


# CYB101 Project 7

 Student Name: Nafis Uddin

 Student Email: nafis.uddin.c@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 worked on so many CTFs related to Open Source Intelligence

 **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:** `http://www.google-gruyere.appspot.com/` **IP Address:** `142.250.115.153`

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

[\[Insert Screenshot Here\]](#)

```
(kali㉿kali)-[~]
$ curl https://internetdb.shodan.io/142.250.115.153
{"cpes":[],"hostnames":["rq-in-f153.1e100.net"],"ip":"142.250.115.153","ports":[80,443],"tags":["self-signed"],"vulns":[]}

(kali㉿kali)-[~]
$
```

## How many CVEs Shodan find? Which ones?

Answer here : Zero Vulnerabilities

## Host #2

<b>Website / URL:</b>	<b>http://www.itsecgames.com/</b>	<b>IP Address:</b>	<b>31.3.96.40</b>
-----------------------	-----------------------------------	--------------------	-------------------

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

### [Insert Screenshot Here]

```
(kali㉿kali)-[~]
$ curl https://internetdb.shodan.io/31.3.96.40
{"cpes":["cpe:/a:php:php","cpe:/a:openbsd:openssh:6.7p1","cpe:/a:apache:http_server","cpe:/a:jquery:jquery","cpe:/a:drupal:drupal:7.69","cpe:/a:drupal:drupal:7"],"hostnames":["www.mmebvba.com","www.mmesec.be","mmebvba.com","mmesec.be","www.mmebv.com","mmebv.com","mmesec.com","mmebv.be","www.mmesec.com","www.mmebv.be","web.mmebvba.com"],"ip":"31.3.96.40","ports":[22,80,443],"tags":[],"vulns":["CVE-2009-3778","CVE-2009-3157","CVE-2009-4534","CVE-2010-3423","CVE-2013-0205","CVE-2020-13671","CVE-2010-4775","CVE-2010-2001","CVE-2009-2083","CVE-2009-3922","CVE-2010-4521","CVE-2010-2030","CVE-2009-3442","CVE-2009-2237","CVE-2008-0462","CVE-2012-2056","CVE-2009-2078","CVE-2010-1976","CVE-2008-5999","CVE-2011-5030","CVE-2009-2291","CVE-2009-2370","CVE-2009-3783","CVE-2009-4557","CVE-2009-4296","CVE-2009-4066","CVE-2008-6909","CVE-2020-13666","CVE-2012-1056","CVE-2008-6134","CVE-2008-6836","CVE-2012-0914","CVE-2010-1536","CVE-2009-4042","CVE-2009-3568","CVE-2020-28949","CVE-2010-0697","CVE-2009-4119","CVE-2009-1501","CVE-2010-5312","CVE-2010-4520","CVE-2009-1037","CVE-2010-1543","CVE-2009-3437","CVE-2009-3206","CVE-2009-3915","CVE-2009-4515","CVE-2010-2158","CVE-2009-3652","CVE-2008-6413","CVE-2009-3651","CVE-2009-3435","CVE-2009-3351","CVE-2012-2340","CVE-2011-1066","CVE-2009-4771","CVE-2009-3350","CVE-2008-6972","CVE-2009-4061","CVE-2009-1507","CVE-2009-1342","CVE-2008-4633","CVE-2009-4532","CVE-2009-2074","CVE-2009-0818","CVE-2009-4429","CVE-2008-6135","CVE-2009-4526","CVE-2009-1505","CVE-2009-3654","CVE-2009-1035","CVE-2008-5998","CVE-2020-28948","CVE-2009-3920","CVE-2010-2724","CVE-2010-2125","CVE-2009-4514","CVE-2009-3784","CVE-2010-1958","CVE-2009-4559","CVE-2008-4710","CVE-2009-5096","CVE-2021-41184","CVE-2010-2002","CVE-2009-3780","CVE-2009-1249","CVE-2009-4990","CVE-2009-3785","CVE-2009-1047","CVE-2023-31250","CVE-2009-4525","CVE-2009-3488","CVE-2022-25275","CVE-2009-4527","CVE-2009-4044","CVE-2011-4560","CVE-2009-4602","CVE-2009-3122","CVE-2009-2371","CVE-2009-2610","CVE-2008-1792","CVE-2012-2341","CVE-2010-4519","CVE-2011-1664","CVE-2010-0370","CVE-2020-11023","CVE-2012-2907","CVE-2009-3914","CVE-2009-1069","CVE-2008-1731","CVE-2010-1107","CVE-2012-2339","CVE-2009-4518","CVE-2009-3353","CVE-2008-6910","CVE-2020-36193","CVE-2009-4062","CVE-2021-41183","CVE-2008-5996","CVE-2009-3657","CVE-2020-13672","CVE-2009-4528","CVE-2009-4517","CVE-2009-3156","CVE-2011-4113","CVE-2012-1057","CVE-2010-2123","CVE-2009-4064","CVE-2010-1584","CVE-2009-3779","CVE-2009-3121","CVE-2010-1074","CVE-2009-4513","CVE-2010-1303","CVE-2012-1060","CVE-2009-3650","CVE-2011-1661","CVE-2008-2629","CVE-2009-4063","CVE-2009-4829","CVE-2010-2048","CVE-2009-3919","CVE-2009-3648","CVE-2008-6383","CVE-2009-2077","CVE-2020-13662","CVE-2010-2000","CVE-2009-4520","CVE-2009-1823","CVE-2009-1344","CVE-2010-1539","CVE-2009-4773","CVE-2010-4813","CVE-2008-6908","CVE-2010-1362","CVE-2009-4558","CVE-2009-3921","CVE-2009-3786","CVE-2009-2572","CVE-2009-4772","CVE-2009-4207","CVE-2020-13663","CVE-2009-4065","CVE-2009-3918","CVE-2009-3653","CVE-2009-3782","CVE-2009-4516","CVE-2009-3207","CVE-2009-0382","CVE-2009-1036","CVE-2008-7150","CVE-2010-1358","CVE-2010-0752","CVE-2020-11022","CVE-2011-1663","CVE-2009-2079","CVE-2009-1343","CVE-2010-1530","CVE-2009-3917","CVE-2009-2075","CVE-2010-2352","CVE-2010-1108","CVE-2008-7151","CVE-2009-4533","CVE-2009-0817","CVE-2009-3479","CVE-2010-1984","CVE-2008-6137","CVE-20
```

## How many CVEs Shodan find? Which ones?

Answer here

So many vulnerabilities existed. Here's the list:

"CVE-2009-3778","CVE-2009-3157","CVE-2009-4534","CVE-2010-3423","CVE-2013-0205","CVE-2020-13671","CVE-2010-4775","CVE-2010-2001","CVE-2009-2083","CVE-2009-3922","CVE-2010-4521","CVE-2010-2030","CVE-2009-3442","CVE-2009-2237","CVE-2008-0462","CVE-2012-2056","CVE-2009-2078","CVE-2010-1976","CVE-2008-5999","CVE-2011-5030","CVE-2009-2291","CVE-2009-2370","CVE-2009-3783","CVE-2009-4557","CVE-2009-4296","CVE-2009-4066","CVE-2008-6909","CVE-2020-13666","CVE-2012-1056","CVE-2008-6134","CVE-2008-6836","CVE-2012-0914","CVE-2010-1536","CVE-2009-4042","CVE-2009-3568","CVE-2020-28949","CVE-2010-0697","CVE-2009-4119","CVE-2009-1501","CVE-2010-5312","CVE-2010-4520","CVE-2009-1037","CVE-2010-1543","CVE-2009-3437","CVE-2009-3206","CVE-2009-3915","CVE-2009-4515","CVE-2010-2158","CVE-2009-3652","CVE-2008-6413","CVE-2009-3651","CVE-2009-3435","CVE-2009-3351","CVE-2012-2340","CVE-2011-1066","CVE-2009-4771","CVE-2009-3350","CVE-2008-6972","CVE-2009-4061","CVE-2009-1507","CVE-2009-1342","CVE-2008-4633","CVE-2009-4532","CVE-2009-2074","CVE-2009-0818","CVE-2009-4429","CVE-2008-6135","CVE-2009-4526","CVE-2009-1505","CVE-2009-3654","CVE-2009-1035","CVE-2008-5998","CVE-2020-28948","CVE-2009-3920","CVE-2010-2724","CVE-2010-2125","CVE-2009-4514","CVE-2009-3784","CVE-2010-1958","CVE-2009-4559","CVE-2008-4710","CVE-2009-5096","CVE-2021-41184","CVE-2010-2002","CVE-2009-3780","CVE-2009-1249","CVE-2009-4990","CVE-2009-3785","CVE-2009-1047","CVE-2020-31250","CVE-2009-4525","CVE-2009-3488","CVE-2022-25275","CVE-2009-4527","CVE-2009-4044","CVE-2011-4560","CVE-2009-4602","CVE-2009-3122","CVE-2009-2371","CVE-2009-2610","CVE-2008-1792","CVE-2012-2341","CVE-2010-4519","CVE-2011-1664","CVE-2010-0370","CVE-2020-11023","CVE-2012-2907","CVE-2009-3914","CVE-2009-1069","CVE-2008-1731","CVE-2010-1107","CVE-2012-2339","CVE-2009-4518","CVE-2009-3353","CVE-2008-6910","CVE-2020-36193","CVE-2009-4062","CVE-2021-41183","CVE-2008-5996","CVE-2009-3657","CVE-2020-13672","CVE-2009-4528","CVE-2009-4517","CVE-2009-3156","CVE-2011-4113","CVE-2012-1057","CVE-2010-2123","CVE-2009-4064","CVE-2010-1584","CVE-2009-3779","CVE-2009-3121","CVE-2010-1074","CVE-2009-4513","CVE-2010-1303","CVE-2012-1060","CVE-2009-3650","CVE-2011-1661","CVE-2008-2629","CVE-2009-4063","CVE-2009-4829","CVE-2010-2048","CVE-2009-3919","CVE-2009-3648","CVE-2008-6383","CVE-2009-2077","CVE-2020-13662","CVE-2010-2000","CVE-2009-4520","CVE-2009-1823","CVE-2009-1344","CVE-2010-1539","CVE-2009-4773","CVE-2010-4813","CVE-2008-6908","CVE-2010-1362","CVE-2009-4558","CVE-2009-3921","CVE-2009-3786","CVE-2009-2572","CVE-2009-4772","CVE-2009-4207","CVE-2020-13663","CVE-2009-4065","CVE-2009-3918","CVE-2009-3653","CVE-2009-3782","CVE-2009-4516","CVE-2009-3207","CVE-2009-0382","CVE-2009-1036","CVE-2008-7150","CVE-2010-1358","CVE-2010-0752","CVE-2020-11022","CVE-2011-1663","CVE-2009-2079","CVE-2009-1343","CVE-2010-1530","CVE-2009-3917","CVE-2009-2075","CVE-2010-2352","CVE-2010-1108","CVE-2008-7151","CVE-2009-4533","CVE-2009-0817","CVE-2009-3479","CVE-2010-1984","CVE-2008-6137","CVE-2009-4524","CVE-2008-6020","CVE-2010-1998","CVE-2009-3656","CVE-2009-3354","CVE-2021-41182","CVE-2009-3210","CVE-2022-25271","CVE-2009-3916","CVE-2008-6835","CVE-2010-2353","CVE-2011-0899","CVE-2009-4043","CVE-2009-207

6","CVE-2011-1662","CVE-2009-3363"]

## Host #3

Website / URL: **www.webappsecmovies.sourceforge.net** IP Address: **172.64.150.145**

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

[Insert Screenshot Here]

```
lcc_min/avg/max/mdev = 12.400/15.419/20.009/3.114 ms

(kali㉿kali)-[~]
$ curl https://internetdb.shodan.io/172.64.150.145
{"cpes":[],"hostnames":["sourceforge.net"],"ip":"172.64.150.145","ports":[80,443,2052,2082,2083,2086,2087,2096,8080,8443,8880],"tags":["cdn"],"vulns":[]}
```

**How many CVEs Shodan find? Which ones?**

Answer here

Zero Vulnerabilities

## Host #4

Website / URL: **https://defendtheweb.net /** IP Address: **3.10.42.19**

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

[Insert Screenshot Here]

```
(kali㉿kali)-[~]
$ curl https://internetdb.shodan.io/3.10.42.19
{"cpes":["cpe:/a:jquery:jquery","cpe:/a:openbsd:openssh"],"hostnames":["www.hackthis.co.uk","ec2-3-10-42-19.eu-west-2.compute.amazonaws.com"],"ip":"3.10.42.19","ports":[22,80,443,8000],"tags":["cloud"],"vulns":[]}
```

**How many CVEs Shodan find? Which ones?**

Answer here  
Zero Vulnerabilities

## Host #5

Website / URL: **https://www.root-me.org /** IP Address: **212.129.28.16**

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

[Insert Screenshot Here]

```
(kali㉿kali)-[~]  
$ curl https://internetdb.shodan.io/212.129.28.16  
{ "cpes": [], "hostnames": [ "www.root-me.org" ], "ip": "212.129.28.16", "ports": [ 80, 443 ], "tags": [], "vulns": [] }  
(kali㉿kali)-[~]  
$
```

**How many CVEs Shodan find? Which ones?**

Answer here  
Zero Vulnerabilities

## 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-2009-3778** Host: **http://www.itsecgames.com/** Risk Level: **7.5**

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

[Insert Screenshot Here]

## Q Search Results (Refine Search)

Sort results by: Publish Date Descending

### Search Parameters:

- Results Type: Overview
- Keyword (text search): CVE-2009-3778
- Search Type: Search All
- Match: Exact
- CPE Name Search: false

There are **1** matching records.  
Displaying matches **1** through **1**.

Vuln ID 基	Summary ⓘ	CVSS Severity ⓘ
<b>CVE-2009-3778</b>	SQL injection vulnerability in Moodle Course List 6.x before 6.x-1.2, a module for Drupal, allows remote attackers to execute arbitrary SQL commands via unspecified vectors.  <b>Published:</b> October 26, 2009; 1:30:00 pm -0400	V3.x:(not available) V2.0: <b>7.5 HIGH</b>

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

Answer here

SQL injection vulnerability, allows remote attackers to execute arbitrary SQL commands

## CVE #2

**CVE:** CVE-2009-4559 **Host:** <http://www.itsecgames.com/> **Risk Level:** 3.5

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

### [Insert Screenshot Here]

Vuln ID 基	Summary ⓘ	CVSS Severity ⓘ
<b>CVE-2009-4559</b>	Cross-site scripting (XSS) vulnerability in the Submitted By module 6.x before 6.x-1.3 for Drupal allows remote authenticated users, with "administer content types" privileges, to inject arbitrary web script or HTML via an input string for "submitted by" text.  <b>Published:</b> January 04, 2010; 4:30:00 pm -0500	V3.x:(not available) V2.0: <b>3.5 LOW</b>

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

Answer here

Cross-site scripting (XSS) vulnerability, allows attackers inject arbitrary web script or HTML via an input string

CVE #3

CVE: CVE-2010-2724

Host: http://www.itsecgames.com/

Risk Level: 2.1

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

[Insert Screenshot Here]

Vuln ID	Summary	CVSS Severity
CVE-2010-2724	Cross-site scripting (XSS) vulnerability in the Hierarchical Select module 5.x before 5.x-3.2 and 6.x before 6.x-3.2 for Drupal allows remote authenticated users, with administer taxonomy permissions, to inject arbitrary web script or HTML via unspecified vectors in the hierarchical_select form.  Published: July 13, 2010; 2:30:02 pm -0400	V3.x:(not available) V2.0: 2.1 LOW

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

Answer here

Cross-site scripting (XSS) vulnerability, allows attackers inject arbitrary web script or HTML via an input string