Vulnerability Scan Report

PREPARED FOR

Demo Organization

FEBRUARY 09, 2026

Scanner Now

Security Assessment Platform

scannernow.com

CONTENTS

Report Overview

FEBRUARY 09, 2026

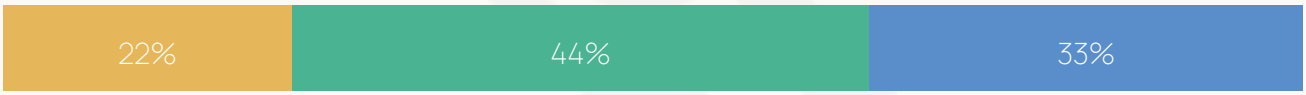
1 Executive Summary

Vulnerability scans were conducted on select servers, networks, websites, and applications. This report contains the discovered potential vulnerabilities from these scans. Vulnerabilities have been classified by severity. Higher severity indicates a greater risk of a data breach, loss of integrity, or availability of the targets.

1.1 Total Vulnerabilities

Below are the total number of vulnerabilities found by severity. Critical vulnerabilities are the most severe and should be evaluated first. An accepted vulnerability is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive detection or an intentional part of the system's architecture.

Critical	High	Medium	Low	Info
0	0	2	4	3



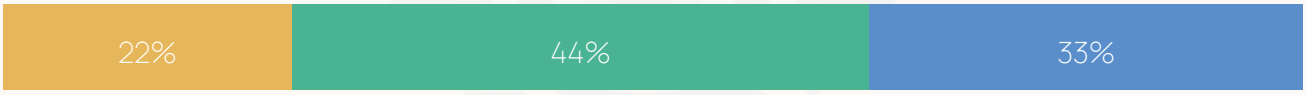
2 Passive Web Application Vulnerabilities

The OWASP ZAP Passive Web Application scan crawls the pages of a website or web application. The passive scan inspects each page as well as the requests and responses sent between the server. The passive scan checks for vulnerabilities such as cross-domain misconfigurations,

2.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.

Critical	High	Medium	Low	Info
0	0	2	4	3



2.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
Content Security Policy (CSP) Header Not Set	Medium	3	0
Missing Anti-clickjacking Header	Medium	1	0
Insufficient Site Isolation Against Spectre V...	Low	3	0
Permissions Policy Header Not Set	Low	3	0
Strict-Transport-Security Header Not Set	Low	3	0
X-Content-Type-Options Header Missing	Low	1	0

Vulnerabilities Breakdown (continued)

Title	Severity	Open	Accepted
Re-examine Cache-control Directives	Info	1	0
Retrieved from Cache	Info	3	0
Storable and Cacheable Content	Info	3	0

3 Detailed Findings

Finding 1

Content Security Policy (CSP) Header Not Set

Medium

CWE: CWE-693 | WASC: 15 | Confidence: 3 | Affected: 3 | Detected: February 09, 2026

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. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Remediation

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Affected Systems

URL / ENDPOINT	METHOD	PARAMETER
https://example.com	GET	
https://example.com/robots.txt	GET	
https://example.com/sitemap.xml	GET	

References

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://www.w3.org/TR/CSP/
- https://w3c.github.io/webappsec-csp/
- https://web.dev/articles/csp

Finding 2

Missing Anti-clickjacking Header

Medium

CWE: CWE-1021 | WASC: 15 | Confidence: 2 | Affected: 1 | Detected: February 09, 2026

Description

The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

Remediation

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Affected Systems

URL / ENDPOINT	METHOD	PARAMETER
https://example.com	GET	x-frame-options

References

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options

Finding 3

Insufficient Site Isolation Against Spectre Vulnerability

Low

CWE: CWE-693 | WASC: 14 | Confidence: 2 | Affected: 3 | Detected: February 09, 2026

Description

Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.

Remediation

Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages.'same-site' is considered as less secured and should be avoided.If resources must be shared, set the header to 'cross-origin'.If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).

Affected Systems

URL / ENDPOINT	METHOD	PARAMETER
https://example.com	GET	Cross-Origin-Resourc
https://example.com	GET	Cross-Origin-Embedde
https://example.com	GET	Cross-Origin-Opener-

References

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cross-Origin-Embedd...

Finding 4

Permissions Policy Header Not Set

Low

CWE: CWE-693 | WASC: 15 | Confidence: 2 | Affected: 3 | Detected: February 09, 2026

Description

Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.

Remediation

Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.

Affected Systems

URL / ENDPOINT	METHOD	PARAMETER
https://example.com	GET	
https://example.com/robots.txt	GET	
https://example.com/sitemap.xml	GET	

References

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Permissions-Policy
- https://developer.chrome.com/blog/feature-policy/
- https://scotthelme.co.uk/a-new-security-header-feature-policy/
- https://w3c.github.io/webappsec-feature-policy/
- https://www.smashingmagazine.com/2018/12/feature-policy/

Finding 5

Strict-Transport-Security Header Not Set

Low

CWE: CWE-319 | WASC: 15 | Confidence: 3 | Affected: 3 | Detected: February 09, 2026

Description

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Remediation

Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Affected Systems

URL / ENDPOINT	METHOD	PARAMETER
https://example.com	GET	
https://example.com/robots.txt	GET	
https://example.com/sitemap.xml	GET	

References

- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_She...
- https://owasp.org/www-community/Security_Headers
- https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- https://caniuse.com/stricttransportsecurity
- https://datatracker.ietf.org/doc/html/rfc6797

Finding 6

X-Content-Type-Options Header Missing

Low

CWE: CWE-693 | WASC: 15 | Confidence: 2 | Affected: 1 | Detected: February 09, 2026

Description

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Remediation

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Affected Systems

URL / ENDPOINT	METHOD	PARAMETER
https://example.com	GET	x-content-type-optio

References

- https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-develo...
- https://owasp.org/www-community/Security_Headers

Finding 7

Re-examine Cache-control Directives

Info

CWE: CWE-525 | WASC: 13 | Confidence: 1 | Affected: 1 | Detected: February 09, 2026

Description

The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Remediation

For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

Affected Systems

URL / ENDPOINT	METHOD	PARAMETER
https://example.com	GET	cache-control

References

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-...
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control
- https://grayduck.mn/2021/09/13/cache-control-recommendations/

Finding 8

Retrieved from Cache

Info

CWE: CWE-525 | WASC: -1 | Confidence: 2 | Affected: 3 | Detected: February 09, 2026

Description

The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Remediation

Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:Cache-Control: no-cache, no-store, must-revalidate, privatePragma: no-cacheExpires: 0This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

Evidence

URL: https://example.com
Evidence: Age: 10927
Details: The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL: https://example.com/robots.txt
Evidence: Age: 79
Details: The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL: https://example.com/sitemap.xml
Evidence: Age: 79
Details: The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

Affected Systems

URL / ENDPOINT	METHOD	PARAMETER
https://example.com	GET	
https://example.com/robots.txt	GET	

Finding 9

Storable and Cacheable Content

Info

CWE: CWE-524 | WASC: 13 | Confidence: 2 | Affected: 3 | Detected: February 09, 2026

Description

The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Remediation

Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:Cache-Control: no-cache, no-store, must-revalidate, privatePragma: no-cacheExpires: 0This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

Affected Systems

URL / ENDPOINT	METHOD	PARAMETER
https://example.com	GET	
https://example.com/robots.txt	GET	
https://example.com/sitemap.xml	GET	

References

- https://datatracker.ietf.org/doc/html/rfc7234
- https://datatracker.ietf.org/doc/html/rfc7231
- https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html

4 Glossary

Vulnerability

A weakness in a system that can be exploited by a threat actor to gain unauthorized access or cause harm.

Risk

The potential for loss or damage when a threat exploits a vulnerability. Measured by likelihood and impact.

Exploit

A piece of software or technique that takes advantage of a vulnerability to cause unintended behavior.

CVE

Common Vulnerabilities and Exposures. A publicly disclosed security flaw with a unique identifier.

CVSS

Common Vulnerability Scoring System. A framework for rating the severity of security vulnerabilities.

Penetration Test

A simulated cyber attack to evaluate the security of a system by exploiting vulnerabilities.

Port Scanning

Probing a server or host for open ports to identify available services and potential entry points.

SSL/TLS

Secure Sockets Layer and Transport Layer Security. Protocols for encrypting data in transit.

XSS

Cross-Site Scripting. An injection attack where malicious scripts are injected into trusted websites.

SQL Injection

An attack technique that exploits SQL vulnerabilities to manipulate database queries.

Firewall

A network security system that monitors and controls incoming and outgoing network traffic.

Patch

A software update that fixes security vulnerabilities and bugs in a system or application.

Report Complete

This vulnerability assessment report has been prepared for Demo Organization. The findings and recommendations outlined in this report are based on industry best practices and security standards.

Recommended Actions

- Review all critical and high severity vulnerabilities immediately
- Prioritize remediation based on severity and business impact
- Implement security patches and configuration changes as recommended
- Schedule follow-up scans to verify remediation effectiveness

Next Steps

- Share this report with your security and development teams
- Create remediation tickets for identified vulnerabilities
- Establish timelines for addressing security findings
- Run periodic scans to monitor your security posture

This report was prepared using

Scanner Now®

For more information, visit scannernow.com

Scanner Now is a security assessment platform that helps organizations identify vulnerabilities and strengthen their security posture through automated scanning and reporting.

Need Assistance?

Email Support	Website
hello@scannernow.com	scannernow.com
For questions about this report	Access your security dashboard

Scanner Now
hello@scannernow.com

Terms & Policies
hello@scannernow.com