Web Application Security

Use Burp and cewl to enumerate users on the Mutillidae site

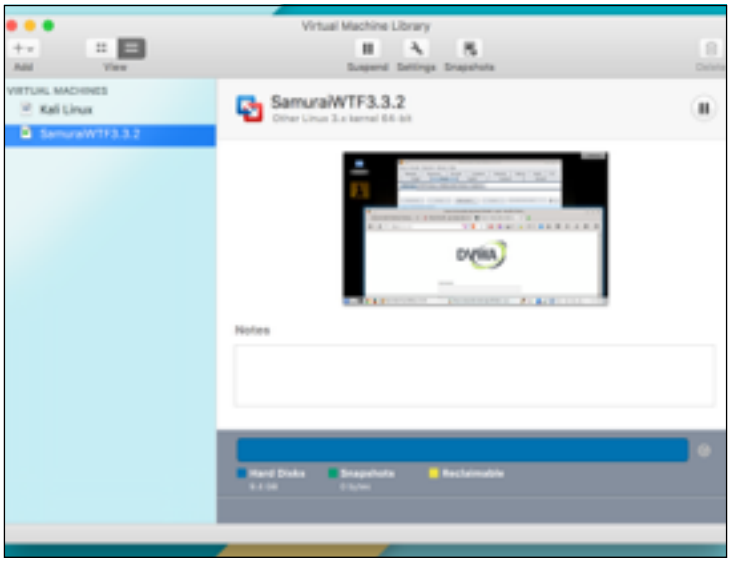
Part 2 - 18 March 2016

Setup

Open Your Vm Fusion

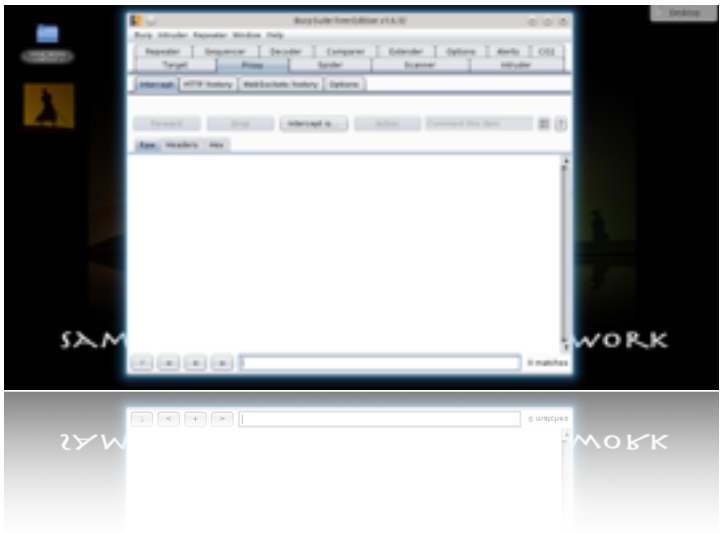
Instructions:

1. On Your Host Computer, Go To
2. Applications --> All Program --> VM Fusion
3. Select Samjuri.wtf and Boot the Vm



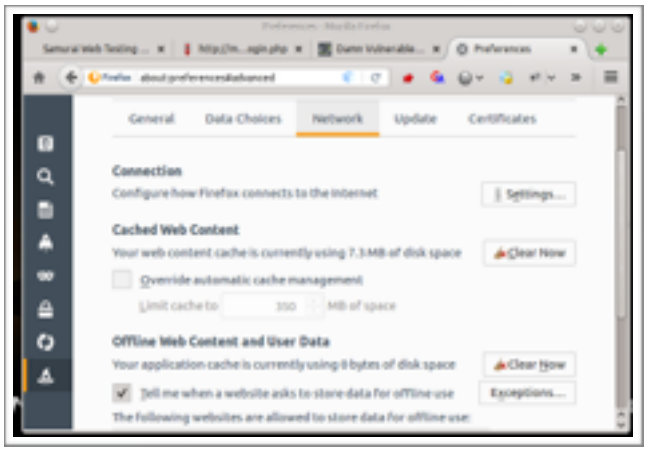
Open the following

1. **Burp Free Suite**
2. **Firefox**

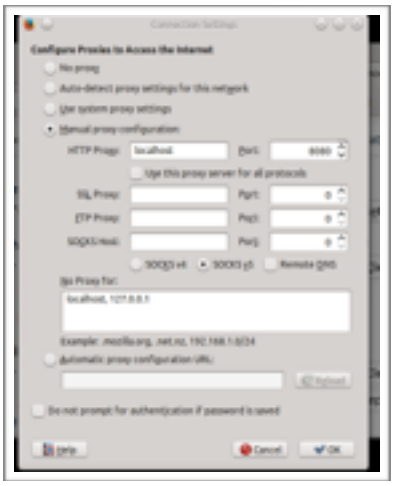


Firefox Setup

1. Switch to Firefox
2. Go to options
3. Click
    1. Advanced
    2. network tab
    3. settings

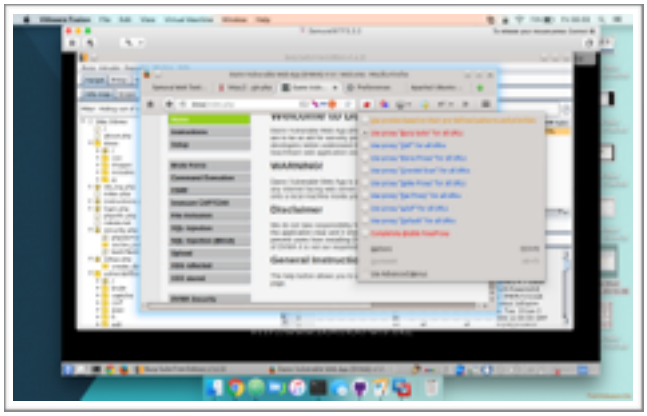


4. When opened, check Manual Proxy Configuration.
5. Make sure the Http Proxy is **localhost**
6. Make sure the Port is **8080**



Or

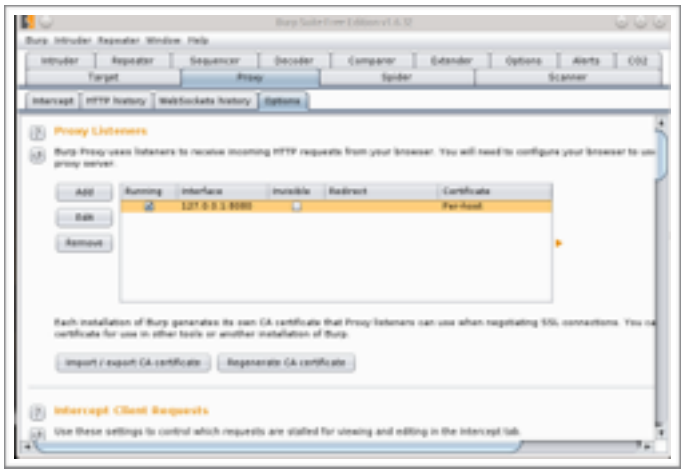
1. Click on foxy Proxy Add-on
2. Click Use “Burp settings”



Visit **http://dvwa/login.php**

Burp Setup

1. Switch Burp suite
2. Make sure you listening to **localhost:8080**
3. To Check this open Burp Suite and click Proxy -> Options



4. Next select Proxy and turn on intercept

Step 1

Now that we have everything set up with our proxy running and it incepting .

Valid account attempt

1. First open up **firefox** and open the following url http://mutillidae/index.php?page=login.php
2. **Create an account, I created one called superAdmin with password GTIBUDDY123**
3. **In Burp suite we have incepted the request and we can see the request being made in this caseusername=superAdmin&Password=**

4. **You then want to right click on the send to request and click send to repeater and then click forword.**

Invalid login attempt

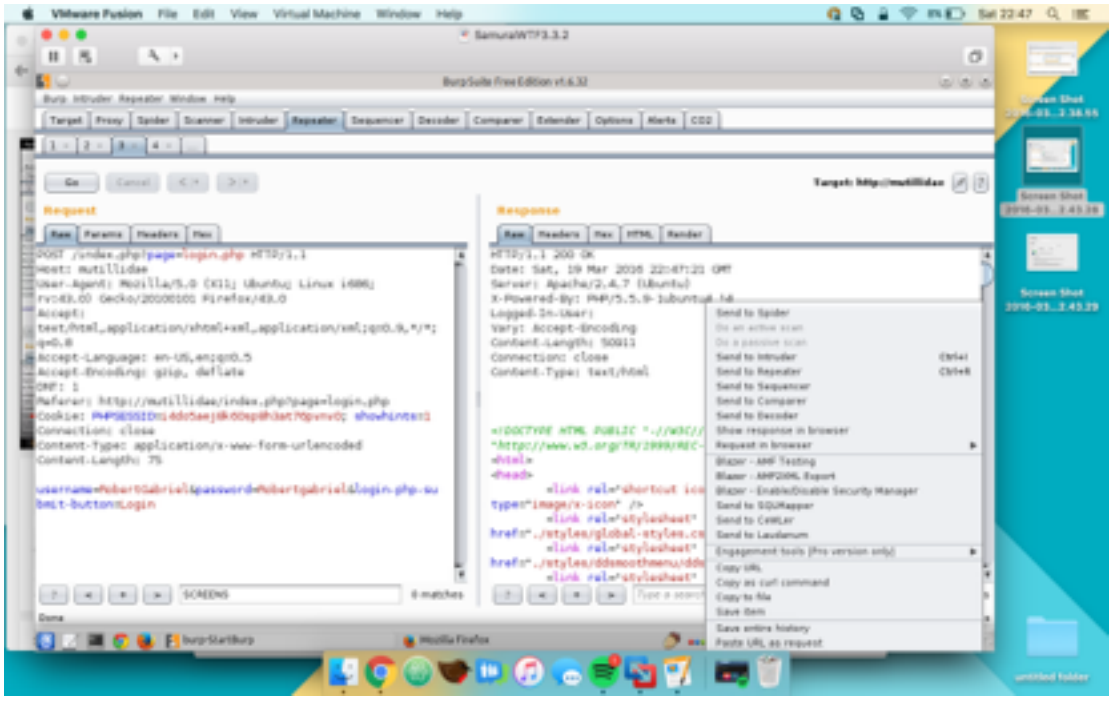
1. First open up **firefox** and open the following url http://mutillidae/index.php?page=login.php
2. **On this page we will want to intercept a invalid login attempt to base our http request on.**
3. **In Burp suite we have incepted the request and we can see the request being made in this caseusername=RobrtGabriel&Password=rObertGABRIEL**
4. **You then want to right click on the request and click send to repeater and then click forword.**

5. **If you switch back to firefox you will see that it say account not found. This is a bad thing.**

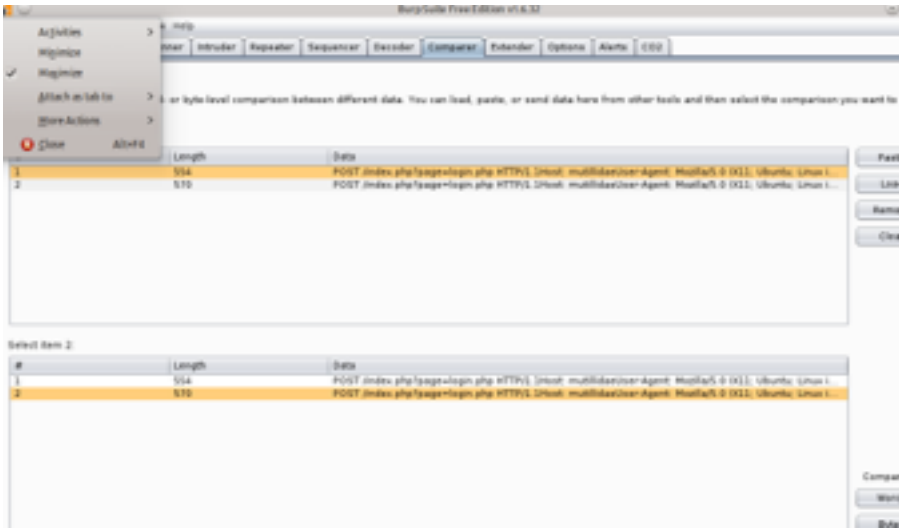
6. **Next Go back to Burp Suite and click on repeater. We need to check that its still working working, do this by clicking Go, this is because .net or newer systems will put in a type of hash to stop hash repeats**

Comparing

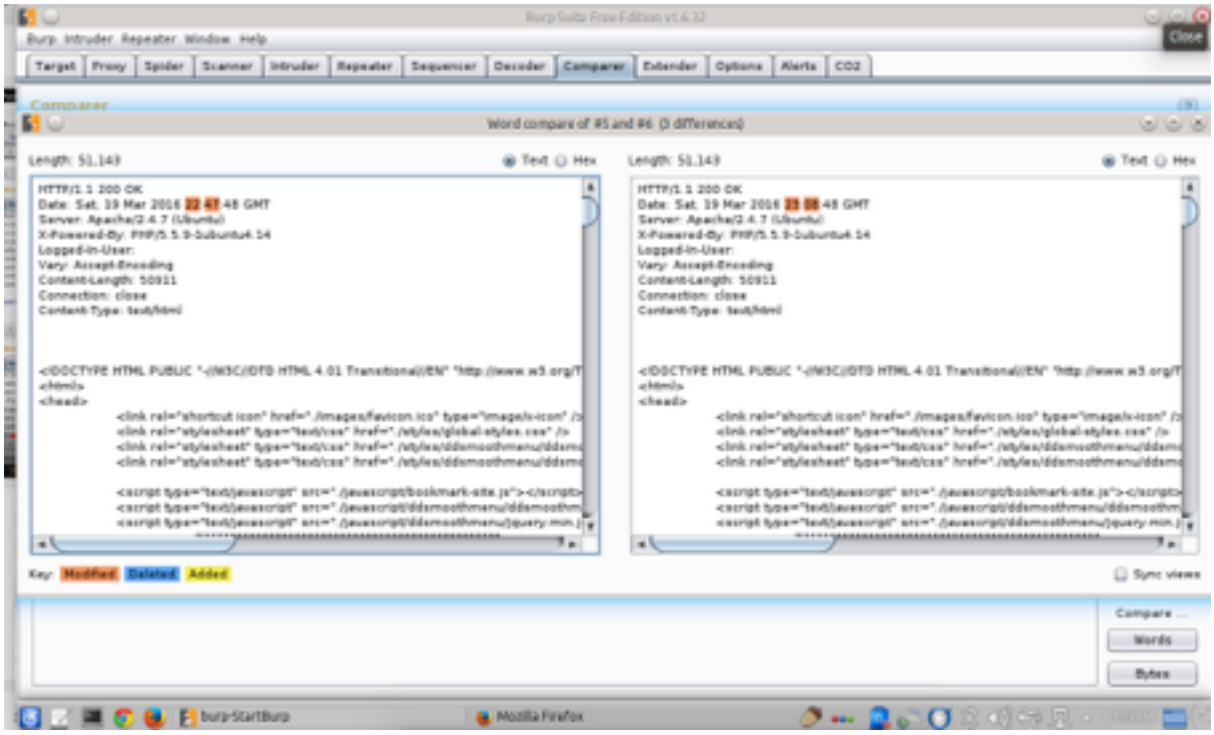
So now go to the repeater tab and click go on both the valid and invalid requests. This will send the responses on the right hand side. Right click and send to to compare



So now that we have sent both the valid and invalid request to the compare tab.



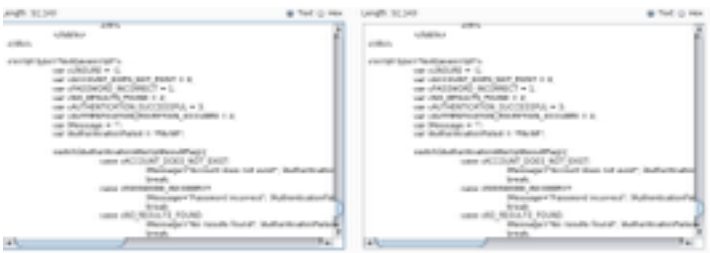
You want to click the compare words button on the bottom right.



We know want to compare the files and look for differences in the responses.

1. First thing we notice is the different flag numbers

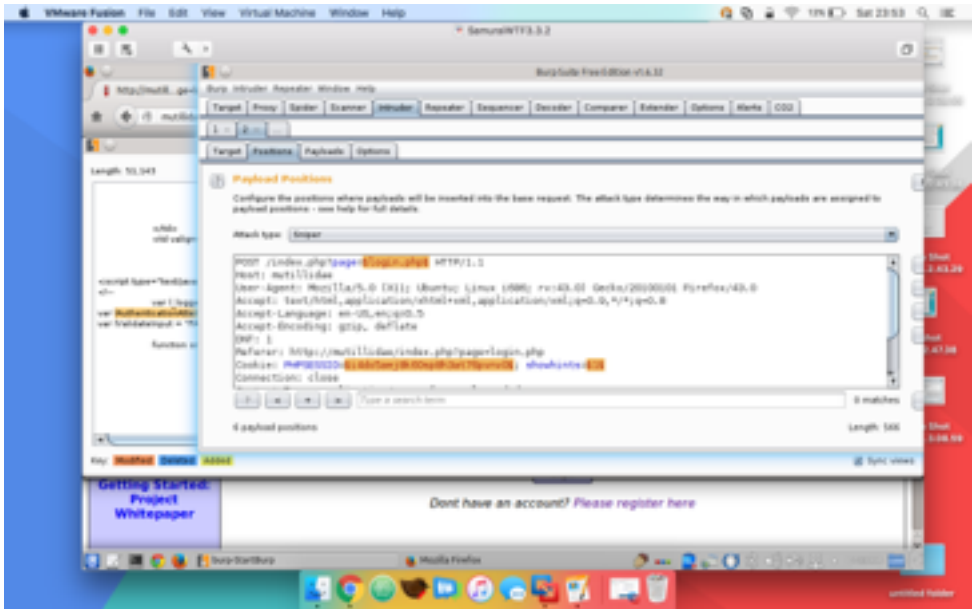
2. Second thing is the error messages if we look one of the responses for **account does not exist**. We discover by searching that term is that the response is used in a javascript switch statement to display a message. So 1 will display account not found. It injects the message into the page after wards.



Next we have to take and remember the variable lAuthenticationAttemptResultFlag.

Next to back to the repeater and send the reponcse to the intruder for lAuthenticationAttemptResultFlag = 1

Here you see all the items are highlighted , clear this by clicking on the right.



Next highlight the username variable and add it by clicking on the right side button add. Also add a fake password input.

```
username=§superAdmin§&password=EDRTFYGHJKL&login-php-submit-button=Login
```

Next click on the payload tab, we will need to get a list of usernames for the payload. Where going to do this using a tool called **cewl. It will scrap usernames from the site to make our list.**

First open up the command line.