

Developer Report

Acunetix Security Audit

2024-03-04

Generated by Acunetix

Scan of peppd.bappenas.go.id

Scan details

Scan information	
Start time	2024-03-04T02:25:44.368092+00:00
Start url	https://peppd.bappenas.go.id/pemantauan/
Host	peppd.bappenas.go.id
Scan time	3 minutes, 28 seconds
Profile	Full Scan
Server information	nginx/1.18.0 (Ubuntu)
Responsive	True
Server OS	Unix
Application build	24.1.240111130

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	15
Critical	0
High Medium	0
Medium	0
∨ Low	5
Informational	10

Alerts summary

∨ Clickjacking: X-Frame-Options header

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC: N/SI:N/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Confidentiality Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N Base Score: 5.8 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021
Affected items	Variation
Web Server	1

∨ Cookies Not Marked as HttpOnly

Classification		
Classification		

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/V N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System Availability Impact to the Vulnerable System Confidentiality Impact to the Subsequent System None Integrity Impact to the Subsequent System Availability Impact System Availability Impac	ystem: None : None :m: None System: n: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None	A:N
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CWE	CWE-1004	
Affected items		Variation
Web Server		1

∨ Cookies Not Marked as Secure

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC: N/SI:N/SA:N Base Score: 2.1 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None

CVVL		
CWE	CWE-614	
CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N//Base Score: 3.1 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None	A:N

∨ Cookies with missing, inconsistent or contradictory properties

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC: N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_c Integrity Requirement: Not_defined Target Distribution: Not_defined	ned defined defined
CWE	CWE-284	
Affected items	·	Variation
Web Server		1

∨ Possible virtual host found

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC: N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	1

© Content Security Policy (CSP) Not Implemented

Classification		
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC: N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CWE	CWE-1021	
Affected items		Variation
Web Server		1

(1) Outdated JavaScript libraries

Classification

CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/V N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable Sy Integrity Impact to the Vulnerable System: Availability Impact to the Subsequent System None Integrity Impact to the Subsequent System Availability Impact to the Subsequent System	vstem: None None m: None System: n: None
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/Base Score: 0.0 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None	A:N
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CWE	CWE-937	
Affected items		Variation
<u>Web Server</u>		7

O Permissions-Policy header not implemented

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC: N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None

CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/ABase Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None	A:N
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CWE	CWE-1021	
Affected items		Variation
Web Server		1

(i) Web Application Firewall Detected

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC: N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined	
CWE	CWE-16	
Affected items		Variation
Web Server		1

Clickjacking: X-Frame-Options header

Severity	Low
Reported by module	/httpdata/X_Frame_Options_not_implemented.js

Description

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

The server 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.

Impact

The impact depends on the affected web application.

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

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

Clickjacking (https://en.wikipedia.org/wiki/Clickjacking)

OWASP Clickjacking (https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)
Frame Buster Buster (https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server

Details

Paths without secure XFO header:

- https://peppd.bappenas.go.id/pemantauan/
- https://peppd.bappenas.go.id/pemantauan/package/images/small/
- https://peppd.bappenas.go.id/pemantauan/package/css/PIE.htc
- https://peppd.bappenas.go.id/pemantauan/Welcome/
- https://peppd.bappenas.go.id/pemantauan/login v1/images/
- https://peppd.bappenas.go.id/pemantauan/assets/images/
- https://peppd.bappenas.go.id/pemantauan/login v1/
- https://peppd.bappenas.go.id/pemantauan/package/js/admin/login/

Request headers

GET /pemantauan/ HTTP/1.1

Referer: https://peppd.bappenas.go.id/pemantauan/

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Cookies Not Marked as HttpOnly

Severity	Low
Reported by module	/RPA/Cookie_Without_HttpOnly.js

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.

Impact

Cookies can be accessed by client-side scripts.

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Affected items

Web 9	Server
-------	--------

Verified vulnerability

Cookies without HttpOnly flag set: https://peppd.bappenas.go.id/pemantauan/ Set-Cookie: csrf cookie peppd=84b9af9ede7fe39a756a43d1845225d5; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/package/images/small/ Set-Cookie: csrf_cookie_peppd=db37c28a9f71615643eb2aa4485452b6; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/package/css/PIE.htc Set-Cookie: csrf cookie peppd=df4e37301cab96f406cfc2538cb58a1d; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/ Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/Welcome/login act Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/ Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/Welcome/ Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/login v1/images/ Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/Welcome/ Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/login v1/ Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/login_v1/ Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/Welcome/

Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/Welcome/login_act

Set-Cookie: csrf cookie peppd=218125980a6510e91f1e21a51a309a8e; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/login v1/images/

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/package/images/small/

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/package/css/PIE.htc

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

Request headers

GET /pemantauan/ HTTP/1.1

Referer: https://peppd.bappenas.go.id/pemantauan/

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Cookies Not Marked as Secure

Severity	Low
Reported by module	/RPA/Cookie_Without_Secure.js

Description

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

Recommendation

If possible, you should set the Secure flag for these cookies.

Affected items

Web Server

Verified vulnerability

Cookies without Secure flag set: https://peppd.bappenas.go.id/pemantauan/ Set-Cookie: csrf cookie peppd=84b9af9ede7fe39a756a43d1845225d5; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/ Set-Cookie: ci_session=lhpan2g686n3egqrq8ipd7fvjt1sdpk9; expires=Mon, 04-Mar-2024 04:25:4 https://peppd.bappenas.go.id/pemantauan/package/images/small/ Set-Cookie: csrf cookie peppd=db37c28a9f71615643eb2aa4485452b6; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/package/css/PIE.htc Set-Cookie: csrf_cookie_peppd=df4e37301cab96f406cfc2538cb58a1d; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/ Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/Welcome/login_act Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/ Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/Welcome/ Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/login_v1/images/ Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/Welcome/ Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024 https://peppd.bappenas.go.id/pemantauan/login_v1/ Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/login_v1/

Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/Welcome/

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/Welcome/login_act

Set-Cookie: csrf cookie peppd=218125980a6510e91f1e21a51a309a8e; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/login v1/images/

Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/package/images/small/

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

https://peppd.bappenas.go.id/pemantauan/package/css/PIE.htc

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

Request headers

GET /pemantauan/ HTTP/1.1

Referer: https://peppd.bappenas.go.id/pemantauan/

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/119.0.0.0 Safari/537.36

Host: peppd.bappenas.go.id

Connection: Keep-alive

Cookies with missing, inconsistent or contradictory properties

Severity	Low
Reported by module	/RPA/Cookie_Validator.js

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.

Impact

Cookies will not be stored, or submitted, by web browsers.

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)
Securing cookies with cookie prefixes (https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/)
Cookies: HTTP State Management Mechanism (https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)
SameSite Updates - The Chromium Projects (https://www.chromium.org/updates/same-site)
draft-west-first-party-cookies-07: Same-site Cookies (https://tools.ietf.org/html/draft-west-first-party-cookies-07)

Affected items

Web Server

Verified vulnerability

List of cookies with missing, inconsistent or contradictory properties:

https://peppd.bappenas.go.id/pemantauan/

Cookie was set with:

Set-Cookie: csrf_cookie_peppd=84b9af9ede7fe39a756a43d1845225d5; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/

Cookie was set with:

Set-Cookie: ci_session=lhpan2g686n3egqrq8ipd7fvjt1sdpk9; expires=Mon, 04-Mar-2024 04:25:4

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/package/images/small/

Cookie was set with:

Set-Cookie: csrf cookie peppd=db37c28a9f71615643eb2aa4485452b6; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/package/css/PIE.htc

Cookie was set with:

Set-Cookie: csrf cookie peppd=df4e37301cab96f406cfc2538cb58ald; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/

Cookie was set with:

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes https://peppd.bappenas.go.id/pemantauan/Welcome/login_act

Cookie was set with:

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/

Cookie was set with:

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/Welcome/

Cookie was set with:

Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/login v1/images/

Cookie was set with:

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/Welcome/

Cookie was set with:

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/login_v1/

Cookie was set with:

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/login_v1/

Cookie was set with:

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/

Cookie was set with:

Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/Welcome/

Cookie was set with:

Set-Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/Welcome/login act

Cookie was set with:

Set-Cookie: csrf cookie peppd=218125980a6510e91f1e21a51a309a8e; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/login v1/images/

Cookie was set with:

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/package/images/small/

Cookie was set with:

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute. When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

https://peppd.bappenas.go.id/pemantauan/package/css/PIE.htc

Cookie was set with:

Set-Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453; expires=Mon, 04-Mar-2024

This cookie has the following issues:

- Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes

Request headers

GET /pemantauan/ HTTP/1.1

Referer: https://peppd.bappenas.go.id/pemantauan/

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Possible virtual host found

Severity	Low
Reported by module	/Scripts/PerServer/VirtualHost_Audit.script

Description

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.

This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

Impact

Possible sensitive information disclosure.

Recommendation

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

References

Virtual hosting (https://en.wikipedia.org/wiki/Virtual hosting)

Affected items

Web Server

Details

Virtual host: localhost

Response:

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/D</pre>

Request headers

GET / HTTP/1.1
Host: localhost

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/119.0.0.0 Safari/537.36

Connection: Keep-alive

Content Security Policy (CSP) Not Implemented

Severity	Informational
Reported by module	/httpdata/CSP_not_implemented.js

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.

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 iQuery library from their CDN, the CSP header could look like the following:

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

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.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

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.

References

<u>Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)</u>
<u>Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)</u>

Affected items

Web Server

Details

Paths without CSP header:

- https://peppd.bappenas.go.id/pemantauan/
- https://peppd.bappenas.go.id/pemantauan/package/images/small/
- https://peppd.bappenas.go.id/pemantauan/package/css/PIE.htc
- https://peppd.bappenas.go.id/pemantauan/assets/images/
- https://peppd.bappenas.go.id/pemantauan/Welcome/
- https://peppd.bappenas.go.id/pemantauan/login v1/images/
- https://peppd.bappenas.go.id/pemantauan/login v1/
- https://peppd.bappenas.go.id/pemantauan/package/js/admin/login/

Request headers

GET /pemantauan/ HTTP/1.1

Referer: https://peppd.bappenas.go.id/pemantauan/

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Outdated JavaScript libraries

Severity	Informational
Reported by module	/deepscan/javascript_library_audit_deepscan.js

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.

Impact

Consult References for more information.

Recommendation

Upgrade to the latest version.

Affected items

Web Server

Details

bootstrap.js 3.3.5

- URL: https://peppd.bappenas.go.id/pemantauan/
- Detection method: The library's name and version were determined based on its dynamic behavior.
- References:
 - https://github.com/twbs/bootstrap/releases

Request headers

GET /pemantauan/ HTTP/1.1

Referer: https://peppd.bappenas.go.id/pemantauan/

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Web Server

Details

Modernizr 2.6.2

- URL: https://peppd.bappenas.go.id/pemantauan/
- Detection method: The library's name and version were determined based on its dynamic behavior.
- · References:
 - https://github.com/Modernizr/Modernizr/releases

Request headers

GET /pemantauan/ HTTP/1.1

Referer: https://peppd.bappenas.go.id/pemantauan/

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Web Server

Details

SweetAlert2 7.28.7

- URL: https://peppd.bappenas.go.id/pemantauan/
- Detection method: The library's name and version were determined based on its dynamic behavior.
- References:
 - https://github.com/sweetalert2/sweetalert2/releases

Request headers

GET /pemantauan/ HTTP/1.1

Referer: https://peppd.bappenas.go.id/pemantauan/

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Web Server

bootstrap.js 4.0.0-beta

• URL:

https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/bootstrap/js/bootstrap.mi n.js

- Detection method: The library's name and version were determined based on the file's contents.
- References:
 - https://github.com/twbs/bootstrap/releases

Request headers

GET /pemantauan/package/plugins/login_v1/vendor/bootstrap/js/bootstrap.min.js HTTP/1.1

Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453;

ci session=lhpan2g686n3egqrq8ipd7fvjt1sdpk9

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Web Server

Details

• jQuery Validation 1.15.0

- URL: https://peppd.bappenas.go.id/pemantauan/package/plugins/jquery-validation-1.15.0/dist/jquery.validate.min.js
- Detection method: The library's name and version were determined based on the file's contents.
- References:
 - https://github.com/jguery-validation/jguery-validation/tags

Request headers

GET /pemantauan/package/plugins/jquery-validation-1.15.0/dist/jquery.validate.min.js HTTP/1.1

Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453;

ci session=lhpan2g686n3eggrq8ipd7fvjt1sdpk9

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id

Connection: Keep-alive

Web Server

Details

moment.js 2.13.0

• URL:

 $https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/daterangepicker/moment.min.js$

- Detection method: The library's name and version were determined based on the file's contents.
- · References:
 - https://github.com/moment/moment/tags

Request headers

GET /pemantauan/package/plugins/login_v1/vendor/daterangepicker/moment.min.js HTTP/1.1

Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453;

ci session=lhpan2g686n3eggrq8ipd7fvjt1sdpk9

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Web Server

Details

Select2 4.0.3

• URL:

https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/select2/select2.min.js

- Detection method: The library's name and version were determined based on the file's contents.
- · References:
 - https://github.com/select2/select2/tags

Request headers

GET /pemantauan/package/plugins/login_v1/vendor/select2/select2.min.js HTTP/1.1

Cookie: csrf cookie peppd=0e029f32747d5e44c07a7bb9ef92f453;

ci session=lhpan2g686n3egqrq8ipd7fvjt1sdpk9

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Permissions-Policy header not implemented

Severity	Informational
Reported by module	/httpdata/permissions_policy.js

Description

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

Recommendation

References

<u>Permissions-Policy / Feature-Policy (MDN) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)</u>

Permissions Policy (W3C) (https://www.w3.org/TR/permissions-policy-1/)

Affected items

Web Server

Locations without Permissions-Policy header:

- https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/
- https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/fonts/
- https://peppd.bappenas.go.id/pemantauan/package/plugins/
- https://peppd.bappenas.go.id/pemantauan/package/
- https://peppd.bappenas.go.id/pemantauan/
- https://peppd.bappenas.go.id/pemantauan/package/plugins/font-awesome/
- https://peppd.bappenas.go.id/pemantauan/package/css/
- https://peppd.bappenas.go.id/pemantauan/package/images/
- https://peppd.bappenas.go.id/pemantauan/package/images/small/
- https://peppd.bappenas.go.id/pemantauan/package/plugins/ionicon/
- https://peppd.bappenas.go.id/pemantauan/package/plugins/font-awesome/fonts/
- https://peppd.bappenas.go.id/pemantauan/package/plugins/ionicon/fonts/
- https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/fonts/font-awesome-4.7.0/
- https://peppd.bappenas.go.id/pemantauan/package/fonts/
- https://peppd.bappenas.go.id/pemantauan/package/css/PIE.htc
- https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/fonts/font-awesome-4.7.0/fonts/
- https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/fonts/montserrat/
- https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/fonts/poppins/
- https://peppd.bappenas.go.id/pemantauan/Welcome/login act
- https://peppd.bappenas.go.id/pemantauan/assets/
- https://peppd.bappenas.go.id/pemantauan/Welcome/

Request headers

GET /pemantauan/package/plugins/login v1/ HTTP/1.1

Referer: https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/

Cookie: csrf cookie peppd=df4e37301cab96f406cfc2538cb58a1d;

ci session=5ehhcrrk3vm7vmi43goh9nqi9v6pu7f3

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id Connection: Keep-alive

Web Application Firewall Detected

Severity	Informational
Reported by module	/Scripts/PerServer/WAF_Detection.script

Description

This server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or an WAF (Web Application Firewall). Acunetix detected this by sending various malicious payloads and detecting changes in the response code, headers and body.

Impact

You may receive incorrect/incomplete results when scanning a server protected by an IPS/IDS/WAF. Also, if the WAF detects a number of attacks coming from the scanner, the IP address can be blocked after a few attempts.

Recommendation

If possible, it's recommended to scan an internal (development) version of the web application where the WAF is not active.

Affected items

Web Server

Detected Imperva SecureSphere from the response body.

Request headers

TESTING /9954379 HTTP/1.1

Cookie: csrf_cookie_peppd=0e029f32747d5e44c07a7bb9ef92f453; ci_session=lhpan2g686n3egqrq8ipd7fvjt1sdpk9

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/119.0.0.0 Safari/537.36 Host: peppd.bappenas.go.id

Connection: Keep-alive

Scanned items (coverage report)

awesome.min.css

```
https://peppd.bappenas.go.id/
https://peppd.bappenas.go.id/pemantauan/
https://peppd.bappenas.go.id/pemantauan/Welcome/
https://peppd.bappenas.go.id/pemantauan/Welcome/login act
https://peppd.bappenas.go.id/pemantauan/assets/
https://peppd.bappenas.go.id/pemantauan/assets/images/
https://peppd.bappenas.go.id/pemantauan/login_v1/
https://peppd.bappenas.go.id/pemantauan/login v1/images/
https://peppd.bappenas.go.id/pemantauan/package/
https://peppd.bappenas.go.id/pemantauan/package/css/
https://peppd.bappenas.go.id/pemantauan/package/css/PIE.htc
https://peppd.bappenas.go.id/pemantauan/package/css/animate.css
https://peppd.bappenas.go.id/pemantauan/package/css/bootstrap.min.css
https://peppd.bappenas.go.id/pemantauan/package/css/helper.css
https://peppd.bappenas.go.id/pemantauan/package/css/material-design-iconic-font.min.css
https://peppd.bappenas.go.id/pemantauan/package/css/style.css
https://peppd.bappenas.go.id/pemantauan/package/css/userdefined.css
https://peppd.bappenas.go.id/pemantauan/package/css/waves-effect.css
https://peppd.bappenas.go.id/pemantauan/package/fonts/
https://peppd.bappenas.go.id/pemantauan/package/images/
https://peppd.bappenas.go.id/pemantauan/package/images/small/
https://peppd.bappenas.go.id/pemantauan/package/js/
https://peppd.bappenas.go.id/pemantauan/package/js/admin/
https://peppd.bappenas.go.id/pemantauan/package/js/admin/login/
https://peppd.bappenas.go.id/pemantauan/package/js/admin/login/login.js
https://peppd.bappenas.go.id/pemantauan/package/js/bootstrap.min.js
https://peppd.bappenas.go.id/pemantauan/package/js/jquery-3.7.1.min.js
https://peppd.bappenas.go.id/pemantauan/package/js/jguery.nicescroll.js
https://peppd.bappenas.go.id/pemantauan/package/js/jguery.scrollTo.min.js
https://peppd.bappenas.go.id/pemantauan/package/is/modernizr.min.js
https://peppd.bappenas.go.id/pemantauan/package/is/universal.is
https://peppd.bappenas.go.id/pemantauan/package/js/waves.js
https://peppd.bappenas.go.id/pemantauan/package/js/wow.min.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/
https://peppd.bappenas.go.id/pemantauan/package/plugins/fastclick/
https://peppd.bappenas.go.id/pemantauan/package/plugins/fastclick/fastclick.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/font-awesome/
https://peppd.bappenas.go.id/pemantauan/package/plugins/font-awesome/css/
https://peppd.bappenas.go.id/pemantauan/package/plugins/font-awesome/css/font-awesome.min.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/font-awesome/fonts/
https://peppd.bappenas.go.id/pemantauan/package/plugins/ionicon/
https://peppd.bappenas.go.id/pemantauan/package/plugins/ionicon/css/
https://peppd.bappenas.go.id/pemantauan/package/plugins/ionicon/css/ionicons.min.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/ionicon/fonts/
https://peppd.bappenas.go.id/pemantauan/package/plugins/jquery-blockui/
https://peppd.bappenas.go.id/pemantauan/package/plugins/jquery-blockui/jquery.blockUI.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/jquery-detectmobile/
https://peppd.bappenas.go.id/pemantauan/package/plugins/jquery-detectmobile/detect.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/jquery-slimscroll/
https://peppd.bappenas.go.id/pemantauan/package/plugins/jquery-slimscroll/jquery.slimscroll.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/jquery-validation-1.15.0/
https://peppd.bappenas.go.id/pemantauan/package/plugins/jquery-validation-1.15.0/dist/
https://peppd.bappenas.go.id/pemantauan/package/plugins/jquery-validation-1.15.0/dist/jquery.validate.min.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/css/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/css/main.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/css/util.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/fonts/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/fonts/Linearicons-Free-v1.0.0/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/fonts/Linearicons-Free-v1.0.0/icon-
font.min.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/fonts/font-awesome-4.7.0/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/fonts/font-awesome-4.7.0/css/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/fonts/font-awesome-4.7.0/css/font-
```

```
https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/fonts/font-awesome-4.7.0/fonts/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/fonts/montserrat/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/fonts/poppins/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/images/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/images/icons/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/js/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/js/main.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/animate/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/vendor/animate/animate.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/animsition/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/vendor/animsition/css/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/vendor/animsition/css/animsition.min.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/animsition/is/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/animsition/js/animsition.min.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/vendor/bootstrap/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/bootstrap/css/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/bootstrap/css/bootstrap.min.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/bootstrap/js/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/bootstrap/js/bootstrap.min.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/bootstrap/js/popper.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/countdowntime/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/countdowntime/countdowntime.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/css-hamburgers/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/css-
hamburgers/hamburgers.min.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/login v1/vendor/daterangepicker/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/daterangepicker/daterangepicker.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/daterangepicker/daterangepicker.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/daterangepicker/moment.min.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/jquery/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/jguery/jguery-3.7.1.min.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/select2/
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/select2/select2.min.css
https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/select2/select2.min.js
https://peppd.bappenas.go.id/pemantauan/package/plugins/sweetalert/
https://peppd.bappenas.go.id/pemantauan/package/plugins/sweetalert/dist/
https://peppd.bappenas.go.id/pemantauan/package/plugins/sweetalert/dist/sweetalert2.all.min.js
```

https://peppd.bappenas.go.id/pemantauan/package/plugins/sweetalert/dist/sweetalert2.min.css https://peppd.bappenas.go.id/pemantauan/package/plugins/sweetalert/dist/sweetalert2.min.is