EXPLORATION OF BURP SUITE

Division - B

Batch - B1

CONTRIBUTED BY -

Darshan Gandhi 1611069

Rushabh Chheda 1611070

Nipun Iyer 1611081

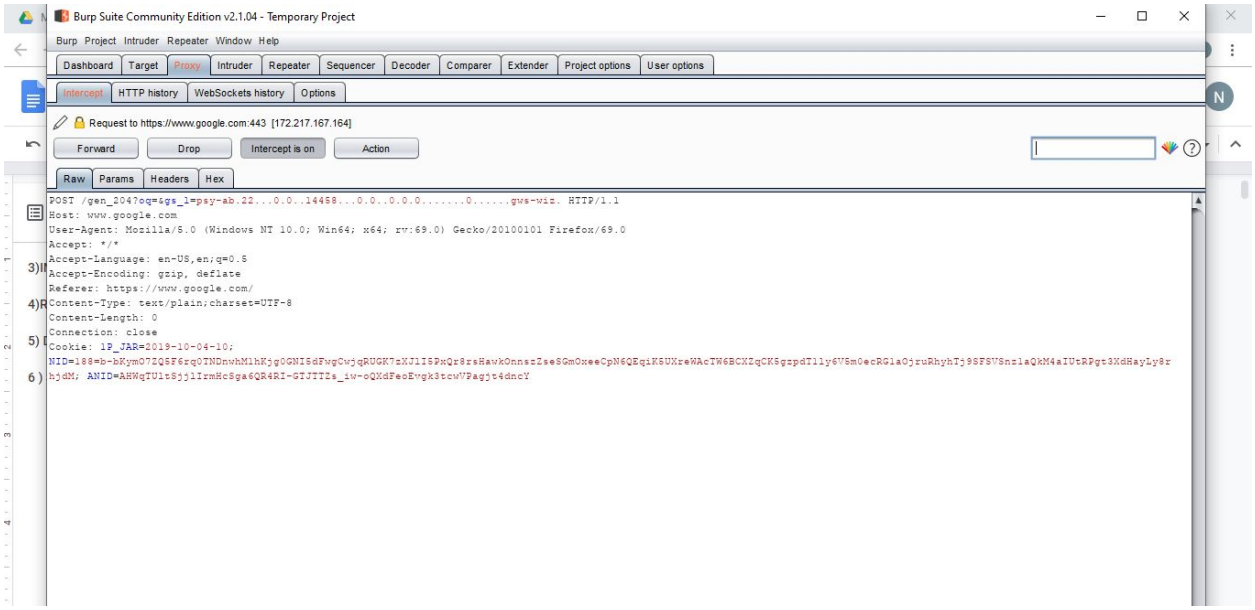
Implemented:

1) Selecting the target
2) Proxy checking
3) Repeater
4) Intruder
5) Decoder
6) Sequencer

1) *SELECTING THE TARGET*

Detailed Stepwise Manual -

1. **Install burp suite and mozilla**
2. **Set up the network networking settings and change the port to 8080 and address to 127.0.0.1**
3. **After installation and setup of CA certificate go back to burp suite**
4. **Go to the proxy tab**
5. **Turn off the inception**
6. **Load any website of your choice**
7. **Go back to the Burp Suite application**
8. **on the left side your target website will be listed.**
9. **Select your target website**



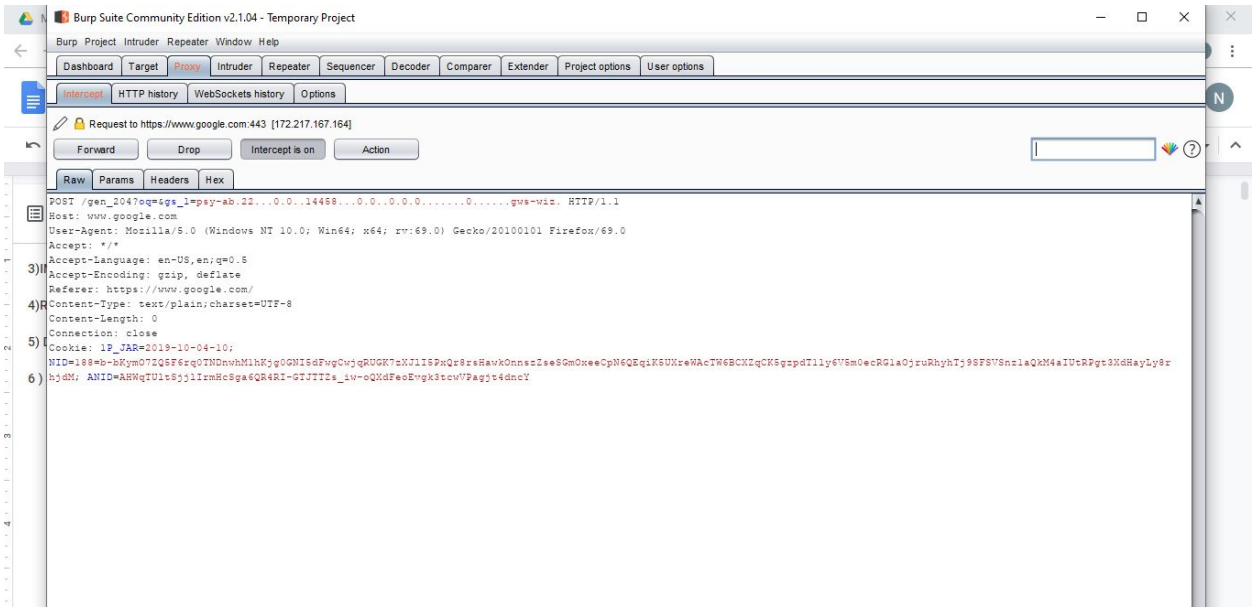
2) *PROXY CHECKING*

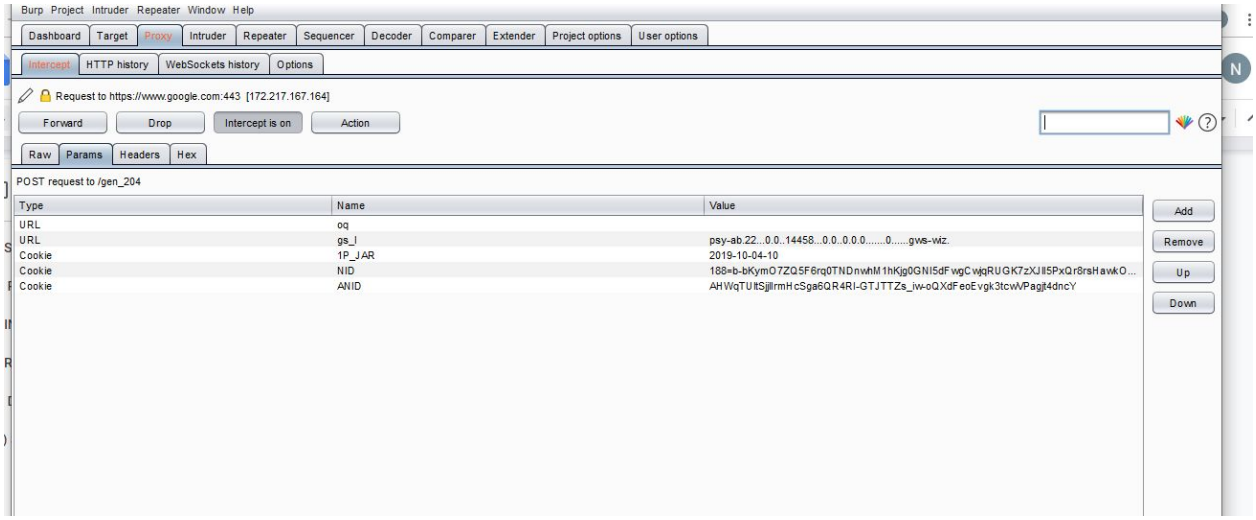
Detailed Stepwise Manual -

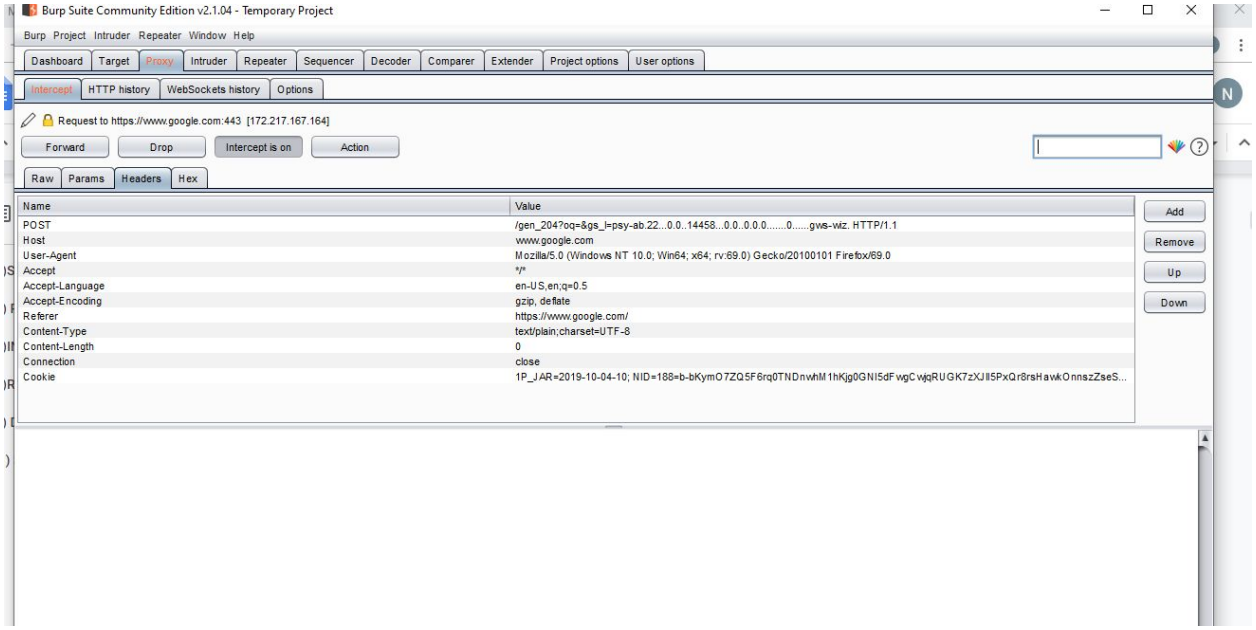
1. Install burp suite and Mozilla
2. Set up the network networking settings and change the port to 8080 and address to 127.0.0.1

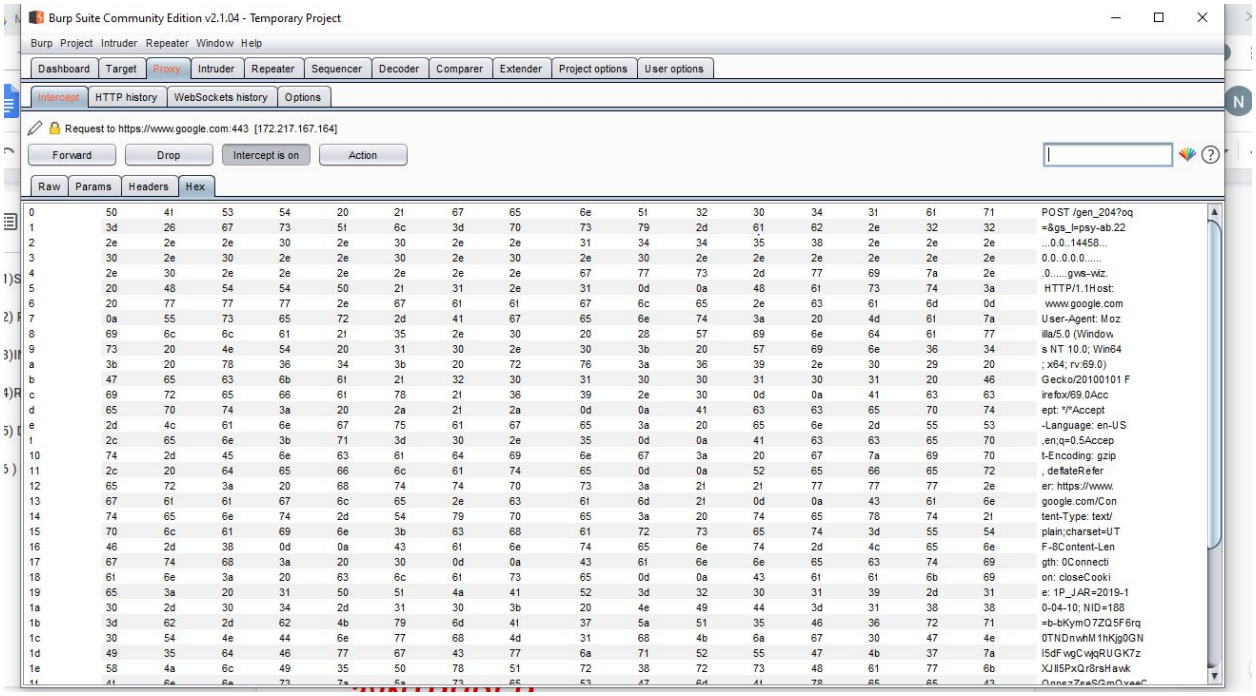
3. Select a target website of your choice
4. Go to your browser, load a login page and fill in some login details. (Don't press the submit option)
5. Go back to the Proxy tab and turn the interception on
6. Go back to the web browser and submit your credentials.
7. Observe the intercepted information.
8. Observe the raw, parameters, headers and hex.
9.

Here the various forms of data can be seen such as the raw, parameters, headers and hex.




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 [172.217.167.164]
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST request to /gen_204
Type Name Value
URL oq
URL gs_l psy-ab.22...0.0..14458...0.0..0.0.0.....0.....gws-wiz.
Cookie 1P_JAR 2019-10-04-10
Cookie NID 188=b-bKymO7ZQ5F6rq0TNDnwhM1hKjg0GNI5dFwgCwjqRUGK7zXJll5PxQr8rsHawkO...
Cookie ANID AHWqTUlt5jllrmHcSga6QR4RI-GTJTTZs_iw-oQXdFeoEvgk3tcwVPagjt4dncY
Add
Remove
Up
Down


Burp Suite Community Edition v2.1.04 - 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 [172.217.167.164]
Forward Drop Intercept is on Action
Raw Params Headers Hex
Name Value
POST /gen_204?oq=&gs_l=psy-ab.22...0.0..14458...0.0..0.0.0.....0.....gws-wiz. HTTP/1.1
Host www.google.com
User-Agent Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept */*
Accept-Language en-US,en;q=0.5
Accept-Encoding gzip, deflate
Referer https://www.google.com/
Content-Type text/plain;charset=UTF-8
Content-Length 0
Connection close
Cookie 1P_JAR=2019-10-04-10; NID=188=b-bKymO7ZQ5F6rq0TNDnwhM1hKjg0GNI5dFwgCwjqRUGK7zXJll5PxQr8rsHawkOnnszZseS...
Add
Remove
Up
Down

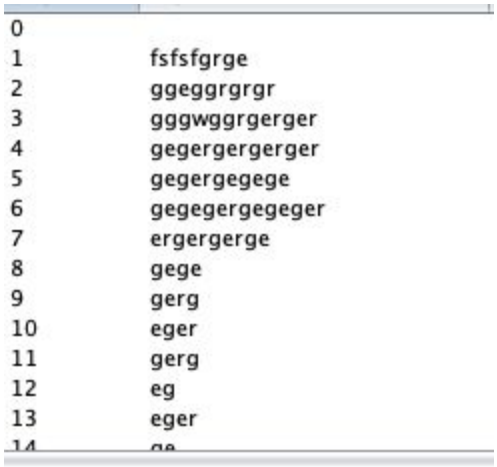


3) INTRUDER

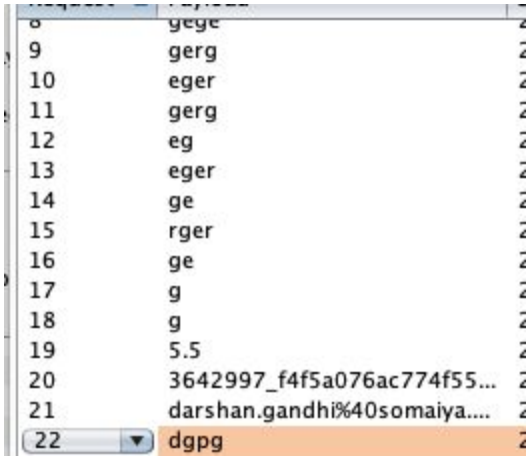
Detailed Stepwise Manual -

1) Go to Mozilla and change the network settings to 127.0.0.1 and port no to 8080.
2) Open burp suite
3) Go to any website's login page.
4) Turn on the interceptor in burp suite and enter the username and any wrong password.
5) Send the request received from the site to intruder.
6) Remove all other variables in the position tab and add the password value as variable that will be brute-forced.
7) Click on payload tab and set payload set as 1 and type as a simple list and add test cases in the word list and click start attack.
8) Password will be brute-forced by word list and their status, length and response to a request are taken into account.
9) Every other wrong password will have the status of 401-unauthorized and 200-ok successful.

Brute force data

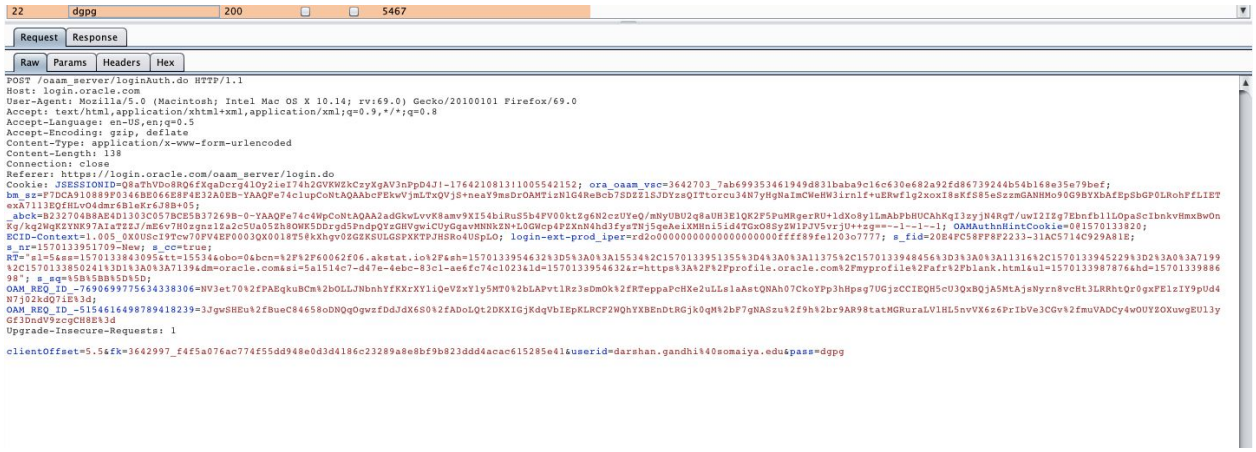


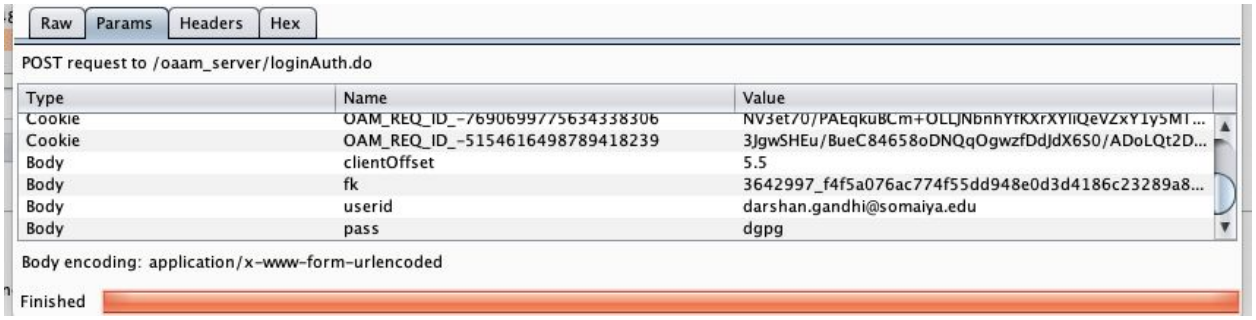
0	
1	fsfsfgrge
2	ggeggrgrgr
3	gggwggrgerger
4	gegergergerger
5	gegergegege
6	gegegergegeger
7	ergergerge
8	gege
9	gerg
10	eger
11	gerg
12	eg
13	eger
14	ge



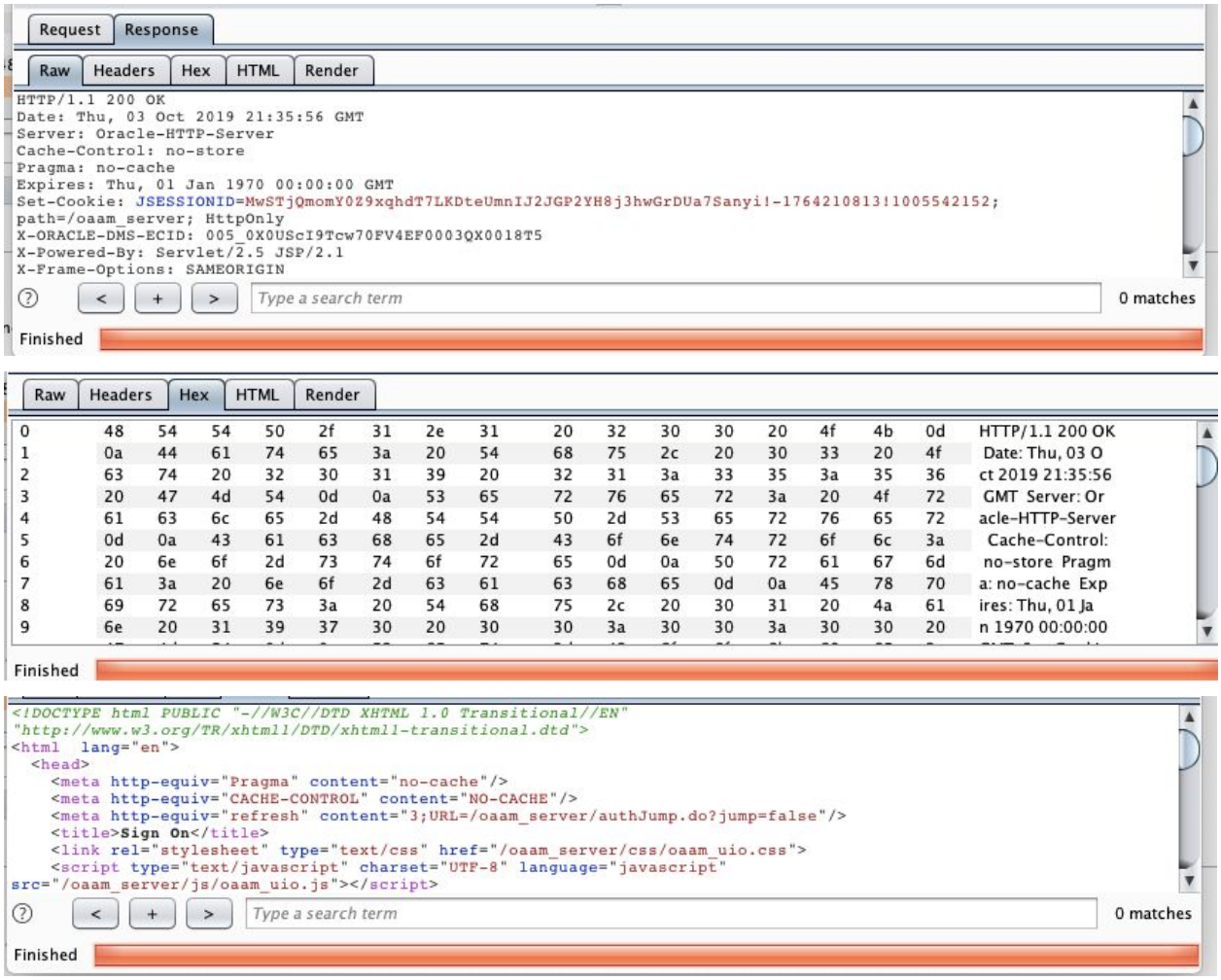
9	gerg
10	eger
11	gerg
12	eg
13	eger
14	ge
15	rger
16	ge
17	g
18	g
19	5.5
20	3642997_f4f5a076ac774f55...
21	darshan.gandhi%40somaiya....
22	dgpg

Request





Response generated



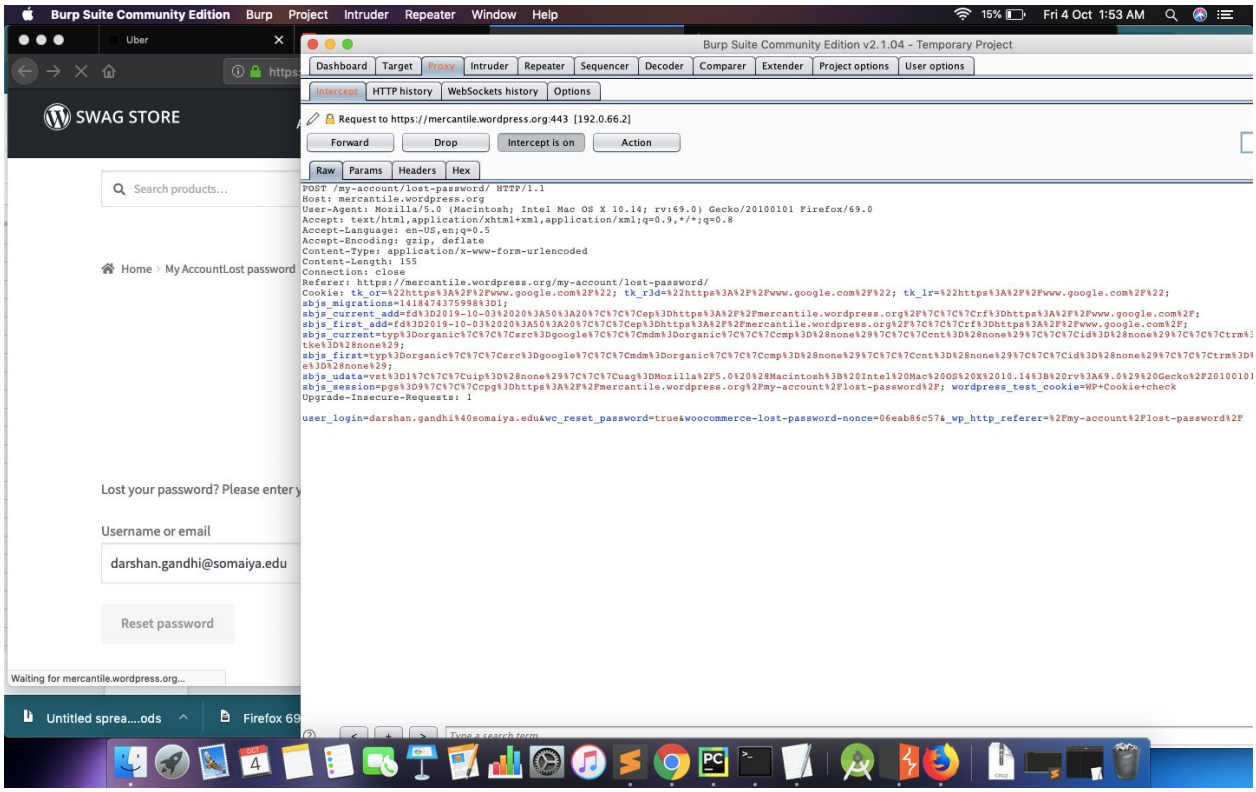
4) REPEATER

Detailed Stepwise Manual -

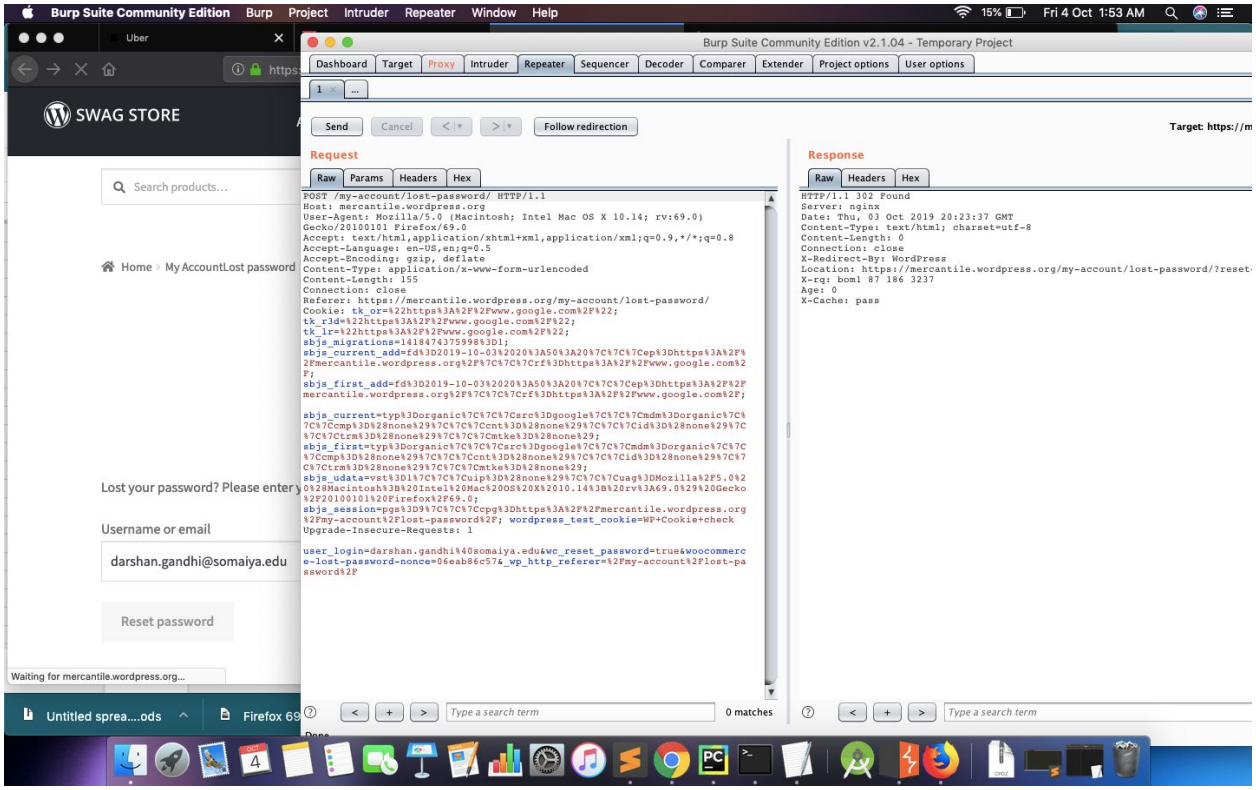
1) Go to Mozilla and change the network settings to 127.0.0.1 and port no to 8080.
2) Open burp suite
3) Go to any website of your choice which contains a login form.
4) In the form click on forget the password (Ensure the interception is turned OFF)
5) Enter the email address
6) Now turn on the interception
7) Click on reset password

8) Observe the raw section of the Intercepter
9) Right-click and send it to the repeater
10) Observe the request section of the repeater
11) Click on the “SEND” button on the top left
12) Observe the response section, it should have the 302: found port displayed
13) If yes, check your entered email and check the inbox.

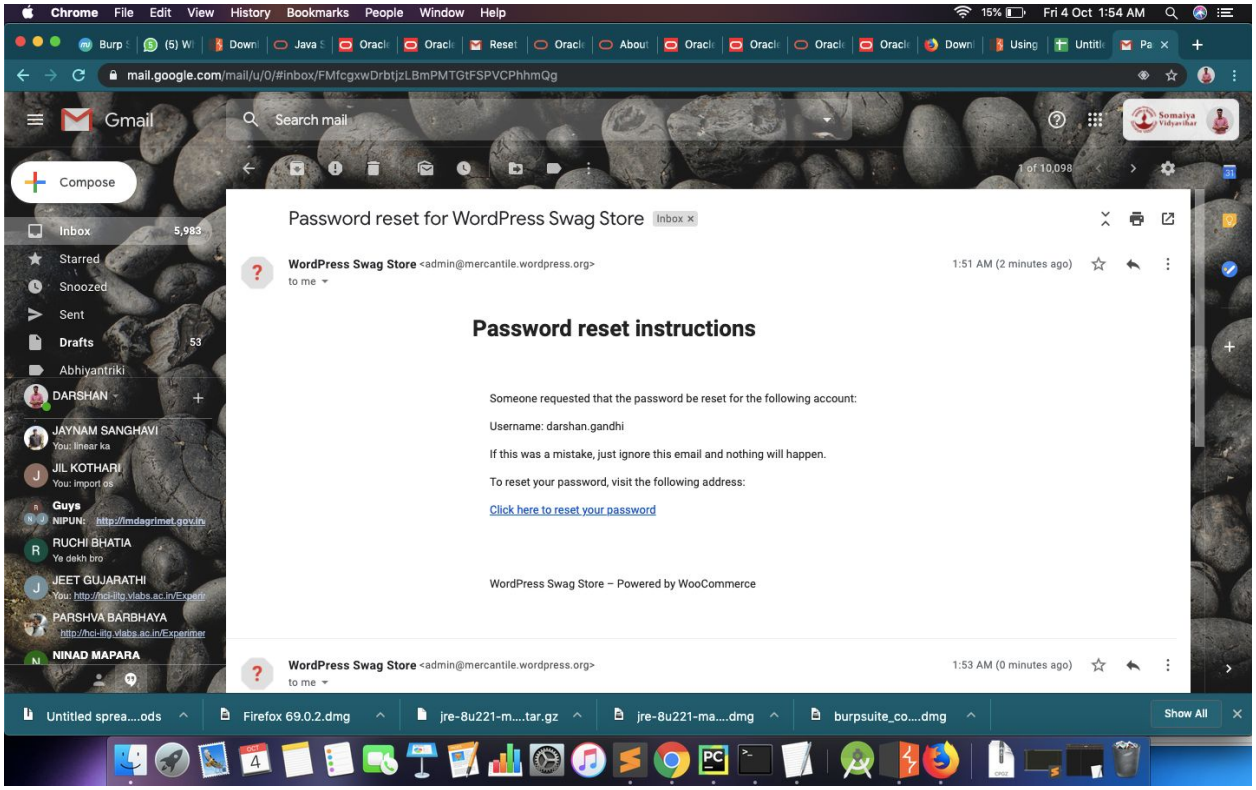
Clicking on resetting the password



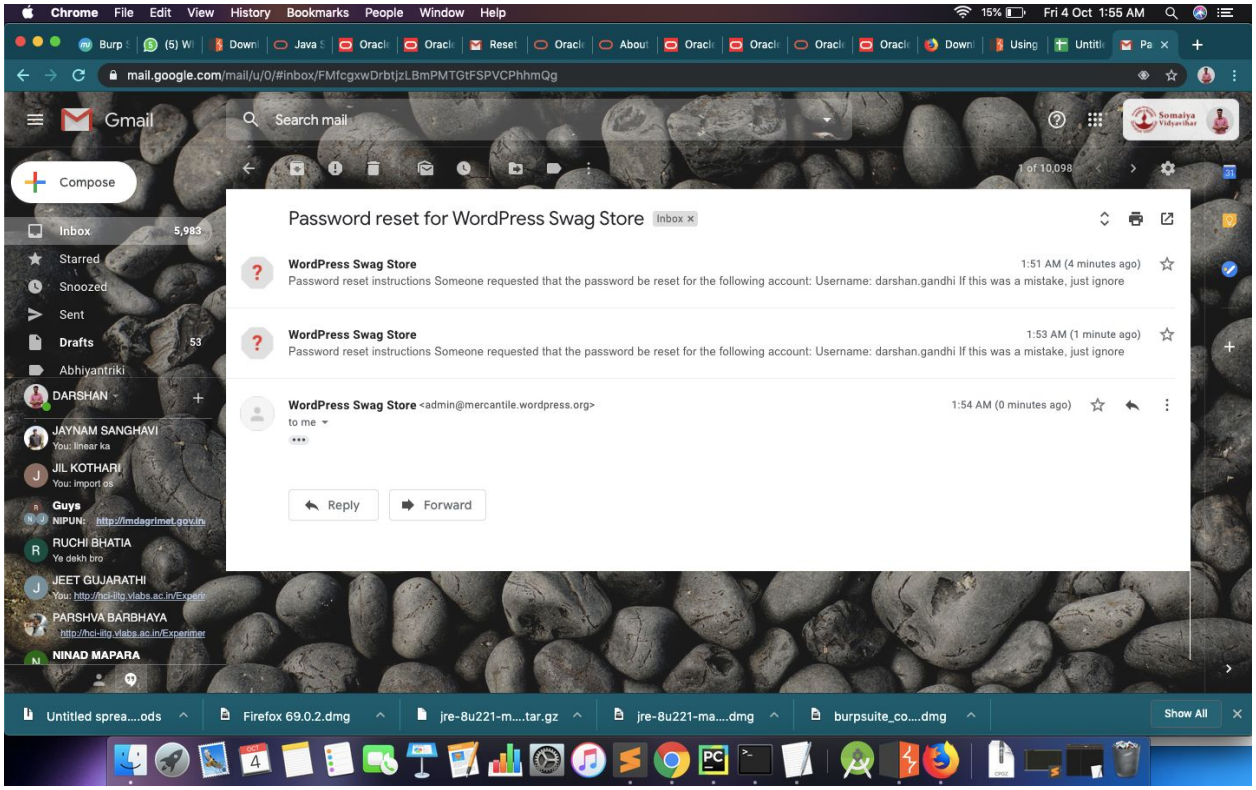
Send the email on the provided mail



Email information



Continuous mails being sent



5) DECODER

Detailed Stepwise Manual -

Go to Mozilla and change the network settings to 127.0.0.1 and port no to 8080.
Open burp suite
Go to any website of your choice.
Observe the answer in the intercepter
Send the corresponding information by right click to the decoder
Open the decoder
Select any of the options from encoding, decode, hash and carry out the detailed view on the same.
For eg-
a) encoding

Click on the encode now and select any from URL , HTML , ASCII HEX ,BASE64 and so on

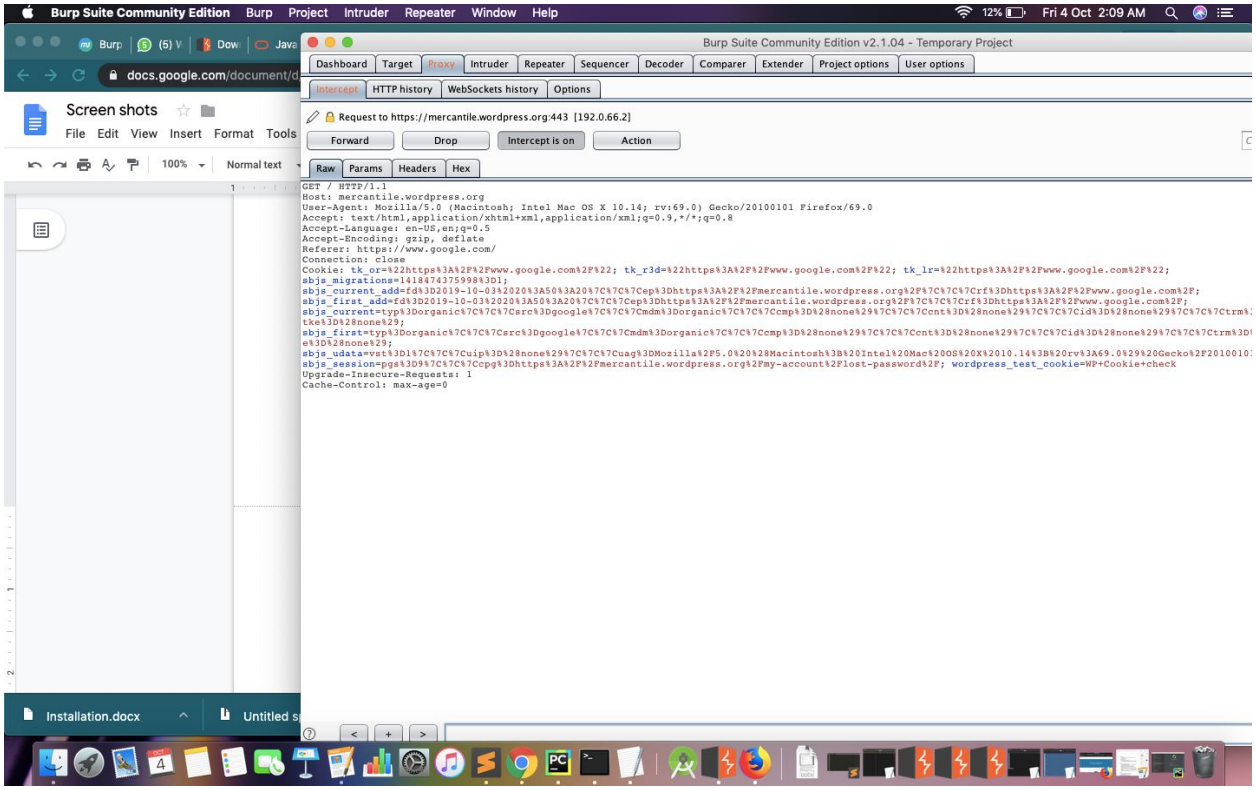
b)decoding

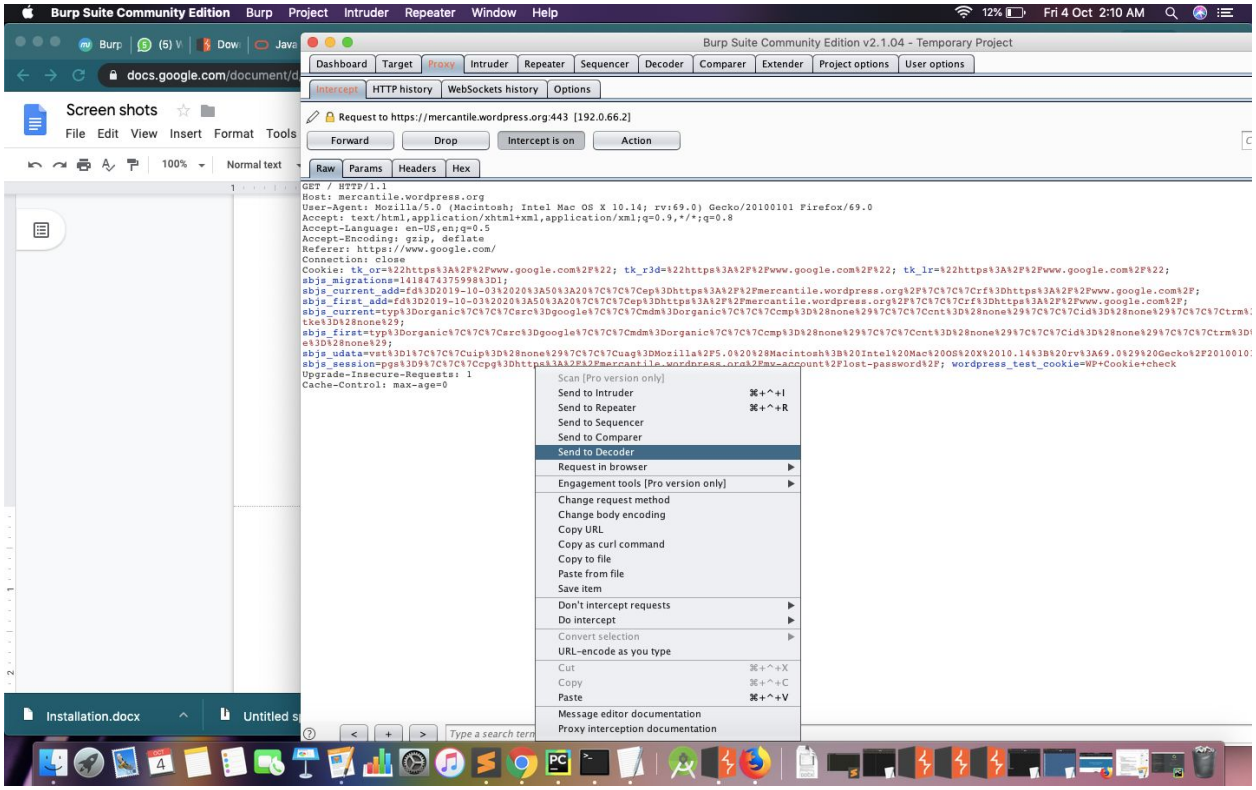
Click on the decode now and select any from URL , HTML, ASCII HEX, BASE64 and so on

c)hash

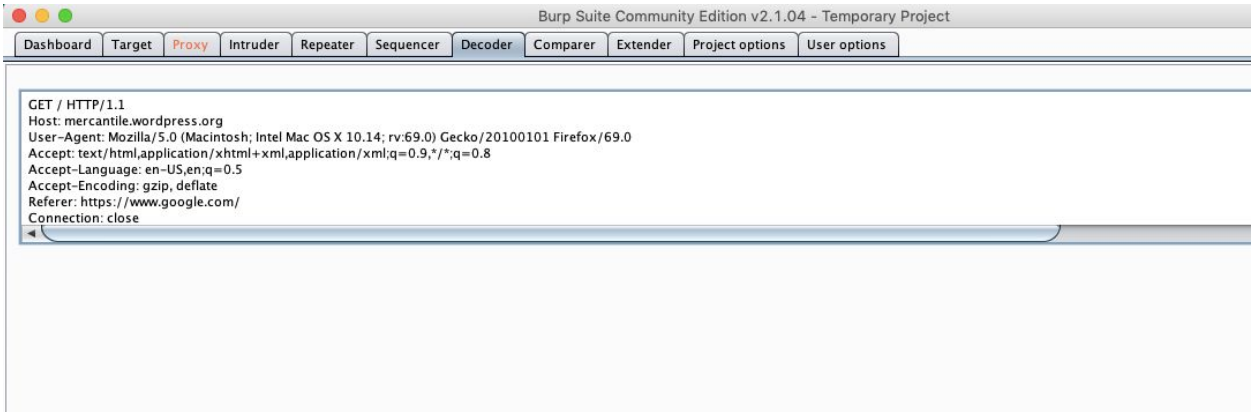
Click on the hash and select any from MD2, MD4, SSH-256, SSH-512 and so on

Observe the results

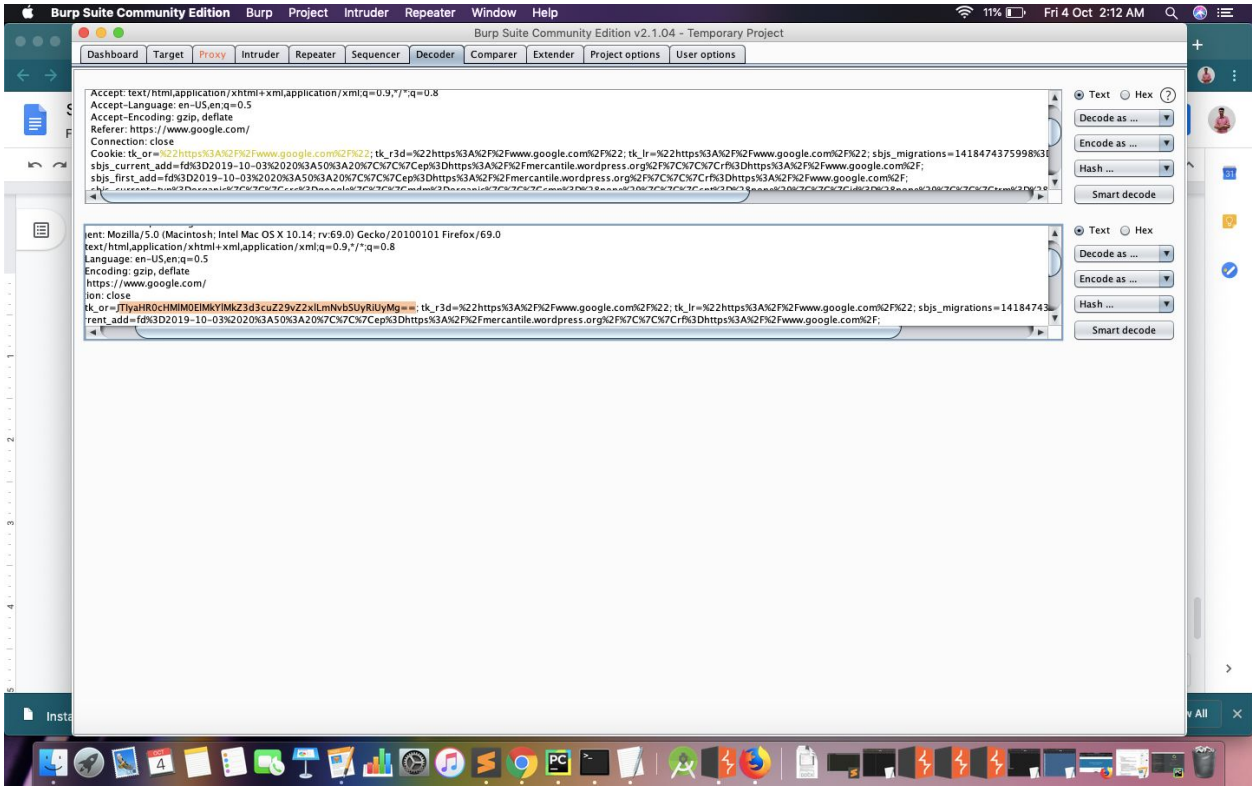

Burp Suite Community Edition Burp Project Intruder Repeater Window Help
12% Fri 4 Oct 2:09 AM
Burp Suite Community Edition v2.1.04 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to https://mercantile.wordpress.org:443 [192.0.66.2]
Forward Drop Intercept is on Action
Raw Params Headers Hex
GET / HTTP/1.1
Host: mercantile.wordpress.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.google.com/
Connection: close
Cookie: tk_or=%22https%3A%2F%2Fwww.google.com%2F%22; tk_r3d=%22https%3A%2F%2Fwww.google.com%2F%22; tk_lr=%22https%3A%2F%2Fwww.google.com%2F%22;
sbjs_migrations=1418474375998%3D1;
sbjs_current_add=fd%3D2019-10-03%2020%3A50%3A20%7C%7C%7Cep%3Dhttps%3A%2F%2Fmercantile.wordpress.org%2F%7C%7C%7Crf%3Dhttps%3A%2F%2Fwww.google.com%2F;
sbjs_first_add=fd%3D2019-10-03%2020%3A50%3A20%7C%7C%7Cep%3Dhttps%3A%2F%2Fmercantile.wordpress.org%2F%7C%7C%7Crf%3Dhttps%3A%2F%2Fwww.google.com%2F;
sbjs_current=typ%3Dorganic%7C%7C%7Csrc%3Dgoogle%7C%7C%7Cmdm%3Dorganic%7C%7C%7Ccmp%3D%28none%29%7C%7C%7Ccnt%3D%28none%29%7C%7C%7Cid%3D%28none%29%7C%7C%7Ctrm%3D%28none%29;
sbjs_first=typ%3Dorganic%7C%7C%7Csrc%3Dgoogle%7C%7C%7Cmdm%3Dorganic%7C%7C%7Ccmp%3D%28none%29%7C%7C%7Ccnt%3D%28none%29%7C%7C%7Cid%3D%28none%29%7C%7C%7Ctrm%3D%28none%29;
sbjs_udata=vst%3D1%7C%7C%7Cuip%3D%28none%29%7C%7C%7Cuag%3DMozilla%2F5.0%20%28Macintosh%3B%20Intel%20Mac%20OS%20X%2010.14%3B%20rv%3A69.0%29%20Gecko%2F20100101;
sbjs_session=pgs%3D9%7C%7C%7Ccpg%3Dhttps%3A%2F%2Fmercantile.wordpress.org%2Fmy-account%2Flost-password%2F; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Screen shots
File Edit View Insert Format Tools
Installation.docx


Burp Suite Community Edition Burp Project Intruder Repeater Window Help
12% Fri 4 Oct 2:10 AM
Burp Suite Community Edition v2.1.04 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to https://mercantile.wordpress.org:443 [192.0.66.2]
Forward Drop Intercept is on Action
Raw Params Headers Hex
GET / HTTP/1.1
Host: mercantile.wordpress.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.google.com/
Connection: close
Cookie: tk_or=%22https%3A%2F%2Fwww.google.com%2F%22; tk_r3d=%22https%3A%2F%2Fwww.google.com%2F%22; tk_lr=%22https%3A%2F%2Fwww.google.com%2F%22;
sbjs_migrations=1418474375998%3D1;
sbjs_current_add=fd%3D2019-10-03%2020%3A50%3A20%7C%7C%7Cep%3Dhttps%3A%2F%2Fmercantile.wordpress.org%2F%7C%7C%7Crf%3Dhttps%3A%2F%2Fwww.google.com%2F;
sbjs_first_add=fd%3D2019-10-03%2020%3A50%3A20%7C%7C%7Cep%3Dhttps%3A%2F%2Fmercantile.wordpress.org%2F%7C%7C%7Crf%3Dhttps%3A%2F%2Fwww.google.com%2F;
sbjs_current=typ%3Dorganic%7C%7C%7Csrc%3Dgoogle%7C%7C%7Cmdm%3Dorganic%7C%7C%7Ccmp%3D%28none%29%7C%7C%7Ccnt%3D%28none%29%7C%7C%7Cid%3D%28none%29%7C%7C%7Ctrm%3D%28none%29;
sbjs_first=typ%3Dorganic%7C%7C%7Csrc%3Dgoogle%7C%7C%7Cmdm%3Dorganic%7C%7C%7Ccmp%3D%28none%29%7C%7C%7Ccnt%3D%28none%29%7C%7C%7Cid%3D%28none%29%7C%7C%7Ctrm%3D%28none%29;
sbjs_udata=vst%3D1%7C%7C%7Cuip%3D%28none%29%7C%7C%7Cuag%3DMozilla%2F5.0%20%28Macintosh%3B%20Intel%20Mac%20OS%20X%2010.14%3B%20rv%3A69.0%29%20Gecko%2F20100101;
sbjs_session=pgs%3D9%7C%7C%7Ccpg%3Dhttps%3A%2F%2Fmercantile.wordpress.org%2Fmy-account%2Flost-password%2F; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Scan [Pro version only]
Send to Intruder ⌘+^+I
Send to Repeater ⌘+^+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut ⌘+^+X
Copy ⌘+^+C
Paste ⌘+^+V
Message editor documentation
Proxy interception documentation
Screen shots
File Edit View Insert Format Tools
Installation.docx

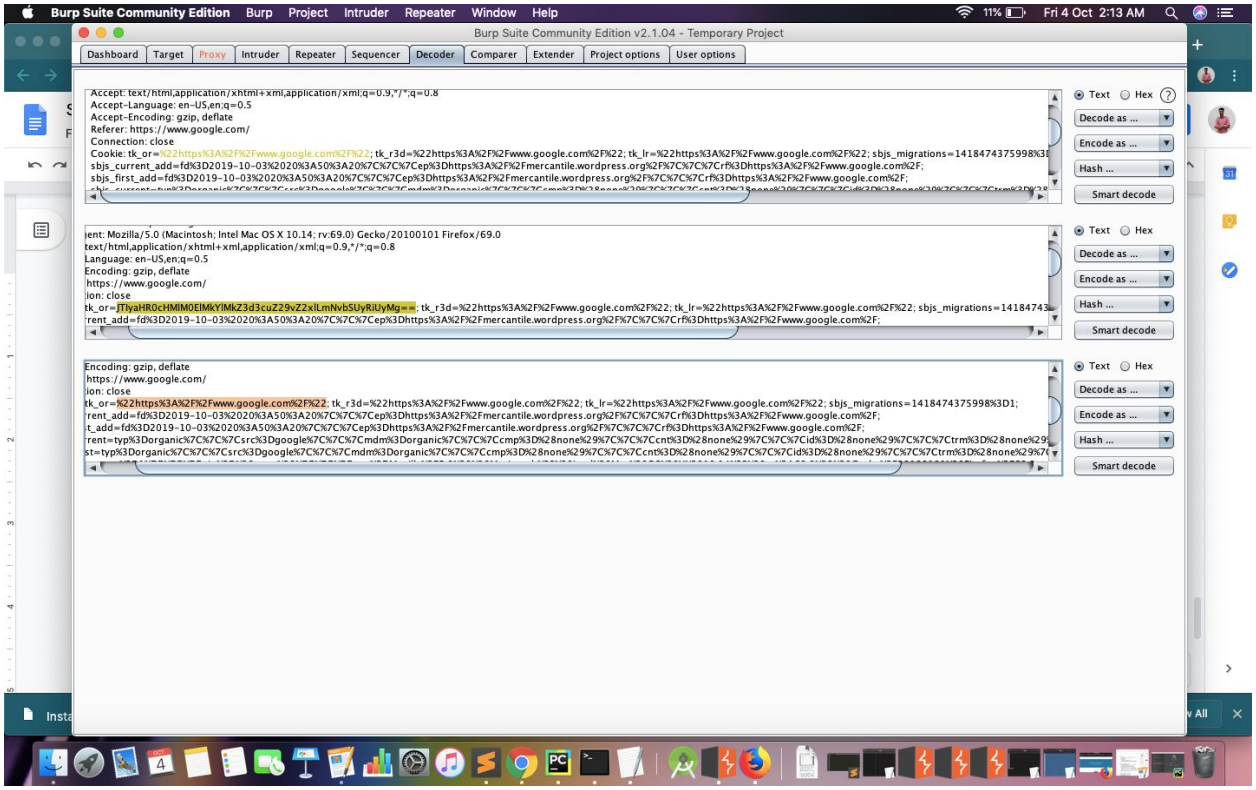
At the decoder



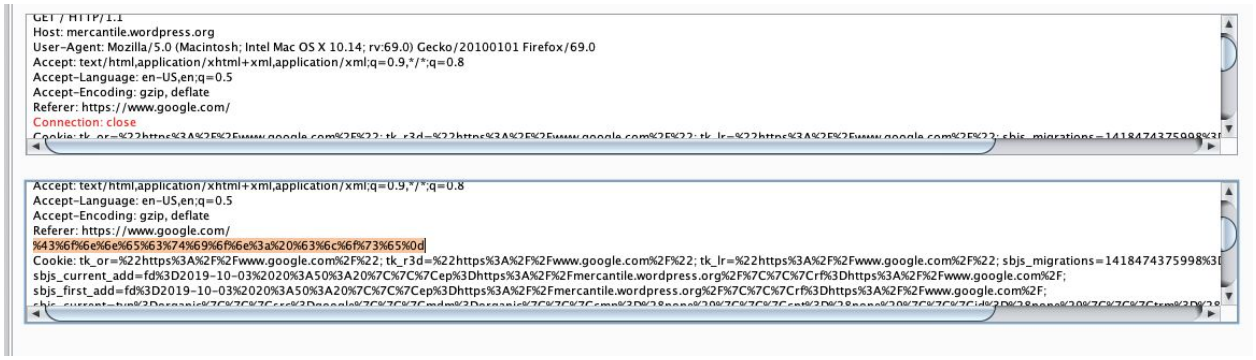
Encoding the given string as Base64



Decoding the given string as Base64 we can see that we get back the same string



Encoding as URL

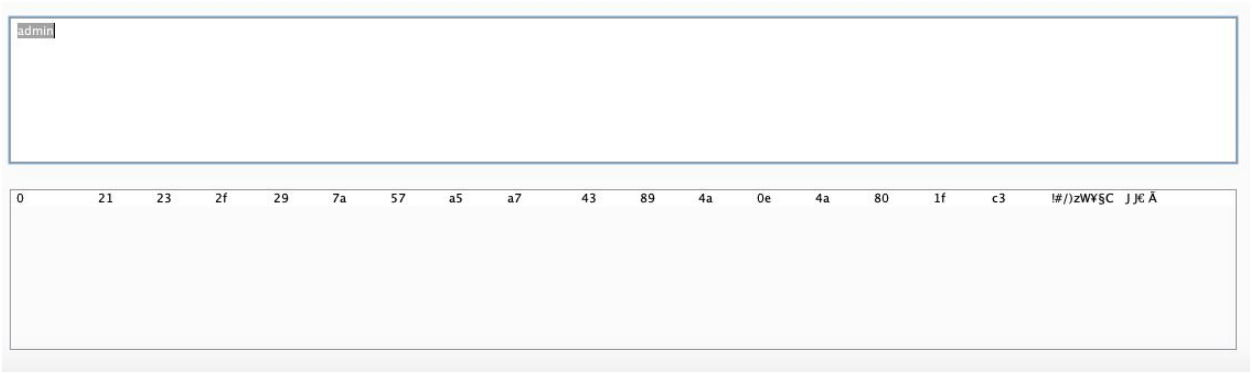


Encoding as ASCII HEX

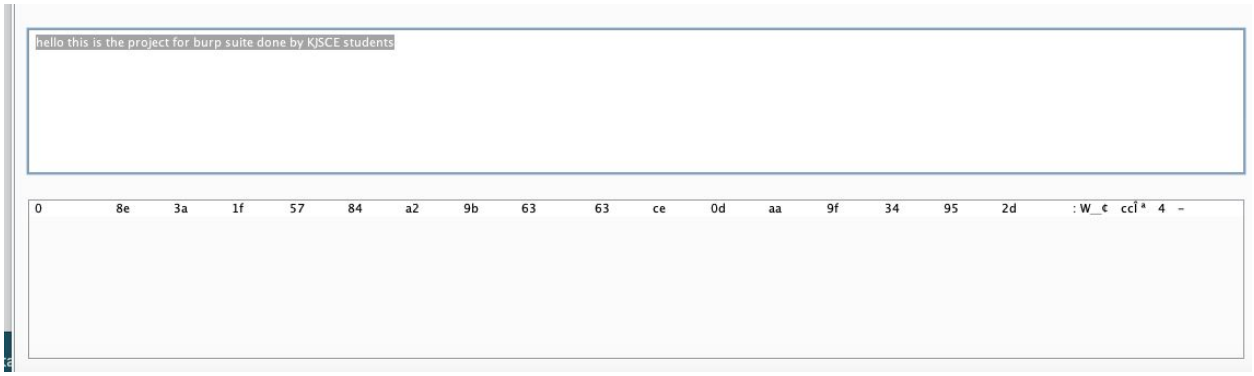
Hashing

MD5

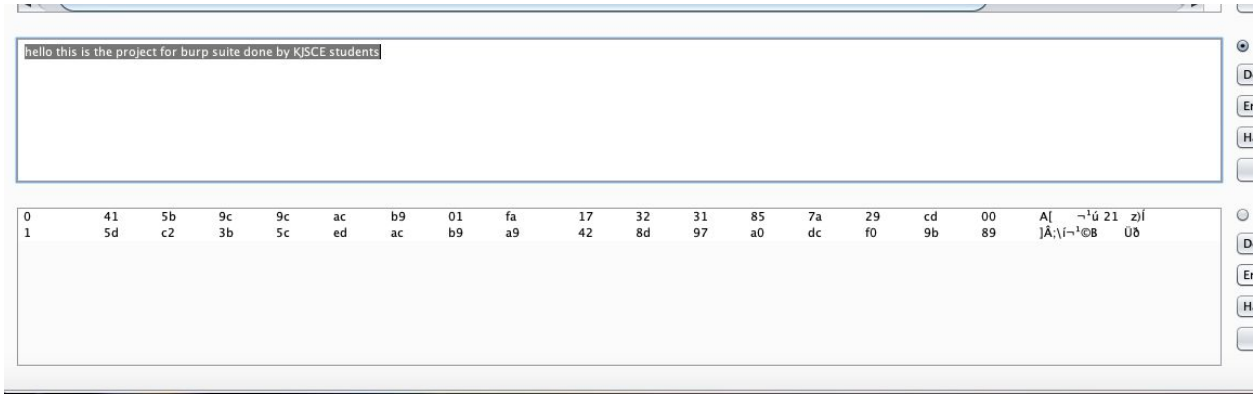
A)



B)

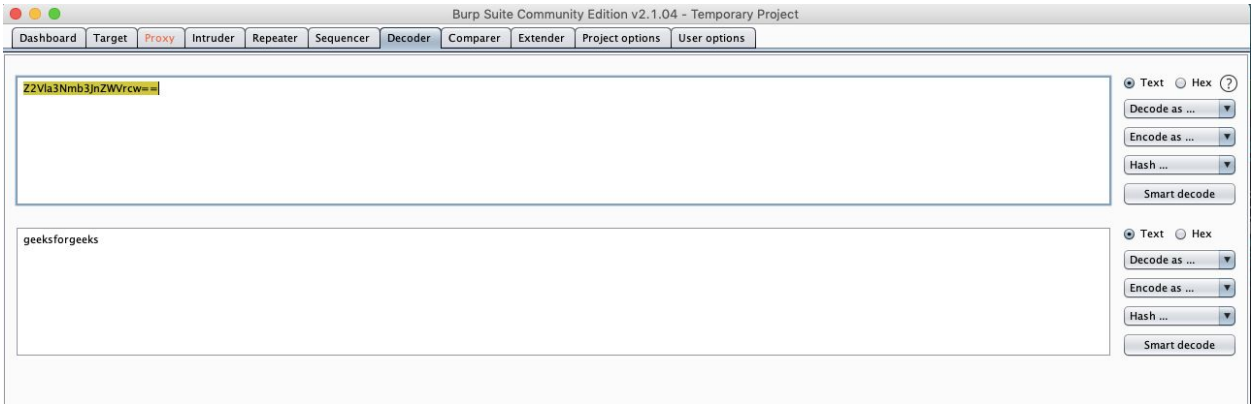


SHA-256 example



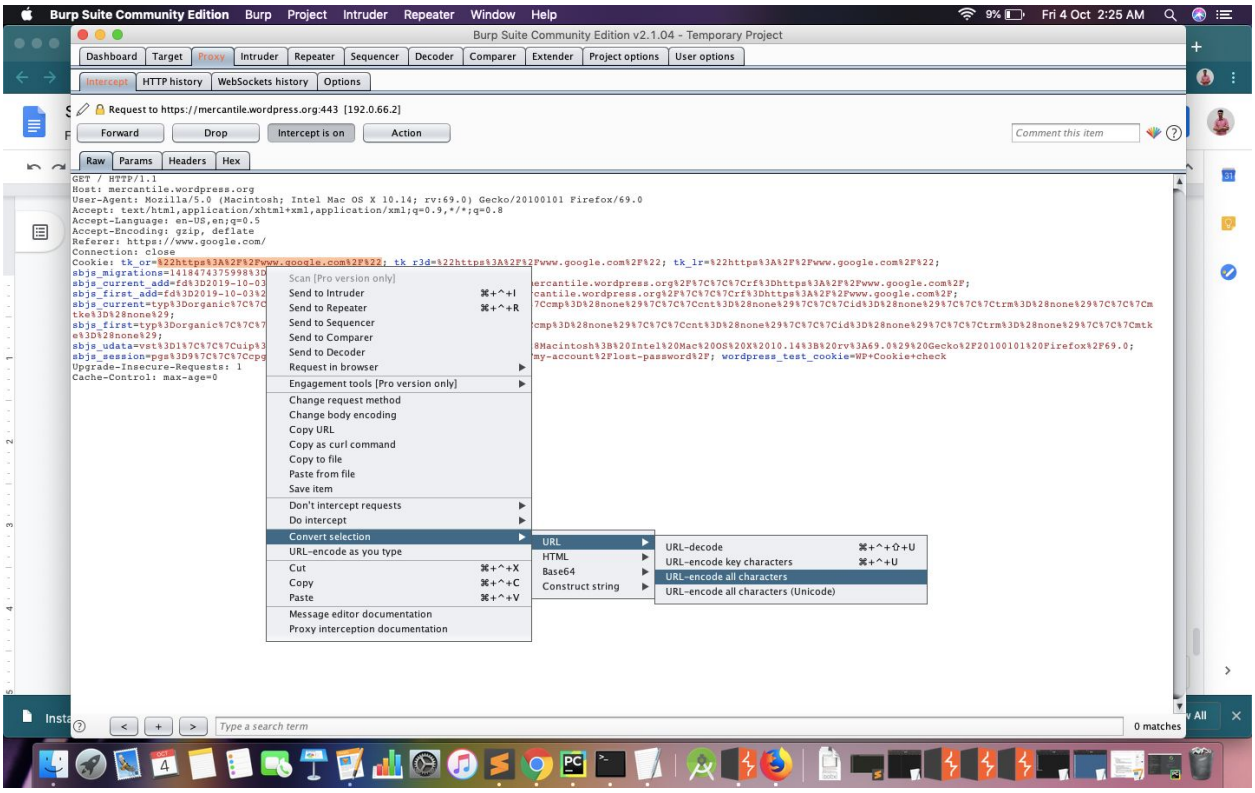
Smart decoing

geeksforgeeks example



Fast way to encode and decode from the proxy area itself

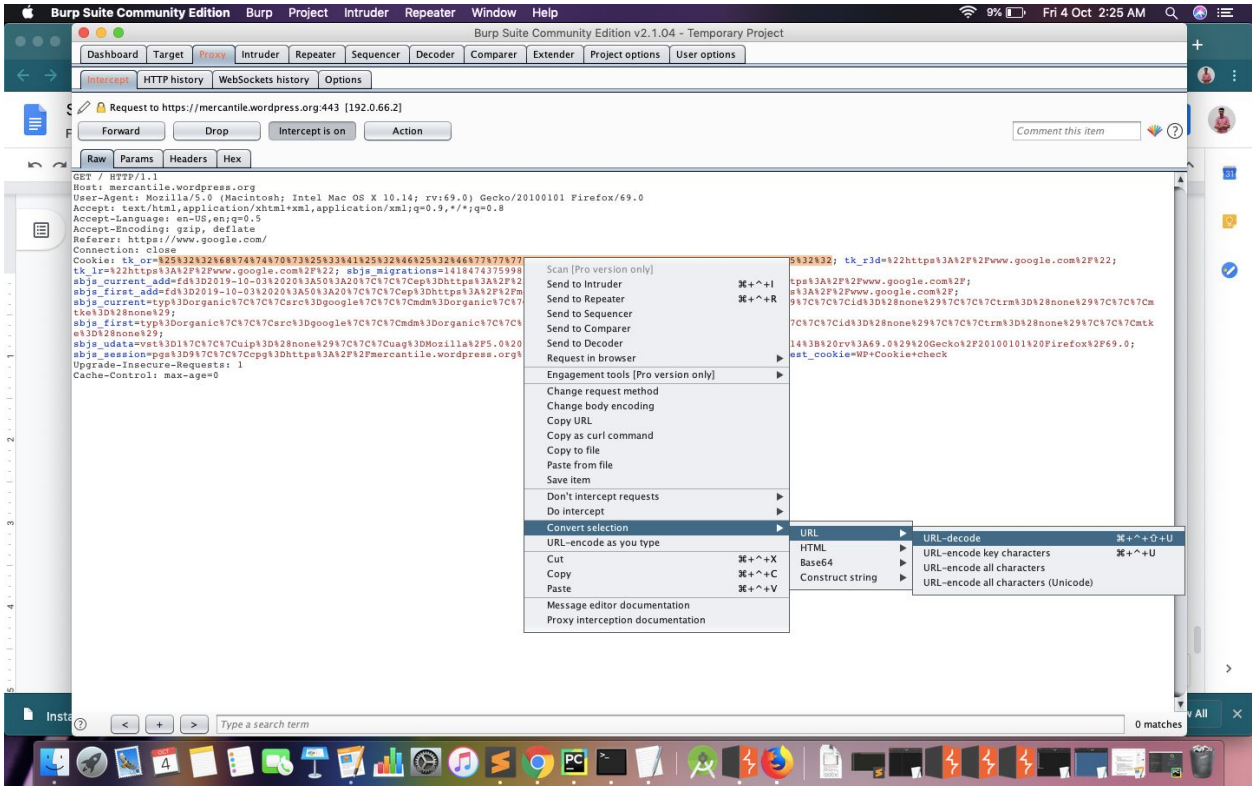
Encoding using URL



ENCODED MESSAGE

```
Referer: https://www.google.com/
Connection: close
Cookie: tk_or=%25%32%32%68%74%74%70%73%25%33%41%25%32%46%25%32%46%77%77%77%2e%67%6f%6f%67%6c%65%2e%63%6f%6d%25%32%46%25%32%32; tk_r3d=%22ht
tk_lr=%22https%3A%2F%2Fwww.google.com%2F%22; sbjs_migrations=1418474375998%3D1;
sbjs_current_add=fd%3D2019-10-03%2020%3A50%3A20%7C%7C%7Cep%3Dhttps%3A%2F%2Fmercantile.wordpress.org%2F%7C%7C%7Crf%3Dhttps%3A%2F%2Fwww.googl
sbjs_first_add=fd%3D2019-10-03%2020%3A50%3A20%7C%7C%7Cep%3Dhttps%3A%2F%2Fmercantile.wordpress.org%2F%7C%7C%7Crf%3Dhttps%3A%2F%2Fwww.google.
```

DECODING USING URL



DECODED MESSAGE

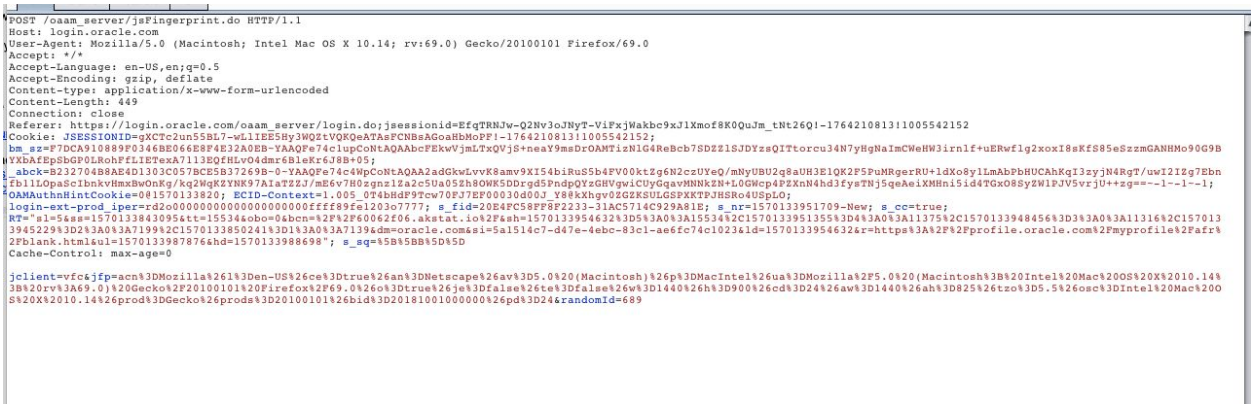
6) SEQUENCER

Detailed Stepwise Manual -

1) Go to Mozilla and change the network settings to 127.0.0.1 and port no to 8080.
2) Open burp suite
3) Go to any website's login page.
4) Turn on the interceptor in burp suite and reload the page to catch the cookie.
5) Request from the site has a set-cookie-header which has a session id. Remove this cookie-header and send this request to the sequencer.
6) New session-id get assigned and the cookie is known.
7) Then start the live-capture where tokens get captured for analysis of randomness and predictability of token sessions.

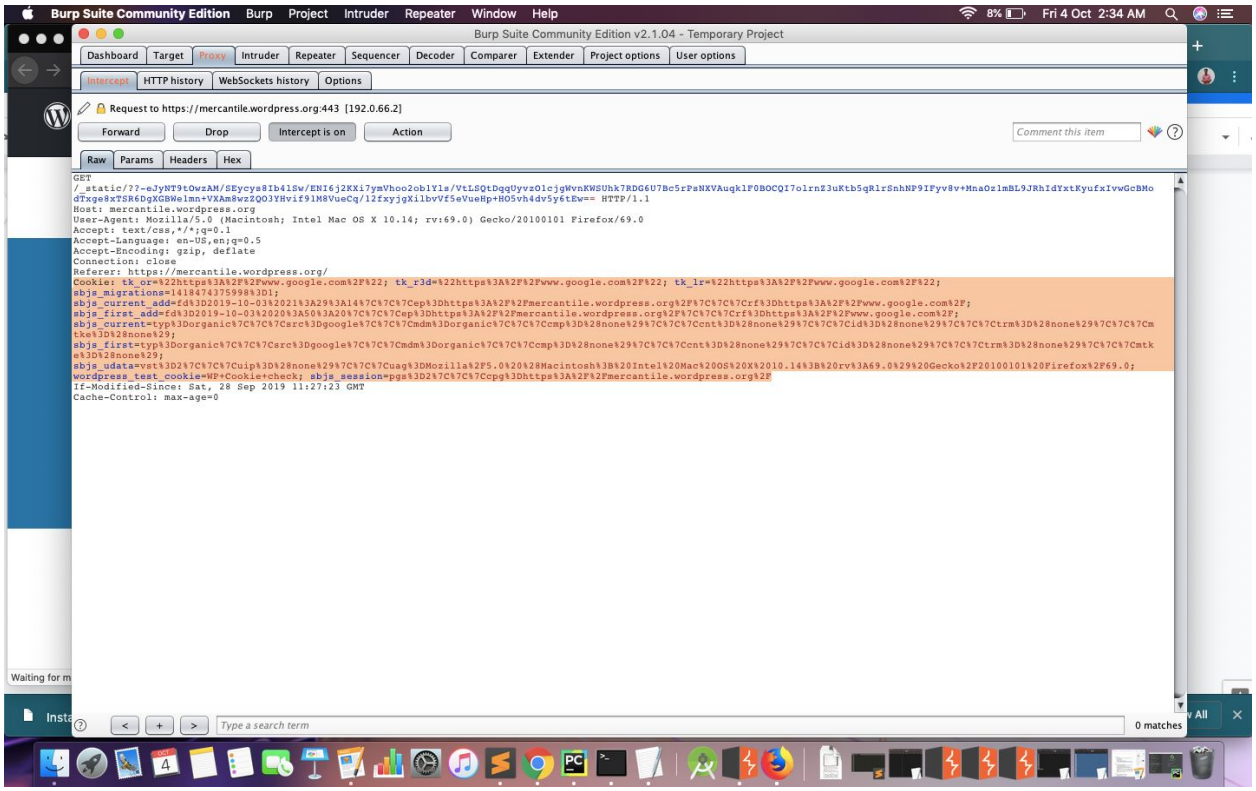
8) We will find effective entropy and histogram data.

Request from the site containing cookie header and session id.



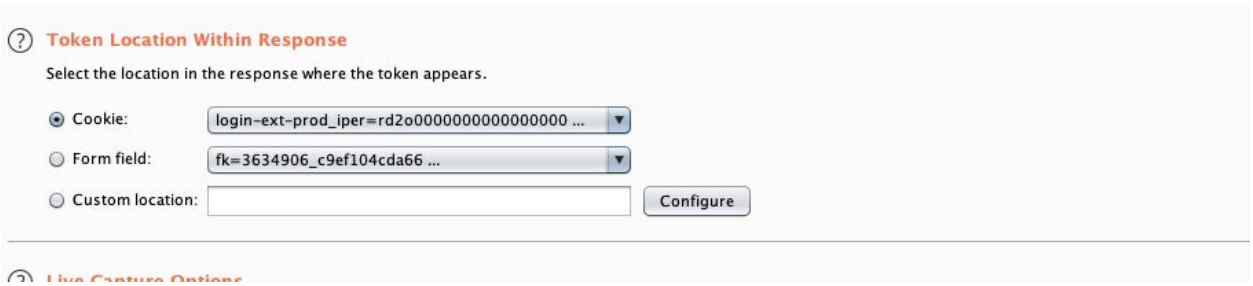
```
POST /oaam_server/jsFingerprint.do HTTP/1.1
Host: login.oracle.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
Content-Length: 449
Connection: close
Referer: https://login.oracle.com/oaam_server/login.do;jsessionid=EfqTRNJw-Q2Nv3oJNyT-ViFxjWakbc9xJ1Xmof8K0QuJm_tNt26Q!-1764210813!1005542152
Cookie: JSESSIONID=gXCTc2un55BL7-wL1IEE5Hy3WQttVQKQeATAsFCNBsAGoaHbNoPF!-1764210813!1005542152;
bm_sz=F7DCA910889F0346BE06EE8F4E32A0EB-YAAQFe7clupCoNtAQAAbcFEkwVjmLTxQVjS+neaY9msDrOAMTizNlG4ReBcb7SDZ1SJDYzsQITtorcu34N7yHgNaImCWeHW3irnlf+uERwflg2xoxI8sKfS85eSzzmGANHMo90G9B
YXbAfEpSbGP0LRohFfLIETexA7113EQfHLvO4dmr6BleKr6J8B+05;
_abck=B232704B8AE4D1303C057BCE5B37269B-0-YAAQFe74c4WpCoNtAQAA2adGkwLvvK8amv9XI54biRuS5b4FV00ktZg6N2czUYeQ/mNyUBU2q8aUH3E1QK2F5PuMRgerRU+ldXo8ylLmAbPbHUCAhKqI3zyjN4RgT/uwI2IZg7Ebn
fb1lLOpaScIbnkvHmxBwOnKg/kq2WqKZYNK97AIaTZZJ/mE6v7H0zgnzIZa2c5Ua05Zh8OWK5DDrgd5PndpQYzGHVgwiCUyGqavMNNkZN+L0GWcp4PZXnN4hd3fysTNj5qeAeiXMHni5id4TGxO8SyZW1PJV5vrjU++zg==--1--1--1;
OAMAuthnHintCookie=0@1570133820; ECID-Context=1.005_QT4bHdF9Tcw70FJ7EF00030d00J_Y88kXhgv0ZGZKSULGSPXKTPJHSRo4USpLO;
login-ext-prod_iper=rd2o00000000000000000000ffff89fe1203o7777; s_fid=20E4FC58FF8F2233-31AC5714C929A81E; s_nr=1570133951709-New; s_cc=true;
RT="sl=5&ss=1570133843095&tt=15534&obo=0&bcn=%2F%2F60062f06.akstat.io%2F&sh=1570133954632%3D5%3A0%3A1553432C1570133951355%3D4%3A0%3A11375%2C1570133948456%3D3%3A0%3A11316%2C157013
3945229%3D2%3A0%3A7199%2C1570133850241%3D1%3A0%3A7139&dm=oracle.com&si=5a1514c7-d47e-4ebc-83c1-ae6fc74c1023&ld=1570133954632&r=https%3A%2F%2Fprofile.oracle.com%2Fmyprofile%2Fafr%
2Fblank.html&ul=1570133987876&hd=1570133988698"; s_sq=%5B%5BB%5D%5D
Cache-Control: max-age=0

jclient=vfc&jfp=acn%3DMozilla%261%3Den-US%26ce%3Dtrue%26an%3DNetscape%26av%3D5.0%20(Macintosh)%26p%3DMacIntel%26ua%3DMozilla%2F5.0%20(Macintosh%3B%20Intel%20Mac%20OS%20X%2010.14%
3B%20rv%3A69.0)%20Gecko%2F20100101%20Firefox%2F69.0%26o%3Dtrue%26je%3Dfalse%26te%3Dfalse%26w%3D1440%26h%3D900%26cd%3D24%26aw%3D1440%26ah%3D825%26tzo%3D5.5%26osc%3DIntel%20Mac%20O
S%20X%2010.14%26prod%3DGecko%26prods%3D20100101%26bid%3D201810010000000%26pd%3D24&randomId=689
```

Deleting the selected cookie and forwarding the request

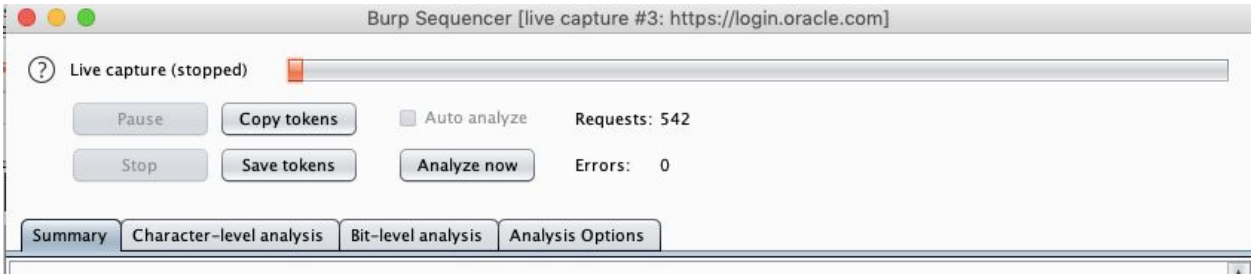


Request

New random cookie assignment



Analysis

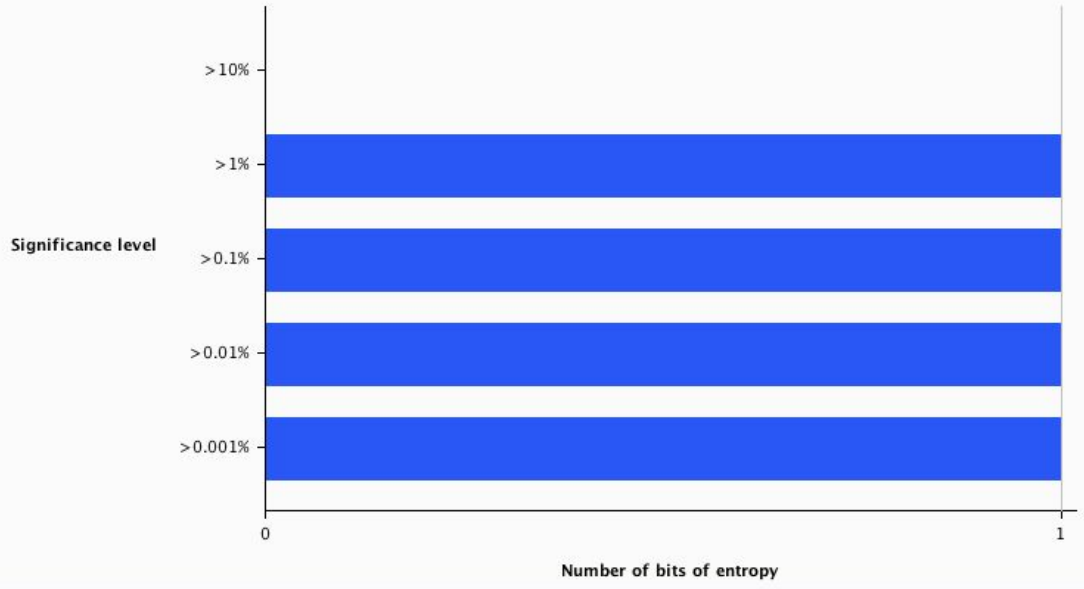


Overall result

The overall quality of randomness within the sample is estimated to be: extremely poor.
At a significance level of 1%, the amount of effective entropy is estimated to be: 1 bits.

Effective Entropy

The chart shows the number of bits of effective entropy at each significance level, based on all tests. Each significance level defines a minimum probability of the observed results occurring if the sample is randomly generated. When the probability of the observed results occurring falls below this level, the hypothesis that the sample is randomly generated is rejected. Using a lower significance level means that stronger evidence is required to reject the hypothesis that the sample is random, and so increases the chance that non-random data will be treated as random.



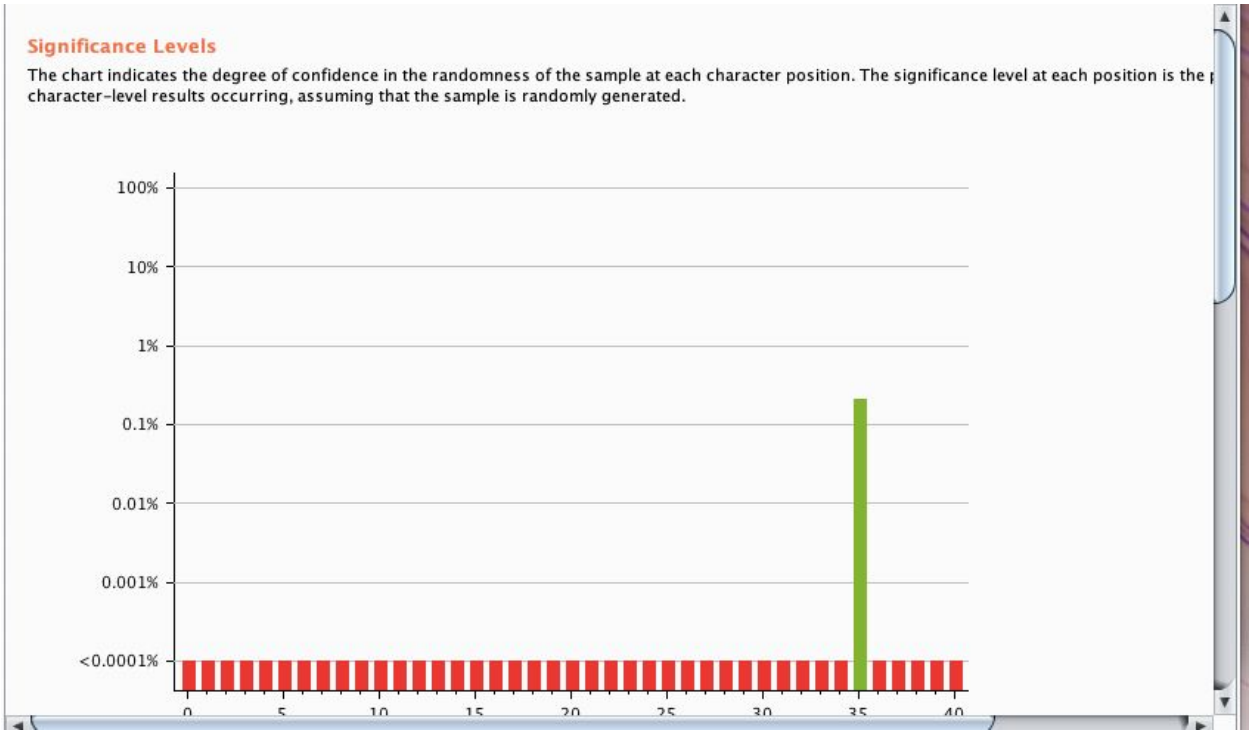
Reliability

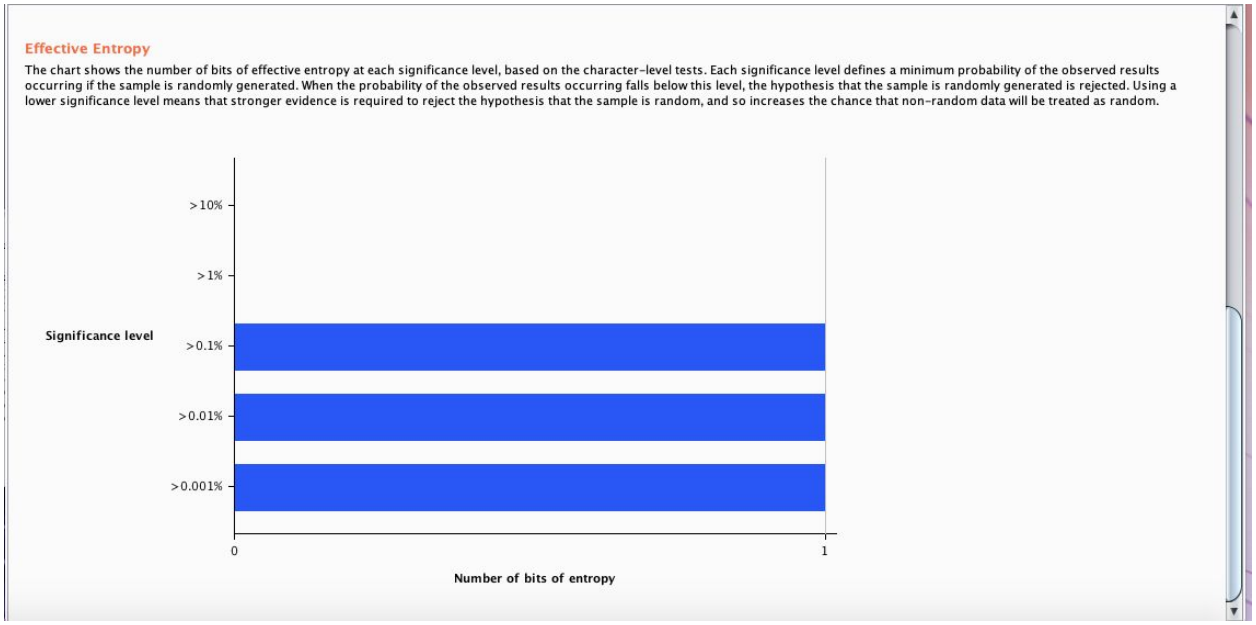
The analysis is based on a sample of 537 tokens. Based on the sample size, the reliability of the results is: poor.
Note that statistical tests provide only an indicative guide to the randomness of the sampled data. Results obtained may contain false positives and negatives, and may not correspond to the practical predictability of the tokens sampled.

Sample

Sample size: 537.
Token length: 41.

Character level analysis

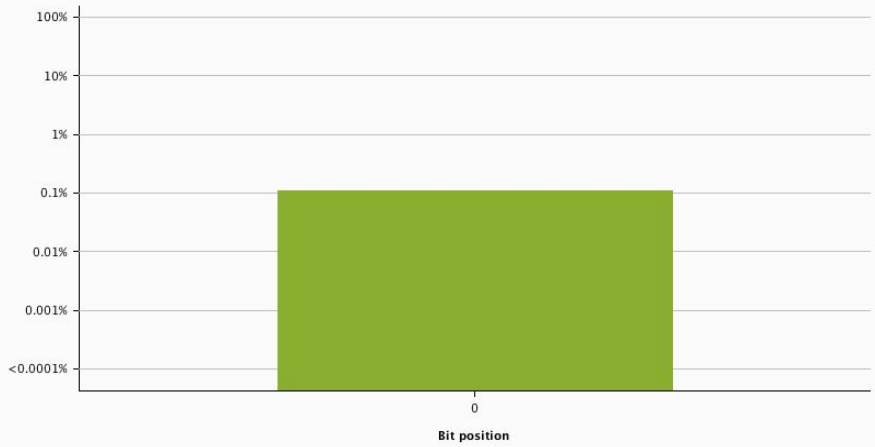




Bit level analysis

Significance Levels

The chart indicates the degree of confidence in the randomness of the sample at each bit position. The significance level at each position is the probability of the observed bit-level results occurring, assuming that the sample is randomly generated.



Effective Entropy

The chart shows the number of bits of effective entropy at each significance level, based on the bit-level tests. Each significance level defines a minimum probability of the observed results occurring if the sample is randomly generated. When the probability of the observed results occurring falls below this level, the hypothesis that the sample is random, and so increases the chance that non-random data will be treated as random.