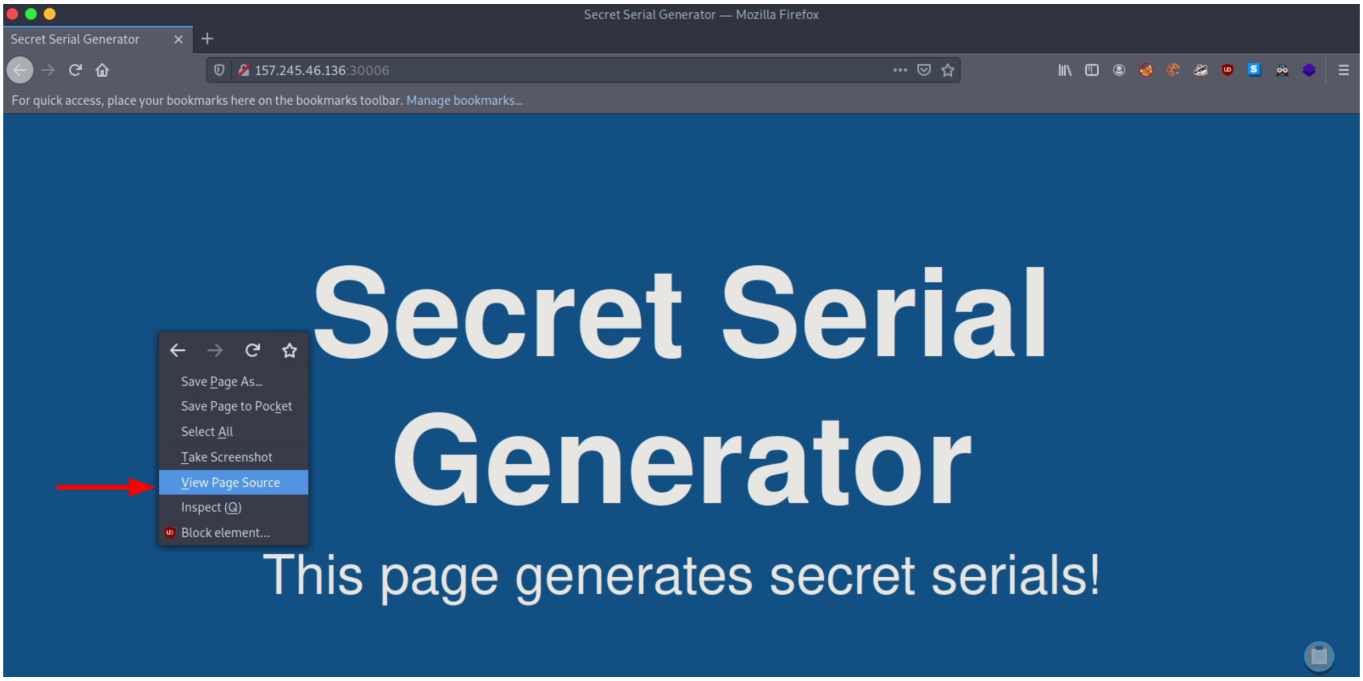
JavaScript Deofuscation

Source Code

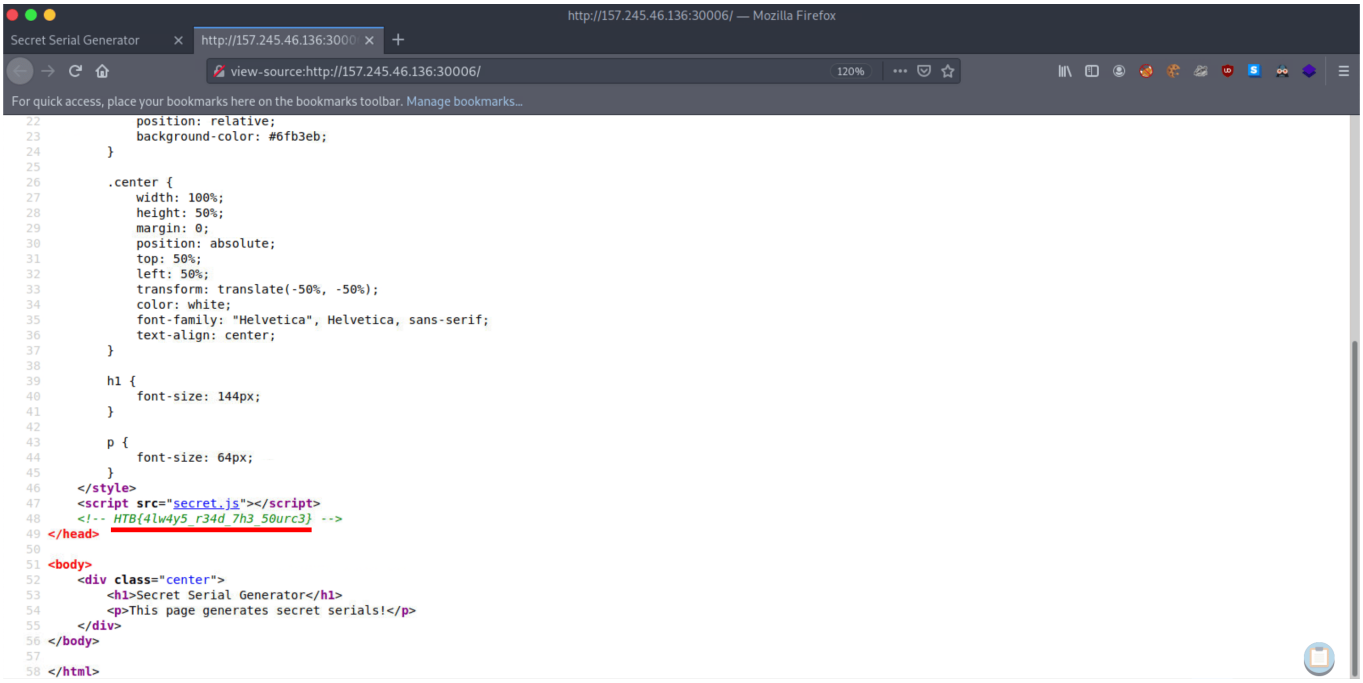
Question 1

"Repeat what you learned in this section, and you should find a secret flag, what is it?"

After spawning the target machine, students need to visit its website's root page and view its source:



Upon viewing the page source, students will find an exposed HTML comment on line 48 which holds the flag:



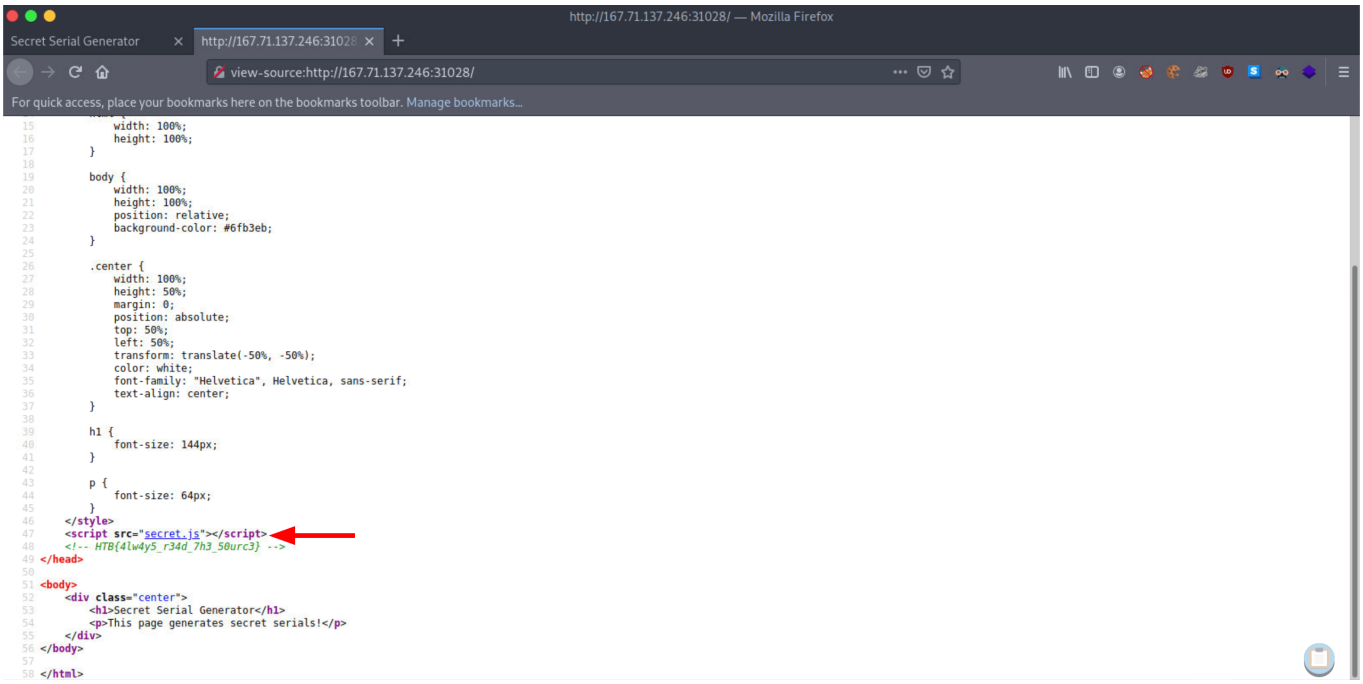
Answer: `HTB{4lw4y5_r34d_7h3_50urc3}`

Deobfuscation

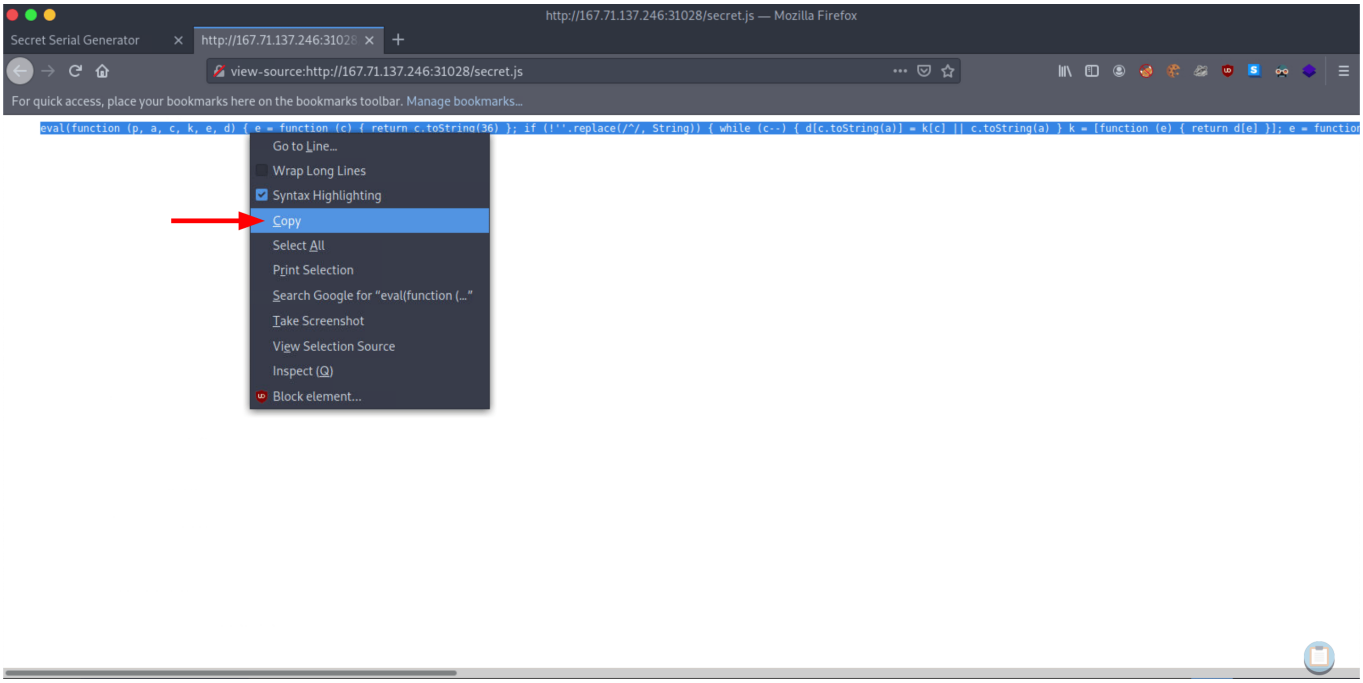
Question 1

"Using what you learned in this function, try to deobfuscate 'secret.js' in order to get the content of the flag. What is the flag?"

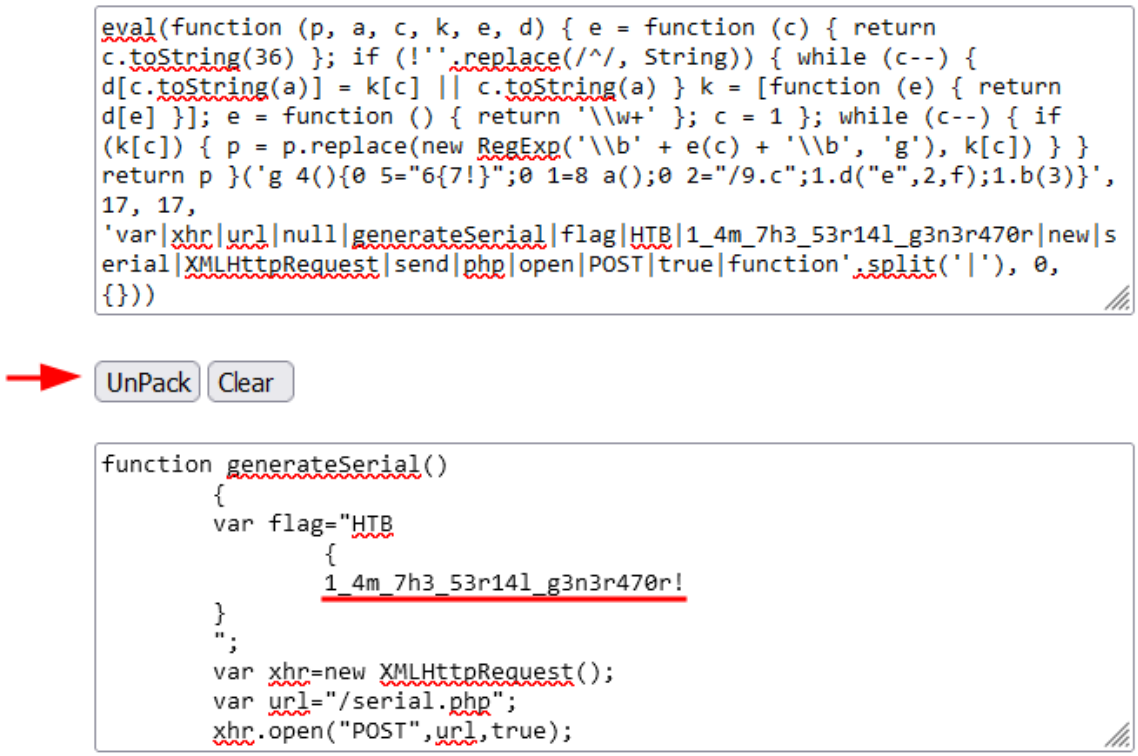
After spawning the target machine, students need to view the page source of its website's root page and notice that on line 47, there is an externally referenced JavaScript file named "secret.js":



Students need to click on it, then double-click on the JavaScript code found within it and copy it:



Then, students need to paste the JavaScript code they pasted into UnPacker and click on "UnPack" to find the flag:



Answer: `HTB{1_4m_7h3_53r14l_g3n3r470r!}`

HTTP Requests

Question 1

"Try applying what you learned in this section by sending a 'POST' request to '/serial.php'. What is the response you get?"

After spawning the target machine, students need to send a `POST` request to `/serial.php` using `cURL` (`-w "\n"` adds a newline character after the response returned by the server) to get back the flag as the response:

Code: shell

```
curl -w "\n" -s -X POST http://STMIP:STMPO/serial.php
```

```
┌─[us-academy-1]─[10.10.14.215]─[htb-ac413848@pwnbox-base]─[~]
└──╼ [★]$ curl -w "\n" -s -X POST http://157.245.46.136:32682/serial.php
```

```
N2gxNV8xNV9hX3MzY3IzN19tMzU1NGcz
```

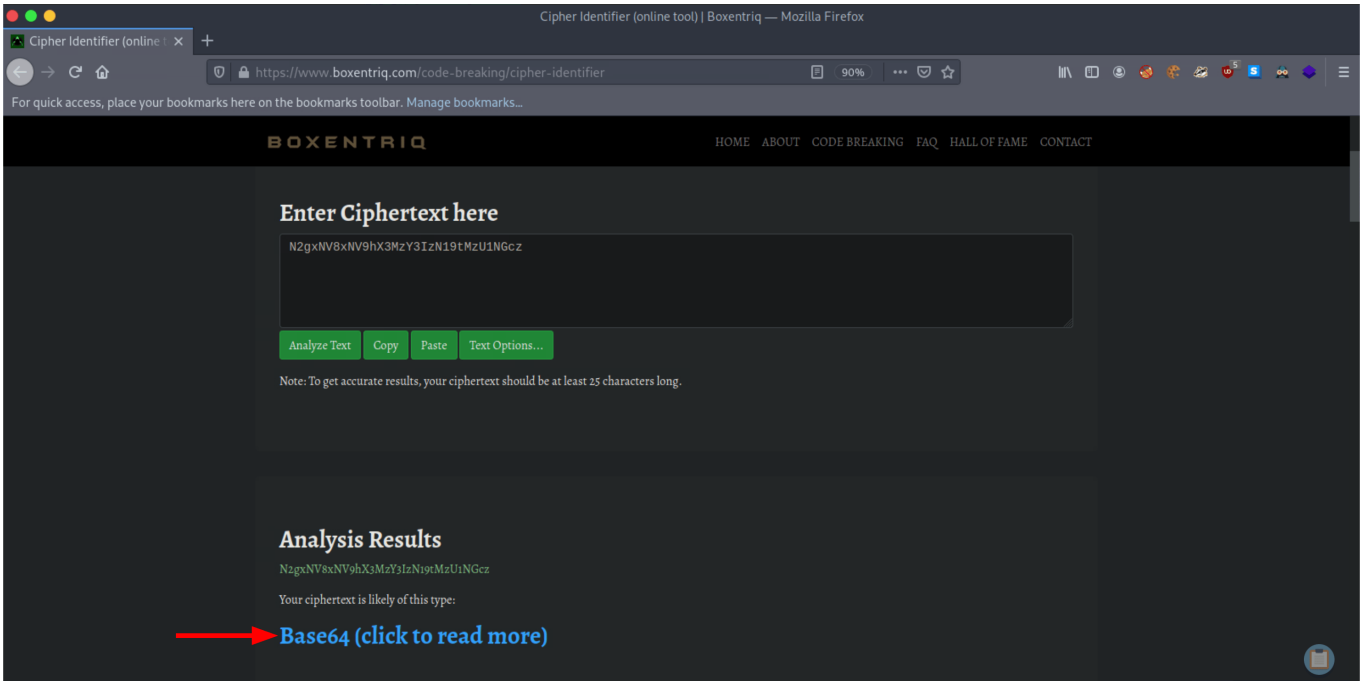
Answer: `N2gxNV8xNV9hX3MzY3IzN19tMzU1NGcz`

Decoding

Question 1

"Using what you learned in this section, determine the type of encoding used in the string you got at previous exercise, and decode it. To get the flag, you can send a 'POST' request to 'serial.php', and set the data as "serial=YOUR_DECODED_OUTPUT"."

Students first need to determine the type of encoding of the previously found flag by using the Cipher Identifier website. After pasting the flag and clicking on "Analyze Text", the website will show that it is base64-encoded:



Thus, to decode it, students can use `echo` and pipe the output to `base64` with the `-d` flag:

Code: shell

```
echo 'N2gxNV8xNV9hX3MzY3IzN19tMzU1NGcz' | base64 -d
```

```
┌─[us-academy-1]─[10.10.14.215]─[htb-ac413848@pwnbox-base]─[~]
└──╼ [★]$ echo 'N2gxNV8xNV9hX3MzY3IzN19tMzU1NGcz' | base64 -d

7h15_15_a_s3cr37_m3554g3
```

Students now need to send a `POST` request to spawned target machine, specifically to `/serial.php`, passing to it the data `serial=7h15_15_a_s3cr37_m3554g3` to get back the flag as the response:

Code: shell

```
curl -w "\n" -s -X POST "http://STMIP:STMPO/serial.php" -d
"serial=7h15_15_a_s3cr37_m3554g3"
```

```
┌─[us-academy-1]─[10.10.14.215]─[htb-ac413848@pwnbox-base]─[~]
└──╼ [★]$ curl -w "\n" -s -X POST "http://167.71.139.140:31464/serial.php" -
d "serial=7h15_15_a_s3cr37_m3554g3"

HTB{ju57_4n07h3r_r4nd0m_53r14l}
```

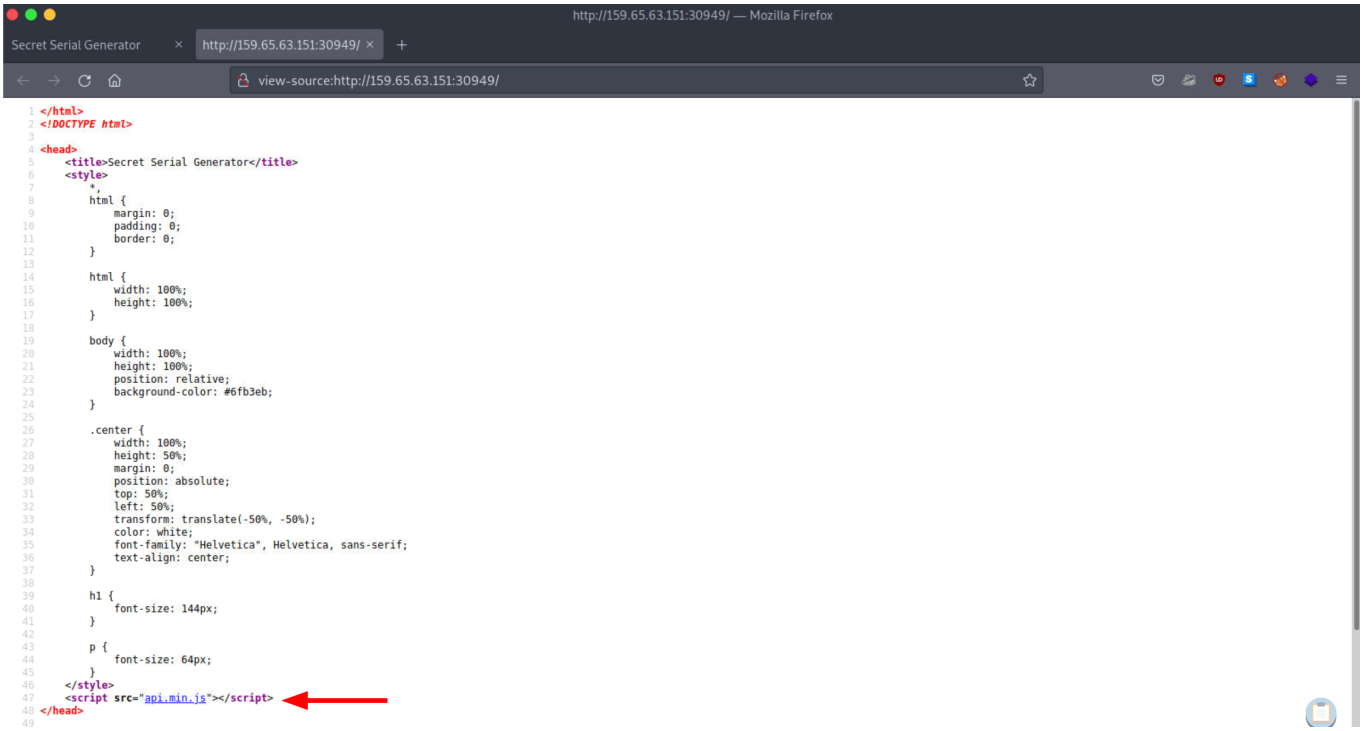
Answer: `HTB{ju57_4n07h3r_r4nd0m_53r14l}`

Skills Assessment

Question 1

"Try to study the HTML code of the webpage, and identify used JavaScript code within it. What is the name of the JavaScript file being used?"

After spawning the target machine, students need to navigate to its website's root page and view its source, to find that on line 47, the file `api.min.js` is included as a JavaScript script:



Answer: `api.min.js`

Skills Assessment

Question 2

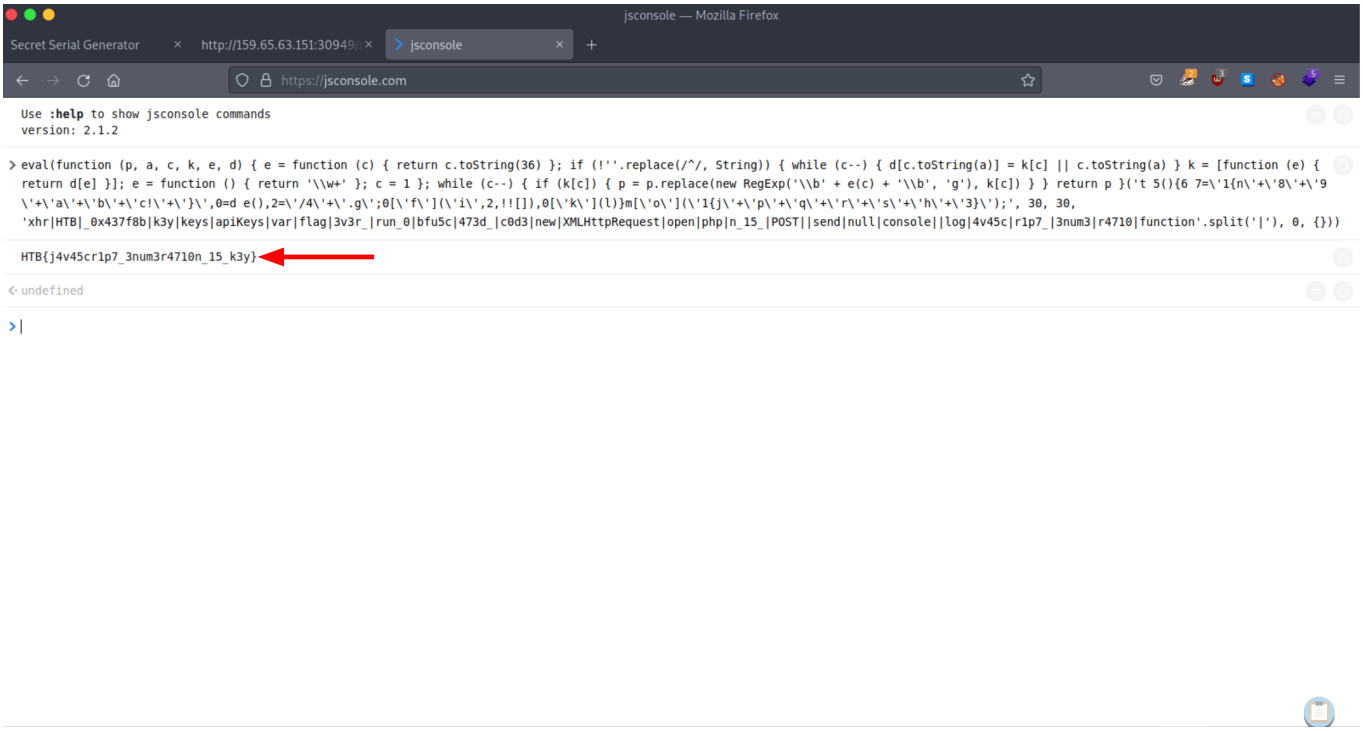
"Once you find the JavaScript code, try to run it to see if it does any interesting functions. Did you get something in return?"

From the previous question, students will know about the `api.min.js` JavaScript file:

Code: javascript

```
eval(function (p, a, c, k, e, d) { e = function (c) { return c.toString(36)
}; if (!''.replace(/^/, String)) { while (c--) { d[c.toString(a)] = k[c] ||
c.toString(a) } k = [function (e) { return d[e] }]; e = function () { return
'\\w+' }; c = 1 }; while (c--) { if (k[c]) { p = p.replace(new RegExp('\\b'
+ e(c) + '\\b', 'g'), k[c]) } } return p }('t 5(){6
7=\'1{n\'+\'8\'+\'9\'+\'a\'+\'b\'+\'c!\'+\'}\',0=d
e(),2=\'/4\'+\'.g\';0[\'f\'](\'i\',2,!![]),0[\'k\'](l)}m[\'o\']
(\'1{j\'+\'p\'+\'q\'+\'r\'+\'s\'+\'h\'+\'3}\');', 30, 30,
'xhr|HTB|_0x437f8b|k3y|keys|apiKeys|var|flag|3v3r_|run_0|bfu5c|473d_|c0d3|ne
w|XMLHttpRequest|open|php|n_15_|POST||send|null|console||log|4v45c|r1p7_|3nu
m3|r4710|function'.split('|'), 0, {}))
```

Thus, students need to paste the code within the file inside of JSConsole to attain the flag `HTB{j4v45cr1p7_3num3r4710n_15_k3y}`:



Answer: `HTB{j4v45cr1p7_3num3r4710n_15_k3y}`

Skills Assessment

Question 3

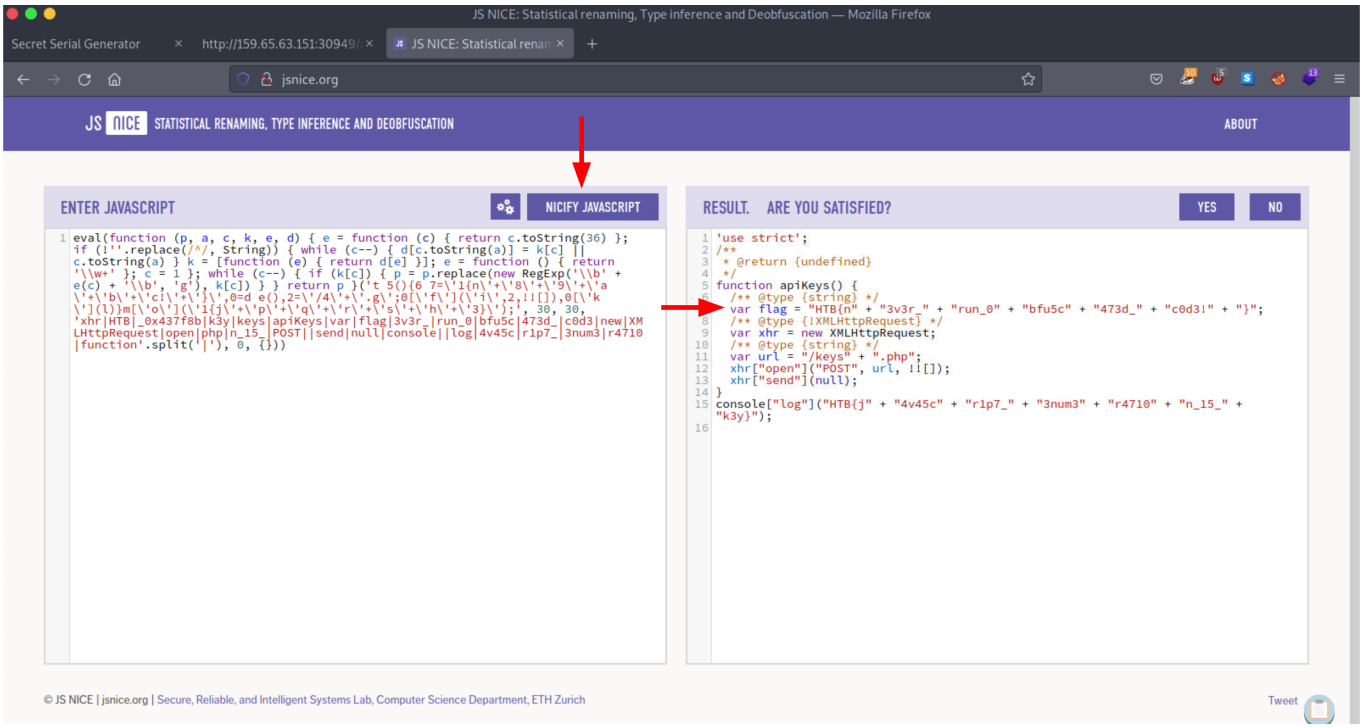
"As you may have noticed, the JavaScript code is obfuscated. Try applying the skills you learned in this module to deobfuscate the code, and retrieve the 'flag' variable."

Students need to use the previously attained `api.min.js` JavaScript code and paste it inside JS Nice then click on "NICIFY JAVASCRIPT":

Code: javascript

```
eval(function (p, a, c, k, e, d) { e = function (c) { return c.toString(36)
}; if (!''.replace(/^/, String)) { while (c--) { d[c.toString(a)] = k[c] ||
c.toString(a) } k = [function (e) { return d[e] }]; e = function () { return
'\\w+' }; c = 1 }; while (c--) { if (k[c]) { p = p.replace(new RegExp('\\b'
+ e(c) + '\\b', 'g'), k[c]) } } return p }('t 5(){6
7=\'1{n\'+\'8\'+\'9\'+\'a\'+\'b\'+\'c!\'+\'}\',0=d
e(),2=\'/4\'+\'.g\';0[\'f\'](\'i\',2,!![]),0[\'k\'](l)}m[\'o\']
```

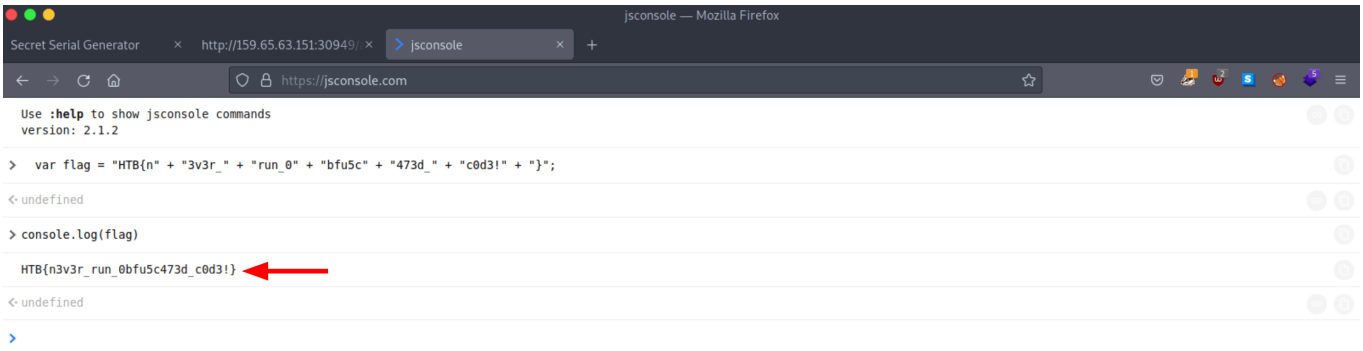
```
(\'1{j\'+\'p\'+\'q\'+\'r\'+\'s\'+\'h\'+\'3}\');', 30, 30,
'xhr|HTB|_0x437f8b|k3y|keys|apiKeys|var|flag|3v3r_|run_0|bfu5c|473d_|c0d3|ne
w|XMLHttpRequest|open|php|n_15_|POST||send|null|console||log|4v45c|r1p7_|3nu
m3|r4710|function'.split('|'), 0, {}))
```



Students will notice that the "flag" variable on line 7 contains the flag for this question, thus, they can copy and paste it into JSConsole, and run `console.log(flag)` to attain the flag `HTB{n3v3r_run_0bfu5c473d_c0d3!}`:

Code: javascript

```
  var flag = "HTB{n" + "3v3r_" + "run_0" + "bfu5c" + "473d_" + "c0d3!" +
"}";
  console.log(flag)
```



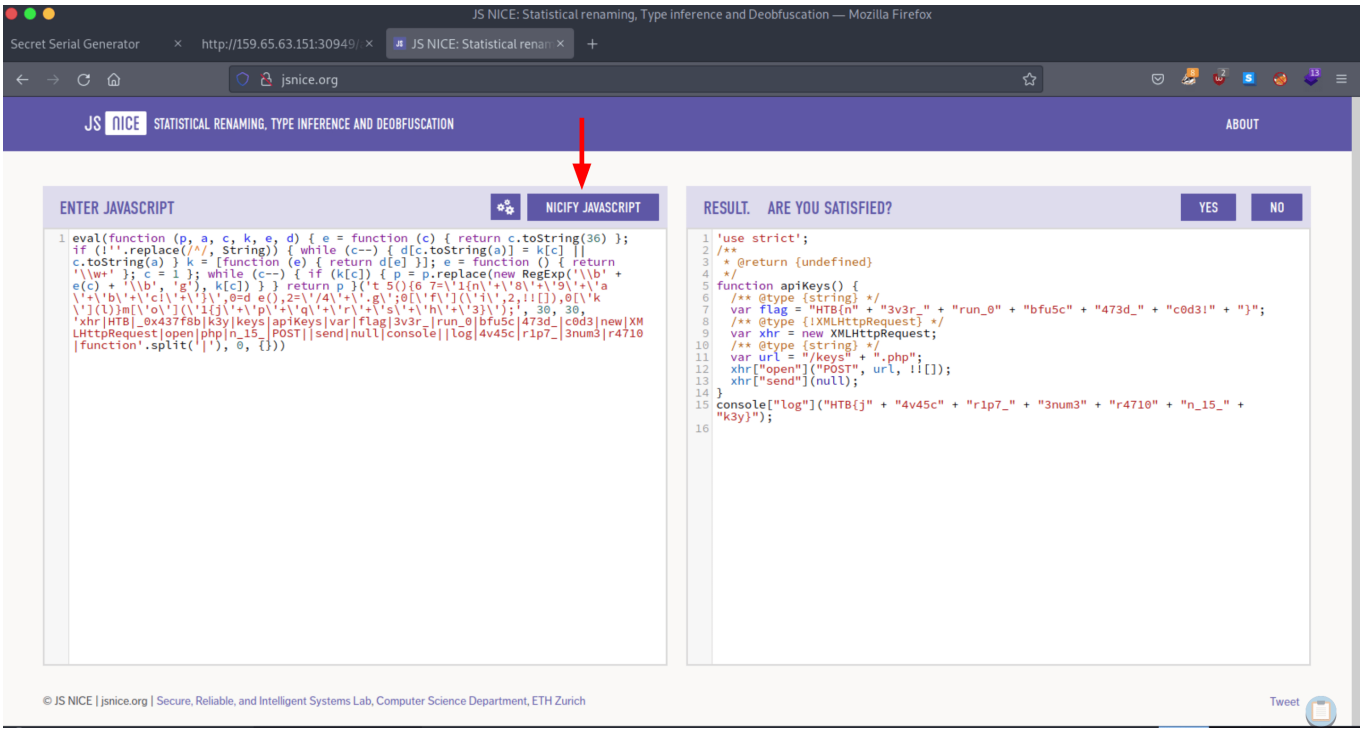
Answer: `HTB{n3v3r_run_0bfu5c473d_c0d3!}`

Skills Assessment

Question 4

"Try to Analyze the deobfuscated JavaScript code, and understand its main functionality. Once you do, try to replicate what it's doing to get a secret key. What is the key?"

Students need to analyze the previously attained `api.min.js` JavaScript code after pasting it in JS Nice and clicking on "NICIFY JAVASCRIPT":



Code: javascript

```
'use strict';
/**
 * @return {undefined}
 */
function apiKeys() {
  /** @type {string} */
  var flag = "HTB{n" + "3v3r_" + "run_0" + "bfu5c" + "473d_" + "c0d3!" +
"}";
  /** @type {!XMLHttpRequest} */
  var xhr = new XMLHttpRequest;
  /** @type {string} */
  var url = "/keys" + ".php";
  xhr["open"]("POST", url, !![]);
  xhr["send"](null);
}
console["log"]("HTB{j" + "4v45c" + "r1p7_" + "3num3" + "r4710" + "n_15_" +
"k3y}");
```

After inspecting the code and analyzing, students will notice that an empty `POST` request is sent to the endpoint `/keys.php`, thus, students need to replicate this behavior, using `cURL`, to attain the secret key `4150495f70336e5f37333537316e365f31355f66756e`:

Code: shell

```
curl -w "\n" -s http://STMIP:STMPO/keys.php -X POST
```

```
┌─[us-academy-1]─[10.10.14.169]─[htb-ac413848@htb-jmae2konio]─[~]
└──╼ [★]$ curl -w "\n" -s http://159.65.63.151:30949/keys.php -X POST

4150495f70336e5f37333537316e365f31355f66756e
```

Answer: `4150495f70336e5f37333537316e365f31355f66756e`

Skills Assessment

Question 5

"Once you have the secret key, try to decide it's encoding method, and decode it. Then send a 'POST' request to the same previous page with the decoded key as "key=DECODED_KEY". What is the flag you got?"

Analyzing the previously attained secret key `4150495f70336e5f37333537316e365f31355f66756e`, students will notice that it consists of hexadecimal characters only, thus, they need to decode it as hexadecimal using `xxd`:

```
echo 4150495f70336e5f37333537316e365f31355f66756e | xxd -p -r
```

```
┌─[us-academy-1]─[10.10.14.169]─[htb-ac413848@htb-jmae2konio]─[~]
└──╼ [★]$ echo 4150495f70336e5f37333537316e365f31355f66756e | xxd -p -r

API_p3n_73571n6_15_fun
```

The secret key decodes to `API_p3n_73571n6_15_fun`, therefore, students need to use it as the value for the `POST` parameter `key` sent to the `/keys.php` endpoint, to attain the flag `HTB{r34dy_70_h4ck_my_w4y_1n_2_HTB}`:

```
curl -w "\n" -s http://STMIP:STMPO/keys.php -X POST -d
'key=API_p3n_73571n6_15_fun'
```

```
┌─[us-academy-1]─[10.10.14.169]─[htb-ac413848@htb-ex7aceozgi]─[~]
└──╼ [★]$ curl -w "\n" -s http://167.99.89.94:30232/keys.php -X POST -d
```

```
 'key=API_p3n_73571n6_15_fun'

HTB{r34dy_70_h4ck_my_w4y_1n_2_HTB}
```

Answer: `HTB{r34dy_70_h4ck_my_w4y_1n_2_HTB}`