acunetix

# Affected Items Report

Acunetix Security Audit

17 January 2019

Generated by Acunetix

# Scan of localhost

## Scan details

| Scan information | |
|---|---|
| Start time | 17/01/2019, 07:46:18 |
| Start url | http://localhost:1234/projects/Atmrs/ |
| Host | localhost |
| Scan time | 10 minutes, 48 seconds |
| Profile | Full Scan |
| Server information | Apache/2.4.27 (Win32) OpenSSL/1.0.2l PHP/7.1.9 |
| Responsive | True |
| Server OS | Windows |

### Threat level

#### Acunetix Threat Level 3

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

### Alerts distribution

| | |
|---|---|
| Total alerts found | 157 |
| High | 84 |
| Medium | 50 |
| Low | 16 |
| Informational | 7 |

## Affected items

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

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

| **Alert group** | **Cross site scripting** |
|---|---|
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |

| | |
|---|---|
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cross site scripting** |
| Severity | High |

| | |
|---|---|
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Cross site scripting** |
| Severity | High |
| Description | Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates. |
| Recommendations | Apply context-dependent encoding and/or validation to user input rendered on a page |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Apache server-info enabled** |
| Severity | Medium |
| Description | Apache /server-info displays information about your Apache configuration. If you are not using this feature, disable it. |

| | |
|---|---|
| Recommendations | Disable this functionality if not required. Comment out the <Location /server-info> section from httpd.conf. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Apache server-status enabled** |
| Severity | Medium |
| Description | Apache /server-status displays information about your Apache status. If you are not using this feature, disable it. |
| Recommendations | Disable this functionality if not required. Comment out the <Location /server-status> section from httpd.conf. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Application error message** |
| Severity | Medium |
| Description | This alert requires manual confirmation<br>Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.<br>Acunetix found an error or warning message that may disclose sensitive information. The message 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. |
| Recommendations | Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Backup files** |
| Severity | Medium |
| Description | A possible backup copy of a directory was found on your web server. These files are usually created by developers to backup their work. |
| Recommendations | Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |

| | |
|---|---|
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |

| | |
|---|---|
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Directory listing** |
| Severity | Medium |

| | |
|---|---|
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |

| | |
|---|---|
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |

| | |
|---|---|
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |

| | |
|---|---|
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |

| | |
|---|---|
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |

| | |
|---|---|
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |

| | |
|---|---|
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |

| | |
|---|---|
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Directory listing** |
| Severity | Medium |
| Description | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. |
| Recommendations | You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Host header attack** |
| Severity | Medium |
| Description | In many cases, developers are trusting the HTTP Host header value and using it to generate links, import scripts and even generate password resets links with its value. This is a very bad idea, because the HTTP Host header can be controlled by an attacker. This can be exploited using web-cache poisoning and by abusing alternative channels like password reset emails. |
| Recommendations | The web application should use the SERVER_NAME instead of the Host header. It should also create a dummy vhost that catches all requests with unrecognized Host headers. This can also be done under Nginx by specifying a non-wildcard SERVER_NAME, and under Apache by using a non-wildcard serverName and turning the UseCanonicalName directive on. Consult references for detailed information. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

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

| **Alert group** | **HTML form without CSRF protection** |
|---|---|
| Severity | Medium |
| Description | This alert requires manual confirmation<br>Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.<br>Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form. |
| Recommendations | Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.<br>The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes.<br>• The anti-CSRF token should be unique for each user session<br>• The session should automatically expire after a suitable amount of time<br>• The anti-CSRF token should be a cryptographically random value of significant length<br>• The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm<br>• The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent)<br>• The server should reject the requested action if the anti-CSRF token fails validation<br>When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Test CGI script leaking environment variables** |
| Severity | Medium |
| Description | A test CGI (Common Gateway Interface) script was found on this server. The response page returned by this CGI script is leaking a list of server environment variables.<br>Environment variables are a set of dynamic named values that can affect the way running processes will behave on a computer. For example, an environment variable with a standard name can designate the location that a particular computer system uses to store temporary files but this may vary from one computer system to another. |
| Recommendations | Restrict access to this CGI file or remove it from your system. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **User credentials are sent in clear text** |
| Severity | Medium |

| | |
|---|---|
| Description | User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users. |
| Recommendations | Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS). |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **User credentials are sent in clear text** |
| Severity | Medium |
| Description | User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users. |
| Recommendations | Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS). |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Vulnerable Javascript library** |
| Severity | Medium |
| Description | You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Vulnerable Javascript library** |
| Severity | Medium |
| Description | You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |
| Details | Not available in the free trial |
| Not available in the free trial | |

| **Web Server** | |
|---|---|
| **Alert group** | **Clickjacking: X-Frame-Options header missing** |
| Severity | Low |

| | |
|---|---|
| Description | Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.<br>The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. |
| Recommendations | Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cookie(s) without HttpOnly flag set** |
| Severity | Low |
| Description | This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies. |
| Recommendations | If possible, you should set the HTTPOnly flag for this cookie. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Cookie(s) without Secure flag set** |
| Severity | Low |
| Description | This cookie 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 channels. This is an important security protection for session cookies. |
| Recommendations | If possible, you should set the Secure flag for this cookie. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation file** |
| Severity | Low |
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

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

| **Alert group** | **Documentation file** |
|---|---|
| Severity | Low |
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation file** |
| Severity | Low |
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation file** |
| Severity | Low |
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation file** |
| Severity | Low |
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation file** |

| | |
|---|---|
| Severity | Low |
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation file** |
| Severity | Low |
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation file** |
| Severity | Low |
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation file** |
| Severity | Low |
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation file** |
| Severity | Low |

| | |
|---|---|
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Documentation file** |
| Severity | Low |
| Description | A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems. |
| Recommendations | Remove or restrict access to all documentation file acessible from internet. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Login page password-guessing attack** |
| Severity | Low |
| Description | A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.<br>This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem. |
| Recommendations | It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **TRACE method is enabled** |
| Severity | Low |
| Description | HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method. |
| Recommendations | Disable TRACE Method on the web server. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

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

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

| **Web Server** | |
|---|---|
| **Alert group** | **Content type is not specified** |
| Severity | Informational |
| Description | This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems. |
| Recommendations | Set a Content-Type header value for this page. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| **Web Server** | |
|---|---|
| **Alert group** | **Content type is not specified** |
| Severity | Informational |
| Description | This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems. |
| Recommendations | Set a Content-Type header value for this page. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Content type is not specified** |
| Severity | Informational |
| Description | This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems. |
| Recommendations | Set a Content-Type header value for this page. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Email address found** |
| Severity | Informational |
| Description | One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found. |
| Recommendations | Check references for details on how to solve this problem. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Email address found** |
| Severity | Informational |
| Description | One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found. |
| Recommendations | Check references for details on how to solve this problem. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Possible username or password disclosure** |
| Severity | Informational |
| Description | A username and/or password was found in this file. This information could be sensitive.<br>This alert may be a false positive, manual confirmation is required. |
| Recommendations | Remove this file from your website or change its permissions to remove access. |
| Alert variants | |
| Details | Not available in the free trial |
| `Not available in the free trial` | |

## Scanned items (coverage report)

```
http://localhost:1234/
http://localhost:1234/projects/
http://localhost:1234/projects/Atmrs/
http://localhost:1234/projects/Atmrs//assets/
http://localhost:1234/projects/Atmrs//assets/admin/
http://localhost:1234/projects/Atmrs//assets/admin/layout/
http://localhost:1234/projects/Atmrs//assets/admin/layout/css/
http://localhost:1234/projects/Atmrs//assets/admin/layout/css/custom.css
http://localhost:1234/projects/Atmrs//assets/admin/layout/css/layout.css
http://localhost:1234/projects/Atmrs//assets/admin/layout/css/themes/
http://localhost:1234/projects/Atmrs//assets/admin/layout/css/themes/default.css
http://localhost:1234/projects/Atmrs//assets/admin/layout/scripts/
http://localhost:1234/projects/Atmrs//assets/admin/layout/scripts/demo.js
http://localhost:1234/projects/Atmrs//assets/admin/layout/scripts/layout.js
http://localhost:1234/projects/Atmrs//assets/admin/pages/
http://localhost:1234/projects/Atmrs//assets/admin/pages/css/
http://localhost:1234/projects/Atmrs//assets/admin/pages/css/login-soft.css
http://localhost:1234/projects/Atmrs//assets/admin/pages/scripts/
http://localhost:1234/projects/Atmrs//assets/admin/pages/scripts/login-soft.js
http://localhost:1234/projects/Atmrs//assets/global/
http://localhost:1234/projects/Atmrs//assets/global/css/
http://localhost:1234/projects/Atmrs//assets/global/css/components-rounded.css
http://localhost:1234/projects/Atmrs//assets/global/css/plugins.css
http://localhost:1234/projects/Atmrs//assets/global/plugins/
http://localhost:1234/projects/Atmrs//assets/global/plugins/backstretch/
http://localhost:1234/projects/Atmrs//assets/global/plugins/backstretch/jquery.backstretch.min.js
http://localhost:1234/projects/Atmrs//assets/global/plugins/bootstrap/
http://localhost:1234/projects/Atmrs//assets/global/plugins/bootstrap/css/
http://localhost:1234/projects/Atmrs//assets/global/plugins/bootstrap/css/bootstrap.min.css
http://localhost:1234/projects/Atmrs//assets/global/plugins/bootstrap/js/
http://localhost:1234/projects/Atmrs//assets/global/plugins/bootstrap/js/bootstrap.min.js
http://localhost:1234/projects/Atmrs//assets/global/plugins/font-awesome/
http://localhost:1234/projects/Atmrs//assets/global/plugins/font-awesome/css/
http://localhost:1234/projects/Atmrs//assets/global/plugins/font-awesome/css/font-awesome.min.css
http://localhost:1234/projects/Atmrs//assets/global/plugins/font-awesome/fonts/
http://localhost:1234/projects/Atmrs//assets/global/plugins/font-awesome/fonts/fontawesome-webfont.woff2
http://localhost:1234/projects/Atmrs//assets/global/plugins/jquery-migrate.min.js
http://localhost:1234/projects/Atmrs//assets/global/plugins/jquery-validation/
http://localhost:1234/projects/Atmrs//assets/global/plugins/jquery-validation/js/
http://localhost:1234/projects/Atmrs//assets/global/plugins/jquery-validation/js/jquery.validate.min.js
http://localhost:1234/projects/Atmrs//assets/global/plugins/jquery.blockui.min.js
http://localhost:1234/projects/Atmrs//assets/global/plugins/jquery.cokie.min.js
http://localhost:1234/projects/Atmrs//assets/global/plugins/jquery.min.js
http://localhost:1234/projects/Atmrs//assets/global/plugins/select2/
http://localhost:1234/projects/Atmrs//assets/global/plugins/select2/select2.css
http://localhost:1234/projects/Atmrs//assets/global/plugins/select2/select2.min.js
http://localhost:1234/projects/Atmrs//assets/global/plugins/simple-line-icons/
http://localhost:1234/projects/Atmrs//assets/global/plugins/simple-line-icons/simple-line-icons.min.css
http://localhost:1234/projects/Atmrs//assets/global/plugins/uniform/
http://localhost:1234/projects/Atmrs//assets/global/plugins/uniform/css/
http://localhost:1234/projects/Atmrs//assets/global/plugins/uniform/css/uniform.default.css
http://localhost:1234/projects/Atmrs//assets/global/plugins/uniform/jquery.uniform.min.js
http://localhost:1234/projects/Atmrs//assets/global/scripts/
http://localhost:1234/projects/Atmrs//assets/global/scripts/metronic.js
http://localhost:1234/projects/Atmrs/assets/
http://localhost:1234/projects/Atmrs/assets/admin/
http://localhost:1234/projects/Atmrs/assets/admin/layout/
http://localhost:1234/projects/Atmrs/assets/admin/layout/css/
http://localhost:1234/projects/Atmrs/assets/admin/layout/css/custom.css
http://localhost:1234/projects/Atmrs/assets/admin/layout/css/layout.css
```

```
http://localhost:1234/projects/Atmrs/assets/admin/layout/css/themes/
http://localhost:1234/projects/Atmrs/assets/admin/layout/css/themes/default.css
http://localhost:1234/projects/Atmrs/assets/admin/layout/img/
http://localhost:1234/projects/Atmrs/assets/admin/layout/scripts/
http://localhost:1234/projects/Atmrs/assets/admin/layout/scripts/demo.js
http://localhost:1234/projects/Atmrs/assets/admin/layout/scripts/layout.js
http://localhost:1234/projects/Atmrs/assets/admin/pages/
http://localhost:1234/projects/Atmrs/assets/admin/pages/css/
http://localhost:1234/projects/Atmrs/assets/admin/pages/css/login-soft.css
http://localhost:1234/projects/Atmrs/assets/admin/pages/img/
http://localhost:1234/projects/Atmrs/assets/admin/pages/scripts/
http://localhost:1234/projects/Atmrs/assets/admin/pages/scripts/login-soft.js
http://localhost:1234/projects/Atmrs/assets/css/
http://localhost:1234/projects/Atmrs/assets/css/boo-coloring.css
http://localhost:1234/projects/Atmrs/assets/css/boo-extension.css
http://localhost:1234/projects/Atmrs/assets/css/boo-utility.css
http://localhost:1234/projects/Atmrs/assets/css/boo.css
http://localhost:1234/projects/Atmrs/assets/css/lib/
http://localhost:1234/projects/Atmrs/assets/css/lib/bootstrap-responsive.css
http://localhost:1234/projects/Atmrs/assets/css/lib/bootstrap.css
http://localhost:1234/projects/Atmrs/assets/css/style.css
http://localhost:1234/projects/Atmrs/assets/datepicker/
http://localhost:1234/projects/Atmrs/assets/datepicker/jquery-ui-timepicker-addon.css
http://localhost:1234/projects/Atmrs/assets/datepicker/jquery-ui-timepicker-addon.js
http://localhost:1234/projects/Atmrs/assets/datepicker/themes/
http://localhost:1234/projects/Atmrs/assets/datepicker/themes/base/
http://localhost:1234/projects/Atmrs/assets/datepicker/themes/base/jquery.ui.all.css
http://localhost:1234/projects/Atmrs/assets/datepicker/ui/
http://localhost:1234/projects/Atmrs/assets/datepicker/ui/jquery.ui.core.js
http://localhost:1234/projects/Atmrs/assets/datepicker/ui/jquery.ui.datepicker.js
http://localhost:1234/projects/Atmrs/assets/datepicker/ui/jquery.ui.mouse.js
http://localhost:1234/projects/Atmrs/assets/datepicker/ui/jquery.ui.slider.js
http://localhost:1234/projects/Atmrs/assets/datepicker/ui/jquery.ui.widget.js
http://localhost:1234/projects/Atmrs/assets/global/
http://localhost:1234/projects/Atmrs/assets/global/css/
http://localhost:1234/projects/Atmrs/assets/global/css/components-rounded.css
http://localhost:1234/projects/Atmrs/assets/global/css/plugins.css
http://localhost:1234/projects/Atmrs/assets/global/img/
http://localhost:1234/projects/Atmrs/assets/global/img/social/
http://localhost:1234/projects/Atmrs/assets/global/plugins/
http://localhost:1234/projects/Atmrs/assets/global/plugins/backstretch/
http://localhost:1234/projects/Atmrs/assets/global/plugins/backstretch/jquery.backstretch.min.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap-datepicker.zip
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap-datepicker/
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap-datetimepicker/
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap-hover-dropdown/
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap-modal.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap-modalmanager.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap-switch/
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap-timepicker/
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap/
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap/css/
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap/css/bootstrap.min.css
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap/fonts/
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap/fonts/glyphicons-halflings-regular.woff2
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap/js/
http://localhost:1234/projects/Atmrs/assets/global/plugins/bootstrap/js/bootstrap.min.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/font-awesome/
http://localhost:1234/projects/Atmrs/assets/global/plugins/font-awesome/css/
http://localhost:1234/projects/Atmrs/assets/global/plugins/font-awesome/css/font-awesome.min.css
http://localhost:1234/projects/Atmrs/assets/global/plugins/font-awesome/fonts/
http://localhost:1234/projects/Atmrs/assets/global/plugins/font-awesome/fonts/fontawesome-webfont.woff2
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery-migrate.min.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery-slimscroll/
```

```
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery-ui/
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery-validation/
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery-validation/js/
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery-validation/js/jquery.validate.min.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery.blockui.min.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery.cokie.min.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery.mCustomScrollbar.concat.min.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery.min.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/jquery.sparkline.min.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/jqvmap/
http://localhost:1234/projects/Atmrs/assets/global/plugins/morris/
http://localhost:1234/projects/Atmrs/assets/global/plugins/scripts.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/select2/
http://localhost:1234/projects/Atmrs/assets/global/plugins/select2/select2.css
http://localhost:1234/projects/Atmrs/assets/global/plugins/select2/select2.min.js
http://localhost:1234/projects/Atmrs/assets/global/plugins/simple-line-icons/
http://localhost:1234/projects/Atmrs/assets/global/plugins/simple-line-icons/fonts/
http://localhost:1234/projects/Atmrs/assets/global/plugins/simple-line-icons/simple-line-icons.min.css
http://localhost:1234/projects/Atmrs/assets/global/plugins/uniform/
http://localhost:1234/projects/Atmrs/assets/global/plugins/uniform/css/
http://localhost:1234/projects/Atmrs/assets/global/plugins/uniform/css/uniform.default.css
http://localhost:1234/projects/Atmrs/assets/global/plugins/uniform/images/
http://localhost:1234/projects/Atmrs/assets/global/plugins/uniform/jquery.uniform.min.js
http://localhost:1234/projects/Atmrs/assets/global/scripts/
http://localhost:1234/projects/Atmrs/assets/global/scripts/datatable.js
http://localhost:1234/projects/Atmrs/assets/global/scripts/metronic.js
http://localhost:1234/projects/Atmrs/assets/jquery_validate/
http://localhost:1234/projects/Atmrs/assets/jquery_validate/css/
http://localhost:1234/projects/Atmrs/assets/jquery_validate/css/screen.css
http://localhost:1234/projects/Atmrs/assets/jquery_validate/dist/
http://localhost:1234/projects/Atmrs/assets/jquery_validate/dist/jquery.validate.js
http://localhost:1234/projects/Atmrs/assets/js/
http://localhost:1234/projects/Atmrs/assets/js/application.js
http://localhost:1234/projects/Atmrs/assets/js/core.js
http://localhost:1234/projects/Atmrs/assets/js/jspdf.js
http://localhost:1234/projects/Atmrs/assets/js/lib/
http://localhost:1234/projects/Atmrs/assets/js/lib/bootstrap/
http://localhost:1234/projects/Atmrs/assets/js/lib/bootstrap/bootstrap.js
http://localhost:1234/projects/Atmrs/assets/js/lib/jquery-ui.js
http://localhost:1234/projects/Atmrs/assets/js/lib/jquery.cookie.js
http://localhost:1234/projects/Atmrs/assets/js/lib/jquery.date.min.js
http://localhost:1234/projects/Atmrs/assets/js/lib/jquery.js
http://localhost:1234/projects/Atmrs/assets/js/lib/jquery.load-image.min.js
http://localhost:1234/projects/Atmrs/assets/js/lib/jquery.mousewheel.js
http://localhost:1234/projects/Atmrs/assets/js/libs/
http://localhost:1234/projects/Atmrs/assets/js/libs/base64.js
http://localhost:1234/projects/Atmrs/assets/js/libs/sprintf.js
http://localhost:1234/projects/Atmrs/assets/js/print.js
http://localhost:1234/projects/Atmrs/assets/js/script.js
http://localhost:1234/projects/Atmrs/assets/plugins/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-bootbox/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-bootbox/bootbox.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-colorpicker/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-colorpicker/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-colorpicker/js/bootstrap-colorpicker.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-datepicker/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-datepicker/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-datepicker/js/bootstrap-datepicker.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-daterangepicker/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-daterangepicker/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-daterangepicker/js/bootstrap-daterangepicker.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-datetimepicker/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-datetimepicker/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-datetimepicker/js/bootstrap-datetimepicker.min.js
```

```
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-fileupload/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-fileupload/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-fileupload/js/bootstrap-fileupload.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-fuelux/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-fuelux/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-fuelux/js/all-fuelux.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-image-gallery/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-image-gallery/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-image-gallery/js/bootstrap-image-gallery.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-modal/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-modal/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-modal/js/bootstrap-modal.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-modal/js/bootstrap-modalmanager.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-multiselect/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-multiselect/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-multiselect/js/bootstrap-multiselect.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-progressbar/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-progressbar/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-progressbar/js/bootstrap-progressbar.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-rowlink/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-rowlink/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-rowlink/js/bootstrap-rowlink.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-select/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-select/bootstrap-select.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-timepicker/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-timepicker/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-timepicker/js/bootstrap-timepicker.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-toggle-button/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-toggle-button/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-toggle-button/js/bootstrap-toggle-button.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wizard-2/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wizard-2/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wizard-2/js/bwizard-only.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wizard/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wizard/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wizard/js/bootstrap-wizard.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wysihtml5/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wysihtml5/lib/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wysihtml5/lib/js/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wysihtml5/lib/js/wysihtml5-0.3.0.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wysihtml5/src/
http://localhost:1234/projects/Atmrs/assets/plugins/bootstrap-wysihtml5/src/bootstrap-wysihtml5.js
http://localhost:1234/projects/Atmrs/assets/plugins/jquery.blockUI.js
http://localhost:1234/projects/Atmrs/assets/plugins/jScrollbar-master/
http://localhost:1234/projects/Atmrs/assets/plugins/jScrollbar-master/jquery/
http://localhost:1234/projects/Atmrs/assets/plugins/jScrollbar-master/jquery/jquery-mousewheel.js
http://localhost:1234/projects/Atmrs/assets/plugins/jScrollbar-master/jquery/jScrollbar.jquery.css
http://localhost:1234/projects/Atmrs/assets/plugins/jScrollbar-master/jquery/jScrollbar.jquery.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/mcustomscrollbar/
http://localhost:1234/projects/Atmrs/assets/plugins/mcustomscrollbar/jquery.mCustomScrollbar.concat.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/mcustomscrollbar/jquery.mCustomScrollbar.css
http://localhost:1234/projects/Atmrs/assets/plugins/messi/
http://localhost:1234/projects/Atmrs/assets/plugins/messi/messi.css
http://localhost:1234/projects/Atmrs/assets/plugins/messi/messi.js
http://localhost:1234/projects/Atmrs/assets/plugins/michael-multiselect-d918211/
http://localhost:1234/projects/Atmrs/assets/plugins/michael-multiselect-d918211/css/
http://localhost:1234/projects/Atmrs/assets/plugins/michael-multiselect-d918211/css/ui.multiselect.css
http://localhost:1234/projects/Atmrs/assets/plugins/michael-multiselect-d918211/js/
http://localhost:1234/projects/Atmrs/assets/plugins/michael-multiselect-d918211/js/plugins/
http://localhost:1234/projects/Atmrs/assets/plugins/michael-multiselect-d918211/js/plugins/localisation/
http://localhost:1234/projects/Atmrs/assets/plugins/michael-multiselect-d918211/js/plugins/localisation/jquery.localisation-min.js
http://localhost:1234/projects/Atmrs/assets/plugins/michael-multiselect-d918211/js/plugins/scrollTo/
http://localhost:1234/projects/Atmrs/assets/plugins/michael-multiselect-d918211/js/plugins/scrollTo/jquery.scrollTo-min.js
```

```
http://localhost:1234/projects/Atmrs/assets/plugins/michael-multiselect-d918211/js/ui.multiselect.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-component/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-component/fullcalendar/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-component/fullcalendar/fullcalendar.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-component/rangeslider/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-component/rangeslider/jqallrangesliders.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-content/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-content/jpages/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-content/jpages/js/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-content/jpages/js/jPages.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-content/list/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-content/list/js/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-content/list/js/list.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-content/list/plugins/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-content/list/plugins/list.paging.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-extension/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-extension/google-code-prettify/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-extension/google-code-prettify/prettify.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/counter/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/counter/jquery.counter.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/elastic/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/elastic/jquery.elastic.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/inputmask/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/inputmask/jquery.inputmask.extensions.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/inputmask/jquery.inputmask.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/select2/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/select2/select2.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/uniform/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/uniform/jquery.uniform.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/validate/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/validate/js/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-form/validate/js/jquery.validate.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-gallery/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-gallery/nailthumb/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-gallery/nailthumb/jquery.nailthumb.1.1.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-gallery/nailthumb/showLoading/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-gallery/nailthumb/showLoading/js/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-gallery/nailthumb/showLoading/js/jquery.showLoading.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-gallery/wookmark/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-gallery/wookmark/jquery.imagesloaded.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-gallery/wookmark/jquery.wookmark.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system-info/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system-info/gritter/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system-info/gritter/js/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system-info/gritter/js/jquery.gritter.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system-info/notyfy/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system-info/notyfy/jquery.notyfy.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system-info/qtip2/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system-info/qtip2/dist/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system-info/qtip2/dist/jquery.qtip.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system/nicescroll/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system/nicescroll/jquery.nicescroll.min.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system/xbreadcrumbs/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-system/xbreadcrumbs/xbreadcrumbs.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-table/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-table/datatables/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-table/datatables/media/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-table/datatables/media/js/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-table/datatables/media/js/jquery.dataTables.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-table/datatables/plugin/
http://localhost:1234/projects/Atmrs/assets/plugins/pl-table/datatables/plugin/jquery.dataTables.columnFilter.js
http://localhost:1234/projects/Atmrs/assets/plugins/pl-table/datatables/plugin/jquery.dataTables.plugins.js
```

```
http://localhost:1234/projects/Atmrs/assets/plugins/tinymce/
http://localhost:1234/projects/Atmrs/assets/plugins/tinymce/tinymce.min.js
http://localhost:1234/projects/Atmrs/assets/user-profile-images/
http://localhost:1234/projects/Atmrs/assets/user-profile-images/Thumbs.db
http://localhost:1234/projects/Atmrs/dashboard-one.html
http://localhost:1234/projects/Atmrs/elog/
http://localhost:1234/projects/Atmrs/elog/mainview
http://localhost:1234/projects/Atmrs/index.html
http://localhost:1234/projects/Atmrs/index/
http://localhost:1234/projects/Atmrs/index/authenticate_user
http://localhost:1234/projects/Atmrs/index/logout
```