Footprinting and Reconnaissance:

Footprinting and reconnaissance are essential phases in the process of hacking and cybersecurity. Footprinting involves gathering information about a target system or network using various passive techniques, such as searching publicly available information, social engineering, or dumpster diving. On the other hand, reconnaissance involves actively probing the target to collect more detailed information, such as network topology, system vulnerabilities, and potential entry points. These initial steps provide hackers with crucial insights into their target's infrastructure, helping them plan and execute successful cyber attacks. Effective defense strategies involve implementing robust security measures to thwart these reconnaissance efforts and safeguard sensitive information.

Footprinting Working:

Footprinting, a crucial phase in cybersecurity, involves gathering information about a target system or network. This process typically unfolds in several steps:

1. **Passive Information Gathering:** Initially, passive techniques are employed to collect publicly available data about the target, such as through search engines, social media, and online forums.

2. **Active Information Gathering:** Next, active techniques are used to gather more specific details about the target, including network infrastructure, IP addresses, domain names, and organizational structure. This may involve network scanning, WHOIS queries, DNS interrogation, and social engineering tactics.

3. **Analysis and Documentation:** The information gathered is then analyzed to identify potential vulnerabilities, weak points, and entry opportunities into the target system. This phase involves organizing and documenting the collected data for use in subsequent stages of the attack.

4. **Risk Assessment:** Finally, a risk assessment is conducted to evaluate the likelihood and potential impact of various attack vectors. This helps hackers

prioritize their strategies and determine the most effective approach for exploiting the target's weaknesses.

Reconnaissance Working:

Reconnaissance, a critical phase in cybersecurity, involves actively probing a target system or network to gather detailed information. Here are the steps typically involved in reconnaissance:

1. **Open Source Intelligence (OSINT) Gathering:** Utilize publicly available sources such as search engines, social media, and online forums to collect initial information about the target.

2. **Network Scanning:** Use specialized tools like Nmap to identify active hosts, open ports, and services running on the target network. This helps in mapping the network topology and discovering potential vulnerabilities.

3. **Enumeration:** Probe deeper into the target network to gather specific information about user accounts, shares, and other resources. Techniques such as DNS enumeration, SNMP enumeration, and SMB enumeration are commonly employed for this purpose.

4. **Vulnerability Scanning:** Employ vulnerability scanning tools like Nessus or OpenVAS to identify weaknesses and security flaws in the target systems. This step helps in assessing the level of risk associated with the target environment.

5. **Social Engineering:** Leverage social engineering tactics to manipulate individuals into divulging sensitive information or providing unauthorized access to systems. This may involve phishing emails, pretexting, or physical infiltration.

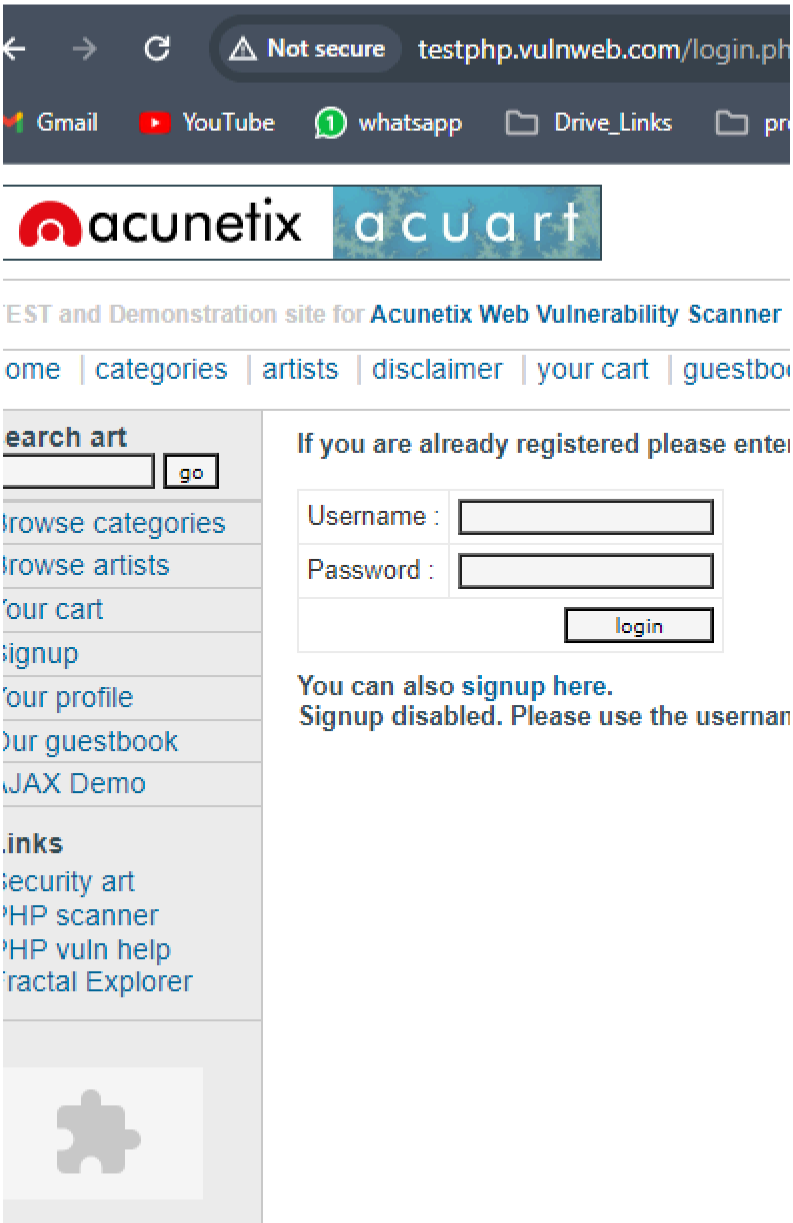
6. **Analysis and Documentation:** Analyze the gathered reconnaissance data to identify potential attack vectors and vulnerabilities. Document the findings for use in planning and executing subsequent stages of the attack.

By systematically conducting reconnaissance, attackers can gain valuable insights into the target environment, allowing them to tailor their attack strategies for maximum effectiveness while minimizing the risk of detection.

In Steps:

Step 1: Access Google by opening a web browser such as Chrome, Firefox, or Safari.

● In the search bar, which is typically located at the top of the browser window, paste the following URL: http://testphp.vulnweb.com/ and then press the "Enter" key on your keyboard. This action will take you to the specified website.



If you are already registered please ente

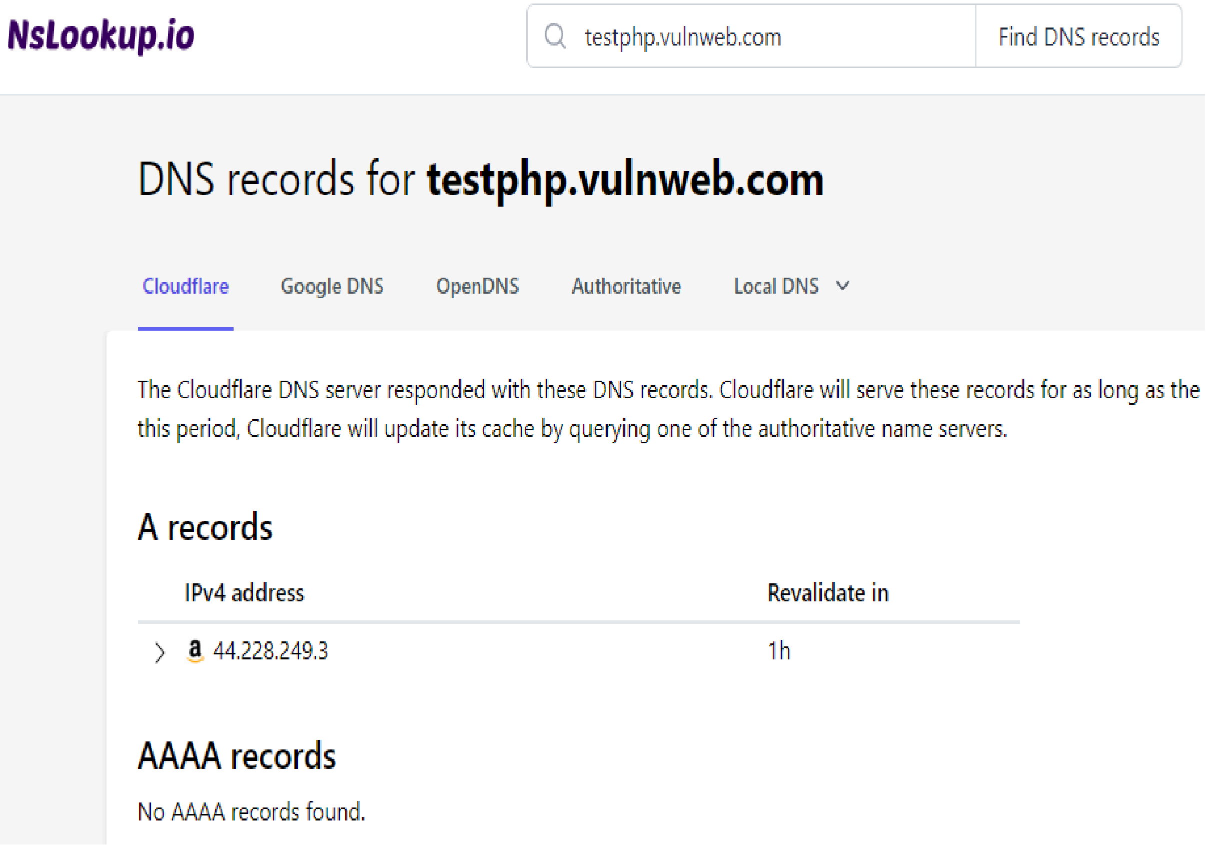
Username :	
Password :	
	login

You can also signup here.
Signup disabled. Please use the usernan

Step 2: Perform footprinting and reconnaissance on the provided website. Footprinting involves gathering information about the target system or network to identify potential vulnerabilities, while reconnaissance involves actively scanning and probing the target to gather more detailed information.

● You can use various tools and techniques such as WHOIS lookup, Google dorking, website analysis tools, and social engineering techniques to gather information about the target website.

Step 3: Use Nmap, a network scanning tool, to collect information about the target website. Nmap allows you to discover hosts and services on a computer network, thus providing valuable insights into the network topology and available services. With Nmap, you can scan for open ports, detect operating systems, and gather other network-related information.



DNS records for **testphp.vulnweb.com**

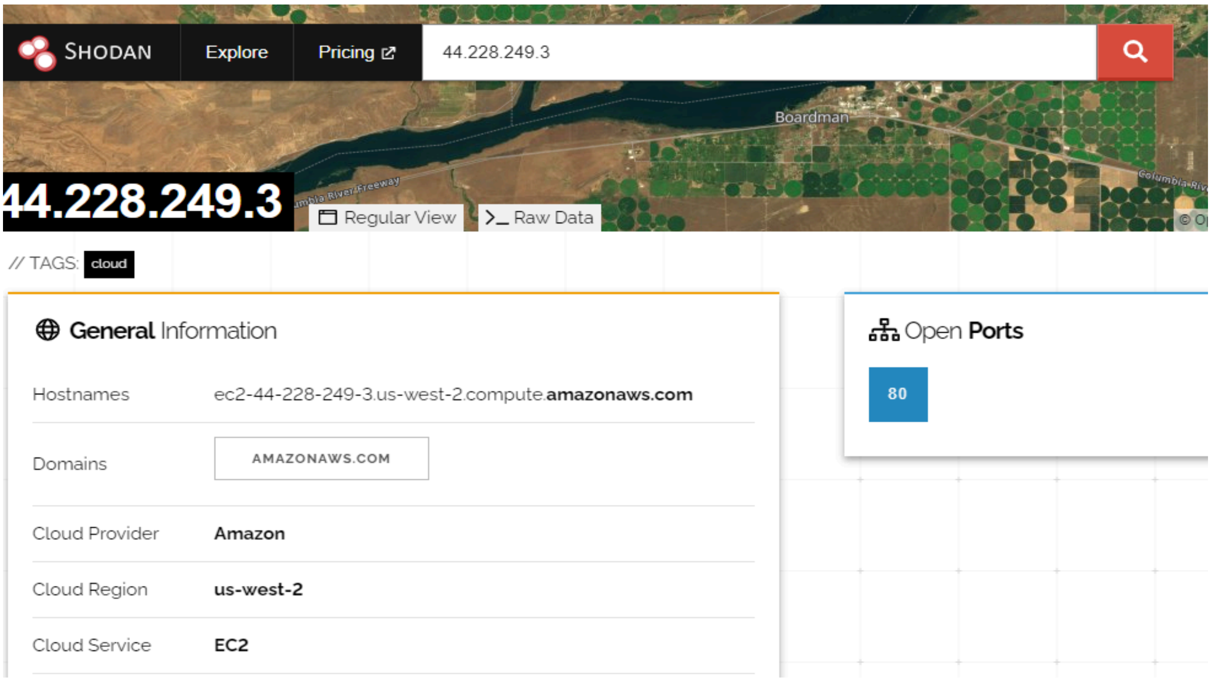
The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
44.228.249.3	1h

AAAA records

No AAAA records found.



44.228.249.3

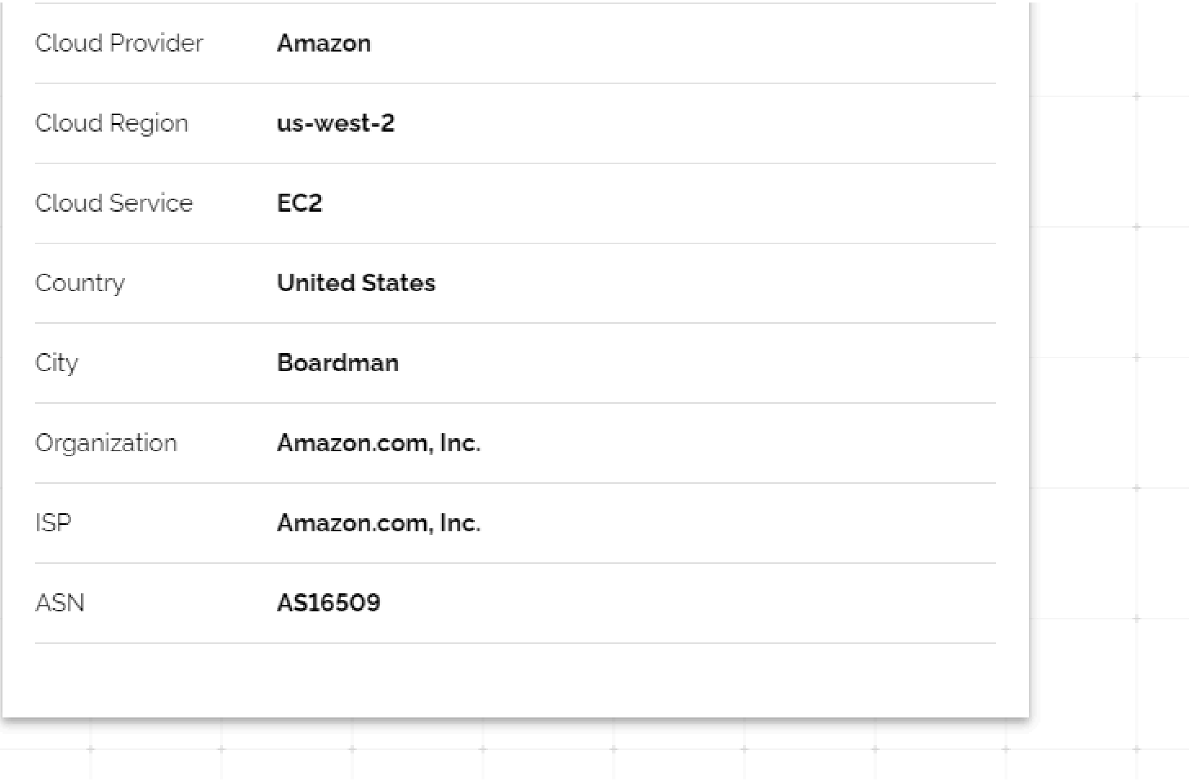
// TAGS: cloud

General Information

Hostnames	ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Domains	AMAZONAWS.COM
Cloud Provider	Amazon
Cloud Region	us-west-2
Cloud Service	EC2

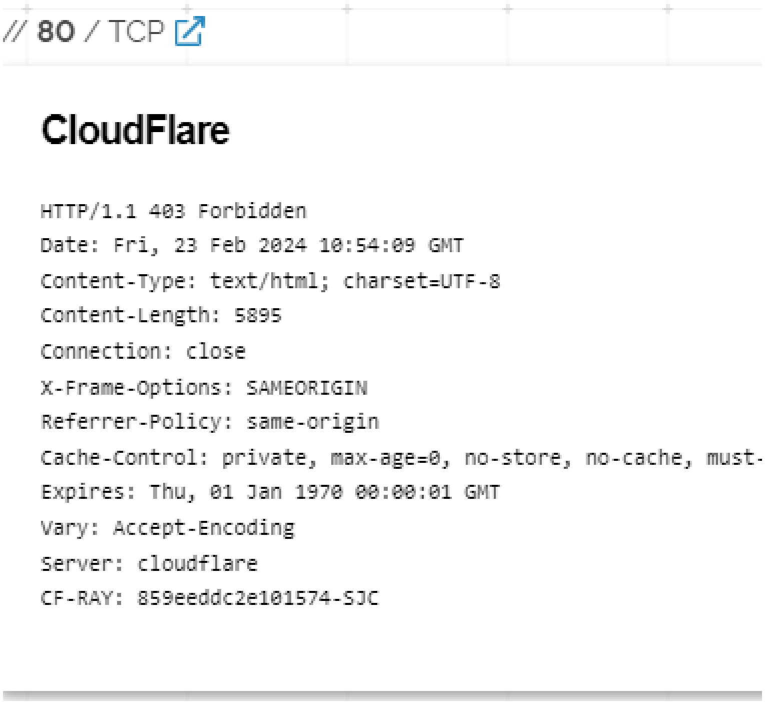
Open Ports

80



Cloud Provider	Amazon
Cloud Region	us-west-2
Cloud Service	EC2
Country	United States
City	Boardman
Organization	Amazon.com, Inc.
ISP	Amazon.com, Inc.
ASN	AS16509

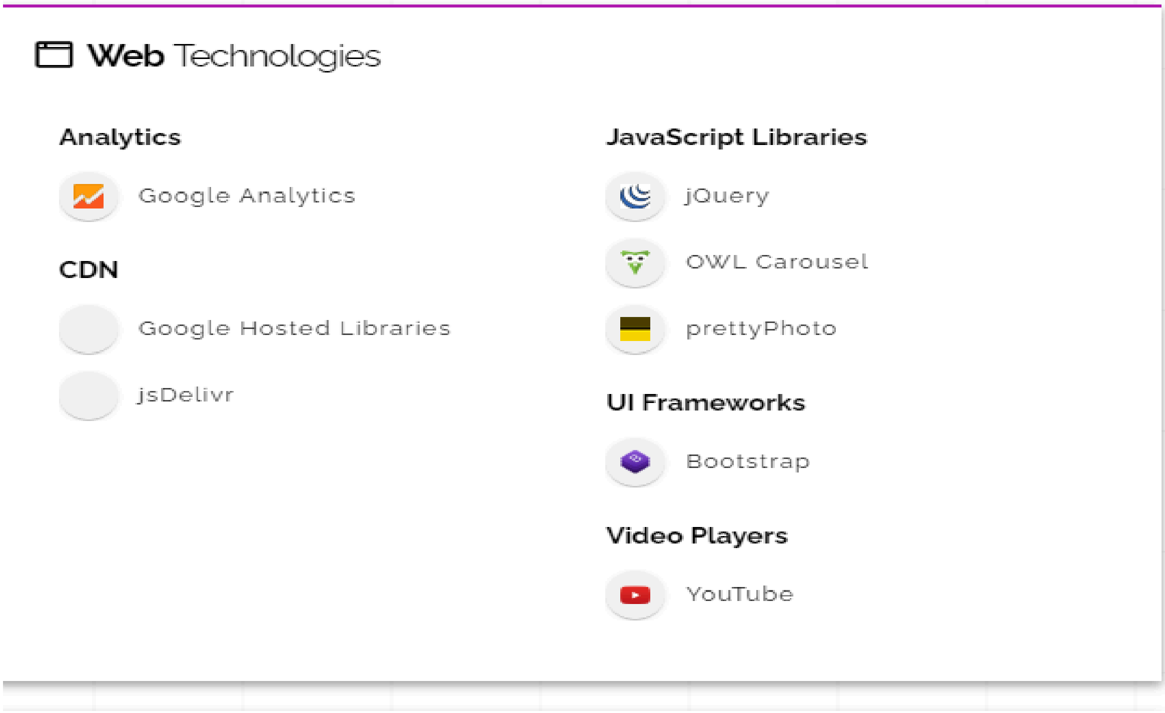
Step 4: Document your findings. It's essential to record all the information you gather during the footprinting, reconnaissance, and Nmap scanning processes.



// 80 / TCP

CloudFlare

```
HTTP/1.1 403 Forbidden
Date: Fri, 23 Feb 2024 10:54:09 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5895
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 859eeddc2e101574-SJC
```



Web Technologies

Analytics

- Google Analytics

CDN

- Google Hosted Libraries
- jsDelivr

JavaScript Libraries

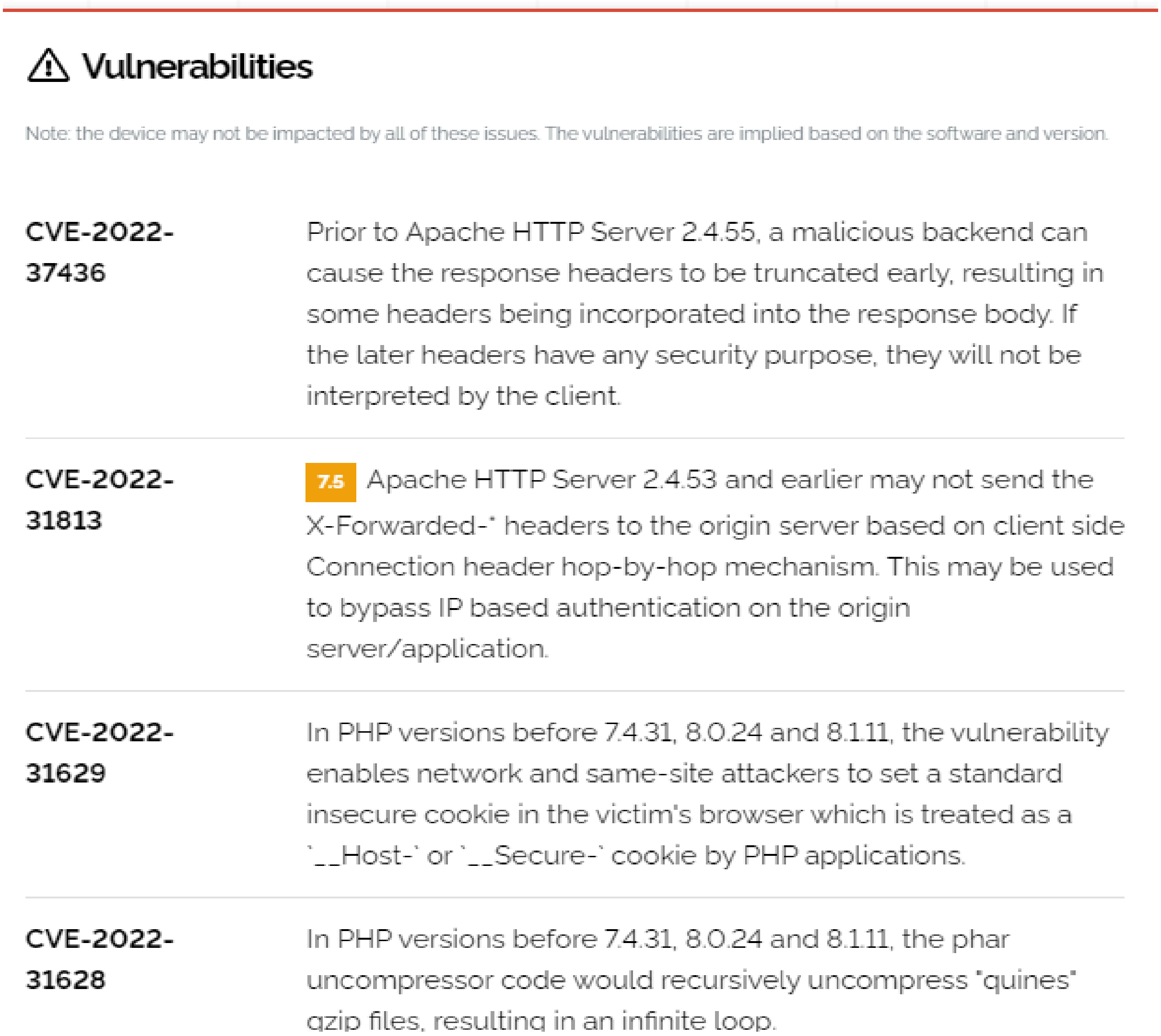
- jQuery
- OWL Carousel
- prettyPhoto

UI Frameworks

- Bootstrap

Video Players

- YouTube



⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2022-37436

Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

CVE-2022-31813

7.5 Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

CVE-2022-31629

In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications.

CVE-2022-31628

In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.

A.Ganesh
PSCMR
B.Tech Final year
21KT5A4701