

**Developer Report**

Acunetix Security Audit

18 February 2020

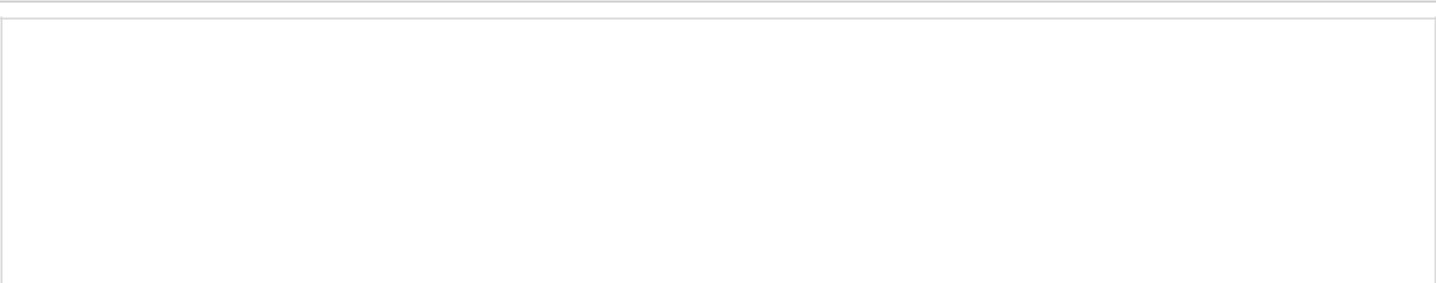
Generated by Acunetix



**Scan of https://thesisbloodwebsite.000webhostapp.com/**



**Scan details**



Scan information

|  |  |
| --- | --- |
| Start time | 18/02/2020, 03:01:45 |
|  |  |
| Start url | https://thesisbloodwebsite.000webhostapp.com/ |
|  |  |
| Host | https://thesisbloodwebsite.000webhostapp.com/ |
|  |  |
| Scan time | 7 minutes, 32 seconds |
|  |  |
| Profile | Full Scan |
|  |  |

**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**



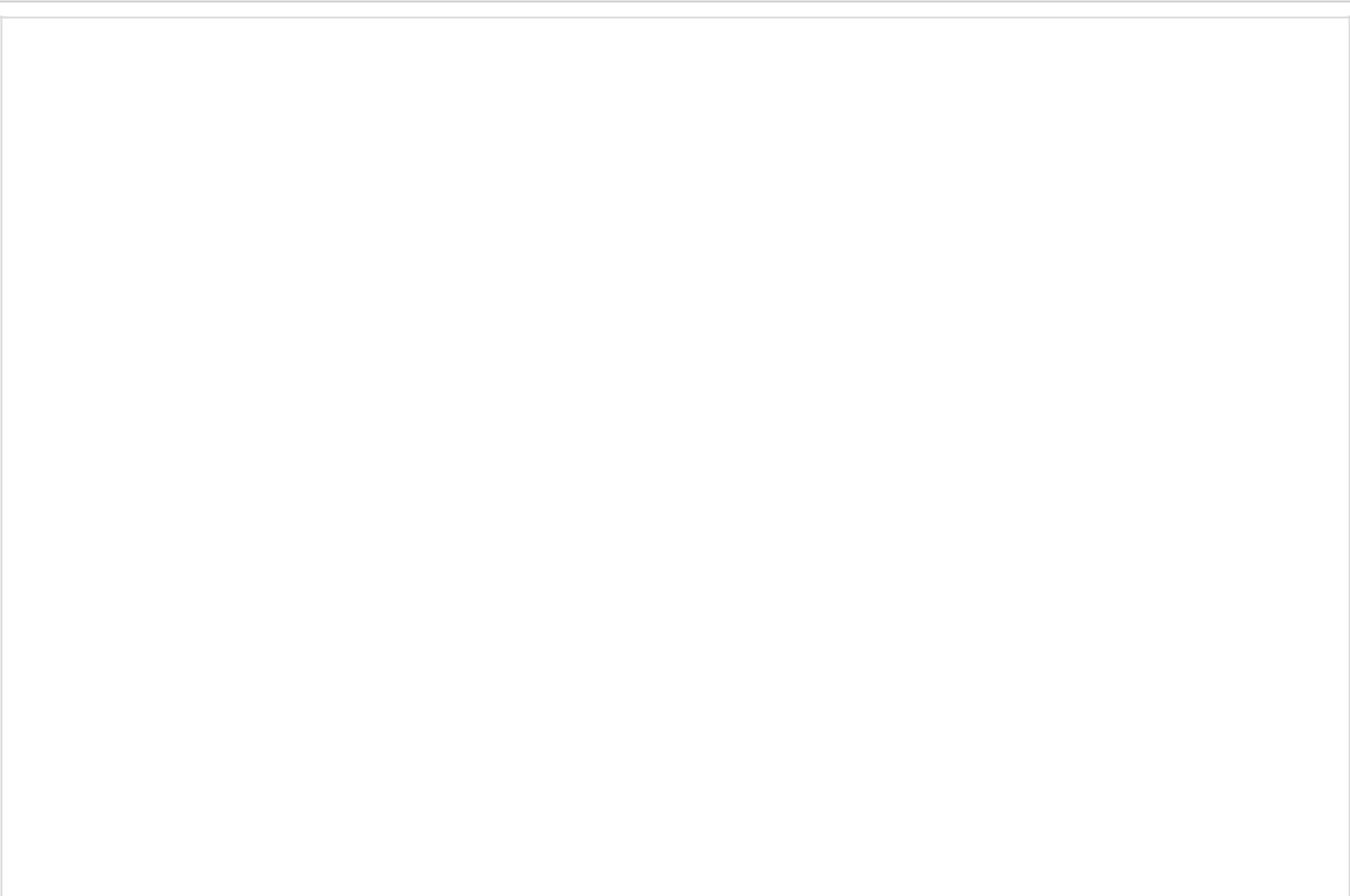
|  |  |
| --- | --- |
| Total alerts found | 31 |
|  |  |
| High | 1 |
|  |  |
| Medium | 10 |
|  |  |
| Low | 8 |
|  |  |
| Informational | 12 |
|  |  |



**Alerts summary**



 **Cross site scripting**

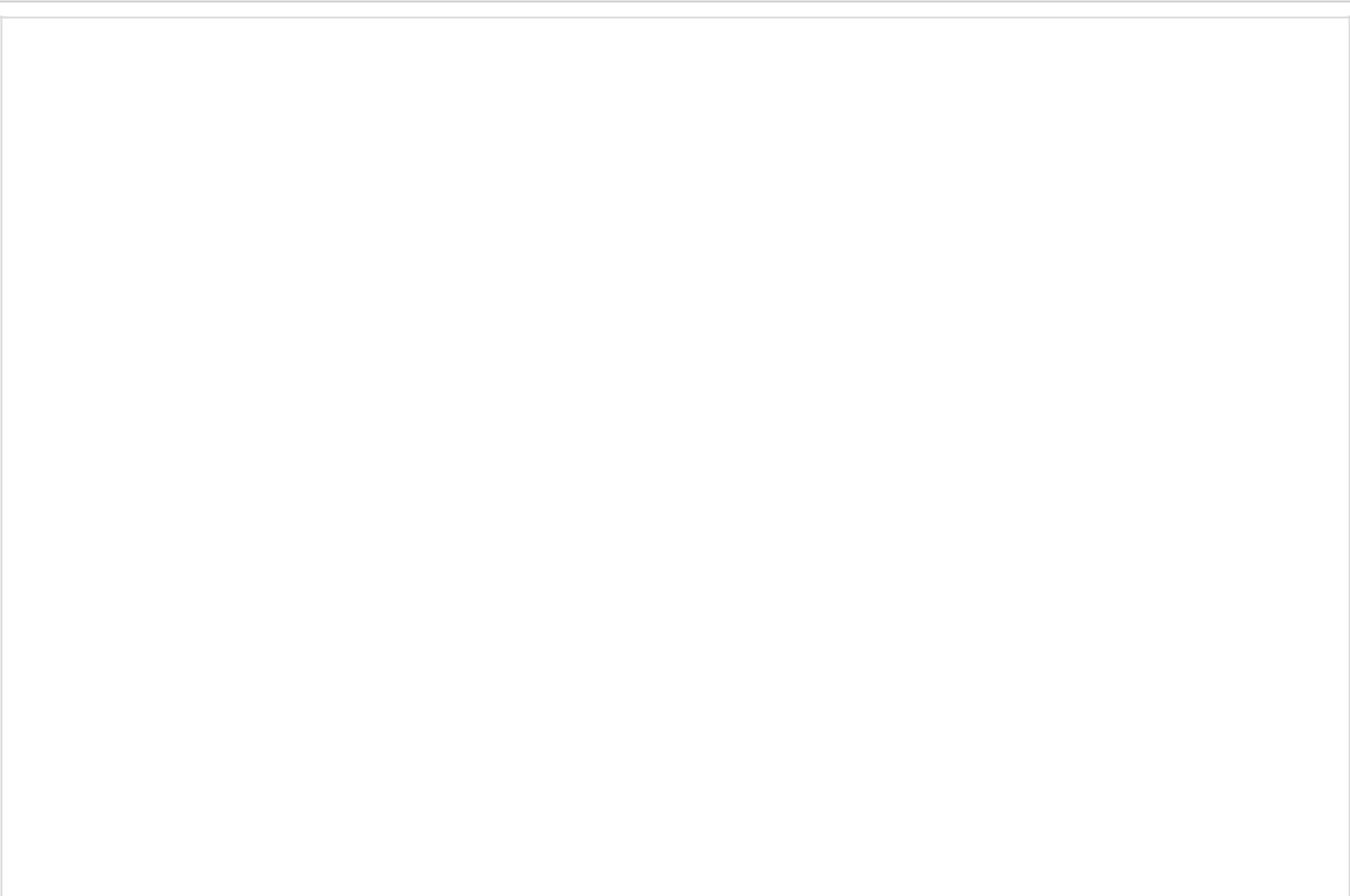


Classification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | Base Score: 6.4 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Low | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: Partial | |
|  |  |  | Integrity Impact: Partial | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  |  |
|  |  |  | Base Score: 5.3 | |
|  |  |  | Attack Vector: Network | |
|  |  |  | Attack Complexity: Low | |
|  |  |  | Privileges Required: None | |
|  | CVSS3 | | User Interaction: None | |
|  |  |  | Scope: Unchanged | |
|  |  |  | Confidentiality Impact: None | |
|  |  |  | Integrity Impact: Low | |
|  |  |  | Availability Impact: None | |
|  |  |  |  |  |
|  | CWE | | CWE-79 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 1 |
|  |  |  |  |  |
|  | **Application error message** | |  |  |
|  |  |  |  |  |
|  | Classification | |  |  |
|  |  |  |  | |
|  |  |  | Base Score: 5.0 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Low | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: Partial | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  | |
|  |  |  | Base Score: 5.3 | |
|  |  |  | Attack Vector: Network | |
|  |  |  | Attack Complexity: Low | |
|  |  |  | Privileges Required: None | |
|  | CVSS3 | | User Interaction: None | |
|  |  |  | Scope: Unchanged | |
|  |  |  | Confidentiality Impact: Low | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  |  |  |  | |
|  | CWE | | CWE-200 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 3 |
|  |  |  |  |  |



 **Directory listing**



Classification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | Base Score: 5.0 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Low | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: Partial | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  |  |
|  |  |  | Base Score: 7.5 | |
|  |  |  | Attack Vector: Network | |
|  |  |  | Attack Complexity: Low | |
|  |  |  | Privileges Required: None | |
|  | CVSS3 | | User Interaction: None | |
|  |  |  | Scope: Unchanged | |
|  |  |  | Confidentiality Impact: High | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  |  |  |  |  |
|  | CWE | | CWE-538 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 1 |
|  |  |  |  |  |
|  | **Error message on page** | |  |  |
|  |  |  |  |  |
|  | Classification | |  |  |
|  |  |  |  | |
|  |  |  | Base Score: 5.0 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Low | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: Partial | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  | |
|  |  |  | Base Score: 5.3 | |
|  |  |  | Attack Vector: Network | |
|  |  |  | Attack Complexity: Low | |
|  |  |  | Privileges Required: None | |
|  | CVSS3 | | User Interaction: None | |
|  |  |  | Scope: Unchanged | |
|  |  |  | Confidentiality Impact: Low | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  |  |  |  | |
|  | CWE | | CWE-200 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 1 |
|  |  |  |  |  |



 **HTML form without CSRF protection**



Classification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | Base Score: 2.6 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: High | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: None | |
|  |  |  | Integrity Impact: Partial | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  |  |
|  |  |  | Base Score: 4.3 | |
|  |  |  | Attack Vector: Network | |
|  |  |  | Attack Complexity: Low | |
|  |  |  | Privileges Required: None | |
|  | CVSS3 | | User Interaction: Required | |
|  |  |  | Scope: Unchanged | |
|  |  |  | Confidentiality Impact: None | |
|  |  |  | Integrity Impact: Low | |
|  |  |  | Availability Impact: None | |
|  |  |  |  |  |
|  | CWE | | CWE-352 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 1 |
|  |  |  |  |  |
|  | **Source code disclosure** | |  |  |
|  |  |  |  |  |
|  | Classification | |  |  |
|  |  |  |  | |
|  |  |  | Base Score: 5.0 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Low | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: Partial | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  | |
|  |  |  | Base Score: 7.5 | |
|  |  |  | Attack Vector: Network | |
|  |  |  | Attack Complexity: Low | |
|  |  |  | Privileges Required: None | |
|  | CVSS3 | | User Interaction: None | |
|  |  |  | Scope: Unchanged | |
|  |  |  | Confidentiality Impact: High | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  |  |  |  | |
|  | CWE | | CWE-538 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 4 |
|  |  |  |  |  |



 **Clickjacking: X-Frame-Options header missing**

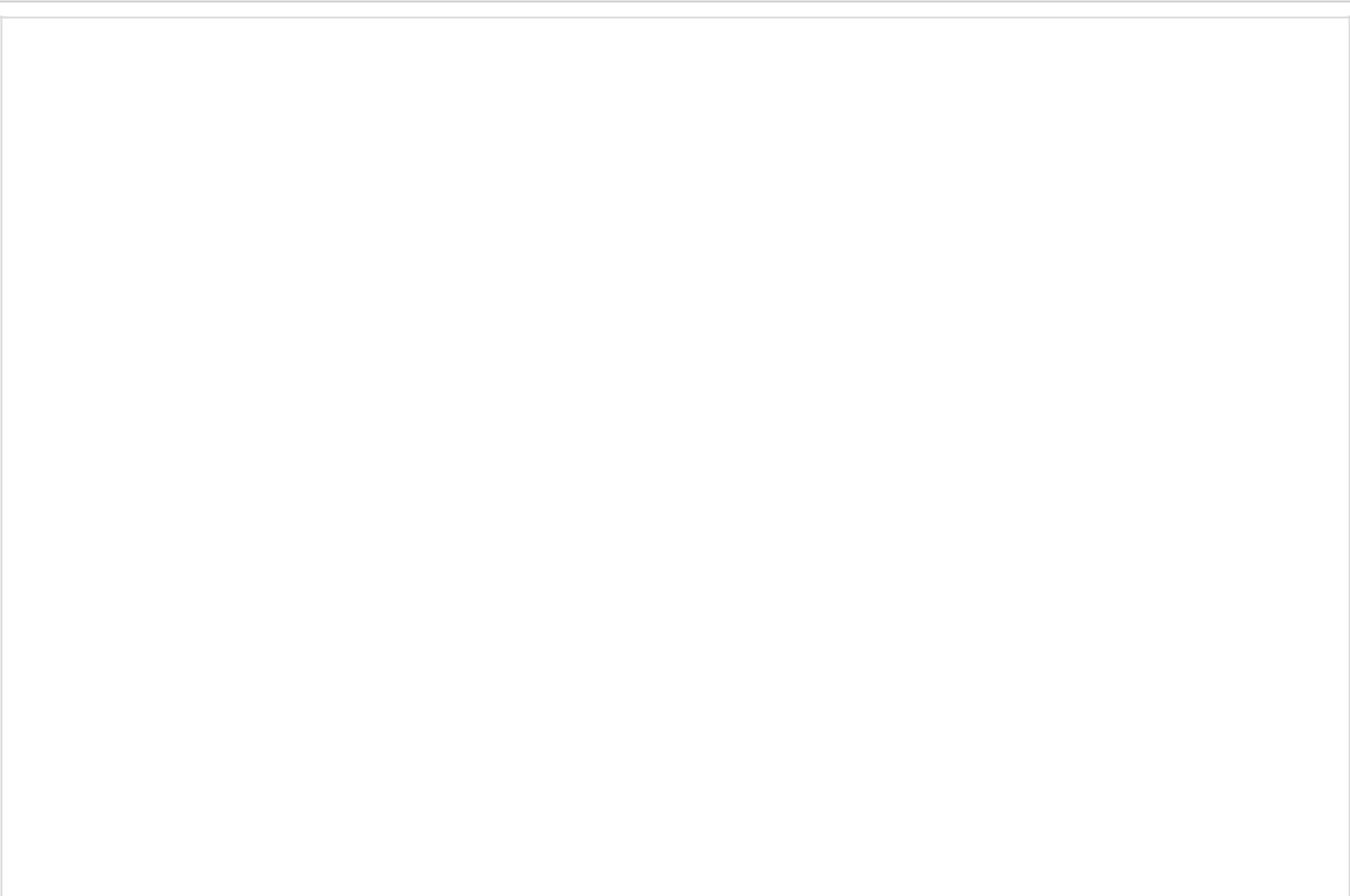


Classification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | Base Score: 6.8 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Medium | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: Partial | |
|  |  |  | Integrity Impact: Partial | |
|  |  |  | Availability Impact: Partial | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  |  |
|  | CWE | | CWE-693 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 1 |
|  |  |  |  |  |
|  | **Cookie(s) without HttpOnly flag set** | |  |  |
|  |  |  |  |  |
|  | Classification | |  |  |
|  |  |  |  | |
|  |  |  | Base Score: 0.0 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Low | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: None | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  | |
|  | CWE | | CWE-16 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 1 |
|  |  |  |  |  |
|  | **Cookie(s) without Secure flag set** | |  |  |
|  |  |  |  |  |
|  | Classification | |  |  |
|  |  |  |  | |
|  |  |  | Base Score: 0.0 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Low | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: None | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  | |
|  | CWE | | CWE-16 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 1 |
|  |  |  |  |  |



 **HTML Form found in redirect page**



Classification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | Base Score: 5.8 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Medium | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: Partial | |
|  |  |  | Integrity Impact: Partial | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Unproven | |
|  |  |  | Remediation Level: Workaround | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  |  |
|  |  |  | Base Score: 6.5 | |
|  |  |  | Attack Vector: Network | |
|  |  |  | Attack Complexity: Low | |
|  |  |  | Privileges Required: None | |
|  | CVSS3 | | User Interaction: None | |
|  |  |  | Scope: Unchanged | |
|  |  |  | Confidentiality Impact: Low | |
|  |  |  | Integrity Impact: Low | |
|  |  |  | Availability Impact: None | |
|  |  |  |  |  |
|  | CWE | | CWE-287 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 5 |
|  |  |  |  |  |
|  | **Email address found** | |  |  |
|  |  |  |  |  |
|  | Classification | |  |  |
|  |  |  |  | |
|  |  |  | Base Score: 0.0 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Low | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: None | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  | |
|  |  |  | Base Score: 0.0 | |
|  |  |  | Attack Vector: Network | |
|  |  |  | Attack Complexity: Low | |
|  |  |  | Privileges Required: None | |
|  | CVSS3 | | User Interaction: None | |
|  |  |  | Scope: Unchanged | |
|  |  |  | Confidentiality Impact: None | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  |  |  |  | |
|  | CWE | | CWE-200 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 11 |
|  |  |  |  |  |



 **Password type input with auto-complete enabled**



Classification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | Base Score: 0.0 | |
|  |  |  | Access Vector: Network\_accessible | |
|  |  |  | Access Complexity: Low | |
|  |  |  | Authentication: None | |
|  |  |  | Confidentiality Impact: None | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  | CVSS2 | | Exploitability: Not\_defined | |
|  |  |  | Remediation Level: Not\_defined | |
|  |  |  | Report Confidence: Not\_defined | |
|  |  |  | Availability Requirement: Not\_defined | |
|  |  |  | Collateral Damage Potential: Not\_defined | |
|  |  |  | Confidentiality Requirement: Not\_defined | |
|  |  |  | Integrity Requirement: Not\_defined | |
|  |  |  | Target Distribution: Not\_defined | |
|  |  |  |  |  |
|  |  |  | Base Score: 7.5 | |
|  |  |  | Attack Vector: Network | |
|  |  |  | Attack Complexity: Low | |
|  |  |  | Privileges Required: None | |
|  | CVSS3 | | User Interaction: None | |
|  |  |  | Scope: Unchanged | |
|  |  |  | Confidentiality Impact: High | |
|  |  |  | Integrity Impact: None | |
|  |  |  | Availability Impact: None | |
|  |  |  |  |  |
|  | CWE | | CWE-200 | |
|  |  |  |  |  |
|  | Affected items | |  | Variation |
|  |  |  |  |  |
|  | [Web Server](file:///C:/ProgramData/Acunetix%20Trial/shared/reports/40d33ead-393c-4fcc-99c2-6316c295bd00.html#link_id_2) | |  | 1 |
|  |  |  |  |  |

**Alerts details**



 **Cross site scripting**



Severity **High**

|  |  |
| --- | --- |
| Reported by module | /Scripts/PerScheme/XSS.script |

**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.

**Impact**



Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

Furthermore, JavaScript can read and make arbitrary modifications to the contents of a page being displayed to a user.

Therefore, XSS in conjunction with some clever social engineering opens up a lot of possibilities for an attacker.

**Recommendation**



Apply context-dependent encoding and/or validation to user input rendered on a page

**References**



[Cross-site Scripting (XSS) Attack - Acunetix (https://www.acunetix.com/websitesecurity/cross-site-scripting/)](https://www.acunetix.com/websitesecurity/cross-site-scripting/)

[Types of XSS - Acunetix (https://www.acunetix.com/websitesecurity/xss/)](https://www.acunetix.com/websitesecurity/xss/)

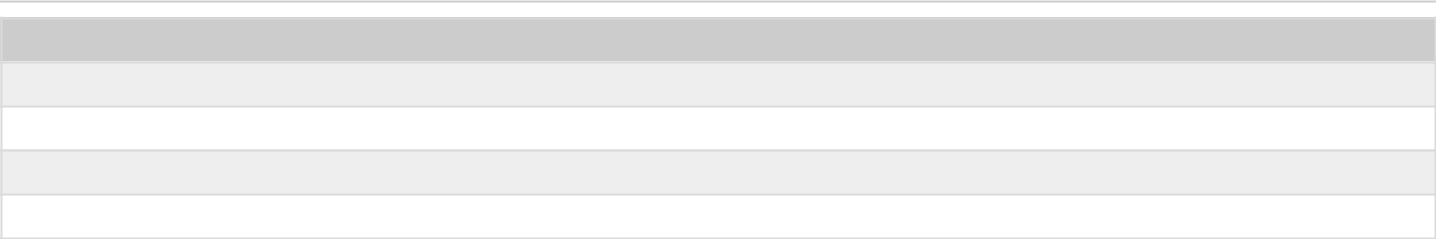
[Cross-site Scripting - OWASP (http://www.owasp.org/index.php/Cross\_Site\_Scripting)](http://www.owasp.org/index.php/Cross_Site_Scripting)

[XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS\_Filter\_Evasion\_Cheat\_Sheet)](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)

[Excess XSS, a comprehensive tutorial on cross-site scripting (https://excess-xss.com/)](https://excess-xss.com/)

[Cross site scripting (http://en.wikipedia.org/wiki/Cross-site\_scripting )](http://en.wikipedia.org/wiki/Cross-site_scripting)

**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

 **Application error message**



Severity **Medium**

|  |  |
| --- | --- |
| Reported by module | /Scripts/PerScheme/XSS.script |

**Description**



This alert requires manual confirmation

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

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.

**Impact**



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

**Recommendation**



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.

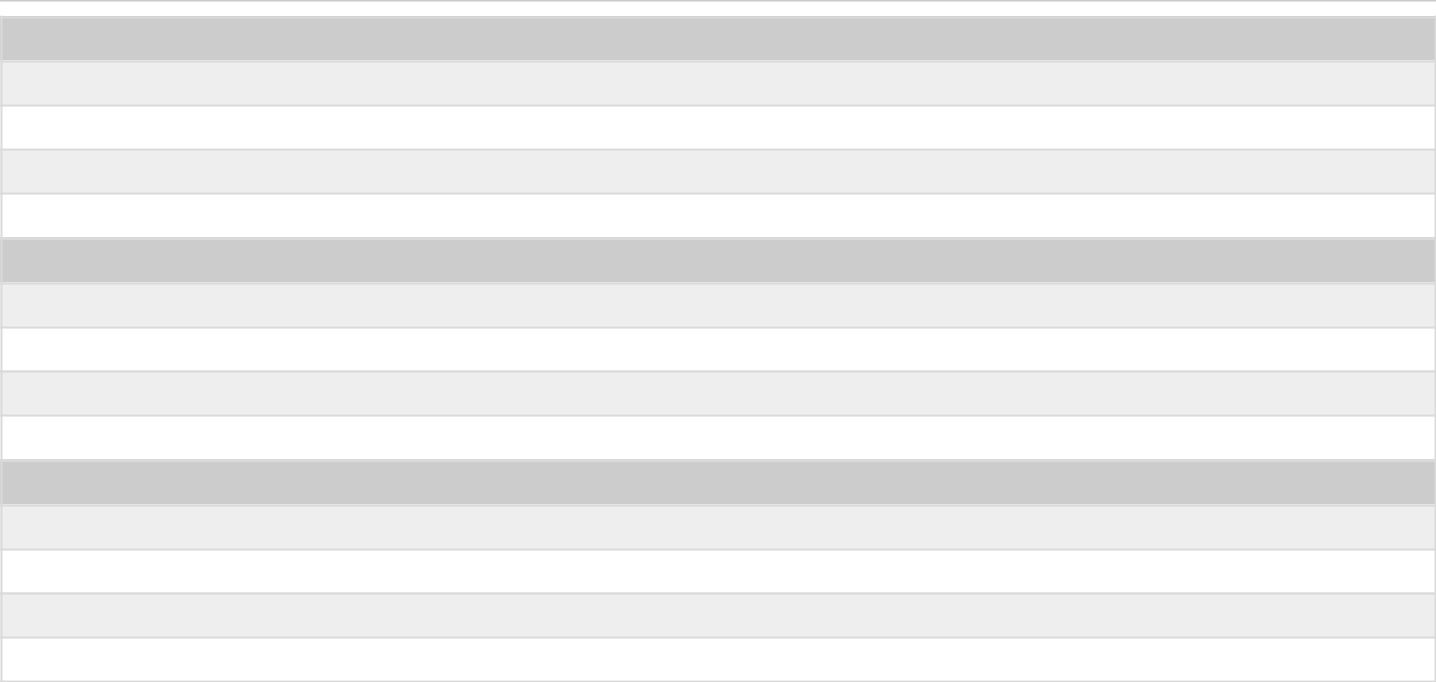
**References**



[PHP Runtime Configuration (http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)](http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)

[Improper Error Handling (https://www.owasp.org/index.php/Improper\_Error\_Handling)](https://www.owasp.org/index.php/Improper_Error_Handling)

**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

 **Directory listing**



Severity **Medium**

|  |  |
| --- | --- |
| Reported by module | /Scripts/PerFolder/Directory\_Listing.script |

**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.

**Impact**



A user can view a list of all files from this directory possibly exposing sensitive information.

**Recommendation**



You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.

**References**



[Directory Listing and Information Disclosure (http://www.acunetix.com/blog/web-security-zone/directory-listing-information-disclosure/)](http://www.acunetix.com/blog/web-security-zone/directory-listing-information-disclosure/)



**Affected items**

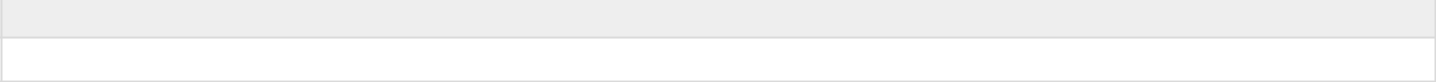


**Web Server**

Details

Not available in the free trial

Request headers



Not available in the free trial

 **Error message on page**



Severity **Medium**

|  |  |
| --- | --- |
| Reported by module | /Scripts/PerFile/Text\_Search\_File.script |

**Description**



This alert requires manual confirmation

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

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.

**Impact**



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

**Recommendation**



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.

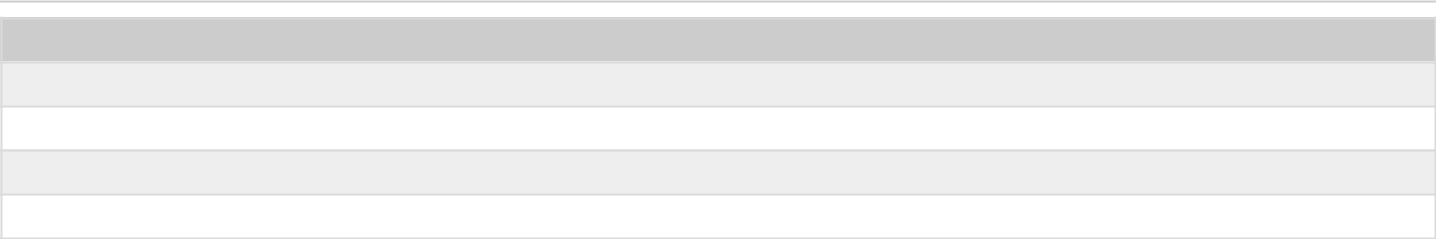
**References**



[PHP Runtime Configuration (http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)](http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)

[Improper Error Handling (https://www.owasp.org/index.php/Improper\_Error\_Handling)](https://www.owasp.org/index.php/Improper_Error_Handling)

**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

 **HTML form without CSRF protection**



Severity **Medium**

|  |  |
| --- | --- |
| Reported by module | /Crawler/12-Crawler\_Form\_NO\_CSRF.js |

**Description**



This alert requires manual confirmation

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.

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.

**Impact**



An attacker could use CSRF to trick a victim into accessing a website hosted by the attacker, or clicking a URL containing malicious or unauthorized requests.

CSRF is a type of 'confused deputy' attack which leverages the authentication and authorization of the victim when the forged request is being sent to the web server. Therefore, if a CSRF vulnerability could affect highly privileged users such as administrators full application compromise may be possible.

**Recommendation**



Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.

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.

The anti-CSRF token should be unique for each user session



The session should automatically expire after a suitable amount of time



The anti-CSRF token should be a cryptographically random value of significant length



The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm



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)



The server should reject the requested action if the anti-CSRF token fails validation



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.

**References**



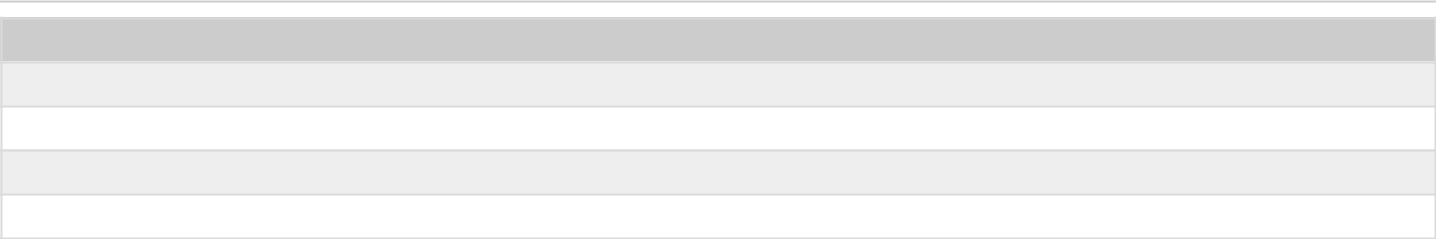
[What is Cross Site Reference Forgery (CSRF)? (https://www.acunetix.com/websitesecurity/csrf-attacks/)](https://www.acunetix.com/websitesecurity/csrf-attacks/) [Cross-Site Request Forgery (CSRF) Prevention Cheatsheet (https://www.owasp.org/index.php/Cross-Site\_Request\_Forgery\_(CSRF)\_Prevention\_Cheat\_Sheet)](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)



[The Cross-Site Request Forgery (CSRF/XSRF) FAQ (http://www.cgisecurity.com/csrf-faq.html)](http://www.cgisecurity.com/csrf-faq.html)

[Cross-site Request Forgery (https://en.wikipedia.org/wiki/Cross-site\_request\_forgery)](https://en.wikipedia.org/wiki/Cross-site_request_forgery)

**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

 **Source code disclosure**



Severity **Medium**

|  |  |
| --- | --- |
| Reported by module | /Scripts/PerFile/Text\_Search\_File.script |

**Description**



Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

**Impact**



An attacker can gather sensitive information (database connection strings, application logic) by analyzing the source code. This information can be used to conduct further attacks.

**Recommendation**



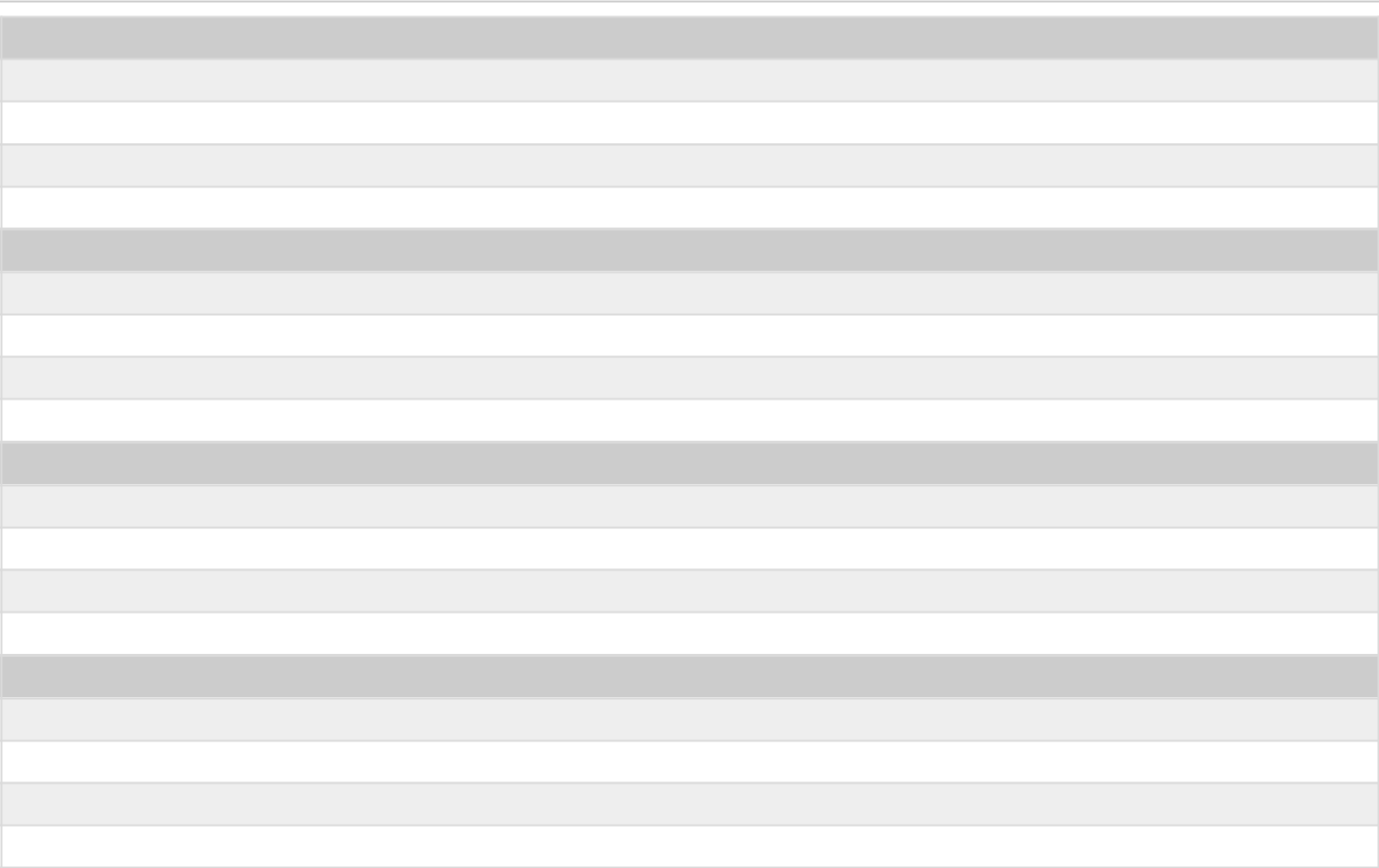
Remove this file from your website or change its permissions to remove access.

**References**



[Source Code Disclosure (http://www.imperva.com/resources/glossary?term=source\_code\_disclosure)](http://www.imperva.com/resources/glossary?term=source_code_disclosure)

**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

 **Clickjacking: X-Frame-Options header missing**



Severity **Low**

|  |  |
| --- | --- |
| Reported by module | /Scripts/PerServer/Clickjacking\_X\_Frame\_Options.script |

**Description**



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

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

**Impact**



The impact depends on the affected web application.

**Recommendation**



Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

**References**



[The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)](https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)

[Clickjacking (http://en.wikipedia.org/wiki/Clickjacking)](http://en.wikipedia.org/wiki/Clickjacking)

[OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)](https://www.owasp.org/index.php/Clickjacking)

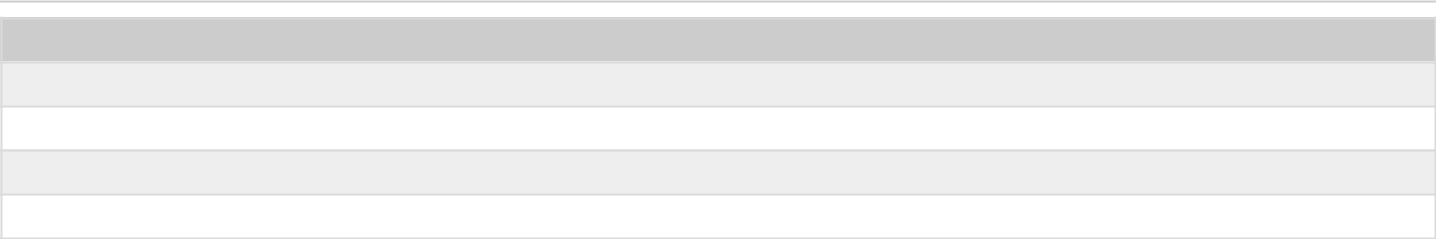
[Defending with Content Security Policy frame-ancestors directive](https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)

[(https://www.owasp.org/index.php/Clickjacking\_Defense\_Cheat\_Sheet#Defending\_with\_Content\_Security\_Policy\_frame-ancestors\_directive)](https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)



[Frame Buster Buster (http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)](http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

 **Cookie(s) without HttpOnly flag set**



Severity **Low**

|  |  |
| --- | --- |
| Reported by module | /RPA/Cookie\_Without\_HttpOnly.js |

**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.

**Impact**



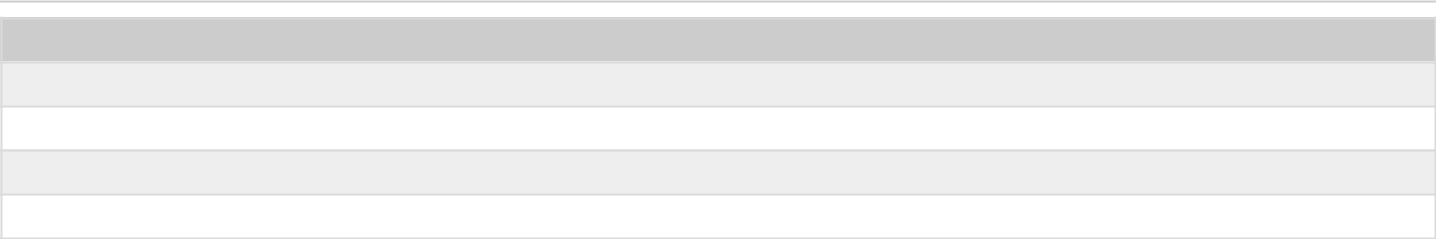
None

**Recommendation**



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

**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

 **Cookie(s) without Secure flag set**



Severity **Low**

|  |  |
| --- | --- |
| Reported by module | /RPA/Cookie\_Without\_Secure.js |

**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.

**Impact**



None

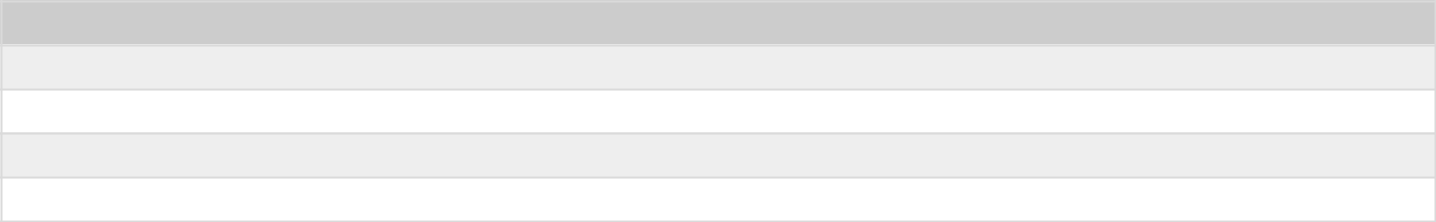
**Recommendation**



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

**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

 **HTML Form found in redirect page**



Severity **Low**

|  |  |
| --- | --- |
| Reported by module | /Scripts/PerFile/HTML\_Form\_In\_Redirect\_Page.script |

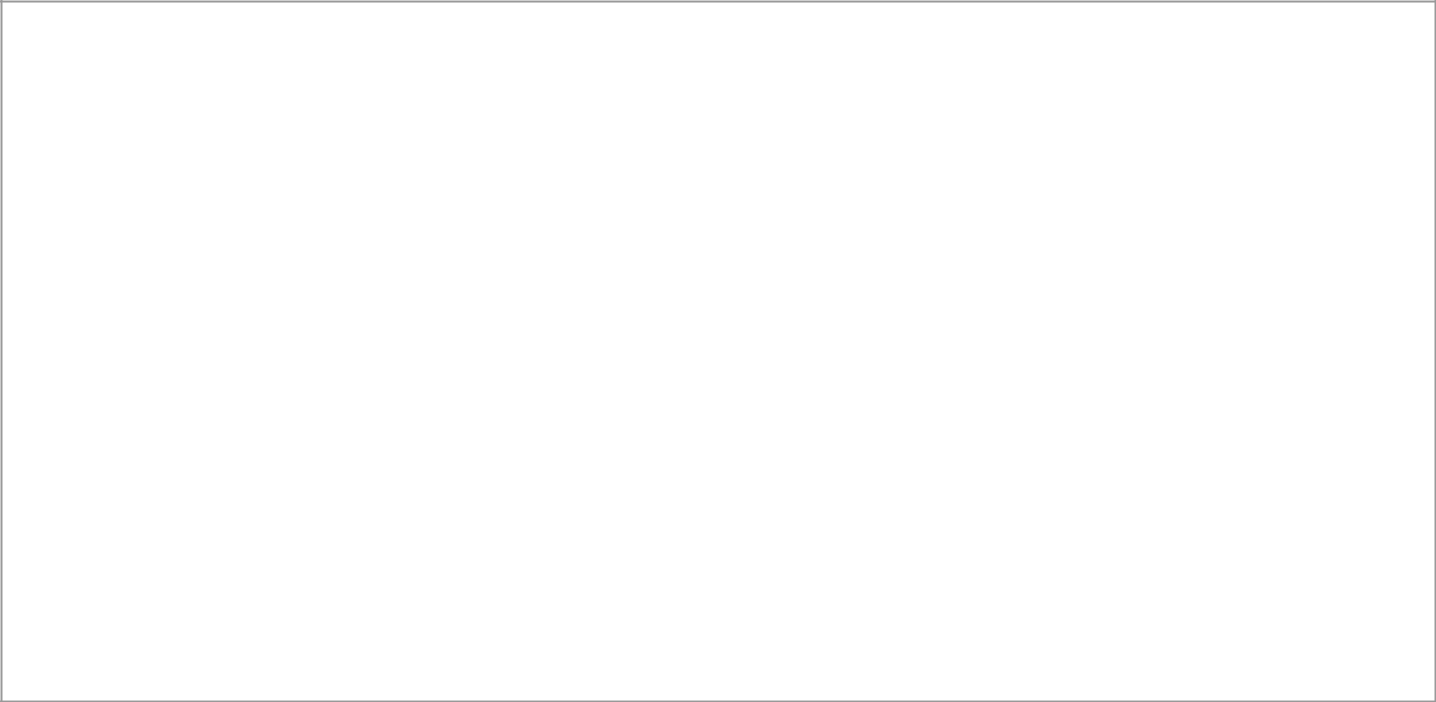
**Description**



Manual confirmation is required for this alert.

An HTML form was found in the response body of this page. However, the current page redirects the visitor to another page by returning an HTTP status code of 301/302. Therefore, all browser users will not see the contents of this page and will not be able to interact with the HTML form.

Sometimes programmers don't properly terminate the script after redirecting the user to another page. For example:



<?php

if (!isset($\_SESSION["authenticated"])) {

header("Location: auth.php");

}

?>

<title>Administration page</title>

<form action="/admin/action" method="post">

<!-- ... form inputs ... -->

</form>

<!-- ... the rest of the administration page ... -->

This script is incorrect because the script is not terminated after the "header("Location: auth.php");" line. An attacker can access

the content the administration page by using an HTTP client that doesn't follow redirection (like HTTP Editor). This creates an

authentication bypass vulnerability.

The correct code would be

<?php

if (!isset($\_SESSION[auth])) {

header("Location: auth.php");

exit();

}

?>

<title>Administration page</title>

<form action="/admin/action" method="post">

<!-- ... form inputs ... -->

</form>

<!-- ... the rest of the administration page ... -->

**Impact**



The impact of this vulnerability depends on the affected web application.

**Recommendation**



Make sure the script is terminated after redirecting the user to another page.

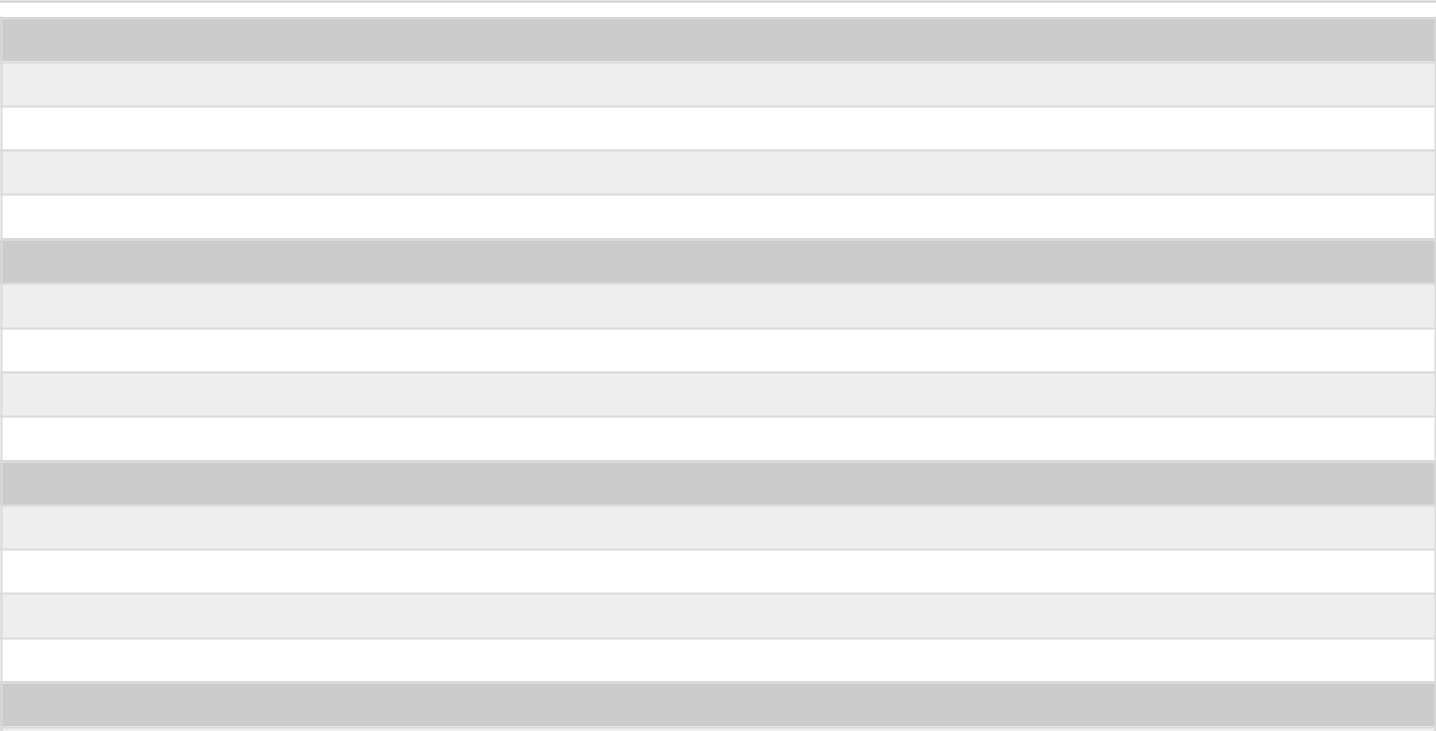
**References**



[HTML Form Found in Redirect Page Web Vulnerability (http://www.acunetix.com/blog/web-security-zone/html-form-found-in-redirect-page/)](http://www.acunetix.com/blog/web-security-zone/html-form-found-in-redirect-page/)



**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

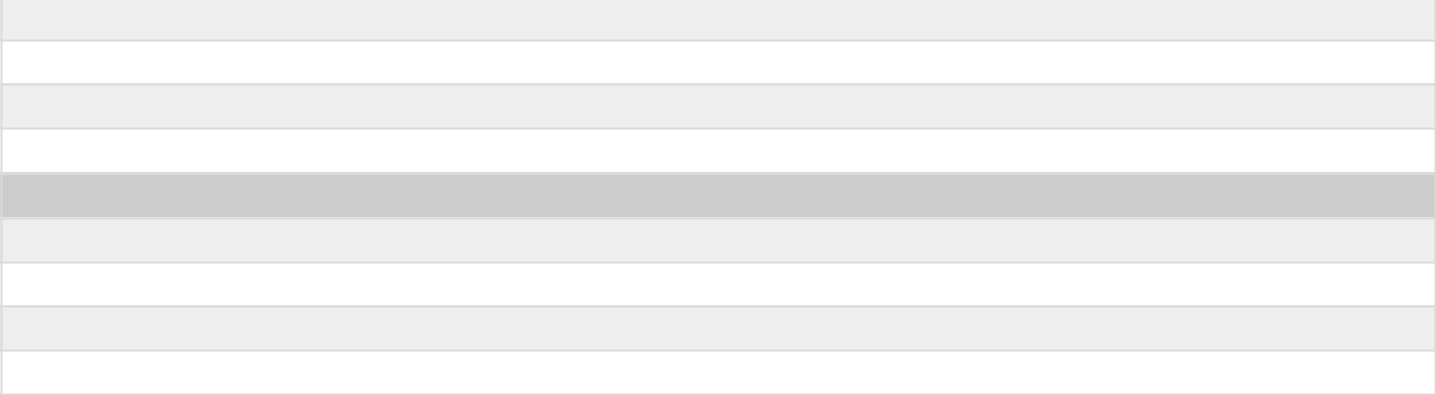
Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

 **Email address found**



Severity **Informational**

|  |  |
| --- | --- |
| Reported by module | /Scripts/PerFolder/Text\_Search\_Dir.script |

**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.

**Impact**



Email addresses posted on Web sites may attract spam.

**Recommendation**



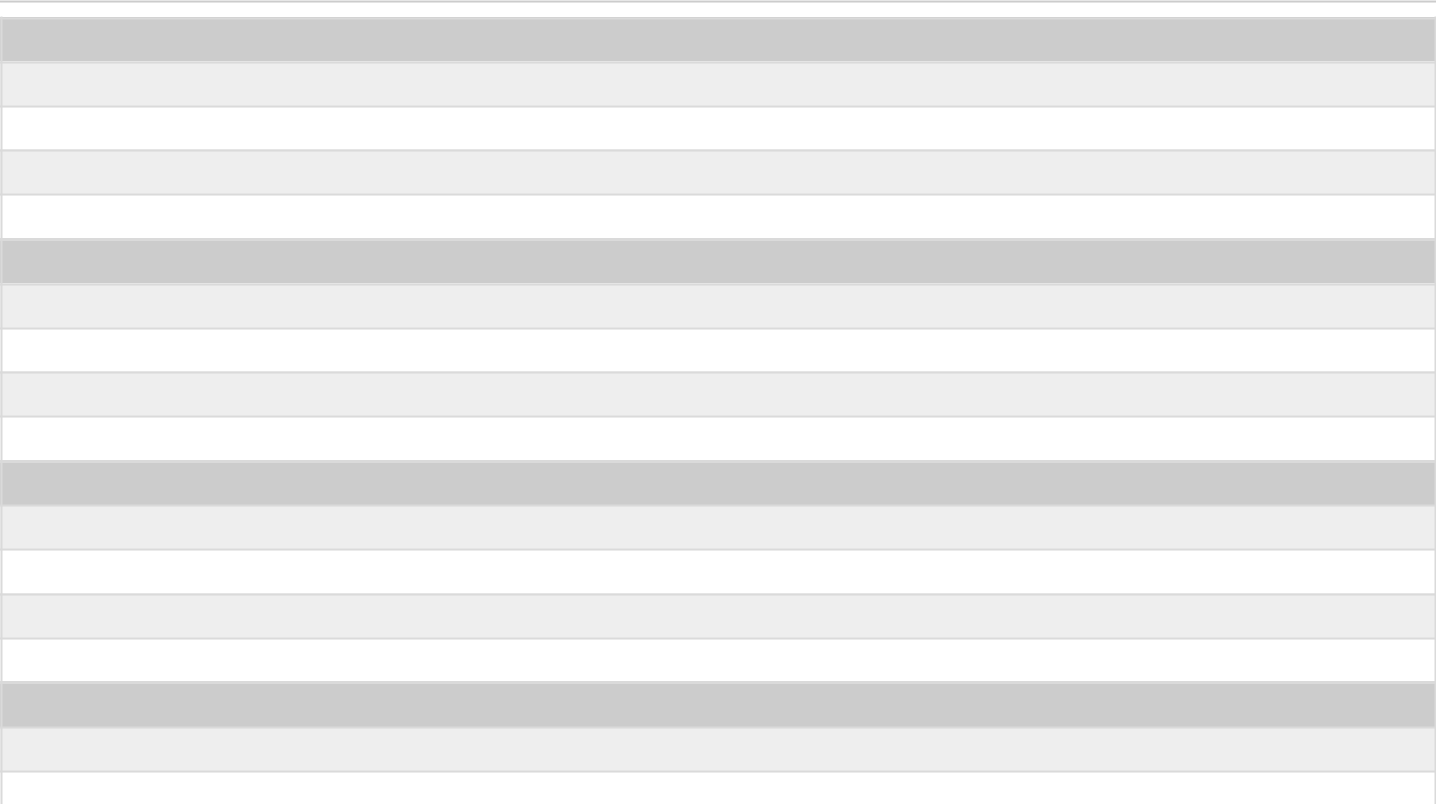
Check references for details on how to solve this problem.

**References**



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

**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial



Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

 **Password type input with auto-complete enabled**



Severity **Informational**

|  |  |
| --- | --- |
| Reported by module | /Crawler/12-Crawler\_Password\_Input\_Autocomplete.js |

**Description**



When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

**Impact**



Possible sensitive information disclosure.

**Recommendation**



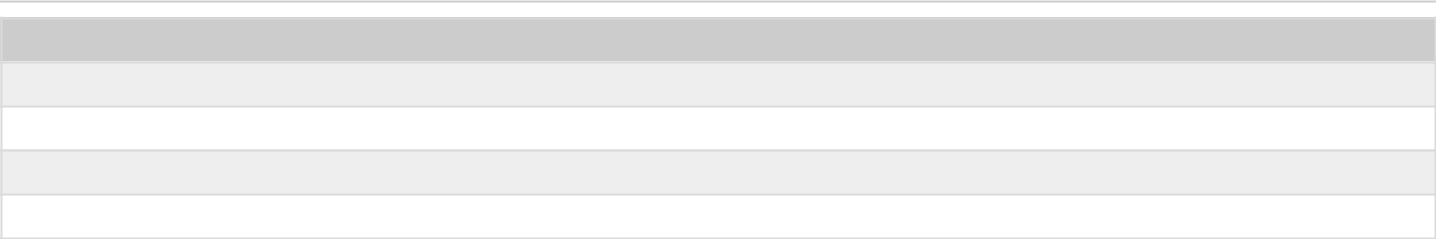
The password auto-complete should be disabled in sensitive applications.

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



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

**Affected items**



**Web Server**

Details

Not available in the free trial

Request headers

Not available in the free trial

**Scanned items (coverage report)**



https://thesisbloodwebsite.000webhostapp.com/

https://thesisbloodwebsite.000webhostapp.com/admin.php https://thesisbloodwebsite.000webhostapp.com/bloodlist https://thesisbloodwebsite.000webhostapp.com/bloodlist/aheader.php https://thesisbloodwebsite.000webhostapp.com/bloodlist/Apositive.php

https://thesisbloodwebsite.000webhostapp.com/bloodlist/logout.php https://thesisbloodwebsite.000webhostapp.com/donor-list.php https://thesisbloodwebsite.000webhostapp.com/donor-reg.php https://thesisbloodwebsite.000webhostapp.com/entry.php https://thesisbloodwebsite.000webhostapp.com/icons https://thesisbloodwebsite.000webhostapp.com/index.php https://thesisbloodwebsite.000webhostapp.com/logout.php https://thesisbloodwebsite.000webhostapp.com/ngo-list.php https://thesisbloodwebsite.000webhostapp.com/out-stock-blood-list.php https://thesisbloodwebsite.000webhostapp.com/stock-blood-list.php