CyberSec Pro
cyber-sec-pro.com

Technical Report — Sample

Technical Report

REPORT DATE	**SCANS PERFORMED**
2026-11-12 01:38 UTC	3 scan(s)
TOTAL FINDINGS	**RISK LEVEL**
21	Critical

CONFIDENTIAL — AUTHORIZED RECIPIENTS ONLY

Generated by CyberSec Pro | cyber-sec-pro.com

© 2026 CyberSec Pro. All rights reserved.

Table of Contents

01 Risk Assessment

02 Executive Summary

03 Action plan

04 Scan results and findings

05 Methodology

06 Content digest

Technical Report — Sample

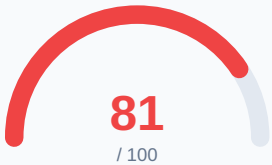
CyberSec Pro cyber-sec-pro.com

Technical Report

Generated: 2026-11-12 01:38 UTC Scans: 3 Findings: 21 **Risk: Critical**

About this sample. This is a sample. Its three scans are real: they were run through CyberSec Pro on 12 November 2026 against scanme.nmap.org and testasp.vulnweb.com, hosts their owners keep online for people to practise on. The tool output is shown as it was recorded and the findings are what the product derived from it. Nothing was added or removed.

Risk Assessment



Overall Risk Score: 81/100

The risk score is calculated based on the severity and quantity of findings discovered during the assessment.

CRITICAL	HIGH	MEDIUM	LOW / INFO
1	0	1	19
4.8%	0.0%	4.8%	90.5%

Executive Summary

The assessment covered **3** target(s) with: **nikto, nmap, sqlmap**. Targets scanned: `http://testasp.vulnweb.com/showforum.asp?id=0`, `scanme.nmap.org`, `testasp.vulnweb.com`.

Fix first: **SQL injection in id (GET)** (critical, 1 target); **SSH** (medium, 1 target). The action plan lists every issue with its first step.

This security assessment was conducted on **2026-11-12** covering **3 scan(s)** across the target infrastructure. A total of **21 finding(s)** were identified, including **1 critical**, **0 high**, **1**

medium, and **17 low** severity issues. Overall risk level: **Critical**.

Action plan

Worst first. Each row is one issue, with every place it was found; the full steps are with each finding under Scan results and findings. Informational findings are left out.

#	FIX BY	ISSUE	WHERE	FIRST STEP
1	CRITICAL Now	**SQL injection in id (GET)**	http://testasp.vulnweb.com/showforum.asp?id=0	Find the query that uses the named parameter and rewrite it as a parameterized query (prepared statement). Never build SQL by joining strings with request values.
2	MEDIUM Within 30 days	**SSH**	scanme.nmap.org, port 22	Restrict SSH to known management addresses with a firewall rule or security group.
3	LOW Next maintenance	**/: Cookie ASPSESSIONIDCCDSSDSA created without the httponly flag.**	testasp.vulnweb.com	Set HttpOnly on every session cookie.
4	LOW Next maintenance	**/: Default IIS server content.**	testasp.vulnweb.com	Remove the default site or page, and the sample applications, manuals and test scripts that came with the server.
5	LOW Next maintenance	**/: Suggested security header missing: content-security-policy.**	testasp.vulnweb.com	Define a CSP starting from `default-src 'self'`.
6	LOW Next maintenance	**/: Suggested security header missing: permissions-policy.**	testasp.vulnweb.com	Send a Permissions-Policy that turns off what the site does not use, for example `Permissions-Policy: camera=(), microphone=(), geolocation=()`.
7	LOW Next maintenance	**/: Suggested security header missing: referrer-policy.**	testasp.vulnweb.com	Send `Referrer-Policy: strict-origin-when-cross-origin`.
8	LOW Next maintenance	**/: Suggested security header missing: strict-transport-security.**	testasp.vulnweb.com	Send `Strict-Transport-Security: max-age=31536000; includeSubDomains`.
9	LOW Next maintenance	**/: X-Frame-Options header is deprecated and was replaced with the Content-Security-Policy HTTP header with the frame-ancestors directive.**	testasp.vulnweb.com	Send `Content-Security-Policy: frame-ancestors 'none'` (or a trusted origin).
10	LOW Next maintenance	**Microsoft-IIS/8.5 may be outdated (current is at least 10.0; IIS 6.0 support is available until 2014).**	testasp.vulnweb.com	Confirm the version on the host itself: a scanner reads it from a banner.
11	LOW Next maintenance	**Plaintext HTTP**	scanme.nmap.org, port 80	Serve the site over HTTPS with a valid certificate.
12	LOW Next maintenance	**Response headers name the server software and its version**	testasp.vulnweb.com	Remove the header: IIS, delete X-Powered-By under HTTP Response Headers and set `enableVersionHeader="false"` on `<httpRuntime>`; Apache `ServerTokens Prod` and `ServerSignature Off`; nginx

				`server_tokens off`.
13	LOW Next maintenance	**The X-Content-Type-Options header is not sent**	testasp.vulnweb.com	Send `X-Content-Type-Options: nosniff` on every response.
14	LOW Next maintenance	**The server accepts HTTP methods the site does not need**	testasp.vulnweb.com	Allow only the methods the application uses, usually GET, HEAD and POST.
15	LOW Next maintenance	**The server reveals an internal address in a response header**	testasp.vulnweb.com	Give the server the public name to use when it builds a redirect, so it stops falling back to its own address: IIS `alternateHostName` in `system.webServer/serverRuntime`, Apache `ServerName` with `UseCanonicalName On`.

Scan results and findings

Scan #1: sqlmap → http://testasp.vulnweb.com/showforum.asp?id=0

Tool	sqlmap
Target	http://testasp.vulnweb.com/showforum.asp?id=0
Started	2026-11-12 01:34
Completed	2026-11-12 01:38
Scan ID	`e7b7a6fa-261f-4048-b677-47293899b729`

FINDINGS (1)

CRITICAL **SQL injection in id (GET)**

sqlmap confirmed 3 working techniques on this parameter: boolean-based blind, stacked queries, time-based blind.

HOW TO FIX THIS

A request parameter reaches a SQL statement as part of the statement

Risk if left unfixed: Anyone who can send the request can read or change whatever the application's database account can reach: other users' records, stored credentials and, on some database servers, commands on the host.

1. Find the query that uses the named parameter and rewrite it as a parameterized query (prepared statement). Never build SQL by joining strings with request values.
2. Look for the same pattern in the rest of the application: one injectable parameter usually means the pattern is used elsewhere.
3. Check the value's type on the server (an id is a whole number) and reject anything else.
4. Give the application's database account only the rights it needs: no schema changes, no administrative role.
5. Show a generic error page; database error text helps whoever is probing.
6. Treat passwords and keys stored in that database as exposed and change them, then run the scan again.

References: OWASP SQL Injection Prevention Cheat Sheet · CWE-89

RAW TOOL OUTPUT

```
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.10.10#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
```

```
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsib
le for any misuse or damage caused by this program

[*] starting @ 01:34:57 /2026-11-12/

[01:34:57] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('ASPSESSIONIDCCDSSDSA=EECDEAOBDHC...OBLDLJECGN'). Do
you want to use those [Y/n] Y
[01:34:57] [INFO] checking if the target is protected by some kind of WAF/IPS
[01:34:57] [INFO] testing if the target URL content is stable
[01:34:58] [INFO] target URL content is stable
[01:34:58] [INFO] testing if GET parameter 'id' is dynamic
[01:34:59] [WARNING] GET parameter 'id' does not appear to be dynamic
[01:34:59] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be SQL injectable
[01:34:59] [INFO] testing for SQL injection on GET parameter 'id'
[01:34:59] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:34:59] [WARNING] reflective value(s) found and filtering out
[01:34:59] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --
code=200)
[01:35:01] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'Microsoft SQL Server'
it looks like the back-end DBMS is 'Microsoft SQL Server'. Do you want to skip test payloads specific for other DBMSes? [
Y/n] Y
for the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and ris
k (1) values? [Y/n] Y
[01:35:01] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[01:35:01] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause (IN)'
[01:35:01] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONVERT)'
[01:35:01] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause (CONVERT)'
[01:35:01] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'
[01:35:01] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause (CONCAT)'
[01:35:01] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'
[01:35:02] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace (integer column)'
[01:35:02] [INFO] testing 'Microsoft SQL Server error-based - Stacking (RAISERROR)'
[01:35:02] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[01:35:02] [INFO] testing 'Generic inline queries'
[01:35:02] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[01:35:02] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[01:37:04] [INFO] GET parameter 'id' appears to be 'Microsoft SQL Server/Sybase stacked queries (comment)' injectable
[01:37:04] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[01:38:34] [INFO] GET parameter 'id' appears to be 'Microsoft SQL Server/Sybase time-based blind (IF)' injectable
[01:38:34] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[01:38:34] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other
(potential) technique found
[01:38:39] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number
of query columns. Automatically extending the range for current UNION query injection technique test
[01:38:40] [INFO] target URL appears to have 2 columns in query
do you want to (re)try to find proper UNION column types with a fuzzy test? [Y/n] Y
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/
n] Y
[01:38:42] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbm
s=mysql')
[01:38:43] [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 100 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=0 AND 8320=8320

    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: id=0;WAITFOR DELAY '0:0:5'--

    Type: time-based blind
    Title: Microsoft SQL Server/Sybase time-based blind (IF)
    Payload: id=0 WAITFOR DELAY '0:0:5'
---
[01:38:44] [INFO] testing Microsoft SQL Server
[01:38:44] [INFO] confirming Microsoft SQL Server
[01:38:44] [INFO] the back-end DBMS is Microsoft SQL Server
[01:38:44] [INFO] target renders 4 rows that a single response could carry data in. You can try switch '--multi-bit' to r
ead several characters per request instead of one bit. Though it widens the result set with OR payloads, as '--risk=3' do
es
```

```
web server operating system: Windows 2012 R2 or 8.1
web application technology: ASP, ASP.NET, Microsoft IIS 8.5, Django
back-end DBMS: Microsoft SQL Server 2014
[01:38:44] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 93 times
[01:38:44] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testasp.vulnweb.com'

[*] ending @ 01:38:44 /2026-11-12/
```

Scan #2: nmap → scanme.nmap.org

Tool	nmap
Target	scanme.nmap.org
Started	2026-11-12 01:31
Completed	2026-11-12 01:31
Scan ID	`baf1f391-6a3c-4e47-ac43-1d7844bc96c6`

DISCOVERED SERVICES

PORT	PROTOCOL	STATE	SERVICE
22	tcp	open	ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80	tcp	open	http Apache httpd 2.4.7 ((Ubuntu))
9929	tcp	open	nping-echo Nping echo

FINDINGS (3)

MEDIUM **22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)**

SSH — SSH is reachable. SSH is the right tool for remote access, but an exposed service is a brute-force target.

HOW TO FIX THIS

SSH is reachable from this network

Risk if left unfixed: SSH is the usual route to a shell on the host, so it is a standing target for credential stuffing and for any CVE in the running version.

1. Restrict SSH to known management addresses with a firewall rule or security group.
2. Disable password authentication and use keys: PasswordAuthentication no.
3. Disable direct root login: PermitRootLogin no.
4. Keep OpenSSH patched, and remove accounts that no longer need shell access.
5. If the host must be reachable from the internet, put SSH behind a VPN or bastion instead.

References: CIS Benchmark — OpenSSH Server · NIST SP 800-123

LOW **80/tcp open http Apache httpd 2.4.7 ((Ubuntu))**

Plaintext HTTP — A plain HTTP service is reachable. Traffic to it is not encrypted.

HOW TO FIX THIS

The service answers over plaintext HTTP

Risk if left unfixed: Anything sent over HTTP — credentials, session cookies, form data — can be read or altered by anyone on the network path.

1. Serve the site over HTTPS with a valid certificate.
2. Redirect HTTP to HTTPS, and keep the redirect relative or hardcoded to https.
3. Add Strict-Transport-Security once HTTPS is confirmed working.
4. Mark session cookies Secure and HttpOnly.

References: OWASP Transport Layer Protection Cheat Sheet · RFC 6797

INFO **9929/tcp open nping-echo Nping echo**

Open port — This port accepts connections. The service name is a guess from the port number.

HOW TO FIX THIS

This port accepts connections. The service name is a guess from the port number.

Risk if left unfixed: Every listening service is something to keep updated; one you do not use is risk with no benefit.

1. Check which app on this device uses the port (on Windows: netstat -abno; on Linux and macOS: sudo lsof -i -P).
2. If you do not need it, turn that app or feature off, or block the port in the device's firewall.
3. If you do, keep the app updated.

References: https://www.cisecurity.org/controls/v8

RAW TOOL OUTPUT

```
Starting Nmap 7.991 ( https://nmap.org ) at 2026-11-12 01:31 +0000
[stderr] Warning: Hostname scanme.nmap.org resolves to 2 IPs. Using 45.33.32.156.
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.087s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
22/tcp   open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp   filtered smtp
80/tcp   open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
9929/tcp open     nping-echo   Nping echo
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.06 seconds
```

CONFIDENTIAL

Scan #3: nikto → testasp.vulnweb.com

Tool	nikto
Target	testasp.vulnweb.com
Started	2026-11-12 01:31

Completed	2026-11-12 01:33
Scan ID	`5dd838ed-d63c-4ec8-bb14-2320b69fdb5c`

FINDINGS (17)

INFO **Server banner: Microsoft-IIS/8.5**

HOW TO FIX THIS

Response headers name the server software and its version

Risk if left unfixed: It tells an attacker which published vulnerabilities to try first. The header is not the weakness; out-of-date software behind it is.

1. Remove the header: IIS, delete X-Powered-By under HTTP Response Headers and set `enableVersionHeader="false"` on `<httpRuntime>`; Apache `ServerTokens Prod` and `ServerSignature Off`; nginx `server_tokens off`.
2. Keep the software itself updated: hiding a version does not fix what that version has.

References: OWASP Secure Headers Project · CWE-200

LOW **/: Cookie ASPSESSIONIDCCDSSDSA created without the httponly flag.**

The tool's reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

HOW TO FIX THIS

A cookie is set without the HttpOnly, Secure or SameSite attribute

Risk if left unfixed: A session cookie that script can read is taken by any script-injection flaw on the site; one sent over plain HTTP can be read on the network path.

1. Set HttpOnly on every session cookie.
2. Set Secure once the site is served over HTTPS only.
3. Set SameSite=Lax (or Strict) unless the cookie must travel with requests from other sites.
4. Most platforms have one setting for this: ASP.NET `<httpCookies httpOnlyCookies="true" requireSSL="true" />`, PHP `session.cookie_httponly` and `session.cookie_secure`.

References: OWASP Session Management Cheat Sheet · CWE-1004 · CWE-614

LOW **/: Retrieved x-powered-by header: ASP.NET.**

HOW TO FIX THIS

Response headers name the server software and its version

Risk if left unfixed: It tells an attacker which published vulnerabilities to try first. The header is not the weakness; out-of-date software behind it is.

1. Remove the header: IIS, delete X-Powered-By under HTTP Response Headers and set `enableVersionHeader="false"` on `<httpRuntime>`; Apache `ServerTokens Prod` and `ServerSignature Off`; nginx `server_tokens off`.
2. Keep the software itself updated: hiding a version does not fix what that version has.

References: OWASP Secure Headers Project · CWE-200

LOW **OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .**

HOW TO FIX THIS

The server accepts HTTP methods the site does not need

Risk if left unfixed: Every extra method is extra surface. TRACE echoes the request back and has been used to read headers that script cannot otherwise see.

1. Allow only the methods the application uses, usually GET, HEAD and POST.
2. Turn TRACE off: IIS Request Filtering (deny the verb), Apache `TraceEnable off` .
3. Send an OPTIONS request from outside afterwards and confirm it lists only what you allowed.

References: OWASP Web Security Testing Guide WSTG-CONF-06

LOW **OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .**

HOW TO FIX THIS

The server accepts HTTP methods the site does not need

Risk if left unfixed: Every extra method is extra surface. TRACE echoes the request back and has been used to read headers that script cannot otherwise see.

1. Allow only the methods the application uses, usually GET, HEAD and POST.
2. Turn TRACE off: IIS Request Filtering (deny the verb), Apache `TraceEnable off` .
3. Send an OPTIONS request from outside afterwards and confirm it lists only what you allowed.

References: OWASP Web Security Testing Guide WSTG-CONF-06

LOW **/index.aspx: Retrieved x-aspnet-version header: 2.0.50727.**

HOW TO FIX THIS

Response headers name the server software and its version

Risk if left unfixed: It tells an attacker which published vulnerabilities to try first. The header is not the weakness; out-of-date software behind it is.

1. Remove the header: IIS, delete X-Powered-By under HTTP Response Headers and set `enableVersionHeader="false"` on `<httpRuntime>` ; Apache `ServerTokens Prod` and `ServerSignature Off` ; nginx `server_tokens off` .
2. Keep the software itself updated: hiding a version does not fix what that version has.

References: OWASP Secure Headers Project · CWE-200

LOW **Microsoft-IIS/8.5 may be outdated (current is at least 10.0; IIS 6.0 support is available until 2014).**

HOW TO FIX THIS

The server software is an old release

Risk if left unfixed: Old releases stop receiving security fixes, so vulnerabilities published for them stay open.

1. Confirm the version on the host itself: a scanner reads it from a banner.
2. Plan the move to a release the vendor still supports (for IIS, that is the Windows Server release underneath it).
3. Until then, install every security update available for the installed release and limit what can reach the server.
4. Scan again after the upgrade.

References: CIS Controls v8 Control 7 · CWE-1104

LOW **/: Default IIS server content.**

The tool's reference: https://www.iis.net/

HOW TO FIX THIS

The web server still serves the content it was installed with

Risk if left unfixed: Default pages name the product and suggest the server was not hardened after installation; sample applications have had vulnerabilities of their own.

1. Remove the default site or page, and the sample applications, manuals and test scripts that came with the server.
2. Go through the vendor's or the CIS hardening guide for this server.
3. Request the page again and confirm it is gone.

References: OWASP Web Security Testing Guide WSTG-CONF-02 · CIS Benchmarks

LOW **/aspnet_client: RFC-1918 IP address found in the 'location' header. The IP is "10.0.0.14".**

The tool's reference: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed

HOW TO FIX THIS

The server reveals an internal address in a response header

Risk if left unfixed: It shows an outsider how the network behind the server is numbered. Low by itself; useful to someone planning a next step.

1. Give the server the public name to use when it builds a redirect, so it stops falling back to its own address: IIS `alternateHostName` in `system.webServer/serverRuntime`, Apache `ServerName` with `UseCanonicalName On`.
2. At the reverse proxy or load balancer, refuse HTTP/1.0 requests that carry no Host header.
3. Request the same path again without a Host header and confirm the address is gone.

References: CVE-2000-0649 · CWE-200

LOW **/aspnet_client: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "10.0.0.14".**

The tool's reference: https://nvd.nist.gov/vuln/detail/CVE-2000-0649

HOW TO FIX THIS

The server reveals an internal address in a response header

Risk if left unfixed: It shows an outsider how the network behind the server is numbered. Low by itself; useful to someone planning a next step.

1. Give the server the public name to use when it builds a redirect, so it stops falling back to its own address: IIS `alternateHostName` in `system.webServer/serverRuntime`, Apache `ServerName` with `UseCanonicalName On`.
2. At the reverse proxy or load balancer, refuse HTTP/1.0 requests that carry no Host header.
3. Request the same path again without a Host header and confirm the address is gone.

References: CVE-2000-0649 · CWE-200

LOW **/: Suggested security header missing: strict-transport-security.**

The tool's reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

HOW TO FIX THIS

HTTP Strict Transport Security (HSTS) is not set

Risk if left unfixed: Users can be downgraded to plaintext HTTP by an on-path attacker before the redirect to HTTPS.

1. Send `Strict-Transport-Security: max-age=31536000; includeSubDomains`.
2. Only enable after confirming every subdomain serves HTTPS.
3. Consider HSTS preloading once stable.

References: OWASP HSTS Cheat Sheet

LOW **/: Suggested security header missing: referrer-policy.**

The tool's reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

HOW TO FIX THIS

No Referrer-Policy is set

Risk if left unfixed: The full address of a page, query string included, can be sent to other sites the page links to or loads from.

1. Send `Referrer-Policy: strict-origin-when-cross-origin`.
2. Use `no-referrer` on pages whose addresses carry anything sensitive.

References: OWASP Secure Headers Project

LOW **/: Suggested security header missing: permissions-policy.**

The tool's reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy

HOW TO FIX THIS

No Permissions-Policy is set

Risk if left unfixed: Script in the page, third-party and injected script included, may ask for the camera, the microphone or the location.

1. Send a Permissions-Policy that turns off what the site does not use, for example `Permissions-Policy: camera=(), microphone=(), geolocation=()`.

References: OWASP Secure Headers Project

LOW **/: Suggested security header missing: x-content-type-options.**

The tool's reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

HOW TO FIX THIS

The X-Content-Type-Options header is not sent

Risk if left unfixed: A browser may guess a file's type from its content, so an uploaded file can be run as script although the server called it something else.

1. Send `X-Content-Type-Options: nosniff` on every response.
2. Make sure every response declares its correct Content-Type, uploads and downloads included.

References: OWASP Secure Headers Project

LOW **/: Suggested security header missing: content-security-policy.**

The tool's reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

HOW TO FIX THIS

No Content-Security-Policy is set

Risk if left unfixed: Without a CSP, an injected script runs with full page privileges — the main defence against XSS is absent.

1. Define a CSP starting from `default-src 'self'`.
2. Remove inline scripts or allow them with a nonce/hash rather than 'unsafe-inline'.
3. Deploy in report-only mode first to find violations before enforcing.

References: OWASP Content Security Policy Cheat Sheet

LOW **/: X-Frame-Options header is deprecated and was replaced with the Content-Security-Policy HTTP header with the frame-ancestors directive.**

The tool's reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options

HOW TO FIX THIS

The X-Frame-Options / frame-ancestors protection is missing

Risk if left unfixed: The page can be framed by a malicious site and used for clickjacking.

1. Send `Content-Security-Policy: frame-ancestors 'none'` (or a trusted origin).
2. For older clients, also send `X-Frame-Options: DENY`.

References: OWASP Clickjacking Defense Cheat Sheet

LOW **/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.**

The tool's reference: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

HOW TO FIX THIS

The X-Content-Type-Options header is not sent

Risk if left unfixed: A browser may guess a file's type from its content, so an uploaded file can be run as script although the server called it something else.

1. Send `X-Content-Type-Options: nosniff` on every response.
2. Make sure every response declares its correct Content-Type, uploads and downloads included.

References: OWASP Secure Headers Project

RAW TOOL OUTPUT

```
- Nikto v2.6.1
---------------------------------------------------------------------------
+ Target IP:          44.238.29.244
+ Target Hostname:    testasp.vulnweb.com
+ Target Port:        80
+ Platform:           Windows
+ Start Time:         2026-11-12 01:31:18 (GMT0)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.5
+ [000029] /: Cookie ASPSESSIONIDCCDSSDSA created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ [000287] /: Retrieved x-powered-by header: ASP.NET.
+ No CGI Directories found (use '-C all' to force check all possible dirs). CGI tests skipped.
+ [999990] OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ [999985] OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ [000287] /index.aspx: Retrieved x-aspnet-version header: 2.0.50727.
+ [600376] Microsoft-IIS/8.5 may be outdated (current is at least 10.0; IIS 6.0 support is available until 2014).
+ [750537] /: Default IIS server content. See: https://www.iis.net/
+ [999979] /aspnet_client: RFC-1918 IP address found in the 'location' header. The IP is "10.0.0.14". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ [999988] /aspnet_client: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "10.0.0.14". See: https://nvd.nist.gov/vuln/detail/CVE-2000-0649
+ [013587] /: Suggested security header missing: strict-transport-security. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ [013587] /: Suggested security header missing: referrer-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy
+ [013587] /: Suggested security header missing: permissions-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy
+ [013587] /: Suggested security header missing: x-content-type-options. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
+ [013587] /: Suggested security header missing: content-security-policy. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
+ [007342] /: X-Frame-Options header is deprecated and was replaced with the Content-Security-Policy HTTP header with the frame-ancestors directive. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options
+ [007352] /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ 1427 requests: 0 errors and 16 items reported on the remote host
+ End Time:           2026-11-12 01:33:02 (GMT0) (104 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Methodology

This assessment was performed with **CyberSec Pro**, using the tools named with each scan under Scan results and findings. Every target was either a public practice host or confirmed in writing, by the person who started the scan, as one they are authorized to test.

Platform	CyberSec Pro v4.0
Report Template	Technical Report
Generated	2026-11-12 01:38 UTC
Classification	Confidential
Data residency	Canada

Automated assessment

Produced by CyberSec Pro — not reviewed by an analyst

Content digest

Generated: 2026-11-12 01:38 UTC | Scan ID: e7b7a6fa-261f-4048-b677-47293899b729

SHA-256: 91ca3cc3d84fdbb90609b2d73787d29ff8ae4d740f658fe8e761d07d60c48fea

Generated by **CyberSec Pro** | **cyber-sec-pro.com**

This report is confidential and intended only for authorized recipients.

© 2026 CyberSec Pro. All rights reserved.