CSE3502 - Information Security Management

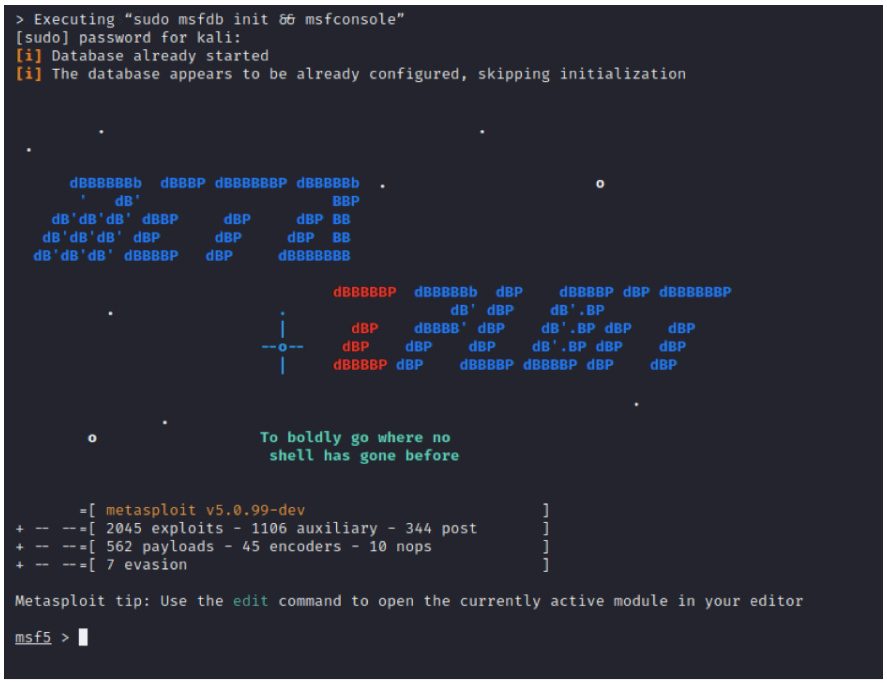
Lab Assignment 6

Metasploit and BurpSuite (Penetration Testing - example.com and Local Chat Application)

SANJIT KUMAR
18BCE0715
DR. ANILKUMAR KAKELLI
LAB - L21 + L22

Metasploit

Comment: Pen Testing Tool that allows you to test and maintain systems in a network. The following commands show the steps to check the local files and exploit vulnerabilities.



Show All

```
msf5 > show all

Encoders
========

   #   Name                          Disclosure Date  Rank    Check  Description
   -   ----                          ---------------  ----    -----  -----------
   0   cmd/brace                                      manual  No     Bash Brace Expansion Command Encoder
   1   cmd/echo                                       manual  No     Echo Command Encoder
   2   cmd/generic_sh                                 manual  No     Generic Shell Variable Substitution Command Encoder
   3   cmd/ifs                                        manual  No     Bourne ${IFS} Substitution Command Encoder
   4   cmd/perl                                       manual  No     Perl Command Encoder
   5   cmd/powershell_base64                          manual  No     Powershell Base64 Command Encoder
   6   cmd/printf_php_mq                              manual  No     printf(1) via PHP magic_quotes Utility Command Encoder
   7   generic/eicar                                  manual  No     The EICAR Encoder
   8   generic/none                                   manual  No     The "none" Encoder
   9   mipsbe/byte_xori                               manual  No     Byte XORi Encoder
   10  mipsbe/longxor                                 manual  No     XOR Encoder
   11  mipsle/byte_xori                               manual  No     Byte XORi Encoder
   12  mipsle/longxor                                 manual  No     XOR Encoder
   13  php/base64                                     manual  No     PHP Base64 Encoder
   14  ppc/longxor                                    manual  No     PPC LongXOR Encoder
   15  ppc/longxor_tag                                manual  No     PPC LongXOR Encoder
   16  ruby/base64                                    manual  No     Ruby Base64 Encoder
   17  sparc/longxor_tag                              manual  No     SPARC DWORD XOR Encoder
   18  x64/xor                                        manual  No     XOR Encoder
   19  x64/xor_context                                manual  No     Hostname-based Context Keyed Payload Encoder
   20  x64/xor_dynamic                                manual  No     Dynamic key XOR Encoder
   21  x64/zutto_dekiru                               manual  No     Zutto Dekiru
   22  x86/add_sub                                    manual  No     Add/Sub Encoder
   23  x86/alpha_mixed                                manual  No     Alpha2 Alphanumeric Mixedcase Encoder
   24  x86/alpha_upper                                manual  No     Alpha2 Alphanumeric Uppercase Encoder
   25  x86/avoid_underscore_tolower                   manual  No     Avoid underscore/tolower
   26  x86/avoid_utf8_tolower                         manual  No     Avoid UTF8/tolower
   27  x86/bloxor                                     manual  No     BloXor - A Metamorphic Block Based XOR Encoder
   28  x86/bmp_polyglot                               manual  No     BMP Polyglot
   29  x86/call4_dword_xor                            manual  No     Call+4 Dword XOR Encoder
   30  x86/context_cpuid                              manual  No     CPUID-based Context Keyed Payload Encoder
   31  x86/context_stat                               manual  No     stat(2)-based Context Keyed Payload Encoder
   32  x86/context_time                               manual  No     time(2)-based Context Keyed Payload Encoder
   33  x86/countdown                                  manual  No     Single-byte XOR Countdown Encoder
```

Show exploits

```
File  Actions  Edit  View  Help

   1882  windows/misc/poppeeper_uidl                                          2009-02-27       manual  No     POP Peeper v3.4 UIDL Buffer Overflow
   1883  windows/misc/realtek_playlist                                        2008-12-16       manual  No     Realtek Media Player Playlist Buffer Overflow
   1884  windows/misc/sap_2005_license                                        2009-08-01       manual  No     SAP Business One License Manager 2005 Buffer Overflow
   1885  windows/misc/sap_netweaver_dispatcher                                2012-05-08       manual  No     SAP NetWeaver Dispatcher DiagTraceR3Info Buffer Overflow
   1886  windows/misc/shixxnote_font                                          2004-10-04       manual  No     ShixxNOTE 6.net Font Field Overflow
   1887  windows/misc/solidworks_workgroup_pdmwservice_file_write             2014-02-22       manual  Yes    SolidWorks Workgroup PDM 2014 pdmwService.exe Arbitrary File Write
   1888  windows/misc/splayer_content_type                                    2011-05-04       manual  No     SPlayer 3.7 Content-Type Buffer Overflow
   1889  windows/misc/stream_down_bof                                         2011-12-27       manual  No     CoCSoft StreamDown 6.8.0 Buffer Overflow
   1890  windows/misc/talkative_response                                      2009-03-17       manual  No     Talkative IRC v0.4.4.16 Response Buffer Overflow
   1891  windows/misc/tiny_identd_overflow                                    2007-05-14       manual  No     TinyIdentD 2.2 Stack Buffer Overflow
   1892  windows/misc/trendmicro_cmdprocessor_addtask                         2011-12-07       manual  No     TrendMicro Control Manger CmdProcessor.exe Stack Buffer Overflow
   1893  windows/misc/ufo_ai                                                  2009-10-28       manual  No     UFO: Alien Invasion IRC Client Buffer Overflow
   1894  windows/misc/veeam_one_agent_deserialization                         2020-04-15       manual  Yes    Veeam ONE Agent .NET Deserialization
   1895  windows/misc/vmhgfs_webdav_dll_sideload                              2016-08-05       manual  No     DLL Side Loading Vulnerability in VMware Host Guest Client Redirector
   1896  windows/misc/webdav_delivery                                         1999-01-01       manual  No     Serve DLL via webdav server
   1897  windows/misc/windows_rsh                                             2007-07-24       manual  No     Windows RSH Daemon Buffer Overflow
   1898  windows/misc/wireshark_lua                                           2011-07-18       manual  No     Wireshark console.lua Pre-Loading Script Execution
   1899  windows/misc/wireshark_packet_dect                                   2011-04-18       manual  No     Wireshark packet-dect.c Stack Buffer Overflow
   1900  windows/mmsp/ms10_025_wmss_connect_funnel                            2010-04-13       manual  No     Windows Media Services ConnectFunnel Stack Buffer Overflow
   1901  windows/motorola/timbuktu_fileupload                                 2008-05-10       manual  No     Timbuktu Pro Directory Traversal/File Upload
   1902  windows/mssql/lyris_listmanager_weak_pass                            2005-12-08       manual  No     Lyris ListManager MSDE Weak sa Password
   1903  windows/mssql/ms02_039_slammer                                       2002-07-24       manual  Yes    MS02-039 Microsoft SQL Server Resolution Overflow
   1904  windows/mssql/ms02_056_hello                                         2002-08-05       manual  Yes    MS02-056 Microsoft SQL Server Hello Overflow
   1905  windows/mssql/ms09_004_sp_replwritetovarbin                          2008-12-09       manual  Yes    MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory Corruption
   1906  windows/mssql/ms09_004_sp_replwritetovarbin_sqli                     2008-12-09       manual  Yes    MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory Corruption via SQL Inject
ion
   1907  windows/mssql/mssql_clr_payload                                      1999-01-01       manual  Yes    Microsoft SQL Server Clr Stored Procedure Payload Execution
   1908  windows/mssql/mssql_linkcrawler                                      2000-01-01       manual  No     Microsoft SQL Server Database Link Crawling Command Execution
   1909  windows/mssql/mssql_payload                                          2000-05-30       manual  Yes    Microsoft SQL Server Payload Execution
   1910  windows/mssql/mssql_payload_sqli                                     2000-05-30       manual  No     Microsoft SQL Server Payload Execution via SQL Injection
   1911  windows/mysql/mysql_mof                                              2012-12-01       manual  Yes    Oracle MySQL for Microsoft Windows MOF Execution
   1912  windows/mysql/mysql_start_up                                         2012-12-01       manual  Yes    Oracle MySQL for Microsoft Windows FILE Privilege Abuse
   1913  windows/mysql/mysql_yassl_hello                                      2008-01-04       manual  No     MySQL yaSSL SSL Hello Message Buffer Overflow
   1914  windows/mysql/scrutinizer_upload_exec                                2012-07-27       manual  Yes    Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential
   1915  windows/nfs/xlink_nfsd                                               2006-11-06       manual  No     Omni-NFS Server Buffer Overflow
   1916  windows/nntp/ms05_030_nntp                                           2005-06-14       manual  No     MS05-030 Microsoft Outlook Express NNTP Response Parsing Buffer Overflow
   1917  windows/novell/file_reporter_fsfui_upload                            2012-11-16       manual  No     NFR Agent FSFUI Record File Upload RCE
   1918  windows/novell/groupwisemessenger_client                             2008-07-02       manual  No     Novell GroupWise Messenger Client Buffer Overflow
   1919  windows/novell/netiq_pum_eval                                        2012-11-15       manual  Yes    NetIQ Privileged User Manager 2.3.1 ldapagmt_eval() Remote Perl Code Execution
   1920  windows/novell/nmap_stor                                             2006-12-23       manual  No     Novell NetMail NMAP STOR Buffer Overflow
   1921  windows/novell/zenworks_desktop_agent                                2005-05-19       manual  No     Novell ZENworks 6.5 Desktop/Server Management Overflow
```

Search IOS

```
msf5 > search ios

Matching Modules
================

   #   Name                                                        Disclosure Date  Rank       Check  Description
   -   ----                                                        ---------------  ----       -----  -----------
   0   auxiliary/admin/netbios/netbios_spoof                                        normal     No     NetBIOS Response Brute Force Spoof (Direct)
   1   auxiliary/admin/networking/cisco_config                                      normal     No     Cisco Configuration Importer
   2   auxiliary/dos/apple_ios/webkit_backdrop_filter_blur         2018-09-15       normal     No     iOS Safari Denial of Service with CSS
   3   auxiliary/dos/cisco/ios_http_percentpercent                 2000-04-26       normal     No     Cisco IOS HTTP GET /%% Request Denial of Service
   4   auxiliary/dos/cisco/ios_telnet_rocem                        2017-03-17       normal     No     Cisco IOS Telnet Denial of Service
   5   auxiliary/dos/smb/smb_loris                                 2017-06-29       normal     No     SMBLoris NBSS Denial of Service
   6   auxiliary/gather/apple_safari_ftp_url_cookie_theft          2015-04-08       normal     No     Apple OSX/iOS/Windows Safari Non-HTTPOnly Cookie Theft
   7   auxiliary/scanner/http/cisco_ios_auth_bypass                2001-06-27       normal     No     Cisco IOS HTTP Unauthorized Administrative Access
   8   auxiliary/scanner/http/ntlm_info_enumeration                                 normal     No     Host Information Enumeration via NTLM Authentication
   9   auxiliary/scanner/ike/cisco_ike_benigncertain               2016-09-29       normal     No     Cisco IKE Information Disclosure
   10  auxiliary/scanner/netbios/nbname                                             normal     No     NetBIOS Information Discovery
   11  auxiliary/scanner/snmp/cisco_config_tftp                                     normal     No     Cisco IOS SNMP Configuration Grabber (TFTP)
   12  auxiliary/scanner/snmp/cisco_upload_file                                     normal     No     Cisco IOS SNMP File Upload (TFTP)
   13  auxiliary/scanner/ssh/fortinet_backdoor                     2016-01-09       normal     No     Fortinet SSH Backdoor Scanner
   14  auxiliary/server/netbios_spoof_nat                          2016-06-14       normal     No     NetBIOS Response "BadTunnel" Brute Force Spoof (NAT Tunnel)
   15  auxiliary/server/wpad                                                        normal     No     WPAD.dat File Server
   16  auxiliary/spoof/llmnr/llmnr_response                                         normal     No     LLMNR Spoofer
   17  auxiliary/spoof/nbns/nbns_response                                           normal     No     NetBIOS Name Service Spoofer
   18  exploit/apple_ios/browser/safari_libtiff                    2006-08-01       good       No     Apple iOS MobileSafari LibTIFF Buffer Overflow
   19  exploit/apple_ios/browser/webkit_createthis                 2018-03-15       manual     No     Safari Webkit Proxy Object Type Confusion
   20  exploit/apple_ios/browser/webkit_trident                    2016-08-25       manual     No     WebKit not_number defineProperties UAF
   21  exploit/apple_ios/email/mobilemail_libtiff                  2006-08-01       good       No     Apple iOS MobileMail LibTIFF Buffer Overflow
   22  exploit/apple_ios/ssh/cydia_default_ssh                     2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
   23  exploit/linux/http/gpsd_format_string                       2005-05-25       average    No     Berlios GPSD Format String Vulnerability
   24  exploit/linux/http/nagios_xi_authenticated_rce              2019-07-29       excellent  Yes    Nagios XI Authenticated Remote Command Execution
   25  exploit/linux/http/nagios_xi_chained_rce                    2016-03-06       excellent  Yes    Nagios XI Chained Remote Code Execution
   26  exploit/linux/http/nagios_xi_chained_rce_2_electric_boogaloo  2018-04-17       manual     Yes    Nagios XI Chained Remote Code Execution
   27  exploit/linux/http/nagios_xi_magpie_debug                   2018-11-14       excellent  Yes    Nagios XI Magpie_debug.php Root Remote Code Execution
   28  exploit/linux/local/ptrace_traceme_pkexec_helper            2019-07-04       excellent  Yes    Linux Polkit pkexec helper PTRACE_TRACEME local root exploit
   29  exploit/linux/misc/nagios_nrpe_arguments                    2013-02-21       excellent  Yes    Nagios Remote Plugin Executor Arbitrary Command Execution
   30  exploit/multi/http/horde_form_file_upload                   2019-03-24       excellent  No     Horde Form File Upload Vulnerability
   31  exploit/unix/webapp/nagios3_history_cgi                     2012-12-09       great      Yes    Nagios3 history.cgi Host Command Execution
   32  exploit/unix/webapp/nagios3_statuswml_ping                  2009-06-22       excellent  No     Nagios3 statuswml.cgi Ping Command Execution
   33  exploit/unix/webapp/nagios_graph_explorer                   2012-11-30       excellent  Yes    Nagios XI Network Monitor Graph Explorer Component Command Injection
```

Use Exploit

```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[-] example.com:21 - Exploit failed: An exploitation error occurred.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > rn
[-] Unknown command: rn.
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > run

[-] example.com:21 - Exploit failed: An exploitation error occurred.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > expoit
[-] Unknown command: expoit.
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[-] example.com:21 - Exploit failed: An exploitation error occurred.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > run

[-] example.com:21 - Exploit failed: An exploitation error occurred.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/proftpd_133c_backdoor) >
```

Set rhost and exploit

```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST example.com
RHOST ⇒ example.com
msf5 exploit(unix/ftp/proftpd_133c_backdoor) >
```

```
msf5 > use exploit/unix/ftp/proftpd_133c_backdoor
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(unix/ftp/proftpd_133c_backdoor) >
```

BurpSuite

Burp Suite is an integrated platform for attacking web applications. It contains a variety of tools with numerous interfaces between them designed to facilitate and speed up the process of attacking an application. All of the tools share the same framework for handling and displaying HTTP messages, persistence, authentication, proxies, logging, alerting and extensibility.

Penetration Testing Example

Link - https://portswigger.net/burp

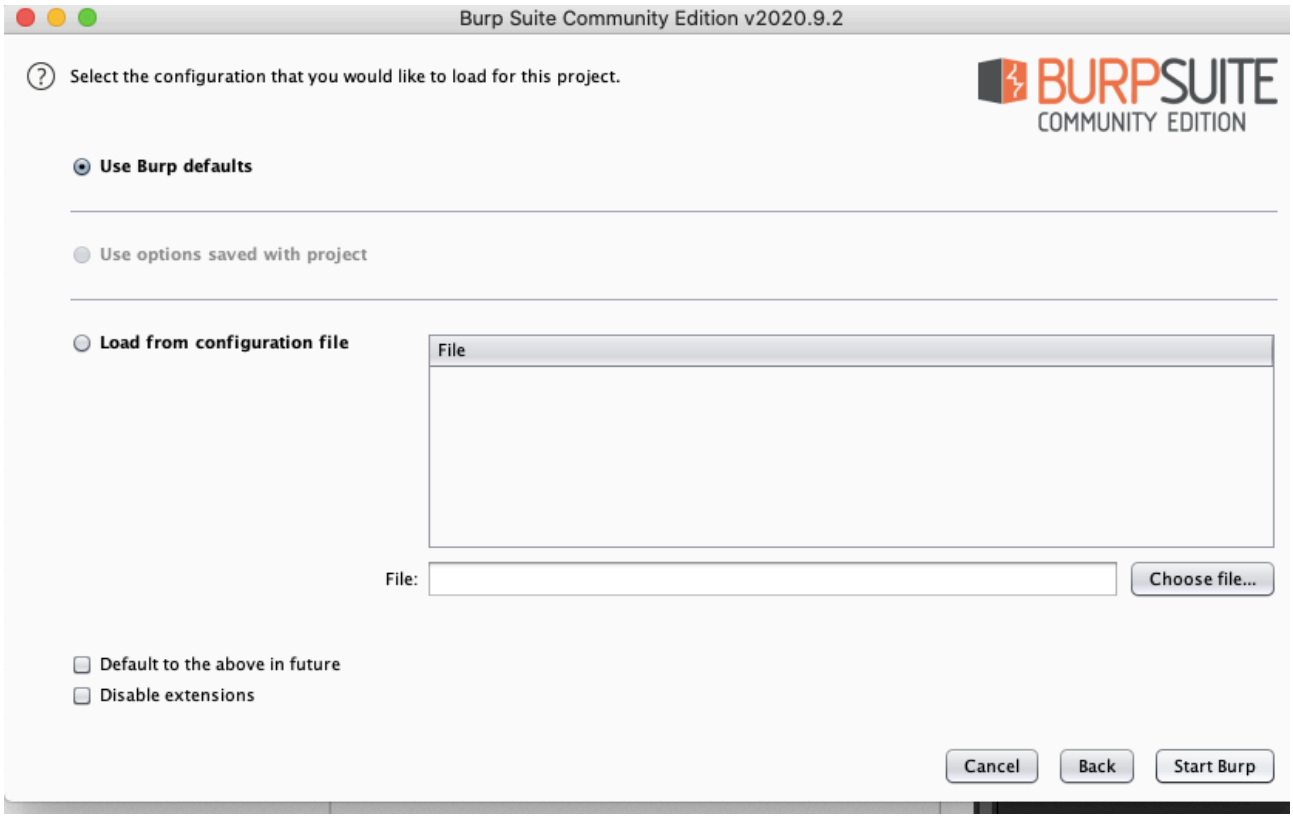
Installation and Start New Project on Mac OSX 10.15

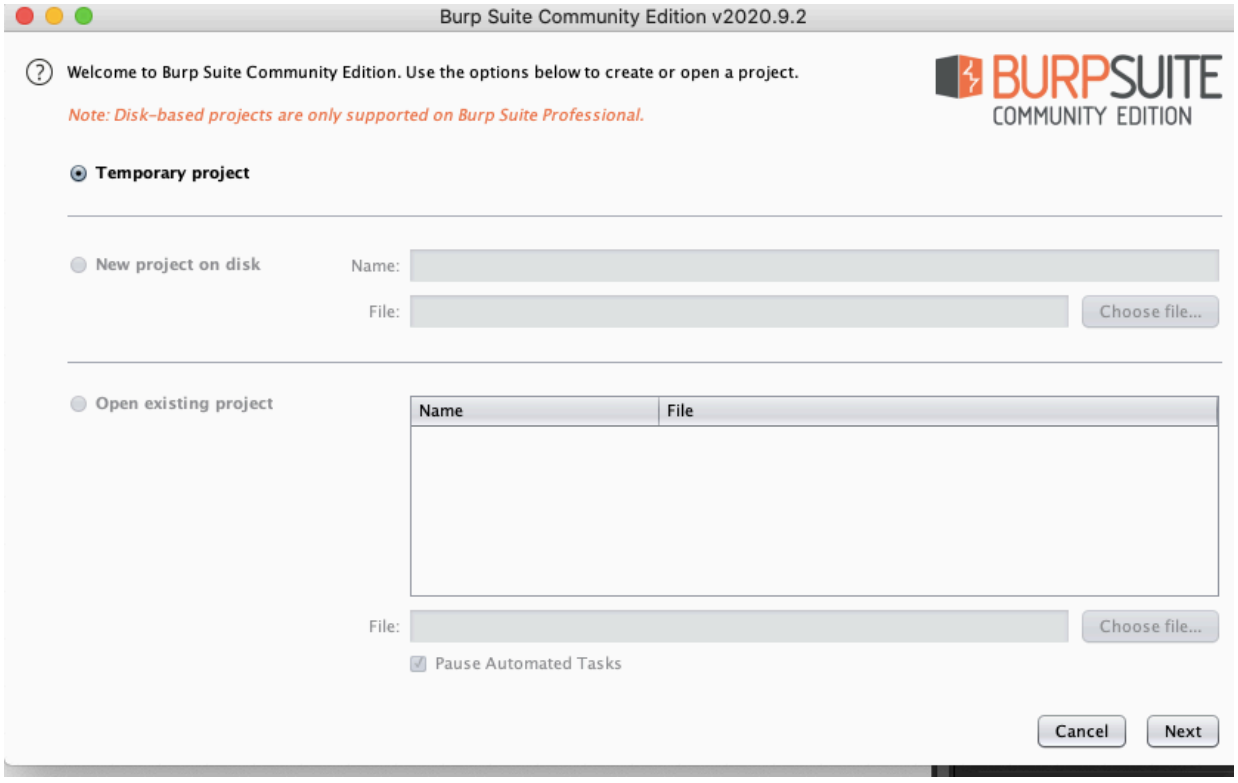
Note: Like Rishi demonstrated interception of packets and attack vector to targets on the internet, in this experiment I have used my previous semester (under you sir) j component project encrypted chat application to demonstrate how to pen test the messages.

Objective: The objective is to compare penetration attacks between 2 applications I have developed previously.

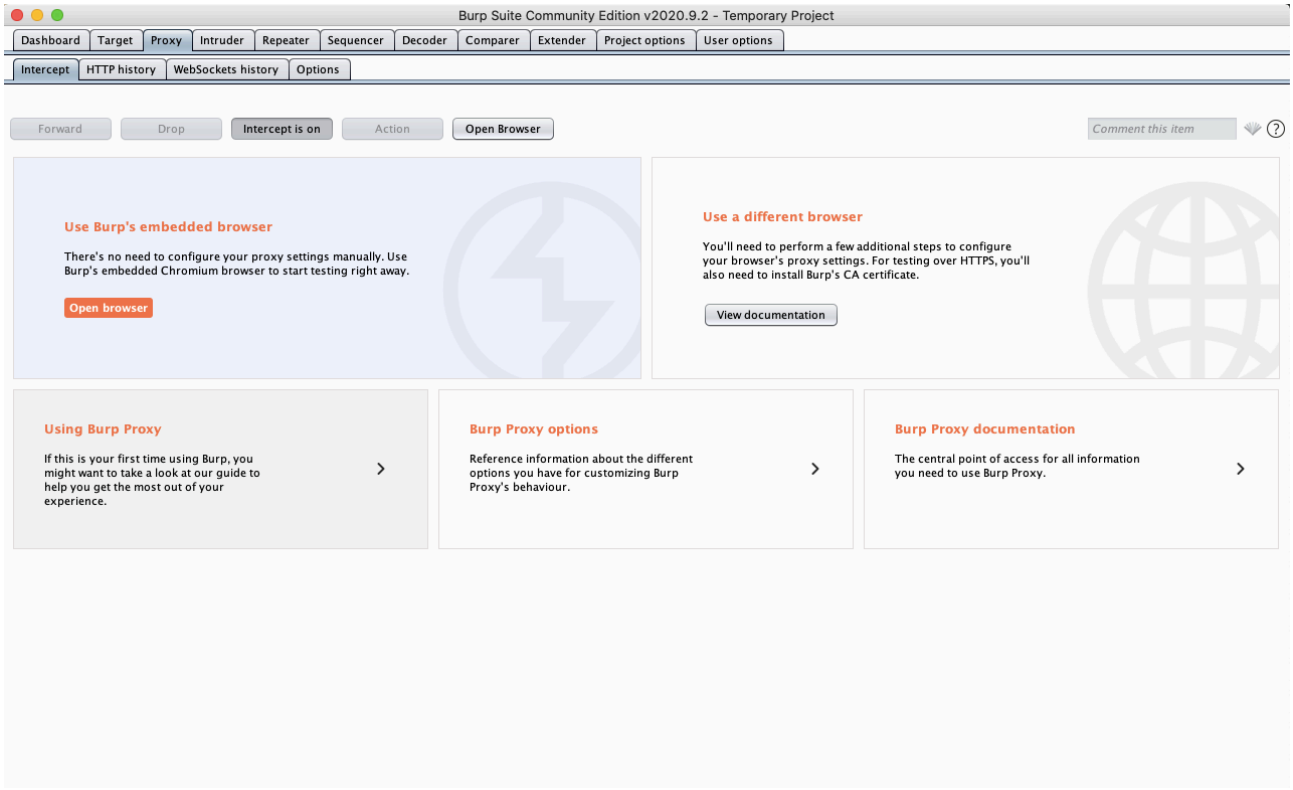
1. Non-Encrypted Chat Application created with node.js and ejs templating engine (attack succeeds)
2. Encrypted Chat Application created with vue.js and node.js - Encrypted with RSA Cryptographic Public Key Algorithm (attack fails due to encryption)

I have already previously installed the CA certificate for https connections.

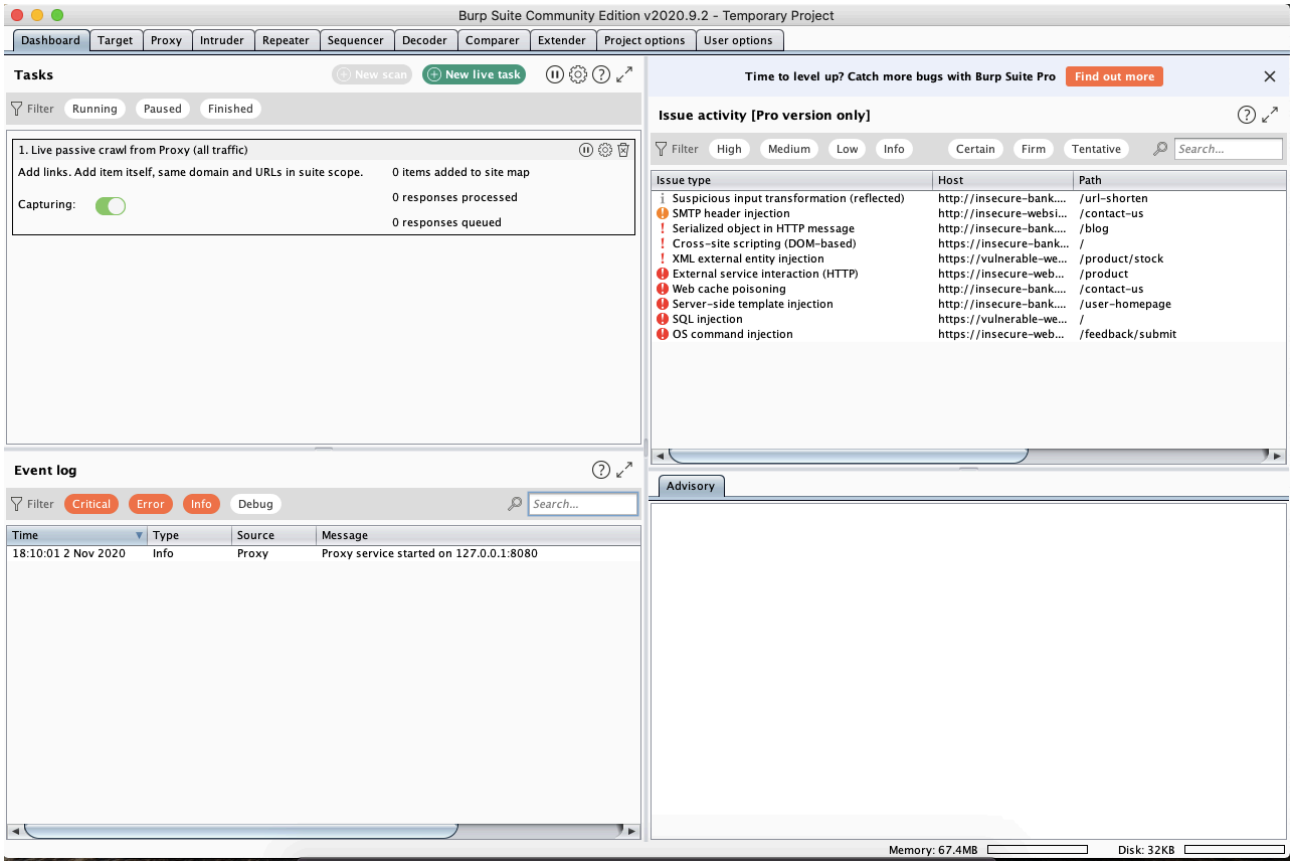

Burp Suite Community Edition v2020.9.2
Select the configuration that you would like to load for this project.
BURPSUITE
COMMUNITY EDITION
Use Burp defaults
Use options saved with project
Load from configuration file
File
File:
Choose file...
Default to the above in future
Disable extensions
Cancel
Back
Start Burp


Burp Suite Community Edition v2020.9.2
Welcome to Burp Suite Community Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
BURPSUITE
COMMUNITY EDITION
Temporary project
New project on disk
Name:
File:
Choose file...
Open existing project
Name
File
File:
Choose file...
Pause Automated Tasks
Cancel
Next

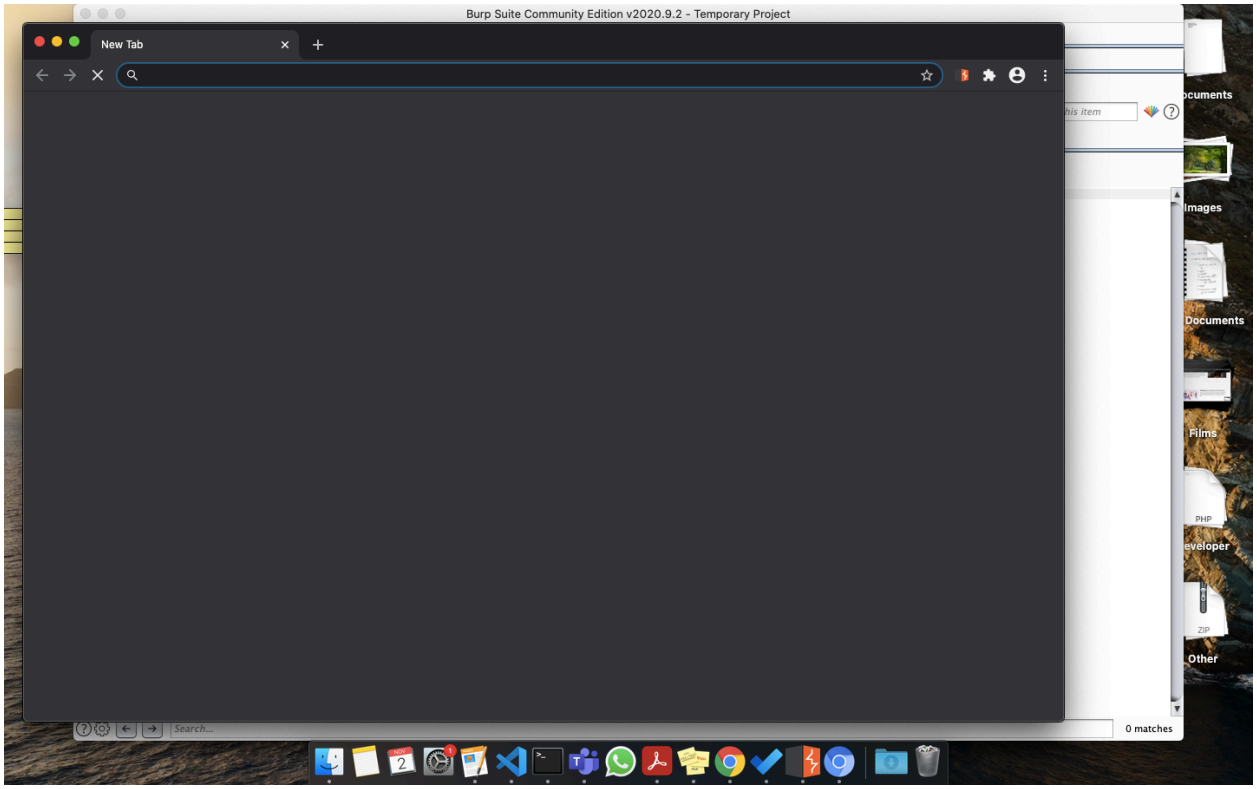
Navigate to Proxy Tab on Menubar



Turn on Capturing of packets and check issue activity



On clicking open browser button -> Chromium Browser Opens By default
This browser auto sets the targets and only receives packets that BurpSuite first intercepts



Pen-testing the Non end to end encrypted Chat Application

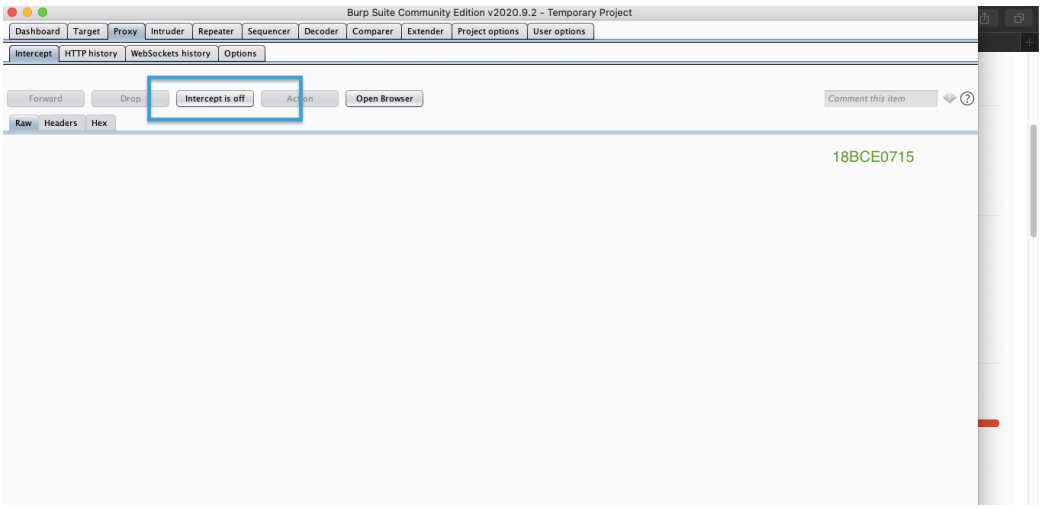
Visit this for live deployed the NON encrypted chat application (deployed as a personal project)- **https://sanjit-chat-app.herokuapp.com/**

Visit this for End to End encrypted chat application (deployed as part of last sem's J component project)

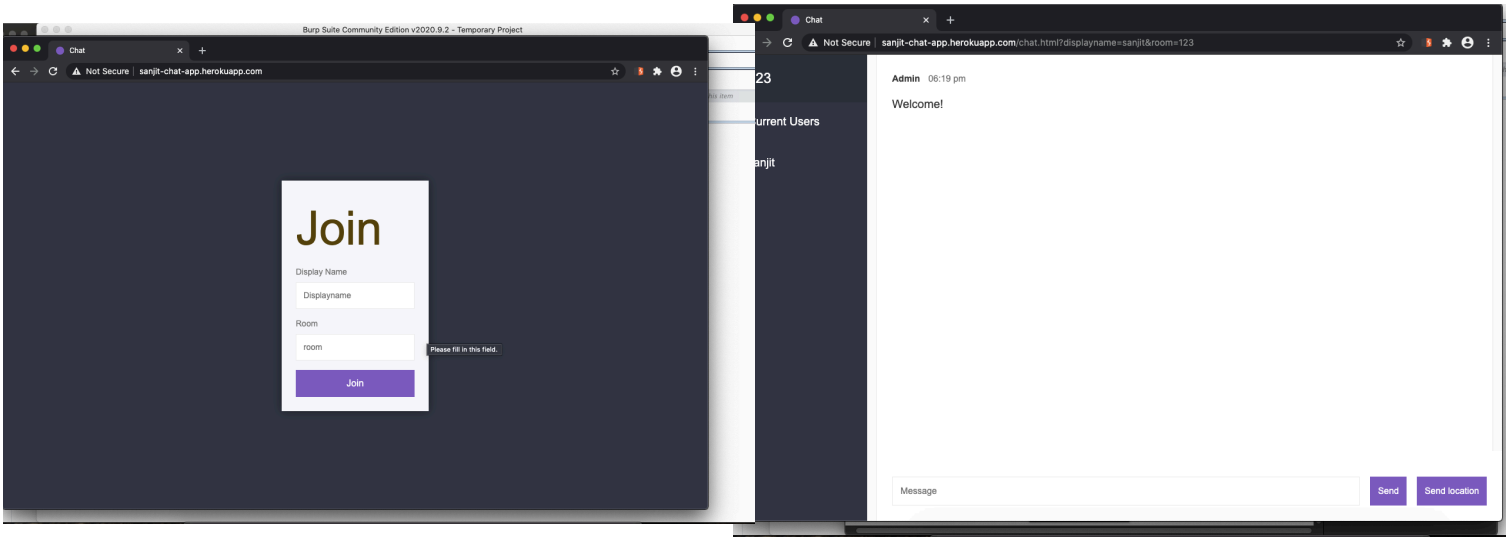
- **https://end-to-end-encrypted-chat-app.herokuapp.com/**

For Non Encrypted chat application

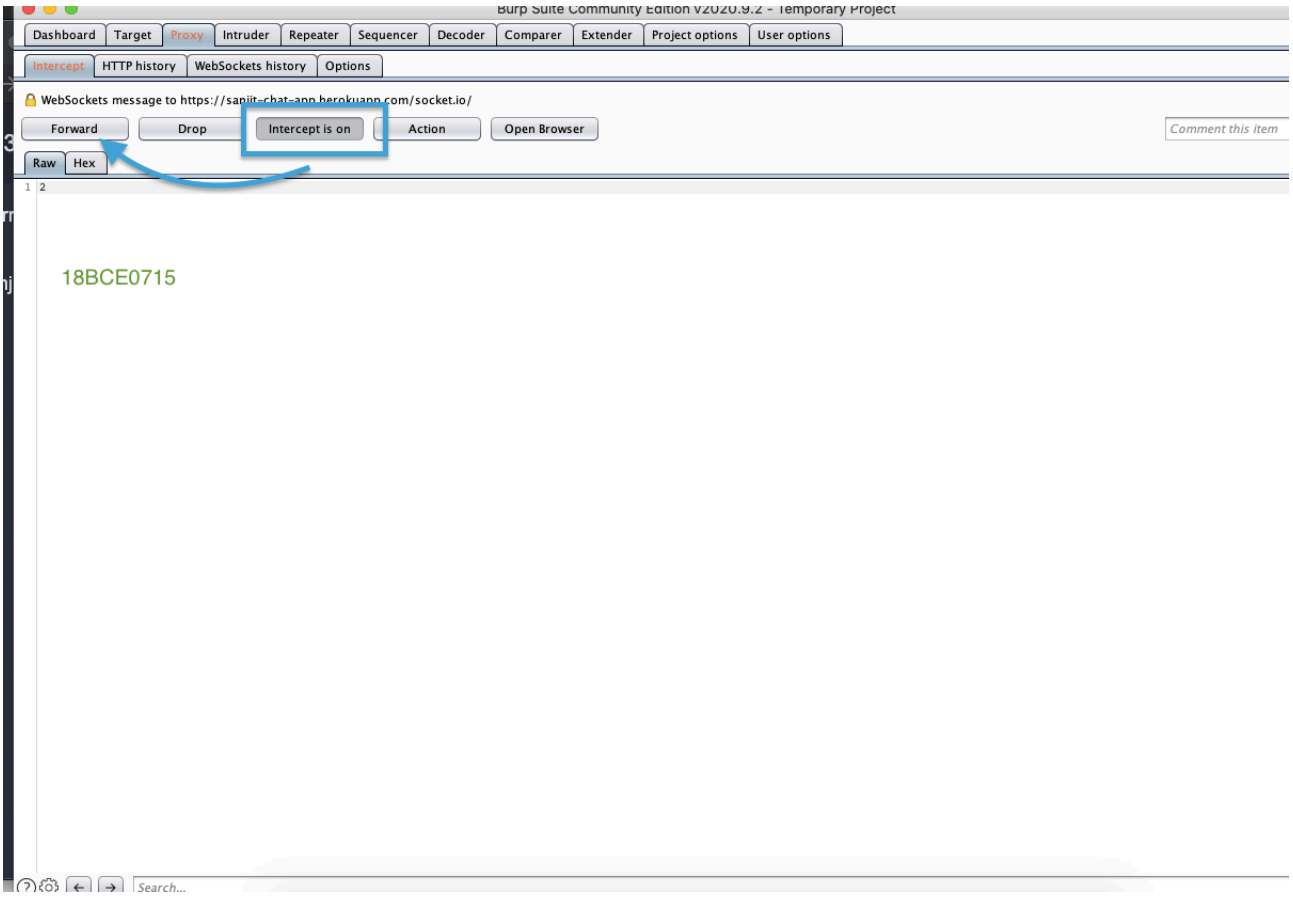
1. First turn intercept off on the Burp Suite to let the page load completely



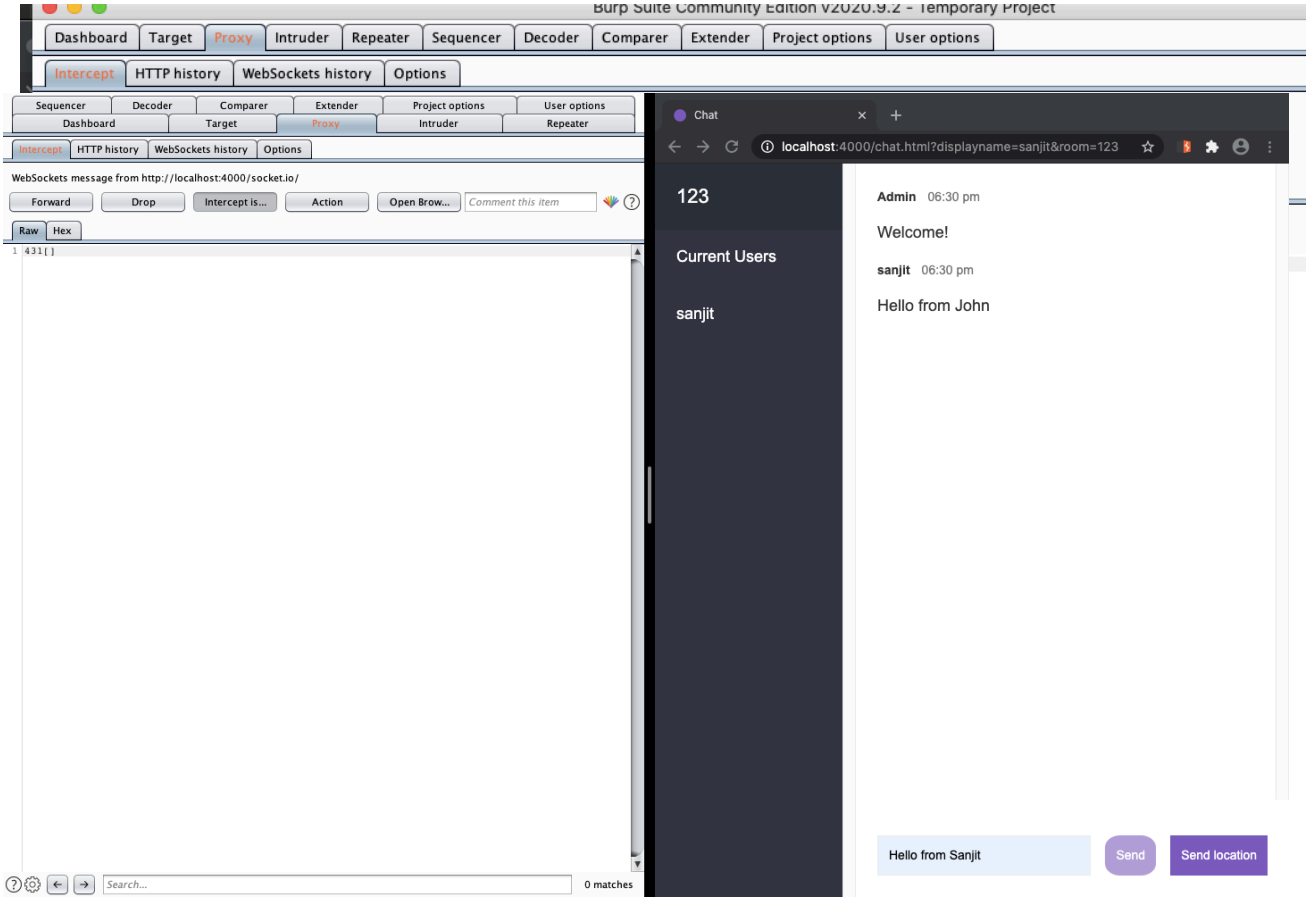
2. Now the page loads completely on BurpSuite Chromium Browser. Enter a chat room



3. Now turn on intercept and click forward

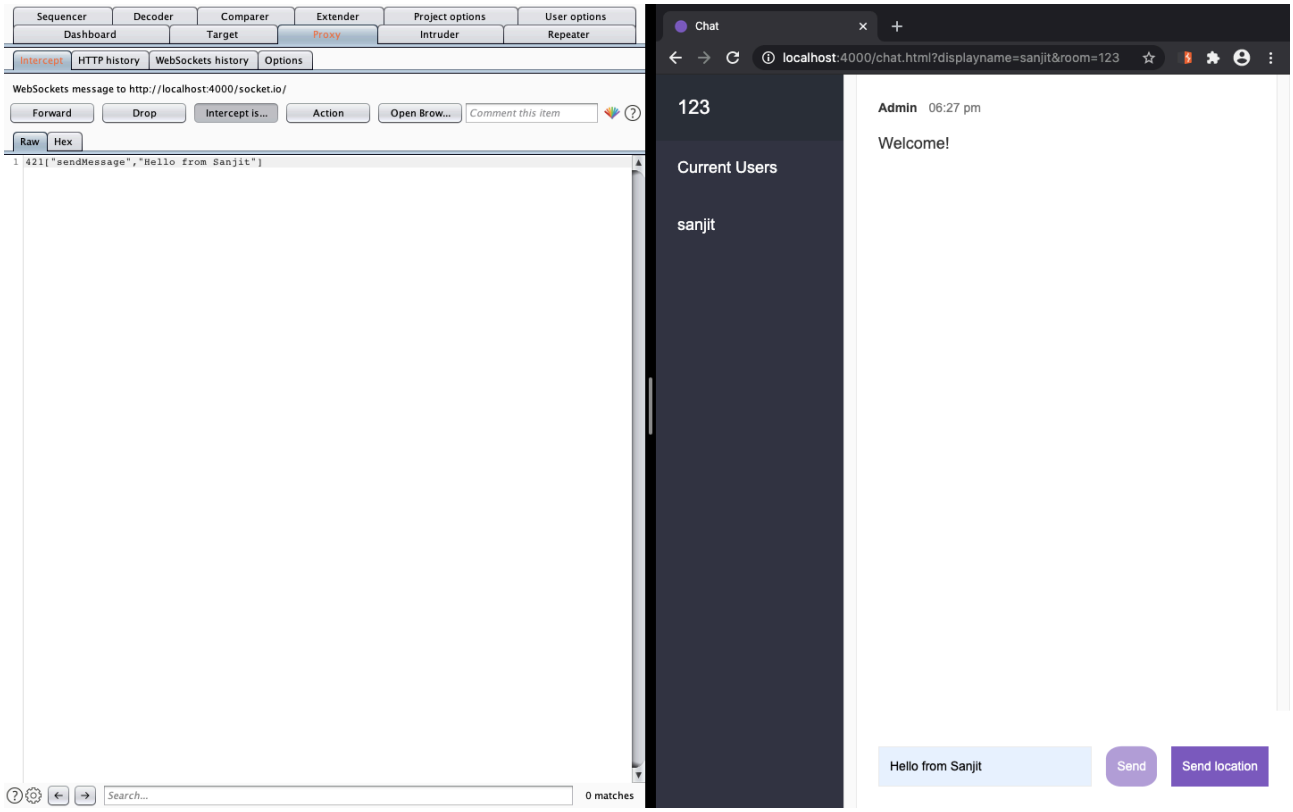


4. HTTP Packets are now intercepted in the browser and information is visible

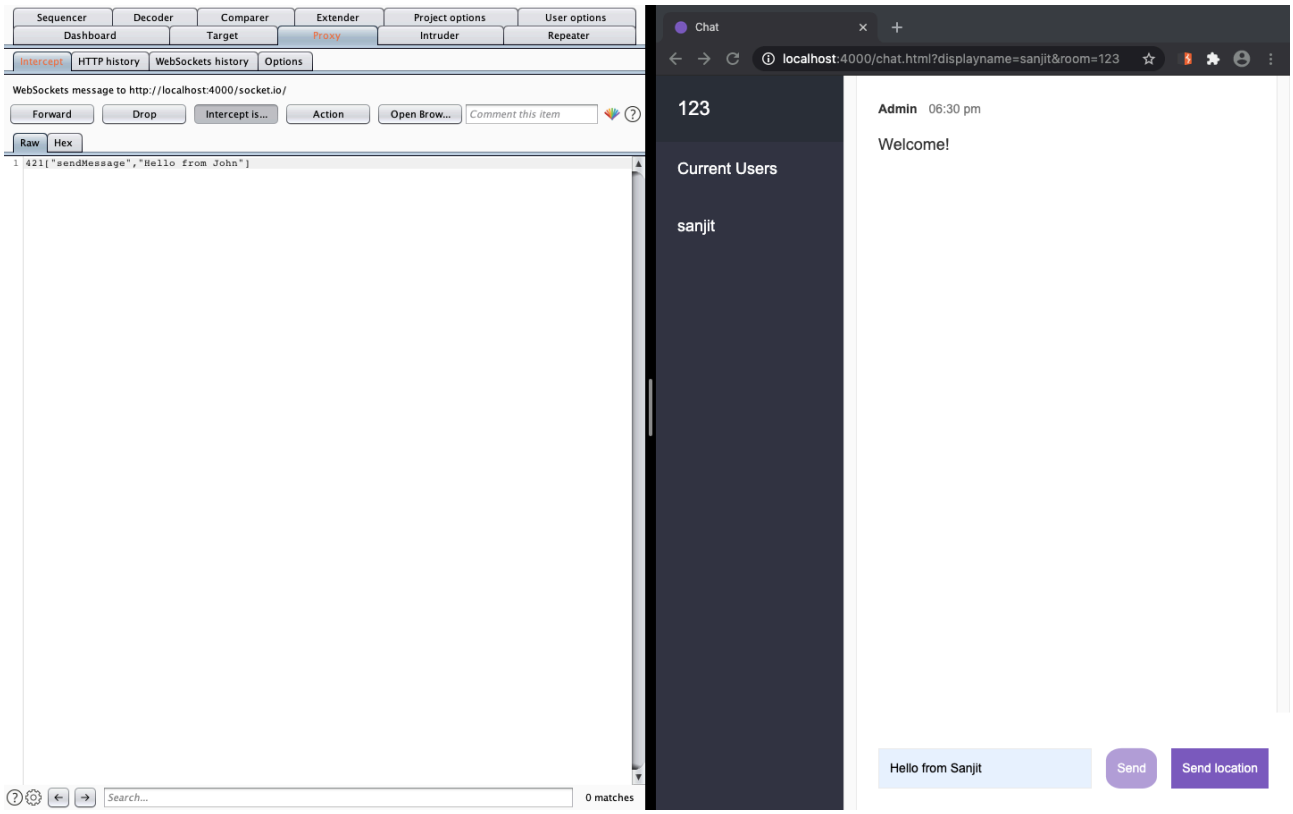


5. Go back to the browser and send a message. After that go to burp suit and click forward.

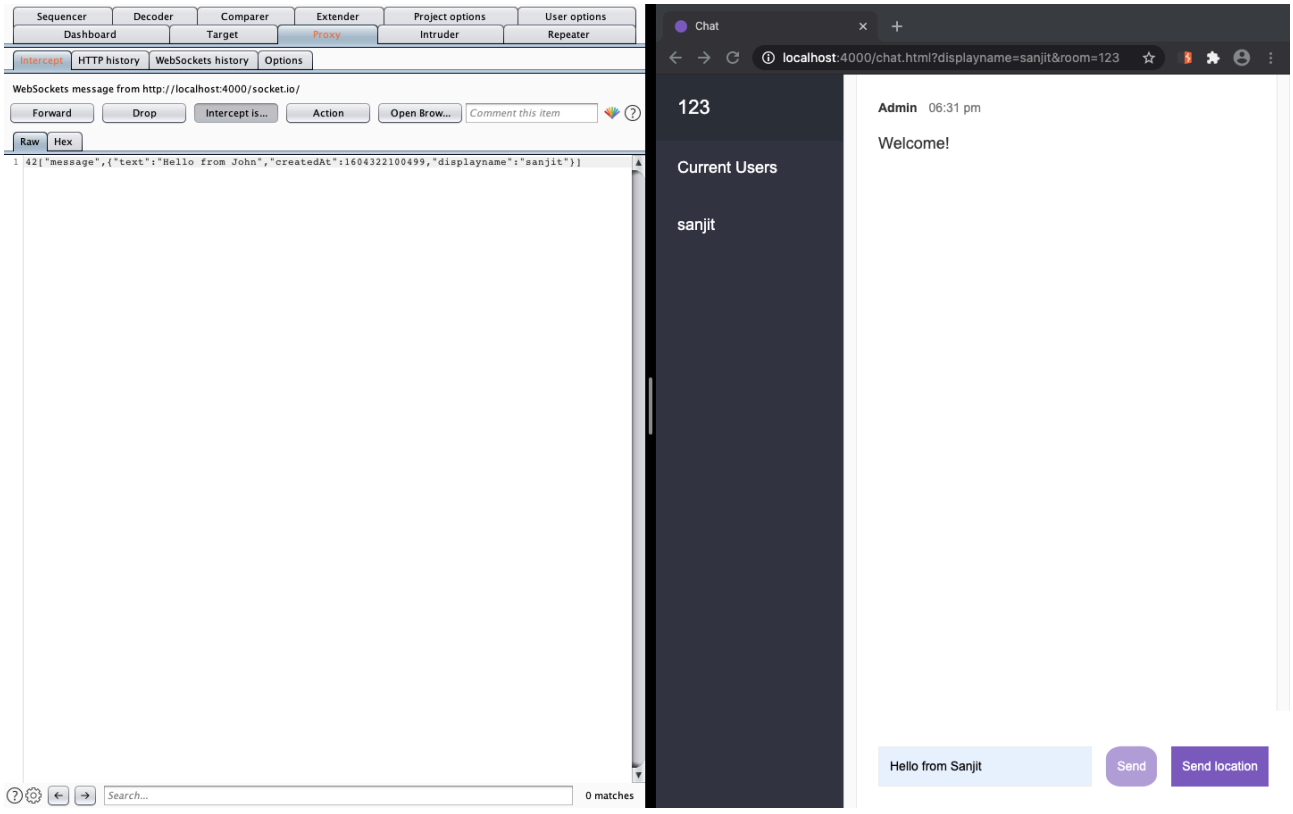
This message is intercepted by the BurpSuite. (Note Left Side Screen)



6. The message “Hello from Sanjit” is intercepted and changed to “Hello from John”

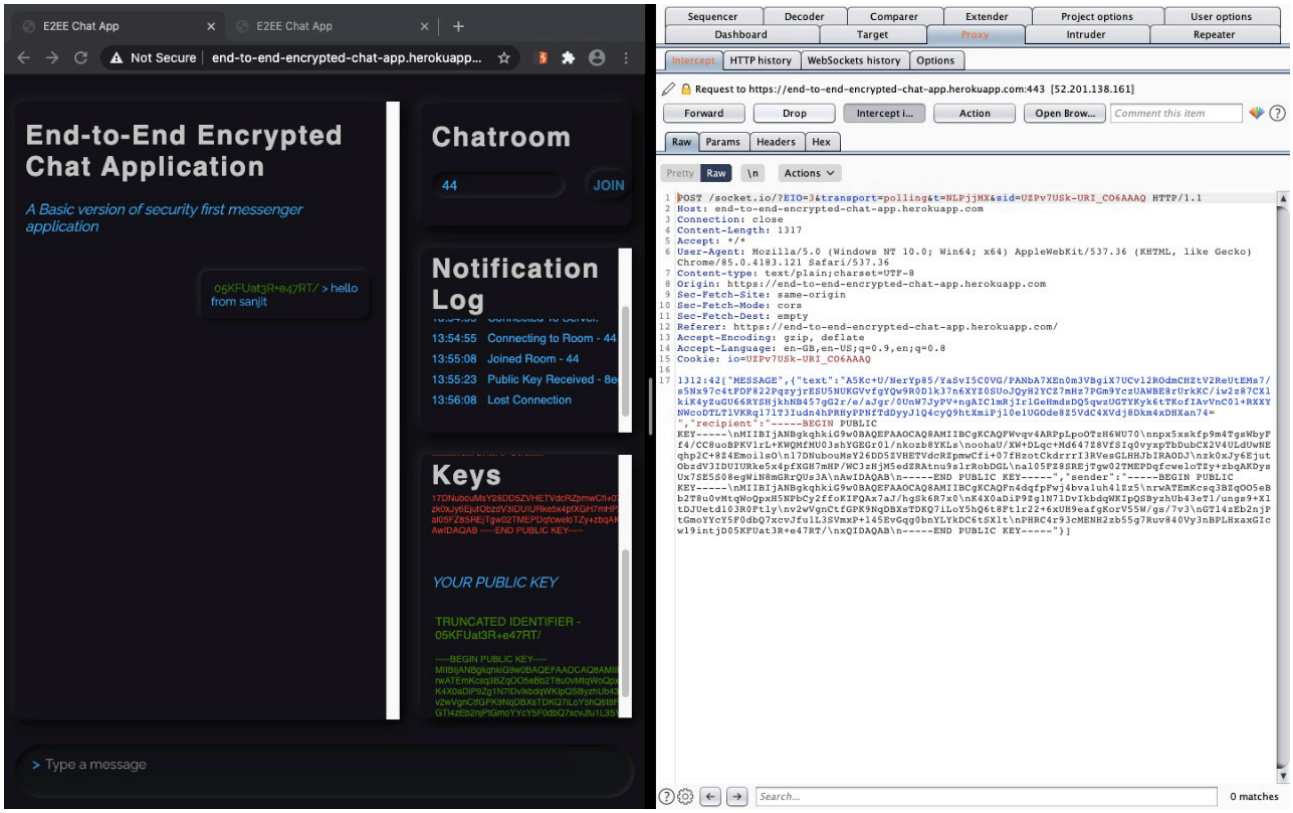


People in the chatroom see the tampered message



Doing the same with encrypted chat application

On tampering the encrypted text that has been interrupted, the decryption on the receivers side with the private key fails and therefore any kind of interruption is impossible.



Conclusion:

Therefore we have seen how to penetration test for tcp/ip/http packets from one socket to another. It was possible to penetration test the non-encrypted chat application but not the encrypted chat application. BurpSuite can still further extensively be used for a variety of other things like 3rd party target monitor and attack testing etc.