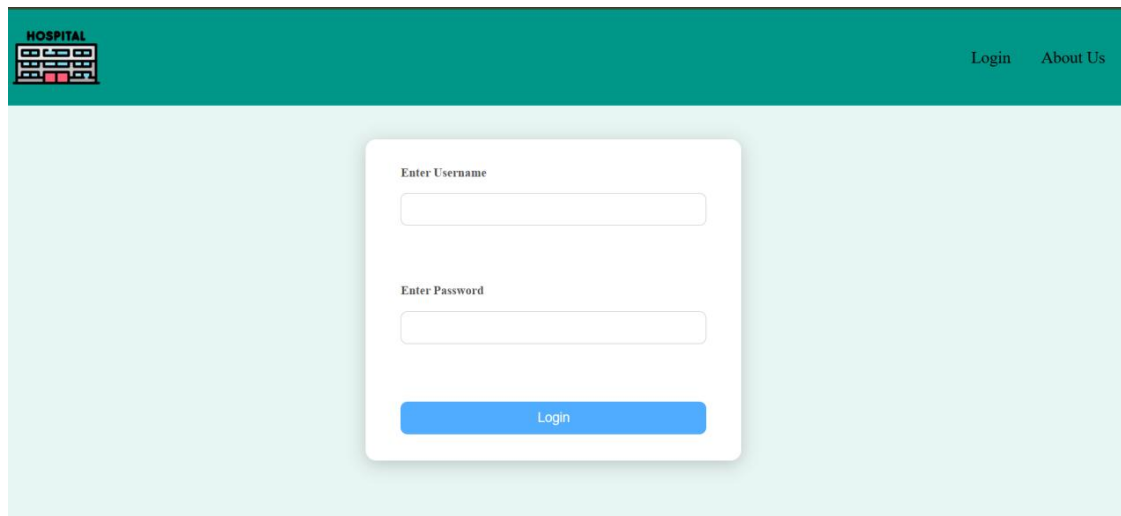


Dr.Adminectomy Writeup

Category : Web Security

Author : Baraa Sabbah



HOSPITAL

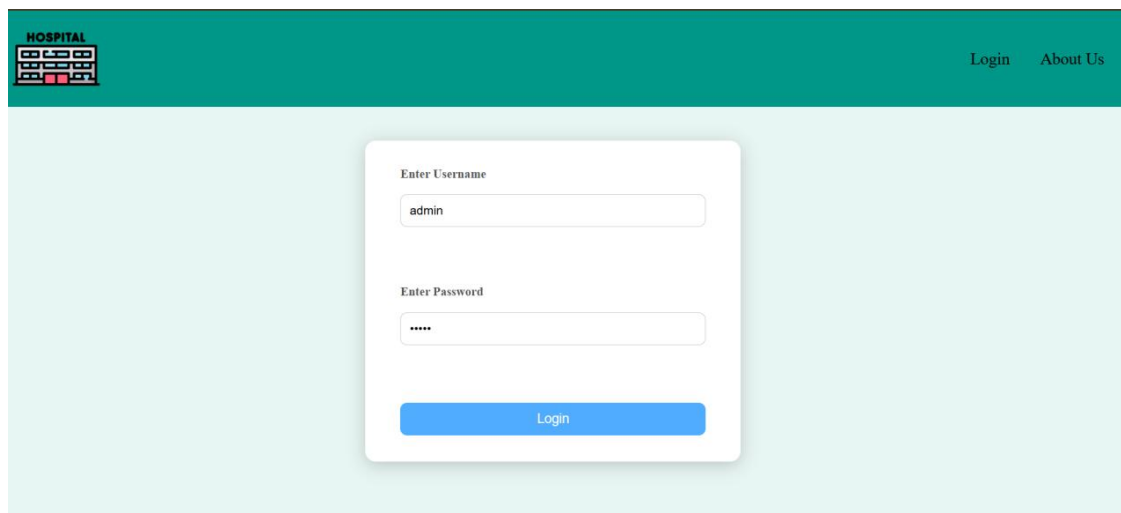
Login About Us

Enter Username

Enter Password

Login

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



HOSPITAL

Login About Us

Enter Username

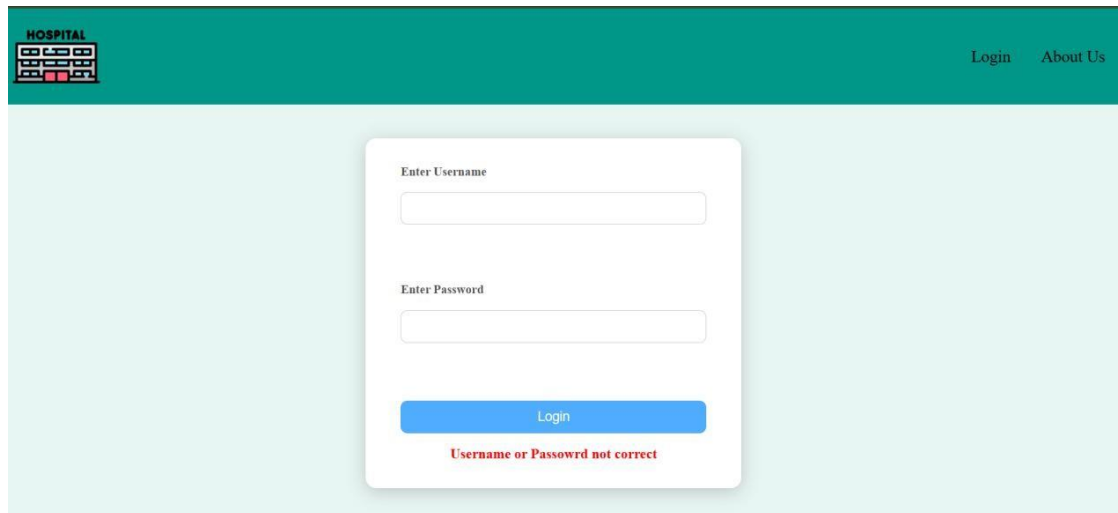
admin

Enter Password

\*\*\*\*

Login

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



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

```
line wrap
<html>
  <head>
    <title>Main Page</title>
    <link rel="stylesheet" type="text/css" href="styles.css">
  </head>
  <body>
    <div class="menu">
      
      <div class="options">
        <a href="index.php?login">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>
        <label>Enter Password</label>
        <input type="password" name="password"><br>
        <input type="submit" name="submit" value="Login">
        <div style="color: red;">Username or Passowrd not correct</div>
      </form>
    </div>
  </body>
</html>
```

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

```
border-radius: 15px;
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: 16px;
  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);
}

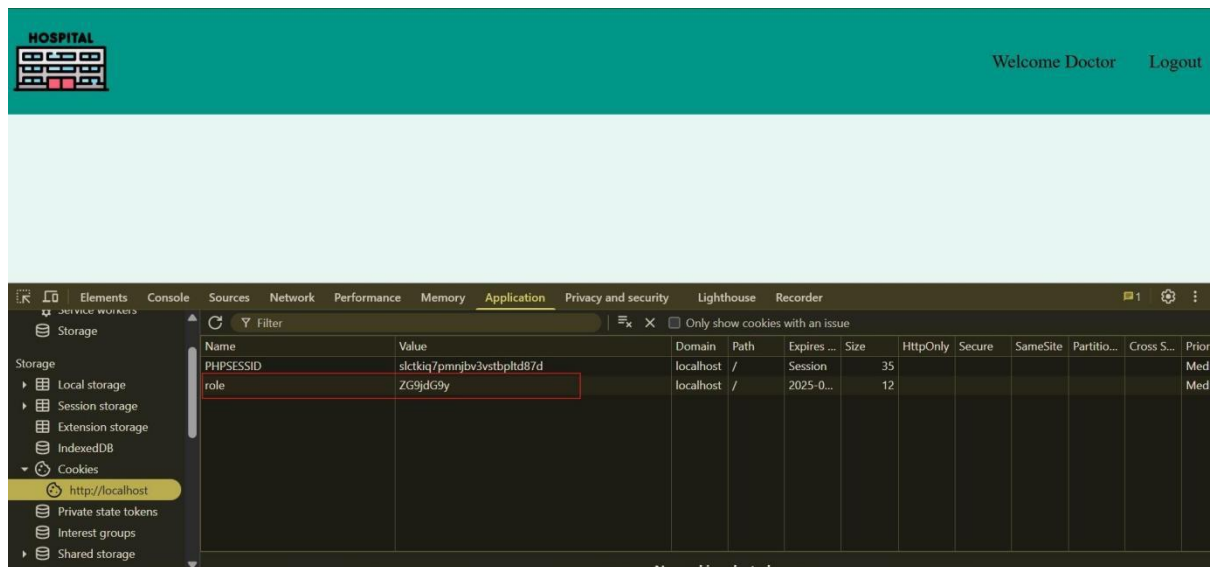
/*
test account
username:baraa
password:baraa@ssword
*/

.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



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 .



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.

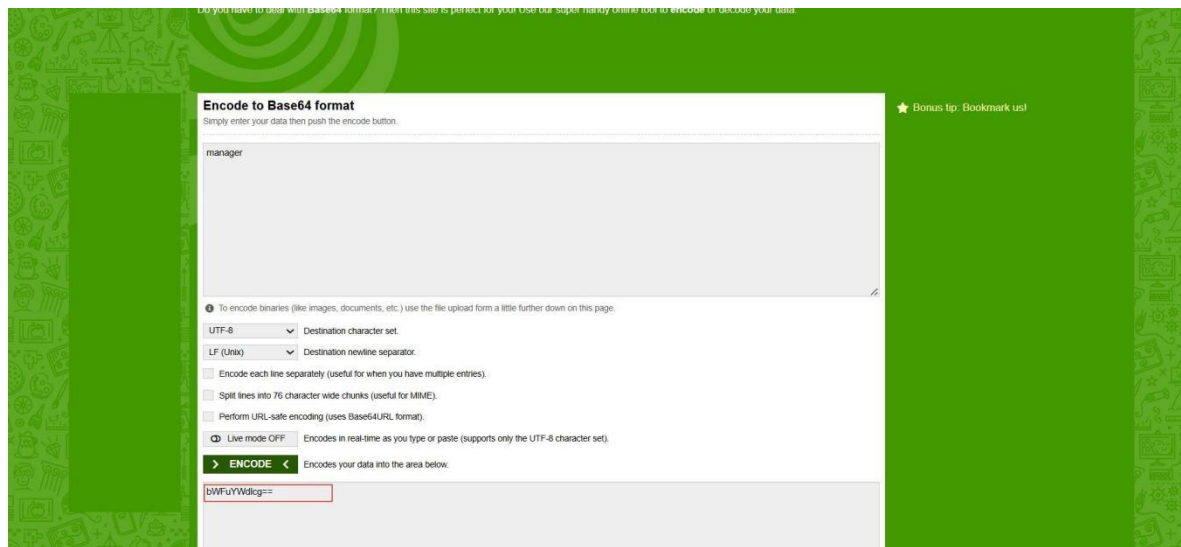
☐ Decode each line separately (useful for when you have multiple entries).

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

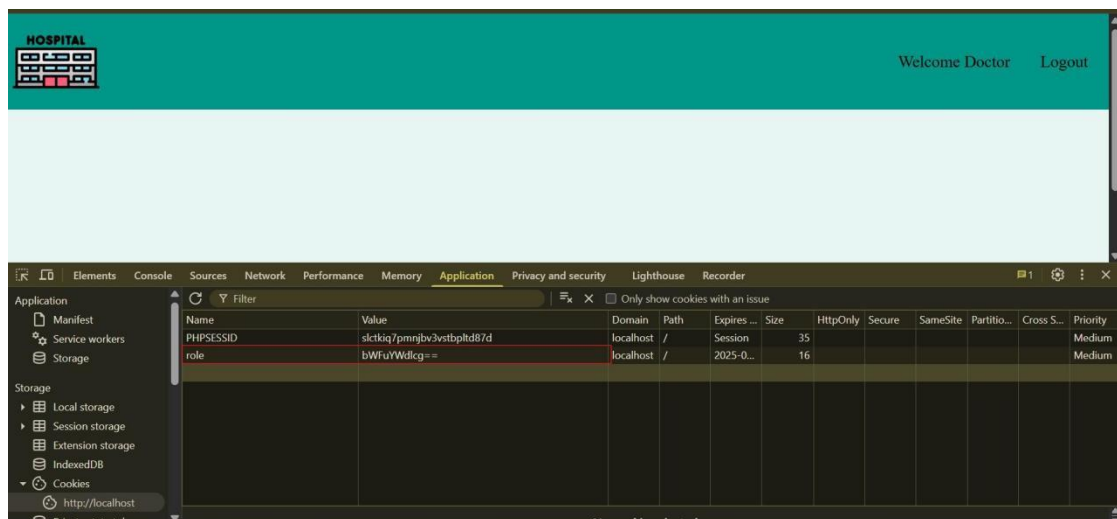
**< DECODE >** Decodes your data into the area below.

doctor

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



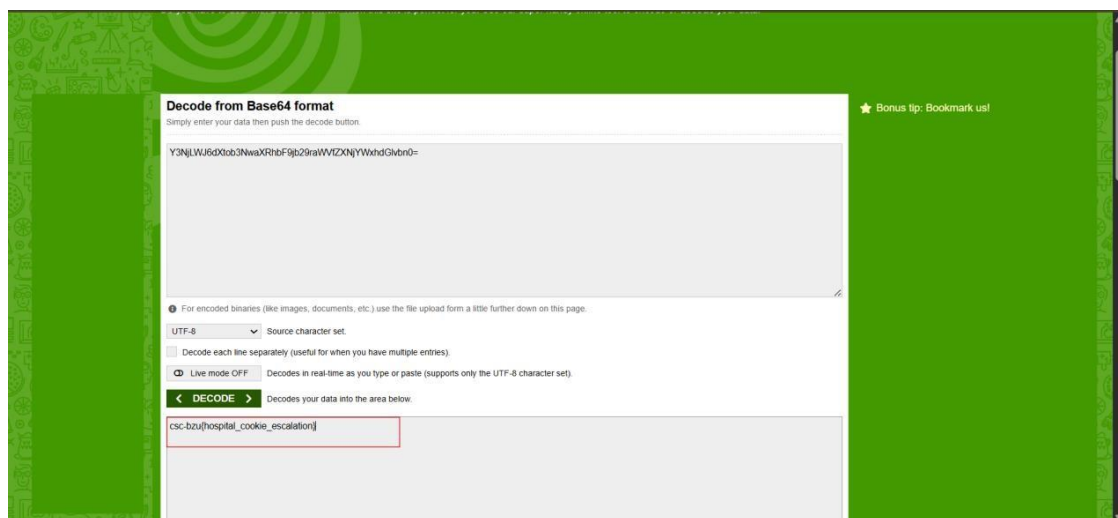
I encoded manager word



I replaced the old cookie value with the encoded manager word



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



I decoded and I got the flag