

It is type of attack where the attacker can perform malicious activities on a website by sending some infected code. It is also referred to as XSS attack. This attack is a mix of HTML and XSS, however in case of XSS it could be used to send infected contents or plugins. With XSS, an attacker can have access to session cookies. In the following pictures, it is shown how we can get the session cookie through XSS vulnerability.

The screenshot shows a Kali Linux terminal window with the following commands and output:

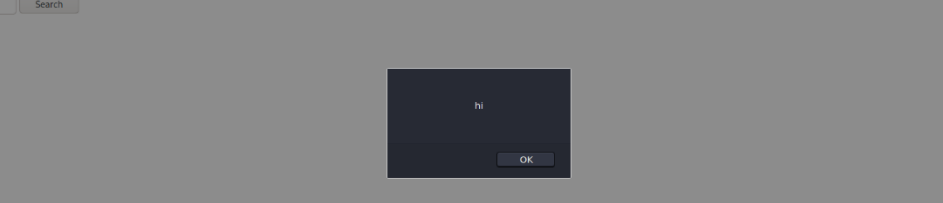
```

kali@kali:~$ git clone https://github.com/Learn-by-doing/ess.git
fatal: destination path 'ess' already exists and is not an empty directory.

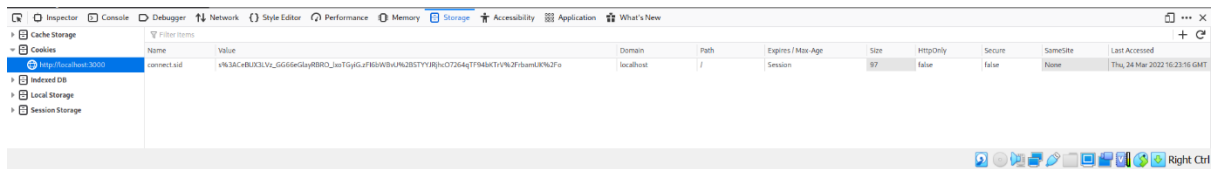
kali@kali:~$ cd ess
kali@kali:~/ess$ sudo su
(sudo) password for kali:
root@kali:~/ess# npm install
up to date, audited 57 packages in 1s
found 0 vulnerabilities

root@kali:~/ess# node server.js
Server listening at localhost:3000
  
```

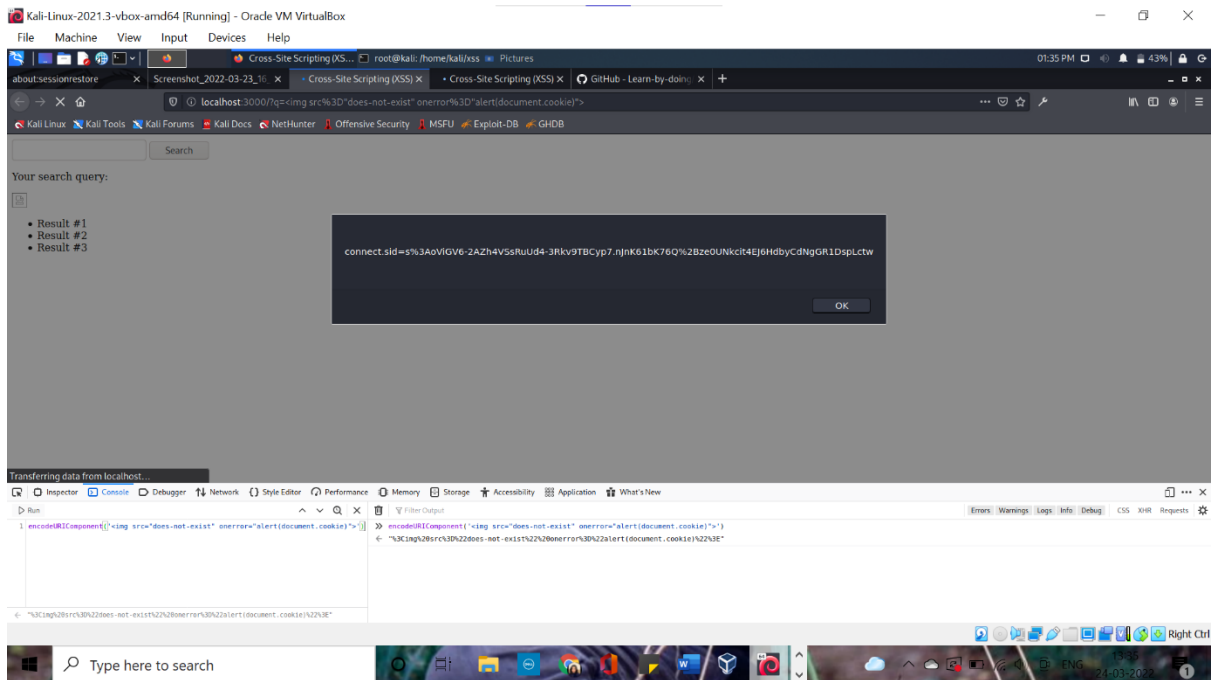
The terminal window is titled "Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox". The top bar shows the time as 01:29 PM and the battery level at 45%.



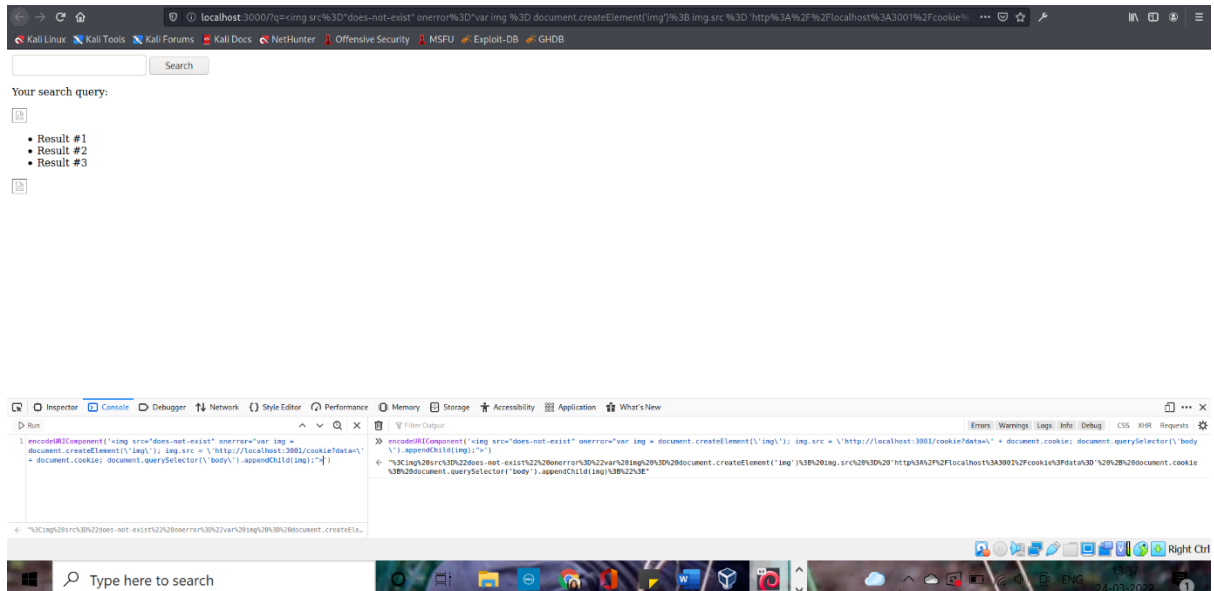
Step 3: We want to access the given localhost session cookie in the storage tab under developer tools.

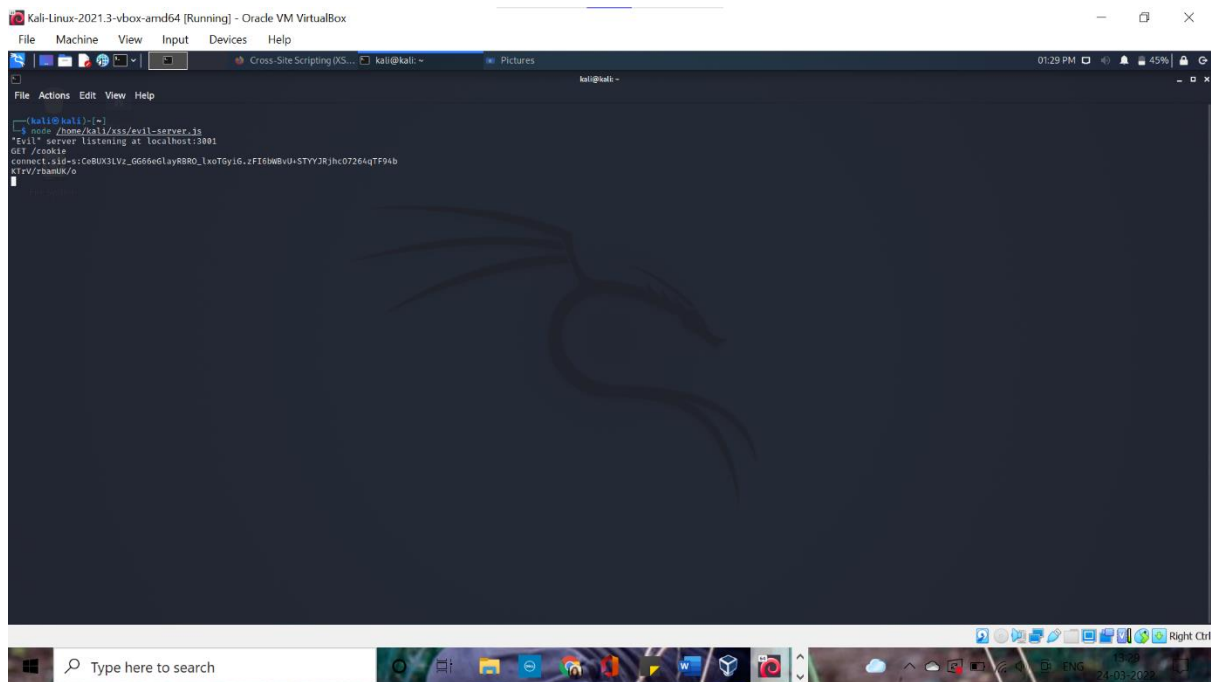


Step 4: In this step, we open console and write commands as shown below and the session cookie content can be seen in popup box.



Step 5: In order to steal the cookies we start another terminal namely evilserver.js. After this, another command is given in the console. Both of the process are depicted in the images below;





Output: We are able to get the session cookies in the terminal.

Referrence:

<https://www.veracode.com/security/xss>

<https://github.com/Learn-by-doing/xss>

https://www.youtube.com/watch?v=cWu_FJUrH5Y