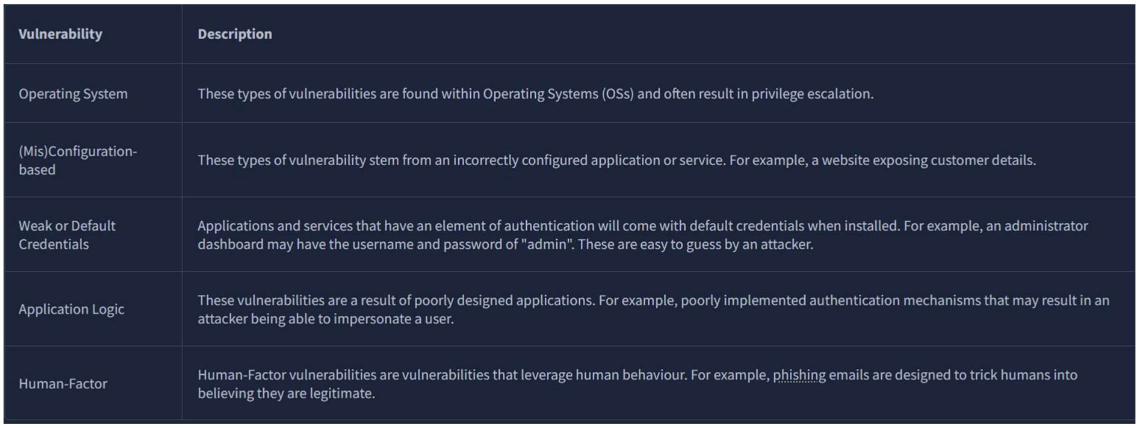
Vulnerabilities 101

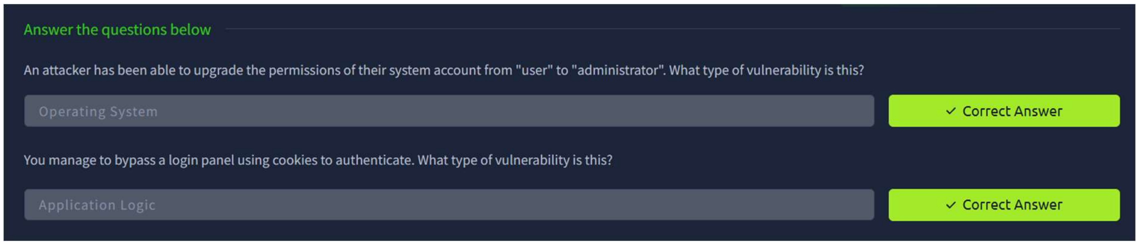
Task 2: - Introduction To Vulnerabilities

Vulnerability:- A vulnerability in cybersecurity is defined as a weakness or flaw in the design, implementation or behaviours of a system or application. An attacker can exploit these weaknesses to gain access to unauthorised information or perform unauthorised actions

Different Types Of Vulnerabilities:-



Vulnerability	Description
Operating System	These types of vulnerabilities are found within Operating Systems (OSs) and often result in privilege escalation.
(Mis)Configuration-based	These types of vulnerability stem from an incorrectly configured application or service. For example, a website exposing customer details.
Weak or Default Credentials	Applications and services that have an element of authentication will come with default credentials when installed. For example, an administrator dashboard may have the username and password of "admin". These are easy to guess by an attacker.
Application Logic	These vulnerabilities are a result of poorly designed applications. For example, poorly implemented authentication mechanisms that may result in an attacker being able to impersonate a user.
Human-Factor	Human-Factor vulnerabilities are vulnerabilities that leverage human behaviour. For example, phishing emails are designed to trick humans into believing they are legitimate.



Answer the questions below

An attacker has been able to upgrade the permissions of their system account from "user" to "administrator". What type of vulnerability is this?

Operating System

You manage to bypass a login panel using cookies to authenticate. What type of vulnerability is this?

Application Logic

Task 3:- Scoring Vulnerabilities (CVSS & VPR)

Vulnerability Management:-Vulnerability management is the process of evaluating, categorising and ultimately remediating threats (vulnerabilities) faced by an organisation.

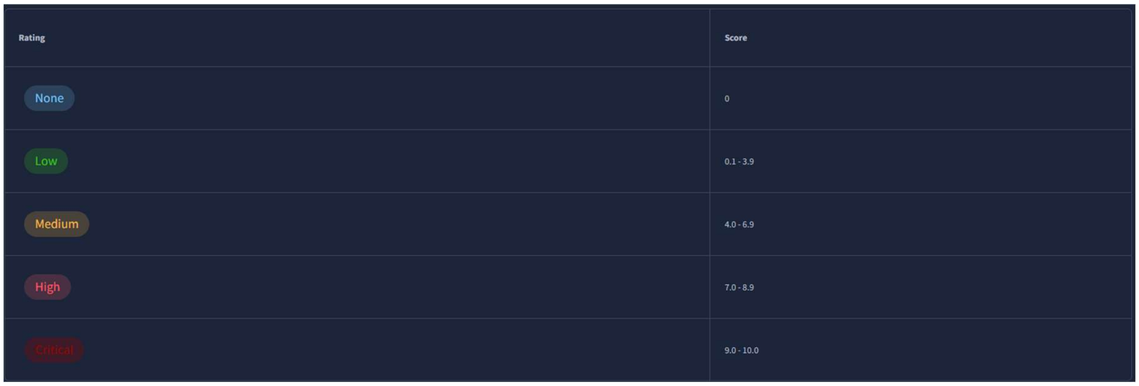
Common Vulnerabilities Scoring System

It is determined by some factor's those are

1. How easy is it to exploit the vulnerability?
2. Do exploits exist for this?

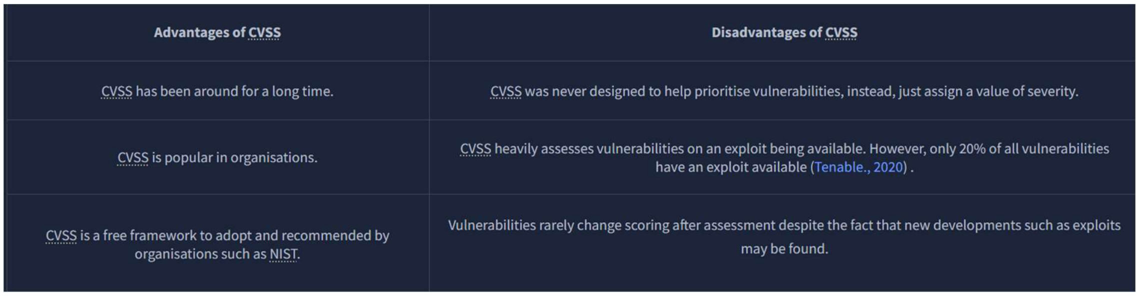
Vulnerabilities 101

3. How does this vulnerability interfere with the CIA triad?



Rating	Score
None	0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Advantages and Disadvantages of CVSS

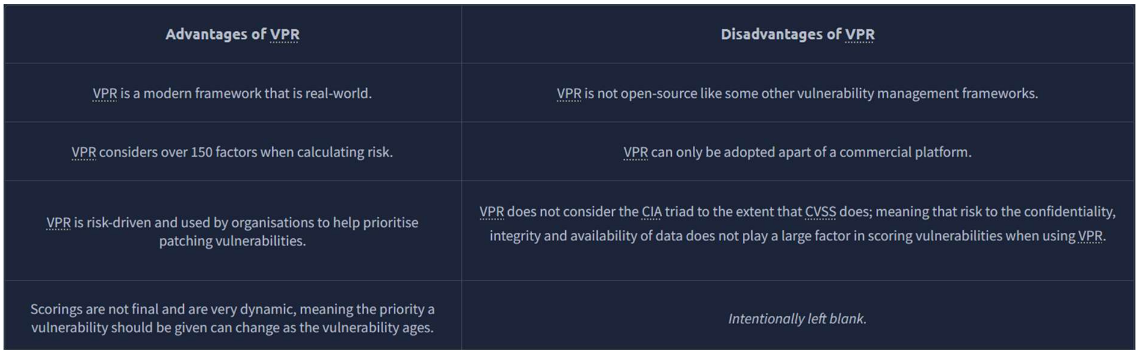


Advantages of CVSS	Disadvantages of CVSS
CVSS has been around for a long time.	CVSS was never designed to help prioritise vulnerabilities, instead, just assign a value of severity.
CVSS is popular in organisations.	CVSS heavily assesses vulnerabilities on an exploit being available. However, only 20% of all vulnerabilities have an exploit available (Tenable., 2020) .
CVSS is a free framework to adopt and recommended by organisations such as NIST.	Vulnerabilities rarely change scoring after assessment despite the fact that new developments such as exploits may be found.

Vulnerability Priority Rating (VPR)

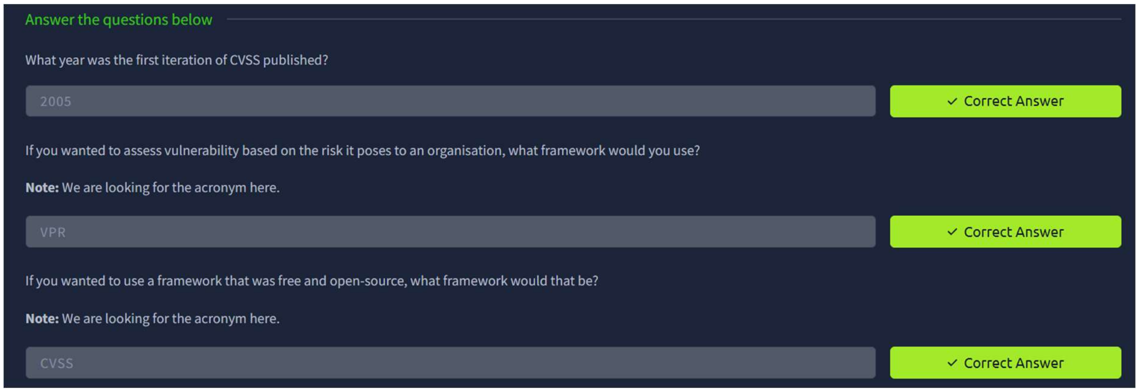
Unlike CVSS, VPR scoring takes into account the relevancy of a vulnerability. For example, no risk is considered regarding a vulnerability if that vulnerability does not apply to the organisation (i.e. they do not use the software that is vulnerable). VPR is also considerably dynamic in its scoring, where the risk that a vulnerability may pose can change almost daily as it ages.

Advantages And Disadvantages of VPR



Advantages of VPR	Disadvantages of VPR
VPR is a modern framework that is real-world.	VPR is not open-source like some other vulnerability management frameworks.
VPR considers over 150 factors when calculating risk.	VPR can only be adopted apart of a commercial platform.
VPR is risk-driven and used by organisations to help prioritise patching vulnerabilities.	VPR does not consider the CIA triad to the extent that CVSS does; meaning that risk to the confidentiality, integrity and availability of data does not play a large factor in scoring vulnerabilities when using VPR.
Scorings are not final and are very dynamic, meaning the priority a vulnerability should be given can change as the vulnerability ages.	*Intentionally left blank.*

Vulnerabilities 101



Answer the questions below

What year was the first iteration of CVSS published?

2005 ✓ Correct Answer

If you wanted to assess vulnerability based on the risk it poses to an organisation, what framework would you use?

Note: We are looking for the acronym here.

VPR ✓ Correct Answer

If you wanted to use a framework that was free and open-source, what framework would that be?

Note: We are looking for the acronym here.

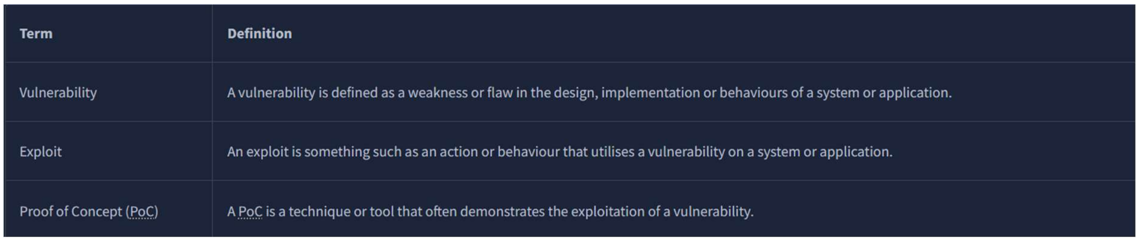
CVSS ✓ Correct Answer

Task 4:- Vulnerability Databases

There are two main vulnerability databases

1. NVD (National Vulnerability Database)

2. Exploit-DB



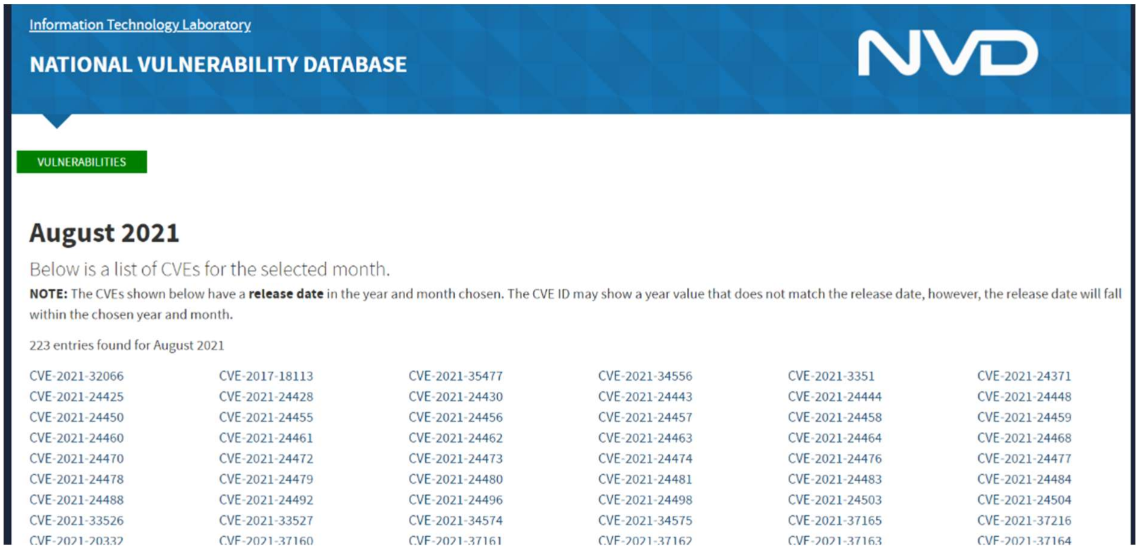
Term	Definition
Vulnerability	A vulnerability is defined as a weakness or flaw in the design, implementation or behaviours of a system or application.
Exploit	An exploit is something such as an action or behaviour that utilises a vulnerability on a system or application.
Proof of Concept (PoC)	A PoC is a technique or tool that often demonstrates the exploitation of a vulnerability.

NVD – National Vulnerability Database

The National Vulnerability Database is a website that lists all publicly categorised vulnerabilities. In cybersecurity, vulnerabilities are classified under “**C**ommon **V**ulnerabilities and **E**xposures” (Or CVE for short).

These CVEs have the formatting of CVE-YEAR-IDNUMBER. For example, the vulnerability that the famous malware WannaCry used was CVE-2017-0144.

Vulnerabilities 101



Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES

August 2021

Below is a list of CVEs for the selected month.

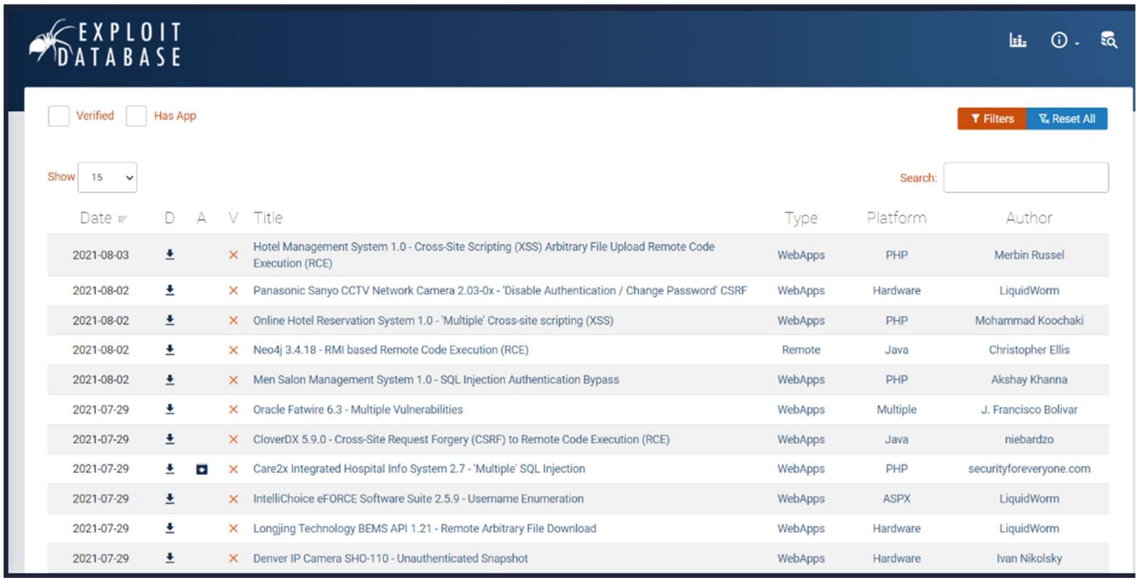
NOTE: The CVEs shown below have a **release date** in the year and month chosen. The CVE ID may show a year value that does not match the release date, however, the release date will fall within the chosen year and month.

223 entries found for August 2021

CVE-2021-32066	CVE-2017-18113	CVE-2021-35477	CVE-2021-34556	CVE-2021-3351	CVE-2021-24371
CVE-2021-24425	CVE-2021-24428	CVE-2021-24430	CVE-2021-24443	CVE-2021-24444	CVE-2021-24448
CVE-2021-24450	CVE-2021-24455	CVE-2021-24456	CVE-2021-24457	CVE-2021-24458	CVE-2021-24459
CVE-2021-24460	CVE-2021-24461	CVE-2021-24462	CVE-2021-24463	CVE-2021-24464	CVE-2021-24468
CVE-2021-24470	CVE-2021-24472	CVE-2021-24473	CVE-2021-24474	CVE-2021-24476	CVE-2021-24477
CVE-2021-24478	CVE-2021-24479	CVE-2021-24480	CVE-2021-24481	CVE-2021-24483	CVE-2021-24484
CVE-2021-24488	CVE-2021-24492	CVE-2021-24496	CVE-2021-24498	CVE-2021-24503	CVE-2021-24504
CVE-2021-33526	CVE-2021-33527	CVE-2021-34574	CVE-2021-34575	CVE-2021-37165	CVE-2021-37216
CVE-2021-20332	CVE-2021-37160	CVE-2021-37161	CVE-2021-37162	CVE-2021-37163	CVE-2021-37164

Exploit-DB

Exploit-DB is a resource that we, as hackers, will find much more helpful during an assessment. Exploit-DB retains exploits for software and applications stored under the name, author and version of the software or application.



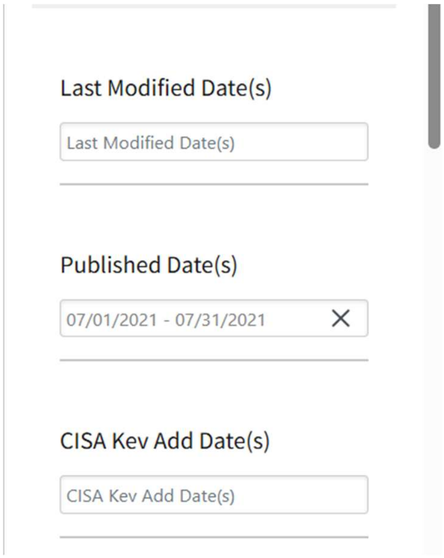
Date	D	A	V	Title	Type	Platform	Author
2021-08-03	⬇		✕	Hotel Management System 1.0 - Cross-Site Scripting (XSS) Arbitrary File Upload Remote Code Execution (RCE)	WebApps	PHP	Merbin Russel
2021-08-02	⬇		✕	Panasonic Sanyo CCTV Network Camera 2.03-0x - 'Disable Authentication / Change Password' CSRF	WebApps	Hardware	LiquidWorm
2021-08-02	⬇		✕	Online Hotel Reservation System 1.0 - 'Multiple' Cross-site scripting (XSS)	WebApps	PHP	Mohammad Koochaki
2021-08-02	⬇		✕	Neo4j 3.4.18 - RMI based Remote Code Execution (RCE)	Remote	Java	Christopher Ellis
2021-08-02	⬇		✕	Men Salon Management System 1.0 - SQL Injection Authentication Bypass	WebApps	PHP	Akshay Khanna
2021-07-29	⬇		✕	Oracle Fatwire 6.3 - Multiple Vulnerabilities	WebApps	Multiple	J. Francisco Bolivar
2021-07-29	⬇		✕	CloverDX 5.9.0 - Cross-Site Request Forgery (CSRF) to Remote Code Execution (RCE)	WebApps	Java	niebardzo
2021-07-29	⬇	▣	✕	Care2x Integrated Hospital Info System 2.7 - 'Multiple' SQL Injection	WebApps	PHP	securityforeveryone.com
2021-07-29	⬇		✕	IntelliChoice eFORCE Software Suite 2.5.9 - Username Enumeration	WebApps	ASPX	LiquidWorm
2021-07-29	⬇		✕	Longjing Technology BEMS API 1.21 - Remote Arbitrary File Download	WebApps	Hardware	LiquidWorm
2021-07-29	⬇		✕	Denver IP Camera SHO-110 - Unauthenticated Snapshot	WebApps	Hardware	Ivan Nikolsky

Answer the questions below

1)Using NVD, how many CVEs were published in July 2021?

Vulnerabilities 101

Step 1:-



Last Modified Date(s)

Last Modified Date(s)

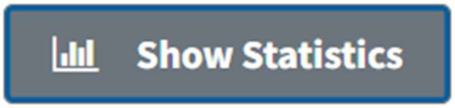
Published Date(s)

07/01/2021 - 07/31/2021 ×

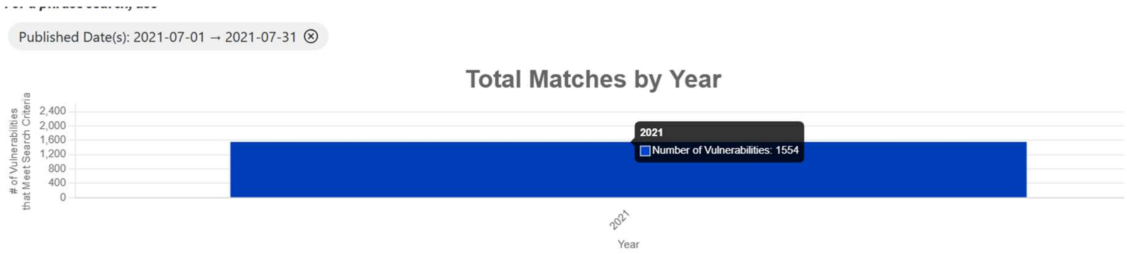
CISA Kev Add Date(s)

CISA Kev Add Date(s)

Step 2:-



Step 3:-



Published Date(s): 2021-07-01 → 2021-07-31 ⊗

Total Matches by Year
# of Vulnerabilities that Meet Search Criteria
2,400
2,000
1,600
1,200
800
400
0
2021
Number of Vulnerabilities: 1554
2021
Year

Ans:- 1554

2)Who is the author of Exploit-DB?

Ans:- OffSec

Showing 0 to 0 of 0 entries

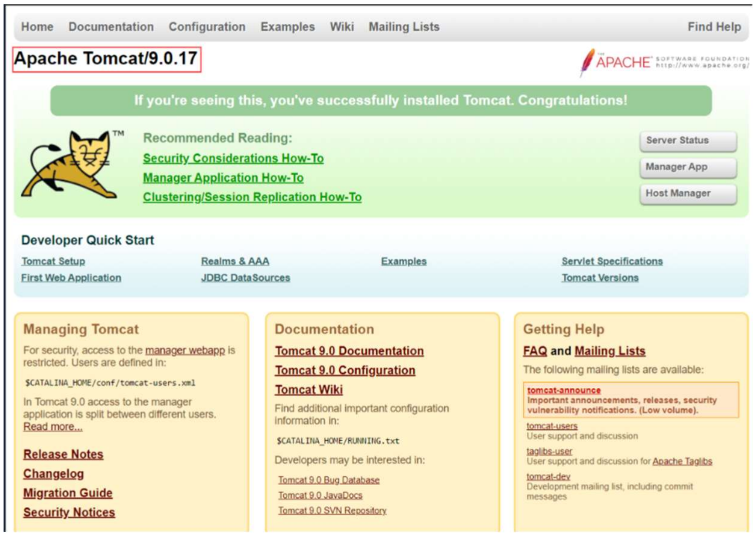
Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	SearchSploit Manual	VulnHub	OffSec Cyber Range
Shellcodes	Exploit Statistics		Proving Grounds
			Penetration Testing Services

Task 5:- An Example Of Finding Vulnerability

Throughout an assessment, you will often combine multiple vulnerabilities to get results. For example, in this task, we will leverage the "**Version Disclosure"** vulnerability to find out the version of an application. With this version, we can then use Exploit-DB to search for any exploits that work with that specific version.

Applications and software usually have a version number. This information is usually left with good intentions; for example, the author can support multiple versions of the software and the likes. Or sometimes, left unintentionally.

For example, in the screenshot below, we can see that the name and version number of this application is "**Apache Tomcat 9.0.17**"



Apache Tomcat/9.0.17

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations How-To
Manager Application How-To
Clustering/Session Replication How-To

Developer Quick Start

Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users. Read more...

Release Notes
Changelog
Migration Guide
Security Notices

Documentation

Tomcat 9.0 Documentation
Tomcat 9.0 Configuration
Tomcat Wiki

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

Tomcat 9.0 Bug Database
Tomcat 9.0 JavaDocs
Tomcat 9.0 SVN Repository

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

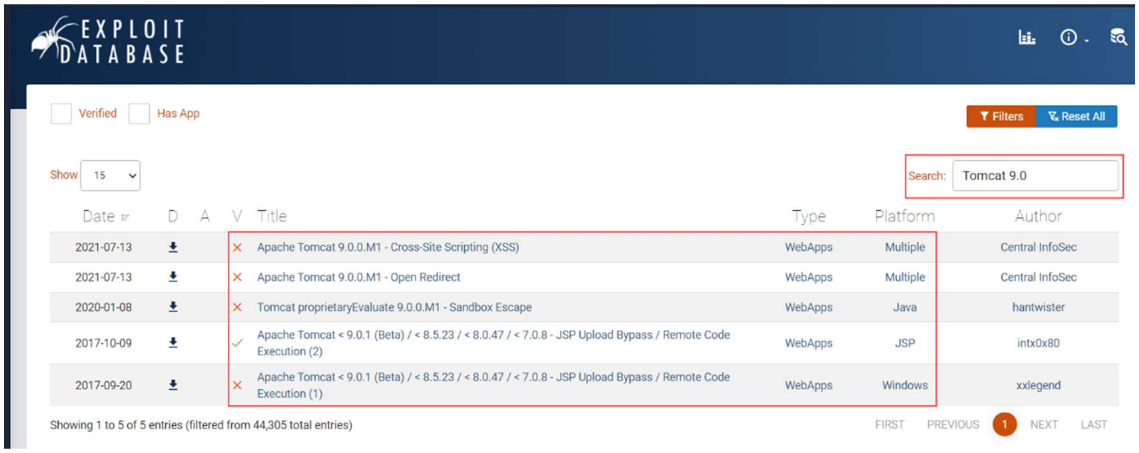
tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

With this information in hand, let's use the search filter on Exploit-DB to look for any exploits that may apply to "**Apache Tomcat 9.0.17**".

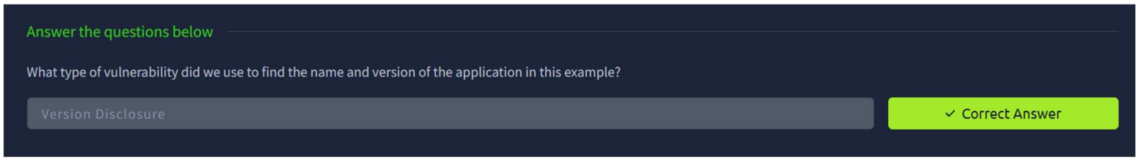
Vulnerabilities 101



Search: Tomcat 9.0

Date	D	A	V	Title	Type	Platform	Author
2021-07-13	⬇		✗	Apache Tomcat 9.0.0.M1 - Cross-Site Scripting (XSS)	WebApps	Multiple	Central InfoSec
2021-07-13	⬇		✗	Apache Tomcat 9.0.0.M1 - Open Redirect	WebApps	Multiple	Central InfoSec
2020-01-08	⬇		✗	Tomcat proprietaryEvaluate 9.0.0.M1 - Sandbox Escape	WebApps	Java	hantwister
2017-10-09	⬇		✓	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	WebApps	JSP	intx0x80
2017-09-20	⬇		✗	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	WebApps	Windows	xxlegend

Showing 1 to 5 of 5 entries (filtered from 44,305 total entries)



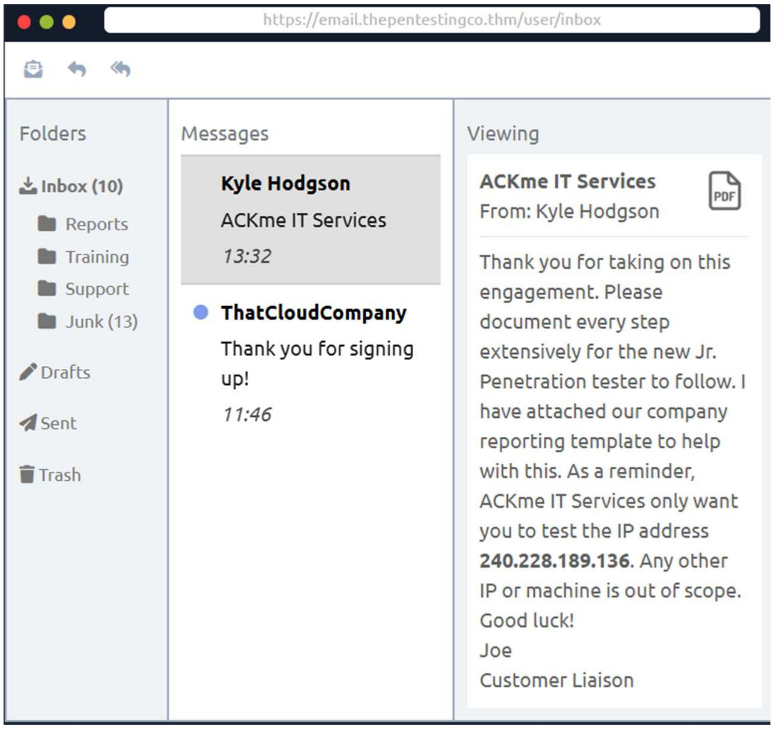
Answer the questions below

What type of vulnerability did we use to find the name and version of the application in this example?

Version Disclosure

Task 6:- Showcase: Exploiting Ackme's Application

Step 1:-



https://email.thepentestingco.thm/user/inbox

Kyle Hodgson
ACKme IT Services
13:32

ThatCloudCompany
Thank you for signing up!
11:46

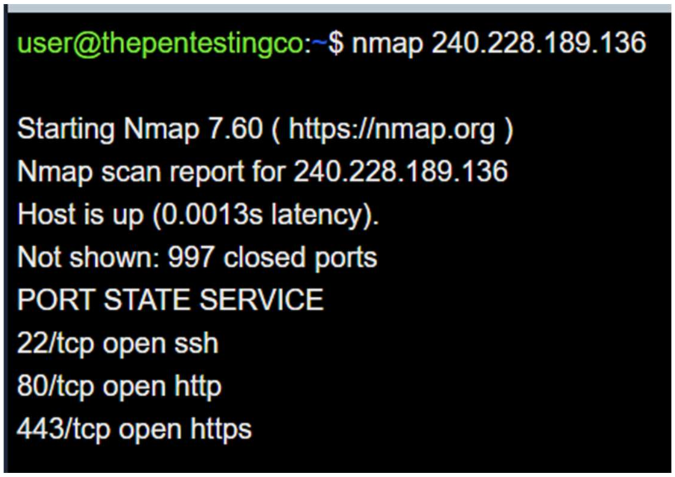
ACKme IT Services
From: Kyle Hodgson

Thank you for taking on this engagement. Please document every step extensively for the new Jr. Penetration tester to follow. I have attached our company reporting template to help with this. As a reminder, ACKme IT Services only want you to test the IP address **240.228.189.136**. Any other IP or machine is out of scope. Good luck!

Joe
Customer Liaison

Vulnerabilities 101

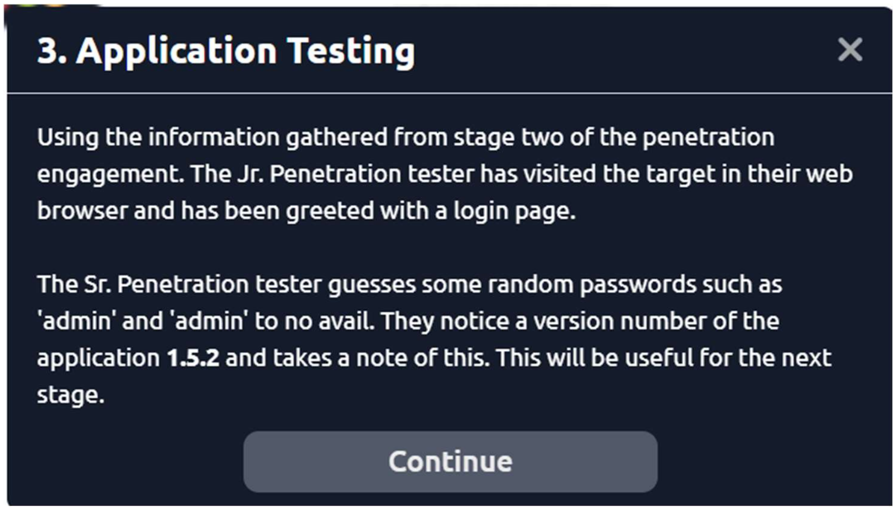
Step 2:-



```
user@thepentestingco:~$ nmap 240.228.189.136

Starting Nmap 7.60 ( https://nmap.org )
Nmap scan report for 240.228.189.136
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
```

Step 3:-

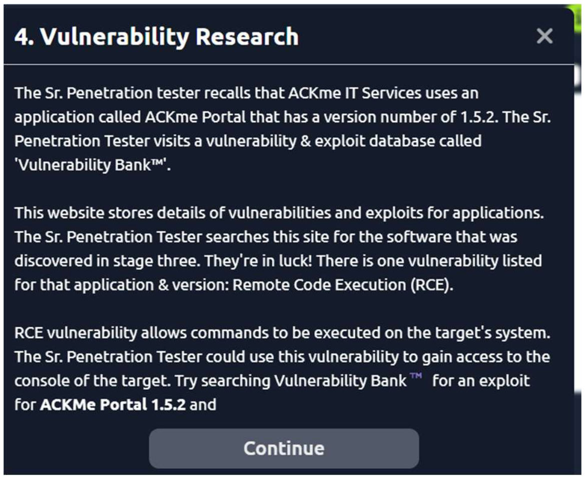


3. Application Testing

Using the information gathered from stage two of the penetration engagement. The Jr. Penetration tester has visited the target in their web browser and has been greeted with a login page.

The Sr. Penetration tester guesses some random passwords such as 'admin' and 'admin' to no avail. They notice a version number of the application **1.5.2** and takes a note of this. This will be useful for the next stage.

Step 4:-



4. Vulnerability Research

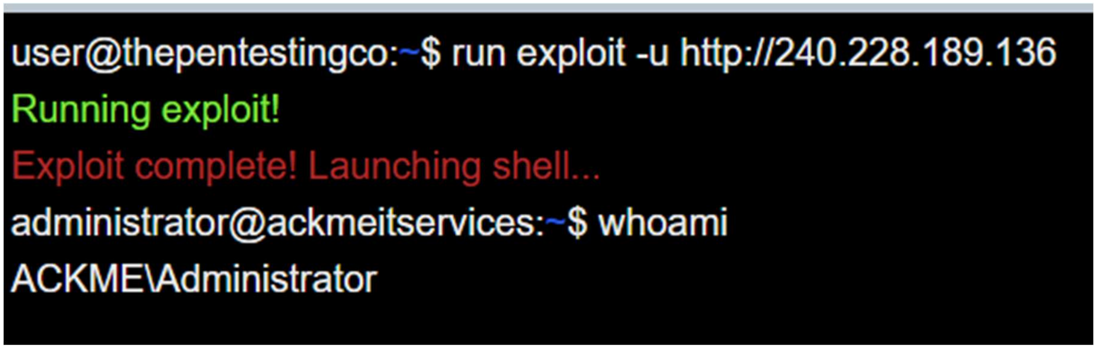
The Sr. Penetration tester recalls that ACKme IT Services uses an application called ACKme Portal that has a version number of 1.5.2. The Sr. Penetration Tester visits a vulnerability & exploit database called 'Vulnerability Bank™'.

This website stores details of vulnerabilities and exploits for applications. The Sr. Penetration Tester searches this site for the software that was discovered in stage three. They're in luck! There is one vulnerability listed for that application & version: Remote Code Execution (RCE).

RCE vulnerability allows commands to be executed on the target's system. The Sr. Penetration Tester could use this vulnerability to gain access to the console of the target. Try searching Vulnerability Bank™ for an exploit for **ACKMe Portal 1.5.2** and

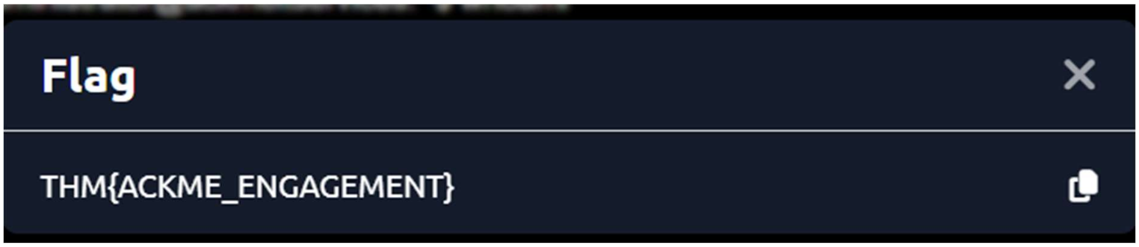
Vulnerabilities 101

Step 5:-



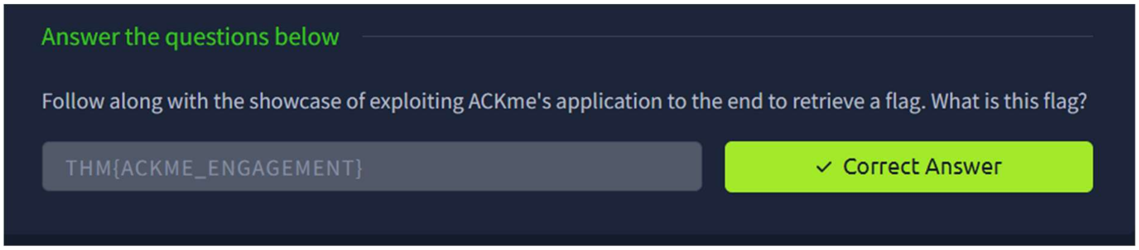
```
user@thepentestingco:~$ run exploit -u http://240.228.189.136
Running exploit!
Exploit complete! Launching shell...
administrator@ackmeitservices:~$ whoami
ACKME\Administrator
```

Step 6:-



Flag

THM{ACKME_ENGAGEMENT}



Answer the questions below

Follow along with the showcase of exploiting ACKme's application to the end to retrieve a flag. What is this flag?

THM{ACKME_ENGAGEMENT}