# **Cybersecurity - Capstone Project**

### Guidelines

* **You need to write down the approach/steps you followed while solving the problems of the capstone project and attach a screenshot of each step**
* **There will be marks for each step**
* **Each problem can be solved using different approaches; you don’t need to worry about the correct or most optimal solution**
* **Each problem have 3 questions/sections:**
  + **Question 1: You need to identify the type or category of challenge. Example. SQL Injection, Cryptography, SSRF etc.**
  + **Question 2: Steps you perform - Here you need to write down the steps you are following along with the screenshot of that step [If extra row(s) is/are required for your solution, feel free to add more rows ]**
  + **Question 3: One subjective question related to each problem, which you need to answer**
* **Download this file and add your solution in the solution template given in next few pages of this document**

**SCOREBOARD:**



### Problems 1: Read the user

Can you find the number of users registered on the portal mentioned below?

URL: [http://10.0.1.5:50111](http://10.0.1.5:50111/)

In this challenge, you don't have to submit the flag; you just need to submit the count. Also, you have only three attempts to submit the answer/complete the challenge.

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** | SQL Injection |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Question 3** | **Write a SQL query to count the total number of learners from a table named ‘upGrad’.** |
| **Answer** | **SELECT \* FROM upGrad WHERE username = " or ""="** |

### Problems 2: WebFun

Can you log in as admin and get the flag?

Portal: [http://10.0.1.5:13370](http://10.0.1.5:13370/)

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **Persistent cookies stay on the client’s machine forever. Write whether the above statement is true or false.** |
| **Answer** | The duration of a cookie can be set when the cookie is created. By default, the cookie is destroyed when the current browser window is closed, but it can be made to persist for a length of time after the page is closed. Persistent cookies survive after your browser or app is closed and can be used by websites or apps to recognize your computer when you re-open your browser or app later. |

### Problems 3: InviteMe

Can you Invite yourself to this portal? (Because only Invited members will be able to read the flag) URL: [http://10.0.1.5:13372](http://10.0.1.5:13372/)

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **Write the numeric value of broadcast domains if your network has four VLANs.** |
| **Answer** |  |

### Problems 4: Explore Chapters

We have created a chapter explorer for you. You can get a list of all the chapters here: [http://10.0.1.25:13373](http://10.0.1.25:13373/)

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Question 3** | **If we access the local server stored file using a given link, will it be an example of LFI or RFI?** |
| **Answer** | If we access the local server stored file using a given link then it will be an LFI attack |

Unlock Hint for 50 points

### Problems 5: Calendar

We have created a calendar app for you to track your entire progress on the cybersecurity course.

URL: [http://10.0.1.25:13375](http://10.0.1.25:13375/)

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **Explain the steps which hacker takes to carry out RFI attack?** |
| **Answer** |  |

### Problems 6: Query Resolution Portal - 1

upGrad has launched its query resolution portal. You can enter your queries, if any, here: [http://10.0.1.25:45501](http://10.0.1.25:45501/).

We have a dedicated admin who will continuously check all the queries and resolve them.

Flag format: upGrad{}.

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Question 3** | **What are the different types of XSS(Cross Site Scripting)? Explain the key differences.** |
| **Answer** | Server XSS occurs when untrusted user supplied data is included in an HTTP response generated by the server. The source of this data could be from the request, or from a stored location. As such, it can have both Reflected Server XSS and Stored Server XSS. Client XSS occurs when untrusted user supplied data is used to update the DOM with an unsafe JavaScript call. As such, it can have both Reflected Client XSS and Stored Client XSS.  Reflected XSS occurs when user input is immediately returned by a web application in an error message, search result, or any other response that includes some or all of the input provided by the user as part of the request, without that data being made safe to render in the browser, and without permanently storing the user provided data.  Stored XSS generally occurs when user input is stored on the target server, such as in a database, in a message forum, visitor log, comment field, etc. And then a victim is able to retrieve the stored data from the web application without that data being made safe to render in the browser.  DOM Based XSS is a form of XSS where the entire tainted data flow from source to sink takes place in the browser, i.e., the source of the data is in the DOM, the sink is also in the DOM, and the data flow never leaves the browser. |

### Problems 7: Query Resolution Portal - 2

We have fixed the issues with the existing query portal. All the functionalities are now working as expected on the new portal. Please use this portal to raise queries: [http://10.0.1.25:45502](http://10.0.1.25:45502/).

The admin will continuously check the portal and resolve queries.

Flag format: upGrad{}

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Question 3** | **Consider all types of XSS you mentioned in the above problem. What steps can you take to prevent these XSS attacks? Explain in detail.** |
| **Answer** | Reflected XSS: Use web application firewall with signature-based security rules. Not to click on any suspicious links.  DOM based XSS: sanitize all untrusted data, even if it is only used in client-side scripts.  Stored XSS: sanitize user data and handle inputs safely. |

### Problems 8: Internet Connectivity

Is the upGrad internet connectivity portal, [http://10.0.1.25:13376](http://10.0.1.25:13376/), vulnerable? Can you identify the vulnerability? Also, check whether you can exploit this vulnerability to see the ports at which other services are running and try to find out all such ports.

Say, you find that there are two services running in the localhost, at the ports 1212 and 1313. The flag for this challenge would then be upGrad{12121313}. Which is a concatenation of both the ports in sorted order and putting it under upGrad{}.

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **Write two measures to prevent SSRF attack.** |
| **Answer** | Whitelists and DNS resolution, Disable unused URL schemas |

### Problems 9: Upload Your Resume

We have created a dedicated application for you to upload your resume: <http://10.0.1.25:13377/>

Flag format: upGrad{}

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **Which two port numbers does FTP use by default?** |
| **Answer** | By default, the FTP protocol uses TCP ports 20 and 21. Port 20 is for transmitting data, and port 21 for transmitting commands. |

### Problems 10: Check What We Offer

Go here to check the courses we offer: [http://10.0.1.25:13378](http://10.0.1.25:13378/)

Flag format: upGrad{}

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **Explain XXE vulnerability. What steps can you take to prevent XXE attacks?** |
| **Answer** | This attack occurs when untrusted XML input containing a reference to an external entity is processed by a weakly configured XML parser.  Steps to prevent XXE: Manually disable DTDs, Harden configuration against XXE |

### Problems 11: Find Your Friends

We know friends are important, and that’s why we have created a portal for you to check whether you can find the friend with the longest name?

URL: [http://10.0.1.5:50113](http://10.0.1.5:50113/)

For this challenge, you need to find the person with the longest name and submit that as the answer: . For example, if the longest name is ‘Rohit’, then your answer for this challenge will be Rohit5.

Starting point hints:

1. Your friend’s name starts **with** `S`

2. The solution **is** **case** insensitive

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** | SQL Injection |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** | sqlmap -u "http://10.0.1.5:50113/index.php" --data 'username=' -a  heuristic (basic) test shows that POST parameter 'username' might be injectable |
| **Step: 2** |  |
| **Step: 3** | Found the table within the schema:  sqlmap -u "http://10.0.1.5:50113/index.php" --data 'username=' -D upgrad\_users\_sqli3 –tables |
| **Step: 4** | sqlmap -u "http://10.0.1.5:50113/index.php" --data 'username=' -D upgrad\_users\_sqli3 --tables users --dump |
| **Step: 5** |  |
| **Question 3** | **What steps would you take to protect your web application from SQL attacks?** |
| **Answer** | Input should be validated as it makes sure it is the accepted type, length, format, and so on. Only the value which passes the validation can be processed.  Queries should be parameterized as it makes it possible for the database to recognize the code and distinguish it from input data.  Data should be sanitised by limiting special characters  OS and applications should be hardened  Virtual or physical firewalls should be in place  Appropriate privilege and strict access to database should be in place |

### Problems 12: Admin Token

Just log in as an admin user and obtain the admin token

URL: [http://10.0.1.5:50112](http://10.0.1.5:50112/)

|  |  |
| --- | --- |
| **Question** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question** | **Write some measures you will take as cybersecurity engineer to achieve database hardening.** |
| **Answer** | Developer workstations should contain firewall and anti-virus software since phishing an employee is the easiest way to get access to the company’s resources.  All the tools, applications, firewalls and web servers should be audited frequently to figure out the threat landscape and mitigate threats at the earliest.  Protected data which is not needed after sometime should be deleted after a certain period of time.  Application, DB servers should not be hosted on the same network to avoid gaining access to the database via a vulnerable application  Protected data should not be sent via insecure medium like emails |

### Problems 13: Int

**ssh to the machine 10.0.1.5 with the username alice and password w3lc0me4alice and read the flag**

**Flag format: upGrad{}**

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** | integer based stack overflow |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **Explain buffer overflow.** |
| **Answer** | A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer.  Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information |

### 

### Problems 14: Buf

ssh to the machine 10.0.1.5 with the username bob and password welc0me4bob and read the flag

Flag format: upGrad{}

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** | Buffer overflow |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Step: 6** |  |
| **Question 3** | **Write two measures to prevent buffer overflows.** |
| **Answer** | Address space randomization (ASLR) - randomly moves around the address space locations of data regions.  Data Execution Prevention (DEP) should be implemented as its helps prevent damage to your computer from viruses and other security threats. |

### Problems 15: Fmt

ssh to the machine 10.0.1.5 with the username qux and password w3lc0m34quX and read the flag

Flag format: upGrad{}

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** | Format overflow |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **Name some common attack vectors.** |
| **Answer** | **Phihshing, malware, weak credentials** |

### Problems 16: Binny - 1

Binny is new to the world of Linux and likes building trendy web apps. He has built this trendy web widget for himself: <http://10.0.1.25:13374/webapp/>

Also, Binny loves web consoles and has created this web console for himself: <http://10.0.1.25:13374/webconsole.php>

However, Binny forgets his password quite often. So, he has it somewhere inside the web app. Can you find it?

For this challenge, you don’t need to submit the flag; you just need to submit the username and password. If you find out the username as foo and the password as bar, then you have to submit foo:bar to get your score.

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** | Cryptography |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** | Downloaded passwd file from webapp/passwd |
| **Step: 2** | Extracted RSA key from webapp/key and saved it as rskey.pem |
| **Step: 3** | Used the following openssl command to extract the credentials |
| **Step: 4** | The credentials: |
| **Step: 5** | Successfully authenticated |
| **Question 3** | **Explain privilege escalation. How can it cause issues in an organisation? Explain with examples.** |
| **Answer** | It is an attack that involves gaining illicit access of elevated rights, or privileges, beyond what is intended or entitled for a user. This attack can involve an external threat actor or an insider.  Credential exploitation: password exposure, password guessing, shoulder surfing etc can cause the exploit  Misconfigurations: failure to configure authentication for a sensitive system, mistakes in firewall configuration, or open ports.  Malware: failure to configure authentication for a sensitive system, mistakes in firewall configuration, or open ports. Attacks who have already escalated privileges can deploy malware at admin or root level, and use it to gain persistent access to an entire environment. |

Unlock Hint for 30 points

### Problems 17: Binny - 2

**Binny is new to the world of Linux and likes building trendy web apps. He has built this trendy web widget for himself:** [**http://10.0.1.25:13374/webapp/**](http://10.0.1.25:13374/webapp/)

**Also, Binny loves webconsoles and has created this webconsole for himself:** [**http://10.0.1.25:13374/webconsole.php**](http://10.0.1.25:13374/webconsole.php)

**Now, you need to log in to the system and read the flag.**

**Flag format: upGrad{}**

**This is a shared environment; so, we suggest that you clean this out before moving ahead from this challenge.**

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **Explain brute force attack.** |
| **Answer** | A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly.  These attacks are done by ‘brute force’ meaning they use excessive forceful attempts to try and ‘force’ their way into your private account(s). |

### Problems 18: Breaking Bad - 1

Can you log in to the machine 10.0.1.5 with the following username-password combination: foobar:f00b4r00r00rar?

After you log in, try to find the domain name of the machine where you think flag will be residing. It should be FQDN.

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** | ARP spoofing |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **Write two measures to prevent ARP spoofing.** |
| **Answer** | **Use static ARP. Setup packet filtering** |

### Problems 19: Breaking Bad - 2

**Can you log in to the machine 10.0.1.5 with the username-password combination foobar:f00b4r00r00rar and find/crawl/dig/locate the flag?**

Unlock Hint for 20 points

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Step: 5** |  |
| **Question 3** | **State whether the following is an example of IP spoofing or ARP spoofing: Intervening into a firewall and making the target computer believe that the frames are from a trusted source.** |
| **Answer** | **Yes it is.** |

### Problems 20: EncryptDecrypt

**Not every encryption is hard.**

**Can you break the encryption used here and read the flag out? URL:** [**http://10.0.1.5:13371**](http://10.0.1.5:13371/)

**Flag format: upGrad{}**

|  |  |
| --- | --- |
| **Question 1** | **Identify the type or category of challenge** |
| **Answer** |  |
| **Question 2** | **Steps to Solve problem** |
| **Step: 1** |  |
| **Step: 2** |  |
| **Step: 3** |  |
| **Step: 4** |  |
| **Question 3** | **How is encoding different from encryption? Highlight some use cases for both encryption and encoding.** |
| **Answer** | Encoding transforms data into another format using a scheme that is publicly available so that it can easily be reversed. It does not require a key as the only thing required to decode it is the algorithm that was used to encode it. Encryption transforms data into another format in such a way that only specific individual can reverse the transformation. It uses a key, which is kept secret, in conjunction with the plaintext and the algorithm, in order to perform the encryption operation. Example for encryption: Securely sending a password over the internet. Example for encoding: viewing special characters on the web page. |