Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2024-03-07

Generated by Acunetix

Scan of peppd.bappenas.go.id

Scan details

Scan information	
Start time	2024-03-07T02:00:31.202015+00:00
Start url	https://peppd.bappenas.go.id/
Host	peppd.bappenas.go.id
Scan time	51 minutes, 15 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 2

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

Alerts distribution

Total alerts found	35
Critical	0
High	0
Medium	7
Low	9
Informational	19

Alerts summary

Vulnerable JavaScript libraries

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/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: Low 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:L/A:N Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial 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-937

Affected items	Variation
Web Server	7

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: Low 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: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	
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_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
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A: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

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
CWE	CWE-614

Affected items	Variation
Web Server	1

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_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-284

Affected items	Variation
Web Server	1

Documentation files

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:3.1/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-538

Affected items	Variation
Web Server	1

Insecure Frame (External)

Classification

CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:A/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L Base Score: 1.8 Attack Vector: Network Attack Complexity: High Privileges Required: High User Interaction: Active Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: Low Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: Low
CVSS3	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:L Base Score: 5.1 Attack Vector: Network Attack Complexity: High Privileges Required: High User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: Low
CVSS2	Base Score: 4.6 Access Vector: Network_accessible Access Complexity: High Authentication: Single Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial 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-829

Affected items	Variation
/media/news/Daerah-Terbaik-Penerima-Penghargaan-Pembangunan-Daerah-2021	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

Programming Error Messages

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-209

Affected items	Variation
Web Server	1

[Possible] Internal IP Address Disclosure

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:3.1/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

Generic Email Address Disclosure

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-200

Affected items	Variation
Web Server	1

HTTP Strict Transport Security (HSTS) Errors and Warnings

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-16

Affected items	Variation
Web Server	1

Javascript Source map 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:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None 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-16

Affected items	Variation
Web Server	1

Outdated JavaScript libraries

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/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: High 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:H/PR:N/UI:R/S:C/C:N/I:N/A: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
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
Web Server	11

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/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

Subresource Integrity (SRI) Not Implemented

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/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: None Integrity Impact to the Vulnerable System: Low 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:N/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None 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-830

Affected items	Variation
Web Server	1

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

[Possible] Internal Path Disclosure (*nix)

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:3.1/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

Alerts details

Vulnerable JavaScript libraries

Severity	**Medium**
Reported by module	/httpdata/javascript_library_audit_external.js

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.

Impact

Consult References for more information.

Recommendation

Upgrade to the latest version.

Affected items

Web Server

Details

- **jQuery 3.4.0**
  - URL: https://ajax.googleapis.com/ajax/libs/jquery/3.4.0/jquery.min.js
  - Detection method: The library's name and version were determined based on the file's CDN URI.
  - CVE-ID: CVE-2020-11022, CVE-2020-11023
  - 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.
  - 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/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

Request headers

```
GET / HTTP/1.1
Referer: https://peppd.bappenas.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/119.0.0.0 Safari/537.36
Host: peppd.bappenas.go.id
Connection: Keep-alive
```

Web Server

Details

- **jQuery 2.1.1**
  - URL: https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js
  - Detection method: The library's name and version were determined based on the file's CDN URI.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - 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.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - 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/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
    - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request headers

```
GET / HTTP/1.1
Referer: https://peppd.bappenas.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/119.0.0.0 Safari/537.36
Host: peppd.bappenas.go.id
Connection: Keep-alive
```

Web Server

Details

- **jQuery 1.10.2**
  - URL: https://peppd.bappenas.go.id/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
  - 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.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
    - 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/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

Request headers

```
GET / HTTP/1.1
Referer: https://peppd.bappenas.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/119.0.0.0 Safari/537.36
Host: peppd.bappenas.go.id
Connection: Keep-alive
```

Web Server

Details

- **jQuery 3.2.1**
  - URL: https://code.jquery.com/jquery-3.2.1.slim.min.js
  - Detection method: The library's name and version were determined based on the file's CDN URI.
  - CVE-ID: CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - 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.
  - 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/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
    - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request headers

```
GET /jumper_ppd/ HTTP/1.1
Referer: https://peppd.bappenas.go.id/
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa
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 3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector**
  - URL: https://peppd.bappenas.go.id/jumper_ppd/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - 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.
  - 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/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
    - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request headers

```
GET /jumper_ppd/ HTTP/1.1
Referer: https://peppd.bappenas.go.id/
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa
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 1.11.1**
  - URL: https://peppd.bappenas.go.id/ppd2021/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
  - 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.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
    - 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/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

Request headers

```
GET /ppd2021/ HTTP/1.1
Referer: https://peppd.bappenas.go.id/jumper_ppd/
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=6663e64a9c8e2b73ae0415352b9e7e67;
csrf_cookie_ppdbappenas=9dd6f694dc52380b2345773bcb4309ff
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 2.1.4**
  - URL: https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/jquery.min.js
  - Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the vulnerability alert has been lowered.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - 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.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - 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/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
    - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request headers

```
GET /media/assets/zircosadmin/assets/js/jquery.min.js HTTP/1.1
Cookie: ci_session=378hmj1ks69q2b8tv62uk5cv301k46eg; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=c20c30aad8f377a16f73388752f744be;
csrf_cookie_ppdbappenas=022766b7257af010aa384936ac391a85;
csrf_cookie_2022ppd=500927e27766ee7ef564379271912a33;
csrf_cookie_2023ppd=3179abfa0a63484fd947c078da65dbed;
csrf_cookie_2024ppd=d5305e0ad1b3b12d6e92973eca3e77ae
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
```

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

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)
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/
- https://peppd.bappenas.go.id/welcome
- https://peppd.bappenas.go.id/9404525
- https://peppd.bappenas.go.id/global.asa.bak
- https://peppd.bappenas.go.id/user_guide/
- https://peppd.bappenas.go.id/php.ini
- https://peppd.bappenas.go.id/users.db
- https://peppd.bappenas.go.id/global.asax.bak
- https://peppd.bappenas.go.id/propel.ini
- https://peppd.bappenas.go.id/htaccess.bak
- https://peppd.bappenas.go.id/users.ini
- https://peppd.bappenas.go.id/web.config.bak
- https://peppd.bappenas.go.id/jumper_ppd/
- https://peppd.bappenas.go.id/pemantauan/
- https://peppd.bappenas.go.id/peppd/Home/demo/
- https://peppd.bappenas.go.id/ppd2021/
- https://peppd.bappenas.go.id/jumper_ppd/video/ppd.ogv
- https://peppd.bappenas.go.id/peppd/Home/
- https://peppd.bappenas.go.id/peppd/
- https://peppd.bappenas.go.id/media/kegiatan/pemantauan
- https://peppd.bappenas.go.id/jumper_ppd/video/ppd.webm

Request headers

```
GET / HTTP/1.1
Referer: https://peppd.bappenas.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/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 Server
Verified vulnerability
Details

Cookies without HttpOnly flag set:

- https://peppd.bappenas.go.id/jumper_ppd/

```
Set-Cookie: csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa; expires=Thu, 07-Mar-2024
```

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

```
Set-Cookie: csrf_cookie_peppd=4d7f436ce1fd274313e65a4c07ca59d4; expires=Thu, 07-Mar-2024
```

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

```
Set-Cookie: csrf_cookie_peppd=4d7f436ce1fd274313e65a4c07ca59d4; expires=Thu, 07-Mar-2024
```

- https://peppd.bappenas.go.id/ppd2021/

```
Set-Cookie: csrf_cookie_ppdbappenas=9dd6f694dc52380b2345773bcb4309ff; expires=Thu, 07-Mar
```

- https://peppd.bappenas.go.id/ppd2021/

```
Set-Cookie: csrf_cookie_ppdbappenas=9dd6f694dc52380b2345773bcb4309ff; expires=Thu, 07-Mar
```

- https://peppd.bappenas.go.id/jumper_ppd/video/ppd.ogv

```
Set-Cookie: csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa; expires=Thu, 07-Mar-2024
```

- https://peppd.bappenas.go.id/jumper_ppd/video/ppd.webm

```
Set-Cookie: csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa; expires=Thu, 07-Mar-2024
```

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

```
Set-Cookie: csrf_cookie_peppd=4b4c275a65530071ae20ccb5afefedf6; expires=Thu, 07-Mar-2024
```

- https://peppd.bappenas.go.id/ppd2021/Welcome/refresh_captcha

```
Set-Cookie: csrf_cookie_ppdbappenas=3f4e890488c2976b3950bff4533abc80; expires=Thu, 07-Mar
```

- https://peppd.bappenas.go.id/ppd2021/Welcome/login_act

```
Set-Cookie: csrf_cookie_ppdbappenas=1904c11683b76791aa6665bd5412a4d3; expires=Thu, 07-Mar
```

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

```
Set-Cookie: csrf_cookie_peppd=6663e64a9c8e2b73ae0415352b9e7e67; expires=Thu, 07-Mar-2024
```

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

```
Set-Cookie: csrf_cookie_peppd=6663e64a9c8e2b73ae0415352b9e7e67; expires=Thu, 07-Mar-2024
```

- https://peppd.bappenas.go.id/ppd2022/

```
Set-Cookie: csrf_cookie_2022ppd=27a95149cb7e91e0c19a33998390d375; expires=Thu, 07-Mar-202
```

- https://peppd.bappenas.go.id/ppd2023/

```
Set-Cookie: csrf_cookie_2023ppd=aa4d686e214e44638d13a4c172812e14; expires=Thu, 07-Mar-202
```

- https://peppd.bappenas.go.id/ppd2022/

```
Set-Cookie: csrf_cookie_2022ppd=27a95149cb7e91e0c19a33998390d375; expires=Thu, 07-Mar-202
```

- https://peppd.bappenas.go.id/ppd2023/

```
Set-Cookie: csrf_cookie_2023ppd=aa4d686e214e44638d13a4c172812e14; expires=Thu, 07-Mar-202
```

- https://peppd.bappenas.go.id/ppd2022/Welcome/refresh_captcha

```
Set-Cookie: csrf_cookie_2022ppd=b850f73cff4f775bccb44446db4f0135; expires=Thu, 07-Mar-202
```

- https://peppd.bappenas.go.id/ppd2023/Welcome/refresh_captcha

```
Set-Cookie: csrf_cookie_2023ppd=aa4d686e214e44638d13a4c172812e14; expires=Thu, 07-Mar-202
```

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

```
Set-Cookie: csrf_cookie_peppd=6663e64a9c8e2b73ae0415352b9e7e67; expires=Thu, 07-Mar-2024
```

- https://peppd.bappenas.go.id/ppd2024/

```
Set-Cookie: csrf_cookie_2024ppd=d12be6cf3fa7e143e70ffa5b2acfea91; expires=Thu, 07-Mar-202
```

- https://peppd.bappenas.go.id/ppd2024/

```
Set-Cookie: csrf_cookie_2024ppd=d12be6cf3fa7e143e70ffa5b2acfea91; expires=Thu, 07-Mar-202
```

Request headers

```
GET /jumper_ppd/ HTTP/1.1
Referer: https://peppd.bappenas.go.id/
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa
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
Details

Cookies without Secure flag set:

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

```
Set-Cookie: ci_session=ghhbduplitt4f0d34lvn3udtilqm3u4d; expires=Thu, 07-Mar-2024 04:00:3
```

- https://peppd.bappenas.go.id/jumper_ppd/

```
Set-Cookie: csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa; expires=Thu, 07-Mar-2024
```

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

```
Set-Cookie: csrf_cookie_peppd=4d7f436ce1fd274313e65a4c07ca59d4; expires=Thu, 07-Mar-2024
```

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

```
Set-Cookie: csrf_cookie_peppd=4d7f436ce1fd274313e65a4c07ca59d4; expires=Thu, 07-Mar-2024
```

- https://peppd.bappenas.go.id/ppd2021/

```
Set-Cookie: csrf_cookie_ppdbappenas=9dd6f694dc52380b2345773bcb4309ff; expires=Thu, 07-Mar
```

- https://peppd.bappenas.go.id/ppd2021/

```
Set-Cookie: csrf_cookie_ppdbappenas=9dd6f694dc52380b2345773bcb4309ff; expires=Thu, 07-Mar
```

- https://peppd.bappenas.go.id/jumper_ppd/video/ppd.ogv

```
Set-Cookie: csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa; expires=Thu, 07-Mar-2024
```

- https://peppd.bappenas.go.id/jumper_ppd/video/ppd.webm

```
Set-Cookie: csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa; expires=Thu, 07-Mar-2024
```

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

```
Set-Cookie: csrf_cookie_peppd=4b4c275a65530071ae20ccb5afefedf6; expires=Thu, 07-Mar-2024
```

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

```
Set-Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; expires=Thu, 07-Mar-2024 04:02:0
```

- https://peppd.bappenas.go.id/ppd2021/Welcome/refresh_captcha

```
Set-Cookie: csrf_cookie_ppdbappenas=3f4e890488c2976b3950bff4533abc80; expires=Thu, 07-Mar
```

- https://peppd.bappenas.go.id/ppd2021/Welcome/login_act

```
Set-Cookie: csrf_cookie_ppdbappenas=1904c11683b76791aa6665bd5412a4d3; expires=Thu, 07-Mar
```

- https://peppd.bappenas.go.id/ppd2021/Welcome/login_act

```
Set-Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; expires=Thu, 07-Mar-2024 04:02:2
```

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

```
Set-Cookie: csrf_cookie_peppd=6663e64a9c8e2b73ae0415352b9e7e67; expires=Thu, 07-Mar-2024
```

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

```
Set-Cookie: csrf_cookie_peppd=6663e64a9c8e2b73ae0415352b9e7e67; expires=Thu, 07-Mar-2024
```

- https://peppd.bappenas.go.id/media/commentController/index

```
Set-Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; expires=Thu, 07-Mar-2024 04:02:3
```

- https://peppd.bappenas.go.id/media/logPortalController/store

```
Set-Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; expires=Thu, 07-Mar-2024 04:00:4
```

- https://peppd.bappenas.go.id/ppd2022/

```
Set-Cookie: csrf_cookie_2022ppd=27a95149cb7e91e0c19a33998390d375; expires=Thu, 07-Mar-202
```

- https://peppd.bappenas.go.id/ppd2023/

```
Set-Cookie: csrf_cookie_2023ppd=aa4d686e214e44638d13a4c172812e14; expires=Thu, 07-Mar-202
```

- https://peppd.bappenas.go.id/ppd2022/

```
Set-Cookie: csrf_cookie_2022ppd=27a95149cb7e91e0c19a33998390d375; expires=Thu, 07-Mar-202
```

- https://peppd.bappenas.go.id/ppd2023/

```
Set-Cookie: csrf_cookie_2023ppd=aa4d686e214e44638d13a4c172812e14; expires=Thu, 07-Mar-202
```

Request headers

```
GET / HTTP/1.1
Referer: https://peppd.bappenas.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/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
Details

List of cookies with missing, inconsistent or contradictory properties:

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

  Cookie was set with:

  ```
  Set-Cookie: ci_session=ghhbduplitt4f0d34lvn3udtilqm3u4d; expires=Thu, 07-Mar-2024 04:00:3
  ```

  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/jumper_ppd/

  Cookie was set with:

  ```
  Set-Cookie: csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa; expires=Thu, 07-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=4d7f436ce1fd274313e65a4c07ca59d4; expires=Thu, 07-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=4d7f436ce1fd274313e65a4c07ca59d4; expires=Thu, 07-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/ppd2021/

  Cookie was set with:

  ```
  Set-Cookie: csrf_cookie_ppdbappenas=9dd6f694dc52380b2345773bcb4309ff; expires=Thu, 07-Mar
  ```

  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/ppd2021/

  Cookie was set with:

  ```
  Set-Cookie: csrf_cookie_ppdbappenas=9dd6f694dc52380b2345773bcb4309ff; expires=Thu, 07-Mar
  ```

  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/jumper_ppd/video/ppd.ogv

  Cookie was set with:

  ```
  Set-Cookie: csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa; expires=Thu, 07-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/jumper_ppd/video/ppd.webm

  Cookie was set with:

  ```
  Set-Cookie: csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa; expires=Thu, 07-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=4b4c275a65530071ae20ccb5afefedf6; expires=Thu, 07-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: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; expires=Thu, 07-Mar-2024 04:02:0
  ```

  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/ppd2021/Welcome/refresh_captcha

  Cookie was set with:

```
Set-Cookie: csrf_cookie_ppdbappenas=3f4e890488c2976b3950bff4533abc80; expires=Thu, 07-Mar
```

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/ppd2021/Welcome/login_act

  Cookie was set with:

```
Set-Cookie: csrf_cookie_ppdbappenas=1904c11683b76791aa6665bd5412a4d3; expires=Thu, 07-Mar
```

  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/ppd2021/Welcome/login_act

  Cookie was set with:

```
Set-Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; expires=Thu, 07-Mar-2024 04:02:2
```

  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=6663e64a9c8e2b73ae0415352b9e7e67; expires=Thu, 07-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=6663e64a9c8e2b73ae0415352b9e7e67; expires=Thu, 07-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/media/commentController/index

  Cookie was set with:

```
Set-Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; expires=Thu, 07-Mar-2024 04:02:3
```

  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/media/logPortalController/store

  Cookie was set with:

```
Set-Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; expires=Thu, 07-Mar-2024 04:00:4
```

  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/ppd2022/

  Cookie was set with:

```
Set-Cookie: csrf_cookie_2022ppd=27a95149cb7e91e0c19a33998390d375; expires=Thu, 07-Mar-202
```

  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/ppd2023/

  Cookie was set with:

```
Set-Cookie: csrf_cookie_2023ppd=aa4d686e214e44638d13a4c172812e14; expires=Thu, 07-Mar-202
```

  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/ppd2022/

  Cookie was set with:

```
Set-Cookie: csrf_cookie_2022ppd=27a95149cb7e91e0c19a33998390d375; expires=Thu, 07-Mar-202
```

  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/ppd2023/

  Cookie was set with:

```
Set-Cookie: csrf_cookie_2023ppd=aa4d686e214e44638d13a4c172812e14; expires=Thu, 07-Mar-202
```

  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 / HTTP/1.1
Referer: https://peppd.bappenas.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/119.0.0.0 Safari/537.36
Host: peppd.bappenas.go.id
Connection: Keep-alive
```

Documentation files

Severity	**Low**
Reported by module	/Scripts/PerFolder/Readme_Files.script

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.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Remove or restrict access to all documentation file acessible from internet.

Affected items

Web Server

Details

Documentation files:

- https://peppd.bappenas.go.id/**license.txt**
  File contents (first 100 characters):

```
The MIT License (MIT)

Copyright (c) 2014 - 2019, British Columbia Institute of Technology

Permissi ...
```

Request headers

```
GET /license.txt HTTP/1.1
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true; poptin_c_visitor=true
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
```

Insecure Frame (External)

Severity	**Low**
Reported by module	/httpdata/iframe_sandbox.js

Description

The web page was found to be using an Inline Frame ("iframe") to embed a resource, such as a different web page. The Inline Frame is either configured insecurely, or not as securely as expected. This vulnerability alert is based on the origin of the embedded resource and the iframe's sandbox attribute, which can be used to apply security restrictions as well as exceptions to these restrictions.

Impact

When a web page uses an insecurely configured iframe to embed another web page, the latter may manipulate the former, and trick its visitors into performing unwanted actions.

Recommendation

Review the iframe's purpose and environment, and use the sandbox attribute to secure the iframe while applying sandbox directives to ease security restrictions if necessary.

References

MDN | iframe: The Inline Frame Element (https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe)
HTML Standard: iframe (https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element)
HTML 5.2: 4.7. Embedded content (https://www.w3.org/TR/html52/semantics-embedded-content.html#element-attrdef-iframe-sandbox)

Affected items

/media/news/Daerah-Terbaik-Penerima-Penghargaan-Pembangunan-Daerah-2021
Verified vulnerability
Details
An iframe tag references an external resource, and no sandbox attribute is set.
Request headers

```
GET /media/news/Daerah-Terbaik-Penerima-Penghargaan-Pembangunan-Daerah-2021 HTTP/1.1
Referer: https://peppd.bappenas.go.id/
Cookie: ci_session=qt2945tgu11teq9q1a9s8oi5op2oqlin; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=c20c30aad8f377a16f73388752f744be;
csrf_cookie_ppdbappenas=022766b7257af010aa384936ac391a85;
csrf_cookie_2022ppd=500927e27766ee7ef564379271912a33;
csrf_cookie_2023ppd=3179abfa0a63484fd947c078da65dbed;
csrf_cookie_2024ppd=d5305e0ad1b3b12d6e92973eca3e77ae
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`
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`

Programming Error Messages

Severity	**Low**
Reported by module	/httpdata/text_search.js

Description

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.
These messages may also contain the location of the file that produced an unhandled exception.
Consult the 'Attack details' section for more information about the affected page(s).

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration (https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
Improper Error Handling (https://www.owasp.org/index.php/Improper_Error_Handling)

Affected items

Web Server
Details
Application error messages: • https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/ **You have an error in your SQL syntax**
Request headers

`GET /media/C_pagesController/article_pagination/ HTTP/1.1`
`Referer: https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/`
`Cookie: ci_session=ausdvrtpmm04hjtgncnrs1b5dh34af1r; poptin_old_user=true;`
`poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;`
`poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;`
`csrf_cookie_peppd=c20c30aad8f377a16f73388752f744be;`
`csrf_cookie_ppdbappenas=022766b7257af010aa384936ac391a85;`
`csrf_cookie_2022ppd=500927e27766ee7ef564379271912a33;`
`csrf_cookie_2023ppd=3179abfa0a63484fd947c078da65dbed;`
`csrf_cookie_2024ppd=d5305e0ad1b3b12d6e92973eca3e77ae`
`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] Internal IP Address Disclosure

Severity	**Low**
Reported by module	/httpdata/text_search.js

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.

The significance of this finding should be confirmed manually.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

Affected items

Web Server

Details

Pages with internal IPs:

- https://peppd.bappenas.go.id/media/logPortalController/store
  10.1.188.10

Request headers

```
POST /media/logPortalController/store HTTP/1.1
Referer: https://peppd.bappenas.go.id/
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
Cookie: ci_session=378hmj1ks69q2b8tv62uk5cv301k46eg; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=c20c30aad8f377a16f73388752f744be;
csrf_cookie_ppdbappenas=022766b7257af010aa384936ac391a85;
csrf_cookie_2022ppd=500927e27766ee7ef564379271912a33;
csrf_cookie_2023ppd=3179abfa0a63484fd947c078da65dbed;
csrf_cookie_2024ppd=d5305e0ad1b3b12d6e92973eca3e77ae
Content-Length: 0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: peppd.bappenas.go.id
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 jQuery 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

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/)

Affected items

Web Server
Details
Paths without CSP header: • https://peppd.bappenas.go.id/ • https://peppd.bappenas.go.id/welcome • https://peppd.bappenas.go.id/9404525 • https://peppd.bappenas.go.id/global.asa.bak • https://peppd.bappenas.go.id/user_guide/ • https://peppd.bappenas.go.id/php.ini • https://peppd.bappenas.go.id/users.db • https://peppd.bappenas.go.id/global.asax.bak • https://peppd.bappenas.go.id/propel.ini • https://peppd.bappenas.go.id/htaccess.bak • https://peppd.bappenas.go.id/users.ini • https://peppd.bappenas.go.id/web.config.bak • https://peppd.bappenas.go.id/jumper_ppd/ • https://peppd.bappenas.go.id/pemantauan/ • https://peppd.bappenas.go.id/peppd/Home/demo/ • https://peppd.bappenas.go.id/ppd2021/ • https://peppd.bappenas.go.id/peppd/Home/ • https://peppd.bappenas.go.id/jumper_ppd/video/ppd.ogv • https://peppd.bappenas.go.id/peppd/ • https://peppd.bappenas.go.id/media/kegiatan/pemantauan • https://peppd.bappenas.go.id/jumper_ppd/video/ppd.webm
Request headers

```
GET / HTTP/1.1
Referer: https://peppd.bappenas.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/119.0.0.0 Safari/537.36
Host: peppd.bappenas.go.id
Connection: Keep-alive
```

Generic Email Address Disclosure

Severity	**Informational**
Reported by module	/target/404_text_search.js

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.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

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

Affected items

Web Server
Details

Emails found:

- https://peppd.bappenas.go.id/
  dit.peppd@bappenas.go.id
- https://peppd.bappenas.go.id/
  ppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/kegiatan/pemantauan
  muhamadmunawiramin@gmail.com
- https://peppd.bappenas.go.id/media/kegiatan/pemantauan
  dit.peppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/kegiatan/pemantauan
  ppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/commentController/index
  rayat@indonesia.id
- https://peppd.bappenas.go.id/media/karir
  muhamadmunawiramin@gmail.com
- https://peppd.bappenas.go.id/media/karir
  dit.peppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/karir
  ppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/aplikasi
  muhamadmunawiramin@gmail.com
- https://peppd.bappenas.go.id/media/aplikasi
  dit.peppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/aplikasi
  ppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/kegiatan
  muhamadmunawiramin@gmail.com
- https://peppd.bappenas.go.id/media/kegiatan
  dit.peppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/kegiatan
  ppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/
  dit.peppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/
  ppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/news
  muhamadmunawiramin@gmail.com
- https://peppd.bappenas.go.id/media/news
  dit.peppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/news
  ppd@bappenas.go.id
- https://peppd.bappenas.go.id/media/publication
  muhamadmunawiramin@gmail.com

Request headers

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

HTTP Strict Transport Security (HSTS) Errors and Warnings

Severity	**Informational**
Reported by module	/httpdata/HSTS_not_implemented.js

Description

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict Transport Security (HSTS) implementation is not as strict as is typically advisable.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

Recommendation

It is recommended to implement best practices of HTTP Strict Transport Security (HSTS) in your web application. Consult web references for more information.

References

hstspreload.org (https://hstspreload.org/)
MDN: Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

Affected items

Web Server
Details
URLs where HSTS configuration is not according to best practices: • https://peppd.bappenas.go.id/global.asa.bak - No includeSubDomains directive • https://peppd.bappenas.go.id/php.ini - No includeSubDomains directive • https://peppd.bappenas.go.id/users.db - No includeSubDomains directive • https://peppd.bappenas.go.id/global.asax.bak - No includeSubDomains directive • https://peppd.bappenas.go.id/propel.ini - No includeSubDomains directive • https://peppd.bappenas.go.id/htaccess.bak - No includeSubDomains directive • https://peppd.bappenas.go.id/users.ini - No includeSubDomains directive • https://peppd.bappenas.go.id/web.config.bak - No includeSubDomains directive • https://peppd.bappenas.go.id/media/assets/images/summernote/%0A%3Cdiv%20style= - No includeSubDomains directive
Request headers

`GET /global.asa.bak HTTP/1.1`
`Referer: https://peppd.bappenas.go.id/`
`Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true; poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true; poptin_c_visitor=true`
`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`

Javascript Source map detected

Severity	**Informational**
Reported by module	/httpdata/sourcemap_detection.js

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.

Impact

Access to source maps may help an attacker to read and debug Javascript code. It simplifies finding client-side vulnerabilities

Recommendation

According to the best practices, source maps should not be accesible for an attacker. Consult web references for more information

References

Using sourcemaps on production without exposing the source code (https://itnext.io/using-sourcemaps-on-production-without-revealing-the-source-code-%EF%B8%8F-d41e78e20c89)
SPA source code recovery by un-Webpacking source maps (https://medium.com/@rarecoil/spa-source-code-recovery-by-un-webpacking-source-maps-ef830fc2351d)

Affected items

Web Server
Details
URLs where links to SourceMaps were found: • sourceMappingURL in JS body - https://peppd.bappenas.go.id/media/assets/assets/bootstrap-4.6.0-dist/js/bootstrap.bundle.min.js
Request headers

```
GET /media/assets/assets/bootstrap-4.6.0-dist/js/bootstrap.bundle.min.js HTTP/1.1
Referer: https://peppd.bappenas.go.id/
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true; poptin_c_visitor=true
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	/httpdata/javascript_library_audit_external.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

- **jQuery 3.5.1**
  - URL: https://code.jquery.com/jquery-3.5.1.slim.min.js
  - Detection method: The library's name and version were determined based on the file's CDN URI.
  - References:
    - https://code.jquery.com/

Request headers

```
GET / HTTP/1.1
Referer: https://peppd.bappenas.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/119.0.0.0 Safari/537.36
Host: peppd.bappenas.go.id
Connection: Keep-alive
```

Web Server

Details

- **bootstrap.js 4.6.0**
  - URL: https://peppd.bappenas.go.id/
  - 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 / HTTP/1.1
Referer: https://peppd.bappenas.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/119.0.0.0 Safari/537.36
Host: peppd.bappenas.go.id
Connection: Keep-alive
```

Web Server

Details

- **bootstrap.js 4.0.0**
  - URL: https://peppd.bappenas.go.id/jumper_ppd/
  - 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 /jumper_ppd/ HTTP/1.1
Referer: https://peppd.bappenas.go.id/
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa
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

- **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/
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=4d7f436ce1fd274313e65a4c07ca59d4
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/
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=4d7f436ce1fd274313e65a4c07ca59d4
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/
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=4d7f436ce1fd274313e65a4c07ca59d4
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

- **bootstrap.js 4.0.0-beta**
  - URL: https://peppd.bappenas.go.id/pemantauan/package/plugins/login_v1/vendor/bootstrap/js/bootstrap.min.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: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=6663e64a9c8e2b73ae0415352b9e7e67;
csrf_cookie_ppdbappenas=3f4e890488c2976b3950bff4533abc80;
csrf_cookie_2022ppd=27a95149cb7e91e0c19a33998390d375;
csrf_cookie_2023ppd=aa4d686e214e44638d13a4c172812e14
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

- **bootstrap.js 3.3.7**
  - URL: https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/bootstrap.min.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 /media/assets/zircosadmin/assets/js/bootstrap.min.js HTTP/1.1
Cookie: ci_session=qt2945tgu11teq9q1a9s8oi5op2oqlin; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=c20c30aad8f377a16f73388752f744be;
csrf_cookie_ppdbappenas=022766b7257af010aa384936ac391a85;
csrf_cookie_2022ppd=500927e27766ee7ef564379271912a33;
csrf_cookie_2023ppd=3179abfa0a63484fd947c078da65dbed;
csrf_cookie_2024ppd=d5305e0ad1b3b12d6e92973eca3e77ae
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: ci_session=ausdvrtpmm04hjtgncnrs1b5dh34af1r; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=c20c30aad8f377a16f73388752f744be;
csrf_cookie_ppdbappenas=022766b7257af010aa384936ac391a85;
csrf_cookie_2022ppd=500927e27766ee7ef564379271912a33;
csrf_cookie_2023ppd=3179abfa0a63484fd947c078da65dbed;
csrf_cookie_2024ppd=d5305e0ad1b3b12d6e92973eca3e77ae
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/jquery-validation/jquery-validation/tags

Request headers

```
GET /pemantauan/package/plugins/jquery-validation-1.15.0/dist/jquery.validate.min.js HTTP/1.1
Cookie: ci_session=378hmj1ks69q2b8tv62uk5cv301k46eg; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=c20c30aad8f377a16f73388752f744be;
csrf_cookie_ppdbappenas=022766b7257af010aa384936ac391a85;
csrf_cookie_2022ppd=500927e27766ee7ef564379271912a33;
csrf_cookie_2023ppd=3179abfa0a63484fd947c078da65dbed;
csrf_cookie_2024ppd=d5305e0ad1b3b12d6e92973eca3e77ae
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: ci_session=378hmj1ks69q2b8tv62uk5cv301k46eg; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=c20c30aad8f377a16f73388752f744be;
csrf_cookie_ppdbappenas=022766b7257af010aa384936ac391a85;
csrf_cookie_2022ppd=500927e27766ee7ef564379271912a33;
csrf_cookie_2023ppd=3179abfa0a63484fd947c078da65dbed;
csrf_cookie_2024ppd=d5305e0ad1b3b12d6e92973eca3e77ae
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

Permissions-Policy / Feature-Policy (MDN) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)
Permissions Policy (W3C) (https://www.w3.org/TR/permissions-policy-1/)

Affected items

Web Server
Details
Locations without Permissions-Policy header: • https://peppd.bappenas.go.id/ • https://peppd.bappenas.go.id/welcome • https://peppd.bappenas.go.id/9404525 • https://peppd.bappenas.go.id/global.asa.bak • https://peppd.bappenas.go.id/user_guide/ • https://peppd.bappenas.go.id/php.ini • https://peppd.bappenas.go.id/users.db • https://peppd.bappenas.go.id/global.asax.bak • https://peppd.bappenas.go.id/propel.ini • https://peppd.bappenas.go.id/htaccess.bak • https://peppd.bappenas.go.id/users.ini • https://peppd.bappenas.go.id/web.config.bak • https://peppd.bappenas.go.id/jumper_ppd/ • https://peppd.bappenas.go.id/pemantauan/ • https://peppd.bappenas.go.id/peppd/Home/demo/ • https://peppd.bappenas.go.id/assets/ • https://peppd.bappenas.go.id/demo/ • https://peppd.bappenas.go.id/ppd2021/ • https://peppd.bappenas.go.id/jumper_ppd/video/ppd.ogv • https://peppd.bappenas.go.id/peppd/Home/ • https://peppd.bappenas.go.id/peppd/
Request headers

`GET / HTTP/1.1`
`Referer: https://peppd.bappenas.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/119.0.0.0 Safari/537.36`
`Host: peppd.bappenas.go.id`
`Connection: Keep-alive`

Subresource Integrity (SRI) Not Implemented

Severity	**Informational**
Reported by module	/RPA/SRI_Not_Implemented.js

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.

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.

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/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
        crossorigin="anonymous"></script>
```

References

Subresource Integrity (https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)
SRI Hash Generator (https://www.srihash.org/)

Affected items

Web Server

Details

Pages where SRI is not implemented:

- https://peppd.bappenas.go.id/
  Script SRC: **https://www.googletagmanager.com/gtag/js?id=G-0M5J29J5Y3**
- https://peppd.bappenas.go.id/
  Script SRC: **https://api.mapbox.com/mapbox-gl-js/v1.11.0/mapbox-gl.js**
- https://peppd.bappenas.go.id/
  Script SRC: **https://cdn.polyfill.io/v2/polyfill.min.js?features=fetch,requestAnimationFrame,Element.prototype.classList,URL**
- https://peppd.bappenas.go.id/
  Script SRC: **https://ajax.googleapis.com/ajax/libs/jquery/3.4.0/jquery.min.js**
- https://peppd.bappenas.go.id/
  Script SRC: **https://code.jquery.com/jquery-3.5.1.slim.min.js**
- https://peppd.bappenas.go.id/
  Script SRC: **https://cdn.popt.in/pixel.js?id=09ea66852b293**
- https://peppd.bappenas.go.id/
  Script SRC: **https://cdn.lordicon.com/libs/mssddfmo/lord-icon-2.1.0.js**

Request headers

```
GET / HTTP/1.1
Referer: https://peppd.bappenas.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/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
Details
Detected Imperva SecureSphere from the response body.
Request headers

```
TESTING /9404525 HTTP/1.1
Cookie: ci_session=kmo25fvc750glgj4tu5brpmqqag7bgkr; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true; poptin_c_visitor=true
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] Internal Path Disclosure (*nix)

Severity	**Informational**
Reported by module	/httpdata/text_search.js

Description

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure (https://www.owasp.org/index.php/Full_Path_Disclosure)

Affected items

Web Server
Details
Pages with paths being disclosed: • https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/ **/var/www/peppd/media/application/controllers/C_pagesController.php** • https://peppd.bappenas.go.id/media/logPortalController/store **/var/www/peppd/media/application/controllers/C_logPortalController.php**
Request headers

```
GET /media/C_pagesController/article_pagination/ HTTP/1.1
Referer: https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/
Cookie: ci_session=ausdvrtpmm04hjtgncnrs1b5dh34af1r; poptin_old_user=true;
poptin_user_id=0.vrncx8qcty; poptin_previous_url=; poptin_session=true;
poptin_c_visitor=true; csrf_cookie_ppsys=a9fa78929b8f27a74d37268d3ca2bbaa;
csrf_cookie_peppd=c20c30aad8f377a16f73388752f744be;
csrf_cookie_ppdbappenas=022766b7257af010aa384936ac391a85;
csrf_cookie_2022ppd=500927e27766ee7ef564379271912a33;
csrf_cookie_2023ppd=3179abfa0a63484fd947c078da65dbed;
csrf_cookie_2024ppd=d5305e0ad1b3b12d6e92973eca3e77ae
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)

https://peppd.bappenas.go.id/
https://peppd.bappenas.go.id/"https:/
https://peppd.bappenas.go.id/"https:/yokbaca.com/
https://peppd.bappenas.go.id/"https:/yokbaca.com/"
https://peppd.bappenas.go.id/"https:/yokbaca.com/kelebihan-dan-kekurangan-ai-artificial-intelligence/
https://peppd.bappenas.go.id/"https:/yokbaca.com/kelebihan-dan-kekurangan-ai-artificial-intelligence/"
https://peppd.bappenas.go.id/9404525
https://peppd.bappenas.go.id/assets/
https://peppd.bappenas.go.id/bookinfo.js
https://peppd.bappenas.go.id/demo/
https://peppd.bappenas.go.id/getuserinfo.js
https://peppd.bappenas.go.id/global.asa.bak
https://peppd.bappenas.go.id/global.asax.bak
https://peppd.bappenas.go.id/htaccess.bak
https://peppd.bappenas.go.id/jumper_ppd/
https://peppd.bappenas.go.id/jumper_ppd/assets/
https://peppd.bappenas.go.id/jumper_ppd/assets/bootstrap/
https://peppd.bappenas.go.id/jumper_ppd/assets/bootstrap/dist/
https://peppd.bappenas.go.id/jumper_ppd/assets/bootstrap/dist/css/
https://peppd.bappenas.go.id/jumper_ppd/assets/bootstrap/dist/css/bootstrap.min.css
https://peppd.bappenas.go.id/jumper_ppd/assets/bootstrap/dist/fonts/
https://peppd.bappenas.go.id/jumper_ppd/assets/custom_select/
https://peppd.bappenas.go.id/jumper_ppd/assets/custom_select/style.css
https://peppd.bappenas.go.id/jumper_ppd/assets/images/
https://peppd.bappenas.go.id/jumper_ppd/assets/js/
https://peppd.bappenas.go.id/jumper_ppd/assets/js/index.js
https://peppd.bappenas.go.id/jumper_ppd/assets/js/jquery.vide.js
https://peppd.bappenas.go.id/jumper_ppd/video/
https://peppd.bappenas.go.id/jumper_ppd/video/ppd.ogv
https://peppd.bappenas.go.id/jumper_ppd/video/ppd.webm
https://peppd.bappenas.go.id/license.txt
https://peppd.bappenas.go.id/media/
https://peppd.bappenas.go.id/media/2
https://peppd.bappenas.go.id/media/3
https://peppd.bappenas.go.id/media/4
https://peppd.bappenas.go.id/media/5
https://peppd.bappenas.go.id/media/6
https://peppd.bappenas.go.id/media/7
https://peppd.bappenas.go.id/media/C_pagesController/
https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/
https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/1
https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/2
https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/3
https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/4
https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/5
https://peppd.bappenas.go.id/media/C_pagesController/article_pagination/6
https://peppd.bappenas.go.id/media/aplikasi
https://peppd.bappenas.go.id/media/assets/
https://peppd.bappenas.go.id/media/assets/assets/
https://peppd.bappenas.go.id/media/assets/assets/bootstrap-4.6.0-dist/
https://peppd.bappenas.go.id/media/assets/assets/bootstrap-4.6.0-dist/css/
https://peppd.bappenas.go.id/media/assets/assets/bootstrap-4.6.0-dist/css/bootstrap.min.css
https://peppd.bappenas.go.id/media/assets/assets/bootstrap-4.6.0-dist/js/
https://peppd.bappenas.go.id/media/assets/assets/bootstrap-4.6.0-dist/js/bootstrap.bundle.min.js
https://peppd.bappenas.go.id/media/assets/documents/
https://peppd.bappenas.go.id/media/assets/documents/pedoman/
https://peppd.bappenas.go.id/media/assets/documents/pedoman/pedoman_ppd_2024/
https://peppd.bappenas.go.id/media/assets/file_publication/
https://peppd.bappenas.go.id/media/assets/file_publication/Knowledge-Sharing-Pembangunan-Daerah-2018/
https://peppd.bappenas.go.id/media/assets/file_publication/Knowledge-Sharing-Pembangunan-Daerah-2019--
-2020/
https://peppd.bappenas.go.id/media/assets/file_publication/Prosiding-Knowledge-Sharing-2018/
https://peppd.bappenas.go.id/media/assets/file_publication/Prosiding-Knowledge-Sharing-2019/
https://peppd.bappenas.go.id/media/assets/images/
https://peppd.bappenas.go.id/media/assets/images/img/

https://peppd.bappenas.go.id/media/assets/images/img/carousel/
https://peppd.bappenas.go.id/media/assets/images/img/evaluasi/
https://peppd.bappenas.go.id/media/assets/images/img/koordinasi/
https://peppd.bappenas.go.id/media/assets/images/img/logo-kegiatan/
https://peppd.bappenas.go.id/media/assets/images/img/pemantauan/
https://peppd.bappenas.go.id/media/assets/images/summernote/
https://peppd.bappenas.go.id/media/assets/images/summernote/ <div style=
https://peppd.bappenas.go.id/media/assets/zircosadmin/
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/css/
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/css/bootstrap.min.css
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/css/components.css
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/css/core.css
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/css/icons.css
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/css/menu.css
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/css/pages.css
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/css/responsive.css
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/fonts/
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/images/
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/bootstrap.min.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/detect.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/fastclick.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/jquery.app.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/jquery.blockUI.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/jquery.core.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/jquery.min.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/jquery.scrollTo.min.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/jquery.slimscroll.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/modernizr.min.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/js/waves.js
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/plugins/
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/plugins/multiselect/
https://peppd.bappenas.go.id/media/assets/zircosadmin/assets/plugins/multiselect/img/
https://peppd.bappenas.go.id/media/assets/zircosadmin/plugins/
https://peppd.bappenas.go.id/media/assets/zircosadmin/plugins/count-down/
https://peppd.bappenas.go.id/media/assets/zircosadmin/plugins/count-down/jquery.lwtCountdown-1.0.js
https://peppd.bappenas.go.id/media/commentController/
https://peppd.bappenas.go.id/media/commentController/destroy
https://peppd.bappenas.go.id/media/commentController/index
https://peppd.bappenas.go.id/media/commentController/store
https://peppd.bappenas.go.id/media/file_publication/
https://peppd.bappenas.go.id/media/file_publication/Knowledge-Sharing-Pembangunan-Daerah-2018/
https://peppd.bappenas.go.id/media/file_publication/Knowledge-Sharing-Pembangunan-Daerah-2019---2020/
https://peppd.bappenas.go.id/media/file_publication/Prosiding-Knowledge-Sharing-2018/
https://peppd.bappenas.go.id/media/file_publication/Prosiding-Knowledge-Sharing-2019/
https://peppd.bappenas.go.id/media/karir
https://peppd.bappenas.go.id/media/kegiatan
https://peppd.bappenas.go.id/media/kegiatan/
https://peppd.bappenas.go.id/media/kegiatan/evaluasi
https://peppd.bappenas.go.id/media/kegiatan/koordinasi
https://peppd.bappenas.go.id/media/kegiatan/pemantauan
https://peppd.bappenas.go.id/media/kegiatan/penghargaan
https://peppd.bappenas.go.id/media/logPortalController/
https://peppd.bappenas.go.id/media/logPortalController/store
https://peppd.bappenas.go.id/media/news
https://peppd.bappenas.go.id/media/news/
https://peppd.bappenas.go.id/media/news/BAPPENAS-HELAT-SOSIALISASI-PENGHARGAAN-PEMBANGUNAN-DAERAH-PPD-TAHUN-2024-KEPADA-38-PROVINSI-DAN-514-KABUPATENKOTA
https://peppd.bappenas.go.id/media/news/Bahas-Pemanfaatan-Pagu-Indikatif-Ombudsman-Tahun-2024-Bappenas-Gelar-Rangkaian-Pertemuan-Dua-Pihak-dan-Tiga-Pihak-secara-Hybrid
https://peppd.bappenas.go.id/media/news/Bappenas-Gelar-Diskusi-Pemantauan-Implementasi-Survei-Kepatuhan-Pelayanan-Publik-Tahun-2021-Bersama-Ombudsman-Republik-Indonesia
https://peppd.bappenas.go.id/media/news/Bappenas-Gelar-Diskusi-Sistem-Informasi-Keuangan-Daerah--Untuk-Pengayaan-Analisis-Evaluasi-Kinerja-Pembangunan-Daerah-2023
https://peppd.bappenas.go.id/media/news/Bappenas-Gelar-Pertemuan-Dua-Pihak-dengan-Ombudsman-RI-Bahas-Tindak-Lanjut-Usulan-Kebijakan-Baru-Tahun-Anggaran-2023

https://peppd.bappenas.go.id/media/news/Bappenas-Libatkan-Kementerian-PAN-RB-dan-Ombudsman-RI-dalam-Evaluasi-dan-Perencanaan-RT-RPJMN-2025-2029-terkait-Substansi-Pengawasan-Eksternal-Pelayanan-Publik
https://peppd.bappenas.go.id/media/news/Bappenas-dan-Ombudsman-RI-Pantau-Langsung-Pelayanan-Publik-di-Provinsi-Nusa-Tenggara-Timur
https://peppd.bappenas.go.id/media/news/Bappenas-gelar-Diskusi-Pendalaman-Evaluasi-Kinerja-Pembangunan-Daerah-2022-dengan-stakeholders-7-Provinsi
https://peppd.bappenas.go.id/media/news/Berbagi-Pandangan-dalam-Kegiatan-Pengawasan-Eksternal-Pelayanan-Publik-Bagi-Kelompok-Marjinal-di-Daerah-3T-Terluar-Terdepan-dan-Tertinggal
https://peppd.bappenas.go.id/media/news/Bilateral-Meeting-Exercise-Pemanfaatan-Pagu-Indikatif-RI-TA-2023-untuk-Ombudsman-RI
https://peppd.bappenas.go.id/media/news/Brainstorming-dan-Transfer-Knowledge-Metodologi-dan-Aturan-Formulasi-Dana-Insentif-Daerah-bersama-Kementerian-Keuangan-dan-Universitas-Indonesia
https://peppd.bappenas.go.id/media/news/Daerah-Terbaik-Penerima-Penghargaan-Pembangunan-Daerah-2021
https://peppd.bappenas.go.id/media/news/Dalam-rangka-pemantauan-Bappenas-lakukan-Diskusi-Pendalaman-Muatan-Substansi-Penjaminan-Mutu-Pencegahan-Maladministrasi-dan-Kajian-3T-Ombudsman-RI-di-Banten-
https://peppd.bappenas.go.id/media/news/Dampak-Refocusing-Anggaran-dan-Perubahan-Kebijakan-Bappenas-Laksanakan-Diskusi-Penyesuaian-Renja-Ombudsman-RI-TA-2021
https://peppd.bappenas.go.id/media/news/Dinamika-Penyelenggaraan-Pengawasan-Pelayanan-Publik-di-Ombudsman-RI-Perwakilan-Nusa-Tenggara-Timur-NTT
https://peppd.bappenas.go.id/media/news/Direktorat-PEPPD-Bappenas-Gelar-Diskusi-EvaluasiPengawasan-Pelayanan-Publik-bersama-Ombudsman-RI-dan-Kementerian-PANRB-
https://peppd.bappenas.go.id/media/news/Diskusi-Awal-Perencanaan-Pengawasan-Eksternal-Pelayanan-Publik-Jangka-Panjang-2025-2045-dan-Jangka-Menengah-2025-2029
https://peppd.bappenas.go.id/media/news/Diskusi-DAK-Fisik-Penugasan-Bidang-Pariwisata-Bersama-Pemerintah-Provinsi-Sulawesi-Tenggara
https://peppd.bappenas.go.id/media/news/Diskusi-Daring-Memotret-Perkembangan-Pelaksanaan-Kebijakan-DAK-Fisik-dan-Nonfisik-dalam-mendukung-Pemulihan-Ekonomi-Nasional-di-Daerah-Tahun-2022
https://peppd.bappenas.go.id/media/news/Diskusi-Pemantauan-DAK-Fisik-Penugasan-Tematik-Penyediaan-Infrastruktur-Ekonomi-Berkelanjutan-Tahun-2021
https://peppd.bappenas.go.id/media/news/Expo-Penghargaan-Pembangunan-Daerah-PPD-2023
https://peppd.bappenas.go.id/media/news/FGD-Pendalaman-Evaluasi-Kinerja-Pembangunan-Daerah-pada-7-Provinsi
https://peppd.bappenas.go.id/media/news/Field-Visit-Evaluasi-Tematis-Optimalisasi-Inklusivitas-Sektor-Ekonomi-Dominan-ke-Tujuh-Daerah
https://peppd.bappenas.go.id/media/news/Focus-Group-Discussion-Pendalaman-Review-Major-Project-MP-Kewilayahan-RKP-2021-dengan-Stakeholders-Daerah
https://peppd.bappenas.go.id/media/news/Insight-Praktik-Praktik-Cerdas-Penghargaan-Pembangunan-Daerah-Tahun-2022
https://peppd.bappenas.go.id/media/news/Knowledge-Sharing-Metodologi-dan-Pelaksanaan-Evaluasi-bersama-Mitra-Pembangunan
https://peppd.bappenas.go.id/media/news/Kolaborasi-Bappenas-dan-Ombudsman-RI-Pusat-dalam-Pendampingan-Proses-Penilaian-Kepatuhan-Penyelenggaraan-Pelayanan-Publik-di-Kota-Tasikmalaya-Tahun-2023
https://peppd.bappenas.go.id/media/news/Kolaborasi-Kementerian-PPNBappenas-dan-Ombudsman-RI-dalam-Pemantauan-Pembangunan-dan-Pengawasan-Pelayanan-Publik-di-Provinsi-Sumatera-Barat
https://peppd.bappenas.go.id/media/news/Koordinasi-Awal-Review-Major-Project-Kewilayahan-RKP-2021
https://peppd.bappenas.go.id/media/news/Koordinasi-Internal-Pelaksanaan-Evaluasi-Pembangunan-Daerah-2021
https://peppd.bappenas.go.id/media/news/Koordinasi-Pembahasan-Pagu-Indikatif-Tahun-2022-Ombudsman-RI-dalam-forum-Trilateral-Meeting
https://peppd.bappenas.go.id/media/news/Kunjungi-Provinsi-Kalimantan-Utara-Kementerian-PPNBappenas-dan-Ombudsman-RI-Tinjau-Pelaksanaan-Kebijakan-Pengawasan-dan-Evaluasi-Kinerja-Pelayanan-Publik-di-Tingkat-Tapak
https://peppd.bappenas.go.id/media/news/Menjaring-Gagasan-Praktisi-Pengawasan-Pelayanan-Publik-di-Daerah-untuk-Penyusunan-Perencanaan-Jangka-Panjang-dan-Menengah
https://peppd.bappenas.go.id/media/news/Menjaring-Masukan-Perencanaan-Pembangunan-Bidang-Industri-Kecil-dan-Menengah-Tahun-2021-di-Daerah-Berbasis-Anggaran-DAK-Fisik
https://peppd.bappenas.go.id/media/news/Menjaring-Masukan-Perencanaan-Pembangunan-dari-Implementasi-Mal-Pelayanan-Publik-dan-Reaksi-Cepat-Ombudsman-RCO-di-Provinsi-Maluku-Utara
https://peppd.bappenas.go.id/media/news/Menteri-PPNKepala-Bappenas-melaunching-Buku-Knowledge-Sharing-dan-menyerahkan-Piala-Penghargaan-Pembangunan-Daerah-2020-2021-serta-Penghargaan-Khusus-kepada-Kepala-Daerah
https://peppd.bappenas.go.id/media/news/Pembahasan-Hasil-Field-Visit-Evaluasi-Tematis-di-7-Daerah-terkait-Optimalisasi-Inklusivitas-Sektor-Ekonomi-Dominan-di-Daerah
https://peppd.bappenas.go.id/media/news/Pembahasan-Rancangan-Awal-Rencana-Kerja-Renja-Tahun-Anggaran-2024-bersama-Biro-Perencanaan-Keuangan-Ombudsman-RI
https://peppd.bappenas.go.id/media/news/Pembahasan-Rencana-Kerja-Ombudsman-RI-Tahun-Anggaran-2023
https://peppd.bappenas.go.id/media/news/Pemutakhiran-Renja-KL-TA-2022-Ombudsman-RI-Berkoordinasi-dengan-Bappenas

https://peppd.bappenas.go.id/media/news/Penilaian-Tahap-III-Verifikasi-PPD-2022-FGD-dan-Kunjungan-Lapangan
https://peppd.bappenas.go.id/media/news/Pentingnya-Kolaborasi-Lintas-Sektor-dalam-Evaluasi-Pembinaan-dan-Pengawasan-Pelayanan-Publik-di-Indonesia
https://peppd.bappenas.go.id/media/news/Penyerahan-Piala-Penghargaan-Pembangunan-Daerah-PPD-dan-Penghargaan-Khusus-serta-Talkshow-Knowledge-Sharing-Pembangunan-Daerah-2022
https://peppd.bappenas.go.id/media/news/Peraih-Penghargaan-Pembangunan-Daerah-2022
https://peppd.bappenas.go.id/media/news/Perencanaan-dan-Implementasi-Pengawasan-Pelayanan-Publik-di-Sulawesi-Selatan
https://peppd.bappenas.go.id/media/news/Pertemuan-Tiga-Pihak-Exercise-Pagu-Indikatif-dan-Rencana-Kerja-Ombudsman-RI-TA-2023
https://peppd.bappenas.go.id/media/news/Pertemuan-Tiga-Pihak-Exercise-Pagu-Indikatif-dan-Rencana-Kerja-Ombudsman-RI-TA-2023-
https://peppd.bappenas.go.id/media/news/Presentasi-dan-Wawancara-KabupatenKota-PPD-2022
https://peppd.bappenas.go.id/media/news/RAPAT-KONSOLIDASI-INTERNAL-DIREKTORAT-PEPPD-2021
https://peppd.bappenas.go.id/media/news/SHARING-SESSION-PEMBANGUNAN-DAERAH-TAHUN-2022
https://peppd.bappenas.go.id/media/news/Sosialisasi-Penghargaan-Pembangunan-Daerah-PPD-2022-untuk--Pemerintah-Daerah-Tingkat-Provinsi-dan-KabupatenKota
https://peppd.bappenas.go.id/media/news/Sosialisasi-Penghargaan-Pembangunan-Daerah-PPD-2023-untuk-Pemerintah-Daerah-Tingkat-Provinsi-dan-KabupatenKota
https://peppd.bappenas.go.id/media/news/Sosialisasi-Penghargaan-Pembangunan-Daerah-PPD-Tahun-2022-untuk-Tim-Penilai-Teknis-TPT
https://peppd.bappenas.go.id/media/news/Sukses-Pelaksanaan-Tahap-II-Presentasi-dan-Wawancara-Tingkat-Provinsi-PPD-2022
https://peppd.bappenas.go.id/media/news/Tinjau-Perkembangan-Pengawasan-Pelayanan-Publik-dengan-Lokalitas-Daerah-Bappenas-Gelar-Diskusi-Bersama-Ombudsman-RI-Perwakilan-DI-Yogyakarta
https://peppd.bappenas.go.id/media/news/Webinar-Strategi-Pencapaian-Kinerja-Pembangunan-Daerah--di-Masa-Pandemi-Covid-19
https://peppd.bappenas.go.id/media/news/shared
https://peppd.bappenas.go.id/media/publication
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/jquery.nicescroll.js
https://peppd.bappenas.go.id/pemantauan/package/js/jquery.scrollTo.min.js
https://peppd.bappenas.go.id/pemantauan/package/js/modernizr.min.js
https://peppd.bappenas.go.id/pemantauan/package/js/universal.js
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-awesome.min.css
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/js/
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/jquery/jquery-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.js
https://peppd.bappenas.go.id/peppd/

https://peppd.bappenas.go.id/peppd/Home/
https://peppd.bappenas.go.id/peppd/Home/demo/
https://peppd.bappenas.go.id/php.ini
https://peppd.bappenas.go.id/ppd2021/
https://peppd.bappenas.go.id/ppd2021/Welcome/
https://peppd.bappenas.go.id/ppd2021/Welcome/login_act
https://peppd.bappenas.go.id/ppd2021/Welcome/refresh_captcha
https://peppd.bappenas.go.id/ppd2021/assets/
https://peppd.bappenas.go.id/ppd2021/assets/images/
https://peppd.bappenas.go.id/ppd2021/assets/js/
https://peppd.bappenas.go.id/ppd2021/assets/js/admin/
https://peppd.bappenas.go.id/ppd2021/assets/js/admin/login/
https://peppd.bappenas.go.id/ppd2021/assets/js/admin/login/login.js
https://peppd.bappenas.go.id/ppd2021/assets/js/universal.js
https://peppd.bappenas.go.id/ppd2021/captcha/
https://peppd.bappenas.go.id/ppd2021/package/
https://peppd.bappenas.go.id/ppd2021/package/css/
https://peppd.bappenas.go.id/ppd2021/package/css/PIE.htc
https://peppd.bappenas.go.id/ppd2021/package/css/animate.css
https://peppd.bappenas.go.id/ppd2021/package/css/bootstrap.min.css
https://peppd.bappenas.go.id/ppd2021/package/css/helper.css
https://peppd.bappenas.go.id/ppd2021/package/css/material-design-iconic-font.min.css
https://peppd.bappenas.go.id/ppd2021/package/css/style.css
https://peppd.bappenas.go.id/ppd2021/package/css/userdefined.css
https://peppd.bappenas.go.id/ppd2021/package/css/waves-effect.css
https://peppd.bappenas.go.id/ppd2021/package/fonts/
https://peppd.bappenas.go.id/ppd2021/package/images/
https://peppd.bappenas.go.id/ppd2021/package/images/small/
https://peppd.bappenas.go.id/ppd2021/package/js/
https://peppd.bappenas.go.id/ppd2021/package/js/bootstrap.min.js
https://peppd.bappenas.go.id/ppd2021/package/js/jquery.min.js
https://peppd.bappenas.go.id/ppd2021/package/js/jquery.nicescroll.js
https://peppd.bappenas.go.id/ppd2021/package/js/jquery.scrollTo.min.js
https://peppd.bappenas.go.id/ppd2021/package/js/modernizr.min.js
https://peppd.bappenas.go.id/ppd2021/package/js/waves.js
https://peppd.bappenas.go.id/ppd2021/package/js/wow.min.js
https://peppd.bappenas.go.id/ppd2021/package/plugins/
https://peppd.bappenas.go.id/ppd2021/package/plugins/fastclick/
https://peppd.bappenas.go.id/ppd2021/package/plugins/fastclick/fastclick.js
https://peppd.bappenas.go.id/ppd2021/package/plugins/font-awesome/
https://peppd.bappenas.go.id/ppd2021/package/plugins/font-awesome/css/
https://peppd.bappenas.go.id/ppd2021/package/plugins/font-awesome/css/font-awesome.min.css
https://peppd.bappenas.go.id/ppd2021/package/plugins/font-awesome/fonts/
https://peppd.bappenas.go.id/ppd2021/package/plugins/ionicon/
https://peppd.bappenas.go.id/ppd2021/package/plugins/ionicon/css/
https://peppd.bappenas.go.id/ppd2021/package/plugins/ionicon/css/ionicons.min.css
https://peppd.bappenas.go.id/ppd2021/package/plugins/ionicon/fonts/
https://peppd.bappenas.go.id/ppd2021/package/plugins/jquery-blockui/
https://peppd.bappenas.go.id/ppd2021/package/plugins/jquery-blockui/jquery.blockUI.js
https://peppd.bappenas.go.id/ppd2021/package/plugins/jquery-detectmobile/
https://peppd.bappenas.go.id/ppd2021/package/plugins/jquery-detectmobile/detect.js
https://peppd.bappenas.go.id/ppd2021/package/plugins/jquery-slimscroll/
https://peppd.bappenas.go.id/ppd2021/package/plugins/jquery-slimscroll/jquery.slimscroll.js
https://peppd.bappenas.go.id/ppd2021/package/plugins/jquery-validation-1.15.0/
https://peppd.bappenas.go.id/ppd2021/package/plugins/jquery-validation-1.15.0/dist/
https://peppd.bappenas.go.id/ppd2021/package/plugins/jquery-validation-1.15.0/dist/jquery.validate.min.js
https://peppd.bappenas.go.id/ppd2021/package/plugins/sweetalert/
https://peppd.bappenas.go.id/ppd2021/package/plugins/sweetalert/dist/
https://peppd.bappenas.go.id/ppd2021/package/plugins/sweetalert/dist/sweetalert2.all.min.js
https://peppd.bappenas.go.id/ppd2021/package/plugins/sweetalert/dist/sweetalert2.min.css
https://peppd.bappenas.go.id/ppd2021/package/plugins/sweetalert/dist/sweetalert2.min.js
https://peppd.bappenas.go.id/ppd2022/
https://peppd.bappenas.go.id/ppd2022/Welcome/
https://peppd.bappenas.go.id/ppd2022/Welcome/login_act
https://peppd.bappenas.go.id/ppd2022/Welcome/refresh_captcha
https://peppd.bappenas.go.id/ppd2022/assets/
https://peppd.bappenas.go.id/ppd2022/assets/images/

https://peppd.bappenas.go.id/ppd2022/assets/js/
https://peppd.bappenas.go.id/ppd2022/assets/js/admin/
https://peppd.bappenas.go.id/ppd2022/assets/js/admin/login/
https://peppd.bappenas.go.id/ppd2022/assets/js/admin/login/login.js
https://peppd.bappenas.go.id/ppd2022/assets/js/universal.js
https://peppd.bappenas.go.id/ppd2022/captcha/
https://peppd.bappenas.go.id/ppd2022/package/
https://peppd.bappenas.go.id/ppd2022/package/css/
https://peppd.bappenas.go.id/ppd2022/package/css/..images/
https://peppd.bappenas.go.id/ppd2022/package/css/PIE.htc
https://peppd.bappenas.go.id/ppd2022/package/css/animate.css
https://peppd.bappenas.go.id/ppd2022/package/css/bootstrap.min.css
https://peppd.bappenas.go.id/ppd2022/package/css/helper.css
https://peppd.bappenas.go.id/ppd2022/package/css/material-design-iconic-font.min.css
https://peppd.bappenas.go.id/ppd2022/package/css/style.css
https://peppd.bappenas.go.id/ppd2022/package/css/userdefined.css
https://peppd.bappenas.go.id/ppd2022/package/css/waves-effect.css
https://peppd.bappenas.go.id/ppd2022/package/fonts/
https://peppd.bappenas.go.id/ppd2022/package/images/
https://peppd.bappenas.go.id/ppd2022/package/images/small/
https://peppd.bappenas.go.id/ppd2022/package/js/
https://peppd.bappenas.go.id/ppd2022/package/js/bootstrap.min.js
https://peppd.bappenas.go.id/ppd2022/package/js/jquery.min.js
https://peppd.bappenas.go.id/ppd2022/package/js/jquery.nicescroll.js
https://peppd.bappenas.go.id/ppd2022/package/js/jquery.scrollTo.min.js
https://peppd.bappenas.go.id/ppd2022/package/js/modernizr.min.js
https://peppd.bappenas.go.id/ppd2022/package/js/waves.js
https://peppd.bappenas.go.id/ppd2022/package/js/wow.min.js
https://peppd.bappenas.go.id/ppd2022/package/plugins/
https://peppd.bappenas.go.id/ppd2022/package/plugins/fastclick/
https://peppd.bappenas.go.id/ppd2022/package/plugins/fastclick/fastclick.js
https://peppd.bappenas.go.id/ppd2022/package/plugins/font-awesome/
https://peppd.bappenas.go.id/ppd2022/package/plugins/font-awesome/css/
https://peppd.bappenas.go.id/ppd2022/package/plugins/font-awesome/css/font-awesome.min.css
https://peppd.bappenas.go.id/ppd2022/package/plugins/font-awesome/fonts/
https://peppd.bappenas.go.id/ppd2022/package/plugins/ionicon/
https://peppd.bappenas.go.id/ppd2022/package/plugins/ionicon/css/
https://peppd.bappenas.go.id/ppd2022/package/plugins/ionicon/css/ionicons.min.css
https://peppd.bappenas.go.id/ppd2022/package/plugins/ionicon/fonts/
https://peppd.bappenas.go.id/ppd2022/package/plugins/jquery-blockui/
https://peppd.bappenas.go.id/ppd2022/package/plugins/jquery-blockui/jquery.blockUI.js
https://peppd.bappenas.go.id/ppd2022/package/plugins/jquery-detectmobile/
https://peppd.bappenas.go.id/ppd2022/package/plugins/jquery-detectmobile/detect.js
https://peppd.bappenas.go.id/ppd2022/package/plugins/jquery-slimscroll/
https://peppd.bappenas.go.id/ppd2022/package/plugins/jquery-slimscroll/jquery.slimscroll.js
https://peppd.bappenas.go.id/ppd2022/package/plugins/jquery-validation-1.15.0/
https://peppd.bappenas.go.id/ppd2022/package/plugins/jquery-validation-1.15.0/dist/
https://peppd.bappenas.go.id/ppd2022/package/plugins/jquery-validation-1.15.0/dist/jquery.validate.min.js
https://peppd.bappenas.go.id/ppd2022/package/plugins/sweetalert/
https://peppd.bappenas.go.id/ppd2022/package/plugins/sweetalert/dist/
https://peppd.bappenas.go.id/ppd2022/package/plugins/sweetalert/dist/sweetalert2.all.min.js
https://peppd.bappenas.go.id/ppd2022/package/plugins/sweetalert/dist/sweetalert2.min.css
https://peppd.bappenas.go.id/ppd2022/package/plugins/sweetalert/dist/sweetalert2.min.js
https://peppd.bappenas.go.id/ppd2023/
https://peppd.bappenas.go.id/ppd2023/Welcome/
https://peppd.bappenas.go.id/ppd2023/Welcome/login_act
https://peppd.bappenas.go.id/ppd2023/Welcome/refresh_captcha
https://peppd.bappenas.go.id/ppd2023/assets/
https://peppd.bappenas.go.id/ppd2023/assets/images/
https://peppd.bappenas.go.id/ppd2023/assets/js/
https://peppd.bappenas.go.id/ppd2023/assets/js/admin/
https://peppd.bappenas.go.id/ppd2023/assets/js/admin/login/
https://peppd.bappenas.go.id/ppd2023/assets/js/admin/login/login.js
https://peppd.bappenas.go.id/ppd2023/assets/js/universal.js
https://peppd.bappenas.go.id/ppd2023/captcha/
https://peppd.bappenas.go.id/ppd2023/package/
https://peppd.bappenas.go.id/ppd2023/package/css/

https://peppd.bappenas.go.id/ppd2023/package/css/..images/
https://peppd.bappenas.go.id/ppd2023/package/css/PIE.htc
https://peppd.bappenas.go.id/ppd2023/package/css/animate.css
https://peppd.bappenas.go.id/ppd2023/package/css/bootstrap.min.css
https://peppd.bappenas.go.id/ppd2023/package/css/helper.css
https://peppd.bappenas.go.id/ppd2023/package/css/material-design-iconic-font.min.css
https://peppd.bappenas.go.id/ppd2023/package/css/style.css
https://peppd.bappenas.go.id/ppd2023/package/css/userdefined.css
https://peppd.bappenas.go.id/ppd2023/package/css/waves-effect.css
https://peppd.bappenas.go.id/ppd2023/package/fonts/
https://peppd.bappenas.go.id/ppd2023/package/images/
https://peppd.bappenas.go.id/ppd2023/package/images/small/
https://peppd.bappenas.go.id/ppd2023/package/js/
https://peppd.bappenas.go.id/ppd2023/package/js/bootstrap.min.js
https://peppd.bappenas.go.id/ppd2023/package/js/jquery.min.js
https://peppd.bappenas.go.id/ppd2023/package/js/jquery.nicescroll.js
https://peppd.bappenas.go.id/ppd2023/package/js/jquery.scrollTo.min.js
https://peppd.bappenas.go.id/ppd2023/package/js/modernizr.min.js
https://peppd.bappenas.go.id/ppd2023/package/js/waves.js
https://peppd.bappenas.go.id/ppd2023/package/js/wow.min.js
https://peppd.bappenas.go.id/ppd2023/package/plugins/
https://peppd.bappenas.go.id/ppd2023/package/plugins/fastclick/
https://peppd.bappenas.go.id/ppd2023/package/plugins/fastclick/fastclick.js
https://peppd.bappenas.go.id/ppd2023/package/plugins/font-awesome/
https://peppd.bappenas.go.id/ppd2023/package/plugins/font-awesome/css/
https://peppd.bappenas.go.id/ppd2023/package/plugins/font-awesome/css/font-awesome.min.css
https://peppd.bappenas.go.id/ppd2023/package/plugins/font-awesome/fonts/
https://peppd.bappenas.go.id/ppd2023/package/plugins/ionicon/
https://peppd.bappenas.go.id/ppd2023/package/plugins/ionicon/css/
https://peppd.bappenas.go.id/ppd2023/package/plugins/ionicon/css/ionicons.min.css
https://peppd.bappenas.go.id/ppd2023/package/plugins/ionicon/fonts/
https://peppd.bappenas.go.id/ppd2023/package/plugins/jquery-blockui/
https://peppd.bappenas.go.id/ppd2023/package/plugins/jquery-blockui/jquery.blockUI.js
https://peppd.bappenas.go.id/ppd2023/package/plugins/jquery-detectmobile/
https://peppd.bappenas.go.id/ppd2023/package/plugins/jquery-detectmobile/detect.js
https://peppd.bappenas.go.id/ppd2023/package/plugins/jquery-slimscroll/
https://peppd.bappenas.go.id/ppd2023/package/plugins/jquery-slimscroll/jquery.slimscroll.js
https://peppd.bappenas.go.id/ppd2023/package/plugins/jquery-validation-1.15.0/
https://peppd.bappenas.go.id/ppd2023/package/plugins/jquery-validation-1.15.0/dist/
https://peppd.bappenas.go.id/ppd2023/package/plugins/jquery-validation-1.15.0/dist/jquery.validate.min.js
https://peppd.bappenas.go.id/ppd2023/package/plugins/sweetalert/
https://peppd.bappenas.go.id/ppd2023/package/plugins/sweetalert/dist/
https://peppd.bappenas.go.id/ppd2023/package/plugins/sweetalert/dist/sweetalert2.all.min.js
https://peppd.bappenas.go.id/ppd2023/package/plugins/sweetalert/dist/sweetalert2.min.css
https://peppd.bappenas.go.id/ppd2023/package/plugins/sweetalert/dist/sweetalert2.min.js
https://peppd.bappenas.go.id/ppd2024/
https://peppd.bappenas.go.id/ppd2024/Welcome/
https://peppd.bappenas.go.id/ppd2024/Welcome/login_act
https://peppd.bappenas.go.id/ppd2024/Welcome/refresh_captcha
https://peppd.bappenas.go.id/ppd2024/assets/
https://peppd.bappenas.go.id/ppd2024/assets/images/
https://peppd.bappenas.go.id/ppd2024/assets/js/
https://peppd.bappenas.go.id/ppd2024/assets/js/admin/
https://peppd.bappenas.go.id/ppd2024/assets/js/admin/login/
https://peppd.bappenas.go.id/ppd2024/assets/js/admin/login/login.js
https://peppd.bappenas.go.id/ppd2024/assets/js/universal.js
https://peppd.bappenas.go.id/ppd2024/captcha/
https://peppd.bappenas.go.id/ppd2024/package/
https://peppd.bappenas.go.id/ppd2024/package/css/
https://peppd.bappenas.go.id/ppd2024/package/css/..images/
https://peppd.bappenas.go.id/ppd2024/package/css/PIE.htc
https://peppd.bappenas.go.id/ppd2024/package/css/animate.css
https://peppd.bappenas.go.id/ppd2024/package/css/bootstrap.min.css
https://peppd.bappenas.go.id/ppd2024/package/css/helper.css
https://peppd.bappenas.go.id/ppd2024/package/css/material-design-iconic-font.min.css
https://peppd.bappenas.go.id/ppd2024/package/css/style.css
https://peppd.bappenas.go.id/ppd2024/package/css/userdefined.css

https://peppd.bappenas.go.id/ppd2024/package/css/waves-effect.css
https://peppd.bappenas.go.id/ppd2024/package/fonts/
https://peppd.bappenas.go.id/ppd2024/package/images/
https://peppd.bappenas.go.id/ppd2024/package/images/small/
https://peppd.bappenas.go.id/ppd2024/package/js/
https://peppd.bappenas.go.id/ppd2024/package/js/bootstrap.min.js
https://peppd.bappenas.go.id/ppd2024/package/js/jquery.min.js
https://peppd.bappenas.go.id/ppd2024/package/js/jquery.nicescroll.js
https://peppd.bappenas.go.id/ppd2024/package/js/jquery.scrollTo.min.js
https://peppd.bappenas.go.id/ppd2024/package/js/modernizr.min.js
https://peppd.bappenas.go.id/ppd2024/package/js/waves.js
https://peppd.bappenas.go.id/ppd2024/package/js/wow.min.js
https://peppd.bappenas.go.id/ppd2024/package/plugins/
https://peppd.bappenas.go.id/ppd2024/package/plugins/fastclick/
https://peppd.bappenas.go.id/ppd2024/package/plugins/fastclick/fastclick.js
https://peppd.bappenas.go.id/ppd2024/package/plugins/font-awesome/
https://peppd.bappenas.go.id/ppd2024/package/plugins/font-awesome/css/
https://peppd.bappenas.go.id/ppd2024/package/plugins/font-awesome/css/font-awesome.min.css
https://peppd.bappenas.go.id/ppd2024/package/plugins/font-awesome/fonts/
https://peppd.bappenas.go.id/ppd2024/package/plugins/ionicon/
https://peppd.bappenas.go.id/ppd2024/package/plugins/ionicon/css/
https://peppd.bappenas.go.id/ppd2024/package/plugins/ionicon/css/ionicons.min.css
https://peppd.bappenas.go.id/ppd2024/package/plugins/ionicon/fonts/
https://peppd.bappenas.go.id/ppd2024/package/plugins/jquery-blockui/
https://peppd.bappenas.go.id/ppd2024/package/plugins/jquery-blockui/jquery.blockUI.js
https://peppd.bappenas.go.id/ppd2024/package/plugins/jquery-detectmobile/
https://peppd.bappenas.go.id/ppd2024/package/plugins/jquery-detectmobile/detect.js
https://peppd.bappenas.go.id/ppd2024/package/plugins/jquery-slimscroll/
https://peppd.bappenas.go.id/ppd2024/package/plugins/jquery-slimscroll/jquery.slimscroll.js
https://peppd.bappenas.go.id/ppd2024/package/plugins/jquery-validation-1.15.0/
https://peppd.bappenas.go.id/ppd2024/package/plugins/jquery-validation-1.15.0/dist/
https://peppd.bappenas.go.id/ppd2024/package/plugins/jquery-validation-1.15.0/dist/jquery.validate.min.js
https://peppd.bappenas.go.id/ppd2024/package/plugins/sweetalert/
https://peppd.bappenas.go.id/ppd2024/package/plugins/sweetalert/dist/
https://peppd.bappenas.go.id/ppd2024/package/plugins/sweetalert/dist/sweetalert2.all.min.js
https://peppd.bappenas.go.id/ppd2024/package/plugins/sweetalert/dist/sweetalert2.min.css
https://peppd.bappenas.go.id/ppd2024/package/plugins/sweetalert/dist/sweetalert2.min.js
https://peppd.bappenas.go.id/propel.ini
https://peppd.bappenas.go.id/user_guide/
https://peppd.bappenas.go.id/users.db
https://peppd.bappenas.go.id/users.ini
https://peppd.bappenas.go.id/web.config.bak
https://peppd.bappenas.go.id/welcome