TASK – 6

Burp Suite

1. **BURPSUITE**

Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. burpsuite mostly focusses on the tcp connections along with viewing the packages we will be able to manage the packets also.

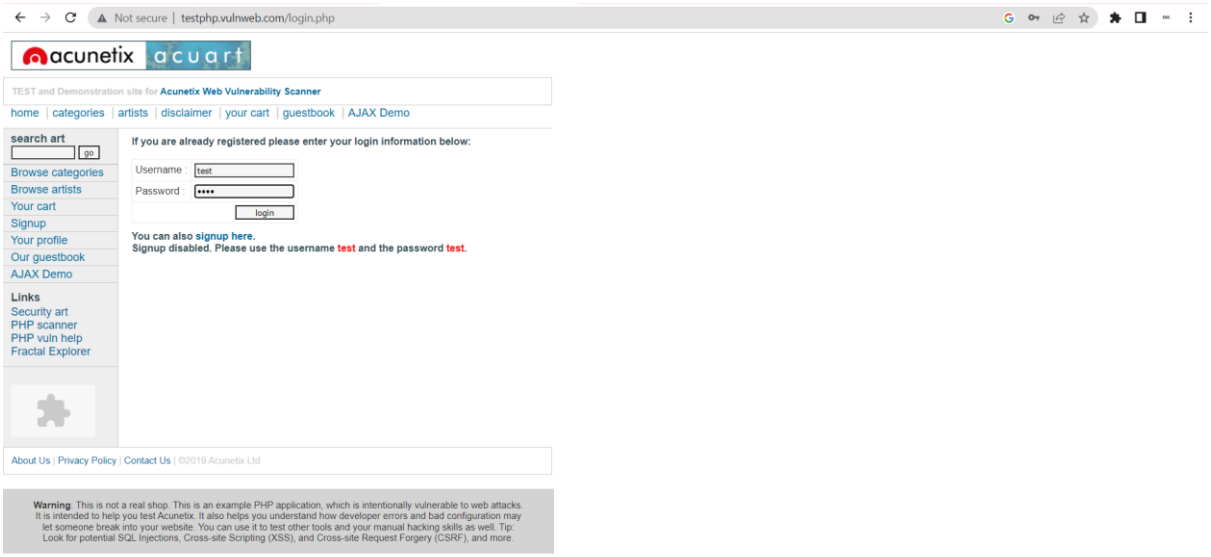
Capturing packets using burpsuites default browser

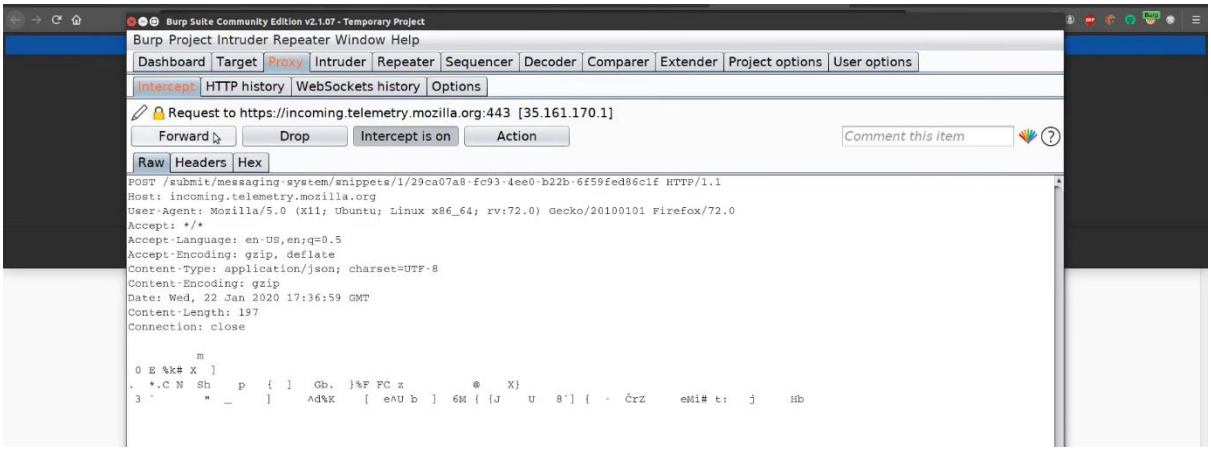
- Open burpsuite
- Goto proxy
- Click open browser to open the burpsuite default browser.
- On the browser we will be opening the vulnweb acuart which is a vulnerable website used to practice web hacking - Turn the intercept on to capture the packets.
- Enter the user name and password on the signup page of the website.
- At the same time the credentials will be visible on the burpsuite window.
- In the proxy window itself you will be able to perform many functions to the packets.
- You will be able to drop and forward packets
- You can also change the values and apply that in the webpage.

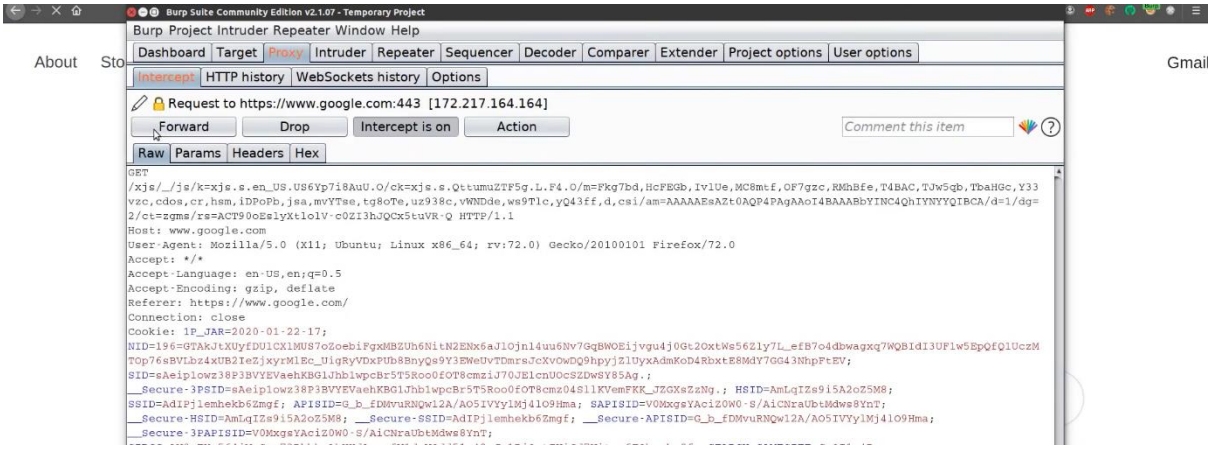
in this form of session hijacking it is only possible to the websites that we are visiting through the default burpsuite web browser to make the same to happen on the default browser you need to set up the proxy in your system.

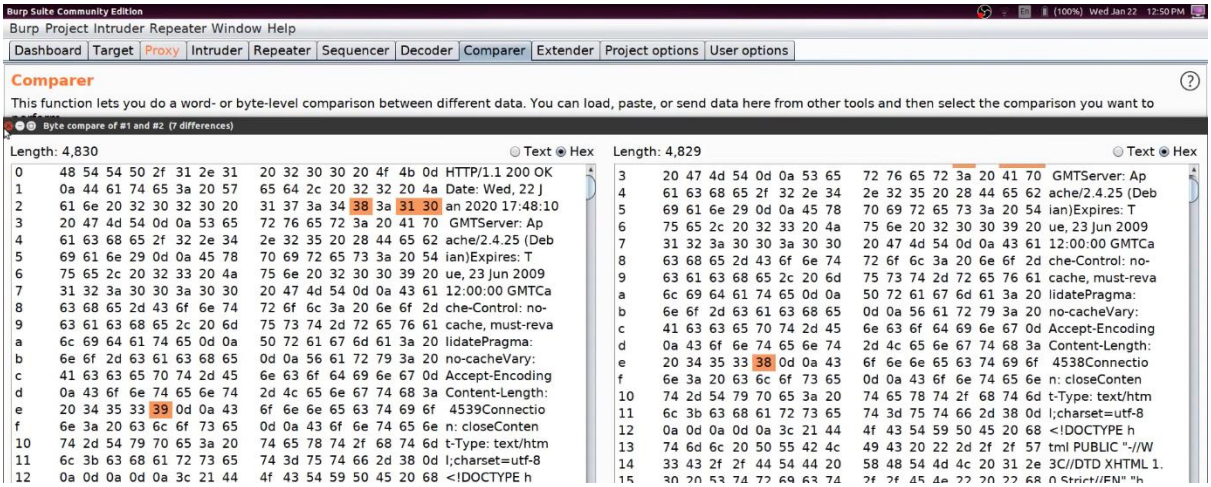
- Go to your systems proxy settings

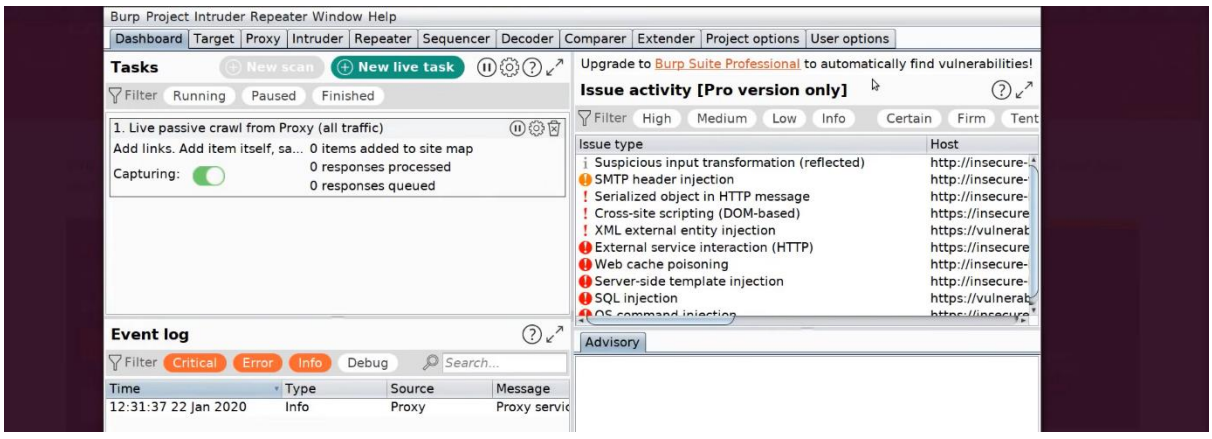
- Ensure that the port is 8080 and ip address is same
- In the burpsuite window go to intercept and turn on
- Now it will start capturing the packets from your default browser also.
- But it will not work with the http and https website as the packets will be encrypted.






Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to https://www.google.com:443 [172.217.164.164]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
GET
/xjs/_/js/k=xjs.s.en_US.US6Yp7i8AuU.O/ck=xjs.s.QttumuZTF5g.L.F4.O/m=Fkg7bd,HcFEGb,IvlUe,MC8mtf,OF7gzc,RMhBfe,T4BAC,TJW5qb,TbaHGc,Y33
vzc,cdos,cr,hsm,iDPoPb,jsa,mvYTse,tg8oTe,uz938c,vWNDde,ws9Tlc,yQ43ff,d,csi/am=AAAAAEsAZt0AQP4PAgAAoI4BAAABbYINC4QhIYNYYQIBCA/d=1/dg=
2/ct=zgms/rs=ACT90oEslyXtlolV-c0Z13hJQCx5tuVR-Q HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.google.com/
Connection: close
Cookie: 1P_JAR=2020-01-22-17;
NID=196=GTAkJtXUyfDUlCXlMUS7oZoebiFgxMBZUh6NitN2ENx6aJ1Ojn14uu6Nv7GqBWOEijvgu4j0Gt2OxtWs56Zly7L_efB7o4dbwagxq7WQBIdI3UF1w5EpQfQ1UczM
TOp76sBVLbz4xUB2IeZjxyrMlEc_UlqRyVDxPUb8BnyQs9Y3EWeUvTDmrsJcXvOwDQ9hpyjZlUyxAdmKoD4RbxtE8MdY7GG43NhpFtEV;
SID=sAeiplowz38P3BVYEVaehKBGlJhb1wpcBr5T5Roo0fOT8cmziJ70JE1cnUOcSZDwSY85Ag.;
__Secure-3PSID=sAeiplowz38P3BVYEVaehKBGlJhb1wpcBr5T5Roo0fOT8cmz04S11KVemFKK_JZGXsZzNg.; HSID=AmLqIZs9i5A2oZ5M8;
SSID=AdIPjlemhekb6Zmgf; APISID=G_b_fDMvuRNQw12A/AO5IVYylMj4lO9Hma; SAPISID=V0MxgsYAciZ0W0-S/AiCNraUbtMdws8YnT;
__Secure-HSID=AmLqIZs9i5A2oZ5M8; __Secure-SSID=AdIPjlemhekb6Zmgf; __Secure-APISID=G_b_fDMvuRNQw12A/AO5IVYylMj4lO9Hma;
__Secure-3PAPISID=V0MxgsYAciZ0W0-S/AiCNraUbtMdws8YnT;


Burp Suite Community Edition
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Comparer
This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to
Byte compare of #1 and #2 (7 differences)
Length: 4,830
Text Hex
Length: 4,829
Text Hex


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, sa... 0 items added to site map
Capturing:
0 responses processed
0 responses queued
Upgrade to Burp Suite Professional to automatically find vulnerabilities!
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Tent
Issue type
Host
Suspicious input transformation (reflected)
SMTP header injection
Serialized object in HTTP message
Cross-site scripting (DOM-based)
XML external entity injection
External service interaction (HTTP)
Web cache poisoning
Server-side template injection
SQL injection
Event log
Filter Critical Error Info Debug
Search...
Time
Type
Source
Message
12:31:37 22 Jan 2020
Info
Proxy
Advisory

Burp Suite is a Java application that can be used to secure or penetrate web applications. The suite consists of different tools, such as a proxy server, a web spider, intruder and repeater.