



Acunetix Threat Level 2

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

Scan Detail

Target	http://disperinaker.smartbojonegoro.id/
Scan Type	Full Scan
Initiated	1/25/2023, 6:01:50 AM
Duration	1 hour, 29 minutes
Total Requests	95951
Average Response Time	1ms
Maximum Response Time	4432ms



High



Medium



Low



Information

Severity	Vulnerabilities	Instances
High	0	0
Medium	4	5
Low	4	4
Information	5	8
Total	13	17

Informational



- Content Security Policy (CSP) not implemented
- Email address found
- Outdated JavaScript library
- Others

Instar

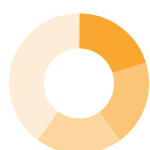
Low Severity



- Clickjacking: X-Frame-Options header missing
- Cookie(s) without HttpOnly flag set
- Login page password-guessing attack
- Others

Instar














Medium Severity



- Laravel debug mode enabled
- Slow HTTP Denial of Service Attack
- User credentials are sent in clear text
- Others

Instar

Impacts

SEVERITY	IMPACT
 Medium	<div>1</div> Laravel debug mode enabled
 Medium	<div>1</div> Slow HTTP Denial of Service Attack
 Medium	<div>1</div> User credentials are sent in clear text
 Medium	<div>2</div> Vulnerable JavaScript library
 Low	<div>1</div> Clickjacking: X-Frame-Options header missing
 Low	<div>1</div> Cookie(s) without HttpOnly flag set
 Low	<div>1</div> Login page password-guessing attack
 Low	<div>1</div> Unencrypted connection
 Information	<div>1</div> Content Security Policy (CSP) not implemented
 Information	<div>1</div> Email address found
 Information	<div>4</div> Outdated JavaScript library
 Information	<div>1</div> Password type input with auto-complete enabled
 Information	<div>1</div> Subresource Integrity (SRI) not implemented

Laravel debug mode enabled

The web application uses Laravel framework. Laravel Debug mode is enabled. Debug mode should be turned off in production environment, as it leads to disclosure of sensitive information about the web application.

Impact

The web application in debug mode discloses sensitive information. This information can be used to launch further attacks.

<http://disperinaker.smartbojonegoro.id/>

Request

GET /_ignition/health-check HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdii6lkp6MDgzUFlWR0JNOWhqVGRZVknBaHc9PSIsInZhbHVljoidndwK2E0VmZ4aHNTbjFNaDJaVFf0VTdZdWFwVWFXRE9oOXJlbXRLWDNWci8zZUd4Q2IwdUI2eTN0L01kTk9IT09QL1E2azd6K2pwQkZ2UlFEYzByaVk0U1BWSUU5ZlVYMxpKYzVueGhKZ2Uxv0RKU09CTU80M3cwVjhlU3NjczMiLCJtYWMiOilwM2U4NzhhOGM3NzMyMDdiMWY0NmQzZjI3MmFkOWY2MzUxOGYwYjVhODY4YjE5ZWUwYmE1OTI0OGIxNDU2ZWVjliwidGFnljoiIn0%3D;laravel_session=eyJpdii6litYNm5vUWNPeENvK3hvd28vSVJWaWc9PSIsInZhbHVljoiieUg2Tk9aVjdza0V1Ui9EVzh4cVNyck12Yy82YTZEUTBrK3oyZ1lOK1ZpVk4xalE2cFpFWEZNOHZneFZxbWRXYlRTdmtVSElRk1RbEZNbUtzMHB5dHN4QzRwTkM0eFNUbHB1N0lIRkdKZ2NseStwcnhXT2RiUGJTTjh5aU1FK0EiLCJtYWMiOiilyNTM3ZjFmM2Y0MzY3M2Q4NjZiNmM5YmM2MWQ4MmYyNzRlNGE1ODAzMTMxMTQ1MDkxZjA0ZTFiZmRkMTg1MDcwliwidGFnljoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: disperinaker.smartbojonegoro.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

Recommendation

Disable the debug mode by setting APP_DEBUG to false

References

[Error Handling](#)
<https://laravel.com/docs/7.x/errors#configuration>

Slow HTTP Denial of Service Attack

Your web server is vulnerable to Slow HTTP DoS (Denial of Service) attacks.

Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service.

Impact

A single machine can take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.

<http://disperinaker.smartbojonegoro.id/>

Time difference between connections: 10001 ms

Recommendation

Consult Web references for information about protecting your web server against this type of attack.

References

[Slowloris DOS Mitigation Guide](#)
https://www.funtoo.org/Slowloris_DOS_Mitigation_Guide
[Protect Apache Against Slowloris Attack](#)
<https://web.archive.org/web/20180329210925/http://blog.secaserver.com/2011/08/protect-apache-slowloris-attack/>

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.

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

Form name: <empty>

Form action: <http://disperinaker.smartbojonegoro.id/login>

Form method: POST

Request

```
GET /login HTTP/1.1
```

Referer: <http://disperinaker.smartbojonegoro.id/>

Cookie: XSRF-

[illegible]

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

Accept-Encoding: gzip,deflate

Host: disperinaker.smartbojonegoro.id

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36

Connection: Keep-alive

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

You are using a vulnerable JavaScript library. 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.

Consult References for more information.

Verified

Detected JavaScript library **jquery** version **2.2.4**.

Detection details: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.

References:

- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>

Request

```
GET /assets/js/jquery.min.js HTTP/1.1
```

Referer: <http://disperinaker.smartbojonegoro.id/>

Cookie: XSRF-

TOKEN=eyJpdjI6InRZRE0rY3V6aHVScQ2VZMkxyRUI3ckE9PSIsInZhbnVHlVjoiF3NmEzYUrd0pEb0VWNNVibnhtdG4yUlZXR0IqdSZNaoVXYXFFb1FfMlNGZm1WMFYzZGN3Z1RRS2h2UXB6NXA5WGE5c3oxcWRxS2ZyTkZCQ2V1VjVjclU1QktWY1FESi9DamNQWjBUC1hQcHFjL2RqYzJXV0VxZ1MNldQS04iLCJyWmMiOiI2JyZmFmZTdmMmNlYjU2MzFhOTc2MmRmRmJmYjU0ZWY4ZGVhYjZmZDIhYtDnTIwOTkyZjZlNDhlMTIwZWZlIiwidGFnIjoiejo03D:laravel session=eyJpdjI6InUvcUlZU21mK09vcXRWRbnk4eXAzZwc9PSIsInZhbnVHlVjoi

3JlZi9ScHUwdGliRmNBtXRRjdscm1YUkN2aVB2bWkxanNFcC9UMnJ6cm1FdmRDTWxQUjliWElsbDR0eS81cHgVb1JudUUrb1hGNE1FYm96T2JZVEJ3aWdBuZBualZEa09HMjFVTzJLdmRiUEd2d2ltN2FzY1VuY2tNWEhucnYiLCJtYWMiOiJmZGQzZjU3YjA3YzY0NmEwOGI3NDM3ODk4ODViZDUxOWZmMzlmM2ZhZWQzZWQ5MzA4Nzk2OTZkYzRlNWVjYTRk1iwiidGFnljoiIn0%3D

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

Accept-Encoding: gzip,deflate

Host: disperinaker.smartbojonegoro.id

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36

Connection: Keep-alive

<http://disperinaker.smartbojonegoro.id/template/vendor/jquery/jquery-3.2.1.min.js>

Verified

Detected JavaScript library **jquery** version **3.2.1**.

Detection details: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.

References:

- https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
- https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
- https://jquery.com/upgrade-guide/3.5/
- https://api.jquery.com/jQuery.htmlPrefilter/

Request

GET /template/vendor/jquery/jquery-3.2.1.min.js HTTP/1.1

Referer: http://disperinaker.smartbojonegoro.id/

Cookie: XSRF-

TOKEN=eyJpdii6InRZRE0rY3V6aHVSQ2VZMkxyRUI3ckE9PSIsInZhbHVlIjoie1F3NmEzYUlrD0pEb0VWNNVibnhtdG4yUlZxR01qSDZNao0VXYXFFb1FFMINGZm1WMFYzZGN3Z1RRS2h2UXB6NXA5WGE5c3oxcWRxS2ZyTkZCQ2V1VVljcUvIQktWY1FESi9DamNQWjBUc1hQcHFjL2RqYzJXV0VxZ11MNldQS04iLCJtYWMiOiI2ZjAyZmFmZTdmMmNIYjU2MzFhOTc2MmRmMjFmYjU0ZWY4ZGVhYjZmZDhYTDlNTlWOTkyYzZlNDlhMTIwZW1ZliwidGFnljoiIn0%3D;laravel_session=eyJpdii6InUvcU1ZU21mK0gvcXRWbnk4eXAzZWc9PSIsInZhbHVlIjoie1F3JlZi9ScHUwdGliRmNBtXRRjdscm1YUkN2aVB2bWkxanNFcC9UMnJ6cm1FdmRDTWxQUjliWElsbDR0eS81cHgVb1JudUUrb1hGNE1FYm96T2JZVEJ3aWdBuZBualZEa09HMjFVTzJLdmRiUEd2d2ltN2FzY1VuY2tNWEhucnYiLCJtYWMiOiJmZGQzZjU3YjA3YzY0NmEwOGI3NDM3ODk4ODViZDUxOWZmMzlmM2ZhZWQzZWQ5MzA4Nzk2OTZkYzRlNWVjYTRk1iwiidGFnljoiIn0%3D

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

Accept-Encoding: gzip,deflate

Host: disperinaker.smartbojonegoro.id

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36

Connection: Keep-alive

Recommendation

Upgrade to the latest version.

Clickjacking: X-Frame-Options header missing

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

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

Impact

The impact depends on the affected web application.

<http://disperinaker.smartbojonegoro.id/>

Request

GET / HTTP/1.1

Cookie: XSRF-

TOKEN=eyJpdii6InRZRE0rY3V6aHVSQ2VZMkxyRUI3ckE9PSIsInZhbHVlIjoie1F3ZsdWg4QlZjZ0p4RjIwMjJlZWQzZWQ5MzA4Nzk2OTZkYzRlNWVjYTRk1iwiidGFnljoiIn0%3D;laravel_session=eyJpdii6InUvcU1ZU21mK0gvcXRWbnk4eXAzZWc9PSIsInZhbHVlIjoie1F3YUWU3Zml3YTc5NTc4MmE4NTljNzg0YzZmZGQzZjU3YjA3YzY0NmEwOGI3NDM3ODk4ODViZDUxOWZmMzlmM2ZhZWQzZWQ5MzA4Nzk2OTZkYzRlNWVjYTRk1iwiidGFnljoiIn0%3D;laravel_session=eyJpdii6InUvcU1ZU21mK0gvcXRWbnk4eXAzZWc9PSIsInZhbHVlIjoie1F3YUWU3Zml3YTc5NTc4MmE4NTljNzg0YzZmZGQzZjU3YjA3YzY0NmEwOGI3NDM3ODk4ODViZDUxOWZmMzlmM2ZhZWQzZWQ5MzA4Nzk2OTZkYzRlNWVjYTRk1iwiidGFnljoiIn0%3D

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: disperinaker.smartbojonegoro.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

Recommendation

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.

References

The X-Frame-Options response header
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

Clickjacking
<https://en.wikipedia.org/wiki/Clickjacking>

OWASP Clickjacking
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

<https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed>

Cookie(s) without HttpOnly flag set

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

Impact

Cookies can be accessed by client-side scripts.

[illegible]

Request

```
GET / HTTP/1.1
Referer: http://disperinaker.smartbojonegoro.id/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: disperinaker.smartbojonegoro.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Recommendation

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

Login page password-guessing attack

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

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

Impact

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

Request

POST /login HTTP/1.1
Referer: http://disperinaker.smartbojonegoro.id/login
Cookie: XSRF-
TOKEN=eyJpdii6Im1RazJBU_nJPYU14N1VSV1NEaIRWVEE9PSIsInZhbHVlIjoiTjJCaU1URXNmN2ZnR3NWRDjmb1NMTWVueUkrRS9aL1luMUY5Qm4vcjhUdzZ3T2tuNHNhbitjY3dSdDRjMkjqNndGVnB5eU1LODBnRDFBTHRfb2Y5dkN5SkRmb3NzQnJ1K05hZEs1N21aQWZudGQ1aVA2ZGZJWbWRKK3k0cW4iLCJtYWMiOiJlYTl2Njk4NzY5OWU3YmE0ZjdINGI3Yzg2ODc0Y2QxMGU2Y2U3ZmQ0Y2M5ZWQ4MDljNWY5YjZlNTQ0NTYzMDkxliwidGFnljoiIn0%3D;laravel_session=eyJpdii6lkVkS3hxYzIPNXNsMENQREU1MUxjSUE9PSIsInZhbHVlIjoisW5SKzZPaEpTaEplTmQ0ZzdUMlM3RW5icmFPMFUxek9yL0JCZkFGRmlhLQ2JhdDBjcWdQWW83cVlaSHA4b1AzaDVITk9WSFB1MjJHRnU2Q3paemR1ZTg2UDN2S00zcjArS25HSFR4TElwdHRZSEc3dUhlRENlczmjV5OGxDTkwiLCJtYWMiOiI0MzU5MTBkYmI1MDkzMmE4ZGU0NjU5ZGJmMmZhYjA5ZTBiZTY5OTk1NDZhZWRjNDIxOTIxOWM1ZjM3ZWJiY2E1liwidGFnljoiIn0%3D;
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 83
Host: disperinaker.smartbojonegoro.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

_token=W9srjPZ4joF4QIYy3mCniYDKevUIId1JM5cZUBuKu&username=author&password=testing&=&

Recommendation

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

References

[Blocking Brute Force Attacks](#)
https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

Request

GET / HTTP/1.1
Referer: http://disperinaker.smartbojonegoro.id/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: disperinaker.smartbojonegoro.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Content Security Policy (CSP) not implemented

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.

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

Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;

Impact

<http://disperinaker.smartbojonegoro.id/>

Request

```
GET / HTTP/1.1
Referer: http://disperinaker.smartbojonegoro.id/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: disperinaker.smartbojonegoro.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Recommendation

References

Content Security Policy (CSP).

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

Implementing Content Security Policy.

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Email address found

One or more email addresses have been found on this page. 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.

Impact

Email addresses posted on Web sites may attract spam.

<http://disperinaker.smartbojonegoro.id/login>

Pattern found:

a@b.c

Request

GET /login HTTP/1.1
Referer: http://disperinaker.smartbojonegoro.id/
Cookie: XSRF-
TOKEN=eyJpdil6Im9xNWQ0ak1QeUQxMklyTHJFNXVGAkc9PSIsInZhbHVlIjoiaSdlVemdd4Vkv6U0M2YmlBakU5S2U3UnBNYk5KV0h4eHdYbWdZbU9PQ3loMDVYU2RDWjZxbUdEQU
Nhb1k0TU1k2cyKzZsK05HcllnanNuQUJlUjRXRVYtRtVxd2VExuZ00vbb29RCdVnVjVMNWJwb21BK0hScnAweTU0SmlFQRk2eXElcJtYWMiOiJhMWM5MWNlMGE1Y2M3NjE4ZnRkY
W10GNIjMjRjN2I1Y2NiYWJmMTQyZjZjQyZDjYTE1ZsA5MW11YWNmZWJmZDYOiwiidGFnljoiIn0%3D;laravel_session=eyJpdil6IlEzbiVleFpYFyM0U0VnVndSb09FNnc9PSIsInZhb
HVlIjoiaSdlRjRtFTB0TGtKUKJWUEl6Q1J5SmtYWNlntK0Z1UE1va1hSbGtXdkdt1WwLk2MzTUuVzGVGEbWcwSXBHZVbUNldvWitKbHBXU2sxSm5uZmw0aktOaUt3cjlmlVnpSRDJ0TTBjazV
KmlajS3dQRURuHwG0a1bVlkaUJhbc9KWFNSekVtYjZDYlClYtYWMiOiJ0ZnNkZDlOTYtZDMvNm01NW0zMjU1YmNlbnR0bDQ2ZW12ZDZlZjZlZGM2Yz01YiA4YTM5Yio1YkkyYTVtbn

VjliwidGFnljoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: disperinaker.smartbojonegoro.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](#)
https://en.wikipedia.org/wiki/Anti-spam_techniques

Outdated JavaScript library

You are using an outdated version of a JavaScript library. A more recent version of the library is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

Impact

Consult References for more information.

<http://disperinaker.smartbojonegoro.id/assets/js/bootstrap.min.js> 95% Confident

Detected JavaScript library **bootstrap.js** version **4.1.3**.
Detection details: The library's name and version were determined based on the file's contents.

- References:
- <https://github.com/twbs/bootstrap/releases>

Request

GET /assets/js/bootstrap.min.js HTTP/1.1
Referer: http://disperinaker.smartbojonegoro.id/
Cookie: XSRF-
TOKEN=eyJpdil6litqQjlzTGVpL3lsTDFDdWNTRHJ1Qmc9PSIsInZhbHVlljoiVVNEak1OUU1UVzF1T04xSDcwOWWkxdk1sUTR1eVJMVmdmRfNvSzcrTDdST0lqSXZxQ3dtM1NzdHp4SmkwQU9ZUS9jd0VZenpOM2sxNzhTdVdNa3Y4Um15b09qZVVCRHFCYkRkK2VRQ09HUE5VV05iVHIZMTVZc0VUaDhYWU5ITk8iLCJtYWMiOiI4MmNmZTM0YWNIYWU2NzE2YWZkYjE0ZjUxZGNIingY1M2QzNWY0ODUzMGUyMGM4NTQ4MDNjNDA5MTAzZDAzM2UwliwidGFnljoiIn0%3D;laravel_session=eyJpdil6lk5PVjZ3TTlZL0FOYVpJMmdsY3pqQ2c9PSIsInZhbHVlljoiUUIPVTFicE91ejI5SmtQUzBiKzYxNjFKeFI5RVU5NEs5NUgvSThHZFdLT1JWa29WSWgyY3lrbnQ3NHZhc2hINDR4SkhxWlFXZm5FVUhhdKYYMEFhS2xWeUlyMWpFUE9heEhpRzRPVFIUTXpMNWZaSGNqZktFYVhYWZGVzRlOFMiLCJtYWMiOiIjOGY1YWU4OWQ4ZDZlNDliMjlxMzYwNzExN2U4NTRiNGYwMDJkNmU0YzYyMDZhMjI4NDVhMmFiZjZlBhOTJkZTI3liwidGFnljoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: disperinaker.smartbojonegoro.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

<http://disperinaker.smartbojonegoro.id/assets/plugins/timepicker/moment.js> 95% Confident

Detected JavaScript library **moment.js** version **2.19.4**.
Detection details: The library's name and version were determined based on the file's contents.

- References:
- <https://github.com/moment/moment/releases>

Request

GET /assets/plugins/timepicker/moment.js HTTP/1.1
Referer: http://disperinaker.smartbojonegoro.id/
Cookie: XSRF-
TOKEN=eyJpdil6ImJqTjJ5M3FzUGU1dTUVdnRsRWxuSnc9PSIsInZhbHVlljoiMDFUOUxRbHpPZ1lwQndLTzJpK01Zb3JxVUtMMGh1S0JCQzJaVjBESjNYVnZLWVlkdTNZQ3JBV0p2VHRRY0JHUHJCV0VDOUtrd3N6K3Z6QkdvS1JEVE92QThrMjhKWUZOVG9kRVVpMzZxR3BMZHozb0dhRDFZano4YVlGUk9sWmwiLCJtYWMiOiI5N2UzMmNmMTRiNzFmZTUwZWlwMTExNDgyZTkzNjE0MWM5NjQ1NzFmNjBmOTFkOTAyMWQxNDllyZiYTE0YjVhliwidGFnljoiIn0%3D;laravel_session=eyJpdil6ImdOK0dLaDlzYzdCODEzcTAxRU1xdHc9PSIsInZhbHVllj

password from the browser cache.

Impact

Possible sensitive information disclosure.

<http://disperinaker.smartbojonegoro.id/>

Form name: <empty>

Form action: <http://disperinaker.smartbojonegoro.id/login>

Form method: POST

Form input:

- password [password]

Request

```
GET /login HTTP/1.1
```

Referer: http://disperinaker.smartbojonegoro.id/

Cookie: XSRF-

[illegible]

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

Accept-Encoding: gzip,deflate

Host: disperinaker.smartbojonegoro.id

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36

Connection: Keep-alive

Recommendation

The password auto-complete should be disabled in sensitive applications.

To disable auto-complete, you may use a code similar to:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

Subresource Integrity (SRI) not implemented

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.

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.

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.

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

<http://disperinaker.smartbojonegoro.id/pencaker/create>

<https://cdnjs.cloudflare.com/ajax/libs/moment.js/2.29.4/locale/id.min.js>

Request

```
GET /pencaker/create HTTP/1.1
```

Referer: http://disperinaker.smartbojonegoro.id/

Cookie: XSRF-

TOKEN=eyJpdii6ill0elcvMi9udFpnQ011ZTRQZexrXzc9PSIsInZhbnVHlJjoiHoic3cm2RzBJZy9ibkpxS1daeVXhQ3NPQjFcbUNdYkcyWEFvd1h3VHQ5eDBJky8zR3Vta0Z3WHV5bmtMN
VvtbCtkdVZQNStsVgPKS2FqVDb1eE85TxlXvDNDTjJaZUN6R0YvMc9oMTNSRUg5NmjVt0xrSDJ3ME9qVgtBdzjKYYxiLCjYWMiOiixNWQwNDjYjY2YNDc3NW10NGZiZGmxZDBiM
mMxN2ViyTVUGZSZy2I2Z45yIyNThlM2Nm0TQyMzRkMzRjMjI0IiwidGFnJoiJoIn0%3D;laravel_session=eyJpdii6llJmbmENiaEVWY1d5S2hYktpZD15N0E9PSIsInZhbnVHlJjoiSG5OSmd
USFjVj09HVUGZ2JvNmZ45bUdWERAajcy2preGpZZlDbPbC1Ra3cQy85dVbsekHJSUGU2tdYskKv29nRDNsoUIMCK3lRpsKtZl0GMVMVW1DVlK3RvpxdnJqNk0qZkNtWs1VFc5
NZuRzUdTeFnrSlYvRzBvXwXlpRwOILCjTYWMI0aiMjYgZWJ1NmMzNTE1ODY5MjYlFmmlZzTgYMcDc0M2YyNDRhMTJhMjdjNTE4ZjZlZDZMmE2YzBiNmZ0AD0Y2VklidGFnJoiJo

n0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: disperinaker.smartbojonegoro.id
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

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.

```
<script src="https://example.com/example-framework.js"
  integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGY11kPzQho1wx4JwY8wC"
  crossorigin="anonymous"></script>
```

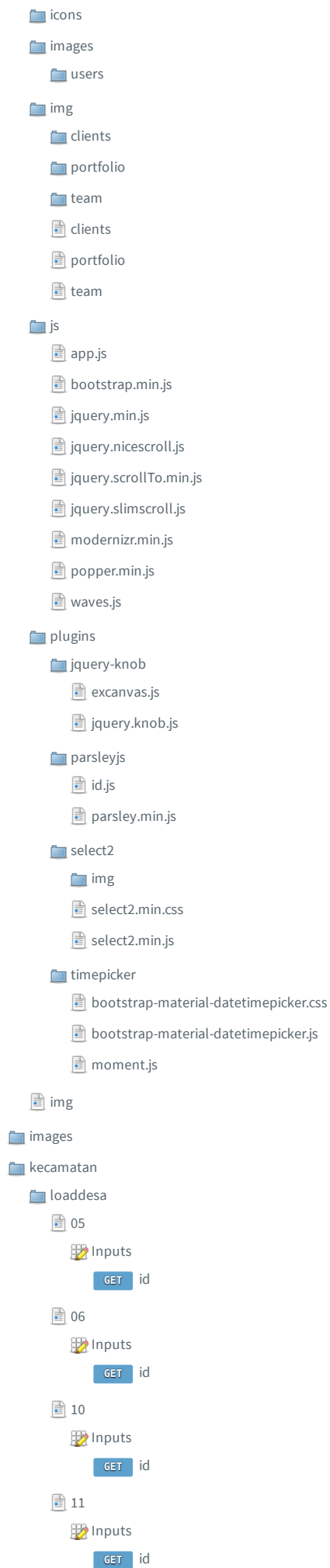
References

[Subresource Integrity](#)
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity





























[SRI Hash Generator](#)
https://www.srihash.org/

Coverage

- Ⓛ http://disperinaker.smartbojonegoro.id
 - Ⓛ _ignition
 - 📄 health-check
 - Ⓛ arsha
 - Ⓛ assets
 - Ⓛ css
 - 📄 style.css
 - Ⓛ img
 - Ⓛ clients
 - Ⓛ js
 - 📄 main.js
 - Ⓛ vendor
 - Ⓛ aos
 - 📄 aos.css
 - 📄 aos.js
 - Ⓛ bootstrap-icons
 - Ⓛ fonts
 - 📄 bootstrap-icons.css
 - Ⓛ bootstrap
 - Ⓛ css
 - 📄 bootstrap.min.css
 - Ⓛ js
 - 📄 bootstrap.bundle.min.js
 - Ⓛ boxicons
 - Ⓛ css
 - 📄 boxicons.min.css
 - Ⓛ fonts
 - Ⓛ glightbox
 - Ⓛ css
 - 📄 glightbox.min.css
 - Ⓛ js
 - 📄 glightbox.min.js
 - Ⓛ isotope-layout
 - 📄 isotope.pkgd.min.js
 - Ⓛ php-email-form
 - 📄 validate.js
 - Ⓛ remixicon
 - 📄 remixicon.css
 - Ⓛ swiper
 - 📄 swiper-bundle.min.css
 - 📄 swiper-bundle.min.js
 - Ⓛ waypoints
 - 📄 noframework.waypoints.js
 - Ⓛ assets
 - Ⓛ css
 - 📄 bootstrap.min.css
 - 📄 icons.css
 - 📄 style.css
 - Ⓛ fonts



- 13
 - Inputs
 - GET id
- 14
 - Inputs
 - GET id
- 15
 - Inputs
 - GET id
- 16
 - Inputs
 - GET id
- 26
 - Inputs
 - GET id
- 28
 - Inputs
 - GET id
- loaddesa
- pencaker
 - create
 - #fragments
 - step-1
- template
 - css
 - main.css
 - util.css
 - fonts
 - font-awesome-4.7.0
 - css
 - font-awesome.min.css
 - fonts
 - iconic
 - css
 - material-design-iconic-font.min.css
 - fonts
 - poppins
 - images
 - icons
 - js
 - main.js
 - vendor
 - animate
 - animate.css
 - ansimition
 - css
 - ansimition.min.css
 - js
 - ansimition.min.js
 - bootstrap
 - css

-  bootstrap.min.css
-  js
 -  bootstrap.min.js
 -  popper.js
-  countdowntime
 -  countdowntime.js
-  css-hamburgers
 -  hamburgers.min.css
-  daterangepicker
 -  daterangepicker.css
 -  daterangepicker.js
 -  moment.min.js
-  jquery
 -  jquery-3.2.1.min.js
-  select2
 -  select2.min.css
 -  select2.min.js
-  _ignition
-  index.php
-  kecamatan
-  login
-  Inputs
 -  _token, password, username
-  pencaker
-  Inputs
 -  _token, agama_id, alamat, desa_id, email, hp, jenis_kelamin_id, kawin_id, kecamatan_id, nama, nik, step, tempat_lahir, tgl_lahir
-  portfolio-details.html
-  robots.txt