

picoCTF

Local Authority

Isaac Falero

IS 401/501

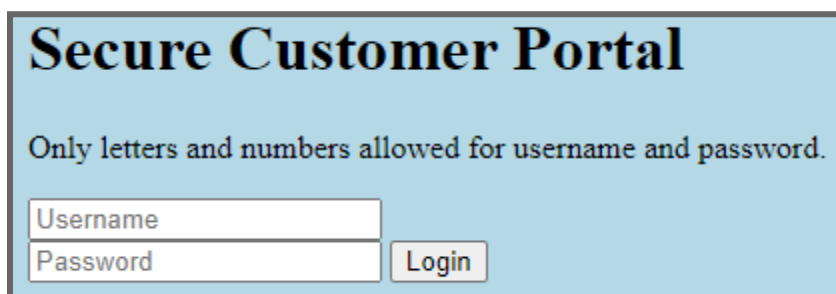
10/24/2023

Description: Can you get the flag? Go to this website and see what you can discover.

Website: <http://saturn.picoctf.net:50920>

Hint: How is the password checked on this website?

Upon opening the link, we are directed to a login page asking for a valid username and password:



1. We'll start by opening the HTML source code to search for any clues.. Upon inspection, we can see an action called "login.php."

```
<p>Only letters and numbers allowed for username and password.</p>

<form role="form" action="login.php" method="post">
  <input type="text" name="username" placeholder="Username" required
    autofocus></br>
  <input type="password" name="password" placeholder="Password" required>
  <button type="submit" name="login">Login</button>
</form>
</body>
</html>
```

2. Using this action at the URL or failing a login attempt will forward us to a new page telling us our login failed. Page: <http://saturn.picoctf.net:50920/login.php>



3. If we open the source code of this /login.php page, we can see a reference to a script called "secure.js."

```
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <link rel="stylesheet" href="style.css">
  <title>Login Page</title>
</head>
<body>
  <script src="secure.js"></script>

  <p id='msg'></p>

  <form hidden action="admin.php" method="post">
    <input type="text" name="hash" required="" value="" />
  </form>
```

4. Opening this file will present the script which displays the valid username and password for the login page.

```
function checkPassword(username, password)
{
  if( username === 'admin' && password === 'strongPassword098765' )
  {
    return true;
  }
  else
  {
    return false;
  }
}
```

5. Using the provided username and password will forward you to a new page containing the flag.

picoCTF{j5_15_7r4n5p4r3n7_05df90c8}

Flag: picoCTF{j5_15_7r4n5p4r3n7_05df90c8}