Acunetix
by Invicti

# Developer Report

Acunetix Security Audit

2022-06-08

Generated by Acunetix

# Scan of localhost:7056

## Scan details

| Scan information | |
|---|---|
| Start time | 2022-06-01T22:46:27.279328-07:00 |
| Start url | https://localhost:7056 |
| Host | localhost:7056 |
| Scan time | 14 minutes, 59 seconds |
| Profile | Full Scan |
| Server information | Kestrel |
| Responsive | True |
| Server OS | Unknown |
| Application build | 14.7.220228146 |

### 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 | 8 |
|---|---|
| High | 1 |
| Medium | 3 |
| Low | 3 |
| Informational | 1 |

## Alerts summary

### TLS 1.0 enabled

| Classification | |
|---|---|
| CVSS3 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N<br>Base Score: 5.4<br>Attack Vector: Network<br>Attack Complexity: High<br>Privileges Required: None<br>User Interaction: None<br>Scope: Changed<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CVSS2 | Base Score: 5.8<br>Access Vector: Network_accessible<br>Access Complexity: Medium<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: Partial<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-326 |

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

### TLS 1.1 enabled

| Classification | |
|---|---|
| CVSS3 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N<br>Base Score: 5.4<br>Attack Vector: Network<br>Attack Complexity: High<br>Privileges Required: None<br>User Interaction: None<br>Scope: Changed<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |

| | |
|---|---|
| CVSS2 | Base Score: 5.8<br>Access Vector: Network_accessible<br>Access Complexity: Medium<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: Partial<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-326 |

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

### TLS/SSL Sweet32 attack

| Classification | |
|---|---|
| CVSS3 | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N<br>Base Score: 7.5<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: High<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 4.3<br>Access Vector: Network_accessible<br>Access Complexity: Medium<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CVE | CVE-2016-2183 |
| CVE | CVE-2016-6329 |
| CWE | CWE-310 |

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

### TLS/SSL Weak Cipher Suites

| Classification |
|---|

| | |
|---|---|
| CVSS3 | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N<br>Base Score: 6.5<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: Low<br>Integrity Impact: Low<br>Availability Impact: None |
| CVSS2 | Base Score: 3.3<br>Access Vector: Local_access<br>Access Complexity: Medium<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: Partial<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-310 |

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

### Clickjacking: X-Frame-Options header

| Classification | |
|---|---|
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N<br>Base Score: 5.8<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Changed<br>Confidentiality Impact: None<br>Integrity Impact: Low<br>Availability Impact: None |
| CVSS2 | Base Score: 4.3<br>Access Vector: Network_accessible<br>Access Complexity: Medium<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: Partial<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |

| CWE | CWE-1021 | |
|---|---|---|
| Affected items | | Variation |
| Web Server | | 1 |

### HTTP Strict Transport Security (HSTS) not implemented

| Classification | |
|---|---|
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-16 |

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

### Sensitive pages could be cached

| Classification | |
|---|---|
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N<br>Base Score: 5.3<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: Low<br>Integrity Impact: None<br>Availability Impact: None |

| | |
|---|---|
| CVSS2 | Base Score: 5.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-200 |

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

### Content Security Policy (CSP) not implemented

| Classification | |
|---|---|
| CVSS3 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N<br>Base Score: 0.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: Required<br>Scope: Changed<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None |
| CVSS2 | Base Score: 0.0<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: None<br>Integrity Impact: None<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CWE | CWE-1021 |

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

## Alerts details

### TLS 1.0 enabled

| | |
|---|---|
| Severity | **High** |
| Reported by module | /Scripts/PerServer/SSL_Audit.script |

#### Description

The web server supports encryption through TLS 1.0, which was formally deprecated in March 2021 as a result of inherent security issues. In addition, TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

#### Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

#### Recommendation

It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

#### References

RFC 8996: Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)
Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)
PCI 3.1 and TLS 1.2 (Cloudflare Support) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

#### Affected items

| **Web Server** |
|---|
| Details |
| The SSL server (port: 7056) encrypts traffic using TLSv1.0. |
| Request headers |

### TLS 1.1 enabled

| | |
|---|---|
| Severity | **Medium** |
| Reported by module | /Scripts/PerServer/SSL_Audit.script |

#### Description

The web server supports encryption through TLS 1.1, which was formally deprecated in March 2021 as a result of inherent security issues. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

### Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

### Recommendation

It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.

### References

RFC 8996: Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)
Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)
PCI 3.1 and TLS 1.2 (Cloudflare Support) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

### Affected items

| Web Server |
| --- |
| Details |
| The SSL server (port: 7056) encrypts traffic using TLSv1.1. |
| Request headers |

## TLS/SSL Sweet32 attack

| | |
| --- | --- |
| Severity | **Medium** |
| Reported by module | /Scripts/PerServer/SSL_Audit.script |

### Description

The Sweet32 attack is a SSL/TLS vulnerability that allows attackers to compromise HTTPS connections using 64-bit block ciphers.

### Impact

An attacker may intercept HTTPS connections between vulnerable clients and servers.

### Recommendation

Reconfigure the affected SSL/TLS server to disable support for obsolete 64-bit block ciphers.

### References

Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN (https://sweet32.info/)
CVE-2016-2183 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2183)
CVE-2016-6329 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6329)

### Affected items

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

Cipher suites susceptible to Sweet32 attack (TLS1.0 on port 7056):

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Cipher suites susceptible to Sweet32 attack (TLS1.1 on port 7056):

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Cipher suites susceptible to Sweet32 attack (TLS1.2 on port 7056):

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Request headers

## TLS/SSL Weak Cipher Suites

| | |
|---|---|
| Severity | **Medium** |
| Reported by module | /Scripts/PerServer/SSL_Audit.script |

### Description

The remote host supports TLS/SSL cipher suites with weak or insecure properties.

### Impact

### Recommendation

Reconfigure the affected application to avoid use of weak cipher suites.

### References

OWASP: TLS Cipher String Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html)
OWASP: Transport Layer Protection Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html)
Mozilla: TLS Cipher Suite Recommendations (https://wiki.mozilla.org/Security/Server_Side_TLS)
SSLlabs: SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
RFC 9155: Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2 (https://datatracker.ietf.org/doc/html/rfc9155)

### Affected items

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

Weak TLS/SSL Cipher Suites: (offered via TLS1.0 on port 7056):

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)

Weak TLS/SSL Cipher Suites: (offered via TLS1.1 on port 7056):

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)

Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 7056):

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)

Request headers

## Clickjacking: X-Frame-Options header

| | |
|---|---|
| Severity | **Low** |
| Reported by module | /httpdata/X_Frame_Options_not_implemented.js |

### Description

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

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

### Impact

The impact depends on the affected web application.

### Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

### References

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)
Clickjacking (https://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)
Frame Buster Buster (https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

### Affected items

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

Paths without secure XFO header:

- https://localhost:7056/swagger/index.html

Request headers

```
GET /swagger/index.html HTTP/1.1

Referer: https://localhost:7056/swagger/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: localhost:7056

Connection: Keep-alive
```

## HTTP Strict Transport Security (HSTS) not implemented

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

### Description

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

### Impact

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

### Recommendation

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

### References

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

### Affected items

**Web Server**

Details

URLs where HSTS is not enabled:

- https://localhost:7056/swagger/index.html

Request headers

```
GET /swagger/index.html HTTP/1.1

Referer: https://localhost:7056/swagger/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: localhost:7056

Connection: Keep-alive
```

## Sensitive pages could be cached

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

### Description

One or more pages contain possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.

### Impact

Possible sensitive information disclosure.

### Recommendation

Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header.

### Affected items

**Web Server**

Details

List of pages that could be cached:

- https://localhost:7056/swagger/index.html?password=g00dPa$$w0rD&username=KfnqDuxw
- https://localhost:7056/swagger/v1/swagger.json?password=g00dPa$$w0rD&username=KfnqDuxw

Request headers

```
GET /swagger/index.html?password=g00dPa%24%24w0rD&username=KfnqDuxw HTTP/1.1

Referer: https://localhost:7056/swagger/index.html

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: localhost:7056

Connection: Keep-alive
```

## Content Security Policy (CSP) not implemented

| Severity | **Informational** |
| --- | --- |
| Reported by module | /httpdata/CSP_not_implemented.js |

### Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

### Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

### Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

### References

Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

### Affected items

| Web Server |
| --- |
| Details |
| Paths without CSP header:<br>• https://localhost:7056/swagger/index.html |
| Request headers |

```
GET /swagger/index.html HTTP/1.1

Referer: https://localhost:7056/swagger/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: localhost:7056

Connection: Keep-alive
```

## Scanned items (coverage report)

https://localhost:7056/
https://localhost:7056/_framework/
https://localhost:7056/_framework/aspnetcore-browser-refresh.js
https://localhost:7056/_framework/blazor-hotreload
https://localhost:7056/_framework/clear-browser-cache
https://localhost:7056/_vs/
https://localhost:7056/_vs/browserLink
https://localhost:7056/swagger/
https://localhost:7056/swagger/index.html
https://localhost:7056/swagger/swagger-ui-bundle.js
https://localhost:7056/swagger/swagger-ui-standalone-preset.js
https://localhost:7056/swagger/swagger-ui.css
https://localhost:7056/swagger/v1/
https://localhost:7056/swagger/v1/Currencies/
https://localhost:7056/swagger/v1/Currencies/fiat/
https://localhost:7056/swagger/v1/Notification/
https://localhost:7056/swagger/v1/Notification/bitpay/
https://localhost:7056/swagger/v1/Notification/coinbase/
https://localhost:7056/swagger/v1/Notification/coinpayments/
https://localhost:7056/swagger/v1/Notification/coinqvest/
https://localhost:7056/swagger/v1/Payment
https://localhost:7056/swagger/v1/Payment/
https://localhost:7056/swagger/v1/swagger.json
https://localhost:7056/swagger/v1/swagger.yaml