secret information, control of application flow, modification of sensitive data, reading arbitrary files, or even authentication bypass, impersonation, and privilege escalation.

---

## Cause

### How does it happen

The application queries an XML document by using a textual XPath query. The application creates the query by simply concatenating strings, including untrusted data potentially under an attacker's control. Since the external data is neither checked for data type validity nor subsequently sanitized, the data could be maliciously crafted to cause the application to select the wrong information from the XML document.

---

## General Recommendations

### How to avoid it

- Validate all external data, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
  - Data type
  - Size
  - Range
  - Format
  - Expected values
- Avoid making the XPath query dependent on external data.
- If it is absolutely necessary to include untrusted data in the query, the data must at least be first properly validated or sanitized.
- If possible, it is preferable to map XPath queries to external parameters, maintaining separation between data and code.

---

## Source Code Examples

# Hardcoded Absolute Path

## Risk

### What might happen

Generally, hardcoding absolute paths makes the application brittle, and will prevent the program from operating properly in some environments that do not have the identical file system structure. This will also cause software maintenance problems in future versions of the application, if the design or requirements were to change.

Additionally, if the application uses this path to read or write data, this can cause a breach of confidentiality or allow malicious input into the program. In some situations, this vulnerability might even allow a malicious user to override the expected functionality, and cause the application to run any arbitrary program and execute any code the attacker deploys to the server.

---

## Cause

### How does it happen

Hardcoded paths are less flexible, and do not allow the application to account for changes in the environment. For example, the program might be installed in a different directory than the default. Likewise, different system languages and OS architectures can change the names of the system folders; for example, in a Spanish Windows machine there could be "`C:\Archivos de programa (x86)\`" instead of "`C:\Program Files\`".

Moreover, on Windows by default all directories and files created outside of the system folders and outside the user's profile, will be allow full read and write access to any authenticated user. An unauthorized, malicious user could access any sensitive data in these folders, despite the application assuming they are protected. Even worse, an attacker could overwrite existing programs in these unprotected folders and plant malicious code, which will be activated by the application.

---

## General Recommendations

### How to avoid it

- Do not hardcode absolute paths into the application.
- Instead, store the absolute paths in an external configuration file, that can be modified as required for each environment.
- Alternatively, use paths relative to the current application, if the target file is in a subdirectory of the application's root.
- Do not assume a specific file system structure, outside of the application's subdirectories. On Windows, use the built-in expandable variables, such as `%WINDIR%`, `%PROGRAMFILES%`, and `%TEMP%`.
- On Linux and other OS where available, implement a system jail (chroot) for the application, and store all programs and data files there only.
- Prefer storing all executables under the protected program directory (under "`C:\Program Files\`" by default on Windows).
- Do not store sensitive data or configuration files in arbitrary folders. Likewise, do not store data files in the program directory. Instead, use the designated folders as intended, i.e. `%PROGRAMDATA%` and `%APPDATA%` on Windows, respectively.
- Configure hardened permissions to the most restricted as possible, according to the Principle of Least Privilege. Consider implementing this automatically in the installation and setup routines.

---

## Source Code Examples

### Java

#### Hardcoded Path to Data File

```
public File getLogFile() {
      String filename = "C:\Logs\myapp.log";
      File logFile = new File(filename);

      return logFile;
}
```

#### Configured Path for Data File

```
public File getLogFile() {
      Properties props = this.Properties;
      String filename = (String)props.get("logDirectory") + (String)props.get("logFilename");

      File logFile = new File(filename);

      return logFile;
}
```

# Use Of Hardcoded Password

## Risk

### What might happen

Hardcoded passwords expose the application to password leakage. If an attacker gains access to the source code, she will be able to steal the embedded passwords, and use them to impersonate a valid user. This could include impersonating end users to the application, or impersonating the application to a remote system, such as a database or a remote web service.
Once the attacker succeeds in impersonating the user or application, she will have full access to the system, and be able to do anything the impersonated identity could do.

---

## Cause

### How does it happen

The application codebase has string literal passwords embedded in the source code. This hardcoded value is used either to compare to user-provided credentials, or to authenticate downstream to a remote system (such as a database or a remote web service).
An attacker only needs to gain access to the source code to reveal the hardcoded password. Likewise, the attacker can reverse engineer the compiled application binaries, and easily retrieve the embedded password. Once found, the attacker can easily use the password in impersonation attacks, either directly on the application or to the remote system.
Furthermore, once stolen, this password cannot be easily changed to prevent further misuse, unless a new version of the application is compiled. Moreover, if this application is distributed to numerous systems, stealing the password from one system automatically allows a class break in to all the deployed systems.

---

## General Recommendations

### How to avoid it

- Do not hardcode any secret data in source code, especially not passwords.
- In particular, user passwords should be stored in a database or directory service, and protected with a strong password hash (e.g. bcrypt, scrypt, PBKDF2, or Argon2). Do not compare user passwords with a hardcoded value.
- Sytem passwords should be stored in a configuration file or the database, and protected with strong encryption (e.g. AES-256). Encryption keys should be securely managed, and not hardcoded.

---

## Source Code Examples

### Java

### Hardcoded Admin Password

```
bool isAdmin(String username, String password) {
    bool isMatch = false;

    if (username.equals("admin")) {
        if (password.equals("P@ssw0rd"))
            return isMatch = true;
    }

    return isMatch;
```

```
}
```

### No Hardcoded Credentials

```
bool isAdmin(String username, String password) {
    bool adminPrivs = false;

    if (authenticateUser(username, password)) {
        UserPrivileges privs = getUserPrivileges(username);

        if (privs.isAdmin)
            adminPrivs = true;
    }

    return adminPrivs;
}
```

# Improper Exception Handling

## Risk

### What might happen

- An attacker could maliciously cause an exception that could crash the application, potentially resulting in a denial of service (DoS).
- Inadvertent application crashes may occur.

---

## Cause

### How does it happen

The application performs some operation, such as database or file access, that could throw an exception. Since the application is not designed to properly handle the exception, the application could crash.

---

## General Recommendations

### How to avoid it

Any method that could cause an exception should be wrapped in a try-catch block that:

- Explicitly handles expected exceptions
- Includes a default solution to explicitly handle unexpected exceptions

---

## Source Code Examples

### CSharp

**Always catch exceptions explicitly.**

```
try
{
// Database access or other potentially dangerous function
}
catch (SqlException ex)
{
// Handle exception
}
catch (Exception ex)
{
// Default handler for unexpected exceptions
}
```

**Java**

**Always catch exceptions explicitly.**

```
try
{
// Database access or other potentially dangerous function
}
catch (SQLException ex)
{
// Handle exception
}
catch (Exception ex)
{
// Default handler for unexpected exceptions
}
```

# Information Exposure Through an Error Message

## Risk

### What might happen

Exposed details about the application's environment, users, or associated data (for example, stack trace) could enable an attacker to find another flaw and help the attacker to mount an attack. This may also leak sensitive data, e.g. passwords or database fields.

---

## Cause

### How does it happen

The application handles exceptions in an insecure manner, including raw details directly in the error message. This could occur in various ways: by not handling the exception; printing it directly to the output or file; explicitly returning the exception object; or by configuration. These exception details may include sensitive information that could leak to the users due to the occurrence of the runtime error.

---

## General Recommendations

### How to avoid it

- Do not expose exception data directly to the output or users, instead return an informative, generic error message. Log the exception details to a dedicated log mechanism.
- Any method that could throw an exception should be wrapped in an exception handling block that:
  - Explicitly handles expected exceptions.
  - Includes a default solution to explicitly handle unexpected exceptions.
- Configure a global handler to prevent unhandled errors from leaving the application.

---

## Source Code Examples

# XSS Evasion Attack

## Risk

### What might happen

An attacker could bypass the regular channels made by the system to avoid Cross-Site Scripting (XSS) attacks in order to inject JavaScript or HTML code. By using social engineering to cause a user to access the website with injection inputs, such as a URL with engineered session attributes, causing the browser to rewrite web pages. The attacker can then pretend to be the original website, which would enable the attacker to steal the user's session, request the user's credentials, provide false information, or run malware. From the victim's point of view, this is the original website's action.

---

## Cause

### How does it happen

The application web page includes data from a client-side controlled data (including the page session). The user input is embedded in the page, causing the browser to display it as part of the web page. If the input includes HTML fragments or JavaScript, these are displayed too, and the user cannot tell that this is not the intended page. The vulnerability is the result of embedding arbitrary client-side controlled input without first encoding it in a format that would prevent the browser from treating it like HTML instead of plain text.

---

## General Recommendations

### How to avoid it

Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:

- Data type
- Size
- Range
- Format
- Expected values

**Secure-Coding Approach**

Fully encode all dynamic data before embedding it in the webpage. Encoding should be context-sensitive. For example:

  - HTML encoding for HTML content.
  - HTML Attribute encoding for data output to attribute values.
  - JavaScript encoding for JavaScript.

It is recommended to use the known libraries for encoding output, such as ESAPI.

---

## Source Code Examples

### JavaScript

**Dynamically calling a function without sanitizing the input:**

```
var input = document.getElementById("id").value;
```

```
window.setInterval( myFunc(input), 1000);
```

**Sanitizing input before using it in a function:**

```
var input = document.getElementById("id").value;
var trusted = escape(input);
window.setInterval( myFunc(trusted), 1000);
```

**For dynamically updating HTML in the DOM, use the OWASP ESAPI4JS library:**

```
document.write("<%=Encoder.encodeForJS(Encoder.encodeForHTML(untrustedData))%>");
```

**If you must set code to be called dynamically, only call predefined methods or hard-coded Javascript. Never call "eval()" or dynamically create code:**

```
window.setInterval( "timedFunction();", 1000);
```

**If you must set code to be called dynamically, only call predefined methods or hard-coded Javascript. Never call "eval()" or dynamically create code:**

```
window.setInterval( "timedFunction();", 1000);
```

# Insufficiently Protected Credentials

## Risk

### What might happen

An attacker could steal user credentials, enabling access to user accounts and confidential data.

## Cause

### How does it happen

User passwords are written to the database without being properly encrypted with a cryptographic hash. The application reads clear passwords straight from the database.

## General Recommendations

### How to avoid it

Store passwords using a cryptographic hash designed as a password protection scheme, such as:

- bcrypt
- scrypt
- PBKDF2 (with random salt) These need to be configured with an appropriately high work effort.

## Source Code Examples

### CSharp

**Always use a secure password protection scheme to store passwords, such as bcrypt:**

```
string hashed = BCrypt.HashPassword(password, BCrypt.GenerateSalt(12));
```

**For password verification, use the matching function:**

```
bool isValid = BCrypt.CheckPassword(candidate, hashed);
```

**Java**

**Always use a secure password protection scheme to store passwords, such as bcrypt:**

```
String hashed = BCrypt.hashpw(password, BCrypt.gensalt(12));
```

**For password verification, use the matching function:**

```
bool isValid = BCrypt.checkpw(candidate, hashed);
```

# Reliance on Cookies in a Decision

## Risk

### What might happen

Cookie values are used in making a decision without validating their contents - this may allow users to tamper with these cookies thus affecting the outcome of this decision, despite not being authorized to do so. This may lead to authorization and authentication bypasses, whose exploitation may lead to account theft, elevation of privilege and more, depending on implementation.

---

## Cause

### How does it happen

Cookie values are usually set by the server, via the Set-Cookie header, or via client-side code - thereby resulting in these values not being transparent to end-users. However, tampering with the values of these cookies is trivial, and therefore their contents should be treated as potentially malicious or tainted inputs.

---

## General Recommendations

### How to avoid it

For any session-related decisions, never rely on user inputs alone - always validate user authority and authenticity from trusted credentials, such as a session variable, before relying on cookie values in a decision.

---

## Source Code Examples

### Java

#### User Creation Relying on Admin Role With Role Derived From Cookies

```
Cookie[] cookiejar = request.getCookies();
if (cookies != null) {
      for (Cookie cookie : cookiejar) {
            if (cookie.getName().equals("role") && cookie.getValue().equals("admin")) {
                  addUser(username, email, password, role);
            }
        else
        {
            unauthorizedError();
        }
      }
}
else
{
      unauthorizedError();
}
```

#### User Creation Relying on Admin Role With Role Derived From Session Variables

```
String role = request.getSession(true).getAttribute("role"); // role attribute must never be
set with input from users
if (role != null) {
      if (role.equals("admin")) {
             addUser(username, email, password, role);
      }
      else
     {
      unauthorizedError();
     }
}
else
{
      unauthorizedError();
}
```

# Use of Broken or Risky Cryptographic Algorithm

## Risk

### What might happen

Using a weak or broken algorithm ruins the protection granted by using cryptographic mechanisms in the first place, harming the confidentiality or integrity of sensitive user data. This could allow an attacker to steal secret information, alter sensitive data, or forge the source of modified messages.

---

## Cause

### How does it happen

The application code specifies the name of the selected cryptographic algorithm, either via a String argument, a factory method, or a specific implementation class. These algorithms have fatal cryptographic weaknesses, that make it trivial to break in a reasonable timeframe. Strong algorithms should withstand attacks far beyond the realm of possible.

---

## General Recommendations

### How to avoid it

- Only use strong, approved cryptographic algorithms, including AES, RSA, ECC, and SHA-256 respectively, amongst others.
- Do not use weak algorithms that are considered completely broken, such as DES, RC4, and MD5, amongst others.
- Avoid, where possible, using legacy algorithms that are not considered "future-proof" with sufficient safety margins, even though they are considered "safe enough" for today. This includes algorithms that are weaker than they should be, and have stronger replacements, even if they are not yet fatally broken - such as SHA-1, 3DES,
- Consider using a relevant official set of classifications, such as NIST or ENISA. If possible, use only FIPS 140-2 certified algorithm implementations.

---

## Source Code Examples

### Java

#### Legacy Encryption with DES

```
private static byte[] encrypt(String plainText) {
      byte[] encData;

    SecretKey key = new SecretKeySpec(SECRET_KEY, "DES");

      Cipher cipher = Cipher.getInstance("DES/ECB/NoPadding");
      cipher.init(Cipher.ENCRYPT_MODE, key);

      encData = cipher.doFinal(plainText.getBytes());
      byte[] iv = cipher.getIV();

      return encData;
```

```
}
```

### Modern Encryption with AES

```
private static byte[] encrypt(String plainText) {
      byte[] encData;

      try {
        SecretKey key = new SecretKeySpec(SECRET_KEY_FROM_CONFIG, "AES");

        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
                    // Consider a stronger mode, such as GCM / CCM / or other AEAD mode, if
required
        cipher.init(Cipher.ENCRYPT_MODE, key);

            encData = cipher.doFinal(plainText.getBytes("UTF-8"));
        byte[] iv = cipher.getIV();

    } catch (GeneralSecurityException e) {
        handleError(e);
    }
      return encData;
}
```

# Client JQuery Deprecated Symbols

## Risk

### What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions. However, even if deprecated code is used in a way that is completely secure, its very use and inclusion in the code base would encourage developers to re-use the deprecated element in the future, potentially leaving the application vulnerable to attack, which is why deprecated code should be eliminated from the code-base as a matter of practice.
Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.

---

## Cause

### How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

---

## General Recommendations

### How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

---

## Source Code Examples

# Client Potential ReDoS In Match

## Risk

### What might happen

ReDoS (regular expression denial of service) can use complex patterns to cause a denial of service (DoS). With certain patterns, processing time can grow exponentially in relation to input size. An attacker can use these regular expressions to cause the application to spend a significant amount of computation time processing a regular expression over a data-set, causing the application to hang.

---

## Cause

### How does it happen

ReDoS (regular expression denial of service) is an algorithmic complexity attack, that exploits exponential time worst case complexity. In particular, certain regex patterns - either explicitly coded in the application, or accepted from user input and used for searching text - can cause extreme levels of processing for some input texts. For example, `(a+)+` would hang on an input of a long string of "aaaaaaaaaaaaaaaaaaaaaaa!"

---

## General Recommendations

### How to avoid it

- Do not use input for constructing a regular expression.
- Ensure all hardcoded regexes are not vulnerable to ReDoS, specifically ensuring worst case complexity does not cause the application to hang.
- Strive to avoid unnecessarily complex expressions; craft regular expressions that are as simple as possible.

---

## Source Code Examples

### Java

**Validating date based on user-supplied format**

```
bool validateInput(HttpServletRequest req) {
    string startDate = req.getParameter("startDate");
    string endDate = req.getParameter("endDate");

    string format = readCookieByName(req, "dateFormat");

    if (startDate.matches(format) && endDate.matches(format))
        return true;
    else
        return false;
}
```

**Validating date based on server format**

```
bool validateInput(HttpServletRequest req) {
```

```
    string startDate = req.getParameter("startDate");
    string endDate = req.getParameter("endDate");

    // Constrain available formats to hardcoded list
    string style = readCookieByName(req, "dateStyle");
    string format;
    if (style == "YMD")
        format = "^\d{4}-\d{2}-\d{2}";
    else
        format = "^\d{2}-\d{2}-\d{4}";

    if (startDate.matches(format) && endDate.matches(format))
        return true;
    else
        return false;
}
```

### Checking for username in password with RegEx

```
bool validatePassword(HttpServletRequest req) {
    string username = req.getParameter("username");
    string password = req.getParameter("password");

    // Verifies password does not contain username
    if (password.matches(username))
        return false;
    else
        return true;
}
```

### Checking for username in password without RegEx

```
bool validatePassword(HttpServletRequest req) {
    string username = req.getParameter("username");
    string password = req.getParameter("password");

    // Verifies password does not contain username
    if (password.contains(username))
        return false;
    else
        return true;
}
```

# Client DOM Open Redirect

## Risk

### What might happen

An attacker could use social engineering to get a victim to click a link to the application, so that the user will be immediately redirected to another, arbitrary site. Users may think that they are still in the original application site. The second site may be offensive, contain malware, or, most commonly, be used for phishing.

---

## Cause

### How does it happen

The application redirects the user's browser to a URL provided in a user request, without warning users that they are being redirected outside the site. An attacker could use social engineering to get a victim to click a link to the application with a parameter defining another site to which the application will redirect the user's browser, and the user may not be aware of the redirection.

---

## General Recommendations

### How to avoid it

1. Ideally, do not allow arbitrary URLs for redirection. Instead, create a server-side mapping from user-provided parameter values to legitimate URLs.
2. If it is necessary to allow arbitrary URLs:
    - For URLs inside the application site, first filter and encode the user-provided parameter, and then use it as a relative URL by prefixing it with the application site domain.
    - For URLs outside the application (if necessary), use an intermediate disclaimer page to provide users with a clear warning that they are leaving your site.

---

## Source Code Examples

### CSharp

**Avoid redirecting to arbitrary URLs, instead map the parameter to a list of static URLs.**

```
Response.Redirect(getUrlById(targetUrlId));
```

### Java

**Avoid redirecting to arbitrary URLs, instead map the parameter to a list of static URLs.**

```
Response.Redirect(getUrlById(targetUrlId));
```

**Apex**

# Client Insufficient ClickJacking Protection

## Risk

### What might happen

Clickjacking attacks allow an attacker to "hijack" a user's mouse clicks on a webpage, by invisibly framing the application, and superimposing it in front of a bogus site. When the user is convinced to click on the bogus website, e.g. on a link or a button, the user's mouse is actually clicking on the target webpage, despite being invisible.
This could allow the attacker to craft an overlay that, when clicked, would lead the user to perform undesirable actions in the vulnerable application, e.g. enabling the user's webcam, deleting all the user's records, changing the user's settings, or causing clickfraud.

---

## Cause

### How does it happen

The root cause of vulnerability to a clickjacking attack, is that the application's web pages can be loaded into a frame of another website. The application does not implement a proper frame-busting script, that would prevent the page from being loaded into another frame. Note that there are many types of simplistic redirection scripts that still leave the application vulnerable to clickjacking techniques, and should not be used.
When dealing with modern browsers, applications mitigate this vulnerability by issuing appropriate Content-Security-Policy or X-Frame-Options headers to indicate to the browser to disallow framing. However, many legacy browsers do not support this feature, and require a more manual approach by implementing a mitigation in Javascript. To ensure legacy support, a framebusting script is required.

---

## General Recommendations

### How to avoid it

Generic Guidance:

- Define and implement a a Content Security Policy (CSP) on the server side, including a frame-ancestors directive. Enforce the CSP on all relevant webpages.
- If certain webpages are required to be loaded into a frame, define a specific, whitelisted target URL.
- Alternatively, return a "X-Frame-Options" header on all HTTP responses. If it is necessary to allow a particular webpage to be loaded into a frame, define a specific, whitelisted target URL.
- For legacy support, implement framebusting code using Javascript and CSS to ensure that, if a page is framed, it is never displayed, and attempt to navigate into the frame to prevent attack. Even if navigation fails, the page is not displayed and is therefore not interactive, mitigating potential clickjacking attacks.

Specific Recommendations:

- Implement a proper framebuster script on the client, that is not vulnerable to frame-buster-busting attacks.
    - Code should first disable the UI, such that even if frame-busting is successfully evaded, the UI cannot be clicked. This can be done by setting the CSS value of the "display" attribute to "none" on either the "body" or "html" tags. This is done because, if a frame attempts to redirect and become the parent, the malicious parent can still prevent redirection via various techniques.
    - Code should then determine whether no framing occurs by comparing self === top; if the result is true, can the UI be enabled. If it is false, attempt to navigate away from the framing page by setting the top.location attribute to self.location.

## Source Code Examples

### JavaScript
### Clickjackable Webpage

```
<html>
    <body>

     <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

### Bustable Framebuster

```
<html>
    <head>

     <script>
            if ( window.self.location != window.top.location ) {
                   window.top.location = window.self.location;
            }
        </script>
    </head>

    <body>
        <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

### Proper Framebusterbusterbusting

```
<html>
    <head>

     <style> html {display : none; } </style>
        <script>
            if ( self === top ) {
                   document.documentElement.style.display = 'block';
            }
            else {
                   top.location = self.location;
            }
        </script>
    </head>

    <body>
        <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

# Client Overly Permissive Message Posting

## Risk

### What might happen

If the application does not restrict communication via Web Messaging to a specific domain, the browser will dispatch the application message to any target web page, regardless of the actual location of the target web page. Thus it is possible that the message will be delivered to the wrong page from an untrusted domain. This could leak sensitive application data or user information, allowing a malicious third party to intercept this information. □

---

## Cause

### How does it happen

The HTML5 Web Messaging API allows the message to be posted with a `targetOrigin` parameter. If the value of this URI does not match the current location of the target window's document, the browser will not allow the message to be delivered. Marking the `targetOrigin` parameter with the literal string `"*"` will indicate no preference, and the browser will send the message regardless of the target's location. This can disclose the data to any malicious site that changes the location of the window, even without the user's knowledge.

---

## General Recommendations

### How to avoid it

- Always provide a specific `targetOrigin` to the `.postMessage` function, not `"*"`.
- The `targetOrigin` should be hardcoded, or at least white-listed.

---

## Source Code Examples

### JavaScript

#### Unspecified Target Origin

```
var data = '{"username": "bob", "password": "secret"}';
var popup = window.open(strUrl, "Popup_Window");

popup.postMessage(data, "*");

function receiveMessage(event)

{

  alert(event.data);
}
window.addEventListener("message", receiveMessage, false);
```

#### Always Specify an Exact Target Origin

```
var data = '{"username": "bob", "password": "secret"}';
var popup = window.open(strUrl, "Popup_Window");
```

```
popup.postMessage(data, strUrl);

function receiveMessage(event)
{
  if (event.origin !== strUrl)
    return;

  alert(event.data);
}
window.addEventListener("message", receiveMessage, false);
```

# Client Use Of Iframe Without Sandbox

## Risk

### What might happen

If an attacker can select the name of the library, or the location of the code file that is loaded by the application, they would be able to cause the application to execute arbitrary code. This effectively allows the attacker to control the code run by the application.

---

## Cause

### How does it happen

The application uses untrusted data to specify the library or code file, without proper sanitization. This causes the application to load any arbitrary code, as specified. The loaded code will then be executed.

---

## General Recommendations

### How to avoid it

- Do not dynamically load code libraries, especially not based on user input.
- If it is necessary to use untrusted data to select the library to be loaded, verify the selected library name matches a predefined set of whitelisted library names. Alternatively, use the value as an identifier to select from the whitelisted libraries.
- Validate any untrusted data used to load or process libraries or code files.

---

## Source Code Examples

# Possible Flow Control

## Risk

### What might happen

An attacker with the ability of controling program's flow might control the output of the program and result with an unexpected output.

---

## Cause

### How does it happen

This will occur when variables from user input are used in control flow decisions.

---

## General Recommendations

### How to avoid it

User input should not be taken into consideration as part of program's control flow.

---

## Source Code Examples

### Java

#### User input affects the while loop

```
boolean public login(user){
      while(user){
     //do something
     }
      return true;
}
```

#### User input does not affects the while loop

```
boolean isAdmin = false;

boolean public login(user){
  boolean isAdmin = isAuthorized(user);
  while(isAdmin){
   // do something
  }
  return true;
}
```

# Client Potential DOM Open Redirect

## Risk

### What might happen

An attacker could use social engineering to get a victim to click a link to the application, so that the user will be immediately redirected to another, arbitrary site. Users may think that they are still in the original application site. The second site may be offensive, contain malware, or, most commonly, be used for phishing.

---

## Cause

### How does it happen

The application redirects the user's browser to a URL provided in a user request, without warning users that they are being redirected outside the site. An attacker could use social engineering to get a victim to click a link to the application with a parameter defining another site to which the application will redirect the user's browser, and the user may not be aware of the redirection.

---

## General Recommendations

### How to avoid it

1. Ideally, do not allow arbitrary URLs for redirection. Instead, create a server-side mapping from user-provided parameter values to legitimate URLs.
2. If it is necessary to allow arbitrary URLs:
    - For URLs inside the application site, first filter and encode the user-provided parameter, and then use it as a relative URL by prefixing it with the application site domain.
    - For URLs outside the application (if necessary), use an intermediate disclaimer page to provide users with a clear warning that they are leaving your site.

---

## Source Code Examples

# Client Hardcoded Domain

## Risk

### What might happen

An externally imported Javascript file may leave users vulnerable to attack - if the Javascript's host is compromised, if communications with the host are intercepted or if the host itself is not trustworthy, then the contents of the Javascript file may change to have malicious code, which could result in a Cross-Site Scripting (XSS) attack.

---

## Cause

### How does it happen

Javascript files can be imported dynamically from remote hosts when they are embedded into HTML. However, this reliance on a remote host for these scripts may diminish security, as web-application's users are only ever as secure as the remote host serving these Javascript files.

---

## General Recommendations

### How to avoid it

Where possible, host all script files locally, rather than remotely. Ensure that locally hosted 3rd party script files are constantly updated and maintained.

---

## Source Code Examples

**JavaScript**

**Remote Importation of A Script File**

```
<script src="https://example.com/scripts/jquery.js" />
```

**Local Importation of A Script File**

```
<script src="/scripts/jquery.js" />
```

# Use Of Hardcoded Password

## Risk

### What might happen

Hardcoded passwords expose the application to password leakage. If an attacker gains access to the source code, she will be able to steal the embedded passwords, and use them to impersonate a valid user. This could include impersonating end users to the application, or impersonating the application to a remote system, such as a database or a remote web service.
Once the attacker succeeds in impersonating the user or application, she will have full access to the system, and be able to do anything the impersonated identity could do.

---

## Cause

### How does it happen

The application codebase has string literal passwords embedded in the source code. This hardcoded value is used either to compare to user-provided credentials, or to authenticate downstream to a remote system (such as a database or a remote web service).
An attacker only needs to gain access to the source code to reveal the hardcoded password. Likewise, the attacker can reverse engineer the compiled application binaries, and easily retrieve the embedded password. Once found, the attacker can easily use the password in impersonation attacks, either directly on the application or to the remote system.
Furthermore, once stolen, this password cannot be easily changed to prevent further misuse, unless a new version of the application is compiled. Moreover, if this application is distributed to numerous systems, stealing the password from one system automatically allows a class break in to all the deployed systems.

---

## General Recommendations

### How to avoid it

- Do not hardcode any secret data in source code, especially not passwords.
- In particular, user passwords should be stored in a database or directory service, and protected with a strong password hash (e.g. bcrypt, scrypt, PBKDF2, or Argon2). Do not compare user passwords with a hardcoded value.
- Sytem passwords should be stored in a configuration file or the database, and protected with strong encryption (e.g. AES-256). Encryption keys should be securely managed, and not hardcoded.

---

## Source Code Examples

# Unprotected Cookie

## Risk

### What might happen

Cookies that contain the user's session identifier, and other sensitive application cookies, are typically accessible by client-side scripts, such as JavaScript. Unless the web application explicitly prevents this using the "httpOnly" cookie flag, these cookies could be read and accessed by malicious client scripts, such as Cross-Site Scripting (XSS). This flag would mitigate the damage done in case XSS vulnerabilities are discovered, according to Defense in Depth.

Likewise, sensitive cookies could be exposed by being sent over unprotected HTTP protocol, allowing attackers to sniff the users' requests and impersonate them to the application.

---

## Cause

### How does it happen

The web application framework, by default, does not set the "httpOnly" flag for the application's sessionid cookie and other sensitive application cookies. Likewise, the application does not explicitly use the "httpOnly" cookie flag, thus allowing client scripts to access the cookies by default.

Similarly, cookies that lack the "secure" flag will be automatically sent by the browser to the web server, regardless of the safety of the underlying protocol, such as unprotected HTTP. Cookies that are flagged with the "secure" attribute will only be sent over a secure HTTPS connection.

---

## General Recommendations

### How to avoid it

- Always set the "httpOnly" flag for any sensitive server-side cookie.

- It is highly recommended to implement HTTP Strict Transport Security (HSTS) in order to ensure that the cookie will be sent over a secured channel.

- Explicitly set the "httpOnly" flag for each cookie set by the application.

- Configure and set all sensitive cookies to be created with the "secure" attribute.

---

## Source Code Examples

### JavaScript

### Setting Cookie with Express

```
var express = require('express');
var app = express();

app.use(express.cookieParser());

app.get('/', function(req, res) {
```

```
      res.cookie('DepartmentID', getUserDept());
      res.send(getUserPage());
});

app.listen(SERVER_PORT);
```

### Using Express for Secure Cookies

```
var express = require('express');
var app = express();

app.use(express.cookieParser());

app.get('/', function(req, res) {
      res.cookie('DepartmentID', getUserDept(),
                {maxAge: 900000,
                 path: APP_ROOT,
                 secure: true,
                 httpOnly: true });

      res.send(getUserPage());
});

app.listen(SERVER_PORT);
```

# Unsafe Use Of Target blank

## Risk

### What might happen

An unsuspecting user might click a vulnerable legitimate-looking link, prepared by an attacker, that leads to a malicious page. The new page that opens can redirect the **original** page to another malicious page and abuse the trust of the user to create a very convincing phishing attack.

---

## Cause

### How does it happen

When opening a new page using an <a> HTML element with the "target" attribute (with any value), or with window.open() within JavaScript, the new page has some access to the original page through the window.opener object. This may allow redirection to a malicious phishing page.

---

## General Recommendations

### How to avoid it

For HTML:

- Do not set the "target" attribute (with any value) for links created by users unless required.
- If required, when using the "target" attribute, also set the "rel" attribute as “noopener noreferrer”:
  - “noopener” for Chrome and Opera
  - “noreferrer” for Firefox and old browsers
  - No similar solution for Safari

For JavaScript:

- When invoking an untrusted new window using "var newWindow = window.open()", set "newWindow.opener=null" before setting "newWindow.location" to a potentially untrusted site, such that when the new site is open in the new window, it has no access to its original "opener" attribute

---

## Source Code Examples

# Unsafe Use Of Target Blank

## Risk

### What might happen

An unsuspecting user might click a vulnerable legitimate-looking link, prepared by an attacker, that leads to a malicious page. The new page that opens can redirect the **original** page to another malicious page and abuse the trust of the user to create a very convincing phishing attack.

---

## Cause

### How does it happen

When opening a new page using an <a> HTML element with the "target" attribute (with any value), or with window.open() within JavaScript, the new page has some access to the original page through the window.opener object. This may allow redirection to a malicious phishing page.

---

## General Recommendations

### How to avoid it

For HTML:

- Do not set the "target" attribute (with any value) for links created by users unless required.
- If required, when using the "target" attribute, also set the "rel" attribute as “noopener noreferrer”:
  - “noopener” for Chrome and Opera
  - “noreferrer” for Firefox and old browsers
  - No similar solution for Safari

For JavaScript:

- When invoking an untrusted new window using "var newWindow = window.open()", set "newWindow.opener=null" before setting "newWindow.location" to a potentially untrusted site, such that when the new site is open in the new window, it has no access to its original "opener" attribute

---

## Source Code Examples

# Unsafe Use Of Target blank

## Risk

### What might happen

An unsuspecting user might click a vulnerable legitimate-looking link, prepared by an attacker, that leads to a malicious page. The new page that opens can redirect the **original** page to another malicious page and abuse the trust of the user to create a very convincing phishing attack.

---

## Cause

### How does it happen

When opening a new page using an <a> HTML element with the "target" attribute (with any value), or with window.open() within JavaScript, the new page has some access to the original page through the window.opener object. This may allow redirection to a malicious phishing page.

---

## General Recommendations

### How to avoid it

For HTML:

- Do not set the "target" attribute (with any value) for links created by users unless required.
- If required, when using the "target" attribute, also set the "rel" attribute as “noopener noreferrer”:
  - “noopener” for Chrome and Opera
  - “noreferrer” for Firefox and old browsers
  - No similar solution for Safari

For JavaScript:

- When invoking an untrusted new window using "var newWindow = window.open()", set "newWindow.opener=null" before setting "newWindow.location" to a potentially untrusted site, such that when the new site is open in the new window, it has no access to its original "opener" attribute

---

## Source Code Examples

### JavaScript

### Unsafe Use of Window.Open()

```
function newWindowOpener(untrustedURL) {
      var newWindow=window.open();
      newWindow.location=untrustedURL;
}
```

### Safe Use of Window.Open()

```
function newWindowOpenerSafe(untrustedURL) {
      var newWindow=window.open();
      newWindow.opener=null;
      newWindow.location=untrustedURL;
}
```

## Scanned Languages

| Language | Hash Number | Change Date |
|---|---|---|
| JavaScript | 0109410431041810 | 1/15/2020 |
| VbScript | 2005446206231574 | 1/15/2020 |
| PHP | 7396726361170830 | 1/15/2020 |
| Typescript | 1488217042171263 | 1/15/2020 |
| Common | 1154814993014328 | 9/25/2020 |