CYB101 Project 7

(🔗 Instructions Page)

👤 Student Name: Weicong Xie
✉️ Student Email: Weicongx.wx@gmail.com

Reflection (Required)

> 🤔 **Reflection Question #1:** If I had to **explain "what is a CVE?" in 3 emojis,** they would be… (Feel free to put other comments about your experience this unit here, too!)
>
> 🐞🔓📋

> 🌐**Reflection Question #2:** Have you ever practiced Open Source Intelligence in your own life?
>
> I have now.

> 📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

Required Challenge Screenshots (Required)

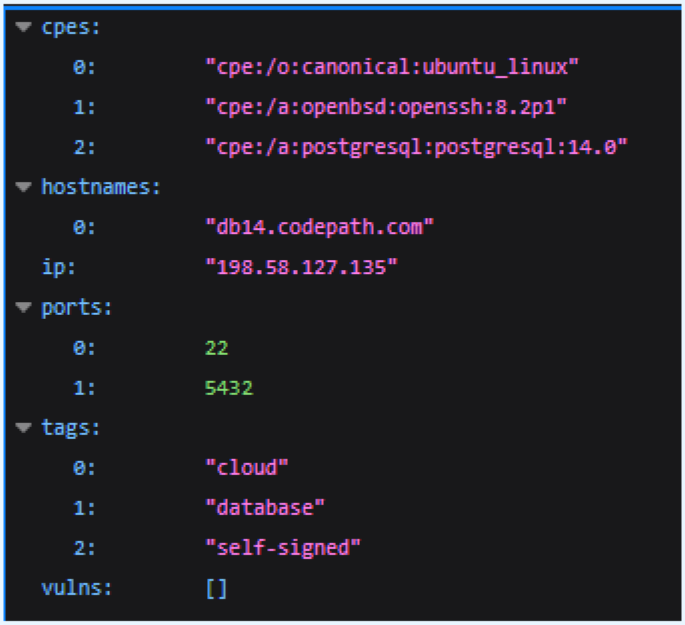
Use the answer boxes below to fill in your results from completing this project.

Part 1: Shodan Lookups on 5 Hosts

Host #1

Website / URL:	**https://www.shodan.io/host/198.58.127.135**	**IP Address:**	**198.58.127.135**

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



```
▼ cpes:
    0:        "cpe:/o:canonical:ubuntu_linux"
    1:        "cpe:/a:openbsd:openssh:8.2p1"
    2:        "cpe:/a:postgresql:postgresql:14.0"
▼ hostnames:
    0:        "db14.codepath.com"
  ip:         "198.58.127.135"
▼ ports:
    0:        22
    1:        5432
▼ tags:
    0:        "cloud"
    1:        "database"
    2:        "self-signed"
  vulns:      []
```

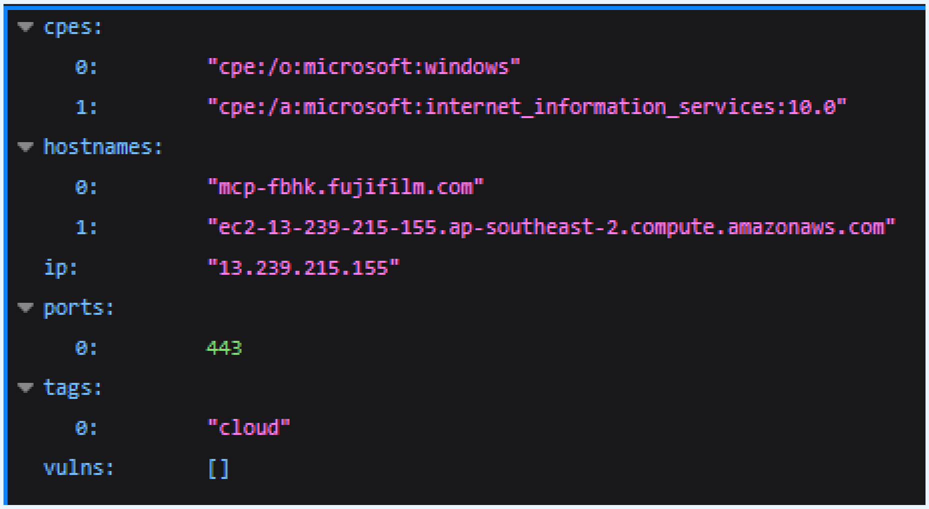
How many CVEs Shodan find? Which ones?

None

Host #2

Website / URL:	**https://www.shodan.io/host/13.239.215.155**	**IP Address:**	**13.239.215.155**

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



```
▼ cpes:
    0:        "cpe:/o:microsoft:windows"
    1:        "cpe:/a:microsoft:internet_information_services:10.0"
▼ hostnames:
    0:        "mcp-fbhk.fujifilm.com"
    1:        "ec2-13-239-215-155.ap-southeast-2.compute.amazonaws.com"
  ip:         "13.239.215.155"
▼ ports:
    0:        443
▼ tags:
    0:        "cloud"
  vulns:      []
```

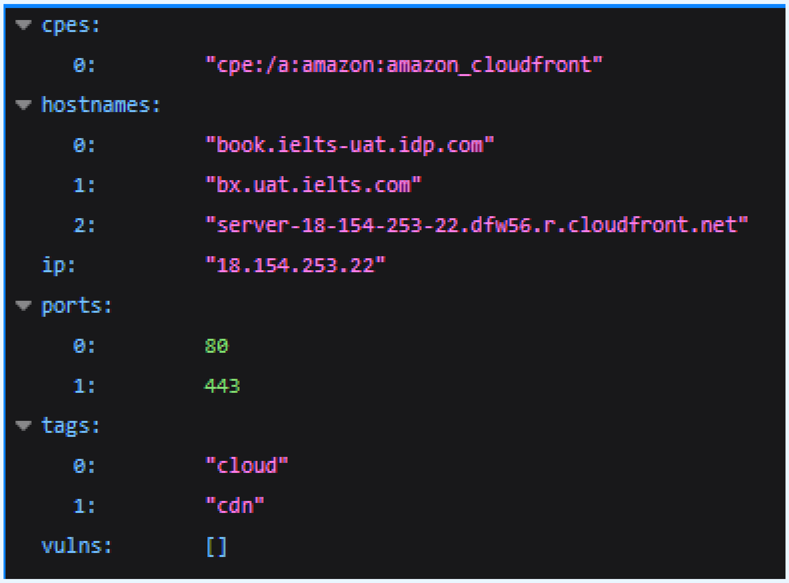
How many CVEs Shodan find? Which ones?

None

Host #3

Website / URL:	**https://www.shodan.io/host/18.154.253.22**	**IP Address:**	**18.154.253.22**

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



```
▼ cpes:
    0:        "cpe:/a:amazon:amazon_cloudfront"
▼ hostnames:
    0:        "book.ielts-uat.idp.com"
    1:        "bx.uat.ielts.com"
    2:        "server-18-154-253-22.dfw56.r.cloudfront.net"
  ip:         "18.154.253.22"
▼ ports:
    0:        80
    1:        443
▼ tags:
    0:        "cloud"
    1:        "cdn"
  vulns:      []
```

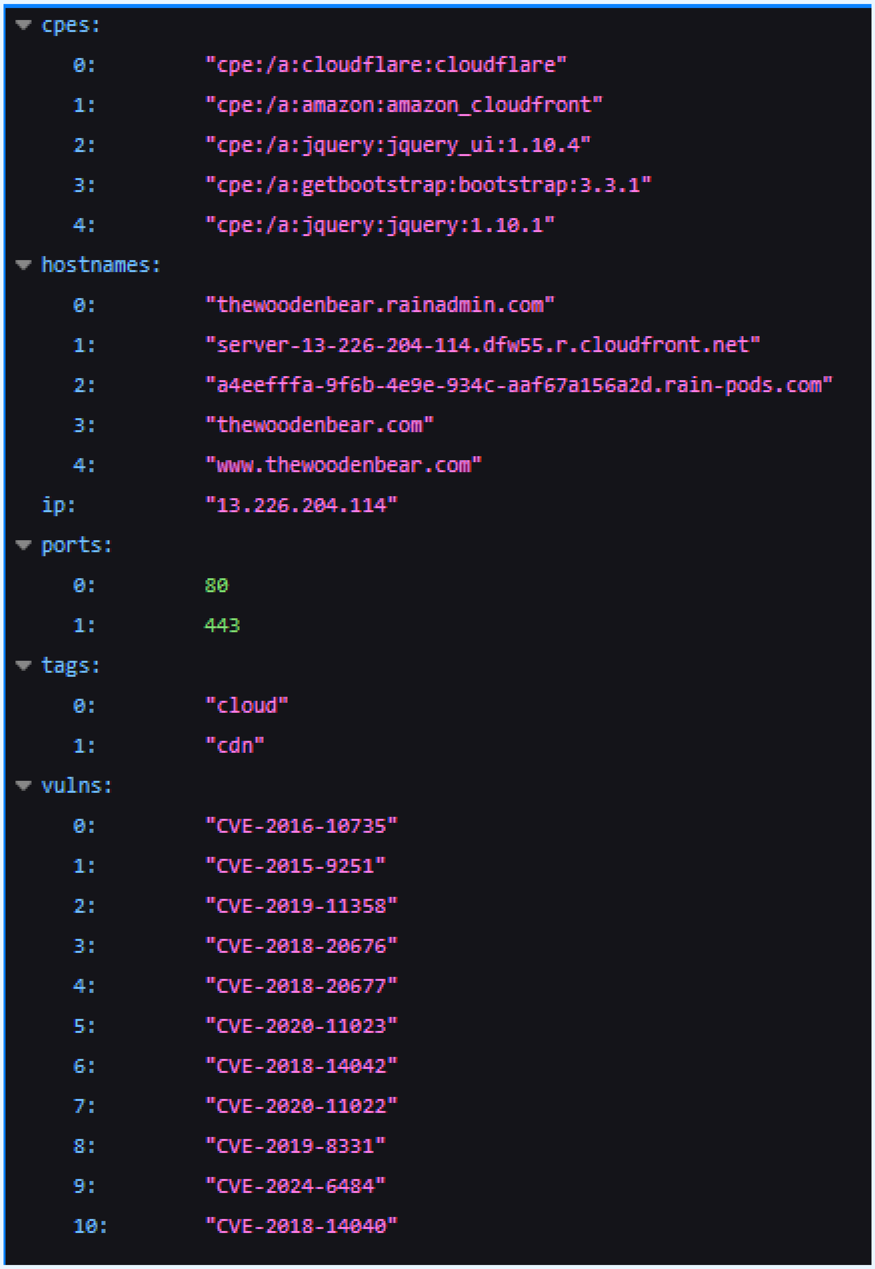
How many CVEs Shodan find? Which ones?

None

Host #4

Website / URL:	**https://www.shodan.io/host/13.226.204.114**	**IP Address:**	**13.226.204.114**

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



```
▼ cpes:
    0:         "cpe:/a:cloudflare:cloudflare"
    1:         "cpe:/a:amazon:amazon_cloudfront"
    2:         "cpe:/a:jquery:jquery_ui:1.10.4"
    3:         "cpe:/a:getbootstrap:bootstrap:3.3.1"
    4:         "cpe:/a:jquery:jquery:1.10.1"
▼ hostnames:
    0:         "thewoodenbear.rainadmin.com"
    1:         "server-13-226-204-114.dfw55.r.cloudfront.net"
    2:         "a4eefffa-9f6b-4e9e-934c-aaf67a156a2d.rain-pods.com"
    3:         "thewoodenbear.com"
    4:         "www.thewoodenbear.com"
  ip:          "13.226.204.114"
▼ ports:
    0:         80
    1:         443
▼ tags:
    0:         "cloud"
    1:         "cdn"
▼ vulns:
    0:         "CVE-2016-10735"
    1:         "CVE-2015-9251"
    2:         "CVE-2019-11358"
    3:         "CVE-2018-20676"
    4:         "CVE-2018-20677"
    5:         "CVE-2020-11023"
    6:         "CVE-2018-14042"
    7:         "CVE-2020-11022"
    8:         "CVE-2019-8331"
    9:         "CVE-2024-6484"
    10:        "CVE-2018-14040"
```

How many CVEs Shodan find? Which ones?

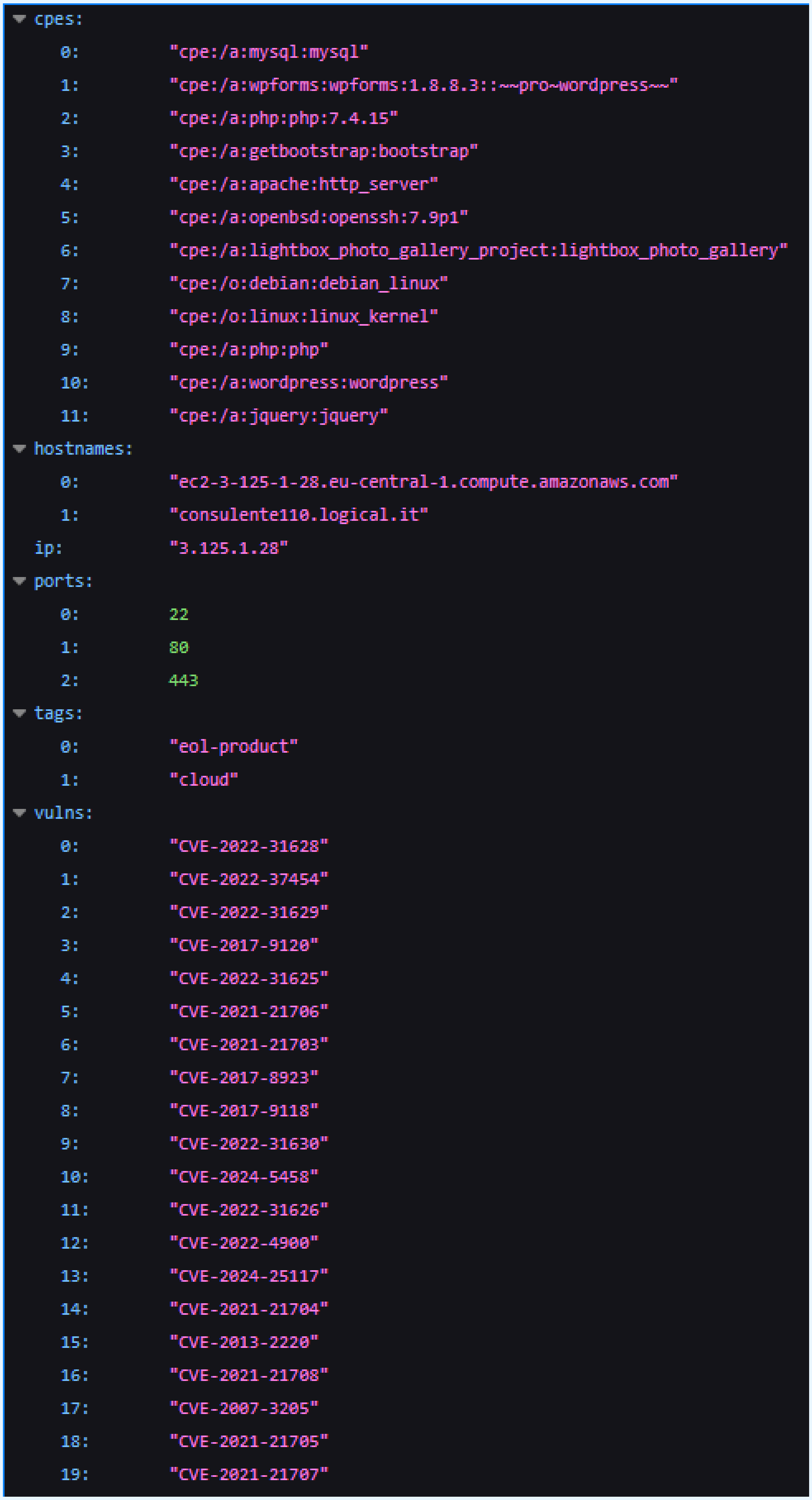
0	**"CVE-2016-10735"**		
1	**"CVE-2015-9251"**		
2	**"CVE-2019-11358"**		

3	**"CVE-2018-20676"**		
4	**"CVE-2018-20677"**		
5	**"CVE-2020-11023"**		
6	**"CVE-2018-14042"**		
7	**"CVE-2020-11022"**		
8	**"CVE-2019-8331"**		
9	**"CVE-2024-6484"**		
10	**"CVE-2018-14040"**		

Host #5

Website / URL:	**https://www.shodan.io/host/3.125.1.28**	**IP Address:**	**3.125.1.28**

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



```
▼ cpes:
    0:          "cpe:/a:mysql:mysql"
    1:          "cpe:/a:wpforms:wpforms:1.8.8.3::~~pro~wordpress~~"
    2:          "cpe:/a:php:php:7.4.15"
    3:          "cpe:/a:getbootstrap:bootstrap"
    4:          "cpe:/a:apache:http_server"
    5:          "cpe:/a:openbsd:openssh:7.9p1"
    6:          "cpe:/a:lightbox_photo_gallery_project:lightbox_photo_gallery"
    7:          "cpe:/o:debian:debian_linux"
    8:          "cpe:/o:linux:linux_kernel"
    9:          "cpe:/a:php:php"
    10:         "cpe:/a:wordpress:wordpress"
    11:         "cpe:/a:jquery:jquery"
▼ hostnames:
    0:          "ec2-3-125-1-28.eu-central-1.compute.amazonaws.com"
    1:          "consulente110.logical.it"
  ip:           "3.125.1.28"
▼ ports:
    0:          22
    1:          80
    2:          443
▼ tags:
    0:          "eol-product"
    1:          "cloud"
▼ vulns:
    0:          "CVE-2022-31628"
    1:          "CVE-2022-37454"
    2:          "CVE-2022-31629"
    3:          "CVE-2017-9120"
    4:          "CVE-2022-31625"
    5:          "CVE-2021-21706"
    6:          "CVE-2021-21703"
    7:          "CVE-2017-8923"
    8:          "CVE-2017-9118"
    9:          "CVE-2022-31630"
    10:         "CVE-2024-5458"
    11:         "CVE-2022-31626"
    12:         "CVE-2022-4900"
    13:         "CVE-2024-25117"
    14:         "CVE-2021-21704"
    15:         "CVE-2013-2220"
    16:         "CVE-2021-21708"
    17:         "CVE-2007-3205"
    18:         "CVE-2021-21705"
    19:         "CVE-2021-21707"
```

How many CVEs Shodan find? Which ones?

0	**"CVE-2022-31628"**		
1	**"CVE-2022-37454"**		
2	**"CVE-2022-31629"**		
3	**"CVE-2017-9120"**		
4	**"CVE-2022-31625"**		
5	**"CVE-2021-21706"**		
6	**"CVE-2021-21703"**		
7	**"CVE-2017-8923"**		
8	**"CVE-2017-9118"**		
9	**"CVE-2022-31630"**		
10	**"CVE-2024-5458"**		
11	**"CVE-2022-31626"**		
12	**"CVE-2022-4900"**		

13	**"CVE-2024-25117"**		
14	**"CVE-2021-21704"**		
15	**"CVE-2013-2220"**		
16	**"CVE-2021-21708"**		
17	**"CVE-2007-3205"**		
18	**"CVE-2021-21705"**		
19	**"CVE-2021-21707"**		

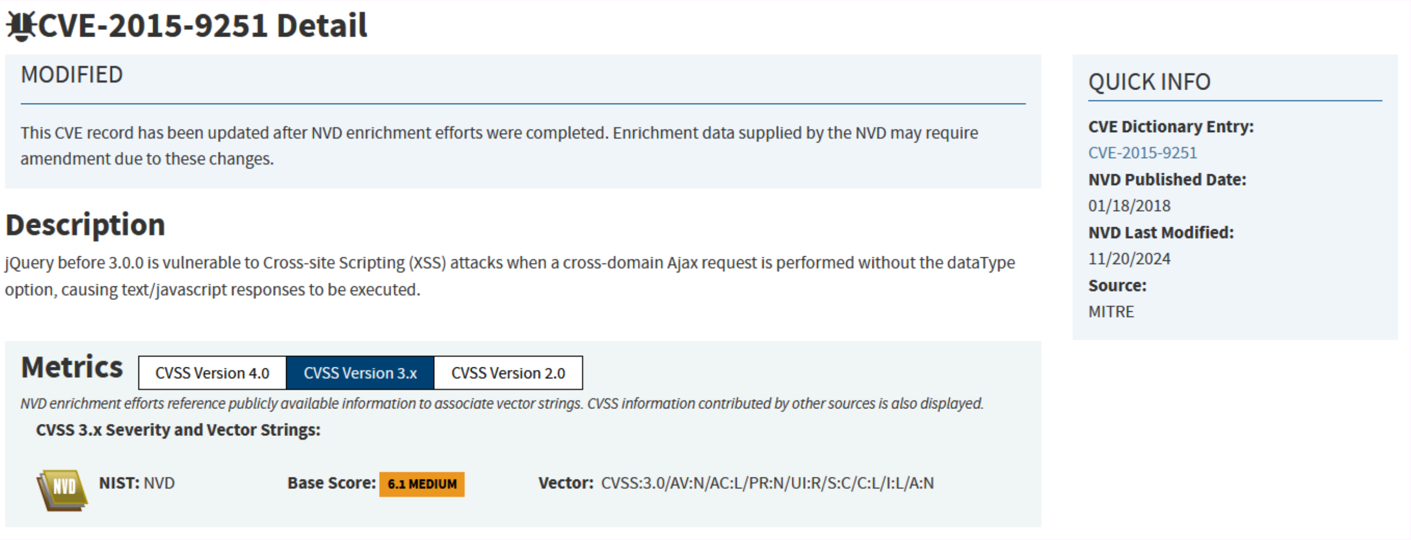
Part 2: Looking up CVEs

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-2015-9251**	**Host:**	**#4**	**Risk Level:**	**5**

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



CVE-2015-9251 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

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Metrics

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:** 6.1 MEDIUM **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

QUICK INFO

CVE Dictionary Entry:
CVE-2015-9251
NVD Published Date:
01/18/2018
NVD Last Modified:
11/20/2024
Source:
MITRE

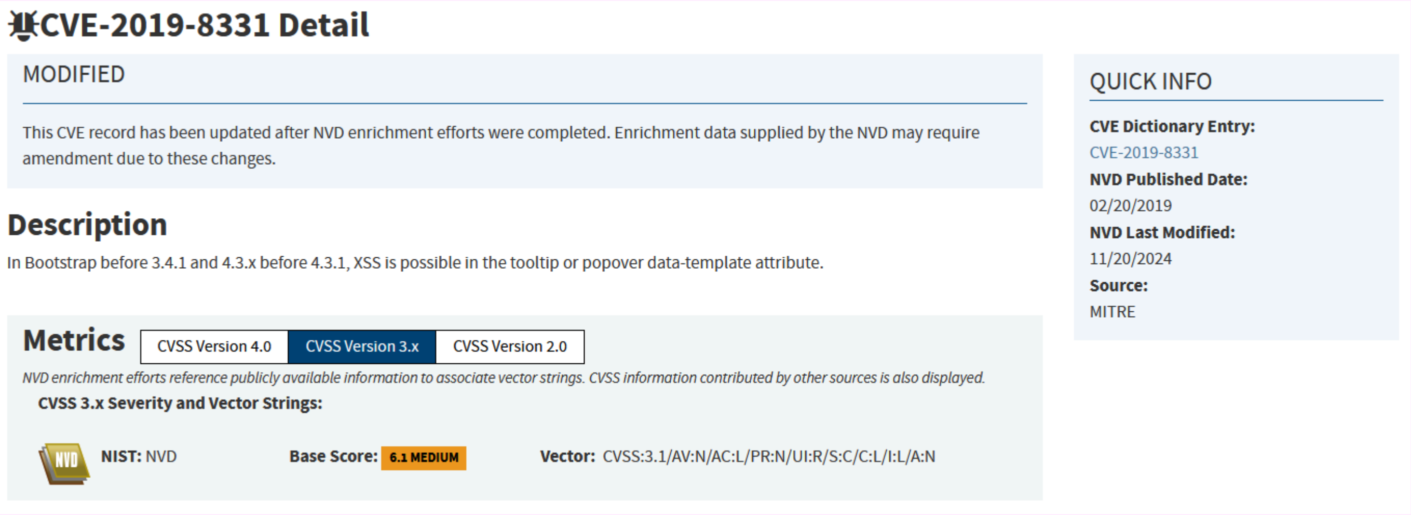
Analysis: In a few words, what does this CVE mean?

Vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option

CVE #2

CVE:	**CVE-2019-8331**	**Host:**	**#4**	**Risk Level:**	**5**

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



CVE-2019-8331 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

In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.

Metrics

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

QUICK INFO

CVE Dictionary Entry:
CVE-2019-8331
NVD Published Date:
02/20/2019
NVD Last Modified:
11/20/2024
Source:
MITRE

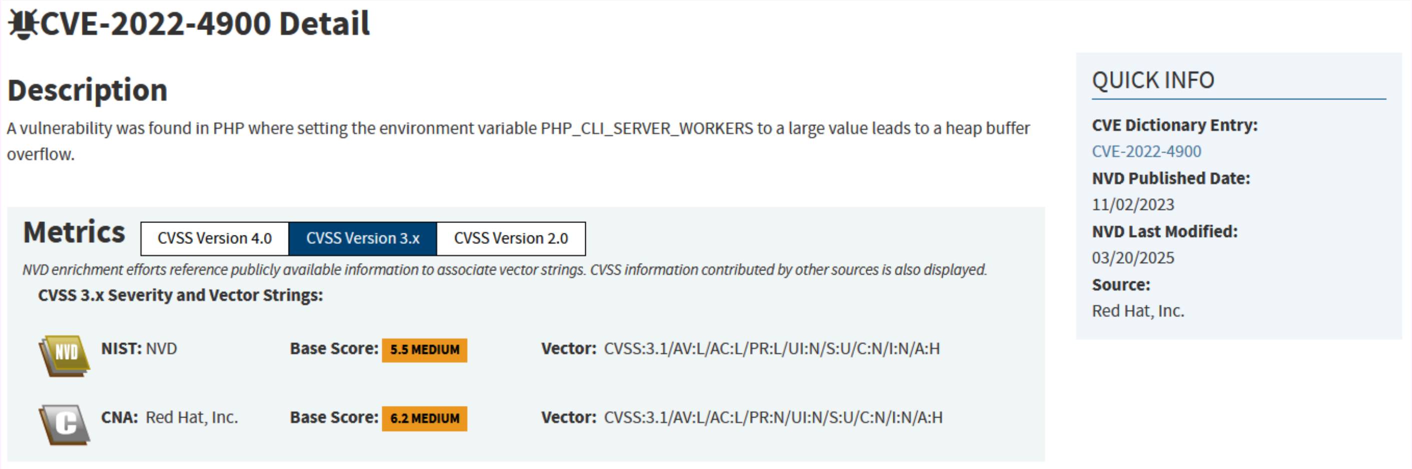
Analysis: In a few words, what does this CVE mean?

XSS is possible in the tooltip or popover data-template attribute

CVE #3

CVE:	**CVE-2022-4900**	**Host:**	**#5**	**Risk Level:**	**6**

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



CVE-2022-4900 Detail

Description

A vulnerability was found in PHP where setting the environment variable PHP_CLI_SERVER_WORKERS to a large value leads to a heap buffer overflow.

Metrics

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:** 5.5 MEDIUM	**Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CNA: Red Hat, Inc.	**Base Score:** 6.2 MEDIUM	**Vector:** CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

QUICK INFO

CVE Dictionary Entry:
CVE-2022-4900
NVD Published Date:
11/02/2023
NVD Last Modified:
03/20/2025
Source:
Red Hat, Inc.

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

PHP vulnerability that leads to a heap buffer overflow.

Stretch Challenge (Optional)

Stretch Challenge #1: A screenshot showing your script (and its' output) for **automatically gathering Shodan information on a given IP address**

[Insert Screenshot Here]

Notes (Optional)**:**

Stretch Challenge #2: A screenshot showing your script (and its' output) for **looking up a given CVE using CIRCL**

[Insert Screenshot Here]

Notes (Optional)**:**

Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

Reflection

- ☑ ~~Reflection Question #1 answered above~~
- ☑ ~~Reflection Question #2 answered above~~
- ☐ Shoutouts Completed (Optional)

Required Challenge

- ☑ ~~Host #1~~
- ☑ ~~Host #2~~
- ☑ ~~Host #3~~
- ☑ ~~Host #4~~
- ☑ ~~Host #5~~
- ☑ ~~CVE #1~~
- ☑ ~~CVE #2~~
- ☑ ~~CVE #3~~

Stretch Challenge

- ☐ Challenge #1
- ☐ Challenge #2