Web Application Security

Describe how you would discover BOTH reflected and stored XSS in DVWA.

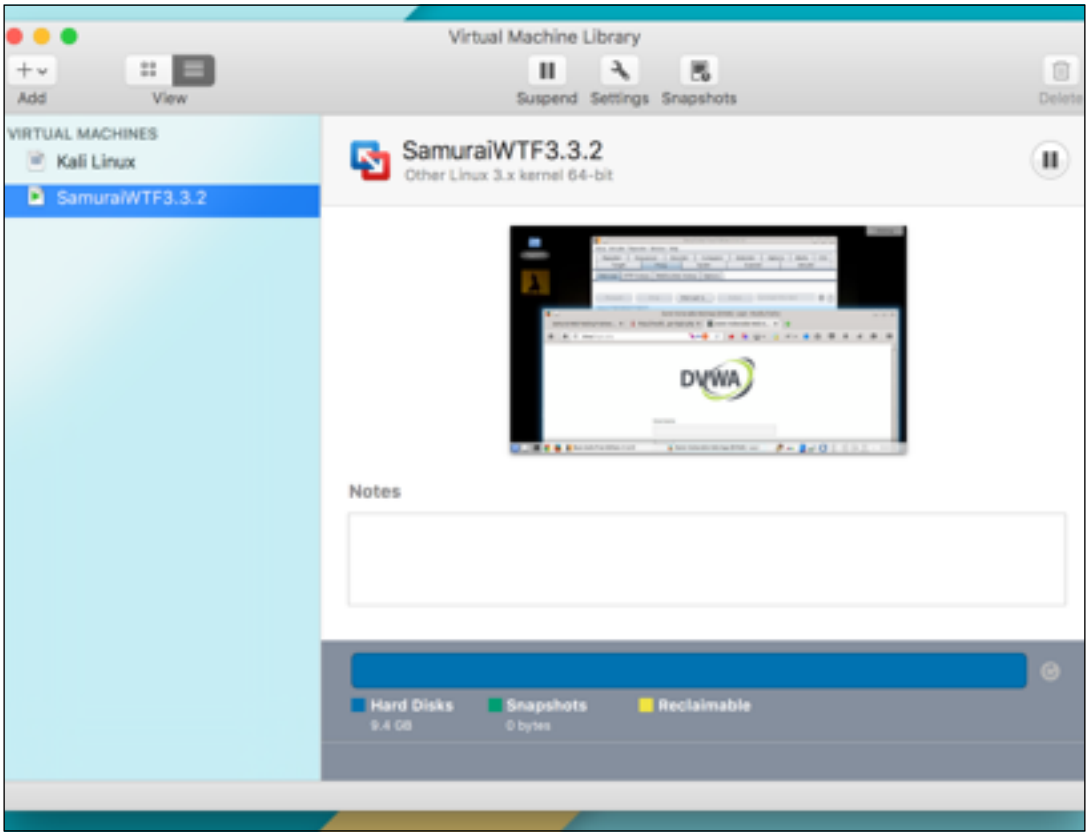
Robert James Gabriel
Part 4 - 13 April 2016

Setup

Open Your Vm Fusion

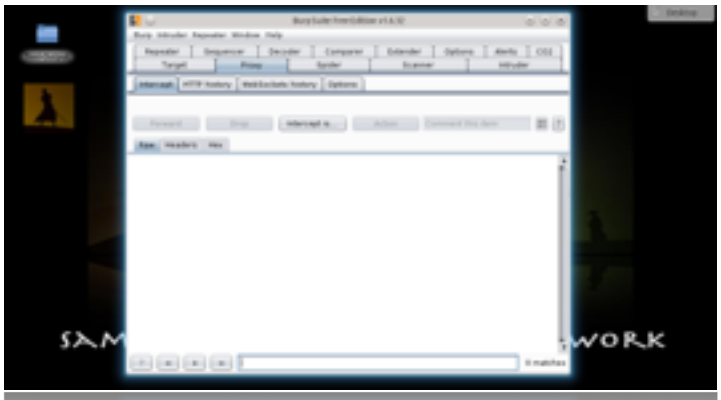
Instructions:

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



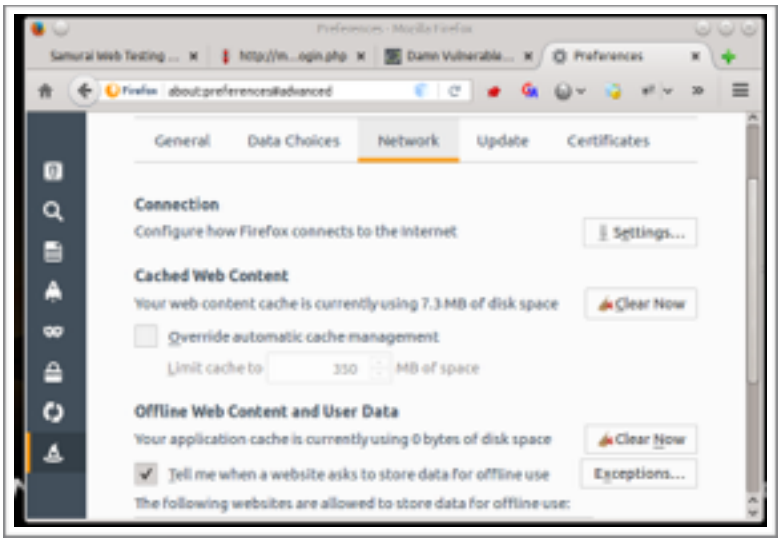
Open the following

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

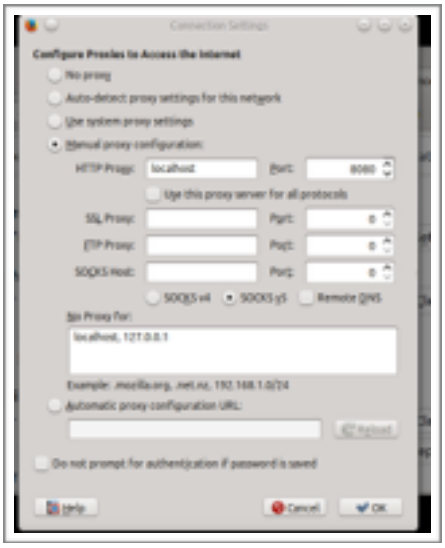


Firefox Setup

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



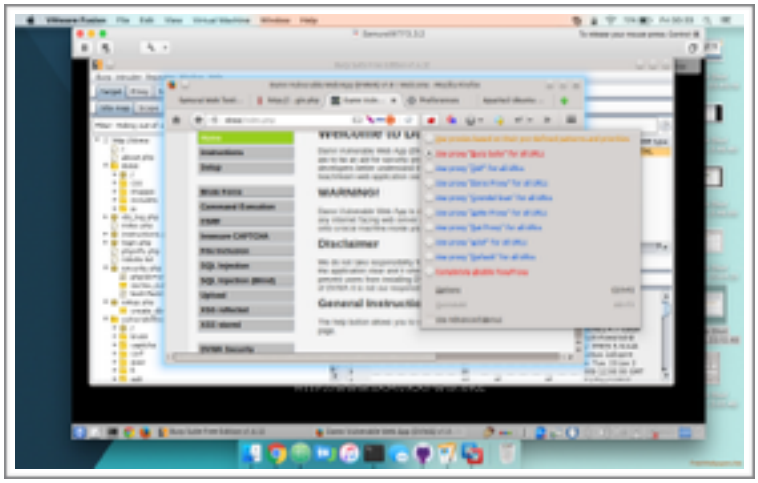
4. When opened, check Manual Proxy Configuration.
5. Make sure the Http Proxy is **localhost**
6. Make sure the Port is **8080**



Or

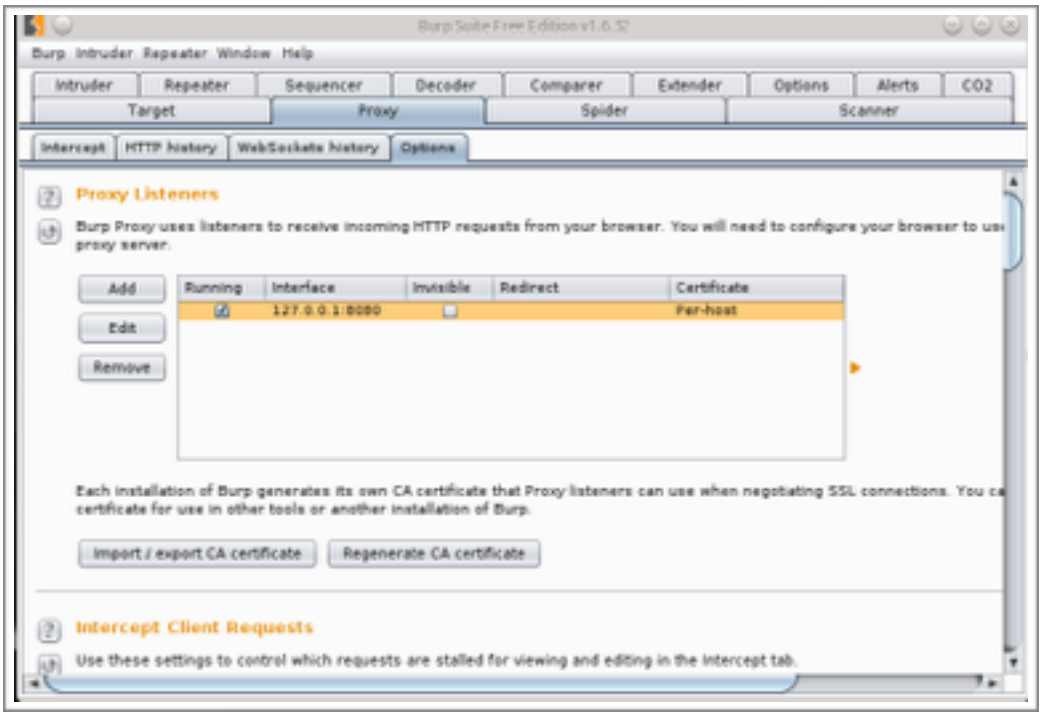
1. Click on foxy Proxy Add-on
2. Click Use “Burp settings”

Visit **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

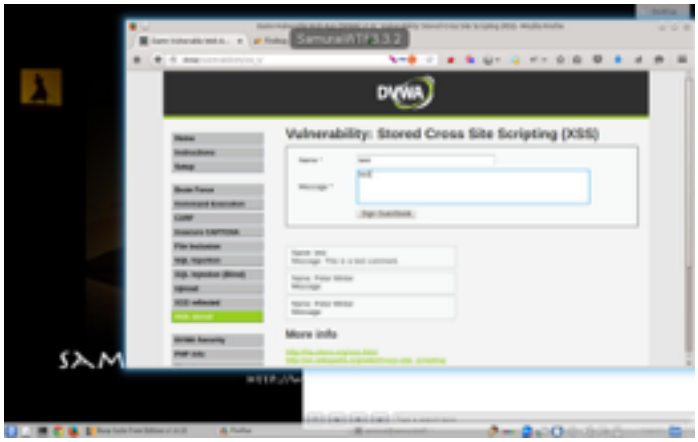


4. Next select Proxy and turn on intercert

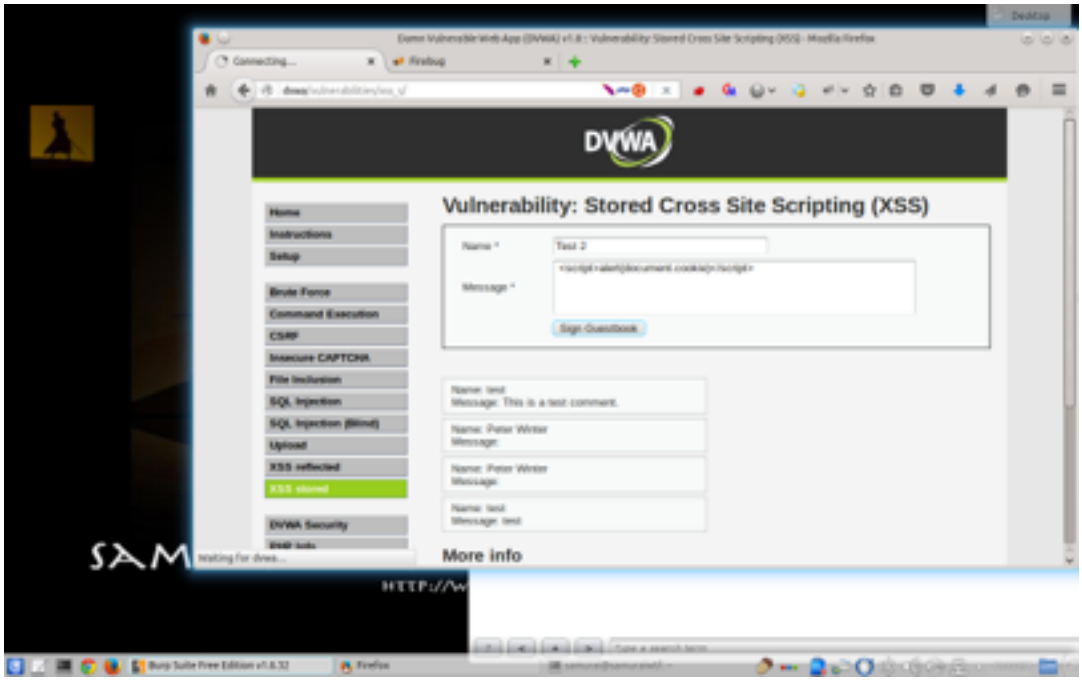
Stored XSS

1. Select “XSS Stored" from the left navigation menu.

So sign into the guest book, I used the following for the inputs test and test.

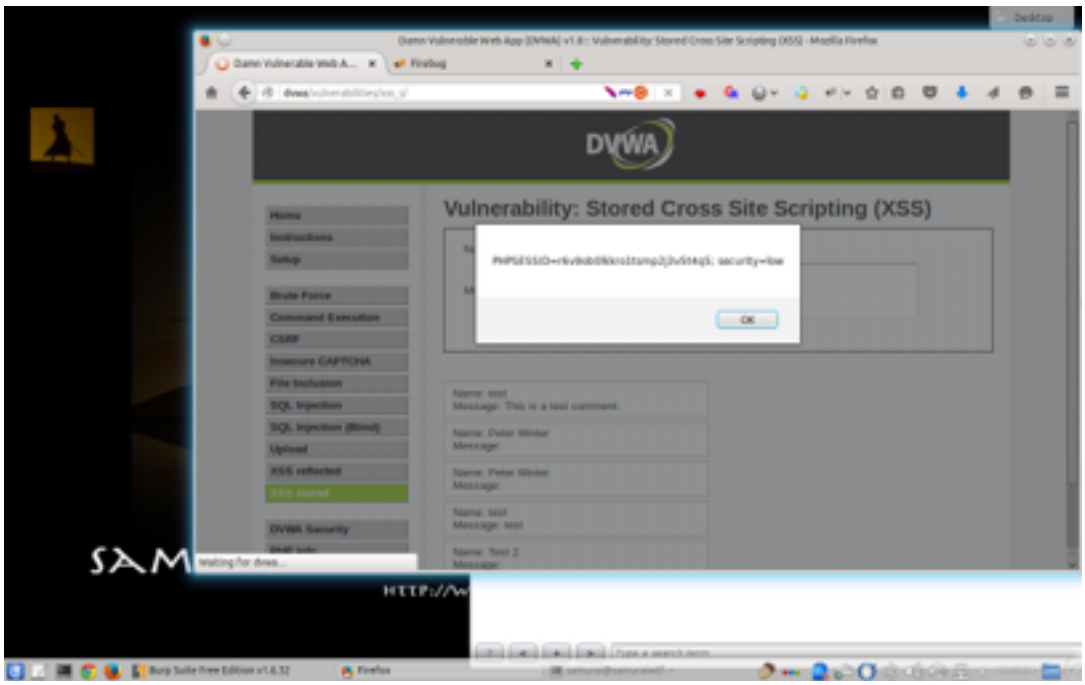


3. Then were going to do it again, but with the following information. name as **test2** and the body as **<script>alert(document.cookie)</script>**



4. Click sign into guest book

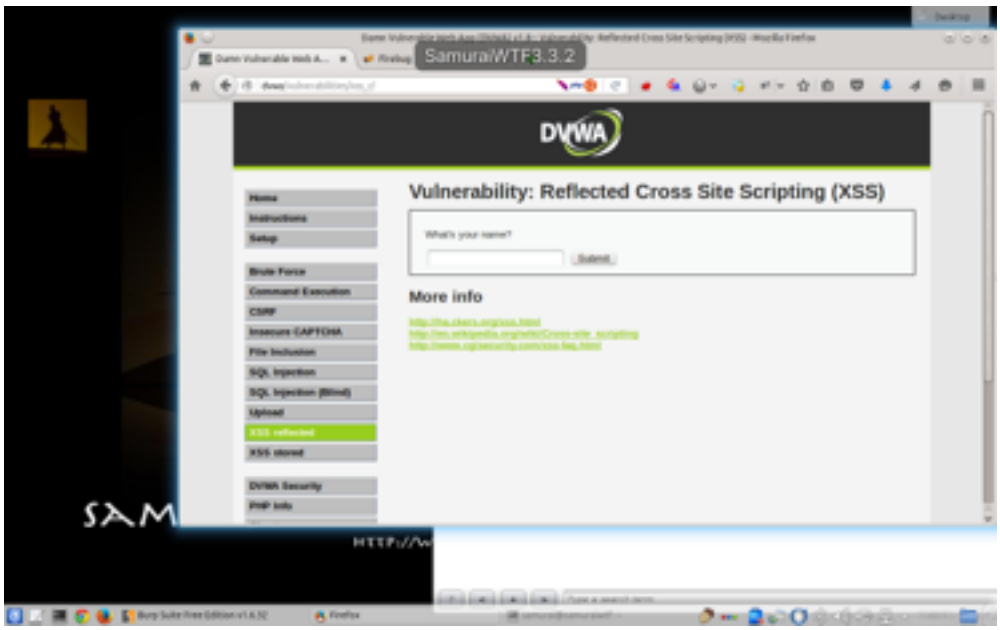
Every time the user goes onto the page the cookie information will be alerted, showing that the stored XSS worked. See attached photo



Reflected XSS

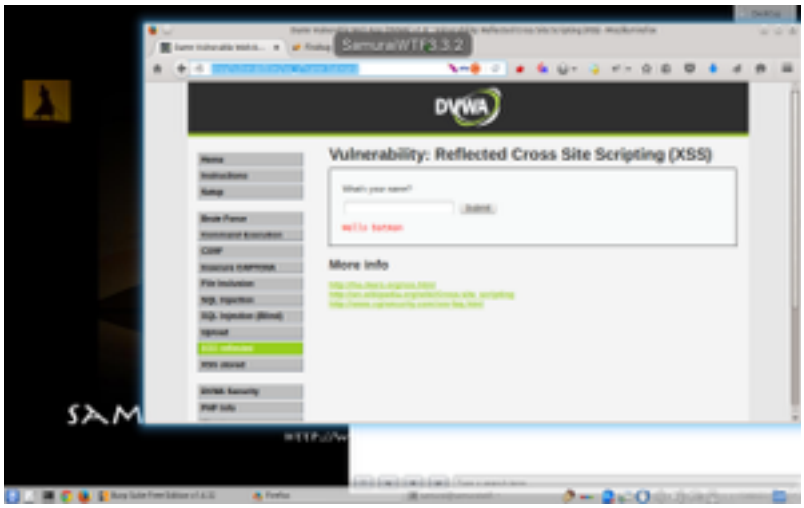
Reflected XSS is basically when a javascript is hidden in the url and then run from the page getting the information

1. Select “XSS Reflected" from the left navigation menu.



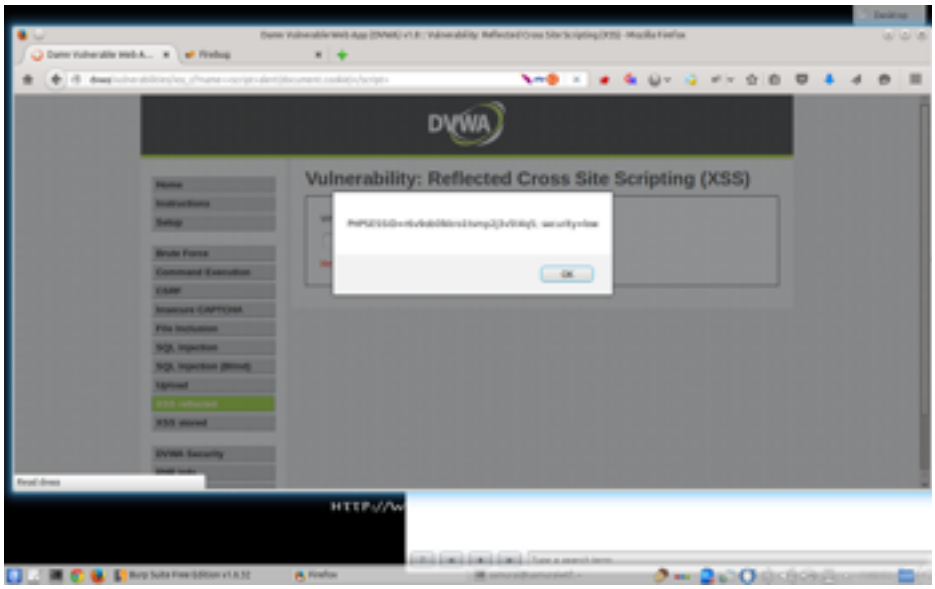
Note the url before we do anything : http://dvwa/vulnerabilities/xss_r/

1. Then we will do a test .
2. I entered batman into the input and clicked submit.
3. After : http://dvwa/vulnerabilities/xss_r/?name=batman#



1. So then we can do what we did last time. By adding javascript after the name parameter . This javascript "**<script>alert(document.cookie)</script>"**

2. **Then click enter**



Note how its working and showing the session cookie information

So how this would work is the the user would paste this link to the victim and the work will work .

1. **dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)</script>**

or

2. **http://dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28document.cookie%29%3C/script%3E**