Sri Lanka Institute of Information Technology

Web Security – IE2062

Topic: Bug Bounty Report 10

Y2S2.WE.CS

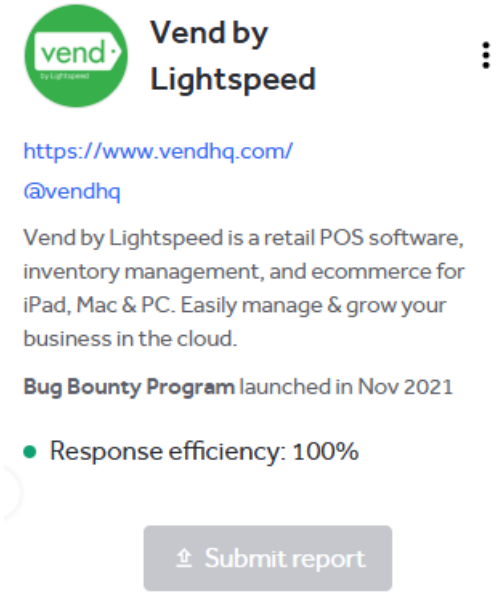
Name: S.D.W.Gunaratne

(IT23241978)

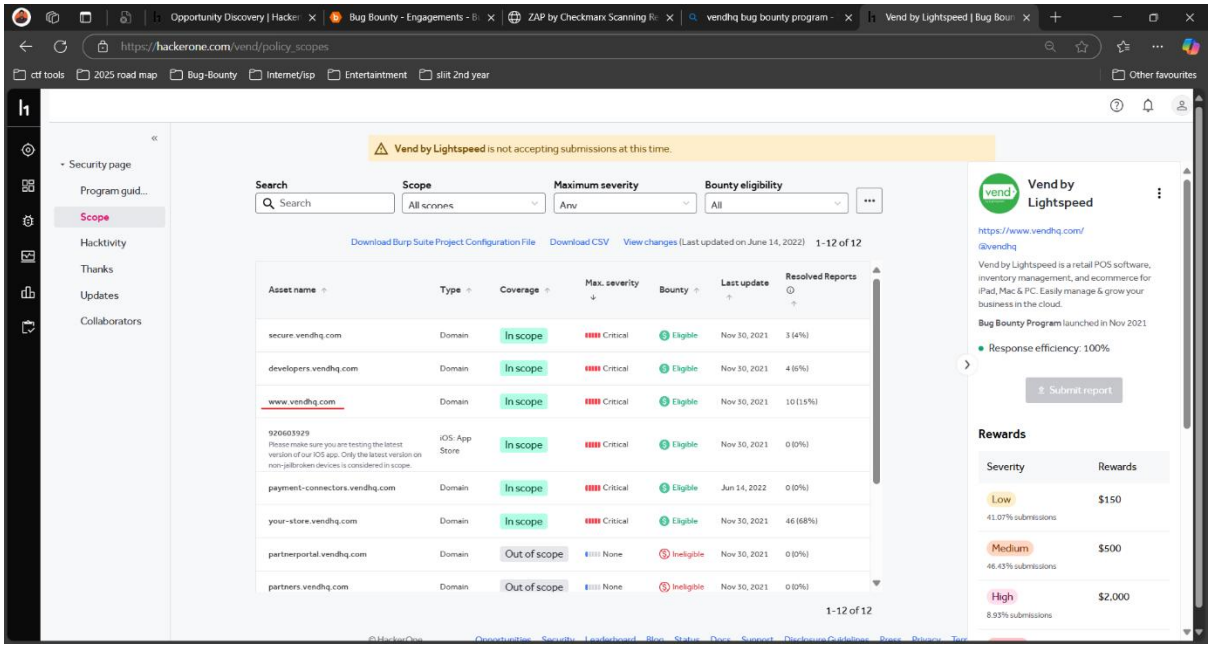
Table of Content

How I started?

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

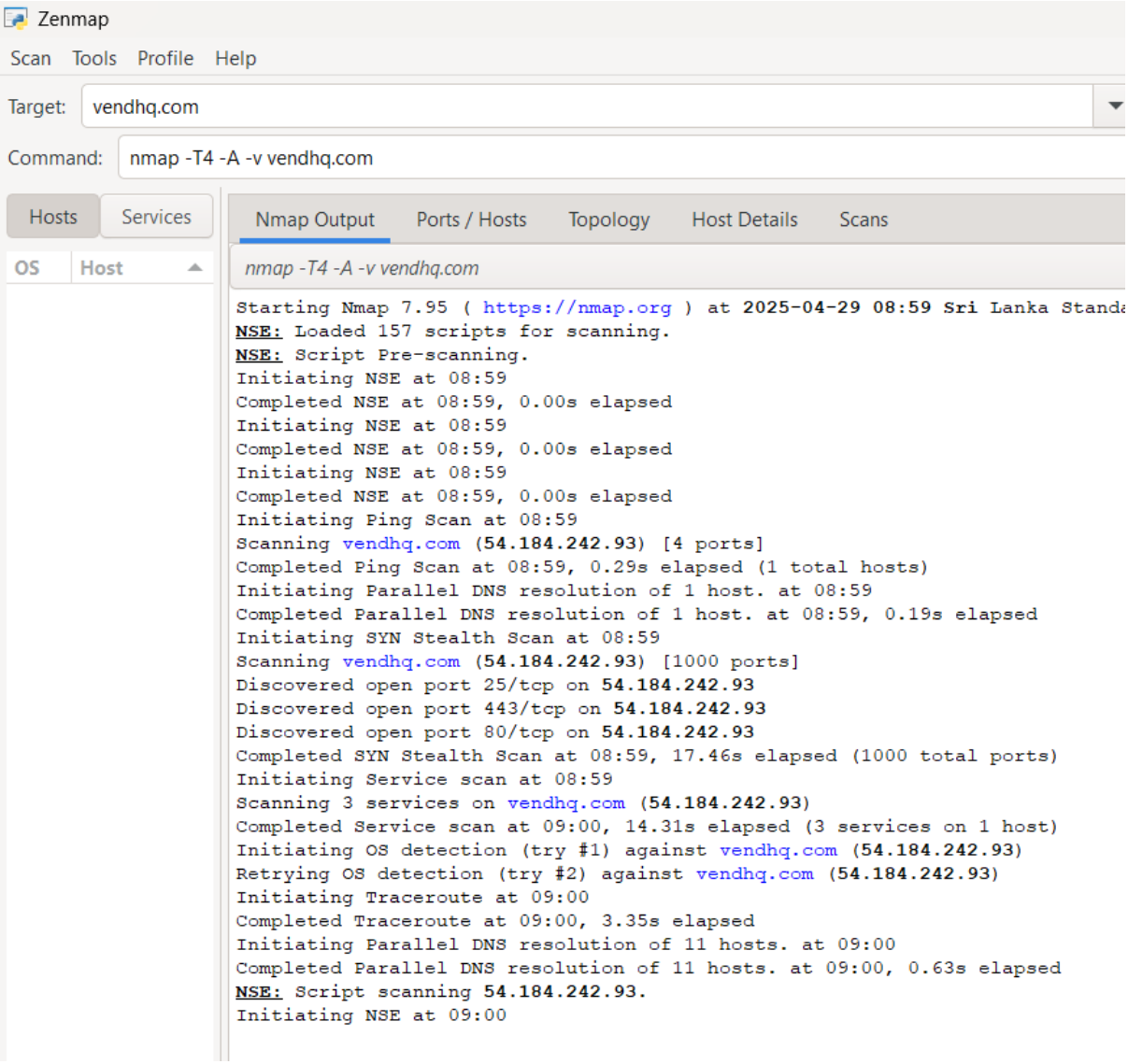


2. Then, I discovered full main domain allowed for scope, so that I choose https://www.vendhq.com .



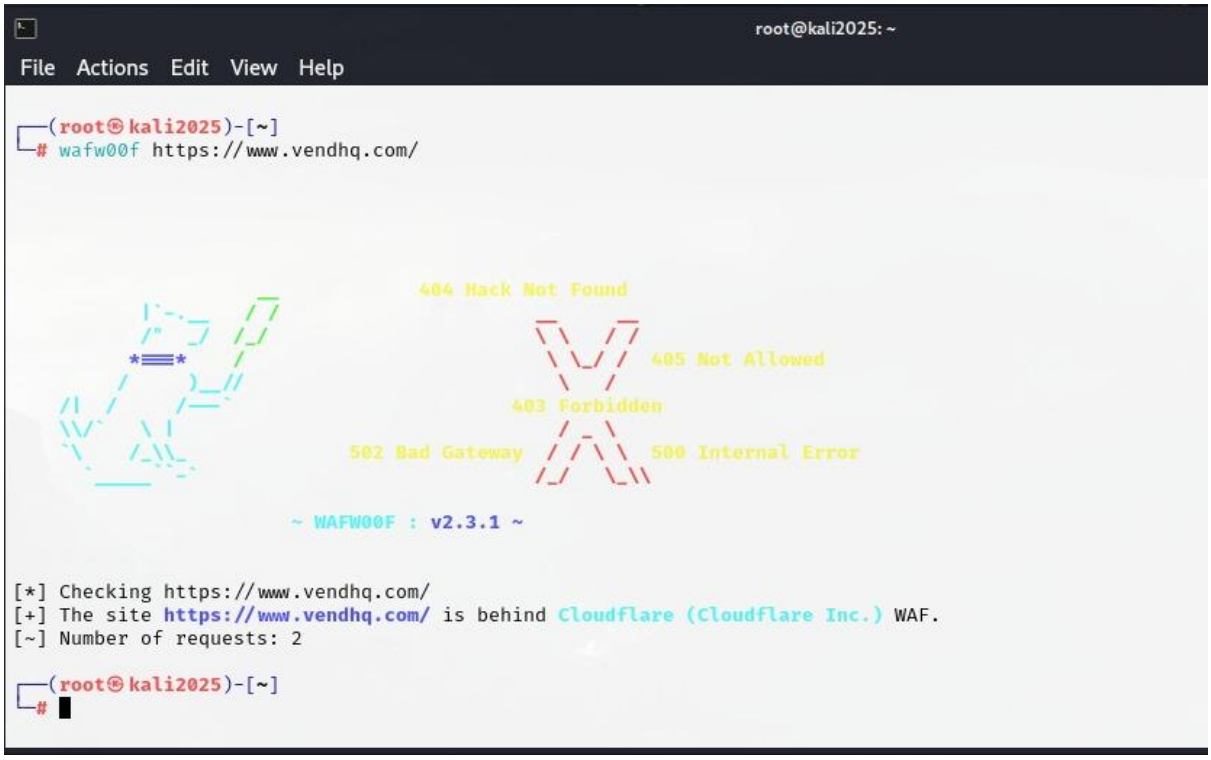
3. I use several methods/tools to do penetration testing.

4. First, I used Nmap. It helps me to find what are the open ports, Identify the web technologies such as webservers.

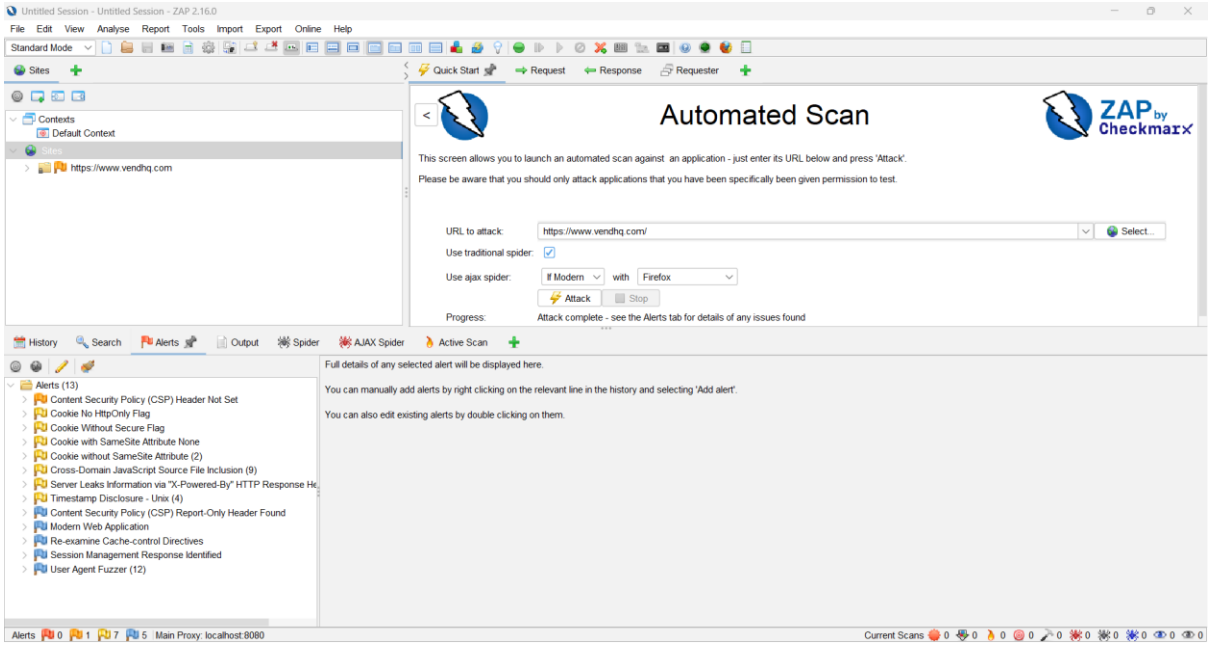


5. Secondly, I used Subfider tool to find hidden or forgotten web asserts. Because hidden web assert can have poor security, unpatched vulnerabilities.

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.



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



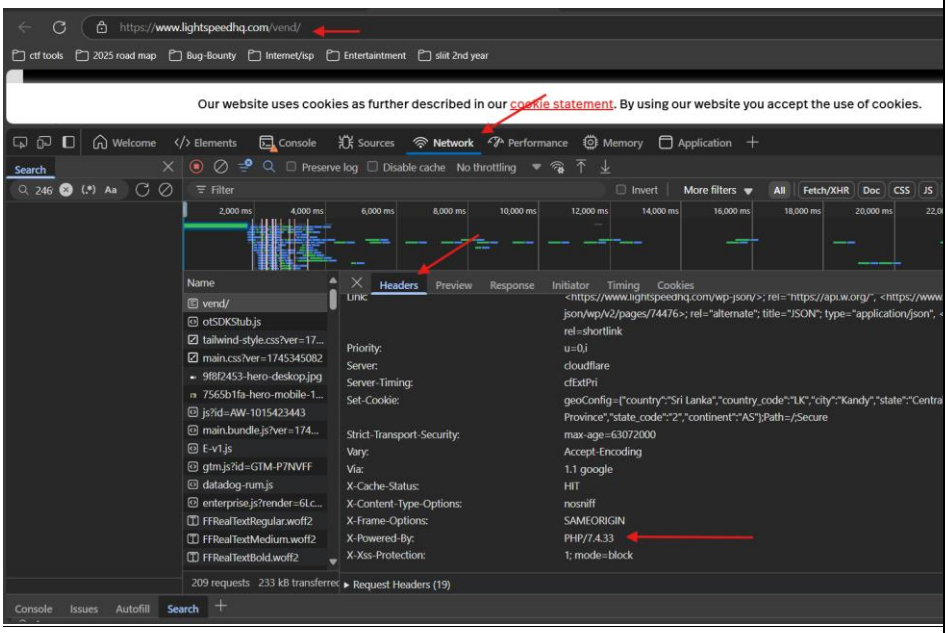
With getting these tool's support, I found below details about vulnerability.

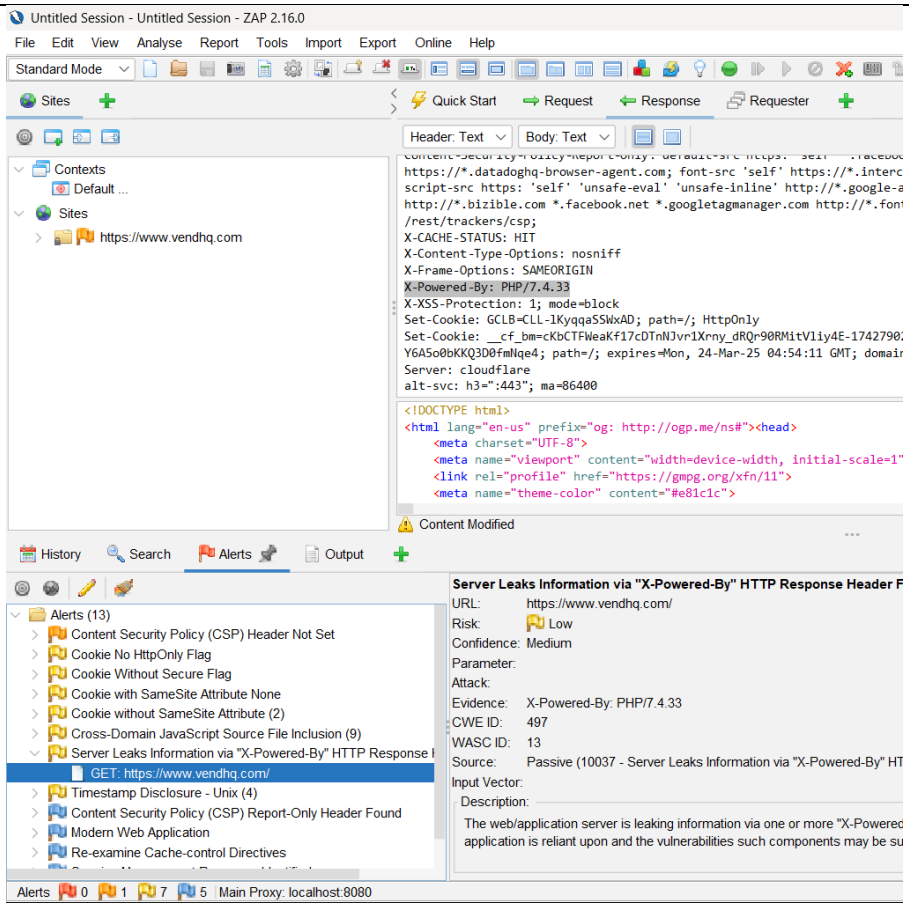
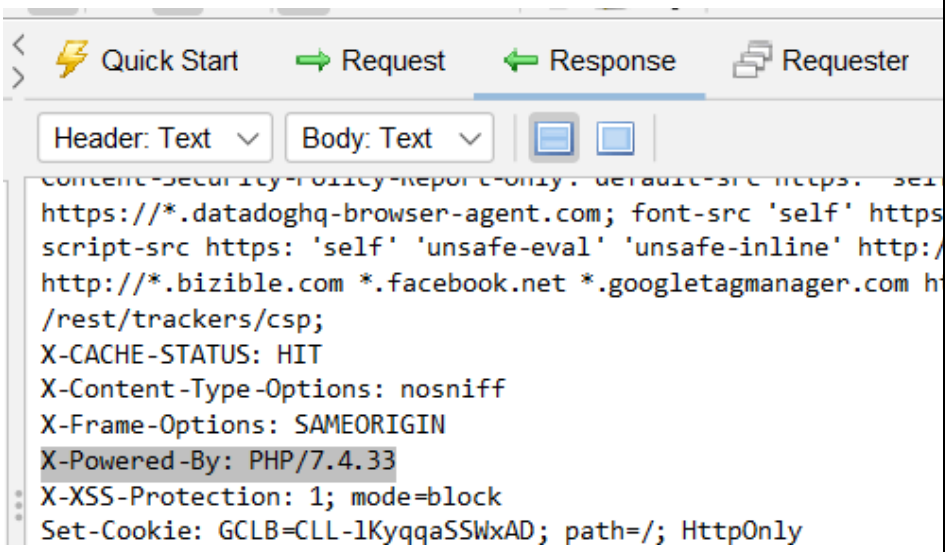
1) Introduction

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 **Evidence** X-Powered-By: PHP/7.4.33 (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	<u>Method 1: by using zap</u> 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 <u>Method2: by using developer tools</u>  Check if the HTTP response has: X-Powered-By: PHP/7.4.33

2.6 Proof of concept	 The HTTP Respond given by ZAP tool  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.

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