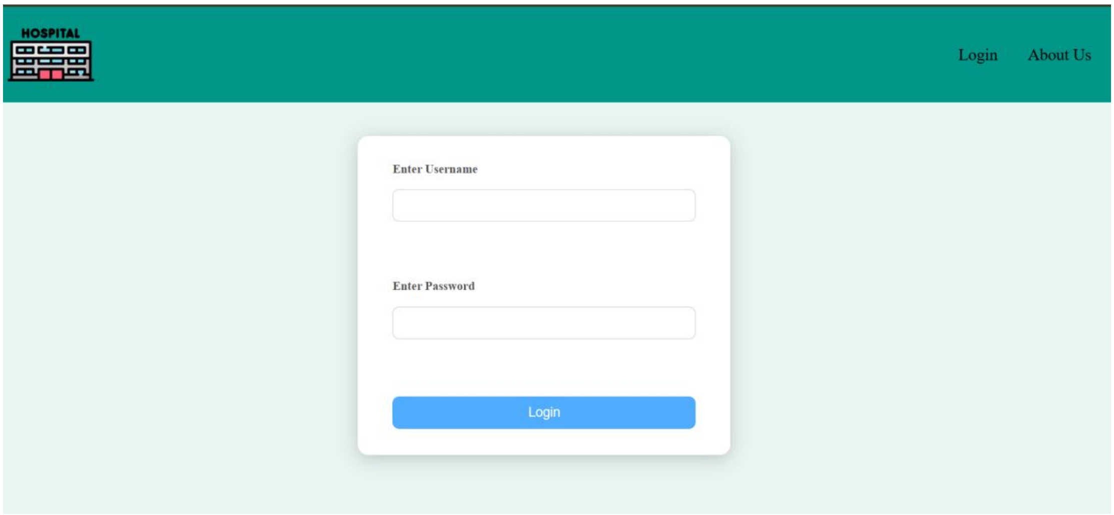
Hospital Writeup

Category : Web Security

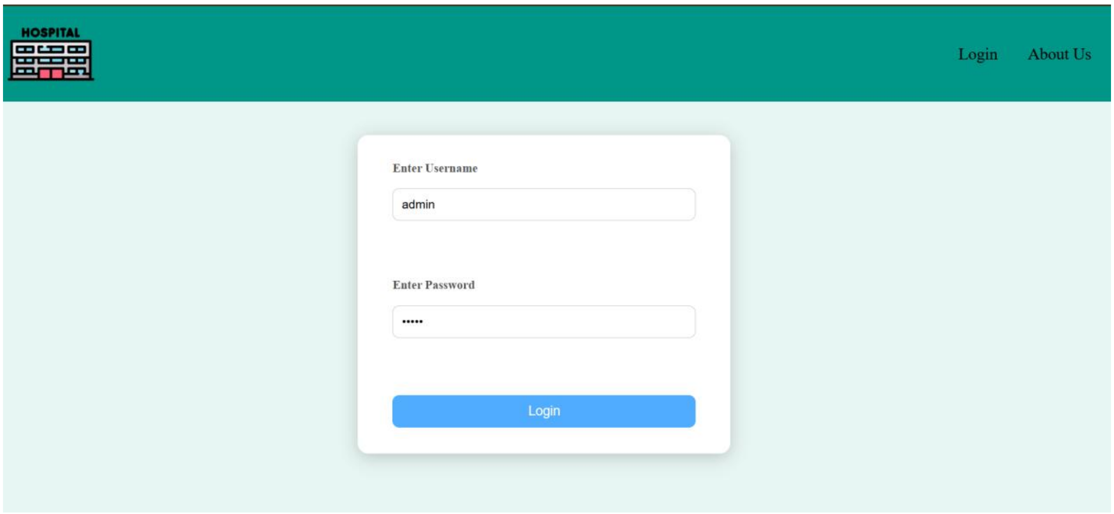
Author : Baraa Sabbah



Enter Username

Enter Password

At the beginning of the CTF it a Hospital login page , nothing else .



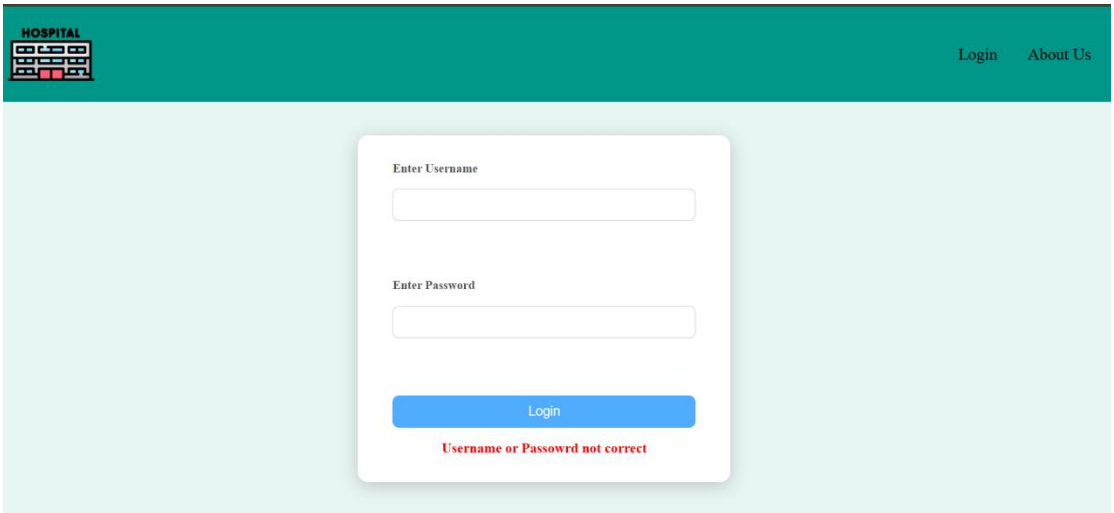
Enter Username

admin

Enter Password

•••••

At first I'll start login with random credentials , like admin , admin .



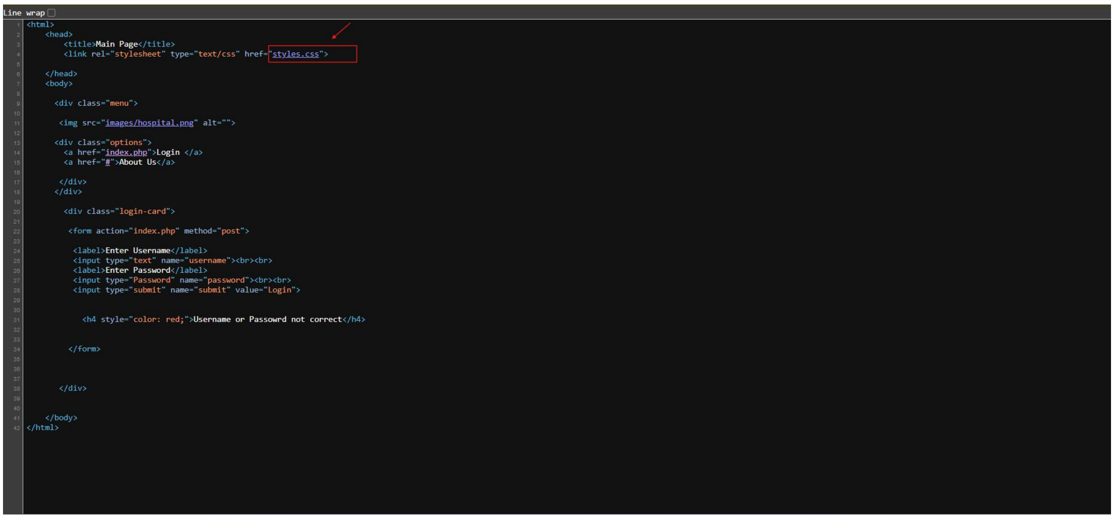
Enter Username

Enter Password

Login

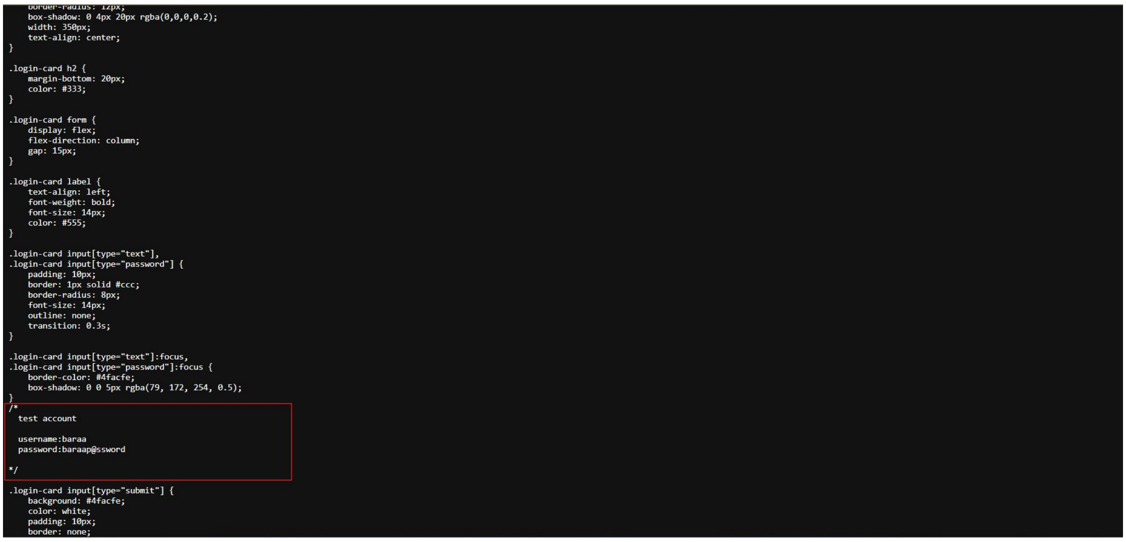
Username or Passowrd not correct

It not work , I tried also sql injection payloads like admin’ AND 1=1 -- , ‘ OR 1=1-- , but nothing work , maybe there's is a leak of credentials in source code



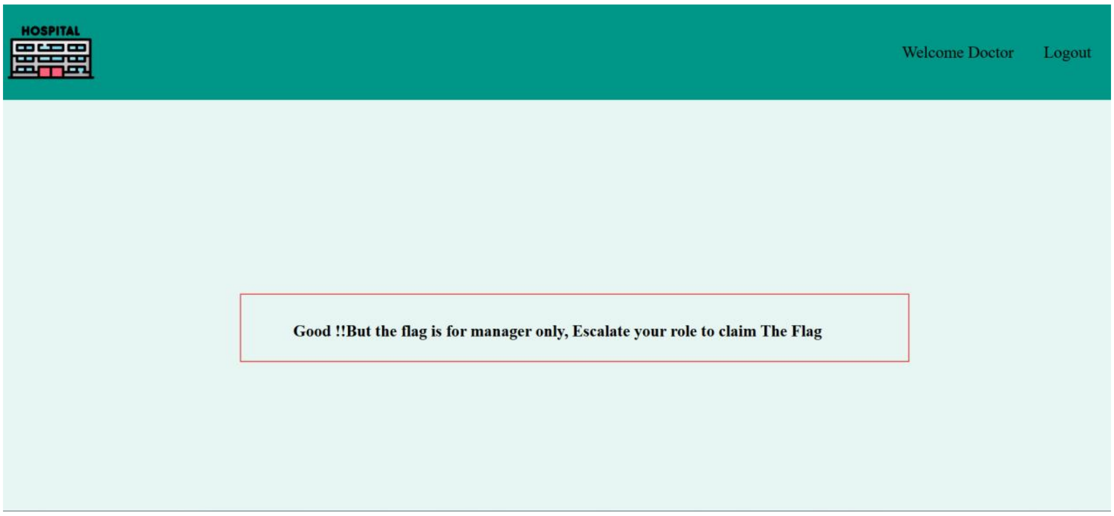
```
<html>
    <head>
        <title>Main Page</title>
        <link rel="stylesheet" type="text/css" href="styles.css">

    </head>
    <body>

      <div class="menu">

       <img src="images/hospital.png" alt="">

      <div class="options">
        <a href="index.php">Login </a>
        <a href="#">About Us</a>

       </div>
      </div>

        <div class="login-card">

         <form action="index.php" method="post">

          <label>Enter Username</label>
          <input type="text" name="username"><br><br>
          <label>Enter Password</label>
          <input type="Password" name="password"><br><br>
          <input type="submit" name="submit" value="Login">


            <h4 style="color: red;">Username or Passowrd not correct</h4>


         </form>



       </div>


    </body>
</html>
```

There was nothing in html page , I try to see if there something in css file



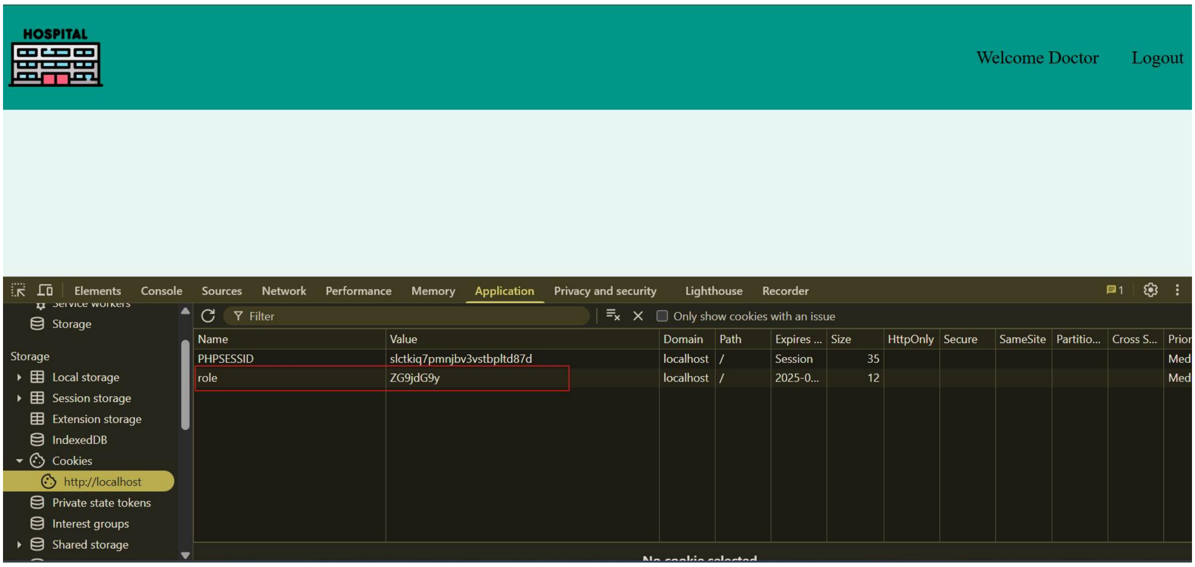
```
    border-radius: 12px;
    box-shadow: 0 4px 20px rgba(0,0,0,0.2);
    width: 350px;
    text-align: center;
}

.login-card h2 {
    margin-bottom: 20px;
    color: #333;
}

.login-card form {
    display: flex;
    flex-direction: column;
    gap: 15px;
}

.login-card label {
    text-align: left;
    font-weight: bold;
    font-size: 14px;
    color: #555;
}

.login-card input[type="text"],
.login-card input[type="password"] {
    padding: 10px;
    border: 1px solid #ccc;
    border-radius: 8px;
    font-size: 14px;
    outline: none;
    transition: 0.3s;
}

.login-card input[type="text"]:focus,
.login-card input[type="password"]:focus {
    border-color: #4facfe;
    box-shadow: 0 0 5px rgba(79, 172, 254, 0.5);
}
/*
  test account

  username:baraa
  password:baraap@ssword

*/
.login-card input[type="submit"] {
    background: #4facfe;
    color: white;
    padding: 10px;
    border: none;
```

Here I noticed there a test account so I try to login with this account



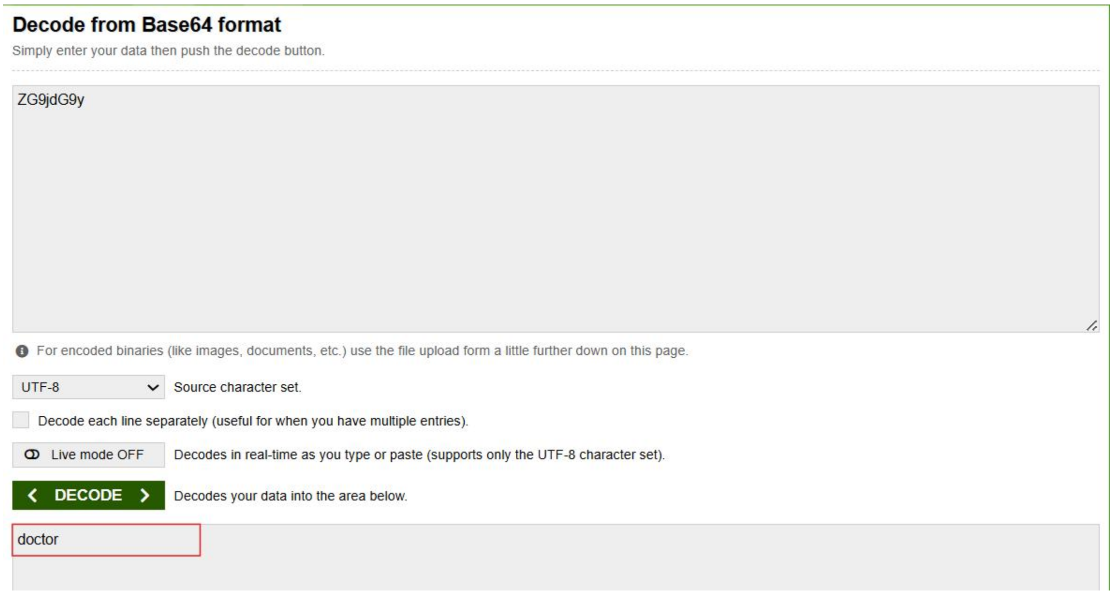
Good !!But the flag is for manager only, Escalate your role to claim The Flag

The account that I login-ed in with it was a doctor account , to get the flag you have to get access to the manager account .



Name	Value	Domain	Path	Expires ...	Size	HttpOnly	Secure	SameSite	Partitio...	Cross S...	Prior
PHPSESSID	slctkiq7pmnjbv3vstbpltd87d	localhost	/	Session	35						Med
role	ZG9jdG9y	localhost	/	2025-0...	12						Med

I opened web developer tools to see what is going on , I noticed there a cookie called role and it's value non readable , it seem a base64 value so I tried to decode the value



Decode from Base64 format

Simply enter your data then push the decode button.

ZG9jdG9y

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

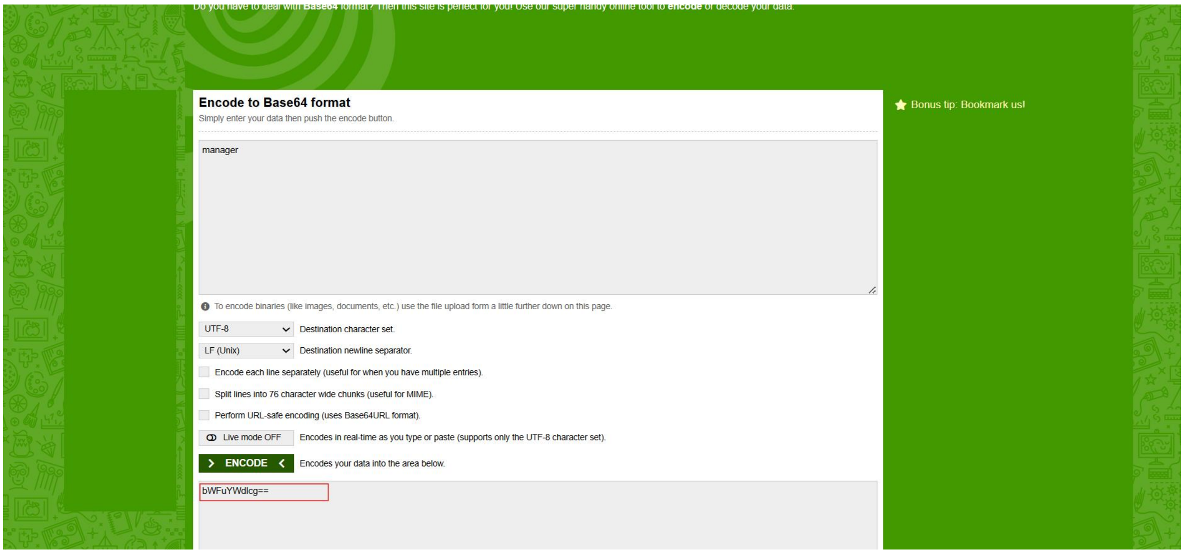
□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

doctor

After decoded the cookie value , it was doctor , what about encode manager and replace it with the old cookie value ?



Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to **encode** or decode your data.

Encode to Base64 format

Simply enter your data then push the encode button.

```
manager
```

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

□ Encode each line separately (useful for when you have multiple entries).

□ Split lines into 76 character wide chunks (useful for MIME).

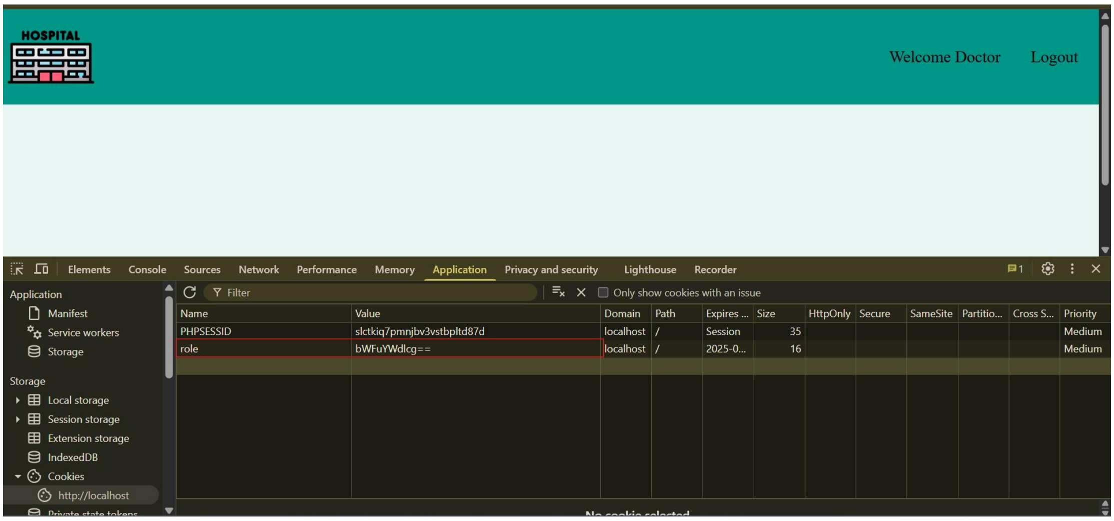
□ Perform URL-safe encoding (uses Base64URL format).

Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

ENCODE Encodes your data into the area below.

```
bWFuYWdlcg==
```

I encoded manager word

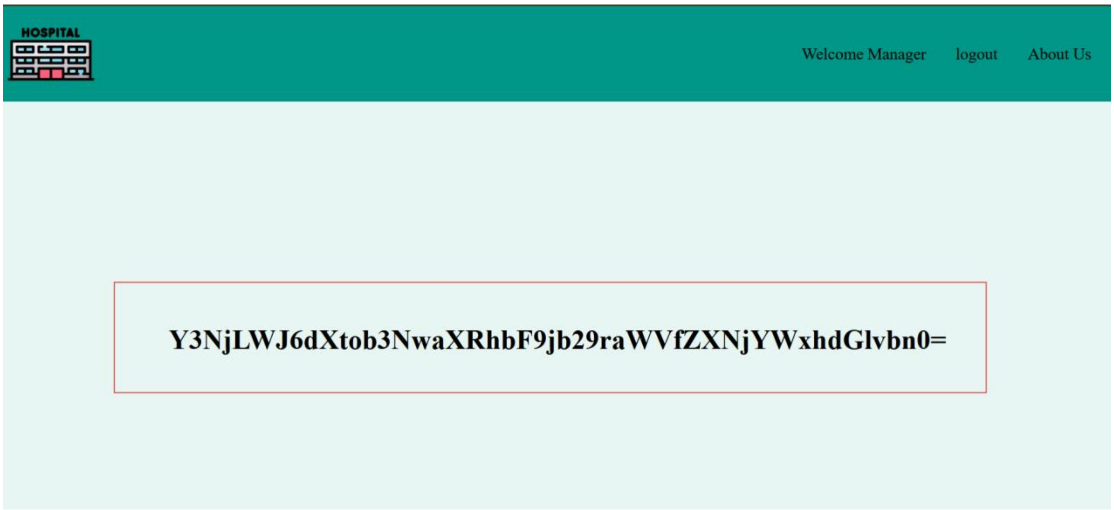


□ Only show cookies with an issue

Name	Value	Domain	Path	Expires ...	Size	HttpOnly	Secure	SameSite	Partitio...	Cross S...	Priority
PHPSESSID	slctkiq7pmnjbv3vstbpltd87d	localhost	/	Session	35						Medium
role	bWFuYWdlcg==	localhost	/	2025-0...	16						Medium

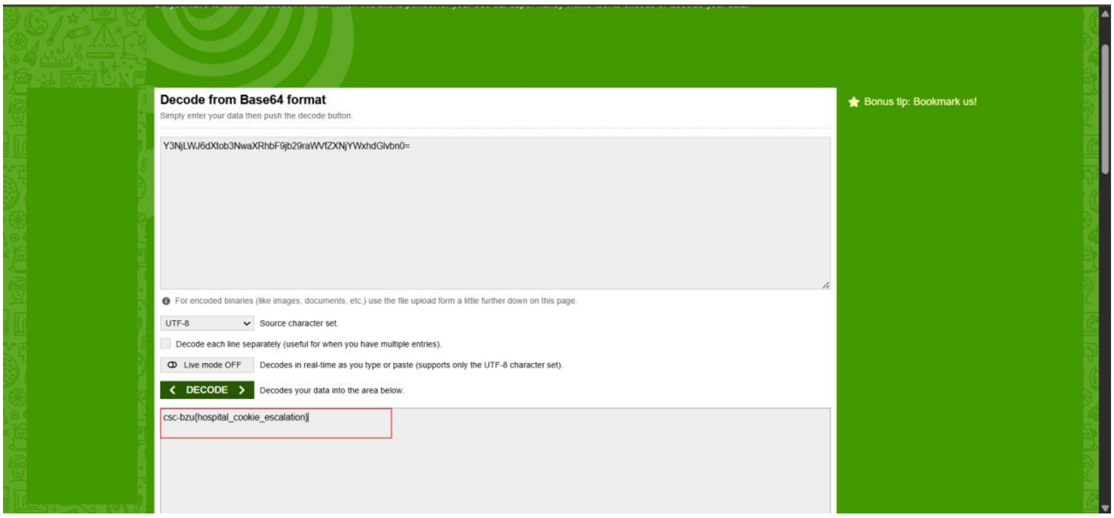
No cookie selected

I replaced the old cookie value with the encoded manager word



Y3NjLWJ6dXtob3NwaXRhbF9jb29raWVfZXNjYWxhdGlvbn0=

I access as manager role , I think it is the flag but it seem the flag encoded with base64.



Decode from Base64 format

Simply enter your data then push the decode button.

```
Y3NjLWJ6dXtob3NwaXRhbF9jb29raWVfZXNjYWxhdGlvbn0=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 — Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF — Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE — Decodes your data into the area below.

```
csc-bzu{hospital_cookie_escalation}
```

I decoded and I got the flag