Pii-Scammer – Cookie Manipulation

Name ▲	Value
user	%7B%22fullname%22%3...

After submitting information to this app, there's a cookie that is set, which specifies which user we're working as

Pii-Scammer – Cookie Manipulation

Well done young Obi-Wan... Here is a flag for your troubles... ETSCTF_6f4d2b8d3f31c9c82781bf195122663e Dont forget to check the /admin section.

If we delete the value of the user cookie (without deleting the entire cookie), we get a different response from the app

Pii-Scammer – Cookie Manipulation

Well done young Obi-Wan... Here is a flag for your troubles... ETSCTF_6f4d2b8d3f31c9c82781bf195122663e Dont forget to check the /admin section.

We're directed toward the /admin.php endpoint, so let's see what's there...

Pii-Scammer – Cookie Manipulation

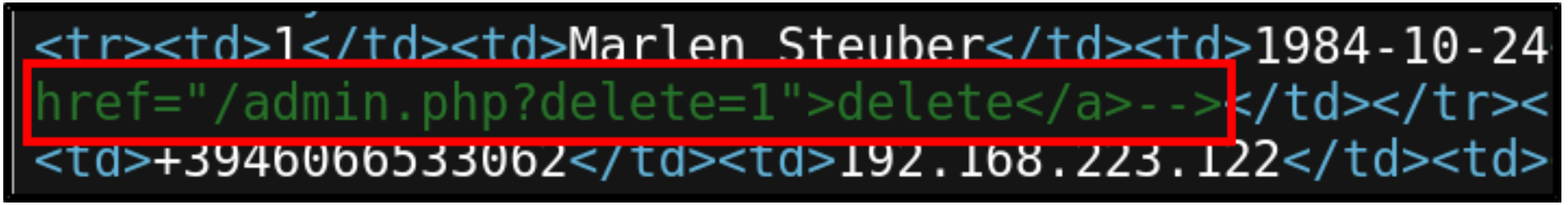
On the /admin.php endpoint, we see the page is expecting an admin cookie, so we can set one for ourselves

Pii-Scammer – SQL Injection

100	Eriberto Tillman	1962-05-06	fingerprint
101	Collin Orn	1938-09-01	[redacted]

Once we have the admin cookie set, we see a table with all sorts of personal information, at the bottom of the table, there's a flag waiting for us...

Pii-Scammer – SQL Injection



We also see there's a function that the app uses to delete users, but the challenge description says we need to delete the entire table all at once

Pii-Scammer – SQL Injection

```
DELETE FROM table_name WHERE id ='number'
```

To delete all of the entries at once, we need to modify the SQL statement with injection

Pii-Scammer – SQL Injection

```
DELETE FROM table_name WHERE id ='number'
```

The app likely uses a SQL statement similar to the one above to delete the entries, and the red part of the statement is where we can inject SQL instructions

Pii-Scammer – SQL Injection

```
DELETE FROM table_name WHERE id ='1' or 1=1
                              -- '
```

If we use an injection like the one above (the red text), it will delete all of the entries

Pii-Scammer – SQL Injection

```
DELETE FROM table_name WHERE id ='1' or 1=1
                              -- '
```

The `or 1=1` part of the statement will adjust the statement so it will match all of the ID numbers

Pii-Scammer – SQL Injection

Then we get the final flag from the challenge