Walkthrough -- getting the invite code for HackTheBox – by Alex

Preface -- HacktheBox is a pretty cool site that offers many pentesting and CTF challenges. The first challenge is finding the invite code to actually log in to the site! Here is how I did it.

1. When you go to `https://www.hackthebox.eu/invite`, you are presented with a simple login form asking for your invite code. Of course, you don't have one so how do we get it?
2. We look around the page and don't see anything obvious on the rendered page, so let's take a look at the source. I'm using Chrome so I use `Ctrl-Shift-I` to open Chrome DevTools. If we click on the Console tab we see a nice ASCII graphic welcoming us to HackTheBox. Now let's inspect our source by clicking on the Elements tab (you can also use `Ctrl-U` to look at the page source but it's a lot messier to look at). The HTML looks ordinary but there are some scripts that are called, let's open each one in a new tab (right-click on a link and select Open in new tab):
    a) `/js/htb-frontend.min.js` -- this seems to be the JavaScript for the page UI
    b) `/js/calm.js` -- this is the ASCII welcome graphic seen in the Console tab
    c) `/js/inviteapi.min.js` -- there's a bunch of weird stuff inside a JS eval function; near the end is the term "makeInviteCode". Hmm….

3) Let's copypaste and unpack that code, I used JavaScript Beautifier at `beautifier.io` and we see a function, `makeInviteCode()`. Let's go back to the Console tab and run that, and we get some encrypted data, click on the arrow next to "data" to see how it is encrypted, it may be Base64, ROT13 or something else. Use an appropriate decoder and you will come up with something like "In order to generate the invite code, make a POST request to /api/invite/generate".
4) We can easily make a POST request using curl from a command line so let's try that. From Linux you can just use curl normally, and from Windows 10 you can use the new curl tool either from the cmd prompt or from PowerShell, like this:
    i) `curl -X POST https://www.hackthebox.eu/api/invite/generate`
    ii) `curl.exe -X POST https://www.hackthebox.eu/api/invite/generate` [In PowerShell you can also use `Invoke-WebRequest` instead of curl if you like]
5) The response we get is in Base64 so again we can turn to an online decoder, I used `base64decode.org`
6) This gives us our invite code which we can now take back to the invite page and paste it into the form, well done!