## 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

À	••••••••••••••••••••••••••••••••••••••	
	Invite Code	
	Sign Up	
X	If you are already a member click here to login.	

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"

n :)	÷	$\rightarrow$	G	☆
	Sav	e <u>P</u> age As e Page to F	Poc <u>k</u> et	
_	Se <u>n</u>	d Page to I	Device	>
	Vie <u>v</u> Sele	<u>w</u> Backgrou ect <u>A</u> ll	und Image	
ra ta lagi	<u>V</u> iev	w Page Sou	irce	

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>
w<body class="blank" style="overflow-y:hidden; ">
 <script> -
 wrapper">
   v<section class="content" style="margin:0px; padding:0px;">
      ::before
    > <div class="container-center centerbox"> ... </div>
    v<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

* bittes //www.backhebox.es	
D /	
* 🦲 agi	
T D invite	
Y 🛅 hara	
T C to	
T 😫 generate	
T 🛄 slads	
a coerview	Requiris Requiring
n 🔁 essets	
D careers	Raw Headers Her
b de suit	WTTRUE & TAN OF
C certificates	Data: Fri. 10 Bar 2010 15:38:40 00V
Companies	(antent-Type: application/issancript: charactentf-8
P C84	Connection: close
P in fuels	Last Hodified: Wed. 18 Dec 2019 18:00:07 GMT
C pilleards	Vary: Accept-Exceding
D home	[Flag: 6]**64 full827-22a*
Internet internet	X-FYame-ByLines: LAMEDFILT
D individuals	3-331-Fritetiani Li mode-black
5 inste	x-canteet-type-optians: exercit
Y in	Cache-Certrol: max-age=/200
R celos la	U-6409-054001 811
Attributered annual	April 1278
C invitenzi min is	Service (newspeer) Security (newspaper) Incompany and the service of Service (Service) Service (Service)
D landing min is	Tarter: Chaddlare
13 modernity-2.6.3-respond-1.1.0 min is	(2-84) 540316/14-000
D gasticlegis-config.ison	Canteet-Leepth: 404
D learn	
C members	eval (function(a,a,c,k,a,d)de=function(c)(return c,toString)800;5f()'',replace(/'/.String)10+klc)(c,toString)a)0+klc)(c,toString)a
permond	[dial]] Section [] (return ")
press	[8+0*4*:+0:6.910#**7*.51*6*.aph/.bst/*/Adve/v/.cc118109.21810.7.2180013.218009103
P 📒 darage	[10195-805ar171.5r361.kr]/n0(k/h/h/m).co300155-20015.f1310105-20013.f131005-20013.f131005-20013.f131005-20013.f131005-20013.f131005-200
C Imarus	ata(var)serityDeviteCode(sateDeviteCode(how)sa(perenate(verity', split)(')').0.()))
15 inc	

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....

	Inspector D C	onsole 🕻	🗅 Debugger	{} Style Editor	Performance	D: Memory	†↓ Ne
1 T	ilter output						
Errors W	arnings Logs Info	Debug	CSS XHR	Requests			
	"\$\$\$	\$\$uu\$\$\$	\$\$\$uu\$\$\$\$		TH	I 5	
	≯: L	>>>>>> 1\$\$\$\$\$\$\$\$!	3333333 1\$\$\$\$\$\$U		В 0	х	
	uuu	\$\$u\$ \$ \$	5 S SuSS	uuu			
	u\$\$\$\$	\$\$\$\$\$u	\$u\$u\$\$\$	u\$\$\$\$			
	\$\$\$\$\$uu	"\$\$\$\$	\$\$\$\$\$"	uu\$\$\$\$\$\$			
	u\$\$\$\$\$\$\$\$\$	u ""	""" uuuu	\$\$\$\$\$\$\$			
	\$\$\$\$"""\$\$\$\$\$	\$\$\$\$\$uuu	uu\$\$\$\$\$\$	\$\$\$"""\$\$\$"			
		\$\$\$\$\$\$\$	\$\$\$uu ""\$""				
	u	uuu ""\$\$!	\$\$\$\$\$\$\$\$uuu				
-	u\$\$\$uuu\$\$\$	\$\$\$\$\$\$uu	""\$\$\$\$\$\$\$	\$\$\$uuu\$\$\$			
-	\$\$\$\$\$\$\$\$		""\$\$	\$\$\$\$\$\$\$\$	HackTheBo:	x v0.9.3	
	"\$\$\$\$\$"			""\$\$\$\$""	info@hackt	hebox.eu	
-	\$\$\$"			\$\$\$\$"			

>> 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:

SW4gb3JkZXIgdG8gZ2VuZXJhdGUgdGhlIGludml0ZSBjb2RILCBtYWtlIGEgUE9TVCByZXF1ZXN0IHRvIC9hcGkvaW52aXRIL

```
🕞 🗘 Inspector 🖸 Console 🕞 Debugger - { } Style Editor 🖓 Performance - 🕄 Memory 🐴 Network 😑 Storage 🛉 Accessibility
📋 🛛 🗑 Filter output
 trors Warnings Logs Info Debug CSS XHR Requests
I > TypeError: n is null <u>[Learn More]</u>
>> makeInviteCode()

undefined

   ₹ {_}}
       0: 200
     ▼ data: {..}
         data: "SW4gb3JkZXIgdG8gZ2VuZXJhdGUgdGhlIGludml0ZSBjb2RlLCBtYWtlIGEgUE9TVCByZXF1ZXN0IHRvIC9hcGkvaW52aXRlL2dlbmVyYXRl*
         enctype: "BASE64"
       ▶ <prototype>: Object { ... }
       success: 1
     ▶ <prototype>: Object { _ }
>> makeInviteCode()
← undefined
   ▼ {_}
       0: 200
     ▼ data: {..}
        data: "Va begre gb trarengr gur vaivgr pbgr, znxr n CBFG erdhrfg gb /ncv/vaivgr/trarengr"
         enctype: "ROT13"
       ▶ <prototype>: Object { _ }
       success: 1
     ▶ <prototype>: Object { _ }
```

We can decode base64 using the terminal as well.

```
echo
'SW4gb3JkZXIgdG8gZ2VuZXJhdGUgdGhlIGludml0ZSBjb2RlLCBtYWtlIGEgUE9TVCByZXF1ZXN0IHRvIC9hcGkvaW52aXRlL2dlbmVyY
XRl' | 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



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



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
<pre>content-type: application/json</pre>
<pre>set-cookie:cfduid=d3b60410b5bff3f4a51ddf19483e8c3931576857323; expires=Sun, 19-Jan-20 15:55:23 G</pre>
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
<pre>strict-transport-security: max-age=0; includeSubDomains</pre>
expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
server: cloudflare
cf-ray: 5482ccdf39c7f794-DEN
<pre>{"success":1,"data":{"code":"QVVXQUwtTk9TV1QtQVdPUUktWUdVTEEtS09HUlE=","format":"encoded"},"0":200}</pre>

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

Burp Project Intruder Repeater Window Help									
Dashboard	Target Pr	оху	Intruder	Repe	ater	Seq	uen		
Intercept HTTP history WebSockets history Options									
WebSockets message from https://notifications.bitwarden.com									

Forward Intercept is on Drop

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

Dashboard Ta	rget Proxy	Intruder	Repeater	Sequencer	Deco
Intercept HTTF	Phistory We	ebSockets hi	story Opti	ons	
Forward	Drop	In	tercept is of	f Ac	tion
Paw Headers	Hay				
Raw neaders	nex				
	Scan [Pro ve	ersion only]			
	Send to Intr	uder		Ctrl+I	
	Send to Rep	eater		Ctrl+R	

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.

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options
1 × 2 × 3 ×										
Send Cancel <   * >   *										
Request										
Raw Par	ams Hea	ders H	lex							
GET /api/in	/ite/gene	rate HT	TP/1.1							
Host: www.h	ackthebox	.eu								
User-Agent:	Mozilla/	5.0 (X1	l; Linux	x86_64; rv	:68.0) Geck	0/20100101	l Firefox/6	8.0		
Accept: tex	t/html,ap	plicati	on/xhtml+	xml,applic	ation/xml;q	=0.9,*/*;q	1=0.8			
Accept-Lang	Jage: en-	US, en; q	=0.5							
Accept-Enco	ding: gzi	.p, defla	ate							
DNT: 1										
Connection:	close									
Cookie:c	fduid=dcf	afla39d	1b8e0ea79	7663a1c6ab	74c81576854	840;				
XSRF-TOKEN=eyJpdiI6IkNoeEdiS604N1lQd0hZWlI4aHV0S0E9PSIsInZhbHVlIjoiQ2llQUVnM2dycWVSNDk4aEQ0aDZIc0xmRnhRc0pvc2hzen										
BYQUFCWXozb0djeGFoOHU4NlZxalg0V0VGdlNPTSIsIm1hYyI6IjE00WVkMjJm0TJlMDkSYWM3ZWZi0WIxZjIw0Tk10DQxYWI0YjAzYWI2NzNhYWE										
yYjg0NjFmYTM0MGViYjYyYmUifQ%3D%3D;										
hackthebox_	session=e	yJpd116	InlyRTZEd	FYONXZWITH	GajRBZLpTTL	E9PSIsInZh	bHVlIjoiek	RpSjRzSFdT	eDBrTFg0YmM1NkJ	tbTZSYLZxbE
NcLONVeGLKW	SOMVVJRE	Z1S3BDb	HJCL1BUNT	IzVU5Ka2dw	MTAZI1W1DWF	] [ ] 01 Y 2 Y 2 N	INEWMINIJOTE.	ZZJAJYJFLY	2FLY2U3NjNmMmEy	NZY4ZDgwYTY
5MmNj ZmUwZW	EXNZEONZY	UMMF1MG	U4YWJKNCJ	9; COOK1eC	onsent_stat	us=d1sm1ss				
Upgrade-Insecure-Requests: 1										

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

Burp Project Intruder Repeater Window Help									
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Exter	
1 × 2 ×									
Send Cancel <   * >   *									
Request									
Raw Headers Hex									
POST /api/in	vite/gen	erate H	TTP/1.1						
Host: hackth	ebox.eu								
User-Agent:	Mozilla/	5.0 (X1)	l; Linux :	x86_64; rv	:68.0) Gecka	0/20100101	l Firefox/68	3.0	
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8									
Accept-Language: en-US, en; q=0.5									
Accept-Encod	Accept-Encoding: gzip, deflate								
DNT: 1									
Connection:	close								
Upgrade-Inse	cure-Req	uests: :	1						

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

Burp Project Intruder Repeater Window Help									
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decode			
1 × 2 ×									
Send	Cancel	<   •	>   *	Follow	redirection				

## Request

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



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

