invicti

06/05/2025 14:57:31 (UTC+07:00)

OWASP Top 10 2021 Report

https://192.168.92.213:5001/

Scan Time	: 06/05/2025 14:34:18 (UTC+07:00)
Scan Duration	: 00:00:22:39
Total Requests	: 41.517
Average Speed	: 30,5r/s

Risk Level:
MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2021 classification.

3	1	0
IDENTIFIED	CONFIRMED	CRITICAL

0	1	2
HIGH	MEDIUM	LOW

0	0
BEST PRACTICE	INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	1
Low	2
Best Practice	0
Information	0
TOTAL	**3**

Confirmed Vulnerabilities

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

Vulnerabilities By OWASP Top Ten 2021

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A02 - CRYPTOGRAPHIC FAILURES				
	SSL Untrusted Root Certificate	GET	https://192.168.92.213:5001/register_candidate	MEDIUM
A05 - SECURITY MISCONFIGURATION				
	Version Disclosure (Python)	GET	https://192.168.92.213:5001/	LOW
	Version Disclosure (Werkzeug Python WSGI Library)	GET	https://192.168.92.213:5001/	LOW

1. SSL Untrusted Root Certificate

MEDIUM 1 | CONFIRMED 1

Invicti Standard detected that the SSL Certificate is not signed by the trusted root.

Impact

It can impact both website and the users:

- Warning error messages displayed by browsers when visiting the site
- Personal information at risk from man-in-the-middle attacks
- Reduction in trust as the site becomes insecure
- Ability for an attacker to create identical phishing website

Vulnerabilities

1.1. https://192.168.92.213:5001/register_candidate

CONFIRMED

Remedy

The process of fixing untrusted root certificate issues varies depending on the host or the certificate authority used. Please refer to the corresponding documentation.

External References

- Certificate Not Trusted

CLASSIFICATION

OWASP Top Ten 2021	A02

CVSS 3.0 SCORE	
Base	5,3 (Medium)
Temporal	5,3 (Medium)
Environmental	5,3 (Medium)

CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS 3.1 SCORE	
Base	5,3 (Medium)
Temporal	5,3 (Medium)
Environmental	5,3 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS 4.0 Score
5,3 / Medium

CVSS 4.0 Score

Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low
Exploitation	High
Security requirements	Medium

CVSS Vector String

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

2. Version Disclosure (Python)

LOW | 1

Invicti Standard identified a version disclosure (Python) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Python.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

2.1. https://192.168.92.213:5001/

Extracted Version

- 3.13.3

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: 192.168.92.213:5001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: session=.eJwlzDsOwyAMANC7eM6AcZQPW7v2EMgQI6EKtzJkinr3Vur2pndBfIs1VtEBYdgpE-
RuJY7XUxQCFLekFXPZidAJenKEG9Mmsu6Yivd5XuacECY4u1isBwT8W7nJb7gdreqjDr6LdW4Mny-
XNiU9.aBm7fQ.7q5TIxAor3q2T74ktO25MkcsX4U
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.265 Safari/537.36
```

Response

Response Time (ms) : 4,119
Total Bytes Received : 10967
Body Length : 9986
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: session=.eJwlzDsOwyAMANC7eM6AcZQPW7v2EMgQI6EKtzJkinr3Vur2pndBfIs1VtEBYdgpE-
RuJY7XUxQCFLekFXPZidAJenKEG9Mmsu6Yivd5XuacECY4u1isBwT8W7nJb7gdreqjDr6LdW4Mny-
XNiU9.aBm7fg.V3RLCKFWHOHLk3iosa5Lrnm2WfQ; Expires=Fri, 06 Jun 2025 07:34:22 GMT; Secure; HttpOnly;
Path=/; SameSite=Lax
Server: Werkzeug/3.1.3 Python/3.13.3
Server: Server
X-Content-Type-Options: nosniff
Connection: close
Content-Security-Policy: default-src 'self'; script-src 'self' https://cdn.jsdelivr.net 'unsafe-
inline'; style-src 'self' https://cdn.jsdelivr.net 'unsafe-inline'; img-src 'self' data:; font-src
'self' https://cdn.jsdelivr.net; connect-src 'self'; object-src 'none'; frame-ancestors 'none'; form-
action 'self';
Content-Length: 9986
X-Frame-Options: DENY
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Referrer-Policy: strict-origin-when-cross-origin
Content-Type: text/html; charset=utf-8
Date: Tue, 06 May 2025 07
…
E-RuJY7XUxQCFLekFXPZidAJenKEG9Mmsu6Yivd5XuacECY4u1isBwT8W7nJb7gdreqjDr6LdW4Mny-
XNiU9.aBm7fg.V3RLCKFWHOHLk3iosa5Lrnm2WfQ; Expires=Fri, 06 Jun 2025 07:34:22 GMT; Secure; HttpOnly;
Path=/; SameSite=Lax
Server: Werkzeug/3.1.3 Python/3.13.3

Server: Server
X-Content-Type-Options: nosniff
Connection: close
Content-Security-Policy: default-src 'self'; script-src 'self' https://cdn.jsdelivr.net 'unsafe-
inline'; style-src 'self' https://c
…
```

Remedy

Configure your web server to prevent information leakage from the `SERVER`header of its HTTP response.

CLASSIFICATION

OWASP Top Ten 2021	A05

3. Version Disclosure (Werkzeug Python WSGI Library)

LOW | 1

Invicti Standard identified a version disclosure (Werkzeug) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Werkzeug.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

3.1. https://192.168.92.213:5001/

Extracted Version

- 3.1.3

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: 192.168.92.213:5001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: session=.eJwlzDsOwyAMANC7eM6AcZQPW7v2EMgQI6EKtzJkinr3Vur2pndBfIs1VtEBYdgpE-
RuJY7XUxQCFLekFXPZidAJenKEG9Mmsu6Yivd5XuacECY4u1isBwT8W7nJb7gdreqjDr6LdW4Mny-
XNiU9.aBm7fQ.7q5TIxAor3q2T74ktO25MkcsX4U
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.265 Safari/537.36
```

Response

Response Time (ms) : 4,119
Total Bytes Received : 10967
Body Length : 9986
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: session=.eJwlzDsOwyAMANC7eM6AcZQPW7v2EMgQI6EKtzJkinr3Vur2pndBfIs1VtEBYdgpE-
RuJY7XUxQCFLekFXPZidAJenKEG9Mmsu6Yivd5XuacECY4u1isBwT8W7nJb7gdreqjDr6LdW4Mny-
XNiU9.aBm7fg.V3RLCKFWHOHLk3iosa5Lrnm2WfQ; Expires=Fri, 06 Jun 2025 07:34:22 GMT; Secure; HttpOnly;
Path=/; SameSite=Lax
Server: Werkzeug/3.1.3 Python/3.13.3
Server: Server
X-Content-Type-Options: nosniff
Connection: close
Content-Security-Policy: default-src 'self'; script-src 'self' https://cdn.jsdelivr.net 'unsafe-
inline'; style-src 'self' https://cdn.jsdelivr.net 'unsafe-inline'; img-src 'self' data:; font-src
'self' https://cdn.jsdelivr.net; connect-src 'self'; object-src 'none'; frame-ancestors 'none'; form-
action 'self';
Content-Length: 9986
X-Frame-Options: DENY
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Referrer-Policy: strict-origin-when-cross-origin
Content-Type: text/html; charset=utf-8
Date: Tue, 06 May 2025 07
…
E-RuJY7XUxQCFLekFXPZidAJenKEG9Mmsu6Yivd5XuacECY4u1isBwT8W7nJb7gdreqjDr6LdW4Mny-
XNiU9.aBm7fg.V3RLCKFWHOHLk3iosa5Lrnm2WfQ; Expires=Fri, 06 Jun 2025 07:34:22 GMT; Secure; HttpOnly;
Path=/; SameSite=Lax
Server: Werkzeug/3.1.3 Python/3.13.3

Server: Server
X-Content-Type-Options: nosniff
Connection: close
Content-Security-Policy: default-src 'self'; script-src 'self' https://cdn.jsdelivr.net 'unsafe-
inline'; style-src 'self' https://c
…
```

Remedy

Configure your application to prevent information leakage from the SERVER header of its HTTP response.

External References

- Werkzeug's official website

CLASSIFICATION

OWASP Top Ten 2021	A05

Show Scan Detail

Enabled Security Checks	:	ActiveMQ OpenWire RCE, Apache Struts S2-045 RCE, Apache Struts S2-046 RCE, Code Evaluation, Code Evaluation (Out of Band), Command Injection, Command Injection (Blind), Content Security Policy, Content-Type Sniffing, Cookie, Cross-Origin Resource Sharing (CORS), 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, Expression Language Injection, File Upload, GraphQL Library Detection, 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, JSON Web Token, Local File Inclusion,

		Log4j Code Evaluation (Out of Band), **Login Page Identifier,** **Malware Analyzer,** **Mixed Content,** **MongoDB Injection (Blind),** **MongoDB Injection (Boolean),** **MongoDB Injection (Error Based),** **MongoDB Injection (Operator),** **Open Redirection,** **Oracle EBS RCE,** **Oracle WebLogic Remote Code Execution,** **Referrer Policy,** **Reflected File Download,** **RegreSSHion Attack,** **Remote File Inclusion,** **Remote File Inclusion (Out of Band),** **Reverse Proxy Detection,** **RoR Code Execution,** **Security Assertion Markup Language (SAML),** **Sensitive Data,** **Server-Side Request Forgery (DNS),** **Server-Side Request Forgery (Pattern Based),** **Server-Side Template Injection,** **Signatures,** **Software Composition Analysis (SCA),** **Spring4Shell Remote Code Execution,** **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),** **TorchServe Management,** **Unicode Transformation (Best-Fit Mapping),** **VmWare Aria RCE,** **WAF Identifier,** **Web App Fingerprint,** **Web Cache Deception,** **WebDAV,** **Windows Short Filename,** **Wordpress Plugin Detection,** **Wordpress Theme Detection,** **XML External Entity,** **XML External Entity (Out of Band)**
URL Rewrite Mode	:	**Heuristic**
Detected URL Rewrite Rule(s)	:	**None**

Excluded URL Patterns	:	**gtm\.js** **WebResource\.axd** **ScriptResource\.axd**
Authentication	:	**Form Authentication**
Authentication Profile	:	**None**
Scheduled	:	**No**
Additional Website(s)	:	**None**