



Web Security – IE2062

Topic: Bug Bounty Report 10

Y2S2.WE.CS

Name: S.D.W.Gunaratne

(IT23241978)

Table of Content

1) How I started?

2) Introduction

2.1 Domain

2.2 Severity

3) Vulnerability

3.1 Vulnerability title

3.2 Vulnerability description

3.3 Affected components

3.4 Impact assessment

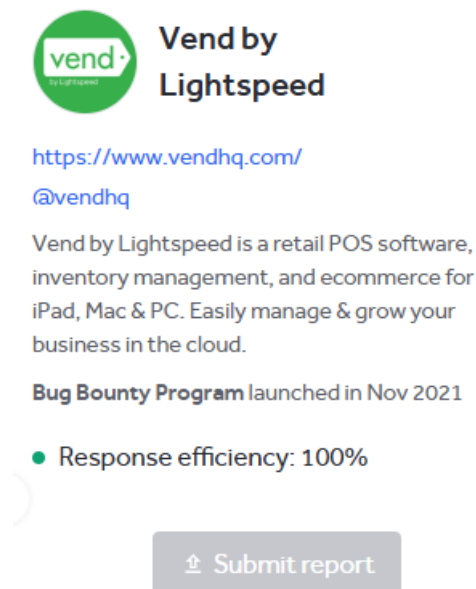
3.5 Steps to reproduce

3.6 Proof of concept

3.7 Proposed mitigation or fix

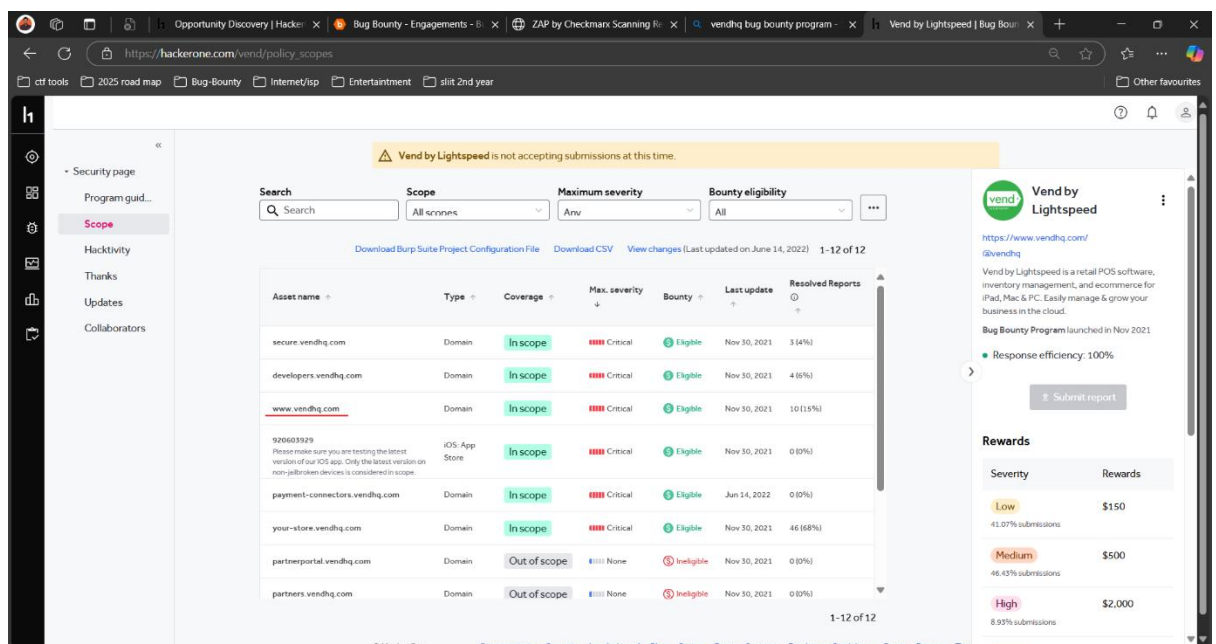
How I started?

1. Once I search from Hacker one, I saw the Vendhq bug bounty program.



The screenshot shows the Vend by Lightspeed bug bounty program page on HackerOne. It includes the Vend by Lightspeed logo, the URL <https://www.vendhq.com/>, the Twitter handle [@vendhq](#), a description of the software, and a 'Bug Bounty Program launched in Nov 2021' badge. A 'Response efficiency: 100%' badge is also visible. A 'Submit report' button is at the bottom.

2. Then, I discovered full main domain allowed for scope, so that I choose <https://www.vendhq.com>.



The screenshot shows the Vend by Lightspeed bug bounty program page on HackerOne, displaying a table of assets and their scope status. A warning banner at the top states: "Vend by Lightspeed is not accepting submissions at this time." The table lists various assets, including domains and an iOS app store, with their respective coverage, maximum severity, bounty status, last update, and resolved reports.

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
secure.vendhq.com	Domain	In scope	Critical	Eligible	Nov 30, 2021	3 (4%)
developers.vendhq.com	Domain	In scope	Critical	Eligible	Nov 30, 2021	4 (6%)
<u>www.vendhq.com</u>	Domain	In scope	Critical	Eligible	Nov 30, 2021	10 (15%)
920603929 <small>Please make sure you are testing the latest version of our iOS app. Only the latest version on non-jailbroken devices is considered in scope.</small>	iOS: App Store	In scope	Critical	Eligible	Nov 30, 2021	0 (0%)
payment-connectors.vendhq.com	Domain	In scope	Critical	Eligible	Jun 14, 2022	0 (0%)
your-store.vendhq.com	Domain	In scope	Critical	Eligible	Nov 30, 2021	46 (68%)
partnerportal.vendhq.com	Domain	Out of scope	None	Ineligible	Nov 30, 2021	0 (0%)
partners.vendhq.com	Domain	Out of scope	None	Ineligible	Nov 30, 2021	0 (0%)

1-12 of 12

3. I use several methods/tools to do penetration testing.
4. First, I used Nmap. It helps me to find what are the open ports, Identify the web technologies such as web servers.

The screenshot shows the Zenmap application window. The 'Target' field contains 'vendhq.com'. The 'Command' field contains 'nmap -T4 -A -v vendhq.com'. The 'Nmap Output' tab is selected, displaying the following text:

```
nmap -T4 -A -v vendhq.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 08:59 Sri Lanka Stand
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:59
Completed NSE at 08:59, 0.00s elapsed
Initiating NSE at 08:59
Completed NSE at 08:59, 0.00s elapsed
Initiating NSE at 08:59
Completed NSE at 08:59, 0.00s elapsed
Initiating Ping Scan at 08:59
Scanning vendhq.com (54.184.242.93) [4 ports]
Completed Ping Scan at 08:59, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:59
Completed Parallel DNS resolution of 1 host. at 08:59, 0.19s elapsed
Initiating SYN Stealth Scan at 08:59
Scanning vendhq.com (54.184.242.93) [1000 ports]
Discovered open port 25/tcp on 54.184.242.93
Discovered open port 443/tcp on 54.184.242.93
Discovered open port 80/tcp on 54.184.242.93
Completed SYN Stealth Scan at 08:59, 17.46s elapsed (1000 total ports)
Initiating Service scan at 08:59
Scanning 3 services on vendhq.com (54.184.242.93)
Completed Service scan at 09:00, 14.31s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against vendhq.com (54.184.242.93)
Retrying OS detection (try #2) against vendhq.com (54.184.242.93)
Initiating Traceroute at 09:00
Completed Traceroute at 09:00, 3.35s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 09:00
Completed Parallel DNS resolution of 11 hosts. at 09:00, 0.63s elapsed
NSE: Script scanning 54.184.242.93.
Initiating NSE at 09:00
```

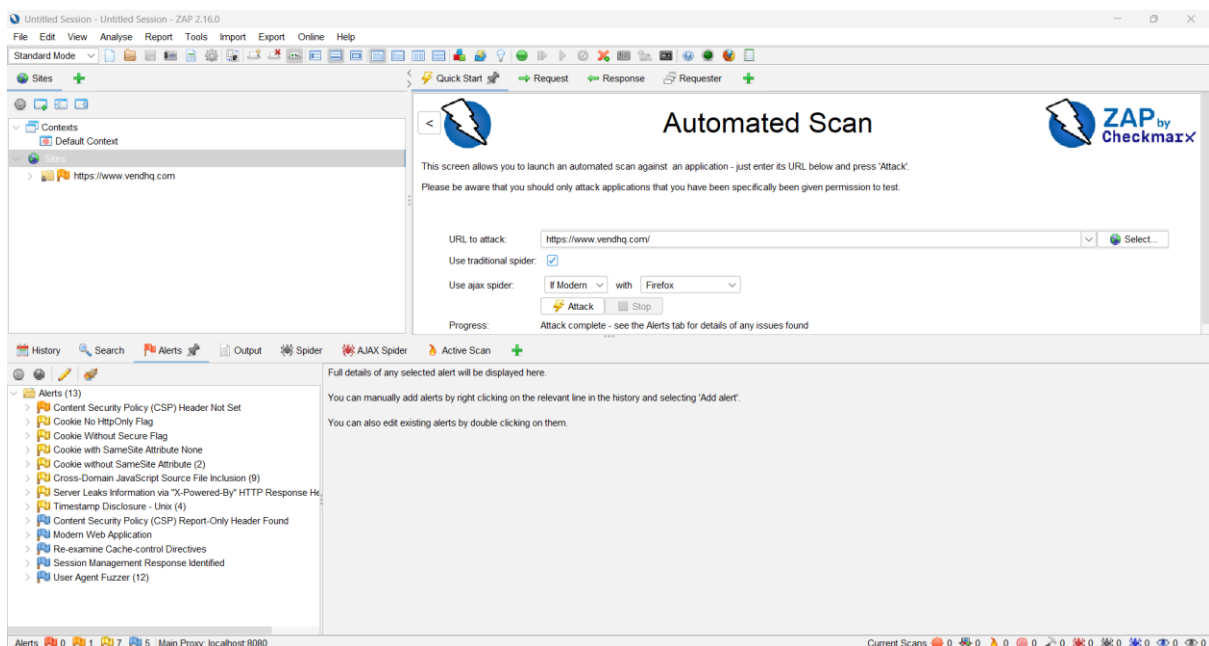
5. Secondly, I used Subfider tool to find hidden or forgotten web asserts. Because hidden web assert can have poor security, unpatched vulnerabilities.

```
SD7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[hackertarget] aws.vendhq.com
[hackertarget] ci.vendhq.com
[hackertarget] feature.vendhq.com
[hackertarget] lb-ube.ord.vendhq.com
[hackertarget] preview.vendhq.com
[hackertarget] rs.vendhq.com
[hackertarget] srt.vendhq.com
[hackertarget] staging.vendhq.com
[hackertarget] office.sys.vendhq.com
[hackertarget] transifex-cds-uobiexohtahveey6boh.vendhq.com
[hackertarget] www.vendhq.com
[alienvault] aws.vendhq.com
[alienvault] secure.vendhq.com
[alienvault] cellairis.vendhq.com
[alienvault] ip.us-east-1.aws.vendhq.com
[alienvault] track.api.vendhq.com
[alienvault] campuscoseattle.vendhq.com
[alienvault] hempcity.vendhq.com
[alienvault] zawayaya.vendhq.com
[alienvault] batteryforce.vendhq.com
[alienvault] hobbymaster.vendhq.com
[alienvault] sthildasags.vendhq.com
[alienvault] xolossshop.vendhq.com
[alienvault] someprefix.vendhq.com
[alienvault] wisani.vendhq.com
[alienvault] goodcycles.vendhq.com
[alienvault] bravenz.vendhq.com
[alienvault] elves.vendhq.com
[alienvault] smartdau123.vendhq.com
[alienvault] threeworlds.vendhq.com
[alienvault] totalcoolnlltd.vendhq.com
[alienvault] millcitymarket.vendhq.com
[alienvault] teste.vendhq.com
[alienvault] payment-connectors.vendhq.com
[alienvault] themusashop.vendhq.com
[alienvault] partnerportal.vendhq.com
[alienvault] massnutritionaustralia.vendhq.com
[alienvault] takemehomeza.vendhq.com
[alienvault] vendteam.vendhq.com
[alienvault] payment-gateway.vendhq.com
[alienvault] staraniseorganic.vendhq.com
[alienvault] houston.test.vendhq.com
[alienvault] backstage.test.vendhq.com
[alienvault] ip.us-west-2.aws.vendhq.com
[alienvault] service.test.vendhq.com
[alienvault] webhooks.api.vendhq.com
[alienvault] zealong.vendhq.com
[alienvault] www.backend.vendhq.com
[alienvault] wcosmeticshq.vendhq.com
[alienvault] manawatusuperstore.vendhq.com
[alienvault] www.vendhq.com
[alienvault] petsoffice.vendhq.com
```

6. Thirdly, I used Wafwoof tool to find website is protected by a WAF (web application firewall). Because if WAF is active, so pen tester do their test without blocked, and they can do their testing with bypass WAF.

```
root@kali2025: ~  
File Actions Edit View Help  
  
(root@kali2025)-[~]  
# wafw00f https://www.vendhq.com/  
  
~ WAFW00F : v2.3.1 ~  
  
[*] Checking https://www.vendhq.com/  
[+] The site https://www.vendhq.com/ is behind Cloudflare (Cloudflare Inc.) WAF.  
[~] Number of requests: 2  
  
(root@kali2025)-[~]  
#
```

7.Finally, I use OWASP zap to automatically find the vulnerabilities.



With getting these tool's support, I found below details about vulnerability.

1) Introduction

1.1 Domain	https://www.vendhq.com/
1.2 Severity	• LOW

2) Vulnerability

2.1 Vulnerability title	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) OWASP_2021_A01 CWE-497
2.2 Vulnerability description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
2.3 Affected components	Affected component is webserver headers. The HTTP response also includes the X-Powered-By header, which reveals the backend technology: X-Powered-By: PHP/7.4.33 <div>Evidence</div> <div>X-Powered-By : PHP/7.4.33</div> (This is from ZAP generated report)
2.4 Impact assessment	Reveals backend technology (e.g : - PHP version) and facilitates easier preparation of attacks on known vulnerabilities by hackers. PHP/7.4.33 may be vulnerable if not patched. Increases attack surface by leaking unwanted information. May help in reconnaissance stage of an attack (e.g: - targeting with known CVEs).

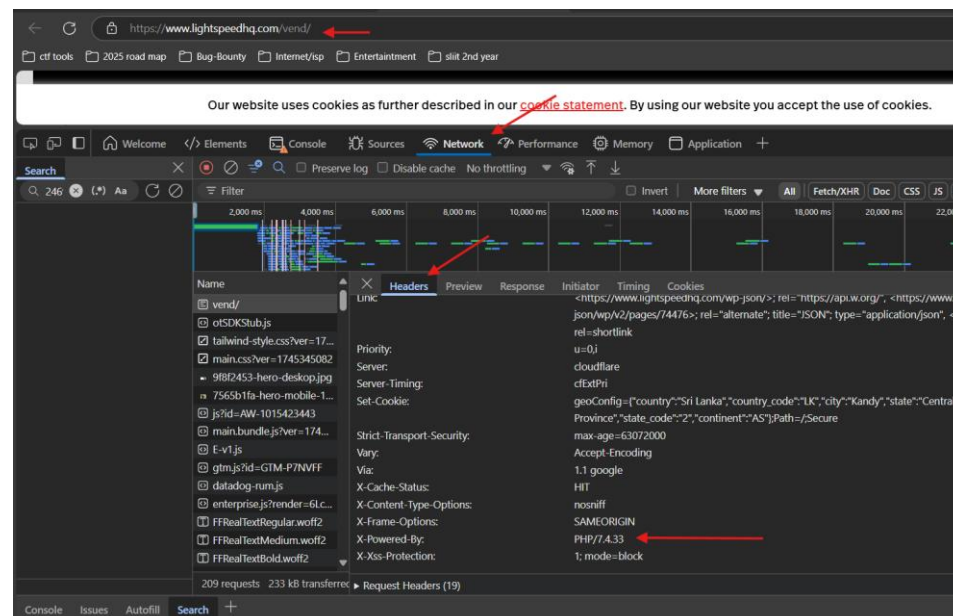
2.5 Steps to reproduce

Method 1: by using zap

1. Launch ZAP tool and scan the <https://www.vendhq.com/>.
2. Once scanned, head over to the “Alerts tab”.
3. Look for an alert called "Server Leaks Information via 'X-Powered-By'".
4. Open up the alert and examine the prove section.

Check if the HTTP response has: X-Powered-By: PHP/7.4.33

Method2: by using developer tools



Check if the HTTP response has: X-Powered-By: PHP/7.4.33

2.6 Proof of concept

The screenshot shows the ZAP 2.16.0 interface. The top pane displays an HTTP response from `https://www.vendhq.com`. The response headers include `X-Powered-By: PHP/7.4.33`. The bottom pane shows an alert titled "Server Leaks Information via 'X-Powered-By' HTTP Response Header". The alert details include the URL `https://www.vendhq.com/`, risk level "Low", confidence "Medium", and a description: "The web/application server is leaking information via one or more 'X-Powered-By' HTTP response headers. This information can be used to identify the underlying technology stack and may be used to exploit vulnerabilities in the underlying technology stack."

The HTTP Response given by ZAP tool

This is a close-up view of the HTTP response headers from the previous screenshot. The header `X-Powered-By: PHP/7.4.33` is highlighted, demonstrating the leakage of backend technology information.

This verifies that the application is leaking backend technology information through the response header.

2.7 Proposed mitigation or fix

Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

	<p>This is how the mitigate X-powered-By header from server configuration(backends).</p> <p>eg:- 1) Apache</p> <p>Header unset X-powered-By</p>
--	---