

# 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@lab000000:~$ curl https://internetdb.shodan.io/3.139.249.238
{"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@lab000000:~$
```

**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@lab0000000:~$ 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@lab0000000:~$
```

**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@lab0000000:~$ curl https://internetdb.shodan.io/158.85.97.214
{"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", "ports": [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-2024-25117", "CVE-2018-16845", "CVE-2019-20372", "CVE-2022-37454", "CVE-2022-31629", "CVE-2007-3205", "CVE-2022-31628", "CVE-2023-44487"]}codepath@lab0000000:~$
```

**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-2019-9516","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: **www.ibm.com**

IP Address: **128.30.86.64**

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

```
codepath@lab0000000:~$ 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@lab0000000:~$ 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:3.4.1","cpe:/a:mysql:mysql","cpe:/a:wordpress:wordpress","cpe:/a:woocommerce:woocommerce:5.0.0:~~~wordpress~~~","cpe:/a:jquery:jquery-ui: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@lab0000000:~$
```

**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](#).

## CVE-2023-52222 Detail

### MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

### Description

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

### Metrics

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

#### CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score: 8.8 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



CNA: Patchstack

Base Score: 4.3 MEDIUM

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

### QUICK INFO

#### CVE Dictionary Entry:

CVE-2023-52222

#### NVD Published Date:

01/08/2024

#### NVD Last Modified:

11/21/2024

#### Source:

Patchstack

### References to Advisories, Solutions, and Tools

**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

**CVE:** CVE-2019-9513

**Host:** CERT/CC

**Risk Level:** 7.5

**Screenshot:** The results of looking up the CVE in the [National Vulnerability Database](#).

## CVE-2019-9513 Detail

### MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

### Description

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.

### Metrics

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

#### CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score: 7.5 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



CNA: CERT/CC

Base Score: 7.5 HIGH

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

### QUICK INFO

#### CVE Dictionary Entry:

CVE-2019-9513

#### NVD Published Date:

08/13/2019

#### NVD Last Modified:

01/14/2025

#### Source:

CERT/CC

**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](#).

### CVE-2022-0775 Detail

#### MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

#### QUICK INFO

**CVE Dictionary Entry:**  
CVE-2022-0775  
**NVD Published Date:**  
01/16/2024  
**NVD Last Modified:**  
11/21/2024  
**Source:**  
WPScan

#### Description


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

#### Metrics

CVSS Version 4.0   CVSS Version 3.x   CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

**CVSS 3.x Severity and Vector Strings:**

 **NIST:** NVD      **Base Score:** 4.3 MEDIUM      **Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

#### References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed,

**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