Web Application Security

Use Burp to analyse CSRF Tokens in DVWA. Note the different security levels in DVWA (low, medium, high)

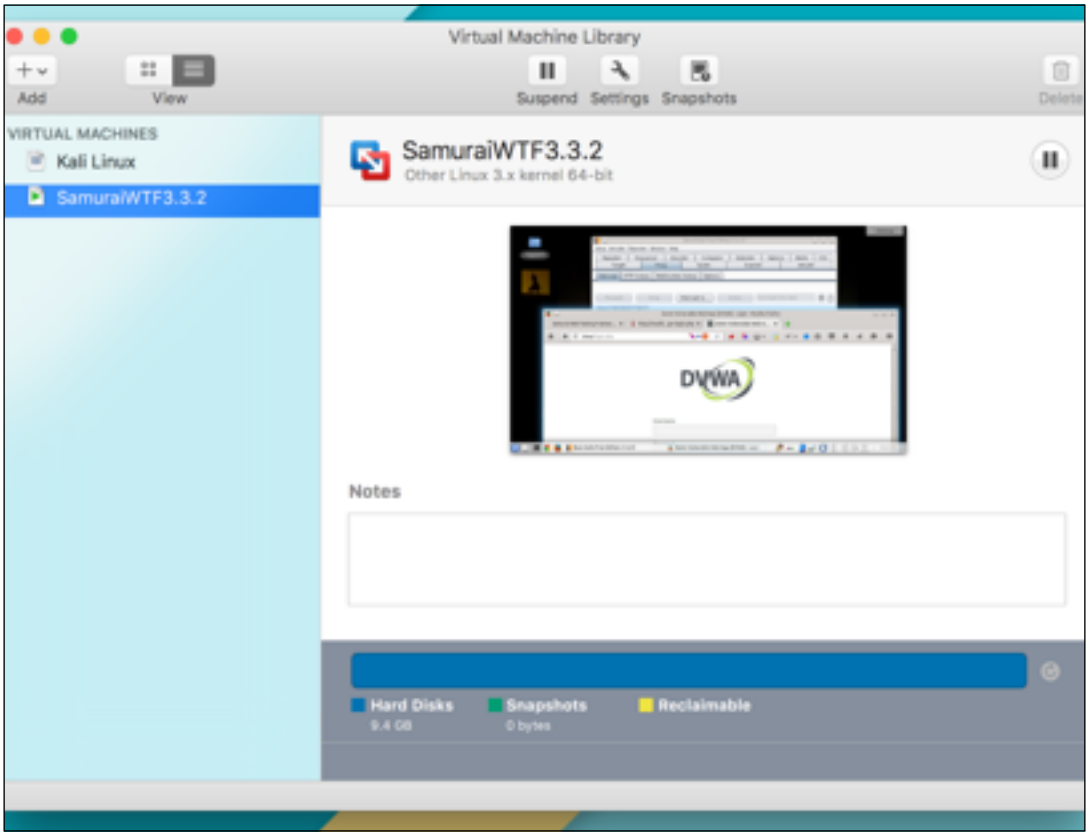
Robert James Gabriel
Part 4 - 13 April 2016

Setup

Open Your Vm Fusion

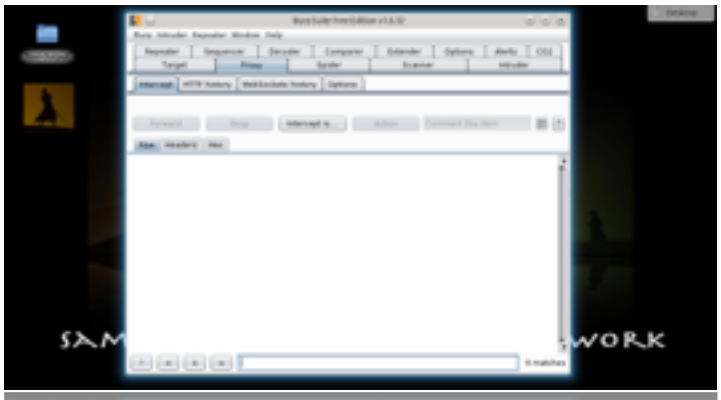
Instructions:

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



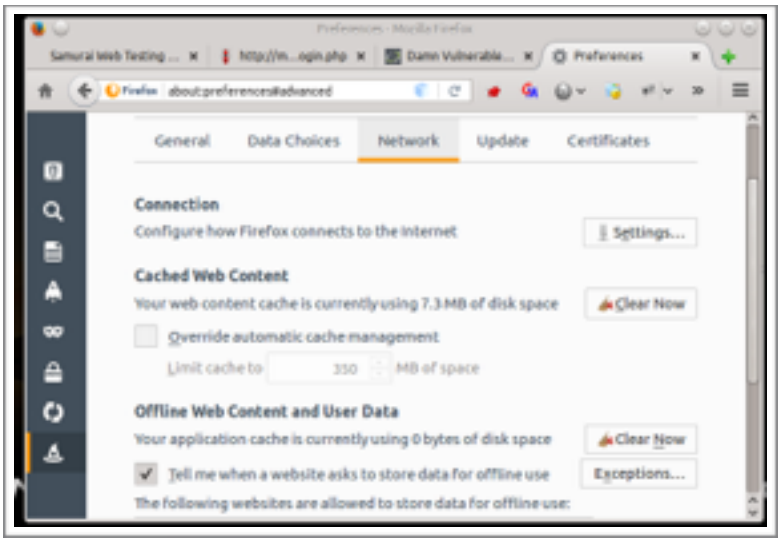
Open the following

1. **Burp Free Suit**
2. **Firefox**

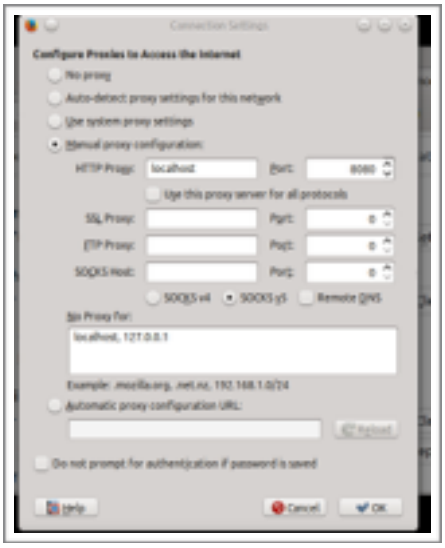


Firefox Setup

1. Switch to Firefox
2. Go to options
3. Click
    1. Advanced
    2. Network tab
    3. Settings

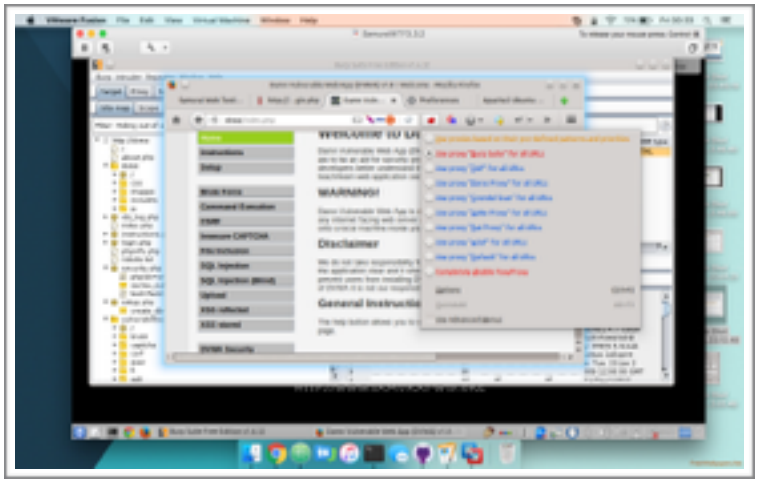


4. When opened, check Manual Proxy Configuration.
5. Make sure the Http Proxy is **localhost**
6. Make sure the Port is **8080**



Or

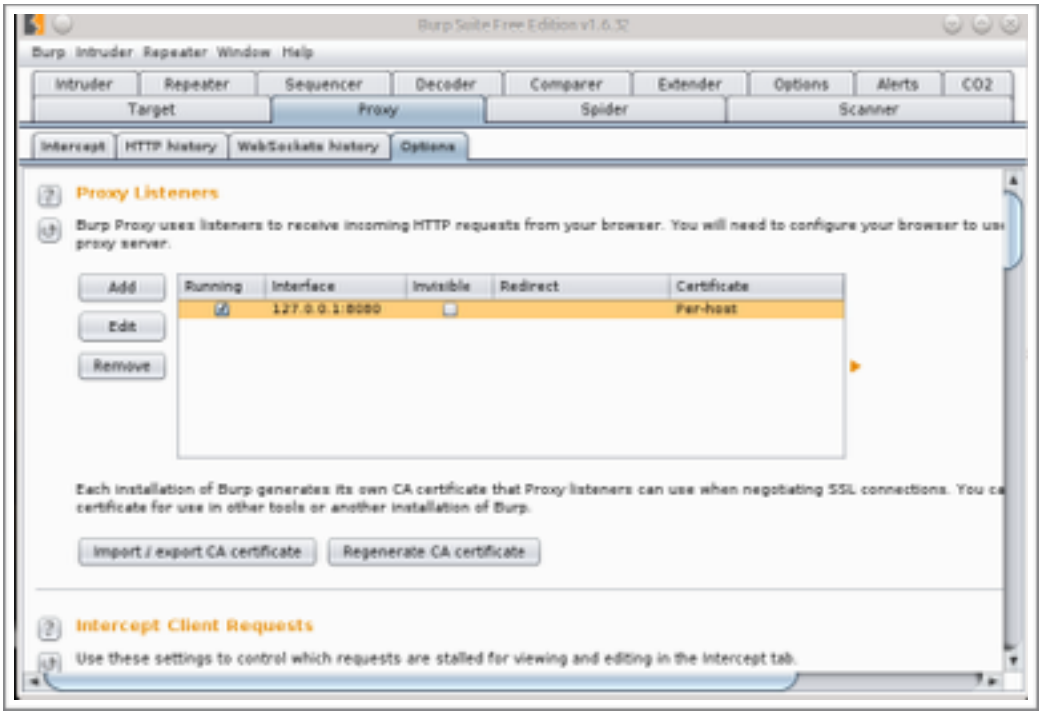
1. Click on foxy Proxy Add-on
2. Click Use “Burp settings”



Visit **hhttp://mutillidae/index.php?page=add-to-your-blog.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 intercert

Use Burp to analyse CSRF Tokens in DVWA. Note the different security levels in DVWA (low, medium, high)

Start Firefox

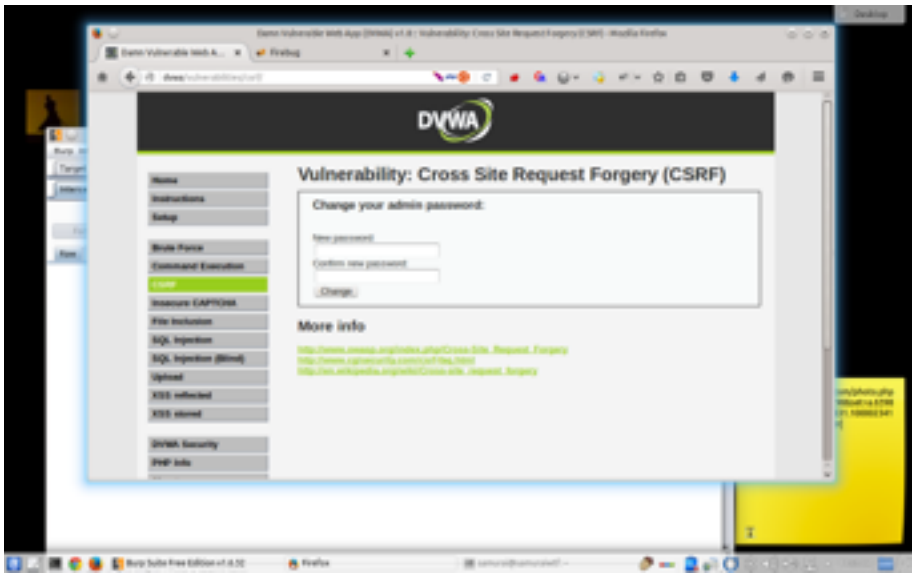
1. Visit: http://dvwa/login.php
2. Login to DVWA
   Login: admin
   Password: password
3. Click on Login

Set DVWA Security Level

4. Click on DVWA Security, in the left hand menu.
5. Select "low"
6. Click Submit

Cross Site Request Forgery (LOW)

1. Select "CSRF" from the left navigation menu.



You need to enter a new and past password, into the two fields above.

Go to Burp Suite, click the Proxy tab, and view the password change http request and forward it after and you will see that your Password Changed on the DVWA site.

Now the part we are interested in is the beginning of the http request which looks something like:

http://dvwa/vulnerabilities/csrf/?
password_new=admin&password_conf=password&Change=Change#

Now all we have to do is construct a link that will perform the same function and hide it in some html so our victim doesn't know it is happening.just until here. There also can be placed in the img tags

Medium settings

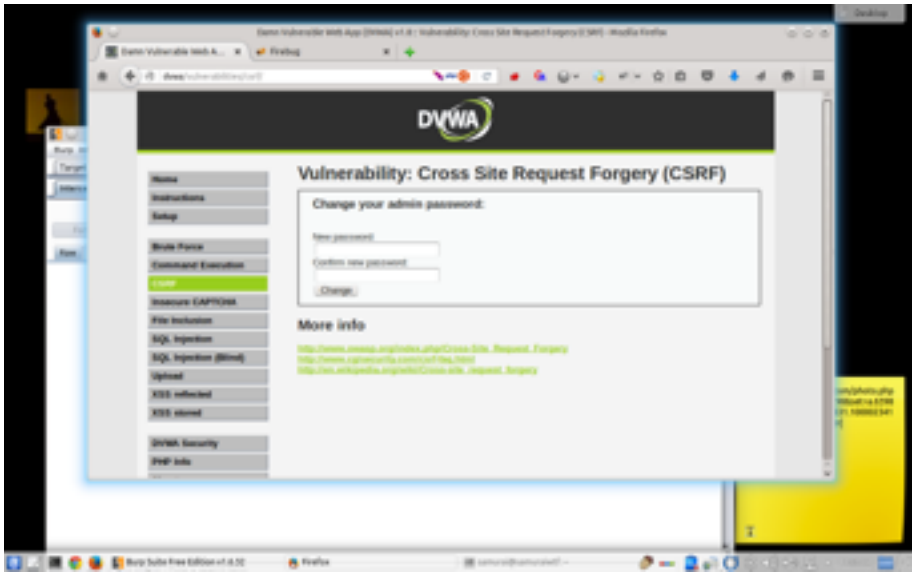
Repeat the following steps but change the settings to medium

Set DVWA Security Level

2. Click on DVWA Security, in the left hand menu.
3. Select "medium"
4. Click Submit

Cross Site Request Forgery (Medium)

1. Select "CSRF" from the left navigation menu.



You need to enter a new and confirm it, into the two fields above.

Go to Burp Suite, click the Proxy tab, and view the password change http request and forward it after and you will see that your Password Changed on the DVWA site.

Now the part we are interested in is the beginning of the http request which looks something like:

http://dvwa/vulnerabilities/csrf/?
password_new=admin&password_conf=password&Change=Change#

Now all we have to do is construct a link that will perform the same function and hide it in some html so our victim doesn't know it is happening.just until here. There also can be placed in the img tags

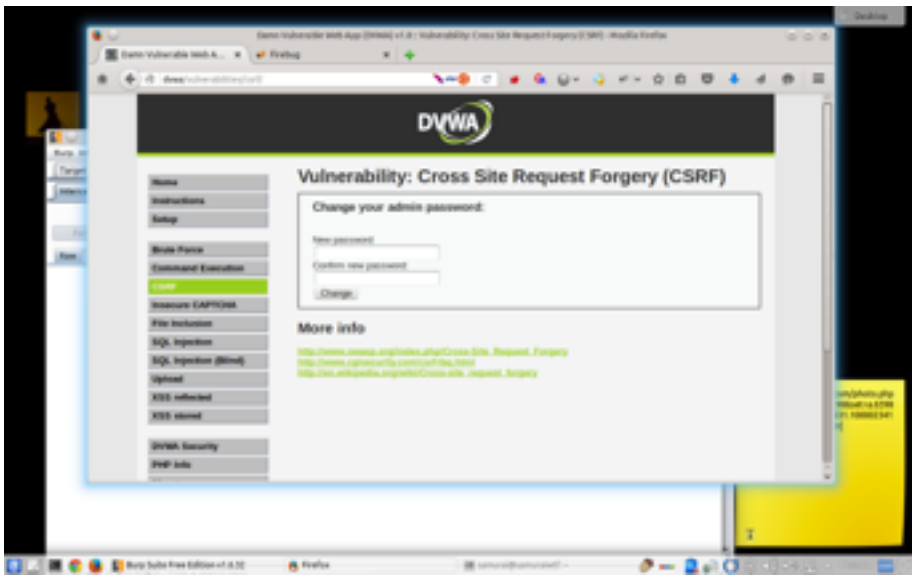
High settings

Repeat the following steps but change the settings to medium

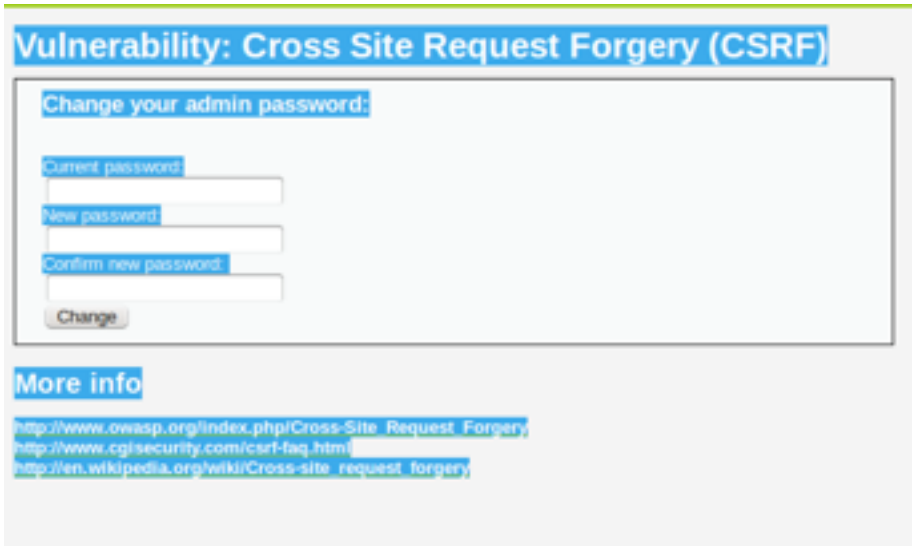
Set DVWA Security Level

2. Click on DVWA Security, in the left hand menu.
3. Select "High"
4. Click Submit

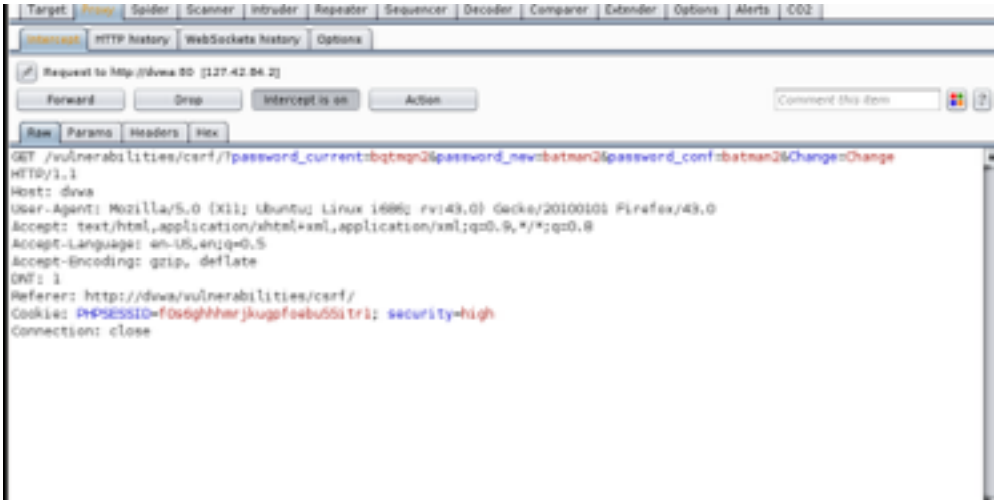
1. Select "CSRF" from the left navigation menu.



You need to enter a new and past password along with a confrirm, into the three fields above. (I did bqtmqn2 as the new password)



Go to Burp Suite, click the Proxy tab, and view the password change http request and forward it after and you will see that your Password Changed on the DVWA site.



Now the part we are interested in is the beginning of the http request which looks something like:

http://dvwa/vulnerabilities/csrf/?password_current=bqtmqn2&password_new=batman2&password_conf=batman2&Change=Change

The difference here you could trick the user into typing in there password and clicking submit which will change there password and send you forward and lock them out.

Now all we have to do is construct a link that will perform the same function and hide it in some html so our victim doesn't know it is happening.just until here. There also can be placed in the img tags