CYB101 Project 7

Required Challenge Screenshots (Required)

Use the answer boxes below to fill in your results from completing this project.

Part 1: Shodan Lookups on 5 Hosts

Host #1

Website / URL: www.roblox.com IP Address: 128.116.102.4

Screenshot #1: The output of the appropriate curl command to internetdb.shodan.io

```
Last login: Tue Apr 15 05:21:43 2025 from 153.33.34.98
codepath@lab0000000:~$ curl https://internetdb.shodan.io/3.139.24
9.238
{"cpes":[],"hostnames":["rx-nonprod.cm-elsevier.com","ec2-3-139-
249-238.us-east-2.compute.amazonaws.com"],"ip":"3.139.249.238","
ports":[80,443],"tags":["cloud"],"vulns":[]}codepath@lab0000000:~
$
```

How many CVEs Shodan find? Which ones?

None

Host #2

Website / URL: www.amazon.com IP Address: 96.45.82.76

Screenshot #1: The output of the appropriate curl command to internetdb.shodan.io

```
codepath@lab000000:~$ curl https://internetdb.shodan.io/96.45.82
.76
{"cpes":[],"hostnames":["redirection.dnsmadeeasy.com"],"ip":"96.
45.82.76","ports":[80,443],"tags":[],"vulns":[]}codepath@lab0000
00:~$
```

How many CVEs Shodan find? Which ones?

None were found

Host #3

Website / URL: www.walmart.com IP Address: 158.85.97.214

Screenshot #1: The output of the appropriate curl command to internetdb.shodan.io

```
codepath@lab000000:~$ curl https://internetdb.shodan.io/158.85.9
7.214
{"cpes":["cpe:/a:f5:nginx:1.14.1", "cpe:/a:php:php:7.2.34", "cpe:/a:pureftpd:pure-ftpd"], "hostnames":["www.0ivei.com", "0ivei.com", "d6.61.559e.ip4.static.sl-reverse.com"], "ip":"158.85.97.214", "po rts":[21,80,443], "tags":["eol-product"], "vulns":["CVE-2019-9513", "CVE-2019-9511", "CVE-2022-4900", "CVE-2017-8923", "CVE-2021-3618", "CVE-2019-9516", "CVE-2013-2220", "CVE-2021-23017", "CVE-2024-2511
7", "CVE-2018-16845", "CVE-2019-20372", "CVE-2022-37454", "CVE-2022-31629", "CVE-2007-3205", "CVE-2022-31628", "CVE-2023-44487"]}codepa
th@lab000000:~$
```

How many CVEs Shodan find? Which ones?

Shodan found 16 CVEs.

"CVE-2019-9513","CVE-2019-9511","CVE-2022-4900","CVE-2017-8923","CVE-2021-3618","CVE-2019-95 16","CVE-2013-2220","CVE-2021-23017","CVE-2024-25117","CVE-2018-16845","CVE-2019-20372","CVE-2022-37454","CVE-2022-31629","CVE-2007-3205","CVE-2022-31628","CVE-2023-44487"]}

Host#4

Website / URL: ww

www.ibm.com

IP Address:

128.30.86.64

Screenshot #1: The output of the appropriate curl command to internetdb.shodan.io

codepath@lab000000:~\$ curl https://internetdb.shodan.io/34.86.30.128
{"cpes":["cpe:/a:f5:nginx","cpe:/a:angularjs:angular.js"],"hostnames":["sysco.turbonomic.io","128.30.86.34.bc.googleusercontent.com"]
,"ip":"34.86.30.128","ports":[80,443],"tags":["cloud"],"vulns":[]}codepath@lab0000000:~\$ |

How many CVEs Shodan find? Which ones?

No CVEs were found

Host #5

Website / URL: google.com IP Address: 70.33.166.130

Screenshot #1: The output of the appropriate curl command to internetdb.shodan.io

codepath@lab000000:~\$ curl https://internetdb.shodan.io/70.33.166.130
{"cpes":["cpe:/a:apache:http_server", "cpe:/a:php:php", "cpe:/a:jquery:jquery:3.5.1", "cpe:/a:getbootstrap:bootstrap:bootstrap:3.4.1", "cpe:/a:mysql", "cpe:/a:wordpress:wordpress:", "cpe:/a:wordpress:", "cpe:/a:jquery:jquery:1.12.1", "cpe:/a:lightbox_photo_gallery_project:lightbox_photo_gallery"], "hostnames":["www.intensivets.com", "intensivets.com"], "ip":"70.33.166.130", "ports":[80,443,8443], "tags":[], "vulns":["CVE-2023-52222", "CVE-2021-24323", "CVE-2022-0775", "CVE-2022-2099", "CVE-2021-32790", "CVE-2024-9944", "CVE-2024-6484"]}codepath@lab000000:~\$

How many CVEs Shodan find? Which ones?

Shodan found 7 CVEs.

"CVE-2023-52222","CVE-2021-24323","CVE-2022-0775","CVE-2022-2099","CVE-2021-32790","CVE-2024-9944","CVE-2024-6484

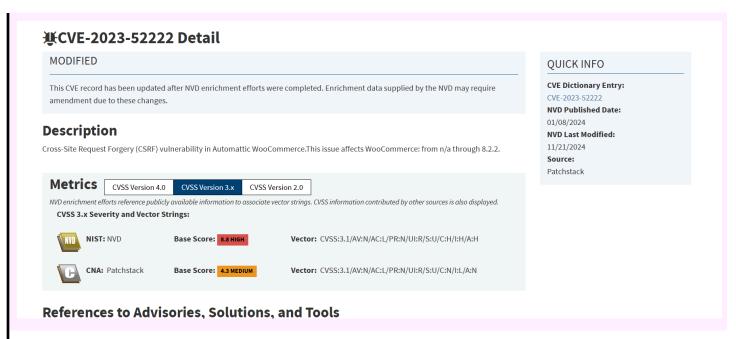
Part 2: Looking up CVEs

Use the answer boxes below to fill in your results when looking up CVEs. For the **Risk Level** field, put either a number rating (e.g., 3/10) or an emoji (e.g., %)!

CVE #1

CVE: CVE-2023-52222 Host: Patchstack Risk Level: 4.3

Screenshot: The results of looking up the CVE in the *National Vulnerability Database*.

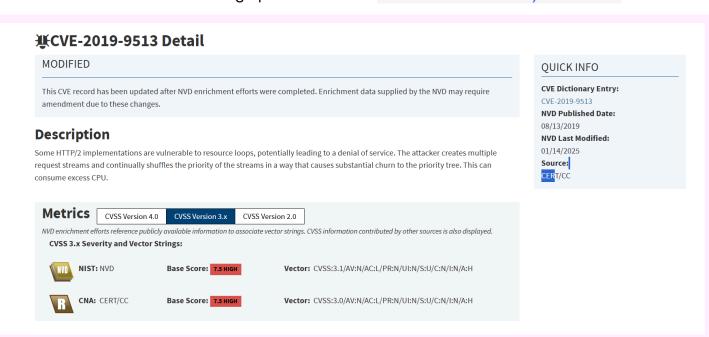


Analysis: In a few words, what does this CVE mean?

Cross-Site Request Forgery (CSRF) vulnerability in Automattic WooCommerce. This issue affects WooCommerce: from n/a through 8.2.2.

CVE #2

Screenshot: The results of looking up the CVE in the National Vulnerability Database.



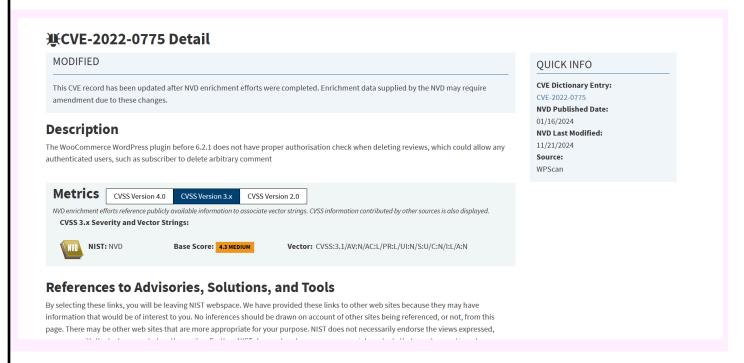
Analysis: In a few words, what does this CVE mean?

Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service. The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU.

CVE #3

CVE: CVE-2022-0775 **Host: WPScan Risk Level: 4.3**

Screenshot: The results of looking up the CVE in the *National Vulnerability Database*.



Analysis: In a few words, what does this CVE mean?

The WooCommerce WordPress plugin before 6.2.1 does not have proper authorisation check when deleting reviews, which could allow any authenticated users, such as subscriber to delete arbitrary comment