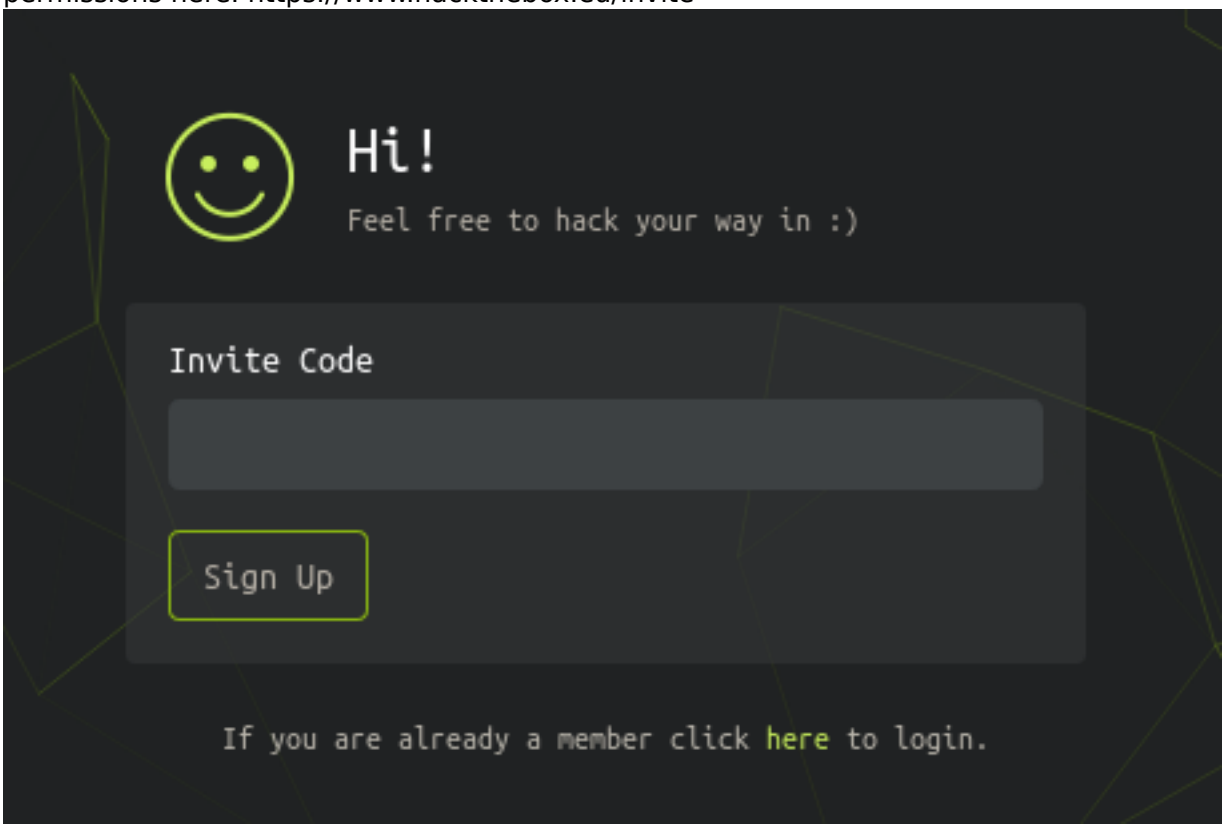
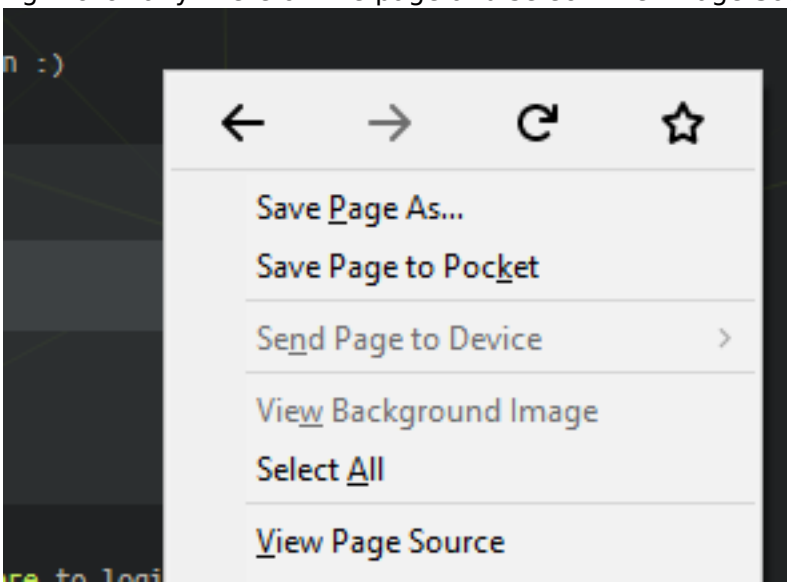
# *Get HTB Invite Code*

To join HackTheBox and have access to their labs you need to hack your way in by generating your own invite code. Do not ever attempt these strategies on sites in which you do not have permission. HackTheBox gives us permissions here. https://www.hackthebox.eu/invite



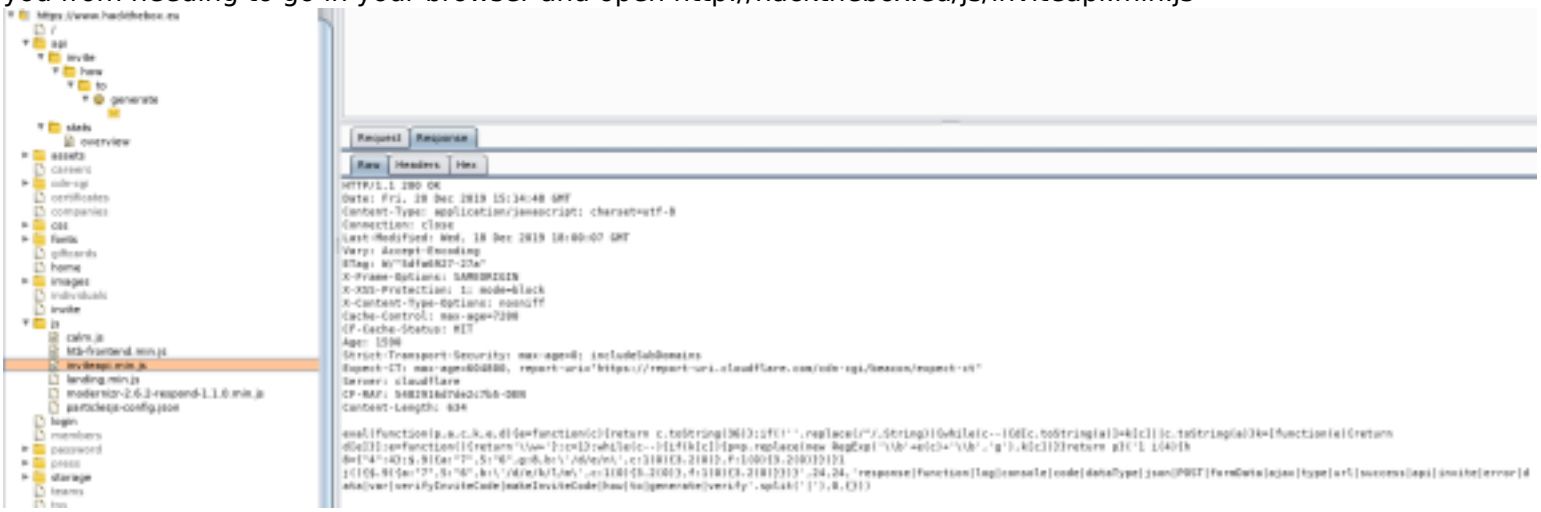

One of the first things we want to do when hacking a site is view the source code to see how it works. In FireFox right click anywhere on the page and select "View Page Source" or "Inspect Element"



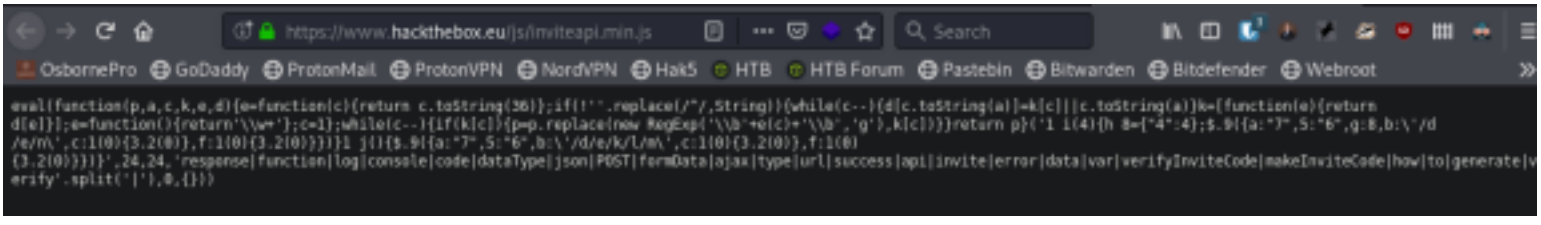

In the source code of the page we see an API is a part of the invite code generation process. We can see a javascript (.js) file is referenced on the page. Its name is /js/inviteapi.min.js

```
<html lang="en"> event
 <head> ··· </head>
 <body class="blank" style="overflow-y:hidden; ">
  <script> ··· </script>
  <div class="wrapper">
   <section class="content" style="margin:0px; padding:0px;">
    ::before
    <div class="container-center centerbox"> ··· </div>
    <div id="particles-js" class="particles_full">
     <canvas class="particles-js-canvas-el" style="width: 100%; height: 100%;'
    </div>
   </section>
  </div>
  <script src="https://www.hackthebox.eu/js/htb-frontend.min.js"></script>
  <script defer="" src="/js/inviteapi.min.js"></script>
  <script defer="" src="https://www.hackthebox.eu/js/calm.js"></script>
 </body>
</html>
```

Newbies most likely will not have BurpSuite catching traffic yet. If you do have your Burp Proxy configured you can add HackTheBox to your scope in the Target - Site Map tabs. We can see by looking in the JS URI directory is the inviteapi.min.js file. We can view the Request and Response in the bottom right hand window. This will save you from needing to go in your browser and open http://hackthebox.eu/js/inviteapi.min.js



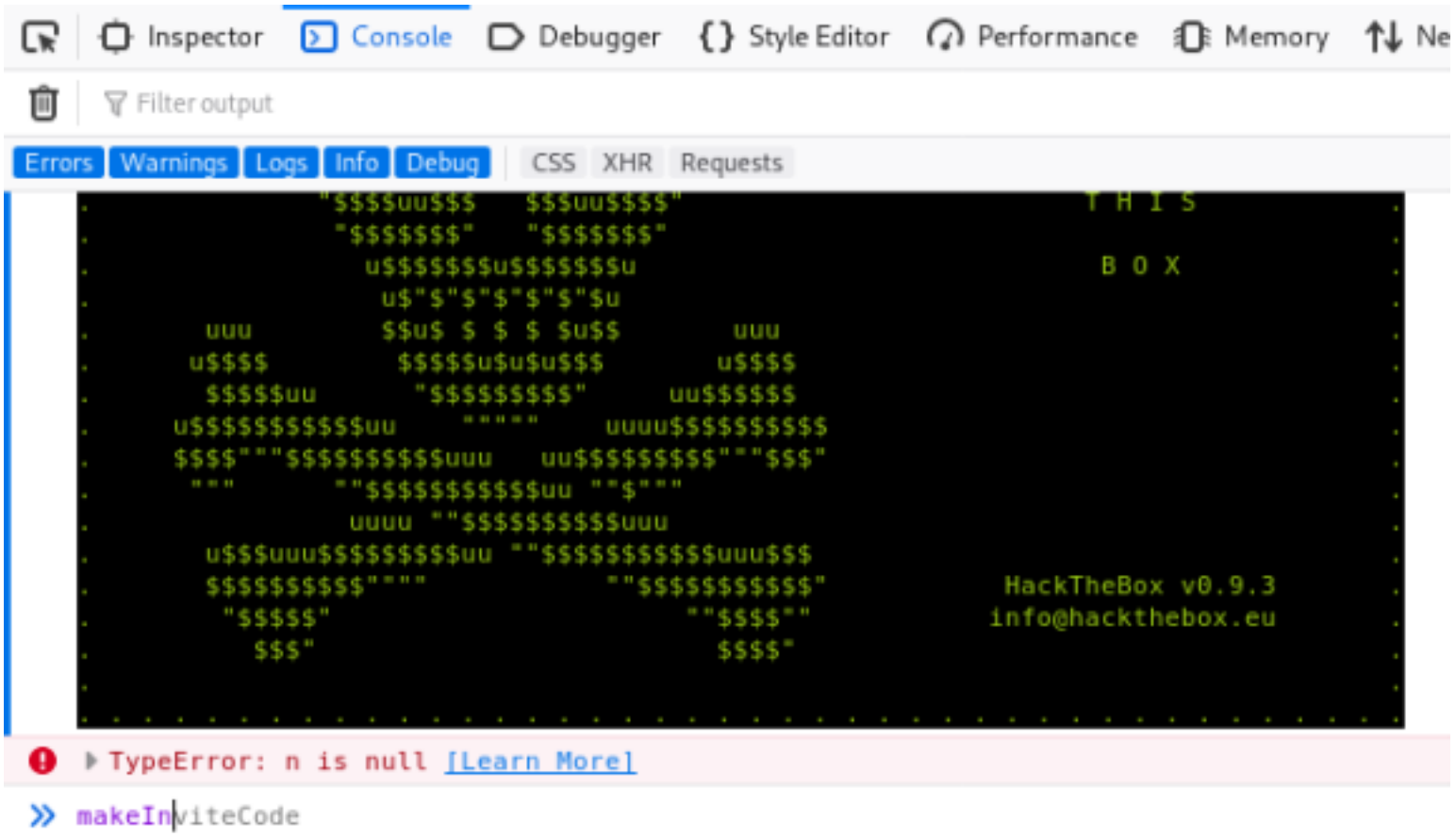
We are going to that site anyway to be thorough as this will be a short write up. We can see visiting that site shows us the same content as above



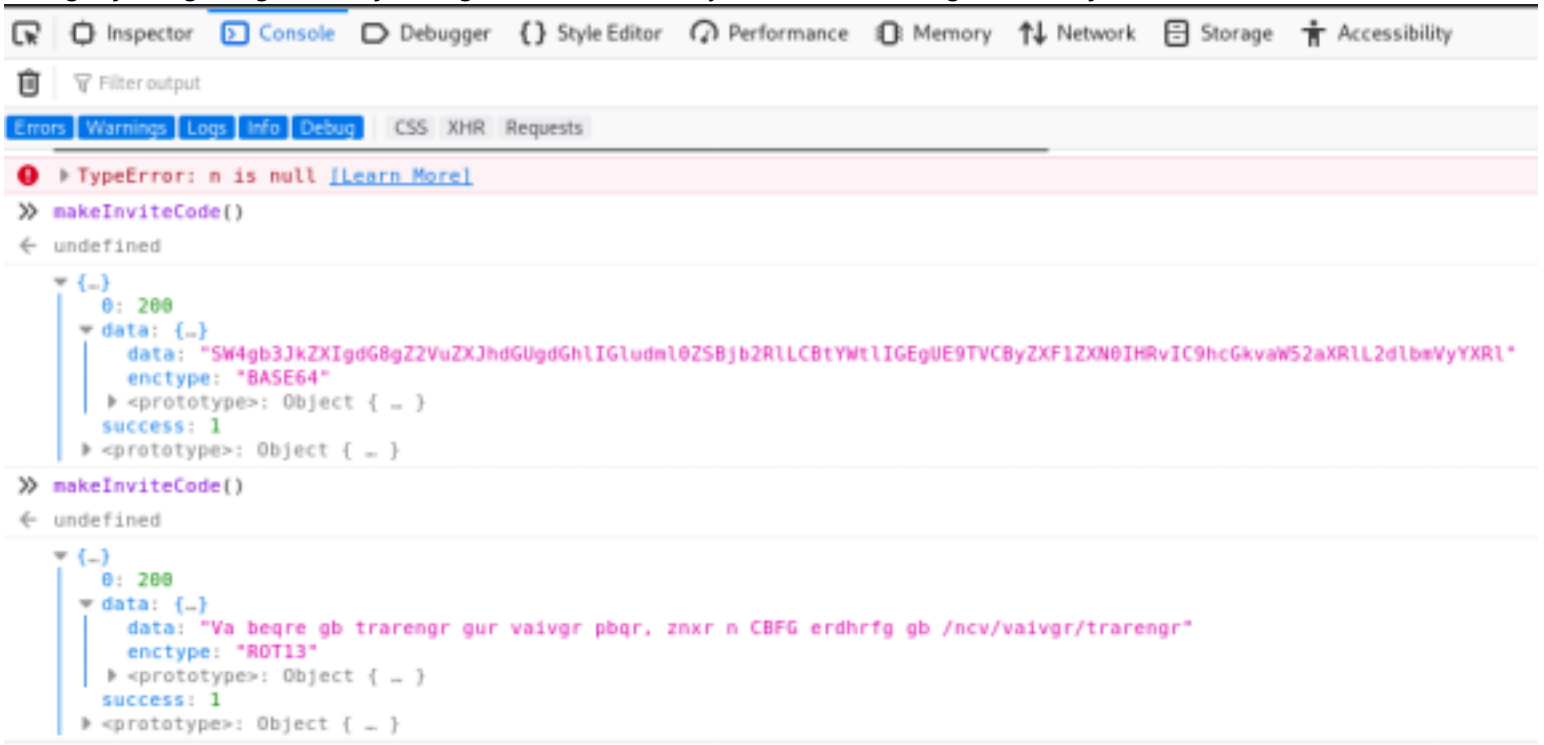

We can see the different functions that exist. MakeInviteCode sure looks like something we are going to want to do.
We can execute this function by going to the Console tab of the Inspect Element window.
(NOTE: This is done at this site: https://www.hackthebox.eu/invite )

You can see below I started typing makeInviteCode which the console recognized and autocompleted for me. This is javascript so in order to execute that function we will need to make the command in the console this....

```
makeInviteCode()
```




Below we can see the results of executing that function. This shows us a Base64 encoded string.
Sometimes this string is encoded using ROT13
ROT13: Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /ncv/vaivgr/trarengr
BASE64:
SW4gb3JkZXIgdG8gZ2VuZXJhdGUgdGhlIGludml0ZSBjb2RlLCBtYWtlIGEgUE9TVCByZXF1ZXN0IHRvIC9hcGkvaW52aXRlL2dlbmVyYXRl



This site can be used to decode and encode base64
RESOURCE: https://www.base64decode.org/

We can decode base64 using the terminal as well.

```
echo
'SW4gb3JkZXIgdG8gZ2VuZXJhdGUgdGhlIGludml0ZSBjb2RlLCBtYWtlIGEgUE9TVCByZXF1ZXN0IHRvIC9hcGkvaW52aXRlL2dlbmVyYXRl' | base64 -d

# RESULT
In order to generate the invite code, make a POST request to /api/invite/generate
```

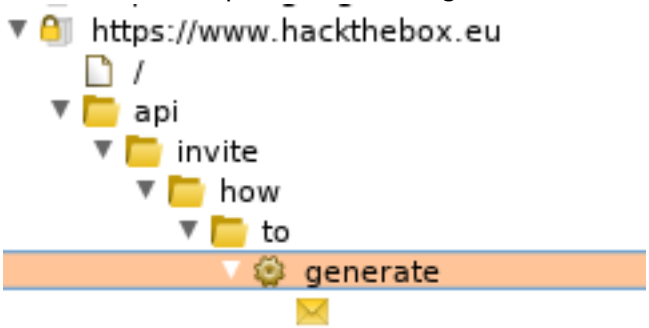
ROT13 can be decoded at the following site
RESOURCE: http://decode.org/

ROT13 is like a Ceasar Cipher where the letters are moved 13 places away from the hidden letter. This means we can decode ROT13 using the tr command. M is 13 places away from the letter A. That is how I determined the values after tr

```
echo 'Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /ncv/vaivgr/trarengr' | tr 'A-Za-z' 'N-ZA-Mn-za-m'

# RESULTS
In order to generate the invite code, make a POST request to /api/invite/generate
```

Now as directed we need to send a POST request to http://hackthebox/api/invite/generate
If you are using Burp it can be done by sending this site to repeater and then replace the word GET with POST. Send the request

When we go to Burp however we can see that location does not exist. It appears to actually be http://hackthebox.eu/api/invite/how/to/generate. We will follow the above instructions and see what happens




I am going to use the terminals command “curl” to demonstrate what happens

```
curl -X POST -i http://hackthebox.eu/api/invite/generate

# RESULTS
HTTP/1.1 301 Moved Permanently
Date: Fri, 20 Dec 2019 15:53:26 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: max-age=3600
Expires: Fri, 20 Dec 2019 16:53:26 GMT
Location: https://hackthebox.eu/api/invite/generate
X-Content-Type-Options: nosniff
Server: cloudflare
CF-RAY: 5482ca04fb83c7cd-DEN
```

Here we can see the page has been “302 Moved Permanently”

```
root@kali:/# curl -X POST -i http://hackthebox.eu/api/invite/generate
HTTP/1.1 301 Moved Permanently
Date: Fri, 20 Dec 2019 15:53:26 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: max-age=3600
Expires: Fri, 20 Dec 2019 16:53:26 GMT
Location: https://hackthebox.eu/api/invite/generate
X-Content-Type-Options: nosniff
Server: cloudflare
CF-RAY: 5482ca04fb83c7cd-DEN
```

We can use the location we found in Burp to send a request to the correct location or we can follow redirects with Curl

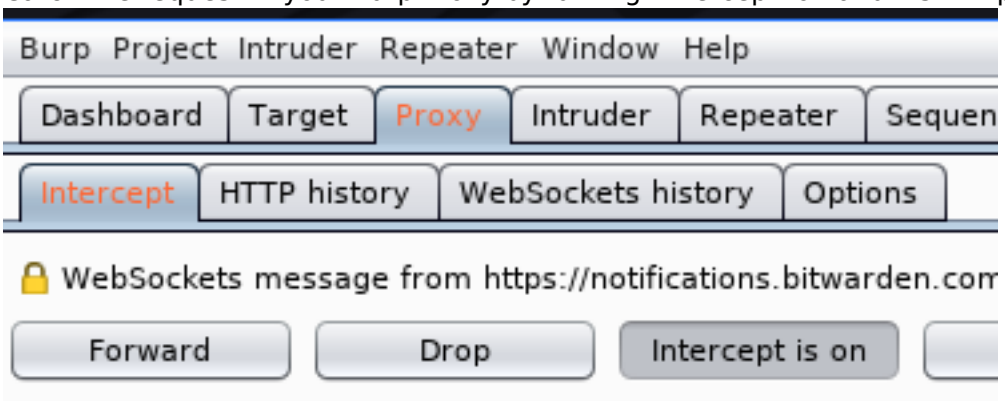
```
curl -X POST -iL http://hackthebox.eu/api/invite/generate

# RESULTS
HTTP/1.1 301 Moved Permanently
Date: Fri, 20 Dec 2019 15:55:23 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: max-age=3600
Expires: Fri, 20 Dec 2019 16:55:23 GMT
Location: https://hackthebox.eu/api/invite/generate
X-Content-Type-Options: nosniff
Server: cloudflare
CF-RAY: 5482ccdccb3ac7bd-DEN

HTTP/2 301
date: Fri, 20 Dec 2019 15:55:23 GMT
content-type: text/html
set-cookie: __cfduid=ddb6ba230cf27023c1510c4673e7bf0dd1576857323; expires=Sun, 19-Jan-20 15:55:23 GMT;
path=/; domain=.hackthebox.eu; HttpOnly; SameSite=Lax; Secure
location: https://www.hackthebox.eu/api/invite/generate
cf-cache-status: DYNAMIC
strict-transport-security: max-age=0; includeSubDomains
x-content-type-options: nosniff
expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
server: cloudflare
cf-ray: 5482ccddcd58c7b1-DEN


HTTP/2 200
date: Fri, 20 Dec 2019 15:55:23 GMT
content-type: application/json
set-cookie: __cfduid=d3b60410b5bff3f4a51ddf19483e8c3931576857323; expires=Sun, 19-Jan-20 15:55:23 GMT;
path=/; domain=.hackthebox.eu; HttpOnly; SameSite=Lax; Secure
vary: Accept-Encoding
cache-control: no-cache, private
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
cf-cache-status: DYNAMIC
strict-transport-security: max-age=0; includeSubDomains
expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
server: cloudflare
cf-ray: 5482ccdf39c7f794-DEN

{"success":1,"data":{"code":"QVVXQUwtTk9TV1QtQVdPUUktWUdVTEEtS09HUlE=","format":"encoded"},"0":200}
```

We can see at the bottom of our request is a base64 encoded string. 90% of the time Base64 ends with = or ==

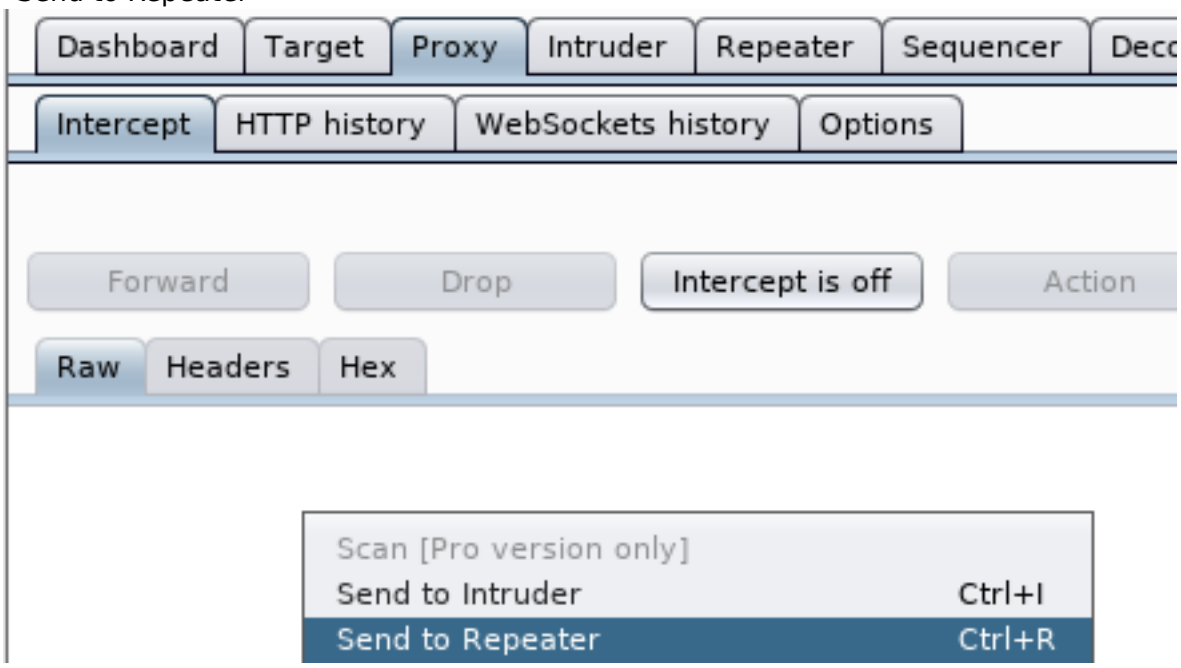
```
HTTP/2 200
date: Fri, 20 Dec 2019 15:55:23 GMT
content-type: application/json
set-cookie: __cfduid=d3b60410b5bff3f4a51ddf19483e8c3931576857323; expires=Sun, 19-Jan-20 15:55:23 G
vary: Accept-Encoding
cache-control: no-cache, private
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
cf-cache-status: DYNAMIC
strict-transport-security: max-age=0; includeSubDomains
expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
server: cloudflare
cf-ray: 5482ccdf39c7f794-DEN

{"success":1,"data":{"code":"QVVXQUwtTk9TV1QtQVdPUUktWUdVTEEtS09HUlE=","format":"encoded"},"0":200}
```

To visit this in Burp we can see the same result on the page.

Catch the request in your Burp Proxy by turning ‘Intercept’ on and visit http://hackthebox.eu/api/invite/generate

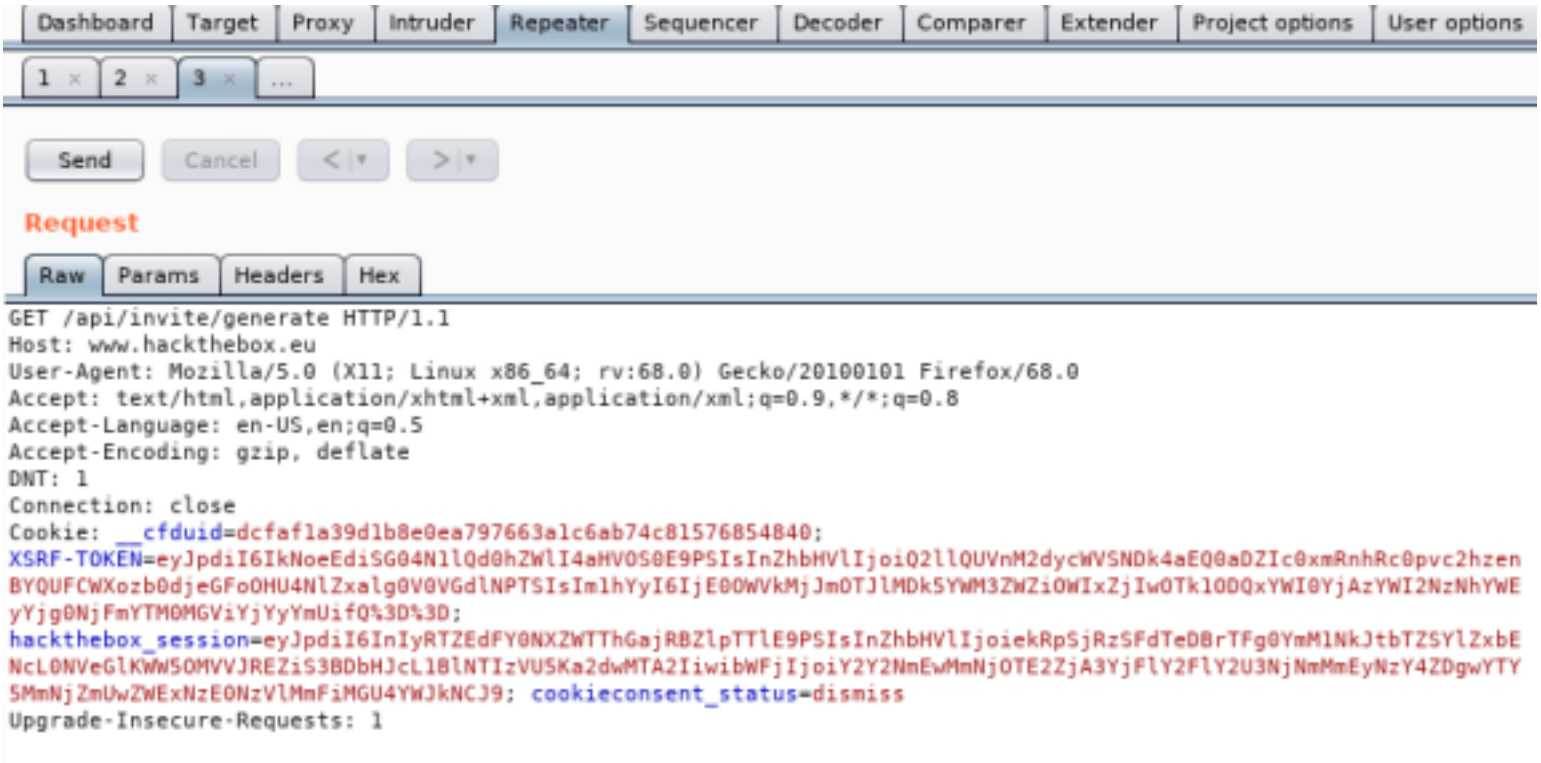



You can send the captured request to BurpSuites “Repeater” tab by doing Ctrl+R or Right Clicking and selecting “Send to Repeater”

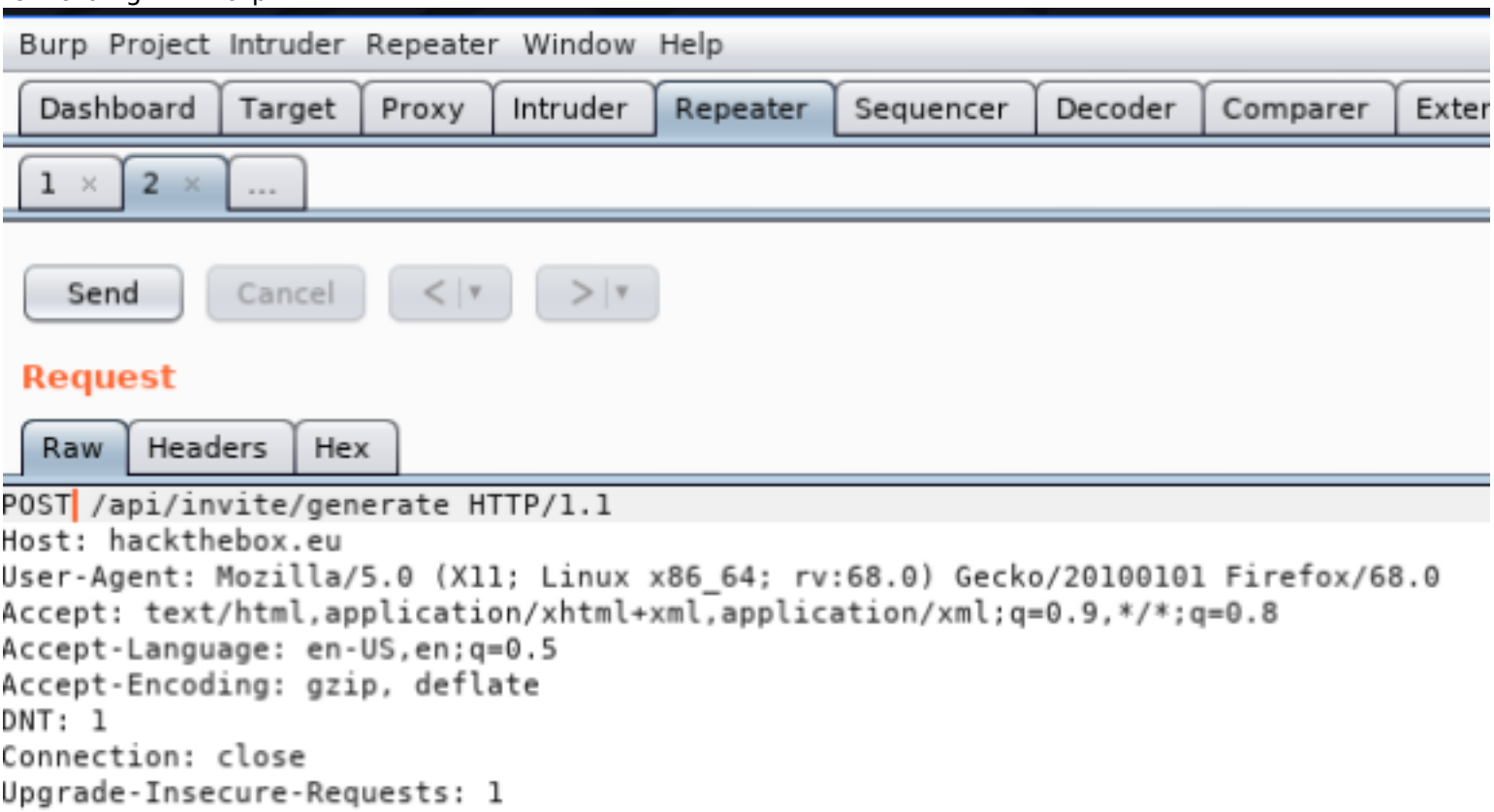



Be sure to click the ‘Forward’ button and not Drop

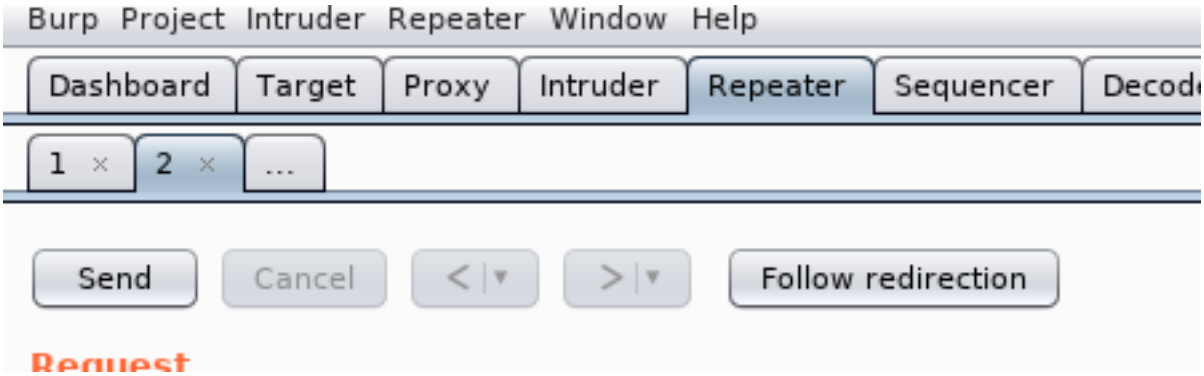
Go to the Repeater tab and change GET to POST and click 'Send'
Notice below I have a cookie and session value. This is required to successfully send the request.



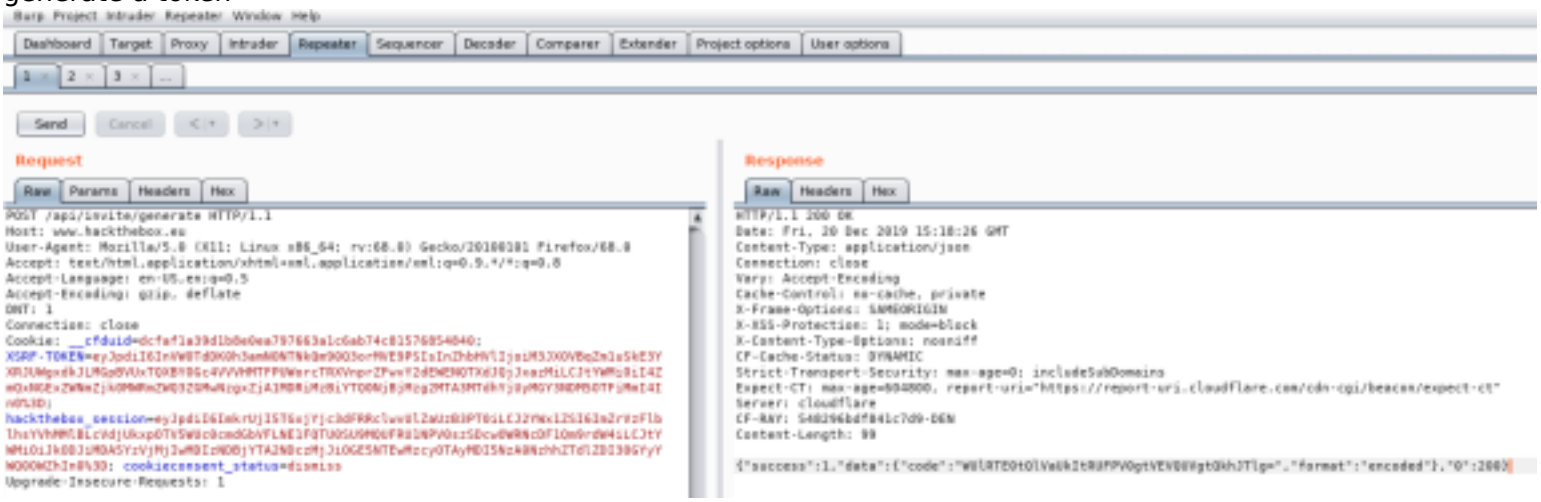

If you do not have these values and see the below request instead it means you dropped the packet instead of forwarding it in Burp




Next click the Follow Redirect button until the button does not show anymore.



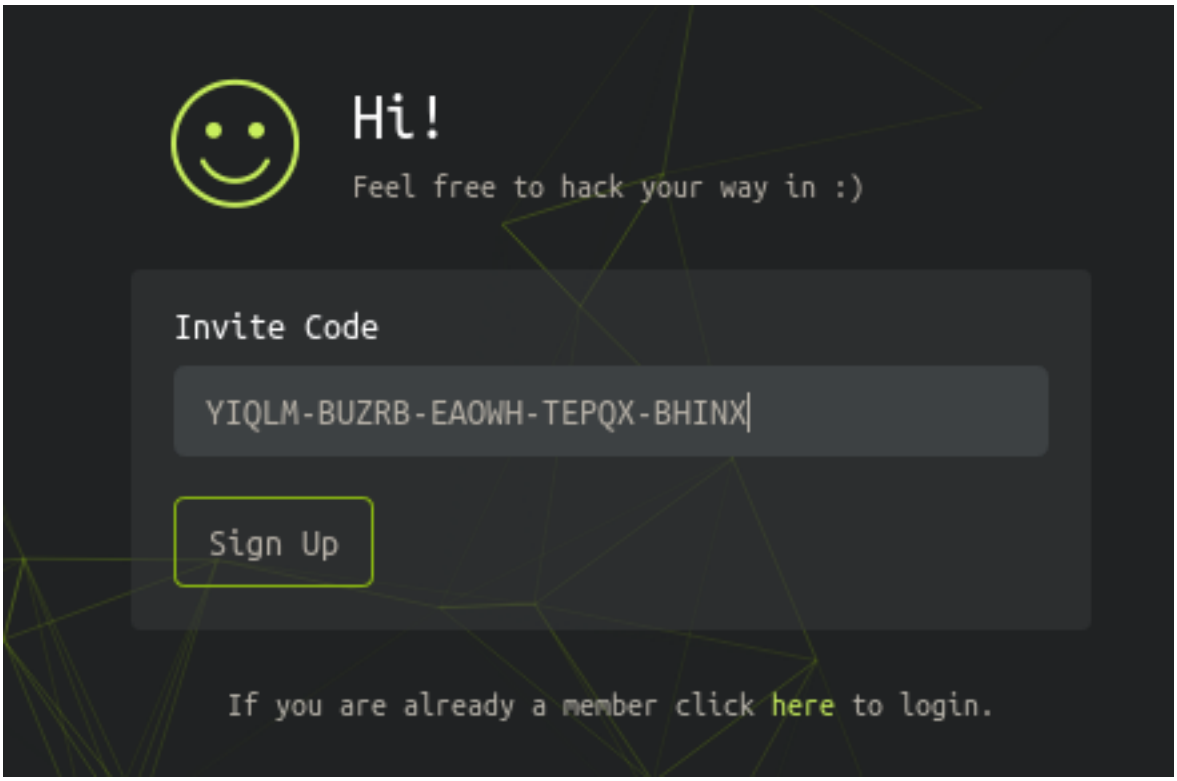

There may be a time limit associated with tokens so dont expect to wait too long while still being able to generate a token




Again in Burp we see the word “Encoded” next to the string. Time to decode the base64 again

```
echo 'WUlRTE0tQlVaUkItRUFPV0gtVEVQUVgtQkhJTlg=' | base64 -d

# RESULTS
YIQLM-BUZRB-EAOWH-TEPQX-BHINX
```

That gave us our Invite Code. Enter it into the Invite Code box at https://www.hackthebox.eu/invite


Hi!
Feel free to hack your way in :)
Invite Code
YIQLM-BUZRB-EAOWH-TEPQX-BHINX
Sign Up
If you are already a member click here to login.