acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

21 November, 2018

Developer Report

Generated by Acunetix WVS Reporter (v10.5 Build 20160217)

Scan of http://simpeg.pushidrosal.id:80/

Scan details

Scan information	
Start time	19/11/2018 8:19:32
Finish time	19/11/2018 10:41:14
Scan time	2 hours, 21 minutes
Profile	Default
Server information	
Responsive	True
Server banner	nginx/1.12.2
Server OS	Unknown
Server technologies	PHP

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	**10**
High	0
Medium	3
Low	6
Informational	1

Knowledge base

List of file extensions

File extensions can provide information on what technologies are being used on this website.
List of file extensions detected:

- css => 3 file(s)
- js => 4 file(s)
- htaccess => 1 file(s)
- php => 1 file(s)

List of client scripts

These files contain Javascript code referenced from the website.

- /asset/js/jquery-latest.js
- /asset/js/bootstrap.min.js
- /asset/js/bootstrap-tooltip.js
- /asset/js/application.js

List of files with inputs

These files have at least one input (GET or POST).

- / - 2 inputs
- /app/index - 1 inputs

List of external hosts

These hosts were linked from this website but they were not scanned because they are not listed in the list of hosts allowed. (Configuration-> Scan Settings ->Scanning Options-> List of hosts allowed).

- fonts.googleapis.com
- simpeg.pushidrosal.id

Alerts summary

.htaccess file readable

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/	1

Application error message

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7,5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/app/index	1

User credentials are sent in clear text

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 9,1 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
CWE	CWE-310

Affected items	Variation
/	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-693

Affected items	Variation
Web Server	1

Cookie without HttpOnly flag set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/	2

Login page password-guessing attack

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 5,3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: Low
CWE	CWE-307

Affected items	Variation
/app/index	1

Possible sensitive directories

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7,5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/system	1

Possible sensitive files

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7,5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/.htaccess	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 7,5 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/	1

Alert details

.htaccess file readable

Severity	**Medium**
Type	Validation
Reported by module	Scripting (htaccess_File_Readable.script)

Description

This directory contains an .htaccess file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

Impact

Possible sensitive information disclosure.

Recommendation

Restrict access to the .htaccess file by adjusting the web server configuration.

Affected items

/

Details

No details are available.

Request headers

```
GET /.htaccess HTTP/1.1
(line truncated) ...ame=fdd0cd1232431ad04c5ca811e7dd4f6d;
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22346489498d0e1ee8abce7253b1
ee52ce%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A10%3A%22user_agent
%22%3Bs%3A107%3A%22Mozilla%2F5.0+%28Windows+NT+6.1%3B+WOW64%29+AppleWebKit%2F537.21+%28K
HTML%2C+like+Gecko%29+Chrome%2F41.0.2228.0+Safari%2F537.21%22%3Bs%3A13%3A%22last_activit
y%22%3Bi%3A1542590439%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Dcdc03bc31302dbc3a2
5ef9e3c59b355b7e08fcaa
Host: simpeg.pushidrosal.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Application error message

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Error_Message.script)

Description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

PHP Runtime Configuration

Affected items

/app/index

Details

URL encoded POST input username was set to 12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'ð??©
Error message found: Internal Server Error

Request headers

```
POST /app/index HTTP/1.1
Content-Length: 125
Content-Type: application/x-www-form-urlencoded
Referer: http://simpeg.pushidrosal.id:80/
(line truncated) ...ame=fdd0cd1232431ad04c5ca811e7dd4f6d;
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22346489498d0e1ee8abce7253b1
ee52ce%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A10%3A%22user_agent
%22%3Bs%3A107%3A%22Mozilla%2F5.0+%28Windows+NT+6.1%3B+WOW64%29+AppleWebKit%2F537.21+%28K
HTML%2C+like+Gecko%29+Chrome%2F41.0.2228.0+Safari%2F537.21%22%3Bs%3A13%3A%22last_activit
y%22%3Bi%3A1542590439%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Dcdc03bc31302dbc3a2
5ef9e3c59b355b7e08fcaa
Host: simpeg.pushidrosal.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

csrf_test_name=fdd0cd1232431ad04c5ca811e7dd4f6d&password=g00dPa%24%24w0rD&username=12345
'"\'\");|]*%00{%0d%0a<%00>%bf%27'ðŸ'©
```

User credentials are sent in clear text

Severity	**Medium**
Type	Configuration
Reported by module	Crawler

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

/

Details

Form name: <empty>
Form action: http://simpeg.pushidrosal.id/app/index
Form method: POST

Form inputs:

- csrf_test_name [Hidden]
- username [Text]
- password [Password]

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: simpeg.pushidrosal.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

Clickjacking Protection for Java EE
Frame Buster Buster
Defending with Content Security Policy frame-ancestors directive
OWASP Clickjacking
Clickjacking
The X-Frame-Options response header

Affected items

Web Server

Details

No details are available.

Request headers

```
GET / HTTP/1.1
Cookie: csrf_cookie_name=fdd0cd1232431ad04c5ca811e7dd4f6d;
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22872af4ba6dc4ac518c3d47719b
644b87%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A10%3A%22user_agent
%22%3Bs%3A50%3A%22Googlebot%2F2.1+%28%2Bhttp%3A%2F%2Fwww.googlebot.com%2Fbot.html%29%22%
3Bs%3A13%3A%22last_activity%22%3Bi%3A1542590439%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%
22%3B%7D3097572f4307277b5a373b1a01efef46b4ac88a0
Host: simpeg.pushidrosal.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Cookie without HttpOnly flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Affected items

/

Details

Cookie name: "ci_session"
Cookie domain: "simpeg.pushidrosal.id"

Request headers

```
GET / HTTP/1.1
Cookie: csrf_cookie_name=fdd0cd1232431ad04c5ca811e7dd4f6d;
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22872af4ba6dc4ac518c3d47719b
644b87%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A10%3A%22user_agent
%22%3Bs%3A50%3A%22Googlebot%2F2.1+%28%2Bhttp%3A%2F%2Fwww.googlebot.com%2Fbot.html%29%22%
3Bs%3A13%3A%22last_activity%22%3Bi%3A1542590439%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%
22%3B%7D3097572f4307277b5a373b1a01efef46b4ac88a0
Host: simpeg.pushidrosal.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/

Details

Cookie name: "csrf_cookie_name"
Cookie domain: "simpeg.pushidrosal.id"

Request headers

```
GET / HTTP/1.1
Cookie: csrf_cookie_name=fdd0cd1232431ad04c5ca811e7dd4f6d;
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22872af4ba6dc4ac518c3d47719b
644b87%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A10%3A%22user_agent
%22%3Bs%3A50%3A%22Googlebot%2F2.1+%28%2Bhttp%3A%2F%2Fwww.googlebot.com%2Fbot.html%29%22%
3Bs%3A13%3A%22last_activity%22%3Bi%3A1542590439%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%
22%3B%7D3097572f4307277b5a373b1a01efef46b4ac88a0
Host: simpeg.pushidrosal.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Login page password-guessing attack

Severity	**Low**
Type	Validation
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks

Affected items

/app/index

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /app/index HTTP/1.1
Content-Length: 59
Content-Type: application/x-www-form-urlencoded
Referer: http://simpeg.pushidrosal.id:80/
Host: simpeg.pushidrosal.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*

csrf_test_name=PlUmVzcD&password=UIRIimqn&username=npypechx
```

Possible sensitive directories

Severity	**Low**
Type	Validation
Reported by module	Scripting (Possible_Sensitive_Directories.script)

Description

A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

This directory may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this directory or remove it from the website.

References

Web Server Security and Database Server Security

Affected items

/system

Details

No details are available.

Request headers

```
GET /system HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
(line truncated) ...ame=fdd0cd1232431ad04c5ca811e7dd4f6d;
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22346489498d0e1ee8abce7253b1
ee52ce%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A10%3A%22user_agent
%22%3Bs%3A107%3A%22Mozilla%2F5.0+%28Windows+NT+6.1%3B+WOW64%29+AppleWebKit%2F537.21+%28K
HTML%2C+like+Gecko%29+Chrome%2F41.0.2228.0+Safari%2F537.21%22%3Bs%3A13%3A%22last_activit
y%22%3Bi%3A1542590439%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Dcdc03bc31302dbc3a2
5ef9e3c59b355b7e08fcaa
Host: simpeg.pushidrosal.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Possible sensitive files

Severity	**Low**
Type	Validation
Reported by module	Scripting (Possible_Sensitive_Files.script)

Description

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security

Affected items

/.htaccess

Details

No details are available.

Request headers

```
GET /.htaccess HTTP/1.1
Accept: acunetix/wvs
(line truncated) ...ame=fdd0cd1232431ad04c5ca811e7dd4f6d;
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22346489498d0e1ee8abce7253b1
ee52ce%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A10%3A%22user_agent
%22%3Bs%3A107%3A%22Mozilla%2F5.0+%28Windows+NT+6.1%3B+WOW64%29+AppleWebKit%2F537.21+%28K
HTML%2C+like+Gecko%29+Chrome%2F41.0.2228.0+Safari%2F537.21%22%3Bs%3A13%3A%22last_activit
y%22%3Bi%3A1542590439%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Dcdc03bc31302dbc3a2
5ef9e3c59b355b7e08fcaa
Host: simpeg.pushidrosal.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Password type input with auto-complete enabled

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:
<INPUT TYPE="password" AUTOCOMPLETE="off">

Affected items

/
Details
Password type input named password from unnamed form with action http://simpeg.pushidrosal.id/app/index has autocomplete enabled.
Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: simpeg.pushidrosal.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Scanned items (coverage report)

Scanned 16 URLs. Found 2 vulnerable.

URL: http://simpeg.pushidrosal.id/

Vulnerabilities have been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
/	Path Fragment
/	Path Fragment

Input scheme 2

Input name	Input type
Host	HTTP Header

URL: http://simpeg.pushidrosal.id/app

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/app/index

Vulnerabilities have been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
csrf_test_name	URL encoded POST
password	URL encoded POST
username	URL encoded POST

URL: http://simpeg.pushidrosal.id/asset

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
	URL encoded GET
bg	URL encoded GET

URL: http://simpeg.pushidrosal.id/asset/css

No vulnerabilities have been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
aside	URL encoded GET
bg	URL encoded GET
brand	URL encoded GET
folded	URL encoded GET

URL: http://simpeg.pushidrosal.id/asset/css/docs.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/asset/css/bootstrap.min.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/asset/css/bootstrap-responsive.min.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/asset/img

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/asset/js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/asset/js/jquery-latest.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/asset/js/bootstrap.min.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/asset/js/bootstrap-tooltip.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/asset/js/application.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/system/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://simpeg.pushidrosal.id/index.php

No vulnerabilities have been identified for this URL

No input(s) found for this URL