Acunetix
by Invicti

# Developer Report

Acunetix Security Audit

2024-07-01

Generated by Acunetix

# Scan of developer3.penang.gov.my

## Scan details

| Scan information | |
|---|---|
| Start time | 2024-07-01T12:54:11.337144+08:00 |
| Start url | https://developer3.penang.gov.my/app_pintas/ |
| Host | developer3.penang.gov.my |
| Scan time | 2 minutes, 48 seconds |
| Profile | Full Scan |
| Server information | Apache/2.4.41 (Ubuntu) |
| Responsive | True |
| Server OS | Unix |
| Server technologies | PHP |
| Application build | 24.6.240626115 |

### Threat level

#### Acunetix Threat Level 4

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

### Alerts distribution

| Total alerts found | 41 |
|---|---|
| Critical | 3 |
| High | 6 |
| Medium | 13 |
| Low | 4 |
| Informational | 15 |

## Alerts summary

### Handlebars CVE-2021-23369 Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br>Base Score: 8.7<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: Low<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: High<br>Integrity Impact to the Vulnerable System: High<br>Availability Impact to the Vulnerable System: High<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>Availability Impact to the Subsequent System: None |
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H<br>Base Score: 9.8<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: High<br>Integrity Impact: High<br>Availability Impact: High |
| CVE | CVE-2021-23369 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Handlebars Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br>Base Score: 8.7<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: Low<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: High<br>Integrity Impact to the Vulnerable System: High<br>Availability Impact to the Vulnerable System: High<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>Availability Impact to the Subsequent System: None |

| | |
|---|---|
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H<br>Base Score: 9.8<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: High<br>Integrity Impact: High<br>Availability Impact: High |
| CWE | CWE-138 |
| CVE | CVE-2019-19919 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Handlebars Other Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br>Base Score: 8.7<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: Low<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: High<br>Integrity Impact to the Vulnerable System: High<br>Availability Impact to the Vulnerable System: High<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>Availability Impact to the Subsequent System: None |
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H<br>Base Score: 9.8<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: High<br>Integrity Impact: High<br>Availability Impact: High |
| CVE | CVE-2021-23383 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Chart.js Improper Input Validation Vulnerability

| Classification |
|---|

| | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L<br>Base Score: 8.7<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: High<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>Availability Impact to the Subsequent System: Low |
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H<br>Base Score: 7.5<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: High |
| CWE | CWE-20 |
| CVE | CVE-2020-7746 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Handlebars Improper Control of Generation of Code ('Code Injection') Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N<br>Base Score: 8.3<br>Attack Vector: Network<br>Attack Complexity: High<br>Privileges Required: None<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: High<br>Integrity Impact to the Vulnerable System: Low<br>Availability Impact to the Vulnerable System: Low<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>Availability Impact to the Subsequent System: None |
| CVSS3 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:L<br>Base Score: 8.1<br>Attack Vector: Network<br>Attack Complexity: High<br>Privileges Required: None<br>User Interaction: None<br>Scope: Changed<br>Confidentiality Impact: High<br>Integrity Impact: Low<br>Availability Impact: Low |
| CWE | CWE-94 |
| CVE | CVE-2019-20920 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Handlebars Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L<br>Base Score: 8.7<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: High<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>Availability Impact to the Subsequent System: Low |
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H<br>Base Score: 7.5<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: High |
| CWE | CWE-835 |
| CVE | CVE-2019-20922 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### jQuery Validation Other Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L<br>Base Score: 8.7<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: High<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>Availability Impact to the Subsequent System: Low |

| | |
|---|---|
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H<br>Base Score: 7.5<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: High |
| CVE | CVE-2022-31147 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### jQuery Validation Other Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L<br>Base Score: 8.7<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: High<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>Availability Impact to the Subsequent System: Low |
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H<br>Base Score: 7.5<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: High |
| CVE | CVE-2021-43306 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### jQuery Validation Uncontrolled Resource Consumption Vulnerability

| Classification |
|---|

| | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L<br>Base Score: 8.7<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: High<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>Availability Impact to the Subsequent System: Low |
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H<br>Base Score: 7.5<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: High |
| CWE | CWE-400 |
| CVE | CVE-2021-21252 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N<br>Base Score: 5.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: Low<br>Integrity Impact to the Subsequent System: Low<br>Availability Impact to the Subsequent System: None |
| CVSS3 | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>Base Score: 6.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CWE | CWE-707 |
| CVE | CVE-2018-14040 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N<br>Base Score: 5.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: Low<br>Integrity Impact to the Subsequent System: Low<br>Availability Impact to the Subsequent System: None |
| CVSS3 | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>Base Score: 6.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CWE | CWE-707 |
| CVE | CVE-2018-14042 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N<br>Base Score: 5.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: Low<br>Integrity Impact to the Subsequent System: Low<br>Availability Impact to the Subsequent System: None |

| | |
|---|---|
| CVSS3 | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>Base Score: 6.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CWE | CWE-707 |
| CVE | CVE-2018-14041 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Development configuration files

| 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<br>Base Score: 2.1<br>Attack Vector: Network<br>Attack Complexity: High<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: Low<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>Availability Impact to the Subsequent System: None |
| CVSS3 | CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N<br>Base Score: 3.1<br>Attack Vector: Network<br>Attack Complexity: High<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Unchanged<br>Confidentiality Impact: Low<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 5.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |

| CWE | CWE-538 | |
|---|---|---|
| Affected items | | Variation |
| Web Server | | 1 |

### HTTP Strict Transport Security (HSTS) Policy Not Enabled

| 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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-16 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| Classification |
|---|

| | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N<br>Base Score: 5.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: Low<br>Integrity Impact to the Subsequent System: Low<br>Availability Impact to the Subsequent System: None |
| CVSS3 | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>Base Score: 6.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CWE | CWE-707 |
| CVE | CVE-2015-9251 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N<br>Base Score: 5.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: Low<br>Integrity Impact to the Subsequent System: Low<br>Availability Impact to the Subsequent System: None |
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>Base Score: 6.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CWE | CWE-707 |
| CVE | CVE-2020-11023 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N<br>Base Score: 5.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: Low<br>Integrity Impact to the Subsequent System: Low<br>Availability Impact to the Subsequent System: None |
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>Base Score: 6.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CWE | CWE-707 |
| CVE | CVE-2020-23064 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N<br>Base Score: 5.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: Low<br>Integrity Impact to the Subsequent System: Low<br>Availability Impact to the Subsequent System: None |

| | |
|---|---|
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>Base Score: 6.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CWE | CWE-707 |
| CVE | CVE-2020-11022 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### JQuery Prototype Pollution Vulnerability

| Classification | |
|---|---|
| CVSS4 | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N<br>Base Score: 5.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: Low<br>Integrity Impact to the Subsequent System: Low<br>Availability Impact to the Subsequent System: None |
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N<br>Base Score: 6.1<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CVE | CVE-2019-11358 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### 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<br>Base Score: 6.9<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: Low<br>Integrity Impact to the Vulnerable System: Low<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 6.5<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CVSS2 | Base Score: 6.4<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: Partial<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-937 |

| Affected items | Variation |
|---|---|
| Web Server | 3 |

## 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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>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<br>Base Score: 2.1<br>Attack Vector: Network<br>Attack Complexity: High<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: Low<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 3.1<br>Attack Vector: Network<br>Attack Complexity: High<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Unchanged<br>Confidentiality Impact: Low<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 2.6<br>Access Vector: Network_accessible<br>Access Complexity: High<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-284 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Missing Content-Type Header

| 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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-16 |

| 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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-1021 |

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### Error page web server version 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<br>Base Score: 6.9<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: Low<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 5.3<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: Low<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 5.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-200 |

| 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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-200 |

| 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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: High<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: High<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: High<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-937 |

| Affected items | Variation |
|---|---|
| Web Server | 9 |

### 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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Active<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: None<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>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<br>Base Score: 6.9<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Confidentiality Impact to the Vulnerable System: None<br>Integrity Impact to the Vulnerable System: Low<br>Availability Impact to the Vulnerable System: None<br>Confidentiality Impact to the Subsequent System: None<br>Integrity Impact to the Subsequent System: None<br>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<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Changed<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-830 |

| Affected items | Variation |
|---|---|
| /app_pintas/fr_faq.php | 1 |
| /app_pintas/login.php | 1 |

## Alerts details

### Handlebars CVE-2021-23369 Vulnerability

| | |
|---|---|
| Severity | **Critical** |
| Reported by module | /deepscan/javascript_library_audit_deepscan.js |

#### Description

The package handlebars before 4.7.7 are vulnerable to Remote Code Execution (RCE) when selecting certain compiling options to compile templates coming from an untrusted source.

#### Impact

#### Recommendation

#### References

CVE-2021-23369 (https://nvd.nist.gov/vuln/detail/CVE-2021-23369)
CVE-2021-23369 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23369)

#### Affected items

| Web Server |
|---|
| Details |
| handlebars.js v4.0.10-4.0.10 |
| Request headers |

### Handlebars Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') Vulnerability

| | |
|---|---|
| Severity | **Critical** |
| Reported by module | /deepscan/javascript_library_audit_deepscan.js |

#### Description

Versions of handlebars prior to 4.3.0 are vulnerable to Prototype Pollution leading to Remote Code Execution. Templates may alter an Object's __proto__ and __defineGetter__ properties, which may allow an attacker to execute arbitrary code through crafted payloads.

#### Impact

#### Recommendation

#### References

CVE-2019-19919 (https://nvd.nist.gov/vuln/detail/CVE-2019-19919)
CVE-2019-19919 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19919)

#### Affected items

| Web Server |
|---|

| Details |
| --- |
| handlebars.js v4.0.10-4.0.10 |
| Request headers |

## Handlebars Other Vulnerability

| Severity | **Critical** |
| --- | --- |
| Reported by module | /deepscan/javascript_library_audit_deepscan.js |

### Description

The package handlebars before 4.7.7 are vulnerable to Prototype Pollution when selecting certain compiling options to compile templates coming from an untrusted source.

### Impact

### Recommendation

### References

CVE-2021-23383 (https://nvd.nist.gov/vuln/detail/CVE-2021-23383)
CVE-2021-23383 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23383)

### Affected items

| **Web Server** |
| --- |
| Details |
| handlebars.js v4.0.10-4.0.10 |
| Request headers |

## Chart.js Improper Input Validation Vulnerability

| Severity | **High** |
| --- | --- |
| Reported by module | /Scripts/PerFile/Javascript_Libraries_Audit.script |

### Description

This affects the package chart.js before 2.9.4. The options parameter is not properly sanitized when it is processed. When the options are processed, the existing options (or the defaults options) are deeply merged with provided options. However, during this operation, the keys of the object being set are not checked, leading to a prototype pollution.

### Impact

### Recommendation

### References

CVE-2020-7746 (https://nvd.nist.gov/vuln/detail/CVE-2020-7746)
CVE-2020-7746 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7746)

### Affected items

| Web Server |
| --- |
| Details |
| chart.js v2.7.1-2.7.1 |
| Request headers |

## Handlebars Improper Control of Generation of Code ('Code Injection') Vulnerability

| | |
| --- | --- |
| Severity | **High** |
| Reported by module | /deepscan/javascript_library_audit_deepscan.js |

### Description

Handlebars before 3.0.8 and 4.x before 4.5.3 is vulnerable to Arbitrary Code Execution. The lookup helper fails to properly validate templates, allowing attackers to submit templates that execute arbitrary JavaScript. This can be used to run arbitrary code on a server processing Handlebars templates or in a victim's browser (effectively serving as XSS).

### Impact

### Recommendation

### References

CVE-2019-20920 (https://nvd.nist.gov/vuln/detail/CVE-2019-20920)
CVE-2019-20920 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20920)

### Affected items

| Web Server |
| --- |
| Details |
| handlebars.js v4.0.10-4.0.10 |
| Request headers |

## Handlebars Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability

| | |
| --- | --- |
| Severity | **High** |
| Reported by module | /deepscan/javascript_library_audit_deepscan.js |

### Description

Handlebars before 4.4.5 allows Regular Expression Denial of Service (ReDoS) because of eager matching. The parser may be forced into an endless loop while processing crafted templates. This may allow attackers to exhaust system resources.

### Impact

### Recommendation

### References

CVE-2019-20922 (https://nvd.nist.gov/vuln/detail/CVE-2019-20922)
CVE-2019-20922 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20922)

### Affected items

| Web Server |
| --- |
| Details |
| handlebars.js v4.0.10-4.0.10 |
| Request headers |

## jQuery Validation Other Vulnerability

| | |
| --- | --- |
| Severity | **High** |
| Reported by module | /Scripts/PerFile/Javascript_Libraries_Audit.script |

### Description

The jQuery Validation Plugin (jquery-validation) provides drop-in validation for forms. Versions of jquery-validation prior to 1.19.5 are vulnerable to regular expression denial of service (ReDoS) when an attacker is able to supply arbitrary input to the url2 method. This is due to an incomplete fix for CVE-2021-43306. Users should upgrade to version 1.19.5 to receive a patch.

### Impact

### Recommendation

### References

CVE-2022-31147 (https://nvd.nist.gov/vuln/detail/CVE-2022-31147)
CVE-2022-31147 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31147)

### Affected items

| Web Server |
| --- |
| Details |
| jquery validation v1.17.0-1.17.0 |
| Request headers |

## jQuery Validation Other Vulnerability

| | |
| --- | --- |
| Severity | **High** |
| Reported by module | /Scripts/PerFile/Javascript_Libraries_Audit.script |

### Description

An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the jquery-validation npm package, when an attacker is able to supply arbitrary input to the url2 method

### Impact

### Recommendation

### References

CVE-2021-43306 (https://nvd.nist.gov/vuln/detail/CVE-2021-43306)
CVE-2021-43306 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43306)

### Affected items

| Web Server |
| --- |
| Details |
| jquery validation v1.17.0-1.17.0 |
| Request headers |

## jQuery Validation Uncontrolled Resource Consumption Vulnerability

| | |
| --- | --- |
| Severity | **High** |
| Reported by module | /Scripts/PerFile/Javascript_Libraries_Audit.script |

### Description

The jQuery Validation Plugin provides drop-in validation for your existing forms. It is published as an npm package "jquery-validation". jquery-validation before version 1.19.3 contains one or more regular expressions that are vulnerable to ReDoS (Regular Expression Denial of Service). This is fixed in 1.19.3.

### Impact

### Recommendation

### References

CVE-2021-21252 (https://nvd.nist.gov/vuln/detail/CVE-2021-21252)
CVE-2021-21252 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21252)

### Affected items

| Web Server |
| --- |
| Details |
| jquery validation v1.17.0-1.17.0 |
| Request headers |

## Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| | |
| --- | --- |
| Severity | **Medium** |
| Reported by module | /Scripts/PerFile/Javascript_Libraries_Audit.script |

### Description

In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.

### Impact

### Recommendation

### References

CVE-2018-14040 (https://nvd.nist.gov/vuln/detail/CVE-2018-14040)
CVE-2018-14040 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14040)

### Affected items

| Web Server |
|---|
| Details |
| bootstrap.js v4.0.0-4.0.0 |
| Request headers |

## Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| | |
|---|---|
| Severity | **Medium** |
| Reported by module | /Scripts/PerFile/Javascript_Libraries_Audit.script |

### Description

In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.

### Impact

### Recommendation

### References

CVE-2018-14042 (https://nvd.nist.gov/vuln/detail/CVE-2018-14042)
CVE-2018-14042 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14042)

### Affected items

| Web Server |
|---|
| Details |
| bootstrap.js v4.0.0-4.0.0 |
| Request headers |

## Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| | |
|---|---|
| Severity | **Medium** |
| Reported by module | /Scripts/PerFile/Javascript_Libraries_Audit.script |

### Description

In Bootstrap before 4.1.2, XSS is possible in the data-target property of scrollspy.

### Impact

### Recommendation

### References

CVE-2018-14041 (https://nvd.nist.gov/vuln/detail/CVE-2018-14041)
CVE-2018-14041 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14041)

### Affected items

| Web Server |
| --- |
| Details |
| bootstrap.js v4.0.0-4.0.0 |
| Request headers |

## Development configuration files

| | |
| --- | --- |
| Severity | **Medium** |
| Reported by module | /Scripts/PerFolder/Development_Files.script |

### Description

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

### Impact

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

### Recommendation

Remove or restrict access to all configuration files acessible from internet.

### Affected items

| Web Server |
| --- |
| Details |
| Development configuration files:<br>• https://developer3.penang.gov.my/app_pintas/**.gitignore**<br>`.gitignore => Git configuration file. Git is a free and open source distributed versi` |
| Request headers |

```
GET /app_pintas/.gitignore HTTP/1.1

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

## HTTP Strict Transport Security (HSTS) Policy Not Enabled

| | |
|---|---|
| Severity | **Medium** |
| Reported by module | /httpdata/HSTS_not_implemented.js |

### Description

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

### Impact

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

### Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

### References

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

### Affected items

| **Web Server** |
|---|
| Details |
| URLs where HSTS is not enabled:<br>• https://developer3.penang.gov.my/app_pintas/login.php<br>• https://developer3.penang.gov.my/app_pintas/fr_faq.php<br>• https://developer3.penang.gov.my/app_pintas/fr_penafian.php<br>• https://developer3.penang.gov.my/app_pintas/fr_terma.php<br>• https://developer3.penang.gov.my/app_pintas/login-ajax.php<br>• https://developer3.penang.gov.my/app_pintas/popup.php<br>• https://developer3.penang.gov.my/app_pintas/register.php |

| Request headers |
| --- |

```
GET /app_pintas/login.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

## jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| Severity | **Medium** |
| --- | --- |
| Reported by module | /Scripts/PerFile/Javascript_Libraries_Audit.script |

### Description

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

### Impact

### Recommendation

### References

CVE-2015-9251 (https://nvd.nist.gov/vuln/detail/CVE-2015-9251)
CVE-2015-9251 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9251)

### Affected items

| **Web Server** |
| --- |
| Details |
| jquery v1.11.2-1.11.2 |
| Request headers |

## jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| Severity | **Medium** |
| --- | --- |
| Reported by module | /deepscan/javascript_library_audit_deepscan.js |

### Description

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

### Impact

### Recommendation

### References

CVE-2020-11023 (https://nvd.nist.gov/vuln/detail/CVE-2020-11023)
CVE-2020-11023 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11023)

### Affected items

| Web Server |
|---|
| Details |
| jquery v3.2.1-3.2.1 |
| Request headers |

## jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| | |
|---|---|
| Severity | **Medium** |
| Reported by module | /deepscan/javascript_library_audit_deepscan.js |

### Description

Cross Site Scripting vulnerability in jQuery 2.2.0 through 3.x before 3.5.0 allows a remote attacker to execute arbitrary code via the <options> element.

### Impact

### Recommendation

### References

CVE-2020-23064 (https://nvd.nist.gov/vuln/detail/CVE-2020-23064)
CVE-2020-23064 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-23064)

### Affected items

| Web Server |
|---|
| Details |
| jquery v3.2.1-3.2.1 |
| Request headers |

## jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

| | |
|---|---|
| Severity | **Medium** |
| Reported by module | /deepscan/javascript_library_audit_deepscan.js |

### 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.

### Impact

### Recommendation

### References

CVE-2020-11022 (https://nvd.nist.gov/vuln/detail/CVE-2020-11022)
CVE-2020-11022 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022)

### Affected items

| Web Server |
|---|
| Details |
| jquery v3.2.1-3.2.1 |
| Request headers |

## JQuery Prototype Pollution Vulnerability

| | |
|---|---|
| Severity | **Medium** |
| Reported by module | /deepscan/javascript_library_audit_deepscan.js |

### Description

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

### Impact

### Recommendation

### References

CVE-2019-11358 (https://nvd.nist.gov/vuln/detail/CVE-2019-11358)
CVE-2019-11358 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11358)

### Affected items

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

| jquery v3.2.1-3.2.1 |
| --- |
| Request headers |

## Vulnerable JavaScript libraries

| Severity | **Medium** |
| --- | --- |
| Reported by module | /deepscan/javascript_library_audit_deepscan.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 3.2.1**
  - URL: https://developer3.penang.gov.my/app_pintas/login.php
  - 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 /app_pintas/login.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

**Web Server**

Details

- **handlebars.js 4.0.10**
  - URL: https://developer3.penang.gov.my/app_pintas/login.php
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: N/A
  - Description: Unsafe direct call of helperMissing and blockHelperMissing / Prototype pollution
  - References:
    - https://github.com/wycats/handlebars.js/blob/master/release-notes.md#v430---september-24th-2019
    - https://github.com/wycats/handlebars.js/blob/master/release-notes.md#v453---november-18th-2019

Request headers

```
GET /app_pintas/login.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

**Web Server**

Verified vulnerability

Details

- **jQuery 1.11.2**
  - URL: https://developer3.penang.gov.my/app_pintas/assets/wowslider/jquery.js
  - Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
  - 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 /app_pintas/assets/wowslider/jquery.js HTTP/1.1

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

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:<br>• https://developer3.penang.gov.my/app_pintas/<br><br>`Set-Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd; path=/` |
| Request headers |
| `GET /app_pintas/ HTTP/1.1`<br><br>`Referer: https://developer3.penang.gov.my/app_pintas/`<br><br>`Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8`<br><br>`Accept-Encoding: gzip,deflate,br`<br><br>`User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36`<br><br>`Host: developer3.penang.gov.my`<br><br>`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:<br>• https://developer3.penang.gov.my/app_pintas/<br><br>`Set-Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd; path=/` |
| Request headers |
| `GET /app_pintas/ HTTP/1.1`<br><br>`Referer: https://developer3.penang.gov.my/app_pintas/`<br><br>`Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8`<br><br>`Accept-Encoding: gzip,deflate,br`<br><br>`User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36`<br><br>`Host: developer3.penang.gov.my`<br><br>`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://developer3.penang.gov.my/app_pintas/

  Cookie was set with:

```
Set-Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd; path=/
```

  This cookie has the following issues:

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

Request headers

```
GET /app_pintas/ HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

## Missing Content-Type Header

| | |
| --- | --- |
| Severity | **Low** |
| Reported by module | /RPA/Content_Type_Missing.js |

### Description

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

### Impact

None

### Recommendation

Set a Content-Type header value for these page(s).

### Affected items

| Web Server |
| --- |
| Verified vulnerability |
| Details |
| Pages where the content-type header is not specified:<br>• https://developer3.penang.gov.my/app_pintas/.gitignore |
| Request headers |

```
GET /app_pintas/.gitignore HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

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://developer3.penang.gov.my/app_pintas/login.php
- https://developer3.penang.gov.my/app_pintas/fr_faq.php
- https://developer3.penang.gov.my/app_pintas/fr_penafian.php
- https://developer3.penang.gov.my/app_pintas/fr_terma.php
- https://developer3.penang.gov.my/app_pintas/popup.php
- https://developer3.penang.gov.my/app_pintas/register.php

Request headers

```
GET /app_pintas/login.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

## Error page web server version disclosure

| | |
|---|---|
| Severity | **Informational** |
| Reported by module | /Scripts/PerServer/Error_Page_Path_Disclosure.script |

### Description

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

### Impact

Error messages information about an application's internal workings may be used to escalate attacks.

### Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

### References

Custom Error Responses (Apache HTTP Server) (https://httpd.apache.org/docs/current/custom-error.html)
server_tokens (Nginx) (http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens)
Remove Unwanted HTTP Response Headers (Microsoft IIS) (https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/)

### Affected items

| Web Server |
|---|
| Details |
| Request headers |

```
GET /dR2d26QVh8 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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

## Generic Email Address Disclosure

| | |
|---|---|
| Severity | **Informational** |
| Reported by module | /httpdata/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:<br>• https://developer3.penang.gov.my/app_pintas/login.php<br>**epintas@penang.gov.my** |
| Request headers |

```
GET /app_pintas/login.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

## Outdated JavaScript libraries

| | |
| --- | --- |
| Severity | **Informational** |
| Reported by module | /deepscan/javascript_library_audit_deepscan.js |

### Description

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

### Impact

Consult References for more information.

### Recommendation

Upgrade to the latest version.

### Affected items

**Web Server**

Details

- **Ion.RangeSlider 2.2.0**
  - URL: https://developer3.penang.gov.my/app_pintas/login.php
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/IonDen/ion.rangeSlider/tags

Request headers

```
GET /app_pintas/login.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

**Web Server**

Details

- **jsTree 3.3.4**
  - URL: https://developer3.penang.gov.my/app_pintas/login.php
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/vakata/jstree/tags

Request headers

```
GET /app_pintas/login.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

**Web Server**

Details

- **SweetAlert2 7.1.0**
  - URL: https://developer3.penang.gov.my/app_pintas/login.php
  - 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 /app_pintas/login.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

**Web Server**

Details

- **bootstrap.js 4.0.0**
  - URL: https://developer3.penang.gov.my/app_pintas/assets/vendors/base/vendors.bundle.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 /app_pintas/assets/vendors/base/vendors.bundle.js HTTP/1.1

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

**Web Server**

Details

- **jQuery Validation 1.17.0**
  - URL: https://developer3.penang.gov.my/app_pintas/assets/vendors/base/vendors.bundle.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 /app_pintas/assets/vendors/base/vendors.bundle.js HTTP/1.1

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

**Web Server**

Details

- **Select2 4.0.6-rc.1**
  - URL: https://developer3.penang.gov.my/app_pintas/assets/vendors/base/vendors.bundle.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 /app_pintas/assets/vendors/base/vendors.bundle.js HTTP/1.1

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

**Web Server**

Details

- **JavaScript Cookie 2.2.0**
  - URL: https://developer3.penang.gov.my/app_pintas/assets/vendors/base/vendors.bundle.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/js-cookie/js-cookie/releases

Request headers


```
GET /app_pintas/assets/vendors/base/vendors.bundle.js HTTP/1.1

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```


**Web Server**

Details

- **Chart.js 2.7.1**
  - URL: https://developer3.penang.gov.my/app_pintas/assets/vendors/base/vendors.bundle.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/chartjs/Chart.js/releases

Request headers

```
GET /app_pintas/assets/vendors/base/vendors.bundle.js HTTP/1.1

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

**Web Server**

Details

- **clipboard.js 1.7.1**
  - URL: https://developer3.penang.gov.my/app_pintas/assets/vendors/base/vendors.bundle.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/zenorocha/clipboard.js/releases

Request headers


```
GET /app_pintas/assets/vendors/base/vendors.bundle.js HTTP/1.1

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

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://developer3.penang.gov.my/app_pintas/login.php
- https://developer3.penang.gov.my/app_pintas/assets/app/media/img/bg/
- https://developer3.penang.gov.my/app_pintas/image/slide/
- https://developer3.penang.gov.my/app_pintas/fr_faq.php
- https://developer3.penang.gov.my/app_pintas/fr_penafian.php
- https://developer3.penang.gov.my/app_pintas/fr_terma.php
- https://developer3.penang.gov.my/app_pintas/login-ajax.php
- https://developer3.penang.gov.my/app_pintas/popup.php
- https://developer3.penang.gov.my/app_pintas/manual/
- https://developer3.penang.gov.my/app_pintas/register.php
- https://developer3.penang.gov.my/app_pintas/rest/
- https://developer3.penang.gov.my/app_pintas/image/slide/apps/
- https://developer3.penang.gov.my/app_pintas/tcpdf/
- https://developer3.penang.gov.my/app_pintas/includes/
- https://developer3.penang.gov.my/app_pintas/image/popup/
- https://developer3.penang.gov.my/app_pintas/image/
- https://developer3.penang.gov.my/app_pintas/assets/demo/default/custom/components/forms/widgets/
- https://developer3.penang.gov.my/app_pintas/assets/app/media/img/error/
- https://developer3.penang.gov.my/app_pintas/assets/vendors/base/fonts/flaticon/
- https://developer3.penang.gov.my/app_pintas/assets/global/
- https://developer3.penang.gov.my/app_pintas/assets/

Request headers

```
GET /app_pintas/login.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

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

| /app_pintas/fr_faq.php |
|---|
| Details |
| Pages where SRI is not implemented:<br>• https://developer3.penang.gov.my/app_pintas/fr_faq.php<br>Script SRC: **https://www.google.com/recaptcha/api.js?onload=CaptchaCallback&render=explicit** |
| Request headers |

```
GET /app_pintas/fr_faq.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/login.php

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

**/app_pintas/login.php**

Details

Pages where SRI is not implemented:

- https://developer3.penang.gov.my/app_pintas/login.php
  Script SRC: **https://ajax.googleapis.com/ajax/libs/webfont/1.6.16/webfont.js**

Request headers

```
GET /app_pintas/login.php HTTP/1.1

Referer: https://developer3.penang.gov.my/app_pintas/

Cookie: PHPSESSID=24dhoedc8hrlbtjpqdo3u77qnd

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/125.0.0.0 Safari/537.36

Host: developer3.penang.gov.my

Connection: Keep-alive
```

## Scanned items (coverage report)

https://developer3.penang.gov.my/
https://developer3.penang.gov.my/app_pintas/
https://developer3.penang.gov.my/app_pintas/.gitignore
https://developer3.penang.gov.my/app_pintas/assets/
https://developer3.penang.gov.my/app_pintas/assets/app/
https://developer3.penang.gov.my/app_pintas/assets/app/js/
https://developer3.penang.gov.my/app_pintas/assets/app/js/dashboard.js
https://developer3.penang.gov.my/app_pintas/assets/app/media/
https://developer3.penang.gov.my/app_pintas/assets/app/media/img/
https://developer3.penang.gov.my/app_pintas/assets/app/media/img/bg/
https://developer3.penang.gov.my/app_pintas/assets/app/media/img/error/
https://developer3.penang.gov.my/app_pintas/assets/app/media/img/files/
https://developer3.penang.gov.my/app_pintas/assets/app/media/img/icons/
https://developer3.penang.gov.my/app_pintas/assets/app/media/img/misc/
https://developer3.penang.gov.my/app_pintas/assets/app/media/img/users/
https://developer3.penang.gov.my/app_pintas/assets/demo/
https://developer3.penang.gov.my/app_pintas/assets/demo/default/
https://developer3.penang.gov.my/app_pintas/assets/demo/default/base/
https://developer3.penang.gov.my/app_pintas/assets/demo/default/base/scripts.bundle.js
https://developer3.penang.gov.my/app_pintas/assets/demo/default/base/style.bundle.css
https://developer3.penang.gov.my/app_pintas/assets/demo/default/custom/
https://developer3.penang.gov.my/app_pintas/assets/demo/default/custom/components/
https://developer3.penang.gov.my/app_pintas/assets/demo/default/custom/components/base/
https://developer3.penang.gov.my/app_pintas/assets/demo/default/custom/components/base/treeview.js
https://developer3.penang.gov.my/app_pintas/assets/demo/default/custom/components/forms/
https://developer3.penang.gov.my/app_pintas/assets/demo/default/custom/components/forms/widgets/
https://developer3.penang.gov.my/app_pintas/assets/demo/default/custom/components/forms/widgets/select2.js
https://developer3.penang.gov.my/app_pintas/assets/demo/default/media/
https://developer3.penang.gov.my/app_pintas/assets/demo/demo11/
https://developer3.penang.gov.my/app_pintas/assets/demo/demo11/base/
https://developer3.penang.gov.my/app_pintas/assets/demo/demo11/base/style.bundle.css
https://developer3.penang.gov.my/app_pintas/assets/demo/demo11/base/style.bundle.rtl.css
https://developer3.penang.gov.my/app_pintas/assets/demo/demo6/
https://developer3.penang.gov.my/app_pintas/assets/demo/demo6/base/
https://developer3.penang.gov.my/app_pintas/assets/demo/demo6/base/scripts.bundle.js
https://developer3.penang.gov.my/app_pintas/assets/global/
https://developer3.penang.gov.my/app_pintas/assets/jquery.gmap/
https://developer3.penang.gov.my/app_pintas/assets/jquery.gmap/jquery.gmap.min.js
https://developer3.penang.gov.my/app_pintas/assets/snippets/
https://developer3.penang.gov.my/app_pintas/assets/snippets/pages/
https://developer3.penang.gov.my/app_pintas/assets/snippets/pages/user/
https://developer3.penang.gov.my/app_pintas/assets/snippets/pages/user/login.js
https://developer3.penang.gov.my/app_pintas/assets/vendors/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/fonts/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/fonts/flaticon/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/fonts/font-awesome/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/fonts/line-awesome/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/fonts/metronic/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/fonts/socicon/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/fonts/summernote/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/images/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/images/ion-rangeslider/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/images/jstree/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/images/malihu-custom-scrollbar-plugin/
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/vendors.bundle.css
https://developer3.penang.gov.my/app_pintas/assets/vendors/base/vendors.bundle.js
https://developer3.penang.gov.my/app_pintas/assets/vendors/custom/
https://developer3.penang.gov.my/app_pintas/assets/vendors/custom/fullcalendar/

https://developer3.penang.gov.my/app_pintas/assets/vendors/custom/fullcalendar/fullcalendar.bundle.css
https://developer3.penang.gov.my/app_pintas/assets/wowslider/
https://developer3.penang.gov.my/app_pintas/assets/wowslider/jquery.js
https://developer3.penang.gov.my/app_pintas/assets/wowslider/script.js
https://developer3.penang.gov.my/app_pintas/assets/wowslider/style.css
https://developer3.penang.gov.my/app_pintas/assets/wowslider/wowslider.js
https://developer3.penang.gov.my/app_pintas/fr_faq.php
https://developer3.penang.gov.my/app_pintas/fr_penafian.php
https://developer3.penang.gov.my/app_pintas/fr_terma.php
https://developer3.penang.gov.my/app_pintas/image/
https://developer3.penang.gov.my/app_pintas/image/popup/
https://developer3.penang.gov.my/app_pintas/image/slide/
https://developer3.penang.gov.my/app_pintas/image/slide/apps/
https://developer3.penang.gov.my/app_pintas/includes/
https://developer3.penang.gov.my/app_pintas/includes/commonFunc.js
https://developer3.penang.gov.my/app_pintas/index.php
https://developer3.penang.gov.my/app_pintas/login-ajax.php
https://developer3.penang.gov.my/app_pintas/login.php
https://developer3.penang.gov.my/app_pintas/manual/
https://developer3.penang.gov.my/app_pintas/popup.php
https://developer3.penang.gov.my/app_pintas/register.php
https://developer3.penang.gov.my/app_pintas/rest/
https://developer3.penang.gov.my/app_pintas/tcpdf/