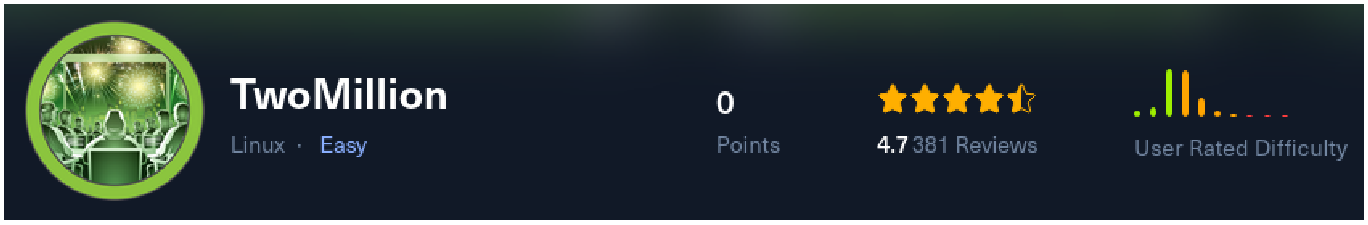

TwoMillion

Linux · Easy

0 Points

4.7 381 Reviews

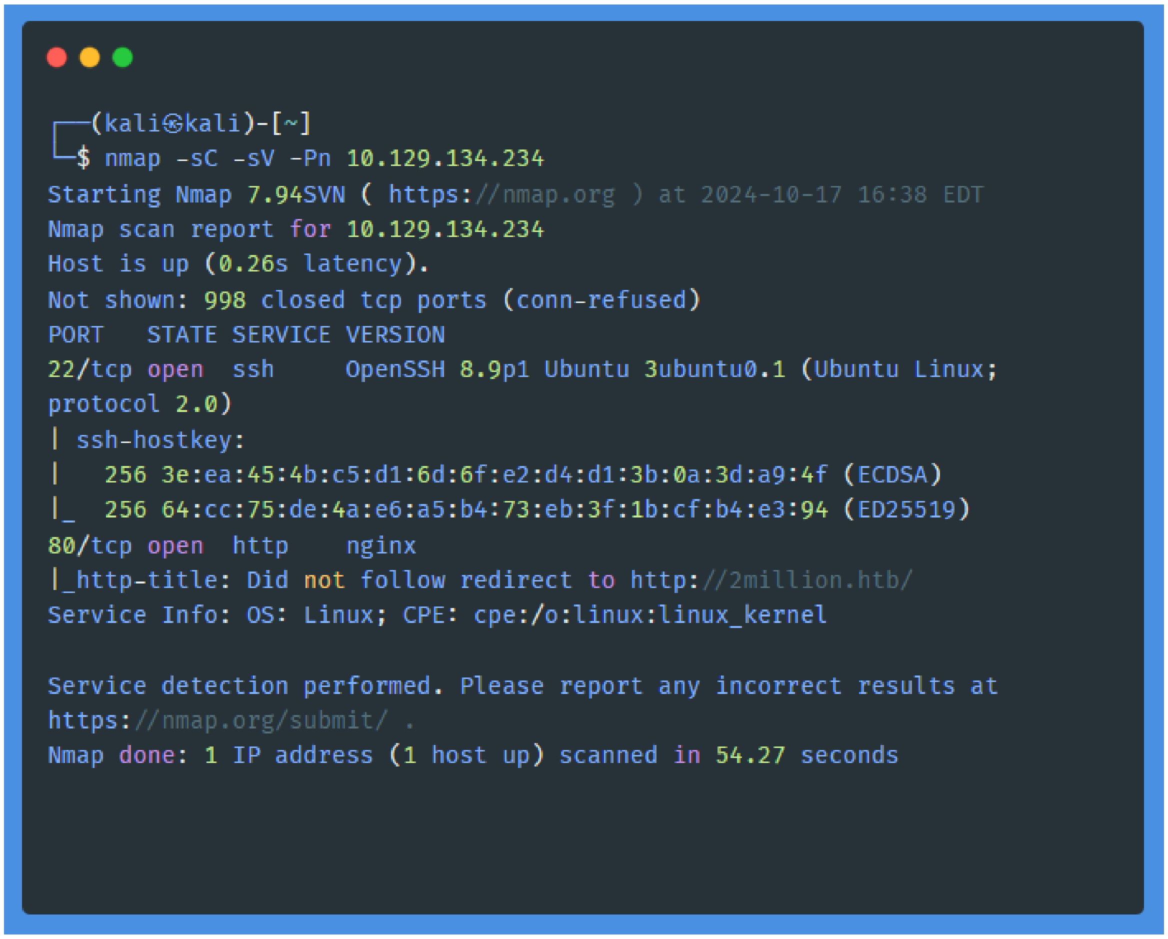
User Rated Difficulty

TwoMillion – Easy Machine

Enumeration

Nmap

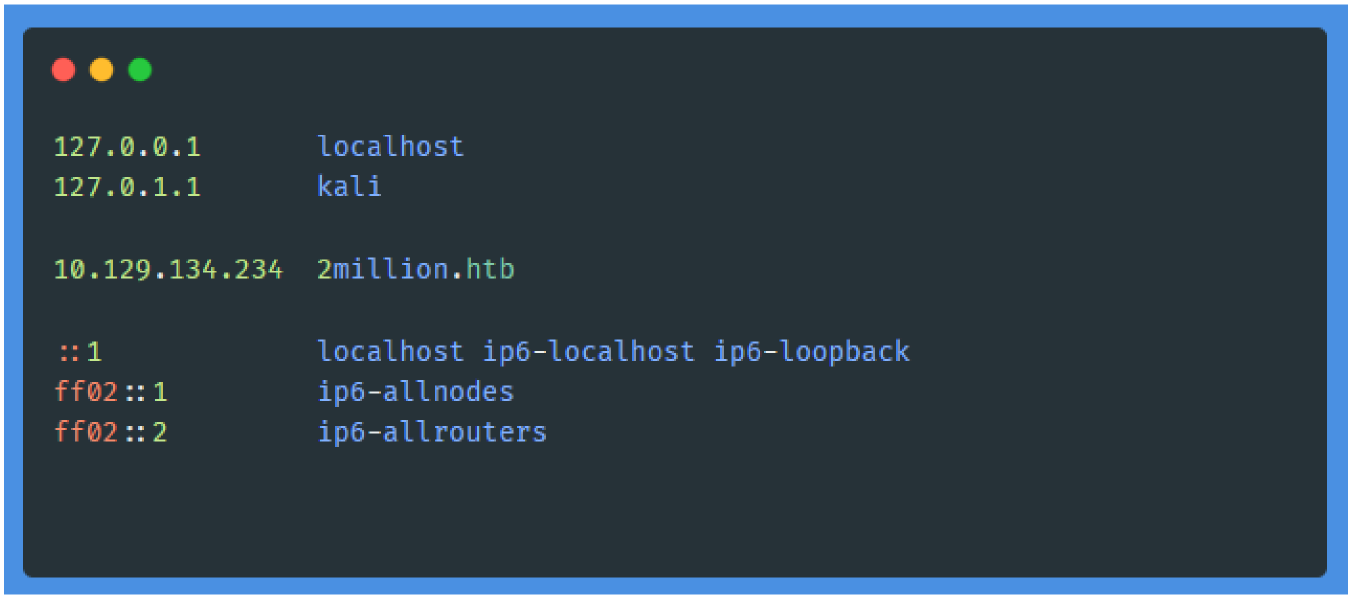
```
nmap -sC -sV -Pn 10.129.134.234
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -Pn 10.129.134.234
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 16:38 EDT
Nmap scan report for 10.129.134.234
Host is up (0.26s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp open  http    nginx
|_http-title: Did not follow redirect to http://2million.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.27 seconds
```

After running an Nmap scan, it shows two ports: 22 (SSH) and 80 (HTTP), which redirects us to the domain http://2million.htb. Let's add this new domain to our hosts file.

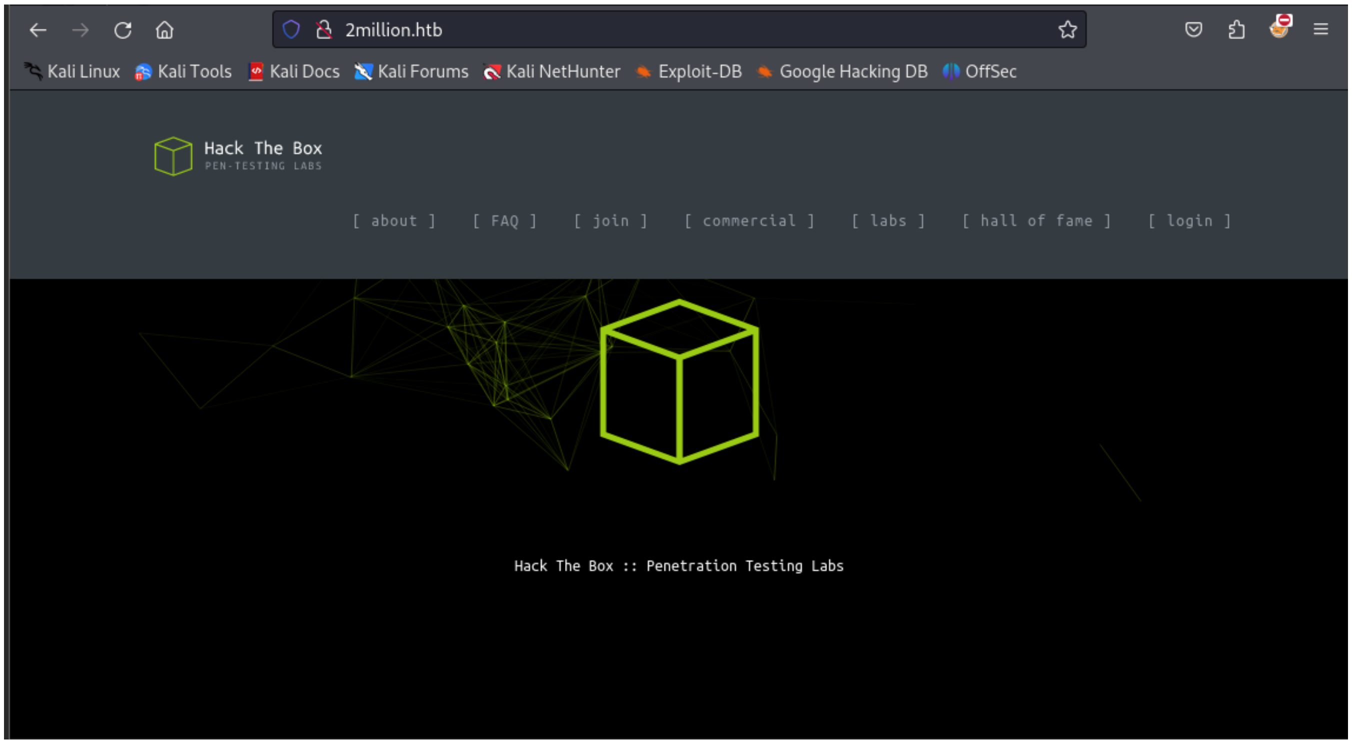
```
sudo nano /etc/hosts
```



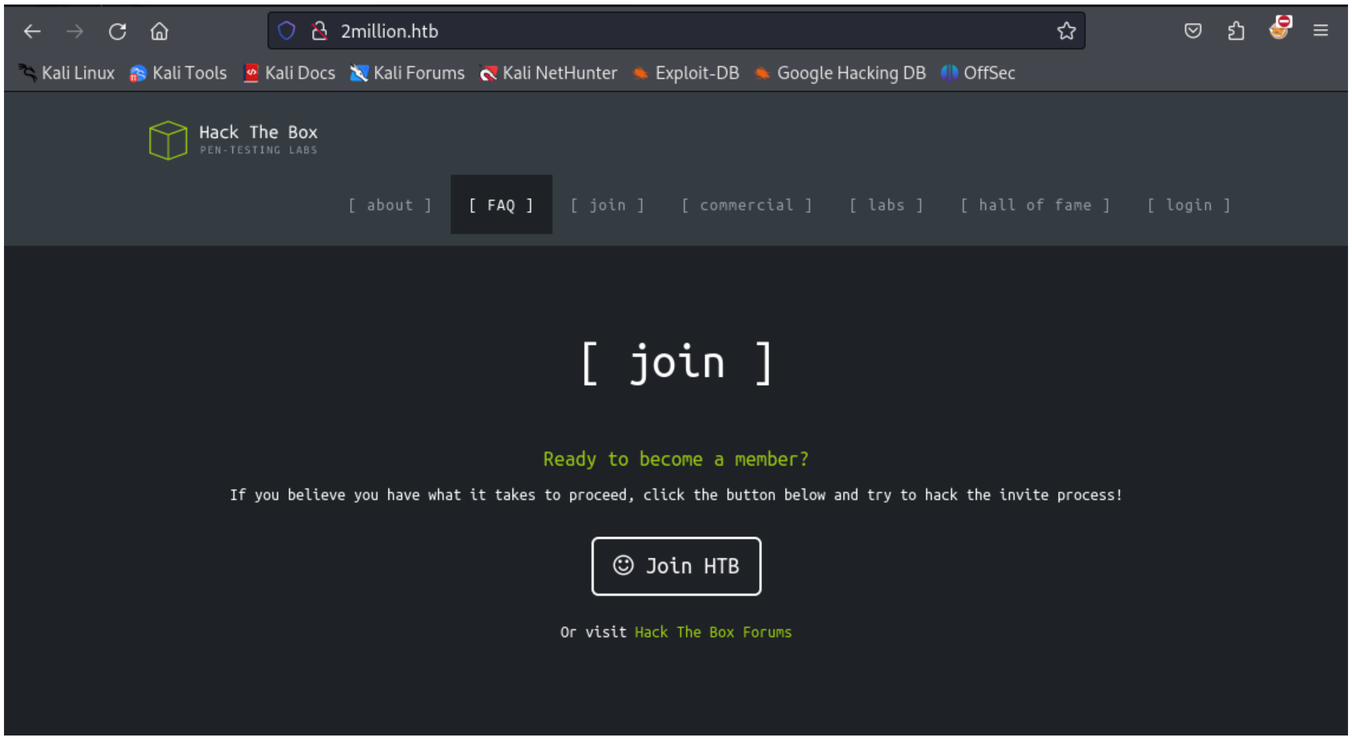
```
127.0.0.1       localhost
127.0.1.1       kali

10.129.134.234  2million.htb

::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
```

WebSite

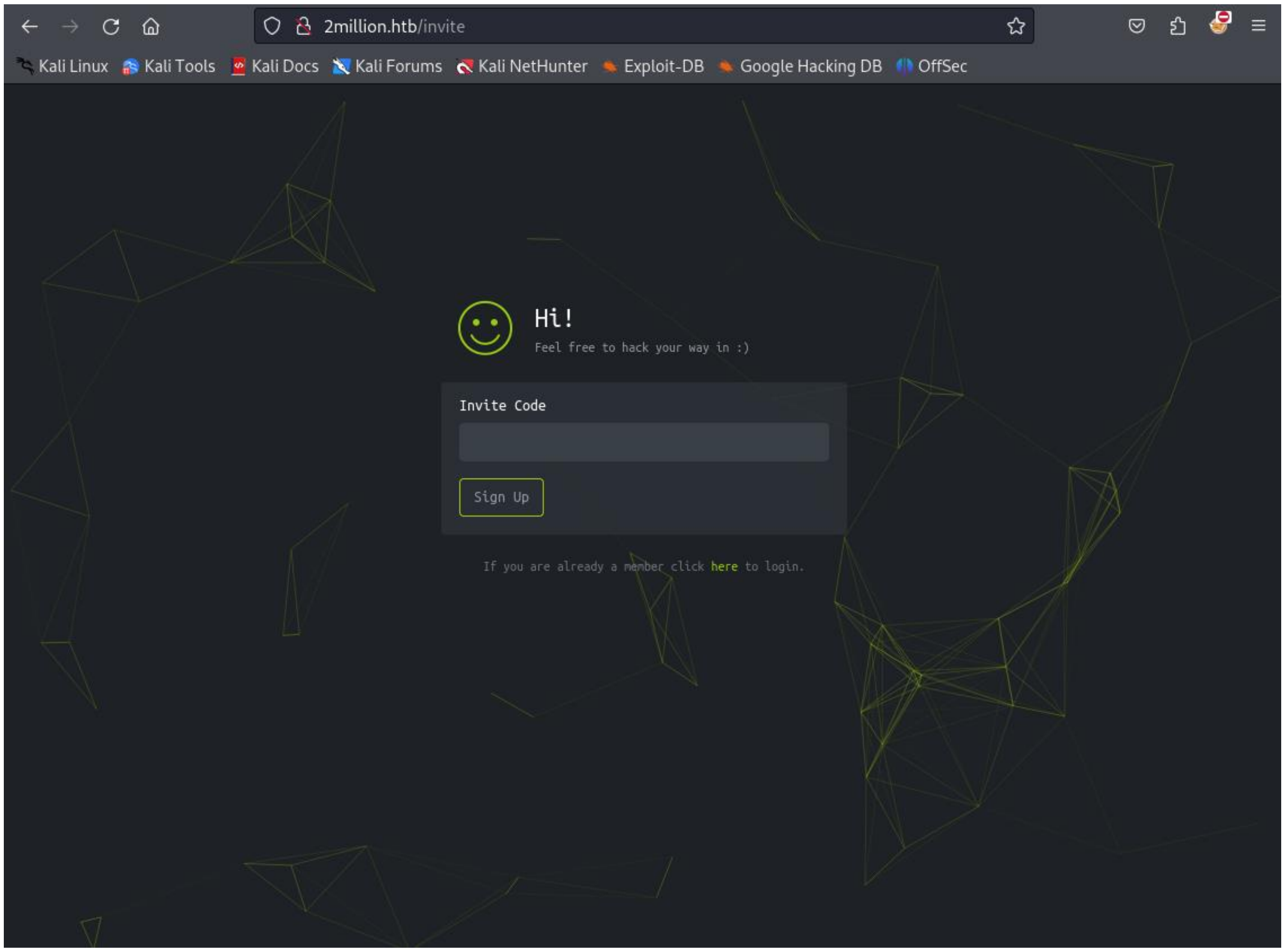
Try typing the domain in your browser, it will display a webpage like this



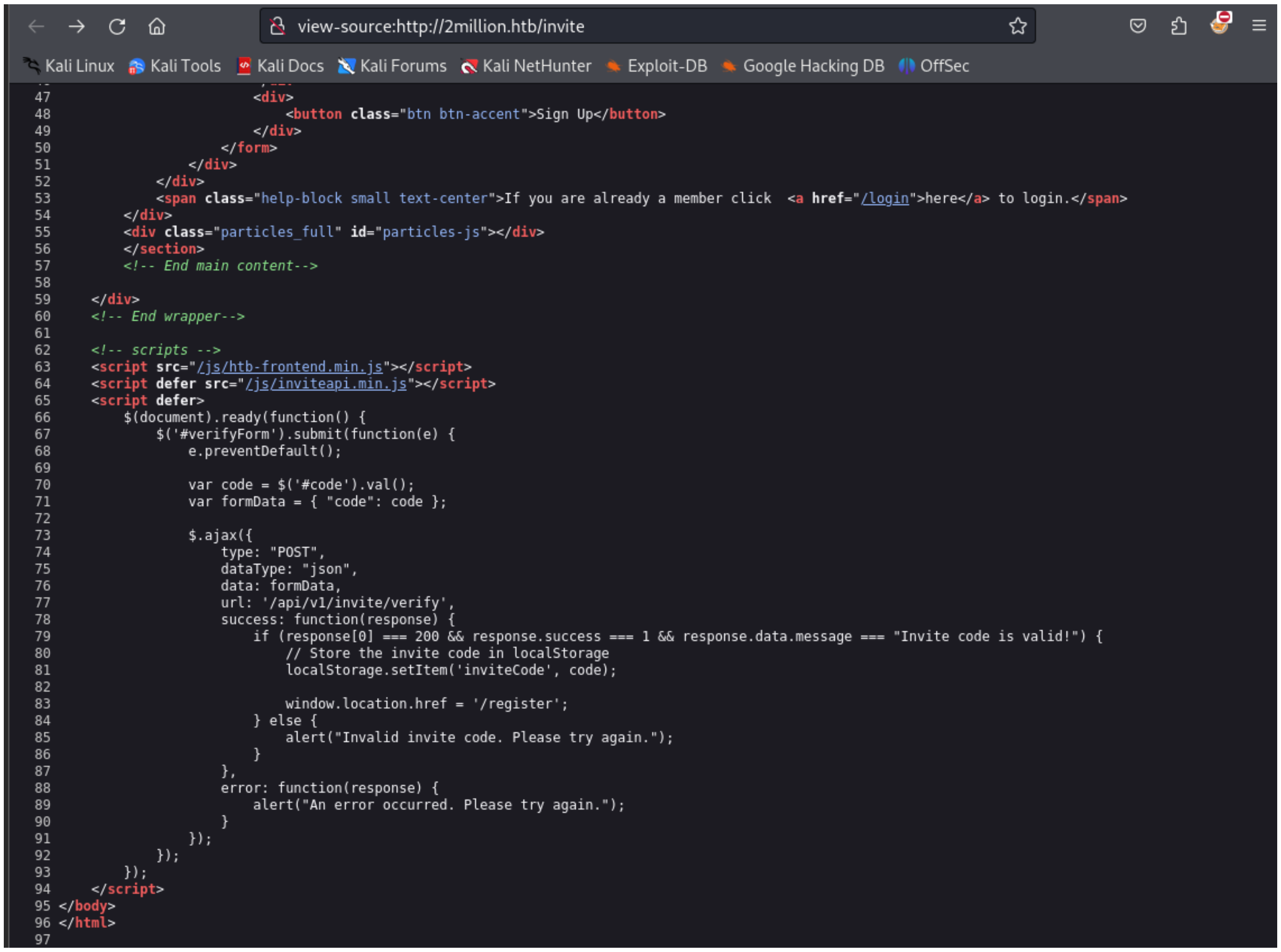
The website contains some interesting sections



If you believe you have what it takes to proceed, click the button below and try to hack the invite process!



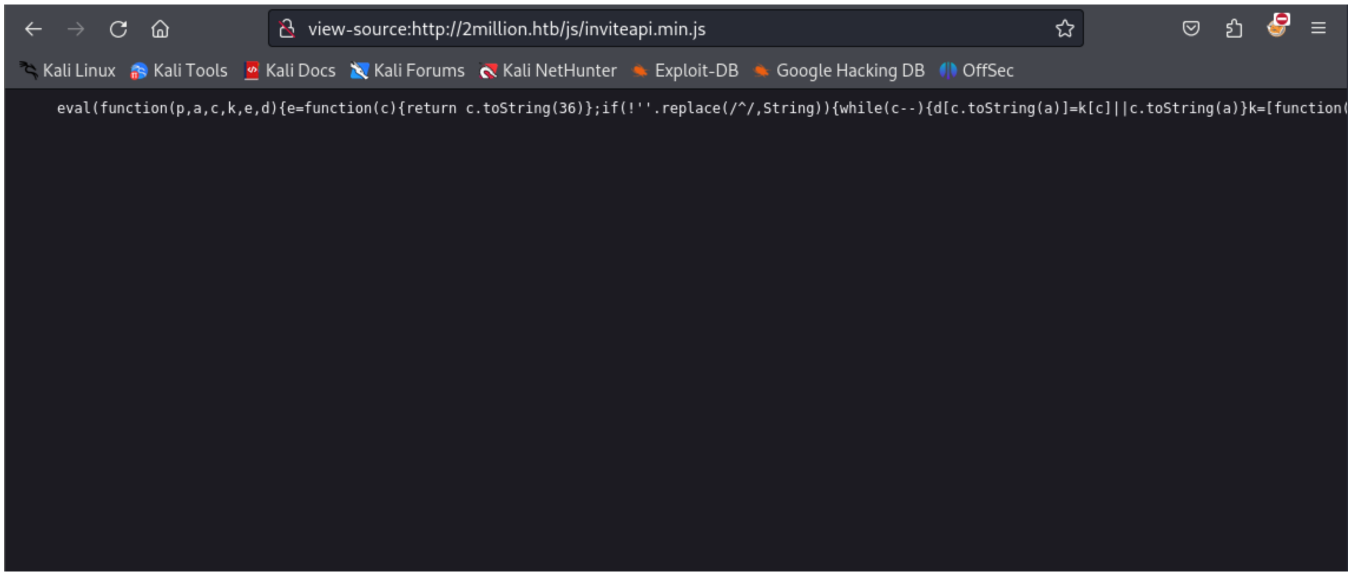
This is one of the most interesting parts. In the /invite directory, we can see that a code is required to sign up. Let's check the source code.



view-source:http://2million.htb/invite

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
                        <div>
                            <button class="btn btn-accent">Sign Up</button>
                        </div>
                    </form>
                </div>
            </div>
            <span class="help-block small text-center">If you are already a member click  <a href="/login">here</a> to login.</span>
        </div>
        <div class="particles_full" id="particles-js"></div>
        </section>
        <!-- End main content-->

    </div>
    <!-- End wrapper-->

    <!-- scripts -->
    <script src="/js/htb-frontend.min.js"></script>
    <script defer src="/js/inviteapi.min.js"></script>
    <script defer>
        $(document).ready(function() {
            $('#verifyForm').submit(function(e) {
                e.preventDefault();

                var code = $('#code').val();
                var formData = { "code": code };

                $.ajax({
                    type: "POST",
                    dataType: "json",
                    data: formData,
                    url: '/api/v1/invite/verify',
                    success: function(response) {
                        if (response[0] === 200 && response.success === 1 && response.data.message === "Invite code is valid!") {
                            // Store the invite code in localStorage
                            localStorage.setItem('inviteCode', code);

                            window.location.href = '/register';
                        } else {
                            alert("Invalid invite code. Please try again.");
                        }
                    },
                    error: function(response) {
                        alert("An error occurred. Please try again.");
                    }
                });
            });
        });
    </script>
</body>
</html>
```

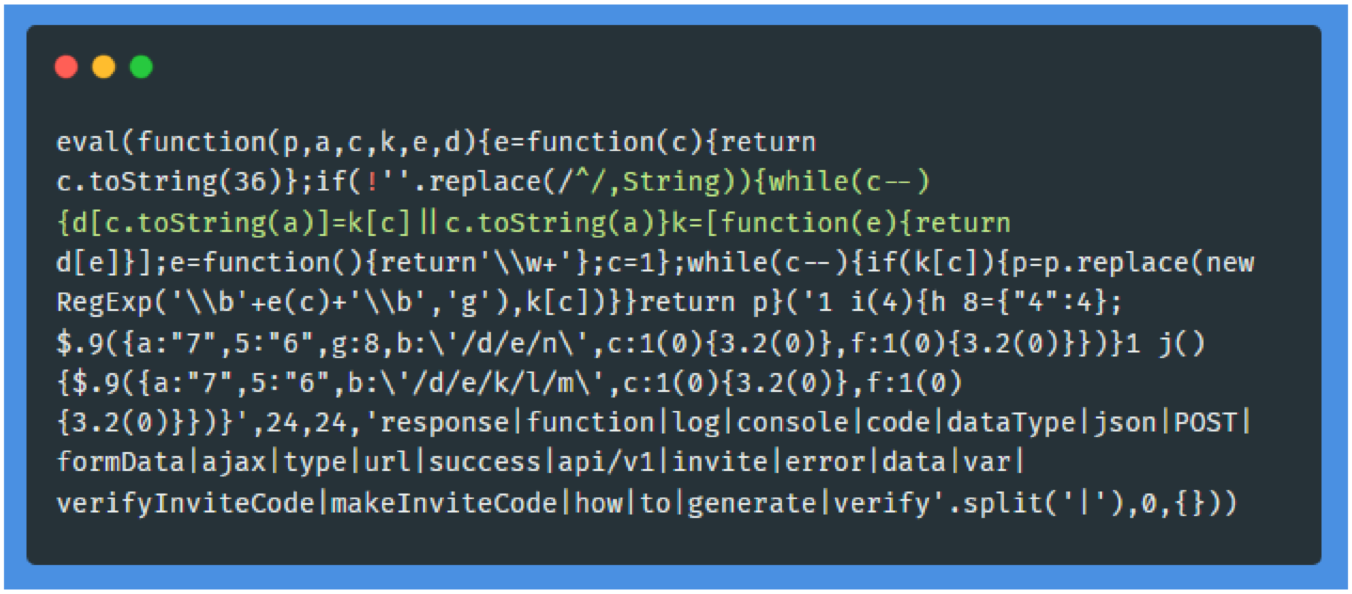


view-source:http://2million.htb/js/inviteapi.min.js

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

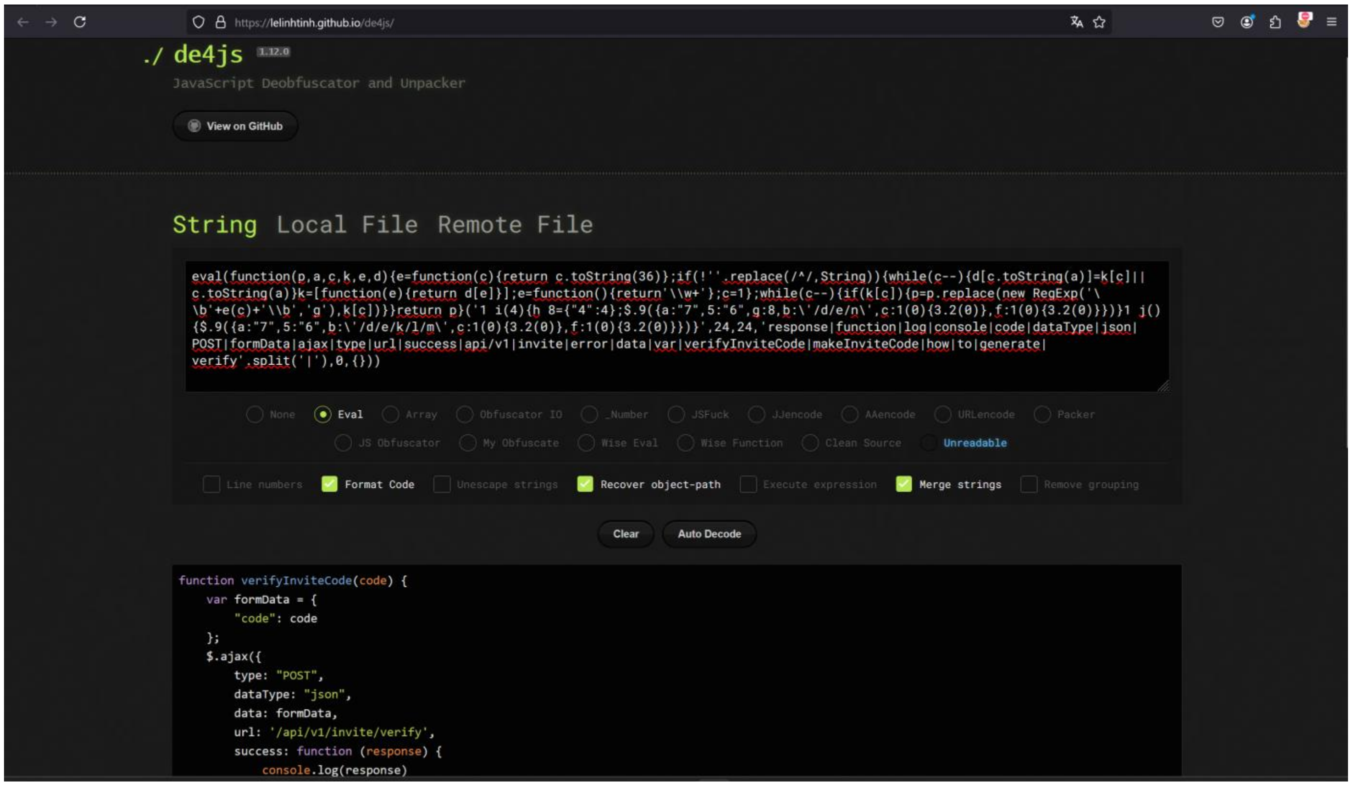
```
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(
```

In the source code, we can see “inviteapi.min.js”. Let’s check this file, but it’s obfuscate, so we need to deobfuscate that two understand that.



```
eval(function(p,a,c,k,e,d){e=function(c){return
c.toString(36)};if(!''.replace(/^/,String)){while(c--)
{d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return
d[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}('1 i(4){h 8={"4":4};
$.9({a:"7",5:"6",g:8,b:\'/d/e/n\',c:1(0){3.2(0)},f:1(0){3.2(0)}})}1 j()
{$.9({a:"7",5:"6",b:\'/d/e/k/l/m\',c:1(0){3.2(0)},f:1(0)
{3.2(0)}})}',24,24,'response|function|log|console|code|dataType|json|POST|
formData|ajax|type|url|success|api/v1|invite|error|data|var|
verifyInviteCode|makeInviteCode|how|to|generate|verify'.split('|'),0,{}))
```

You can use https://lelinhtinh.github.io/de4js/ to deobfuscate the code and understand it.

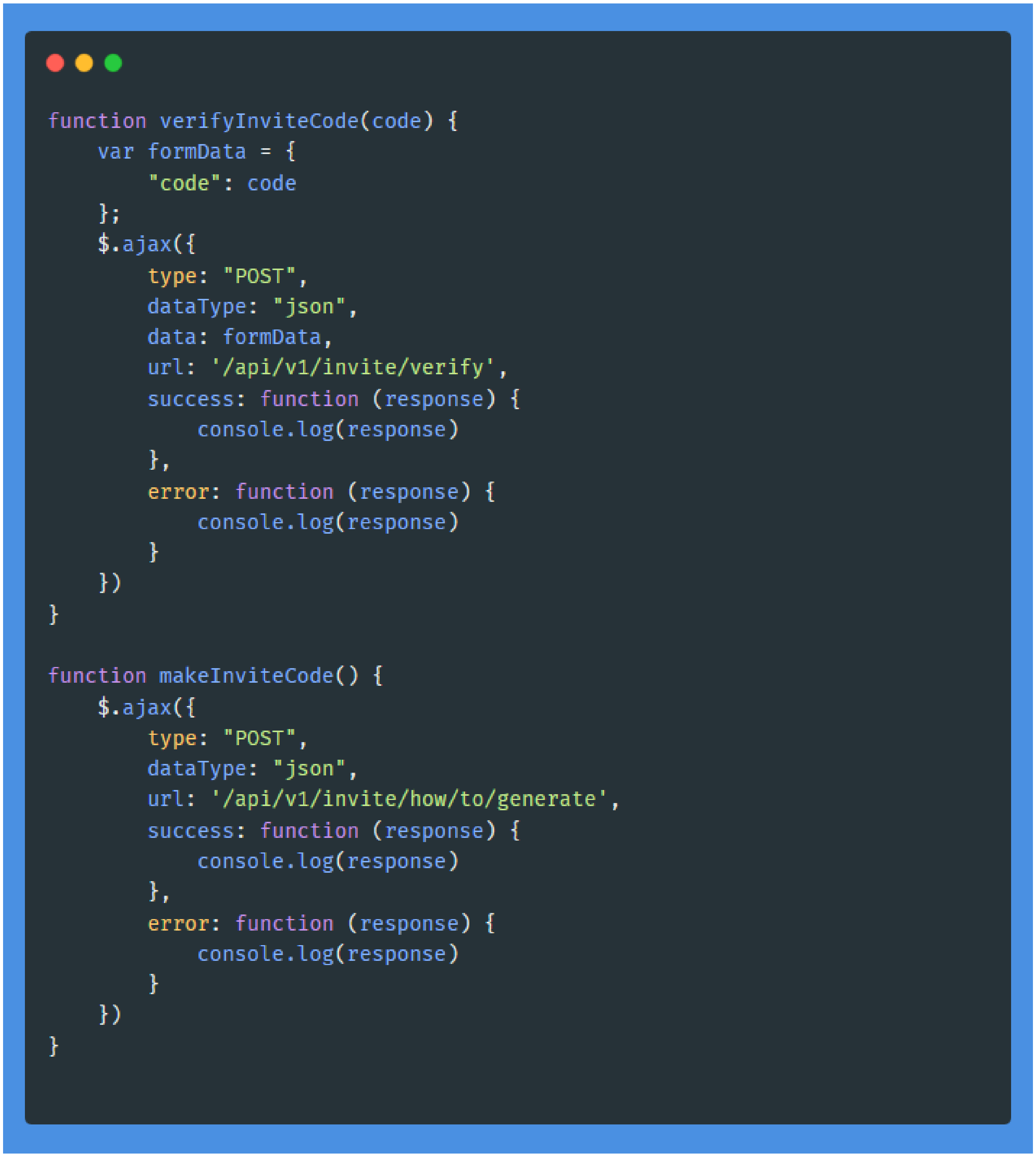

https://lelinhtinh.github.io/de4js/
./ de4js 1.12.0
JavaScript Deobfuscator and Unpacker
View on GitHub
String Local File Remote File

```
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--){d[c.toString(a)]=k[c]||
c.toString(a)}k=[function(e){return d[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}('1 i(4){h 8={"4":4};$.9({a:"7",5:"6",g:8,b:\'/d/e/n\',c:1(0){3.2(0)},f:1(0){3.2(0)}})}1 j()
{$.9({a:"7",5:"6",b:\'/d/e/k/l/m\',c:1(0){3.2(0)},f:1(0){3.2(0)}})}',24,24,'response|function|log|console|code|dataType|json|
POST|formData|ajax|type|url|success|api/v1|invite|error|data|var|verifyInviteCode|makeInviteCode|how|to|generate|
verify'.split('|'),0,{}))
```

None [✓ Eval] Array Obfuscator IO _Number JSFuck JJencode AAencode URLencode Packer
JS Obfuscator My Obfuscate Wise Eval Wise Function Clean Source Unreadable

Line numbers [✓ Format Code] Unescape strings [✓ Recover object-path] Execute expression [✓ Merge strings] Remove grouping

```
function verifyInviteCode(code) {
    var formData = {
        "code": code
    };
    $.ajax({
        type: "POST",
        dataType: "json",
        data: formData,
        url: '/api/v1/invite/verify',
        success: function (response) {
            console.log(response)
```



```
function verifyInviteCode(code) {
    var formData = {
        "code": code
    };
    $.ajax({
        type: "POST",
        dataType: "json",
        data: formData,
        url: '/api/v1/invite/verify',
        success: function (response) {
            console.log(response)
        },
        error: function (response) {
            console.log(response)
        }
    })
}

function makeInviteCode() {
    $.ajax({
        type: "POST",
        dataType: "json",
        url: '/api/v1/invite/how/to/generate',
        success: function (response) {
            console.log(response)
        },
        error: function (response) {
            console.log(response)
        }
    })
}
```

The code has two functions, verifyInviteCode and makeInviteCode, the second function is so interesting, this function makes a POST request to /api/v1/invite/how/to/generate