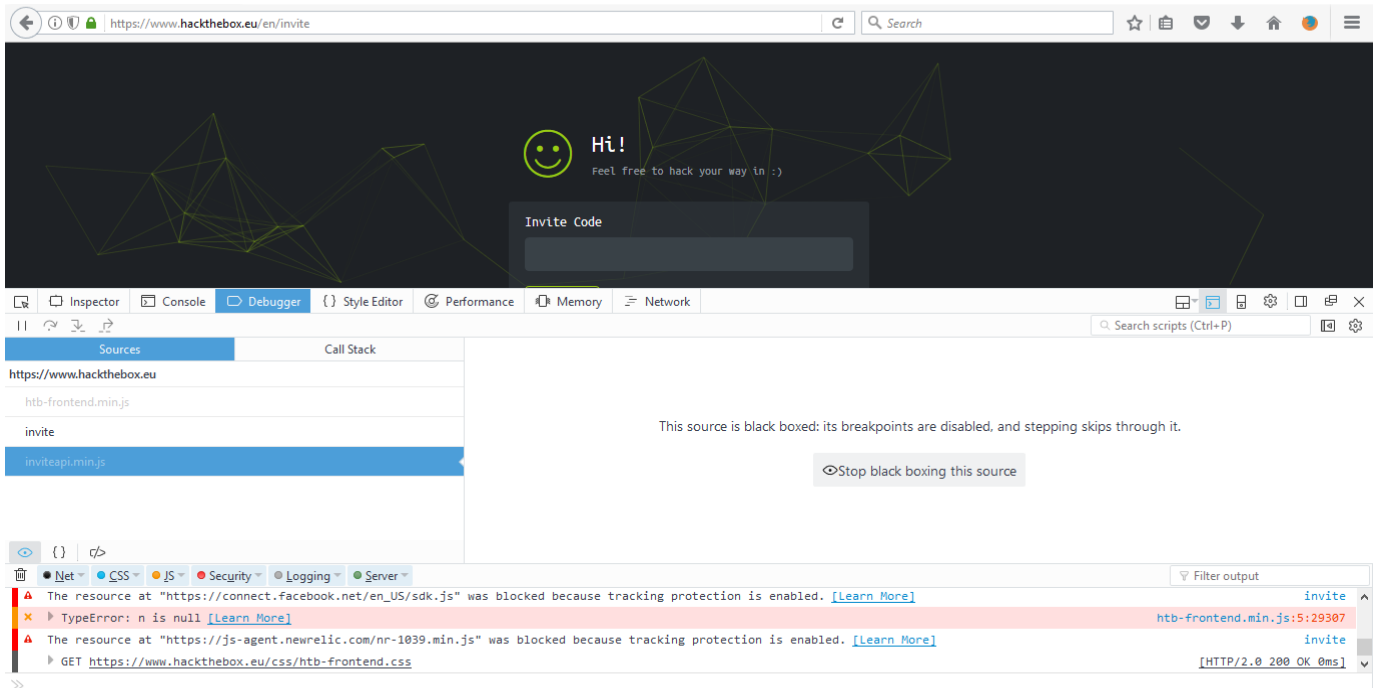
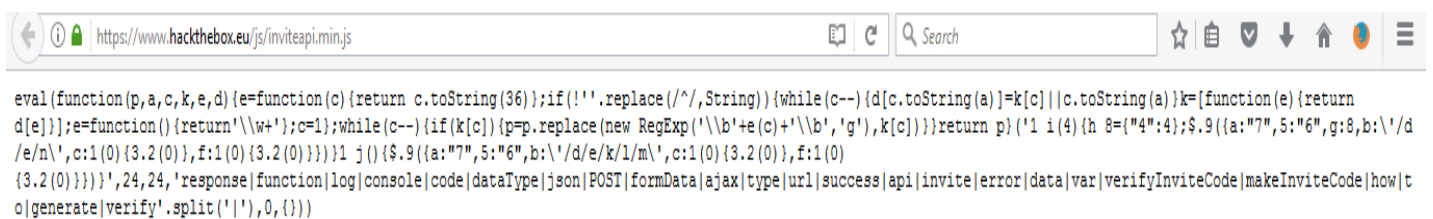


HACK THE BOX INVITE

>> Open the inviteapi.min.js url found within the debugger tab.



>> We can see the javascript code is packed/obfuscated. So now we need to unpack/deobfuscate it.



```

1 function verifyInviteCode(code) {
2   var formData = {
3     "code": code
4   };
5   $.ajax({
6     type: "POST",
7     dataType: "json",
8     data: formData,
9     url: '/api/invite/verify',
10    success: function(response) {
11      console.log(response)
12    },
13    error: function(response) {
14      console.log(response)
15    }
16  })
17 }
18
19 function makeInviteCode() {
20   $.ajax({
21     type: "POST",
22     dataType: "json",
23     url: '/api/invite/how/to/generate',
24     success: function(response) {
25       console.log(response)
26     },
27     error: function(response) {
28       console.log(response)
29     }
30   })
31 }

```

>> Execute the function makeInviteCode in the js console

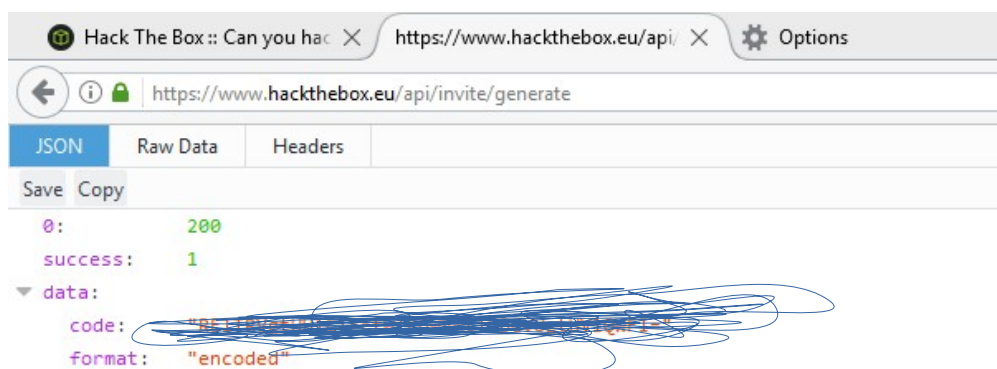
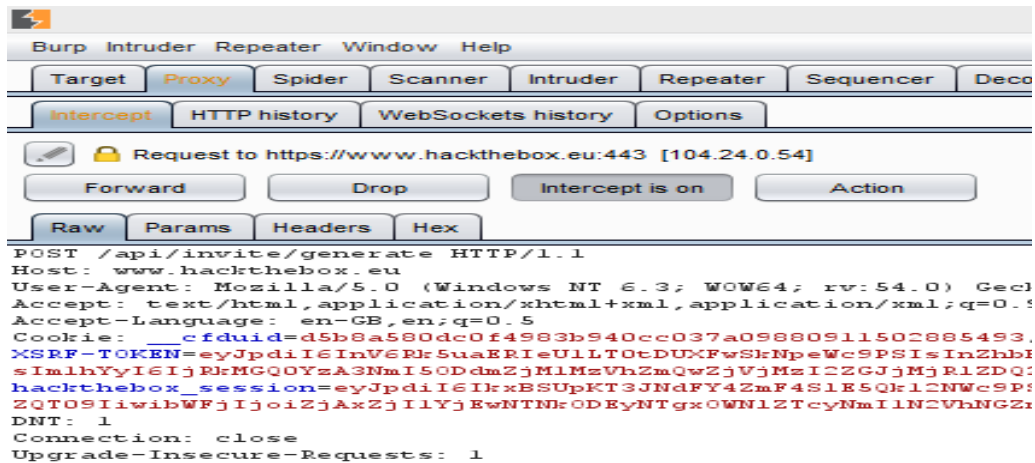
The screenshot shows a web browser's developer console. The top part displays a list of network requests, including a POST request to `https://www.hackthebox.eu/api/invite/how/to/generate`. The bottom part shows the console log, which includes a message from `makeInviteCode()` that is `undefined`. The right-hand side of the console shows the response object, which has a `data` property containing a ROT13 encoded string: `"Va beqre gb trarengr...ncv/vaivgr/trarengr"`.

>> On the right-hand side we can see the encrypted data in rot13 format.

The diagram illustrates the process of decoding a ROT13 encoded string. It starts with a box containing the encoded string: `"Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFg erdhrg gb /ncv/vaivgr /trarengr"`. An arrow points down to a box with a `ROT13` button. Another arrow points down to a box containing the decoded message: `"In order to generate the invite code, make a POST request to /api/invite /generate"`.

>> So now we need to send post request to /api/invite/generate to get the code.

>> So start the burpsuite and then lets pass the /api/invite/generate to the url <https://www.hackthebox.eu>. Within burpsuite change the 'GET' to 'POST' and forward it.



>> The code is in base64 format. Decrypt and get the code!

