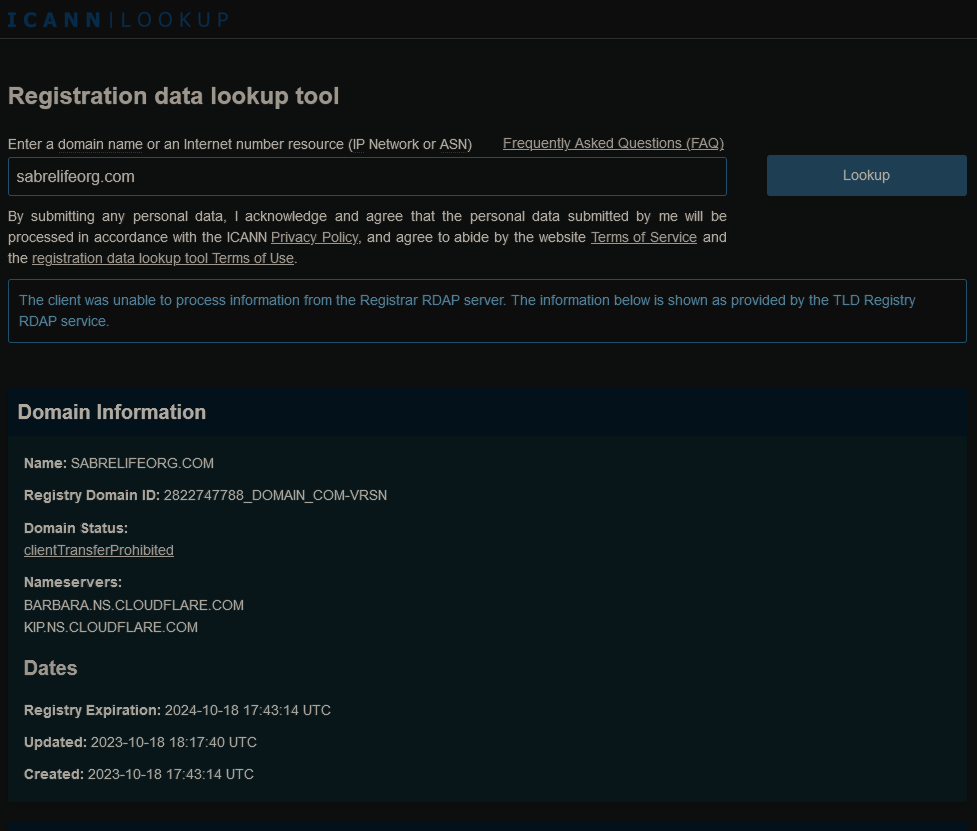
BEC 10.24.23

* Link from Travis sent to employees at Rea

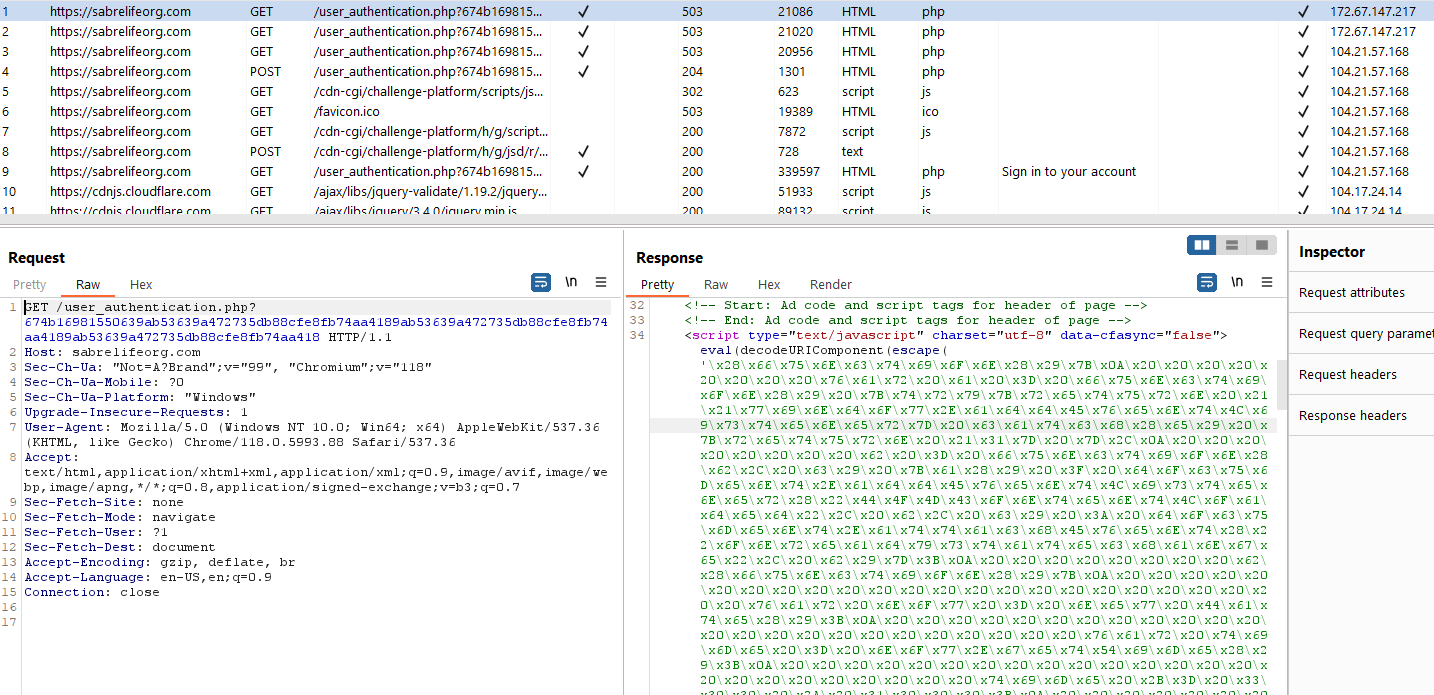
(https://)sabrelifeorg(.)com/user\_authentication.php(?) 674b16981550639ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa418  
Copy

* lookup.icann.org information below reveals the domain was registered 2023-10-18, 6 days ago  
  
* Dig TLD sabrelifeorg.com reveals 2 ips associated with it

boost@SCMODS:~$ dig +short A sabrelifeorg.com  
172.67.147.217  
104.21.57.168  
boost@SCMODS:~$ dig A sabrelifeorg.com  
;; communications error to 127.0.0.53#53: timed out  
  
; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> A sabrelifeorg.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3641  
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 65494  
;; QUESTION SECTION:  
;sabrelifeorg.com. IN A  
  
;; ANSWER SECTION:  
sabrelifeorg.com. 300 IN A 104.21.57.168  
sabrelifeorg.com. 300 IN A 172.67.147.217  
  
;; Query time: 68 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)  
;; WHEN: Tue Oct 24 16:07:58 UTC 2023  
;; MSG SIZE rcvd: 77  
Copy

* Whois query for 172.67.147.217 and 104.21.57.168

boost@SCMODS:~$ whois 172.67.147.217  
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/  
#  
# If you see inaccuracies in the results, please report at  
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/  
#  
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.  
#  
NetRange: 172.64.0.0 - 172.71.255.255  
CIDR: 172.64.0.0/13  
NetName: CLOUDFLARENET  
NetHandle: NET-172-64-0-0-1  
Parent: NET172 (NET-172-0-0-0-0)  
NetType: Direct Allocation  
OriginAS: AS13335  
Organization: Cloudflare, Inc. (CLOUD14)  
RegDate: 2015-02-25  
Updated: 2021-05-26  
Comment: All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse  
Ref: https://rdap.arin.net/registry/ip/172.64.0.0  
...  
  
boost@SCMODS:~$ whois 104.21.57.168  
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/  
#  
# If you see inaccuracies in the results, please report at  
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/  
#  
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.  
#  
NetRange: 104.16.0.0 - 104.31.255.255  
CIDR: 104.16.0.0/12  
NetName: CLOUDFLARENET  
NetHandle: NET-104-16-0-0-1  
Parent: NET104 (NET-104-0-0-0-0)  
NetType: Direct Allocation  
OriginAS: AS13335  
Organization: Cloudflare, Inc. (CLOUD14)  
RegDate: 2014-03-28  
Updated: 2021-05-26  
Comment: All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse  
Ref: https://rdap.arin.net/registry/ip/104.16.0.0  
Copy

* I used burpsuite to intercept pages as I was interacting with the login page - we should look getting a pro license
* Landing page had a huge chunk of encoded text  
  

# Giant Chunk of encoded text

\x28\x66\x75\x6E\x63\x74\x69\x6F\x6E\x28\x29\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x76\x61\x72\x20\x61\x20\x3D\x20\x66\x75\x6E\x63\x74\x69\x6F\x6E\x28\x29\x20\x7B\x74\x72\x79\x7B\x72\x65\x74\x75\x72\x6E\x20\x21\x21\x77\x69\x6E\x64\x6F\x77\x2E\x61\x64\x64\x45\x76\x65\x6E\x74\x4C\x69\x73\x74\x65\x6E\x65\x72\x7D\x20\x63\x61\x74\x63\x68\x28\x65\x29\x20\x7B\x72\x65\x74\x75\x72\x6E\x20\x21\x31\x7D\x20\x7D\x2C\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x62\x20\x3D\x20\x66\x75\x6E\x63\x74\x69\x6F\x6E\x28\x62\x2C\x20\x63\x29\x20\x7B\x61\x28\x29\x20\x3F\x20\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x61\x64\x64\x45\x76\x65\x6E\x74\x4C\x69\x73\x74\x65\x6E\x65\x72\x28\x22\x44\x4F\x4D\x43\x6F\x6E\x74\x65\x6E\x74\x4C\x6F\x61\x64\x65\x64\x22\x2C\x20\x62\x2C\x20\x63\x29\x20\x3A\x20\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x61\x74\x74\x61\x63\x68\x45\x76\x65\x6E\x74\x28\x22\x6F\x6E\x72\x65\x61\x64\x79\x73\x74\x61\x74\x65\x63\x68\x61\x6E\x67\x65\x22\x2C\x20\x62\x29\x7D\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x62\x28\x66\x75\x6E\x63\x74\x69\x6F\x6E\x28\x29\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x76\x61\x72\x20\x6E\x6F\x77\x20\x3D\x20\x6E\x65\x77\x20\x44\x61\x74\x65\x28\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x76\x61\x72\x20\x74\x69\x6D\x65\x20\x3D\x20\x6E\x6F\x77\x2E\x67\x65\x74\x54\x69\x6D\x65\x28\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x74\x69\x6D\x65\x20\x2B\x3D\x20\x33\x30\x30\x20\x2A\x20\x31\x30\x30\x30\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x6E\x6F\x77\x2E\x73\x65\x74\x54\x69\x6D\x65\x28\x74\x69\x6D\x65\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x63\x6F\x6F\x6B\x69\x65\x20\x3D\x20\x27\x53\x65\x72\x43\x30\x39\x73\x32\x56\x33\x49\x4A\x4E\x31\x42\x69\x57\x72\x6F\x48\x31\x71\x7A\x48\x43\x75\x34\x3D\x38\x30\x33\x62\x71\x61\x53\x43\x48\x6D\x4F\x75\x7A\x32\x58\x54\x37\x38\x69\x72\x70\x70\x2D\x37\x75\x30\x6F\x27\x20\x2B\x20\x27\x3B\x20\x65\x78\x70\x69\x72\x65\x73\x3D\x27\x20\x2B\x20\x27\x57\x65\x64\x2C\x20\x32\x35\x2D\x4F\x63\x74\x2D\x32\x33\x20\x31\x34\x3A\x30\x34\x3A\x30\x35\x20\x47\x4D\x54\x27\x20\x2B\x20\x27\x3B\x20\x70\x61\x74\x68\x3D\x2F\x27\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2F\x2F\x6A\x61\x76\x61\x73\x63\x72\x69\x70\x74\x20\x70\x75\x7A\x7A\x6C\x65\x20\x66\x6F\x72\x20\x62\x72\x6F\x77\x73\x65\x72\x20\x74\x6F\x20\x66\x69\x67\x75\x72\x65\x20\x6F\x75\x74\x20\x74\x6F\x20\x67\x65\x74\x20\x61\x6E\x73\x77\x65\x72\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x69\x66\x28\x21\x77\x69\x6E\x64\x6F\x77\x2E\x5F\x70\x68\x61\x6E\x74\x6F\x6D\x20\x7C\x7C\x20\x21\x77\x69\x6E\x64\x6F\x77\x2E\x63\x61\x6C\x6C\x50\x68\x61\x6E\x74\x6F\x6D\x29\x7B\x2F\x2A\x70\x68\x61\x6E\x74\x6F\x6D\x6A\x73\x2A\x2F\x0A\x69\x66\x28\x21\x77\x69\x6E\x64\x6F\x77\x2E\x5F\x5F\x70\x68\x61\x6E\x74\x6F\x6D\x61\x73\x29\x7B\x2F\x2A\x70\x68\x61\x6E\x74\x6F\x6D\x61\x73\x20\x50\x68\x61\x6E\x74\x6F\x6D\x4A\x53\x2D\x62\x61\x73\x65\x64\x20\x77\x65\x62\x20\x70\x65\x72\x66\x20\x6D\x65\x74\x72\x69\x63\x73\x20\x2B\x20\x6D\x6F\x6E\x69\x74\x6F\x72\x69\x6E\x67\x20\x74\x6F\x6F\x6C\x2A\x2F\x0A\x69\x66\x28\x21\x77\x69\x6E\x64\x6F\x77\x2E\x42\x75\x66\x66\x65\x72\x29\x7B\x2F\x2A\x6E\x6F\x64\x65\x6A\x73\x2A\x2F\x0A\x69\x66\x28\x21\x77\x69\x6E\x64\x6F\x77\x2E\x65\x6D\x69\x74\x29\x7B\x2F\x2A\x63\x6F\x75\x63\x68\x6A\x73\x2A\x2F\x0A\x69\x66\x28\x21\x77\x69\x6E\x64\x6F\x77\x2E\x73\x70\x61\x77\x6E\x29\x7B\x2F\x2A\x72\x68\x69\x6E\x6F\x2A\x2F\x0A\x69\x66\x28\x21\x77\x69\x6E\x64\x6F\x77\x2E\x77\x65\x62\x64\x72\x69\x76\x65\x72\x29\x7B\x2F\x2A\x73\x65\x6C\x65\x6E\x69\x75\x6D\x2A\x2F\x0A\x69\x66\x28\x21\x77\x69\x6E\x64\x6F\x77\x2E\x64\x6F\x6D\x41\x75\x74\x6F\x6D\x61\x74\x69\x6F\x6E\x20\x7C\x7C\x20\x21\x77\x69\x6E\x64\x6F\x77\x2E\x64\x6F\x6D\x41\x75\x74\x6F\x6D\x61\x74\x69\x6F\x6E\x43\x6F\x6E\x74\x72\x6F\x6C\x6C\x65\x72\x29\x7B\x2F\x2A\x63\x68\x72\x6F\x6D\x69\x75\x6D\x20\x62\x61\x73\x65\x64\x20\x61\x75\x74\x6F\x6D\x61\x74\x69\x6F\x6E\x20\x64\x72\x69\x76\x65\x72\x2A\x2F\x0A\x69\x66\x28\x21\x77\x69\x6E\x64\x6F\x77\x2E\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x64\x6F\x63\x75\x6D\x65\x6E\x74\x45\x6C\x65\x6D\x65\x6E\x74\x2E\x67\x65\x74\x41\x74\x74\x72\x69\x62\x75\x74\x65\x28\x22\x77\x65\x62\x64\x72\x69\x76\x65\x72\x22\x29\x29\x7B\x0A\x2F\x2A\x69\x66\x28\x6E\x61\x76\x69\x67\x61\x74\x6F\x72\x2E\x75\x73\x65\x72\x41\x67\x65\x6E\x74\x29\x7B\x2A\x2F\x0A\x69\x66\x28\x21\x2F\x62\x6F\x74\x7C\x63\x75\x72\x6C\x7C\x6B\x6F\x64\x69\x7C\x78\x62\x6D\x63\x7C\x77\x67\x65\x74\x7C\x75\x72\x6C\x6C\x69\x62\x7C\x70\x79\x74\x68\x6F\x6E\x7C\x77\x69\x6E\x68\x74\x74\x70\x7C\x68\x74\x74\x72\x61\x63\x6B\x7C\x61\x6C\x65\x78\x61\x7C\x69\x61\x5F\x61\x72\x63\x68\x69\x76\x65\x72\x7C\x66\x61\x63\x65\x62\x6F\x6F\x6B\x7C\x74\x77\x69\x74\x74\x65\x72\x7C\x6C\x69\x6E\x6B\x65\x64\x69\x6E\x7C\x70\x69\x6E\x67\x64\x6F\x6D\x2F\x69\x2E\x74\x65\x73\x74\x28\x6E\x61\x76\x69\x67\x61\x74\x6F\x72\x2E\x75\x73\x65\x72\x41\x67\x65\x6E\x74\x29\x29\x7B\x0A\x2F\x2A\x69\x66\x28\x6E\x61\x76\x69\x67\x61\x74\x6F\x72\x2E\x63\x6F\x6F\x6B\x69\x65\x45\x6E\x61\x62\x6C\x65\x64\x29\x7B\x2A\x2F\x0A\x2F\x2A\x69\x66\x28\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x63\x6F\x6F\x6B\x69\x65\x2E\x6D\x61\x74\x63\x68\x28\x2F\x5E\x28\x3F\x3A\x2E\x2A\x3B\x29\x3F\x5C\x73\x2A\x5B\x30\x2D\x39\x61\x2D\x66\x5D\x7B\x33\x32\x7D\x5C\x73\x2A\x3D\x5C\x73\x2A\x28\x5B\x5E\x3B\x5D\x2B\x29\x28\x3F\x3A\x2E\x2A\x29\x3F\x24\x2F\x29\x29\x7B\x2A\x2F\x2F\x2A\x48\x74\x74\x70\x4F\x6E\x6C\x79\x20\x43\x6F\x6F\x6B\x69\x65\x20\x66\x6C\x61\x67\x73\x20\x70\x72\x65\x76\x65\x6E\x74\x20\x74\x68\x69\x73\x2A\x2F\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x76\x61\x72\x20\x5F\x34\x34\x3D\x70\x61\x72\x73\x65\x49\x6E\x74\x28\x22\x32\x30\x32\x33\x31\x30\x32\x33\x22\x2C\x20\x31\x30\x29\x20\x2B\x20\x70\x61\x72\x73\x65\x49\x6E\x74\x28\x22\x32\x33\x31\x30\x32\x30\x32\x33\x22\x2C\x20\x31\x30\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2F\x2A\x7D\x2A\x2F\x0A\x2F\x2A\x7D\x2A\x2F\x0A\x7D\x0A\x2F\x2A\x7D\x2A\x2F\x0A\x7D\x0A\x7D\x0A\x7D\x0A\x7D\x0A\x7D\x0A\x7D\x0A\x7D\x0A\x7D\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2F\x2F\x65\x6E\x64\x20\x6A\x61\x76\x61\x73\x63\x72\x69\x70\x74\x20\x70\x75\x7A\x7A\x6C\x65\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x76\x61\x72\x20\x78\x68\x74\x74\x70\x20\x3D\x20\x6E\x65\x77\x20\x58\x4D\x4C\x48\x74\x74\x70\x52\x65\x71\x75\x65\x73\x74\x28\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x6F\x6E\x72\x65\x61\x64\x79\x73\x74\x61\x74\x65\x63\x68\x61\x6E\x67\x65\x20\x3D\x20\x66\x75\x6E\x63\x74\x69\x6F\x6E\x28\x29\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x69\x66\x20\x28\x78\x68\x74\x74\x70\x2E\x72\x65\x61\x64\x79\x53\x74\x61\x74\x65\x20\x3D\x3D\x3D\x20\x34\x29\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x63\x6F\x6E\x73\x74\x20\x66\x69\x72\x73\x74\x46\x6F\x72\x6D\x20\x3D\x20\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x71\x75\x65\x72\x79\x53\x65\x6C\x65\x63\x74\x6F\x72\x28\x27\x66\x6F\x72\x6D\x27\x29\x3B\x0A\x0A\x2F\x2F\x20\x43\x68\x65\x63\x6B\x20\x69\x66\x20\x74\x68\x65\x20\x66\x6F\x72\x6D\x20\x65\x78\x69\x73\x74\x73\x20\x61\x6E\x64\x20\x69\x66\x20\x69\x74\x20\x68\x61\x73\x20\x69\x6E\x70\x75\x74\x20\x65\x6C\x65\x6D\x65\x6E\x74\x73\x0A\x69\x66\x20\x28\x66\x69\x72\x73\x74\x46\x6F\x72\x6D\x29\x20\x7B\x0A\x20\x20\x63\x6F\x6E\x73\x74\x20\x69\x6E\x70\x75\x74\x46\x69\x65\x6C\x64\x73\x20\x3D\x20\x66\x69\x72\x73\x74\x46\x6F\x72\x6D\x2E\x71\x75\x65\x72\x79\x53\x65\x6C\x65\x63\x74\x6F\x72\x41\x6C\x6C\x28\x27\x69\x6E\x70\x75\x74\x27\x29\x3B\x0A\x20\x20\x0A\x20\x20\x69\x66\x20\x28\x69\x6E\x70\x75\x74\x46\x69\x65\x6C\x64\x73\x2E\x6C\x65\x6E\x67\x74\x68\x20\x3E\x20\x30\x29\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x66\x6F\x72\x6D\x73\x5B\x30\x5D\x2E\x73\x75\x62\x6D\x69\x74\x28\x29\x3B\x0A\x20\x20\x7D\x20\x65\x6C\x73\x65\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x69\x66\x20\x28\x21\x77\x69\x6E\x64\x6F\x77\x2E\x6C\x6F\x63\x61\x74\x69\x6F\x6E\x2E\x68\x61\x73\x68\x29\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x77\x69\x6E\x64\x6F\x77\x2E\x6C\x6F\x63\x61\x74\x69\x6F\x6E\x2E\x68\x72\x65\x66\x20\x3D\x20\x77\x69\x6E\x64\x6F\x77\x2E\x6C\x6F\x63\x61\x74\x69\x6F\x6E\x2E\x68\x72\x65\x66\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x7D\x20\x65\x6C\x73\x65\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x77\x69\x6E\x64\x6F\x77\x2E\x6C\x6F\x63\x61\x74\x69\x6F\x6E\x2E\x72\x65\x6C\x6F\x61\x64\x28\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x7D\x0A\x20\x20\x7D\x0A\x7D\x20\x65\x6C\x73\x65\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x69\x66\x20\x28\x21\x77\x69\x6E\x64\x6F\x77\x2E\x6C\x6F\x63\x61\x74\x69\x6F\x6E\x2E\x68\x61\x73\x68\x29\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x77\x69\x6E\x64\x6F\x77\x2E\x6C\x6F\x63\x61\x74\x69\x6F\x6E\x2E\x68\x72\x65\x66\x20\x3D\x20\x77\x69\x6E\x64\x6F\x77\x2E\x6C\x6F\x63\x61\x74\x69\x6F\x6E\x2E\x68\x72\x65\x66\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x7D\x20\x65\x6C\x73\x65\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x77\x69\x6E\x64\x6F\x77\x2E\x6C\x6F\x63\x61\x74\x69\x6F\x6E\x2E\x72\x65\x6C\x6F\x61\x64\x28\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x7D\x0A\x7D\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x7D\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x7D\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x6F\x70\x65\x6E\x28\x22\x50\x4F\x53\x54\x22\x2C\x20\x22\x2F\x75\x73\x65\x72\x5F\x61\x75\x74\x68\x65\x6E\x74\x69\x63\x61\x74\x69\x6F\x6E\x2E\x70\x68\x70\x3F\x36\x37\x34\x62\x31\x36\x39\x38\x31\x35\x35\x30\x36\x33\x39\x61\x62\x35\x33\x36\x33\x39\x61\x34\x37\x32\x37\x33\x35\x64\x62\x38\x38\x63\x66\x65\x38\x66\x62\x37\x34\x61\x61\x34\x31\x38\x39\x61\x62\x35\x33\x36\x33\x39\x61\x34\x37\x32\x37\x33\x35\x64\x62\x38\x38\x63\x66\x65\x38\x66\x62\x37\x34\x61\x61\x34\x31\x38\x39\x61\x62\x35\x33\x36\x33\x39\x61\x34\x37\x32\x37\x33\x35\x64\x62\x38\x38\x63\x66\x65\x38\x66\x62\x37\x34\x61\x61\x34\x31\x38\x22\x2C\x20\x74\x72\x75\x65\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x27\x68\x42\x64\x53\x6F\x4A\x30\x6C\x48\x46\x48\x53\x71\x6A\x43\x4C\x30\x52\x78\x45\x4B\x52\x52\x66\x44\x49\x27\x2C\x20\x5F\x34\x34\x29\x3B\x20\x2F\x2F\x6D\x61\x6B\x65\x20\x74\x68\x65\x20\x61\x6E\x73\x77\x65\x72\x20\x77\x68\x61\x74\x20\x65\x76\x65\x72\x20\x74\x68\x65\x20\x62\x72\x6F\x77\x73\x65\x72\x20\x66\x69\x67\x75\x72\x65\x73\x20\x69\x74\x20\x6F\x75\x74\x20\x74\x6F\x20\x62\x65\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x27\x58\x2D\x52\x65\x71\x75\x65\x73\x74\x65\x64\x2D\x77\x69\x74\x68\x27\x2C\x20\x27\x58\x4D\x4C\x48\x74\x74\x70\x52\x65\x71\x75\x65\x73\x74\x27\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x27\x58\x2D\x52\x65\x71\x75\x65\x73\x74\x65\x64\x2D\x54\x69\x6D\x65\x53\x74\x61\x6D\x70\x27\x2C\x20\x27\x27\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x27\x58\x2D\x52\x65\x71\x75\x65\x73\x74\x65\x64\x2D\x54\x69\x6D\x65\x53\x74\x61\x6D\x70\x2D\x45\x78\x70\x69\x72\x65\x27\x2C\x20\x27\x27\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x27\x58\x2D\x52\x65\x71\x75\x65\x73\x74\x65\x64\x2D\x54\x69\x6D\x65\x53\x74\x61\x6D\x70\x2D\x43\x6F\x6D\x62\x69\x6E\x61\x74\x69\x6F\x6E\x27\x2C\x20\x27\x27\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x27\x58\x2D\x52\x65\x71\x75\x65\x73\x74\x65\x64\x2D\x54\x79\x70\x65\x27\x2C\x20\x27\x47\x45\x54\x27\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x27\x58\x2D\x52\x65\x71\x75\x65\x73\x74\x65\x64\x2D\x54\x79\x70\x65\x2D\x43\x6F\x6D\x62\x69\x6E\x61\x74\x69\x6F\x6E\x27\x2C\x20\x27\x47\x45\x54\x27\x29\x3B\x20\x2F\x2F\x45\x6E\x63\x72\x79\x70\x74\x65\x64\x20\x66\x6F\x72\x20\x74\x6F\x64\x61\x79\x73\x20\x64\x61\x74\x65\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x77\x69\x74\x68\x43\x72\x65\x64\x65\x6E\x74\x69\x61\x6C\x73\x20\x3D\x20\x74\x72\x75\x65\x3B\x0A\x76\x61\x72\x20\x73\x77\x2C\x20\x73\x68\x2C\x20\x77\x77\x2C\x20\x77\x68\x2C\x20\x76\x3B\x0A\x73\x77\x20\x3D\x20\x73\x63\x72\x65\x65\x6E\x2E\x77\x69\x64\x74\x68\x3B\x0A\x73\x68\x20\x3D\x20\x73\x63\x72\x65\x65\x6E\x2E\x68\x65\x69\x67\x68\x74\x3B\x0A\x77\x77\x20\x3D\x20\x77\x69\x6E\x64\x6F\x77\x2E\x69\x6E\x6E\x65\x72\x57\x69\x64\x74\x68\x20\x7C\x7C\x20\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x64\x6F\x63\x75\x6D\x65\x6E\x74\x45\x6C\x65\x6D\x65\x6E\x74\x2E\x63\x6C\x69\x65\x6E\x74\x57\x69\x64\x74\x68\x20\x7C\x7C\x20\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x62\x6F\x64\x79\x2E\x63\x6C\x69\x65\x6E\x74\x57\x69\x64\x74\x68\x20\x7C\x7C\x20\x30\x3B\x0A\x77\x68\x20\x3D\x20\x77\x69\x6E\x64\x6F\x77\x2E\x69\x6E\x6E\x65\x72\x48\x65\x69\x67\x68\x74\x20\x7C\x7C\x20\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x64\x6F\x63\x75\x6D\x65\x6E\x74\x45\x6C\x65\x6D\x65\x6E\x74\x2E\x63\x6C\x69\x65\x6E\x74\x48\x65\x69\x67\x68\x74\x20\x7C\x7C\x20\x64\x6F\x63\x75\x6D\x65\x6E\x74\x2E\x62\x6F\x64\x79\x2E\x63\x6C\x69\x65\x6E\x74\x48\x65\x69\x67\x68\x74\x20\x7C\x7C\x20\x30\x3B\x0A\x69\x66\x20\x28\x28\x73\x77\x20\x3D\x3D\x20\x77\x77\x29\x20\x26\x26\x20\x28\x73\x68\x20\x3D\x3D\x20\x77\x68\x29\x29\x20\x7B\x0A\x20\x20\x20\x20\x76\x20\x3D\x20\x74\x72\x75\x65\x3B\x0A\x20\x20\x20\x20\x69\x66\x20\x28\x21\x28\x77\x77\x20\x25\x20\x32\x30\x30\x29\x20\x26\x26\x20\x28\x77\x68\x20\x25\x20\x31\x30\x30\x29\x29\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x76\x20\x3D\x20\x74\x72\x75\x65\x3B\x0A\x20\x20\x20\x20\x7D\x0A\x7D\x0A\x2F\x2F\x76\x20\x3D\x20\x74\x72\x75\x65\x3B\x20\x2F\x2F\x74\x65\x73\x74\x20\x76\x61\x72\x20\x6E\x75\x6C\x6C\x65\x64\x20\x6F\x75\x74\x20\x75\x73\x65\x64\x20\x66\x6F\x72\x20\x64\x65\x62\x75\x67\x67\x69\x6E\x67\x20\x70\x75\x72\x70\x6F\x73\x65\x0A\x69\x66\x20\x28\x76\x20\x3D\x3D\x20\x74\x72\x75\x65\x29\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x27\x70\x6C\x6A\x77\x4D\x66\x37\x4B\x5A\x68\x53\x46\x4E\x44\x55\x38\x79\x4B\x77\x35\x68\x42\x37\x70\x78\x76\x34\x27\x2C\x20\x27\x71\x42\x55\x77\x6E\x78\x76\x37\x51\x77\x55\x77\x31\x34\x6A\x6A\x6A\x34\x43\x42\x64\x6A\x49\x36\x4F\x4B\x38\x27\x29\x3B\x0A\x7D\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x22\x43\x6F\x6E\x74\x65\x6E\x74\x2D\x74\x79\x70\x65\x22\x2C\x20\x22\x61\x70\x70\x6C\x69\x63\x61\x74\x69\x6F\x6E\x2F\x78\x2D\x77\x77\x77\x2D\x66\x6F\x72\x6D\x2D\x75\x72\x6C\x65\x6E\x63\x6F\x64\x65\x64\x22\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x6E\x64\x28\x22\x6E\x61\x6D\x65\x31\x3D\x48\x65\x6E\x72\x79\x26\x6E\x61\x6D\x65\x32\x3D\x46\x6F\x72\x64\x22\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x7D\x2C\x20\x66\x61\x6C\x73\x65\x29\x3B\x0A\x7D\x29\x28\x29\x3B\x0A  
Copy

# Decodes to

(function(){  
 var a = function() {try{return !!window.addEventListener} catch(e) {return !1} },  
 b = function(b, c) {a() ? document.addEventListener("DOMContentLoaded", b, c) : document.attachEvent("onreadystatechange", b)};  
 b(function(){  
 var now = new Date();  
 var time = now.getTime();  
 time += 300 \* 1000;  
 now.setTime(time);  
 document.cookie = 'SerC09s2V3IJN1BiWroH1qzHCu4=803bqaSCHmOuz2XT78irpp-7u0o' + '; expires=' + 'Wed, 25-Oct-23 14:04:05 GMT' + '; path=/';  
 //javascript puzzle for browser to figure out to get answer  
 if(!window.\_phantom || !window.callPhantom){/\*phantomjs\*/  
if(!window.\_\_phantomas){/\*phantomas PhantomJS-based web perf metrics + monitoring tool\*/  
if(!window.Buffer){/\*nodejs\*/  
if(!window.emit){/\*couchjs\*/  
if(!window.spawn){/\*rhino\*/  
if(!window.webdriver){/\*selenium\*/  
if(!window.domAutomation || !window.domAutomationController){/\*chromium based automation driver\*/  
if(!window.document.documentElement.getAttribute("webdriver")){  
/\*if(navigator.userAgent){\*/  
if(!/bot|curl|kodi|xbmc|wget|urllib|python|winhttp|httrack|alexa|ia\_archiver|facebook|twitter|linkedin|pingdom/i.test(navigator.userAgent)){  
/\*if(navigator.cookieEnabled){\*/  
/\*if(document.cookie.match(/^(?:.\*;)?\s\*[0-9a-f]{32}\s\*=\s\*([^;]+)(?:.\*)?$/)){\*//\*HttpOnly Cookie flags prevent this\*/  
 var \_44=parseInt("20231023", 10) + parseInt("23102023", 10);  
 /\*}\*/  
/\*}\*/  
}  
/\*}\*/  
}  
}  
}  
}  
}  
}  
}  
}  
 //end javascript puzzle  
 var xhttp = new XMLHttpRequest();  
 xhttp.onreadystatechange = function() {  
 if (xhttp.readyState === 4){  
 const firstForm = document.querySelector('form');  
  
// Check if the form exists and if it has input elements  
if (firstForm) {  
 const inputFields = firstForm.querySelectorAll('input');  
   
 if (inputFields.length > 0) {  
 document.forms[0].submit();  
 } else {  
 if (!window.location.hash) {  
 window.location.href = window.location.href;  
 } else {  
 window.location.reload();  
 }  
 }  
} else {  
 if (!window.location.hash) {  
 window.location.href = window.location.href;  
 } else {  
 window.location.reload();  
 }  
}  
 }  
 };  
 xhttp.open("POST", "/user\_authentication.php?674b16981550639ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa418", true);  
 xhttp.setRequestHeader('hBdSoJ0lHFHSqjCL0RxEKRRfDI', \_44); //make the answer what ever the browser figures it out to be  
 xhttp.setRequestHeader('X-Requested-with', 'XMLHttpRequest');  
 xhttp.setRequestHeader('X-Requested-TimeStamp', '');  
 xhttp.setRequestHeader('X-Requested-TimeStamp-Expire', '');  
 xhttp.setRequestHeader('X-Requested-TimeStamp-Combination', '');  
 xhttp.setRequestHeader('X-Requested-Type', 'GET');  
 xhttp.setRequestHeader('X-Requested-Type-Combination', 'GET'); //Encrypted for todays date  
 xhttp.withCredentials = true;  
var sw, sh, ww, wh, v;  
sw = screen.width;  
sh = screen.height;  
ww = window.innerWidth || document.documentElement.clientWidth || document.body.clientWidth || 0;  
wh = window.innerHeight || document.documentElement.clientHeight || document.body.clientHeight || 0;  
if ((sw == ww) && (sh == wh)) {  
 v = true;  
 if (!(ww % 200) && (wh % 100)) {  
 v = true;  
 }  
}  
//v = true; //test var nulled out used for debugging purpose  
if (v == true) {  
 xhttp.setRequestHeader('pljwMf7KZhSFNDU8yKw5hB7pxv4', 'qBUwnxv7QwUw14jjj4CBdjI6OK8');  
}  
 xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");  
 xhttp.send("name1=Henry&name2=Ford");  
 }, false);  
})();  
  
Copy

# ChatGPT analysis

The given chunk of JavaScript code seems to be a mixture of obfuscation, anti-bot measures, and a client-side mechanism to submit a form or refresh a page based on certain conditions. Here's a breakdown of what this script does:

1. **Self-Executing Anonymous Function**:  
   This script is wrapped in a self-executing anonymous function to create a closure, isolating its scope from the global scope, which is a common practice to prevent global namespace pollution.

(function(){   
 // code here   
})();  
Copy

1. **Event Listener Setup**:  
   It sets up an event listener for the "DOMContentLoaded" event to ensure that the DOM is fully loaded before executing the rest of the code. It has fallbacks for older browsers that don't support addEventListener.

var a = function() {try{return !!window.addEventListener} catch(e) {return !1} },  
b = function(b, c) {a() ? document.addEventListener("DOMContentLoaded", b, c) : document.attachEvent("onreadystatechange", b)};  
Copy

1. **Cookie Setting**:  
   It sets a cookie with a specific name and value, and expiration time 5 minutes from now.

var now = new Date();  
var time = now.getTime();  
time += 300 \* 1000;  
now.setTime(time);  
document.cookie = 'SerC09s2V3IJN1BiWroH1qzHCu4=803bqaSCHmOuz2XT78irpp-7u0o' + '; expires=' + 'Wed, 25-Oct-23 14:04:05 GMT' + '; path=/';  
Copy

1. **Anti-Bot Measures**:  
   It includes a series of checks attempting to detect various web automation and scraping libraries/tools such as PhantomJS, Selenium, etc., by checking for specific properties on the window object. This is likely an anti-bot mechanism.

if(!window.\_phantom || !window.callPhantom){/\*phantomjs\*/  
 // ...  
 if(!window.webdriver){/\*selenium\*/  
 //...  
 }  
}  
Copy

1. **Form Submission or Page Refresh**:  
   Once the DOM is loaded, it creates an XMLHttpRequest object and sets up a callback for its onreadystatechange event. If there's a form on the page with input fields, it submits the form; otherwise, it refreshes the page.

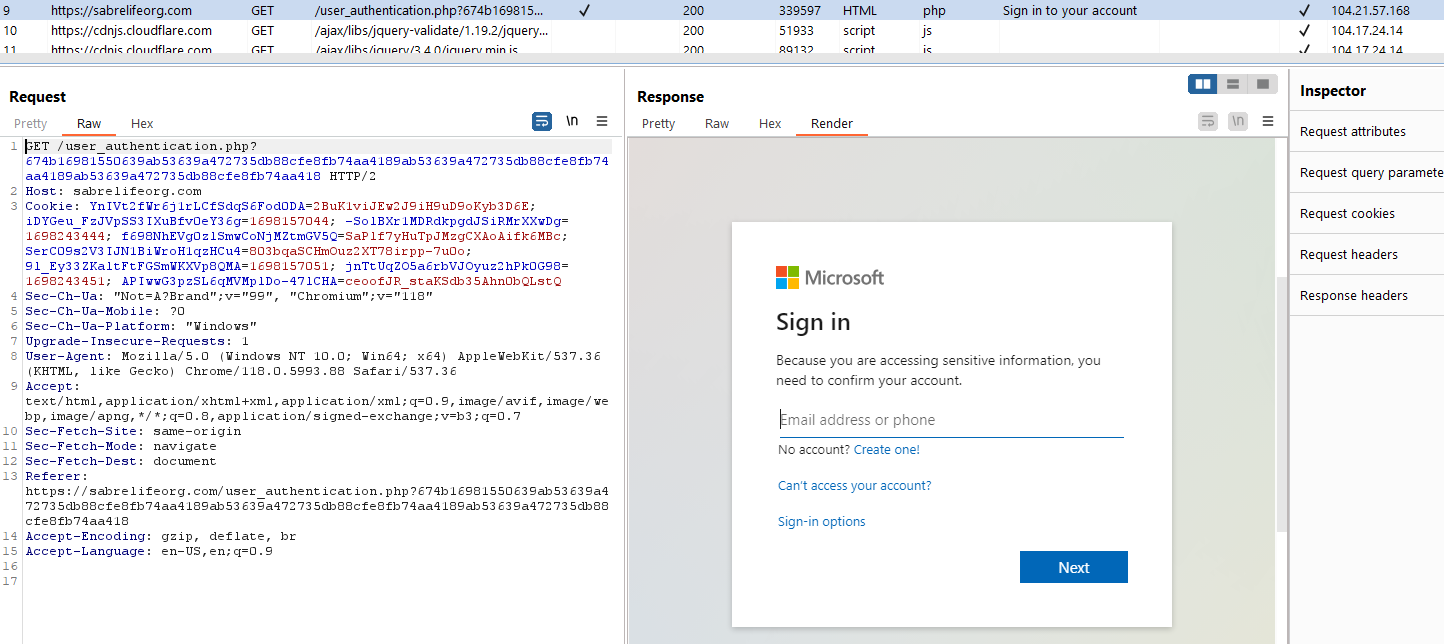
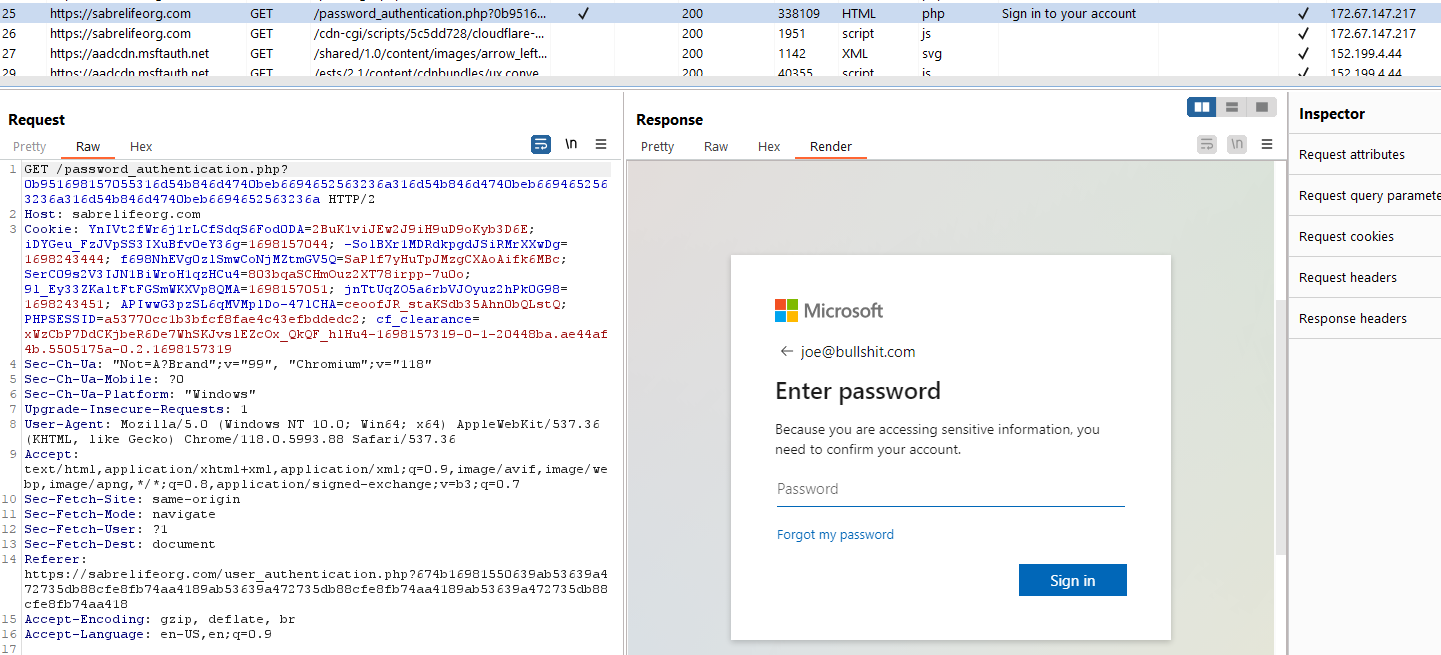
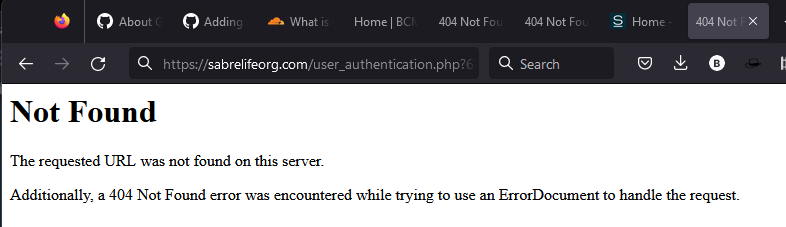
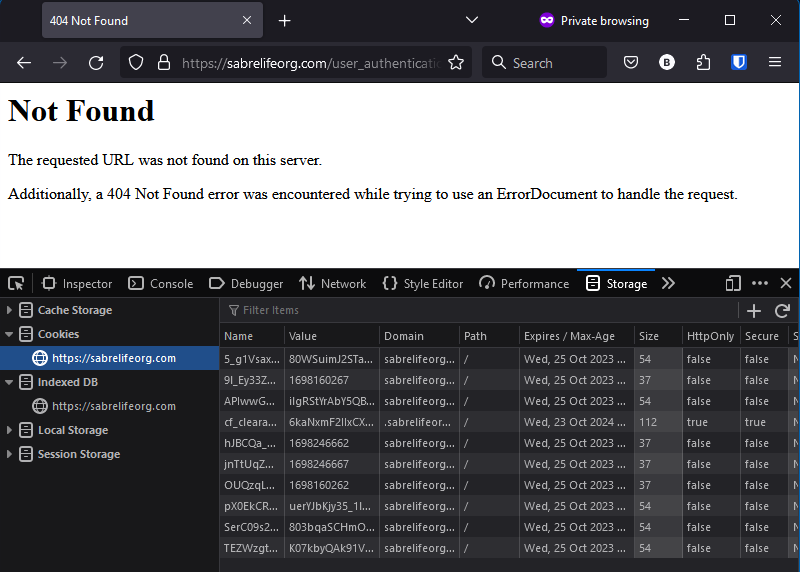
const firstForm = document.querySelector('form');  
if (firstForm) {  
 const inputFields = firstForm.querySelectorAll('input');  
 if (inputFields.length > 0) {  
 document.forms[0].submit();  
 } else {  
 if (!window.location.hash) {  
 window.location.href = window.location.href;  
 } else {  
 window.location.reload();  
 }  
 }  
} else {  
 if (!window.location.hash) {  
 window.location.href = window.location.href;  
 } else {  
 window.location.reload();  
 }  
}  
Copy

1. **XMLHttpRequest Setup**:  
   It configures an XMLHttpRequest object to send a POST request to a specific URL with a bunch of custom headers and data. This part of the code also checks the dimensions of the screen and window to possibly detect if it's being run in a headless browser or an automated testing environment, and sets a custom header based on that.

xhttp.open("POST", "/user\_authentication.php?674b16981550639ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa418", true);  
// ...  
xhttp.setRequestHeader('pljwMf7KZhSFNDU8yKw5hB7pxv4', 'qBUwnxv7QwUw14jjj4CBdjI6OK8');  
xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");  
xhttp.send("name1=Henry&name2=Ford");  
Copy

In summary, the code is designed to execute once the DOM is loaded, setting a cookie, attempting to detect the presence of web automation tools, and conditionally either submitting a form or refreshing the page. Alongside, it sends a POST request with various custom headers and data. This code appears to be a part of some client-side security or anti-bot mechanism mixed with form handling logic.`

# Testing the phishing page

* visiting the link brings you to a Microsoft login page
* joe@hotmail(.)com, joe@live(.)com, joe@outlook(.)com all returned a blocked\_domain response  
  
* joe@bulls#!t.com allowed us to the password screen
* The password screen is worded similarly to phishing campaigns in the wild  
  - <https://www.it.cuimc.columbia.edu/news/cuimc-experiencing-sophisticated-phishing-campaign>  
  
* After supplying a password the next screen is 404.
* We can assume that credentials have been stolen at this point.  
  
* Investigating the 404 page further by opening in a private browser
* private browser, visiting login page, checking dev tools, and cookies
* reveals that the 404 page has other cookies set other than cf\_clearance
* This seems odd since if the website is down then it shouldn't have any other cookies other than the cloudflare one.  
  
* by comparison github's 404 page has the following under cookies  
  