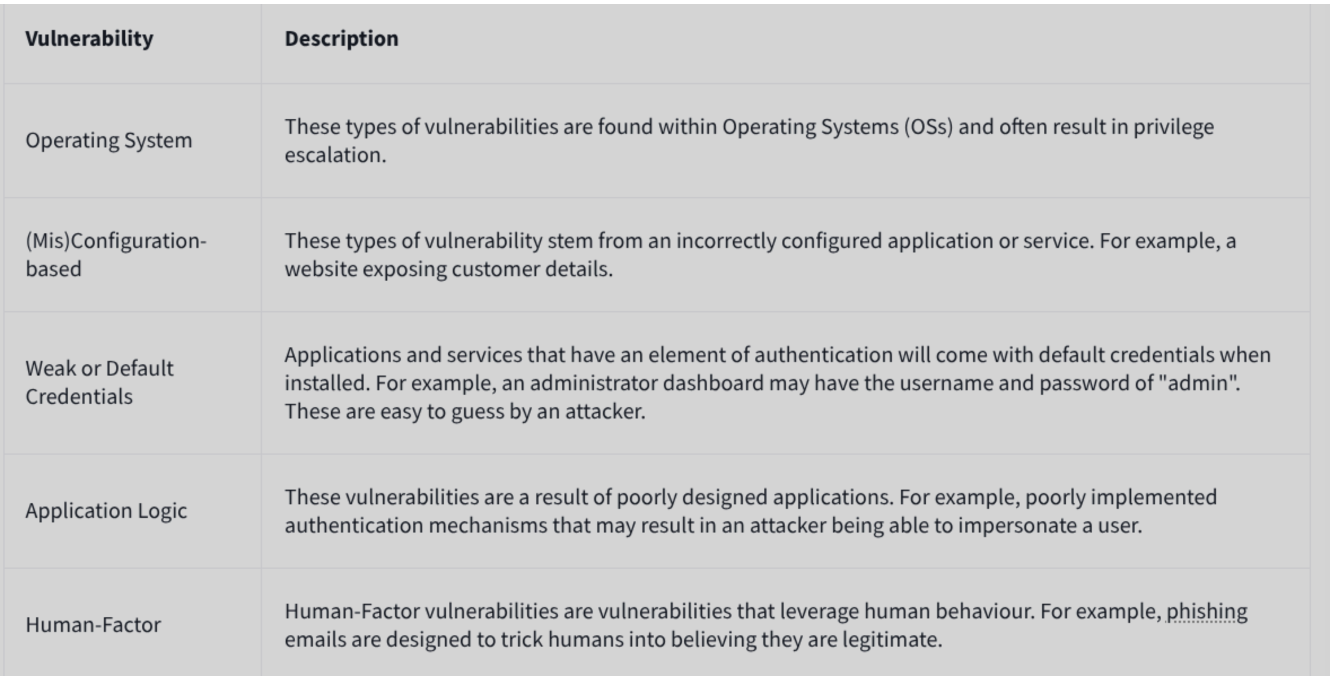
Vulnerabilities 101

Task 2: Introduction to Vulnerabilities

A vulnerability in cybersecurity is defined as a weakness or flaw in the design, implementation or behaviours of a system or application.

Vulnerabilities include Vulnerabilities on Operating System, (Mis)Configuration-based, Weak or Default Credentials, Application Logic, Human-Factor



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.

Questions:

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

Answer: Operating Systems

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

Answer: Application Logic

Task 3: Scoring Vulnerabilities (CVSS & VPR)

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

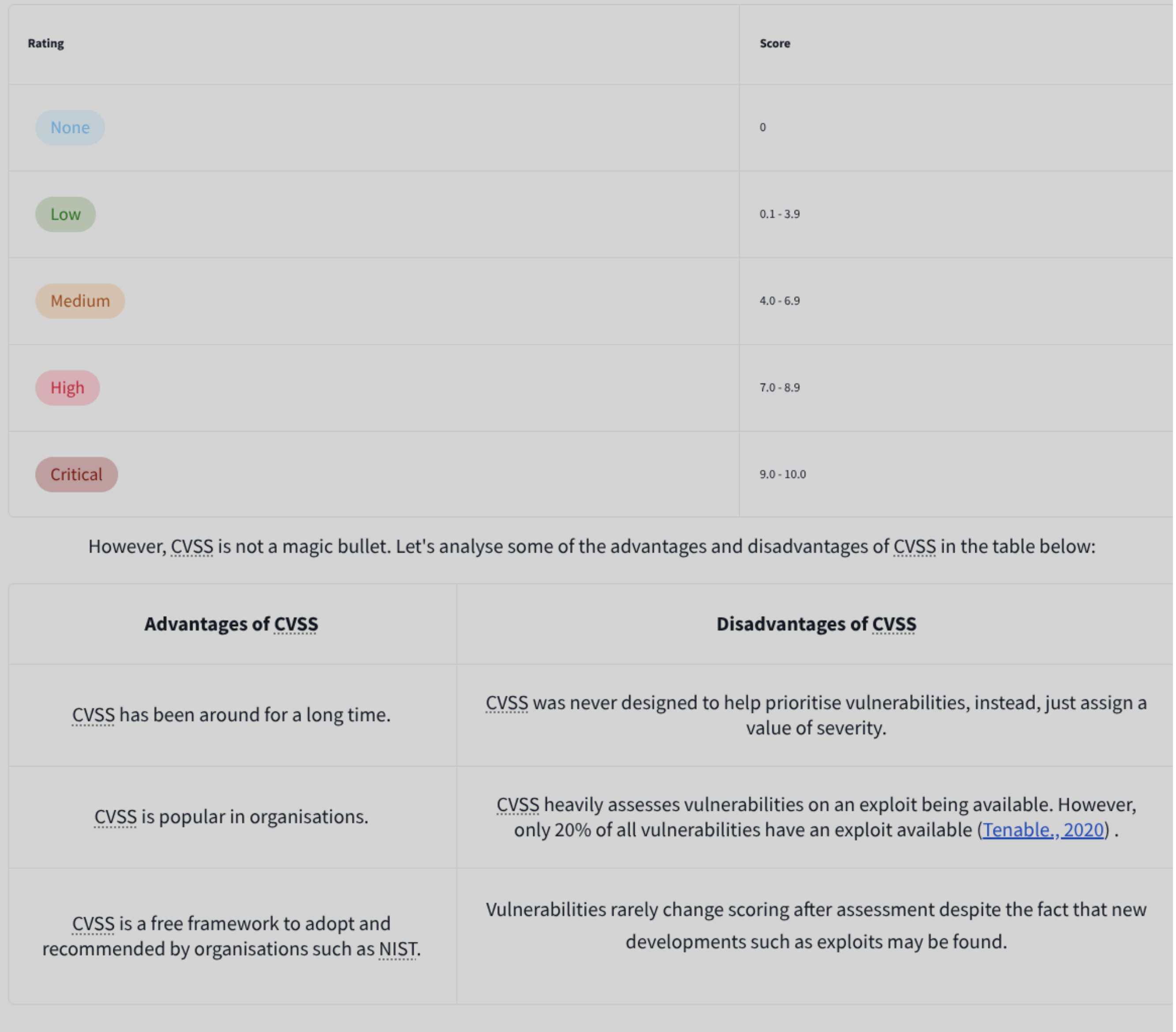
CVSS and VPR:

First introduced in 2005, the Common Vulnerability Scoring System (or CVSS) is a very popular framework for vulnerability scoring and has three major iterations. As it stands, the current version is CVSSv3.1 (with version 4.0 currently in draft) a score is essentially determined by some of the following factors (but many more):

1. How easy is it to exploit the vulnerability?

2. Do exploits exist for this?

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

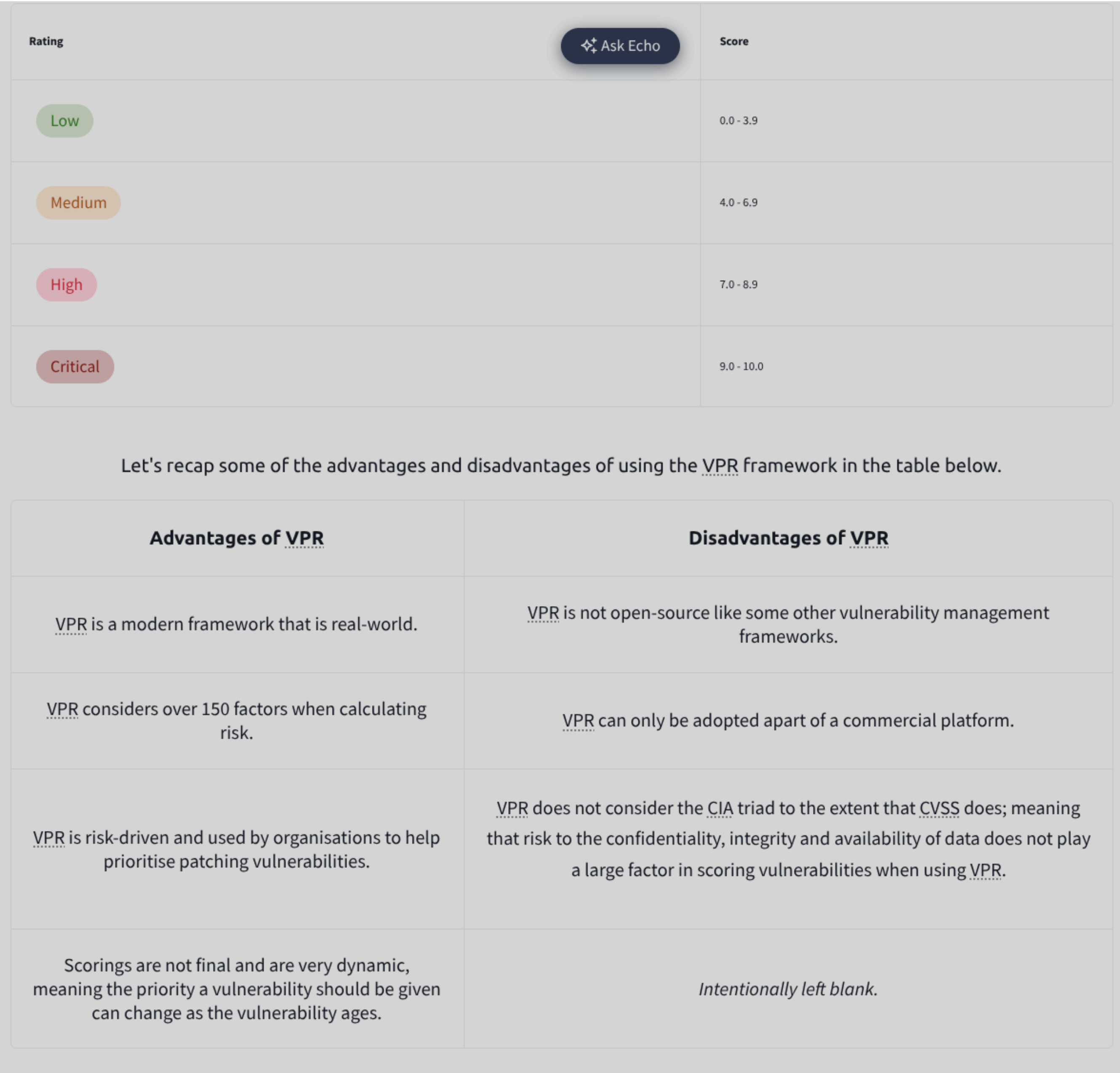
However, CVSS is not a magic bullet. Let's analyse some of the advantages and disadvantages of CVSS in the table below:

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.

The VPR framework is a much more modern framework in vulnerability management - developed by Tenable, an industry solutions provider for vulnerability management. This framework is considered to be risk-driven; meaning that vulnerabilities are given a score with a heavy focus on the risk a vulnerability poses to the organisation itself, rather than factors such as impact (like with CVSS).

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.

VPR uses a similar scoring range as CVSS, which I have also put into the table below. However, two notable differences are that VPR does not have a *"None/Informational"* category, and because VPR uses a different scoring method, the same vulnerability will have a different score using VPR than when using CVSS.



Rating	Score
Low	0.0 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Let's recap some of the advantages and disadvantages of using the VPR framework in the table below.

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.*

Questions:

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

Answer: 2005

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

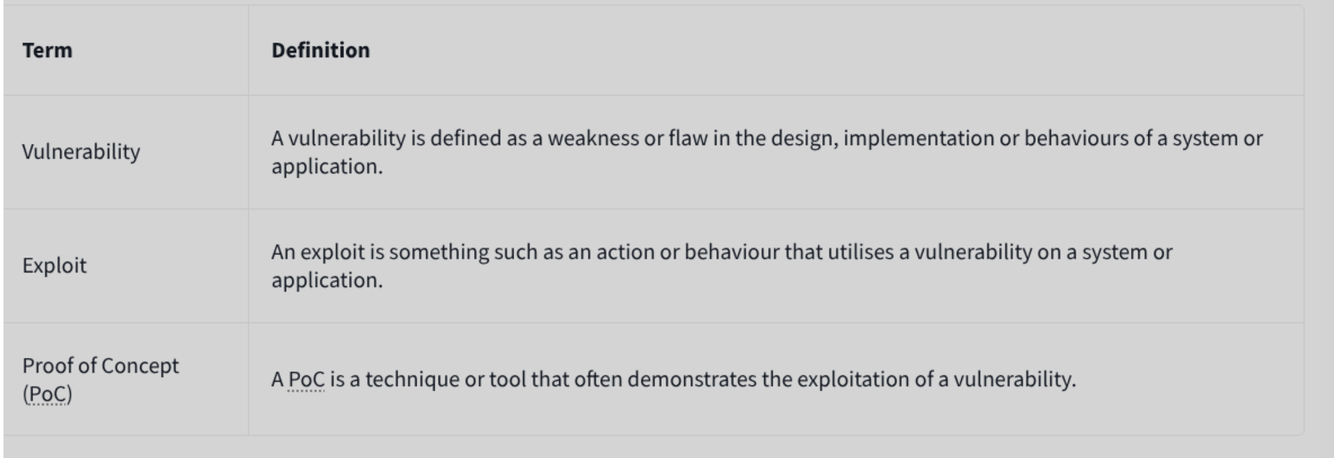
Answer: VPR

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

Answer: CVSS

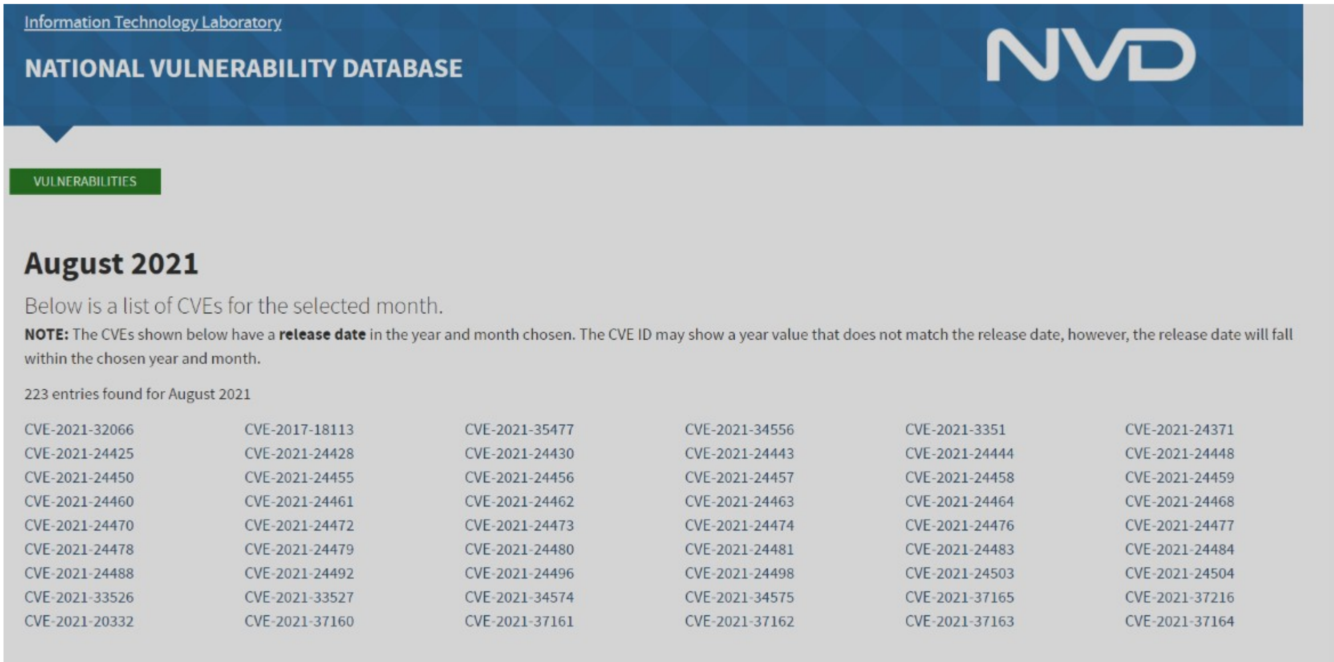
Task 4: Vulnerability Databases

```
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:



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

August 2021

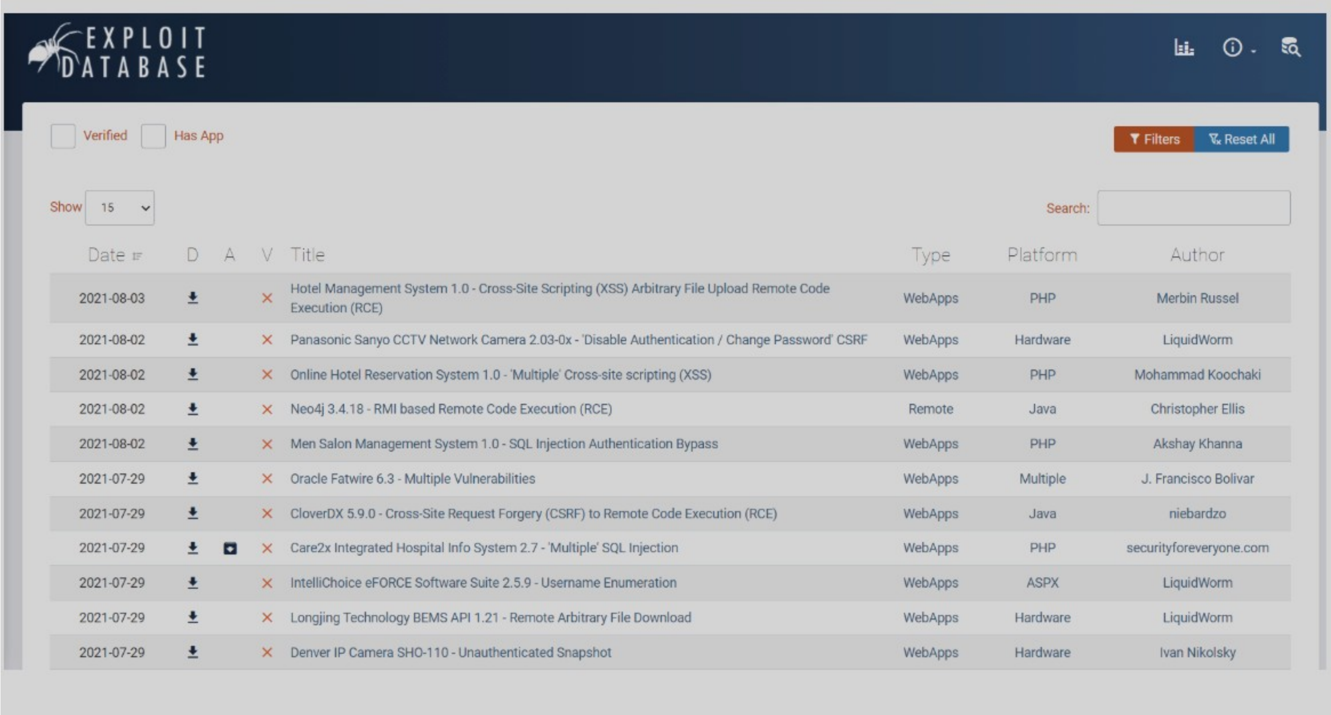
Below is a list of CVEs for the selected month.

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:

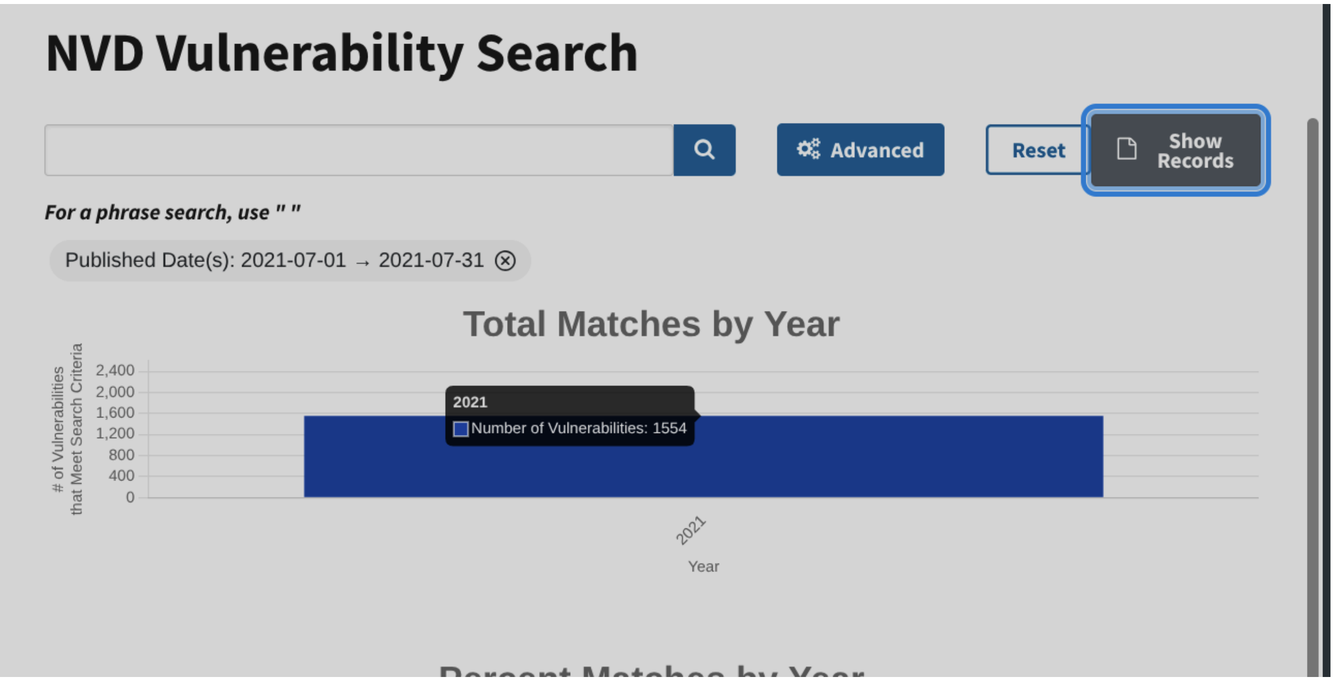


Date	D	A	V	Title	Type	Platform	Author
2021-08-03	⬇		✗	Hotel Management System 1.0 - Cross-Site Scripting (XSS) Arbitrary File Upload Remote Code Execution (RCE)	WebApps	PHP	Merbin Russel
2021-08-02	⬇		✗	Panasonic Sanyo CCTV Network Camera 2.03-0x - 'Disable Authentication / Change Password' CSRF	WebApps	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

Questions:

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

Answer: 1554



NVD Vulnerability Search

For a phrase search, use " "

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

Who is the author of Exploit-DB?

Answer: Offsec

Task 5: An Example of Finding a Vulnerability

In this Task, we used Version Disclosure to know the Vulnerabilities of Apache Tomcat/9.0.17

Questions:

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

Answer: Version Disclosure

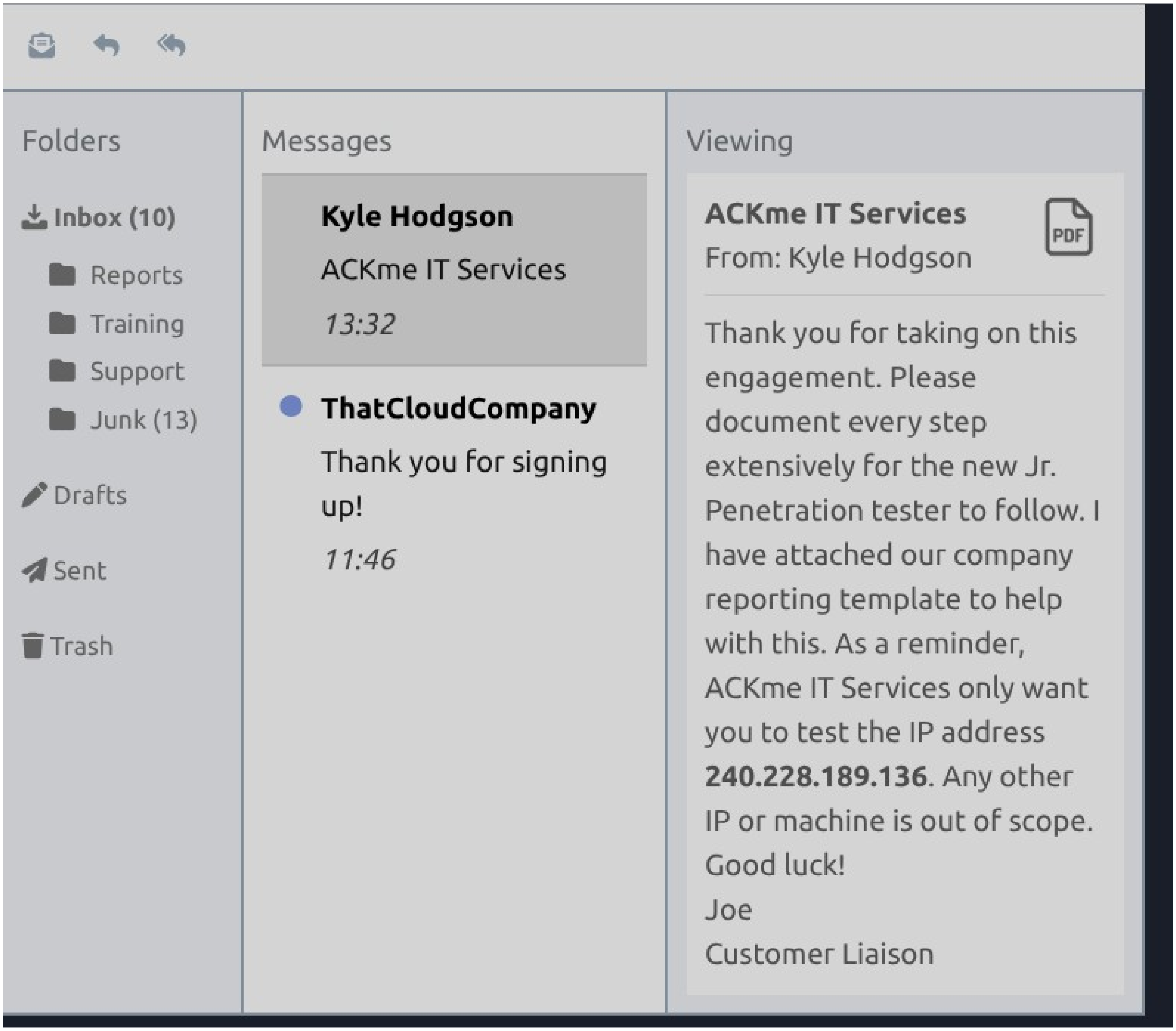
Task 6: Showcase:Exploiting Ackme's Application

Given Scenario:

It is your first week at ThePentestingCo as a Jr. Penetration tester. To ease into the role, you are shadowing a Sr. Penetration tester on your first engagement.

The Sr. Penetration tester has managed to find a vulnerability in a web application that the client (ACKme IT Services) uses.

Follow the steps that the Sr. Penetration tester took to ultimately exploit ACKme IT Service's infrastructure.



Kyle Hodgson
ACKme IT Services
13:32

ThatCloudCompany
Thank you for signing up!
11:46

ACKme IT Services
From: Kyle Hodgson

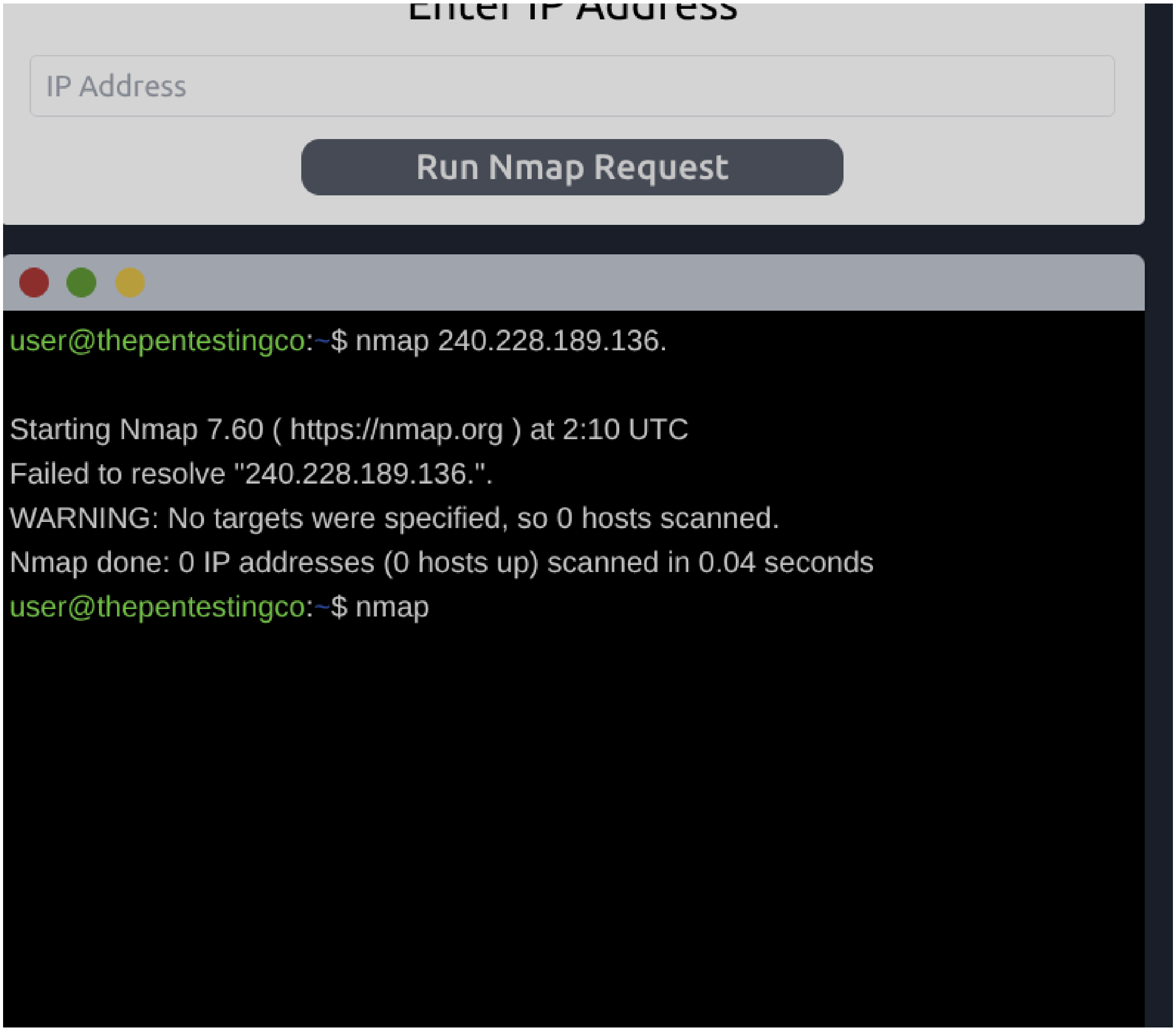
Thank you for taking on this engagement. Please document every step extensively for the new Jr. Penetration tester to follow. I have attached our company reporting template to help with this. As a reminder, ACKme IT Services only want you to test the IP address **240.228.189.136**. Any other IP or machine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

We also gather the info that this company has 800+ clients
This information is useful because we can begin to think of possible software that they are using for us to attack. For example, helpdesk or a support application.

Also we recall that in the e-mail its given that the IP address to be used is

240.228.189.136.

We can now run nmap on this ip address to know the open ports



```
user@thepentestingco:~$ nmap 240.228.189.136.

Starting Nmap 7.60 ( https://nmap.org ) at 2:10 UTC
Failed to resolve "240.228.189.136.".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
user@thepentestingco:~$ nmap
```

The version no. that we have noticed 1.5.2 can be used to exploit the portal by searching for vulnerabilities on this particular version and we can see that its a REMOTE CODE EXECUTION (RCE) vulnerability.

And now by using the vulnerability on that particular version and exploiting it on the open port will give us the command interface.