



# Blinker Fluid

☰ Event	Cyber Apocalypse 2022
☰ Tags	Web
👤 Author	 Jun Peng Tan


## Challenge Description




CHALLENGE INFO

**BlinkerFluids**

*Once known as an imaginary liquid used in automobiles to make the blinkers work is now one of the rarest fuels invented on Klaus' home planet Vinyr. The Golden Fang army has a free reign over this miraculous fluid essential for space travel thanks to the Blinker Fluids™ Corp. Ulysses has infiltrated this supplier organization's one of the HR department tools and needs your help to get into their server. Can you help him?*

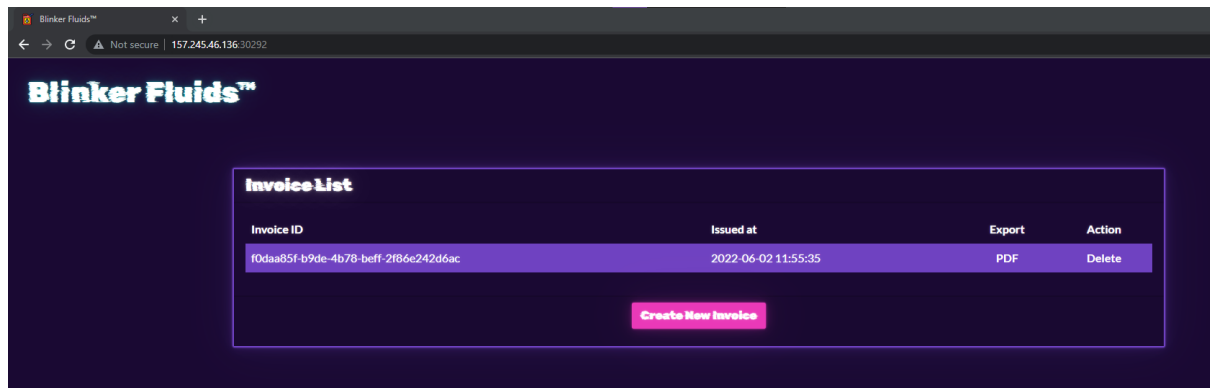
 This challenge is started on-demand.

 This challenge has a downloadable part.

## Challenge Walkthrough

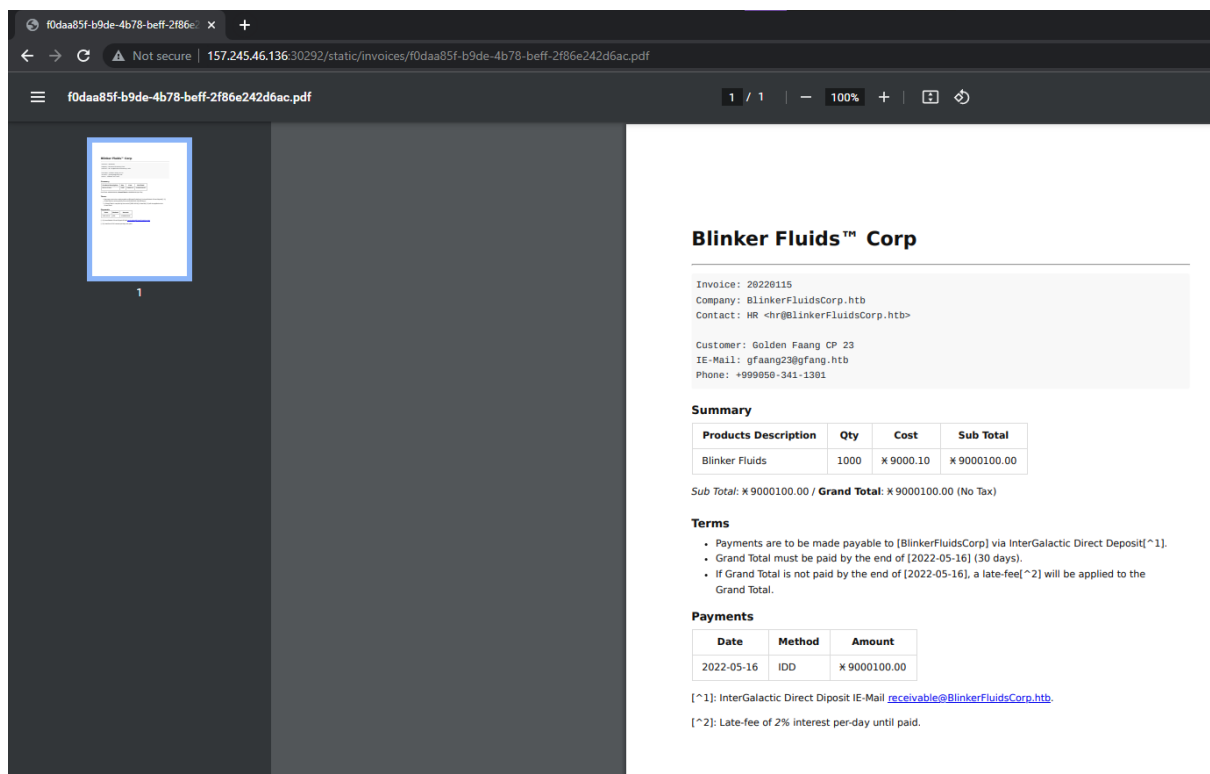
In this challenge, we're given a bunch of files related to the website and the link is provided. Going through the link given, the website let us to generate the new pdf invoice.





Inside the website, there is a pdf inside. We can take a look with the path `/static/invoices/[filename].pdf`

This doesn't any info to us to solve this challenge.



Let's take deep look over the files given. In the `package.json` file, we can find the version of the plugins within the website and notice that there is "md-to-pdf: 4.1.0" plugin.

After Google “md-to-pdf”, it is one of the vulnerable plugin reported which is CVE-2021-23639. You can check more about this CVE details over the link.

<https://nvd.nist.gov/vuln/detail/CVE-2021-23639>

<https://security.snyk.io/vuln/SNYK-JS-MDTOPDF-1657880>



```
1 {
2   "name": "blinker-fluids",
3   "version": "1.0.0",
4   "description": "",
5   "main": "index.js",
6   "scripts": {
7     "start": "node index.js"
8   },
9   "keywords": [],
10  "author": "rayhan0x01",
11  "license": "ISC",
12  "dependencies": {
13    "express": "4.17.3",
14    "md-to-pdf": "4.1.0",
15    "nunjucks": "3.2.3",
16    "sqlite-async": "1.1.3",
17    "uuid": "8.3.2"
18  },
19  "devDependencies": {
20    "nodemon": "^1.19.1"
21  }
22 }
```

Based on the CVE details, this vulnerable plugin version is before 5.0.0. Therefore, we can perform an exploit into it as the website version provided is 4.1.0.

## 🚩 CVE-2021-23639 Detail

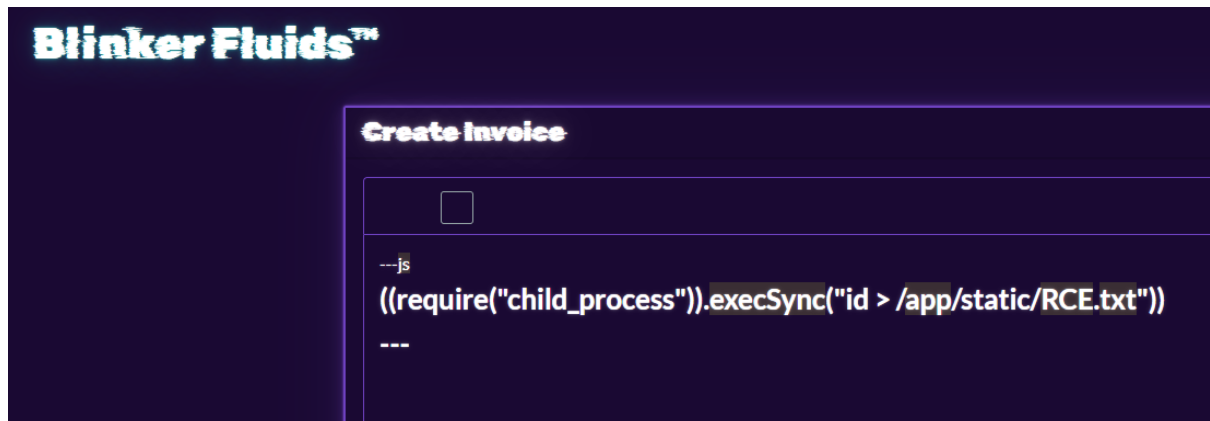
### Current Description

The package md-to-pdf before 5.0.0 are vulnerable to Remote Code Execution (RCE) due to utilizing the library gray-matter to parse front matter content, without disabling the JS engine.

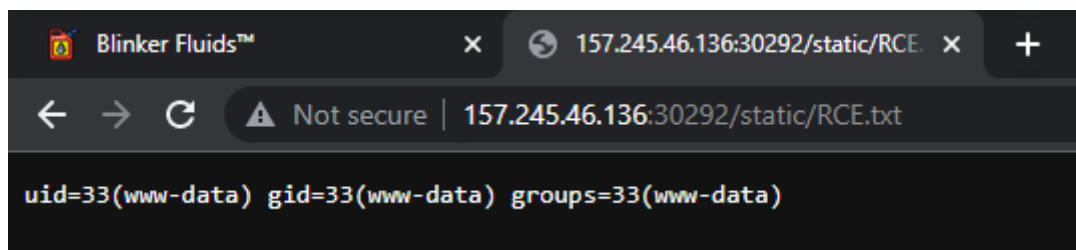
You can find for the md-to-pdf payload in this issues which people have posted <https://github.com/simonhaenisch/md-to-pdf/issues/99> that can be injected into the website.

This payload, we can retrieve the id which store at the server and you can store it at the specific path.

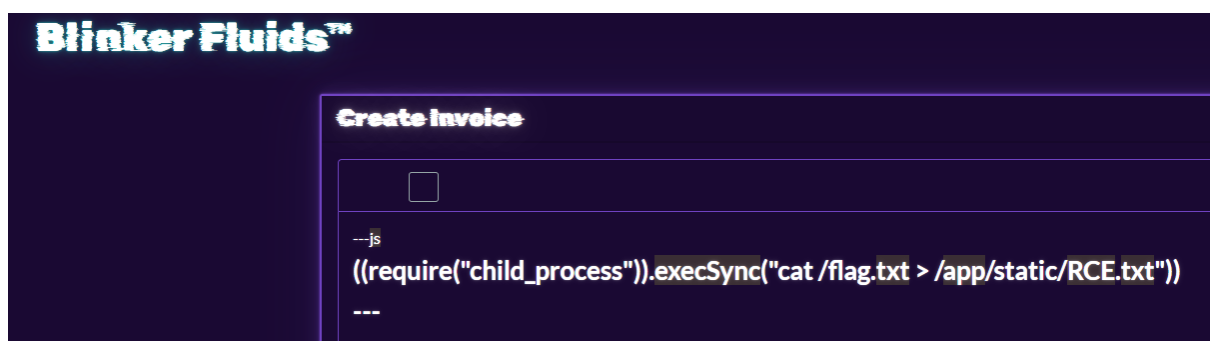
```
# payload
---js
((require("child_process")).execSync("id > /app/static/RCE.txt"))
---
```



Then, go to the path that we've uploaded the txt file and we get the response with the data.



Thus, lets modify the payload to retrieved the flag from the server.



## Flag

Then finally you will get the flag !

