



**Developer**

**Report**

**Acunetix Security Audit**

18 February 2020

Generated by Acunetix

**Scan of** [**http://rimonrony.info**](http://rimonrony.info/)

# Scan details

|  |  |
| --- | --- |
| **Scan information** | |
| **Start time** | **18/02/2020, 04:45:54** |
| **Start url** | [**http://rimonrony.info**](http://rimonrony.info/) |
| **Host** | [**http://rimonrony.info**](http://rimonrony.info/) |
| **Scan time** | **5 minutes, 15 seconds** |
| **Profile** | **Full Scan** |

Threat level

Acunetix Threat Level 1

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

Alerts distribution

|  |  |
| --- | --- |
| **Total alerts found** | **2** |
| **High** | **0** |
| **Medium** | **0** |
| **Low** | **1** |
| **Informational** | **1** |

# Alerts summary

 Clickjacking: X-Frame-Options header missing

|  |  |  |
| --- | --- | --- |
| **Classification** | | |
| **CVSS2** | **Base Score: 6.8**  **Access Vector: Network\_accessible Access Complexity: Medium Authentication: None**  **Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not\_defined Remediation Level: Not\_defined Report Confidence: Not\_defined**  **Availability Requirement: Not\_defined Collateral Damage Potential: Not\_defined Confidentiality Requirement: Not\_defined Integrity Requirement: Not\_defined Target Distribution: Not\_defined** | |
| **CWE** | **CWE-693** | |
| **Affected items** | | **Variation** |
| **Web Server** | | **1** |

 Email address found

|  |  |  |
| --- | --- | --- |
| **Classification** | | |
| **CVSS2** | **Base Score: 0.0**  **Access Vector: Network\_accessible Access Complexity: Low Authentication: None**  **Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not\_defined Remediation Level: Not\_defined Report Confidence: Not\_defined**  **Availability Requirement: Not\_defined Collateral Damage Potential: Not\_defined Confidentiality Requirement: Not\_defined Integrity Requirement: Not\_defined Target Distribution: Not\_defined** | |
| **CVSS3** | **Base Score: 0.0**  **Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None** | |
| **CWE** | **CWE-200** | |
| **Affected items** | | **Variation** |
| **Web Server** | | **1** |

# Alerts details

 **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) Clickjacking (<http://en.wikipedia.org/wiki/Clickjacking)>

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

Affected items

|  |
| --- |
| **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](mailto:myname@mydomain.com) and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

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

Affected items

|  |
| --- |
| **Web Server** |
| **Details** |
| **Not available in the free trial** |
| **Request headers** |
| **Not available in the free trial** |

# Scanned items (coverage report)

<http://rimonrony.info/> <http://rimonrony.info/image> <http://rimonrony.info/labhome.php>