Skills Assessment

Introduction

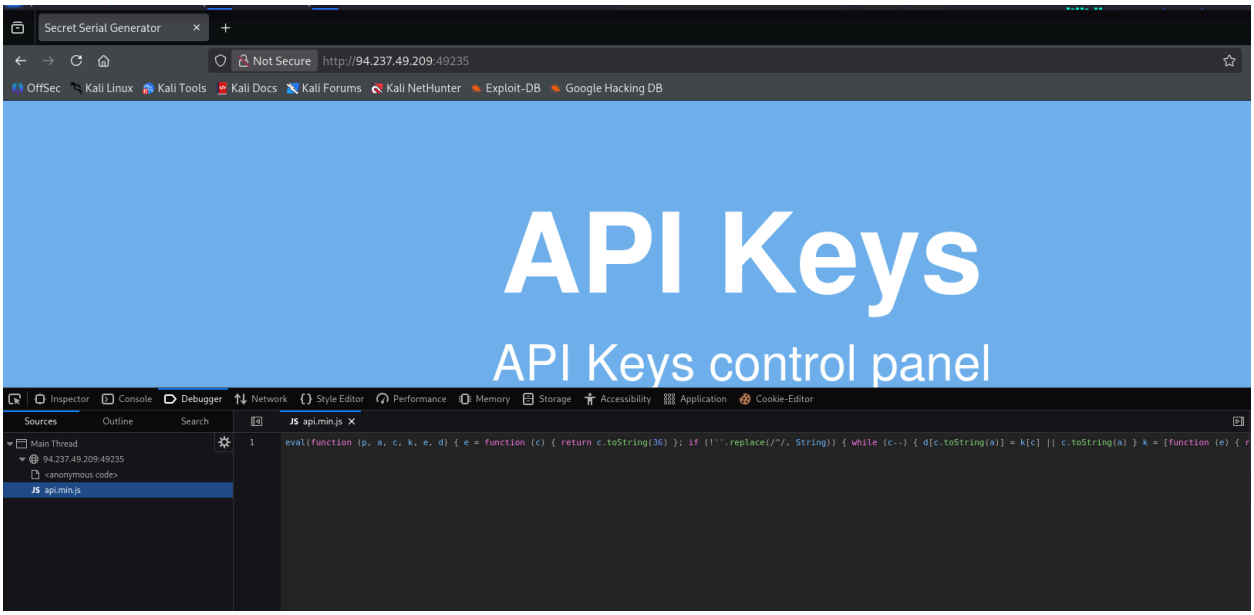
During our Penetration Test, we came across a web server that contains JavaScript and APIs. We need to determine their functionality to understand how it can negatively affect our customer.

Target: 94.237.49.209:49235

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?

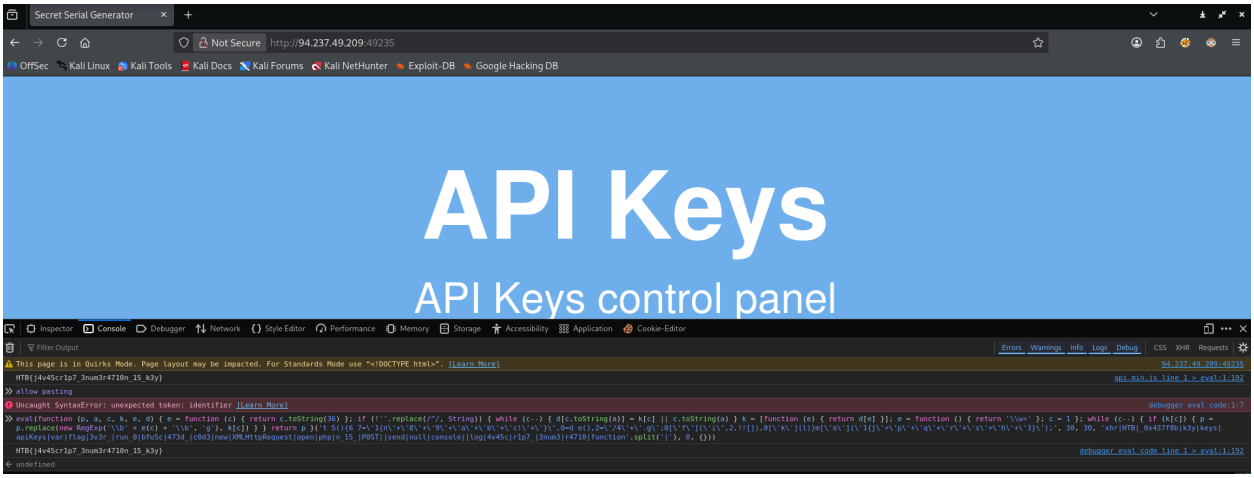
Navigating to the page at the location specified for the lab and then using the fire fox dev tools I am able to identify the javascript file being loaded

The JavaScript file being loaded is api.min.js



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

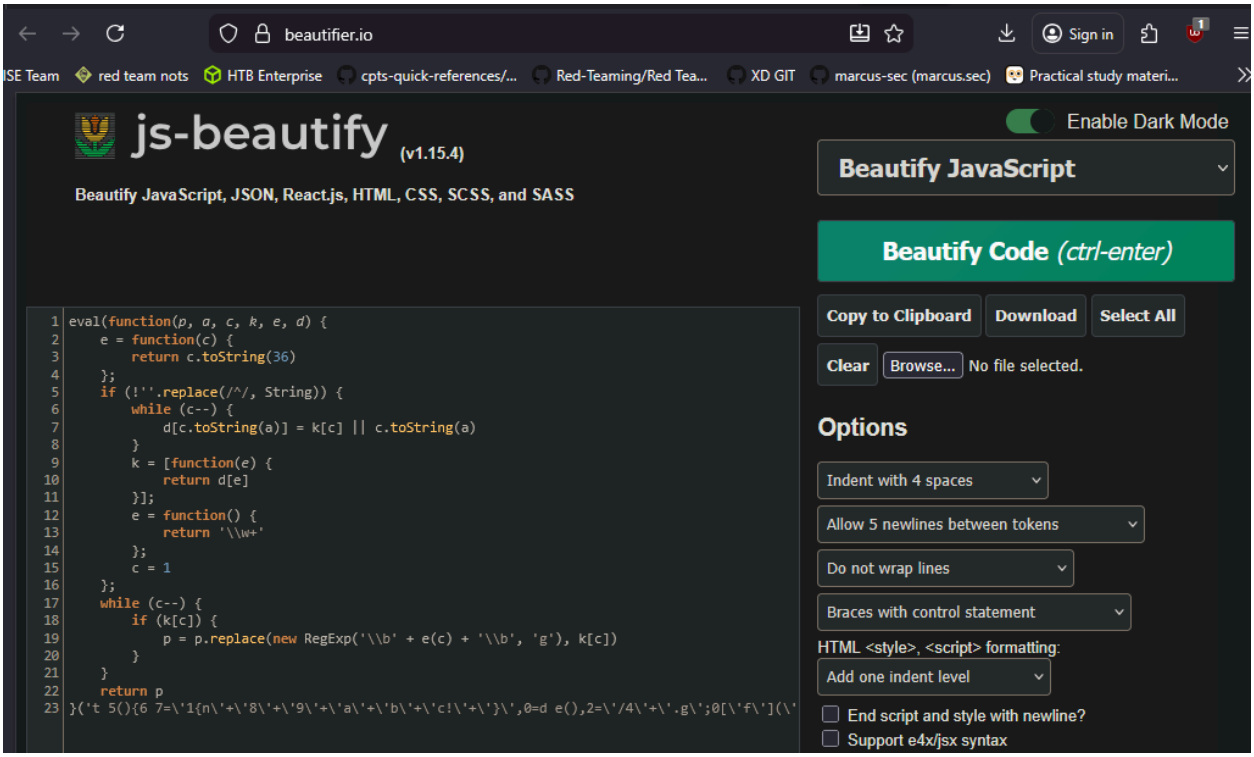
Running the function in the dev tools console I get the flag for this question in return. To run the function I just copied the contents of api.min.js and pasted it into the console.



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.

Looking at the contents of the code in api.min.js (and given the name of the file) I can guess that this java script has been minified. Looking at the contents of the file it is also packed.

The first step I will take is using beautifier.io to deminify the javascript to make it more readable.



Then I wanted to unpack the contents of the file as well. I did so using this website: https://matthewfl.com/unPacker.html

Looking at the bottom pane I can see the contents of the flag variable for this question. After some cleanup I get the following string.

```
HTB{n3v3r_run_0bfu5c473d_c0d3!}
```

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?

```
function apiKeys()
   {
   var flag='HTB
      {
      n'+'3v3r_'+'run_0'+'bfu5c'+'473d_'+'c0d3!'+'
   }
   ',xhr=new XMLHttpRequest(),_0x437f8b='/keys'+'.php';
   xhr['open']('POST',_0x437f8b,!![]),xhr['send'](null)
}
console['log']('HTB
   {
   j'+'4v45c'+'r1p7_'+'3num3'+'r4710'+'n_15_'+'k3y
}
');
```

The console.log is just printing the flag for the previous question. The intresting part is the HTTP request object being made to what looks like a /keys.php endpoint and sending it with null data.

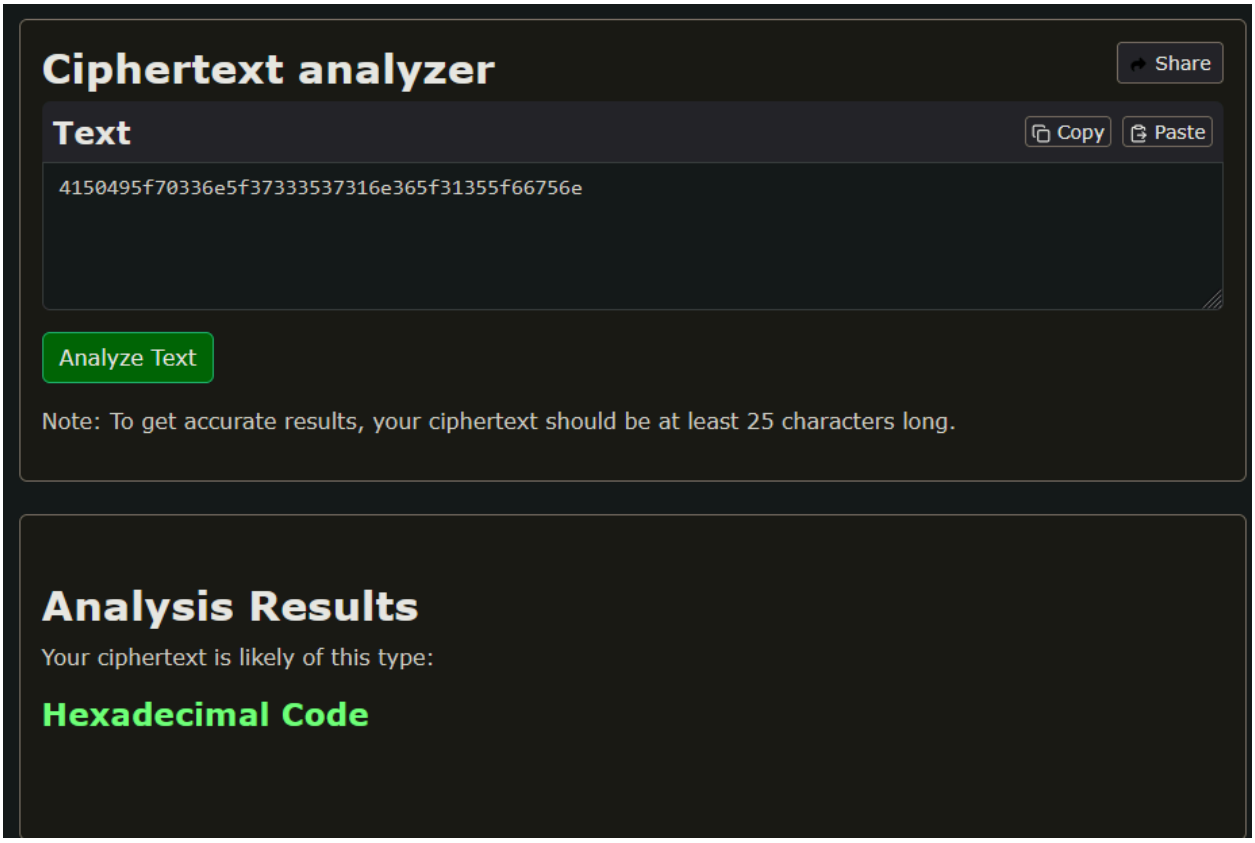
Using curl to send a post request to the keys.php endpoint I get a string in return

```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl -s http://94.237.49.209:49235/keys.php -X POST
4150495f70336e5f37333537316e365f31355f66756e
```

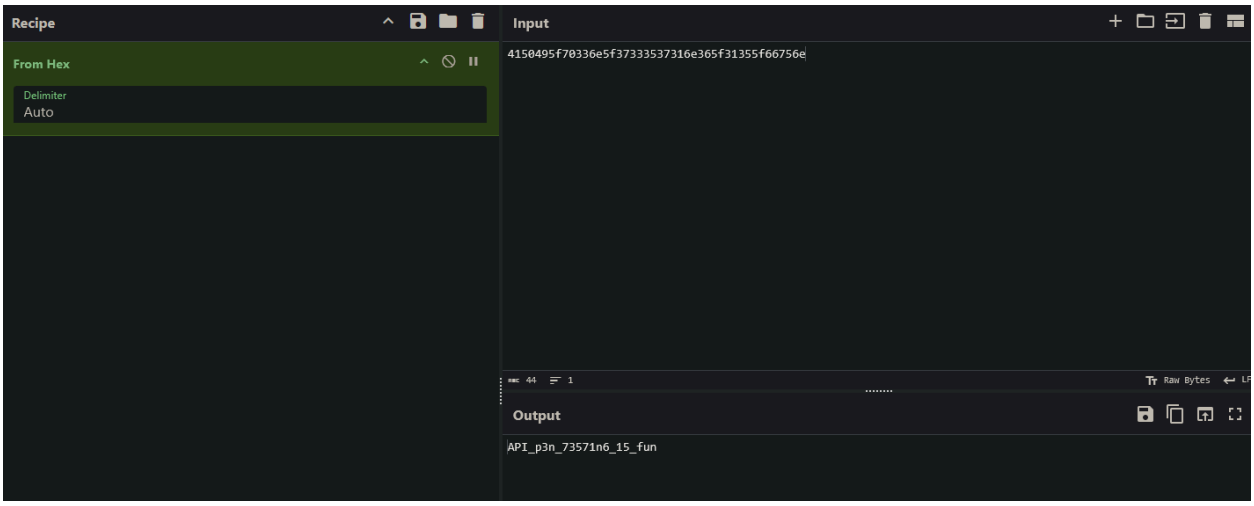
Once you have the secret key, try to decide it's encoding method, and decode it. Then send a 'POST' request to the same previous page with the decoded key as "key=DECODED_KEY". What is the flag you got?

Taking the output from sending a post request to the keys.php endpoint and putting it into a cipher identifier it tells me that it is hexadecimal

https://www.boxentriq.com/code-breaking/cipher-identifier



Putting that hexadecimal string into cyber chef It gives me a string in return



Sending a post request to the /keys.php end point setting the data to the string identified, I get the flag in reutrn

```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl -s http://94.237.49.209:49235/keys.php -X POST -d "key=API_p3n_73571n6_15_fun"
HTB{r34dy_70_h4ck_my_w4y_1n_2_HTB}
```