

Hack the Box

Invite Challenge

Involves...

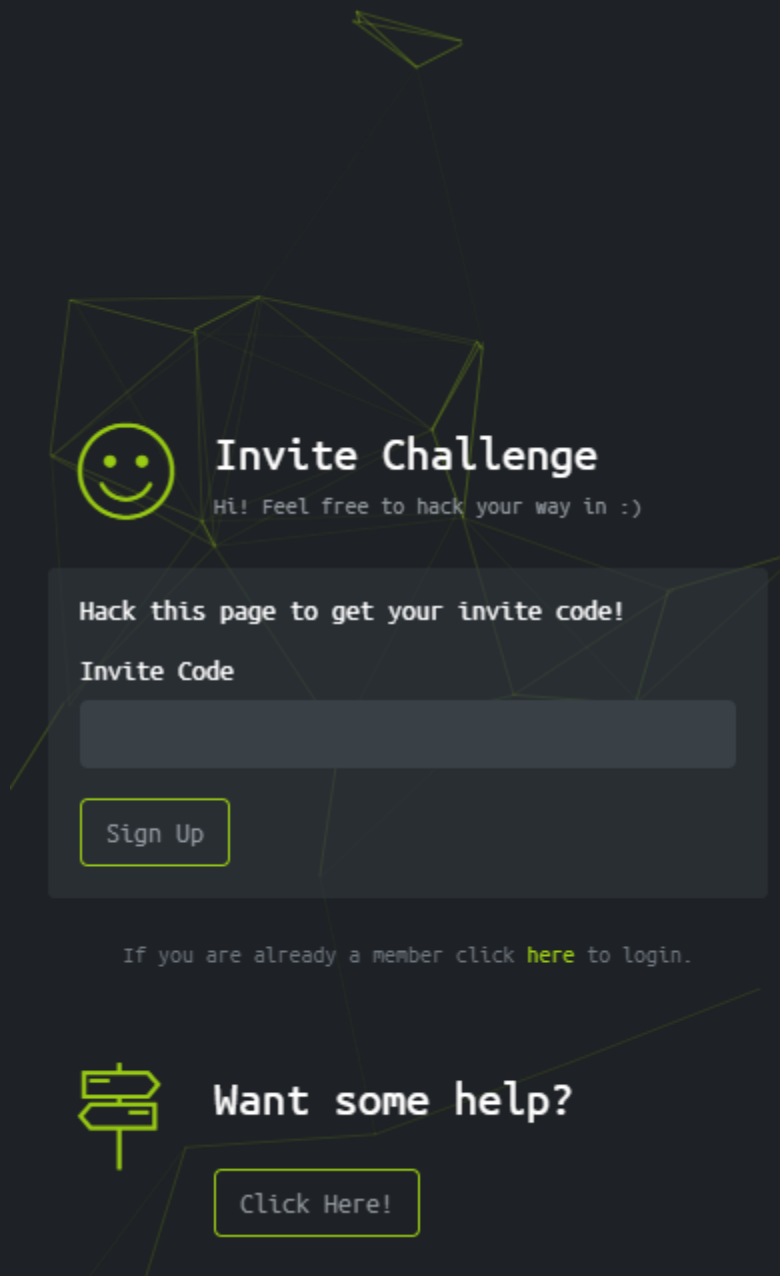
- JavaScript
- Code Obfuscation
- Decryption/Decoding

I Used...

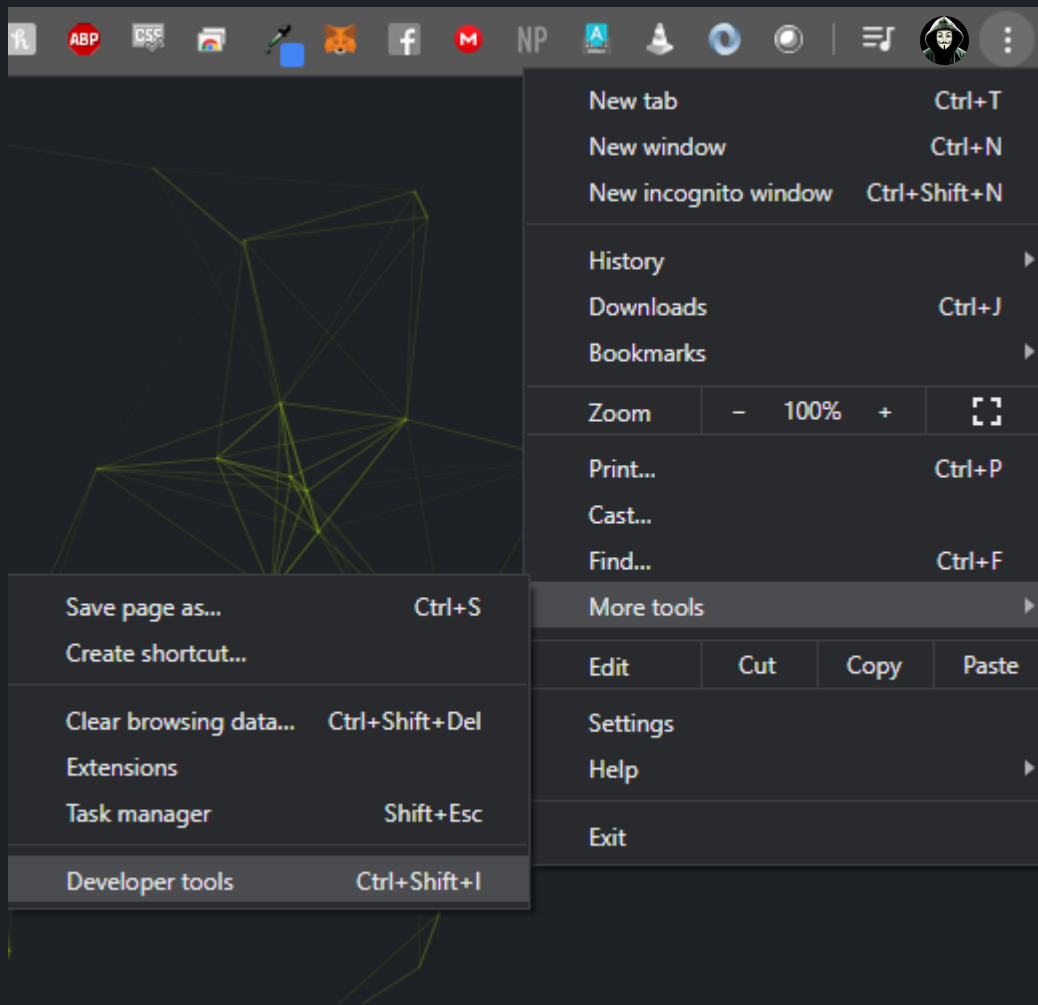
- Google Chrome
- JSFiddle
- Kali Linux

*Can be accomplished with other tools just as well.

To begin, navigate your browser to www.hackthebox.eu/invite which will present the initial challenge.

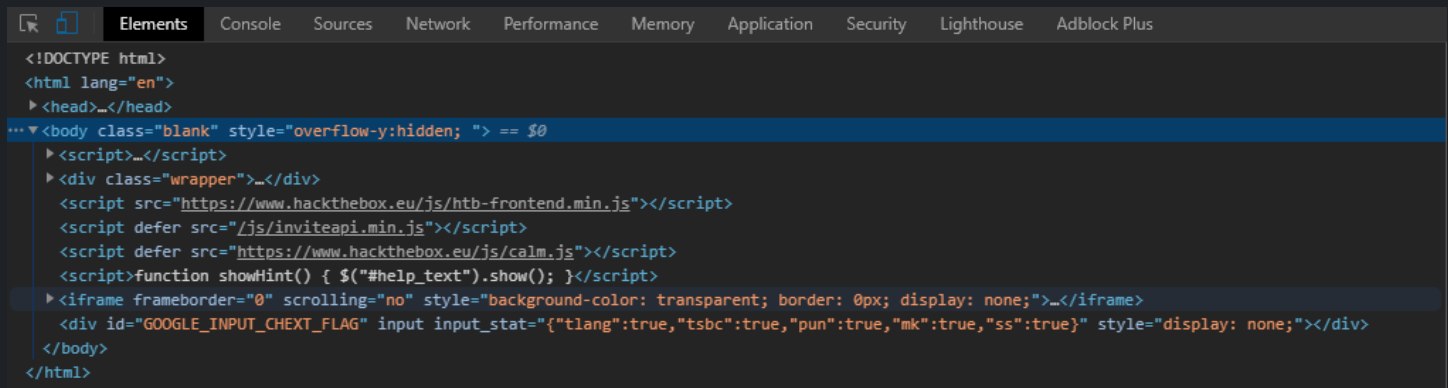


There's no shame in using the hint, if you click it, you'll be told "You could check the console".



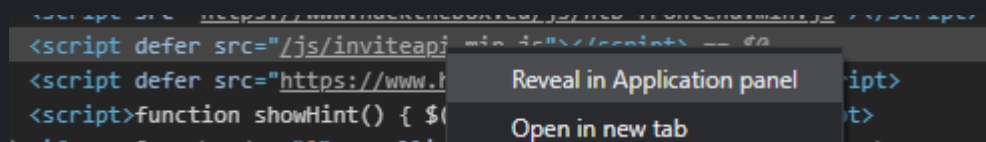
So, open the developer tools.
Check the Console's Info tab. You'll see this message:





```
<!DOCTYPE html>
<html lang="en">
  <head>...</head>
  <body class="blank" style="overflow-y:hidden; "> == $0
    <script>...</script>
    <div class="wrapper">...</div>
    <script src="https://www.hackthebox.eu/js/htb-frontent.min.js"></script>
    <script defer src="/js/inviteapi.min.js"></script>
    <script defer src="https://www.hackthebox.eu/js/calm.js"></script>
    <script>function showHint() { $("#help_text").show(); }</script>
    <iframe frameborder="0" scrolling="no" style="background-color: transparent; border: 0px; display: none;"></iframe>
    <div id="GOOGLE_INPUT_CHEXT_FLAG" input input_stat="{\"tlang\":true,\"tsbc\":true,\"pun\":true,\"mk\":true,\"ss\":true}" style="display: none;"></div>
  </body>
</html>
```

We'll find that the "Elements" tab has a reference to a JavaScript file called "inviteapi.min.js".

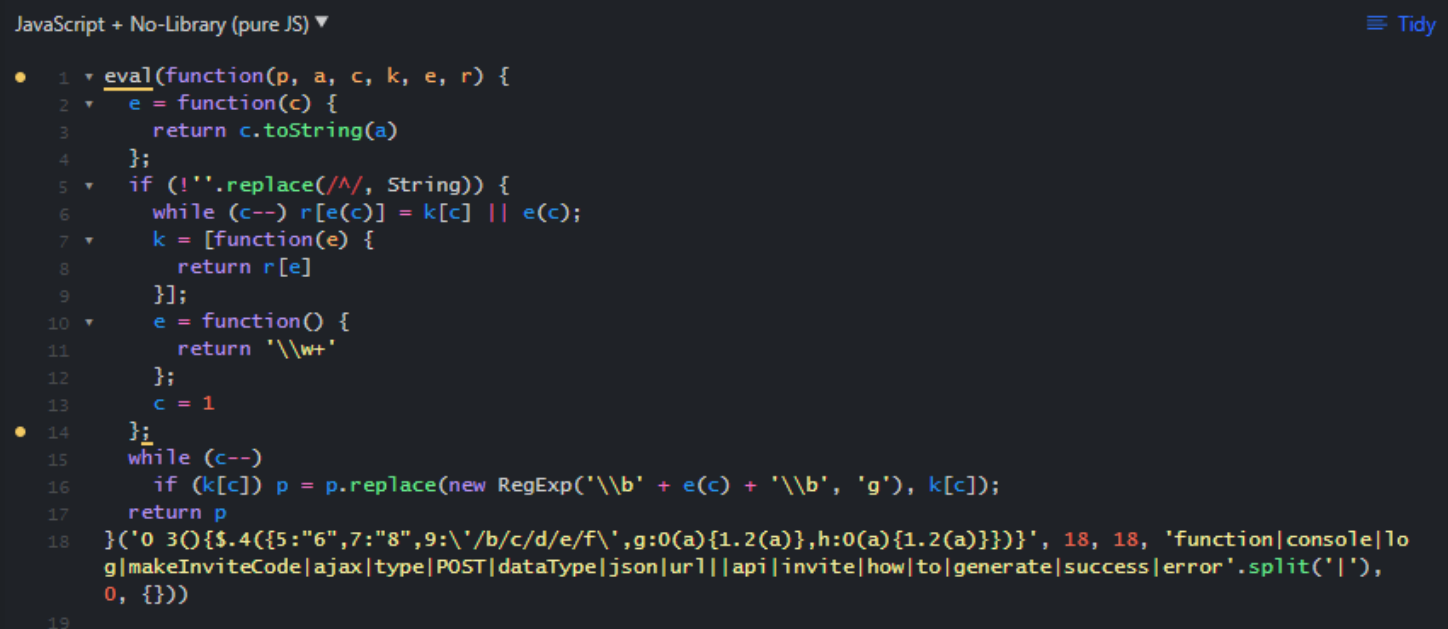


The name is a bit of a tip-off. You can right-click the reference to view the content. You're given a bunch of obfuscated JavaScript:

```
//This JavaScript looks strange...is it obfuscated???

eval(function(p,a,c,k,e,r){e=function(c){return c.toString(a)};if(!''.replace(/^/,String)){while(c--){r[e(c)]=k[c]||e(c);k=[function(e){return r[e]}];e=function(){return '\\w+'};c=1;}while(c--){if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);}return p}('0 3(){$.4({5:"6",7:"8",9:\\'/b/c/d/e/f\\',g:0(a){1.2(a)},h:0(a){1.2(a)}})},18,18,'function|console|log|makeInviteCode|ajax|type|POST|dataType|json|url||api|invite|how|to|generate|success|error'.split('|'),0,{}))
```

Now is the time to open www.jsfiddle.net and paste the code into the bottom-left canvas. Hit the "Tidy" button in the top right corner to make the code readable.



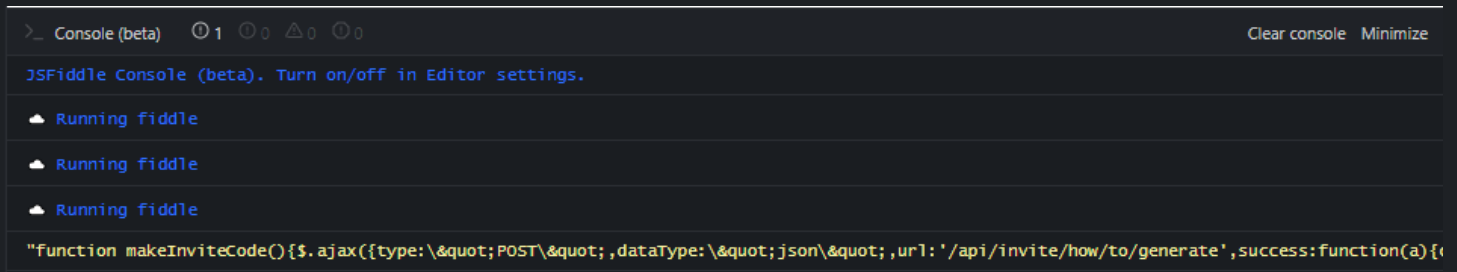
```
JavaScript + No-Library (pure JS) ▼ Tidy

1 eval(function(p, a, c, k, e, r) {
2   e = function(c) {
3     return c.toString(a)
4   };
5   if (!''.replace(/^/, String)) {
6     while (c--) r[e(c)] = k[c] || e(c);
7     k = [function(e) {
8       return r[e]
9     }];
10    e = function() {
11      return '\\w+'
12    };
13    c = 1
14  };
15  while (c--)
16    if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c]);
17  return p
18 }('0 3(){$.4({5:"6",7:"8",9:\\'/b/c/d/e/f\\',g:0(a){1.2(a)},h:0(a){1.2(a)}})},18,18,'function|console|log|makeInviteCode|ajax|type|POST|dataType|json|url||api|invite|how|to|generate|success|error'.split('|'),0,{}))
19
```

The script contains multiple function calls, but all return to assign a value. The only “final” return is on line 17, “return p”. We want to read this value quickly, so change “return p” to “console.log(p)”.

```
};  
while (c--)  
  if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c]);  
console.log(p)  
(function(){$.ajax({type:"POST",dataType:"json",url:'/api/invite/how/to/generate',success:function(a){  
  console.log(a);
```

Finally, hit the “Run” button on the top of the page. It will populate the console on the bottom right:

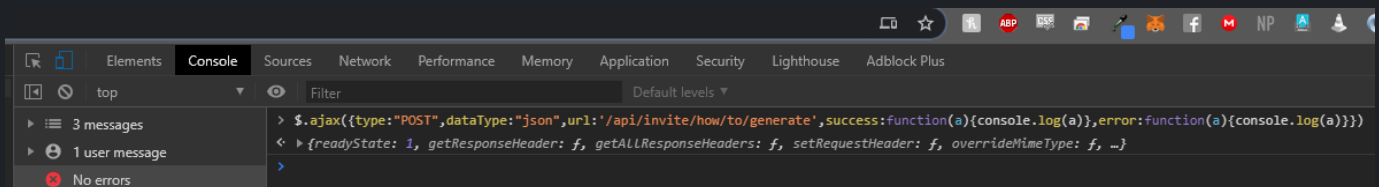


Copy the text out of the console to inspect it. This is a function that needs to run on the www.hackthebox.eu/invite page’s console. It needs some modification before we can run it. Use whatever text editor you want to replace the string ‘\"’ with the standard double quote character.

```
function  
makeInviteCode(){$.ajax({type:"POST",dataType:"json",url:'/api/invite/how/to/generate',success:function(a){console.log(a)},error:f  
unction(a){console.log(a)}}}  
  
function  
makeInviteCode(){$.ajax({type:"POST",dataType:"json",url:'/api/invite/how/to/  
generate',success:function(a){console.log(a)},error:function(a){console.log(a  
)}}})
```

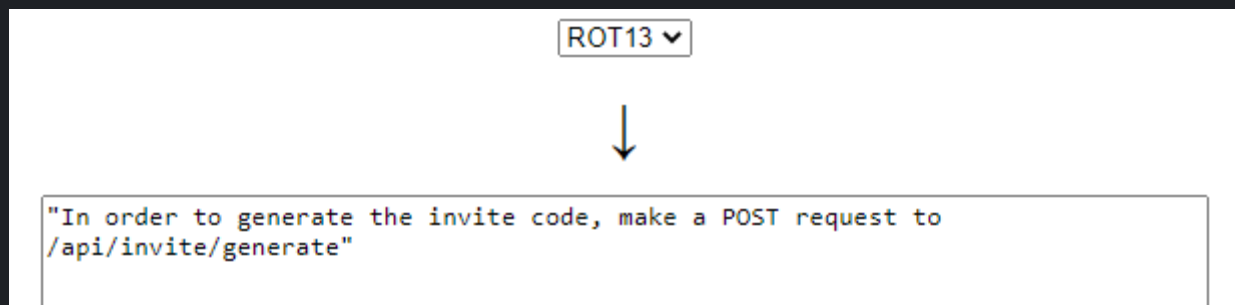
Finally, we don't need the function's declaration in order to run its body. Remove the ‘function’ keyword and name as well as the curly brace. Paste this into the console on the invite page.

```
$.ajax({type:"POST",dataType:"json",url:'/api/invite/how/to/generate',success  
:function(a){console.log(a)},error:function(a){console.log(a)}})
```



When the command runs, we're returned a JSON object. Expand the responseJSON section to find some ciphertext and its cipher. It may be ROT, Base64 encoded, or something else. Either way, copy the data text into an appropriate decoder:

```
< ▾ {readyState: 1, getResponseHeader: f, getAllResponseHeaders: f, setRequestHeader: f, overrideMimeType
  ▶ abort: f (e)
  ▶ always: f ()
  ▶ complete: f ()
  ▶ done: f ()
  ▶ error: f ()
  ▶ fail: f ()
  ▶ getAllResponseHeaders: f ()
  ▶ getResponseHeader: f (e)
  ▶ overrideMimeType: f (e)
  ▶ pipe: f ()
  ▶ progress: f ()
  ▶ promise: f (e)
  readyState: 4
  ▾ responseJSON:
    0: 200
    ▾ data:
      data: "Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFg erdhfrfg gb /ncv/vaivgr/trarengr"
      enctype: "ROT13"
      ▶ __proto__: Object
    hint: "Data is encrypted ... We should probably check the encryption type in order to decrypt it..."
    success: 1
```




This step is simple, use whatever method you like to generate a POST request to the specified endpoint:

```
curl -X POST "https://www.hackthebox.eu/api/invite/generate"
{"success":1,"data":{"code":"SFBPVVctSUJaTUwtVFFaVkJtR0dYVkgT0FLQU8=","format":"encoded"},"0":200}
```


The “code” is always Base64 encoded. Once more, copy the text and paste it into your favorite decoder:


SFBPVVctSUJaTUwtVFFaVkMtR0dYVkgT0FLQU8=

 For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

UTF-8  Source character set.

☐ Decode each line separately (useful for multiple entries).

 Live mode OFF Decodes in real-time when you type or paste (supports only UTF-8 character set).

 < DECODE > Decodes your data into the textarea below.

HPOUW-IBZML-TQZVC-GGXVH-OAKAO

Finally, paste your Invite Code into the invite page and you're done! Your offensive security quest begins.



Invite Challenge

Hi! Feel free to hack your way in :)

Hack this page to get your invite code!

Invite Code

HPOUW-IBZML-TQZVC-GGXVH-OAKAO

Sign Up

If you are already a member click [here](#) to login.



Want some help?

Click Here!

You could check the console...



Hack The Box

PEN-TESTING LABS

Congratulations!

Hello, and thank you for taking the time to read my guide.

I greatly enjoyed creating it and tinkering with this challenge. I hope I find the time and motivation to complete more challenges and produce more documents like this one. Please follow me on LinkedIn as I continue my journey in Cyber Security while sharing what I can along the way.

- Omar "Michael" Abdo, B.IT