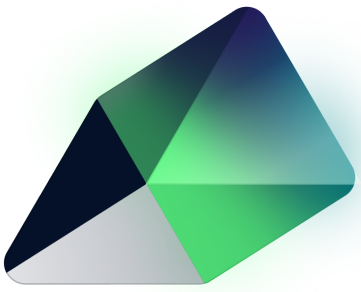
November 28, 2024

Vulnerability Scan Report

Prepared By

HostedScan Security



hostedscan.com

Overview

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	Accepted
0	0	3	8	0

1.2 Report Coverage

This report includes findings for 1 target scanned. Each target is a single URL, IP address, or fully qualified domain name (FQDN).

Vulnerability Categories

0 Active Web Application Vulnerabilities	8 Passive Web Application Vulnerabilities	1 Network Vulnerabilities
0 SSL/TLS Security	2 Open TCP Ports	0 Open UDP Ports

2 Vulnerabilities By Target

This section contains the vulnerability findings for each scanned target. Prioritization should be given to the targets with the highest severity vulnerabilities. However, it is important to take into account the purpose of each system and consider the potential impact a breach or an outage would have for the particular target.

2.1 Targets Summary

The number of potential vulnerabilities found for each target by severity.

Target	Critical	High	Medium	Low	Accepted
https://rubberduckiesftw.wpcomstaging.com/	0	0	3	8	0

2.2 Target Breakdowns

Details for the potential vulnerabilities found for each target by scan type.

https://rubberduckiesftw.wpcomstaging.com/

Total Risks

0	0	3	8	0

Passive Web Application Vulnerabilities	Severity	First Detected	Last Detected
Cross-Domain Misconfiguration	Medium	7 days ago	7 days ago
Absence of Anti-CSRF Tokens	Medium	7 days ago	7 days ago
Content Security Policy (CSP) Header Not Set	Medium	7 days ago	7 days ago
Cookie No HttpOnly Flag	Low	7 days ago	7 days ago
Cookie Without Secure Flag	Low	7 days ago	7 days ago
Cross-Domain JavaScript Source File Inclusion	Low	7 days ago	7 days ago
X-Content-Type-Options Header Missing	Low	7 days ago	7 days ago
Cookie without SameSite Attribute	Low	7 days ago	7 days ago

Network Vulnerabilities	Severity	First Detected	Last Detected
ICMP Timestamp Reply Information Disclosure cvss score: 2.1	Low	7 days ago	7 days ago

Open TCP Ports	Severity	First Detected	Last Detected
Open TCP Port: 80	Low	7 days ago	7 days ago
Open TCP Port: 443	Low	7 days ago	7 days ago

3 Active Web Application Vulnerabilities

The OWASP ZAP Active Web Application scan crawls the pages of a website or web application testing for vulnerabilities and configuration weaknesses. The active scan includes all of the passive scan tests and additionally makes requests and submits forms to actively test an application for more vulnerabilities. The active scan tests for vulnerabilities such as SQL injection, remote command execution, XSS, and more.

3.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	0	0

3.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
No vulnerabilities detected			

4 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, insecure cookies, vulnerable Javascript dependencies, and more.

4.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.

Critical	High	Medium	Low	Accepted
0	0	3	5	0

4.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
Cross-Domain Misconfiguration	Medium	1	0
Absence of Anti-CSRF Tokens	Medium	1	0
Content Security Policy (CSP) Header Not Set	Medium	1	0
Cookie No HttpOnly Flag	Low	1	0
Cookie Without Secure Flag	Low	1	0
Cross-Domain JavaScript Source File Inclusion	Low	1	0
X-Content-Type-Options Header Missing	Low	1	0
Cookie without SameSite Attribute	Low	1	0

4.3 Vulnerability Details

Detailed information about each potential vulnerability found by the scan.

Cross-Domain Misconfiguration

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Medium	1 target	7 days ago

Description

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Solution

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

Instances (1 of 95)

uri: https://rubberduckiesftw.wpcomstaging.com/wp-admin/js/password-strength-meter.min.js?ver=6.7
method: GET
evidence: Access-Control-Allow-Origin: *
otherinfo: The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

References

https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

Absence of Anti-CSRF Tokens

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Medium	1 target	7 days ago

Description

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

* The victim has an active session on the target site.

* The victim is authenticated via HTTP auth on the target site.

* The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

Solution

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Instances (1 of 19)

uri: https://rubberduckiesftw.wpcomstaging.com/product/blanket-3/
method: POST
evidence: <form class="cart" action="https://rubberduckiesftw.wpcomstaging.com/product/blanket-3/" method="post" enctype='multipart/form-data'>
otherinfo: No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, data[_Token][key]] was found in the following HTML form: [Form 1: "is-descendent-of-single-product-block" "quantity_673e17777b278"].

References

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
https://cwe.mitre.org/data/definitions/352.html

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

Content Security Policy (CSP) Header Not Set

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Medium	1 target	7 days ago

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.

Solution

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

Instances (1 of 100)

uri: https://rubberduckiesftw.wpcomstaging.com/
method: GET

References

https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
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
https://caniuse.com/#feat=contentsecuritypolicy
https://content-security-policy.com/

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

Cookie No HttpOnly Flag

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Low	1 target	7 days ago

Description

A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

Solution

Ensure that the HttpOnly flag is set for all cookies.

Instances (1 of 36)

uri: https://rubberduckiesftw.wpcomstaging.com/
method: GET
param: PHPSESSID
evidence: Set-Cookie: PHPSESSID

References

https://owasp.org/www-community/HttpOnly

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

Cookie Without Secure Flag

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Low	1 target	7 days ago

Description

A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Solution

Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Instances (1 of 31)

uri: https://rubberduckiesftw.wpcomstaging.com/
method: GET
param: PHPSESSID
evidence: Set-Cookie: PHPSESSID

References

https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

Cross-Domain JavaScript Source File Inclusion

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Low	1 target	7 days ago

Description

The page includes one or more script files from a third-party domain.

Solution

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Instances (1 of 100)

uri: https://rubberduckiesftw.wpcomstaging.com/
method: GET
param: https://s0.wp.com/wp-content/js/bilmur.min.js?m=202447
evidence: <script defer id="bilmur" data-customproperties="{"woo_active":"1"}" data-provider="wordpress.com" data-service="atomic" src="https://s0.wp.com/wp-content/js/bilmur.min.js?m=202447"></script>

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

X-Content-Type-Options Header Missing

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Low	1 target	7 days ago

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.

Solution

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.

Instances (1 of 100)

uri: https://rubberduckiesftw.wpcomstaging.com/_static/??-eJwrL9BNzs8rSc0r0S/IKU3PzCvWL8/PT87PzU0tSk7VLUiszAXKFeunZBaX6CcnFpXoZRXrlJOqSTcpJz85G6jVPtfW0NzY0NTMyNLCCADS9C5C
method: GET
param: x-content-type-options
otherinfo: This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

References

https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)
https://owasp.org/www-community/Security_Headers

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

Cookie without SameSite Attribute

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Low	1 target	7 days ago

Description

A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Solution

Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Instances (1 of 46)

uri: https://rubberduckiesftw.wpcomstaging.com/
method: GET
param: PHPSESSID
evidence: Set-Cookie: PHPSESSID

References

https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

5 SSL/TLS Security

The SSLyze security scan tests for misconfigured SSL/TLS certificates, expired certificates, weak ciphers, and SSL/TLS vulnerabilities such as Heartbleed.

5.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	0	0

5.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
No vulnerabilities detected			

6 Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 150,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

6.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	1	0

6.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	CVSS Score	Open	Accepted
ICMP Timestamp Reply Information Disclosure	Low	2.1	1	0

6.3 Vulnerability Details

Detailed information about each potential vulnerability found by the scan.

ICMP Timestamp Reply Information Disclosure

SEVERITY	AFFECTED TARGETS	LAST DETECTED	CVSS SCORE
Low	1 target	7 days ago	2.1

Description

The remote host responded to an ICMP timestamp request.

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

References

CVE-1999-0524
https://datatracker.ietf.org/doc/html/rfc792
https://datatracker.ietf.org/doc/html/rfc2780

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

7 Open TCP Ports

The NMAP TCP port scan discovers open TCP ports with a complete scan of ports 0 to 65535.

7.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	2	0

7.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
Open TCP Port: 80	Low	1	0
Open TCP Port: 443	Low	1	0

7.3 Vulnerability Details

Detailed information about each potential vulnerability found by the scan.

Open TCP Port: 80

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Low	1 target	7 days ago

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

Open TCP Port: 443

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Low	1 target	7 days ago

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

Vulnerable Target	First Detected	Last Detected
https://rubberduckiesftw.wpcomstaging.com/	7 days ago	7 days ago

8 Open UDP Ports

The NMAP UDP port scan discovers open ports of common UDP services

8.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	0	0

8.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
No vulnerabilities detected			

9 Glossary

Accepted Vulnerability

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 scan result or an intentional part of the system's architecture.

Active Web Application Vulnerabilities

The OWASP ZAP Active Web Application scan crawls the pages of a website or web application testing for vulnerabilities and configuration weaknesses. The active scan includes all of the passive scan tests and additionally makes requests and submits forms to actively test an application for more vulnerabilities. The active scan tests for vulnerabilities such as SQL injection, remote command execution, XSS, and more.

Fully Qualified Domain Name (FQDN)

A fully qualified domain name is a complete domain name for a specific website or service on the internet. This includes not only the website or service name, but also the top-level domain name, such as .com, .org, .net, etc. For example, 'www.example.com' is an FQDN.

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, insecure cookies, vulnerable Javascript dependencies, and more.

Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 150,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

Open TCP Ports

The NMAP TCP port scan discovers open TCP ports with a complete scan of ports 0 to 65535.

Open UDP Ports

The NMAP UDP port scan discovers open ports of common UDP services

Vulnerability

A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety).

SSL/TLS Security

The SSLyze security scan tests for misconfigured SSL/TLS certificates, expired certificates, weak ciphers, and SSL/TLS vulnerabilities such as Heartbleed.

Target

A target represents target is a single URL, IP address, or fully qualified domain name (FQDN) that was scanned.

Severity

Severity represents the estimated impact potential of a particular vulnerability. Severity is divided into 5 categories: Critical, High, Medium, Low and Accepted.

CVSS Score

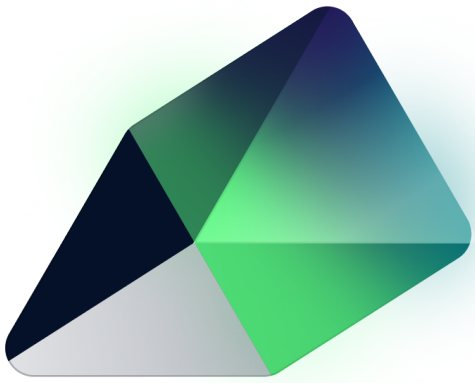
The CVSS 3.0 score is a global standard for evaluating vulnerabilities with a 0 to 10 scale. CVSS maps to threat levels:
0.1 - 3.9 = Low
4.0 - 6.9 = Medium
7.0 - 8.9 = High
9.0 - 10.0 = Critical

This report was prepared using

HostedScan Security ®

For more information, visit **hostedscan.com**

Founded in Seattle, Washington in 2019, HostedScan, LLC. is dedicated to making continuous vulnerability scanning and risk management much more easily accessible to more businesses.



HostedScan, LLC.

2212 Queen Anne Ave N
Suite #521
Seattle, WA 98109

Terms & Policies
hello@hostedscan.com