netsparker

6/1/2023 6:04:15 PM (UTC+05:30)

ISO 27001 Compliance Report

http://localhost:8000/

Scan Time	: 6/1/2023 6:00:53 PM (UTC+05:30)
Scan Duration	: 00:00:00:27
Total Requests	: 419
Average Speed	: 15.0r/s

Risk Level:
MEDIUM

Explanation

This report is generated based on ISO 27001 classification.

2
IDENTIFIED

0
CONFIRMED

0
CRITICAL

0
HIGH

1
MEDIUM

0
LOW

1
BEST PRACTICE

0
INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	1
Low	0
Best Practice	1
Information	0
TOTAL	**2**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	0
Low	0
Best Practice	0
Information	0
TOTAL	**0**

Vulnerabilities By ISO27001

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A.14				
1.3 - PROTECTING APPLICATION SERVICES TRANSACTIONS				
	SSL/TLS Not Implemented	GET	https://localhost/	MEDIUM
2.5 - SECURE SYSTEM ENGINEERING				
	Missing X-XSS-Protection Header	GET	http://localhost:8000/	BEST PRACTICE

1. SSL/TLS Not Implemented

MEDIUM | 1

Netsparker detected that SSL/TLS is not implemented.

Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Vulnerabilities

1.1. https://localhost/

Certainty

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1   **Total Bytes Received** : 27   **Body Length** : 0   **Is Compressed** : No

```
[NETSPARKER] SSL Connection
```

Remedy

We suggest that you implement SSL/TLS properly, for example by using the Certbot toolprovided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

CLASSIFICATION

ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

2. Missing X-XSS-Protection Header

BEST PRACTICE | 1

Netsparker detected a missing `X-XSS-Protection`header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

2.1. http://localhost:8000/

Certainty

Request

```
GET / HTTP/1.1
Host: localhost:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 47.5462 **Total Bytes Received** : 154 **Body Length** : 22 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
server: uvicorn
content-length: 22
content-type: application/json
date: Thu, 01 Jun 2023 12:30:55 GMT

{"detail":"Not Found"}
```

Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

-
  ```
  X-XSS-Protection: 1; mode=block
  ```

External References

- Internet Explorer 8 Security Features - MSDN
- X-XSS-Protection HTTP Header
- Internet Explorer 8 XSS Filter

CLASSIFICATION

ISO27001	A.14.2.5

Show Scan Detail

Enabled Security Checks : Apache Struts S2-045 RCE,
Apache Struts S2-046 RCE,
BREACH Attack,
Code Evaluation,
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
Content Security Policy,
Content-Type Sniffing,
Cookie,
Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Drupal Remote Code Execution,
Expect Certificate Transparency (Expect-CT),
Expression Language Injection,
File Upload,

		Header Analyzer, Heartbleed, HSTS, HTML Content, HTTP Header Injection, HTTP Methods, HTTP Status, HTTP.sys (CVE-2015-1635), IFrame Security, Insecure JSONP Endpoint, Insecure Reflected Content, JavaScript Libraries, Local File Inclusion, Login Page Identifier, Mixed Content, Open Redirection, Referrer Policy, Reflected File Download, Remote File Inclusion, Remote File Inclusion (Out of Band), Reverse Proxy Detection, RoR Code Execution, Server-Side Request Forgery (DNS), Server-Side Request Forgery (Pattern Based), Server-Side Template Injection, Signatures, SQL Injection (Blind), SQL Injection (Boolean), SQL Injection (Error Based), SQL Injection (Out of Band), SSL, Static Resources (All Paths), Static Resources (Only Root Path), Unicode Transformation (Best-Fit Mapping), WAF Identifier, Web App Fingerprint, Web Cache Deception, WebDAV, Windows Short Filename, XML External Entity, XML External Entity (Out of Band)
URL Rewrite Mode	:	Heuristic
Detected URL Rewrite Rule(s)	:	None
Excluded URL Patterns	:	(log|sign)\-?(out|off) exit endsession gtm\.js WebResource\.axd ScriptResource\.axd

Authentication	: None
Scheduled	: No
Additional Website(s)	: None

This report created with 5.8.1.28119-master-bca4e4e
https://www.netsparker.com