Website Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the DEEP scanner can do

Perform in-depth website scanning and discover high risk vulnerabilities.

Testing areas	Light scan	Deep scan
Website fingerprinting	✔	✔
Version-based vulnerability detection	✔	✔
Common configuration issues	✔	✔
SQL injection	–	✔
Cross-Site Scripting	–	✔
Local/Remote File Inclusion	–	✔
Remote command execution	–	✔
Discovery of sensitive files	–	✔

✔ **https://mi-linux.wlv.ac.uk/~2213214/fullstackassignment.php**

The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:
High

Risk ratings:

Critical:	0
High:	1
Medium:	0
Low:	1
Info:	37

Scan information:

Start time:	Nov 25, 2025 / 05:13:39 UTC+02
Finish time:	Nov 25, 2025 / 05:14:04 UTC+02
Scan duration:	25 sec
Tests performed:	39/39
Scan status:	Finished

Findings

Vulnerabilities found for http_server 2.4.52

port 443/tcp

CVE	CVSS	EPSS Score	EPSS Percentile	Summary
CVE-2024-38476	9.8	0.03452	0.87031	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue.

CVE-2024-38474	9.8	0.0081	0.73471	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
CVE-2023-25690	9.8	0.67037	0.9847	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.
CVE-2022-31813	9.8	0.0004	0.11966	Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
CVE-2022-23943	9.8	0.68553	0.98531	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

Details

Risk description:
The risk is that an attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Since the vulnerabilities were discovered using only version-based testing, the risk level for this finding will not exceed 'high' severity. Critical risks will be assigned to vulnerabilities identified through accurate active testing methods.

Recommendation:
In order to eliminate the risk of these vulnerabilities, we recommend you check the installed software version and upgrade to the latest version.

Classification:
EPSS score : 0.68553
EPSS percentile : 0.98531
CISA KEV: False
CVE : CVE-2024-38476, CVE-2024-38474, CVE-2023-25690, CVE-2022-31813, CVE-2022-23943
CVSS V3 : 9.8
CWE : CWE-1035

Server software and technology found

UNCONFIRMED

port 443/tcp

Software / Version	Category
Apache HTTP Server 2.4.52	Web servers
Sectigo	SSL/TLS certificate authorities
Basic	Security

Ubuntu	Operating systems

Details

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Login Interface Found

CONFIRMED

port 443/tcp

URL	Evidence
https://mi-linux.wlv.ac.uk/~2213214/fullstackassignment.php	HTTP authentication found in header `'WWW-Authenticate: Basic realm="System Users Login"'` Request / Response

Details

Risk description:
The risk is that an attacker could use this interface to mount brute force attacks against known passwords and usernames combinations leaked throughout the web.

Recommendation:
Ensure each interface is not bypassable using common knowledge of the application or leaked credentials using occasional password audits.

References:
https://pentest-tools.com/network-vulnerability-scanning/password-auditor
http://capec.mitre.org/data/definitions/16.html

Security.txt file is missing

CONFIRMED

port 443/tcp

URL
Missing: https://mi-linux.wlv.ac.uk/.well-known/security.txt

Details

Risk description:
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

- Website is accessible.
- Nothing was found for client access policies.
- Nothing was found for robots.txt file.
- Nothing was found for use of untrusted certificates.
- Nothing was found for enabled HTTP debug methods.
- Nothing was found for enabled HTTP OPTIONS method.
- Nothing was found for secure communication.
- Nothing was found for directory listing.
- Nothing was found for passwords submitted unencrypted.
- Nothing was found for error messages.
- Nothing was found for debug messages.
- Nothing was found for code comments.
- Nothing was found for missing HTTP header - Strict-Transport-Security.
- Nothing was found for missing HTTP header - Content Security Policy.
- Nothing was found for missing HTTP header - X-Content-Type-Options.
- Nothing was found for missing HTTP header - Referrer.
- Nothing was found for passwords submitted in URLs.
- Nothing was found for domain too loose set for cookies.
- Nothing was found for mixed content between HTTP and HTTPS.

Nothing was found for cross domain file inclusion.

Nothing was found for internal error code.

Nothing was found for HttpOnly flag of cookie.

Nothing was found for Secure flag of cookie.

Nothing was found for secure password submission.

Nothing was found for sensitive data.

Nothing was found for unsafe HTTP header Content Security Policy.

Nothing was found for OpenAPI files.

Nothing was found for file upload.

Nothing was found for SQL statement in request parameter.

Nothing was found for password returned in later response.

Nothing was found for Path Disclosure.

Nothing was found for Session Token in URL.

Nothing was found for API endpoints.

Nothing was found for emails.

Nothing was found for missing HTTP header - Rate Limit.

Scan coverage information

List of tests performed (39/39)

- Test initial connection
- Scanned for login interfaces
- Scanned for website technologies
- Scanned for version-based vulnerabilities of server-side software
- Scanned for client access policies
- Scanned for robots.txt file

- Scanned for absence of the security.txt file
- Scanned for use of untrusted certificates
- Scanned for enabled HTTP debug methods
- Scanned for enabled HTTP OPTIONS method
- Scanned for secure communication
- Scanned for directory listing
- Scanned for passwords submitted unencrypted
- Scanned for error messages
- Scanned for debug messages
- Scanned for code comments
- Scanned for missing HTTP header - Strict-Transport-Security
- Scanned for missing HTTP header - Content Security Policy
- Scanned for missing HTTP header - X-Content-Type-Options
- Scanned for missing HTTP header - Referrer
- Scanned for passwords submitted in URLs
- Scanned for domain too loose set for cookies
- Scanned for mixed content between HTTP and HTTPS
- Scanned for cross domain file inclusion
- Scanned for internal error code
- Scanned for HttpOnly flag of cookie
- Scanned for Secure flag of cookie
- Scanned for secure password submission
- Scanned for sensitive data
- Scanned for unsafe HTTP header Content Security Policy
- Scanned for OpenAPI files
- Scanned for file upload
- Scanned for SQL statement in request parameter
- Scanned for password returned in later response
- Scanned for Path Disclosure
- Scanned for Session Token in URL
- Scanned for API endpoints
- Scanned for emails
- Scanned for missing HTTP header - Rate Limit

Scan parameters

target:	https://mi-linux.wlv.ac.uk/~2213214/fullstackassignment.php
scan_type:	Light
authentication:	False

Scan stats

Unique Injection Points Detected:	1
URLs spidered:	1
Total number of HTTP requests:	10
Average time until a response was received:	65ms