



HACKTHEBOX



Flag Command

22nd April 2022 / Document No. D24.102.197

Prepared By: w3th4nds

Challenge Author(s): Xclow3n

Difficulty: **Very Easy**

Classification: Official

Description:

Embark on the "Dimensional Escape Quest" where you wake up in a mysterious forest maze that's not quite of this world. Navigate singing squirrels, mischievous nymphs, and grumpy wizards in a whimsical labyrinth that may lead to otherworldly surprises. Will you conquer the enchanted maze or find yourself lost in a different dimension of magical challenges? The journey unfolds in this mystical escape!

Objective

Find a secret command in json response and use it to get the flag

Application Overview

Visiting the home page we are provided with the following page:

```
You abruptly find yourself lucid in the middle of a bizarre, alien forest.  
How the hell did you end up here?  
Eerie, indistinguishable sounds ripple through the gnarled trees, setting the hairs on your neck on edge.  
Glancing around, you spot a gangly, grinning figure lurking in the shadows, muttering 'Xclow3n' like some sort of deranged  
mantra, clearly waiting for you to pass out or something. Creepy much?  
Heads up! This forest isn't your grandmother's backyard.  
It's packed with enough freaks and frights to make a horror movie blush. Time to find your way out.  
The stakes? Oh, nothing big. Just your friends, plunged into an abyss of darkness and despair.  
Punch in 'start' to kick things off in this twisted adventure!
```

```
>> |
```

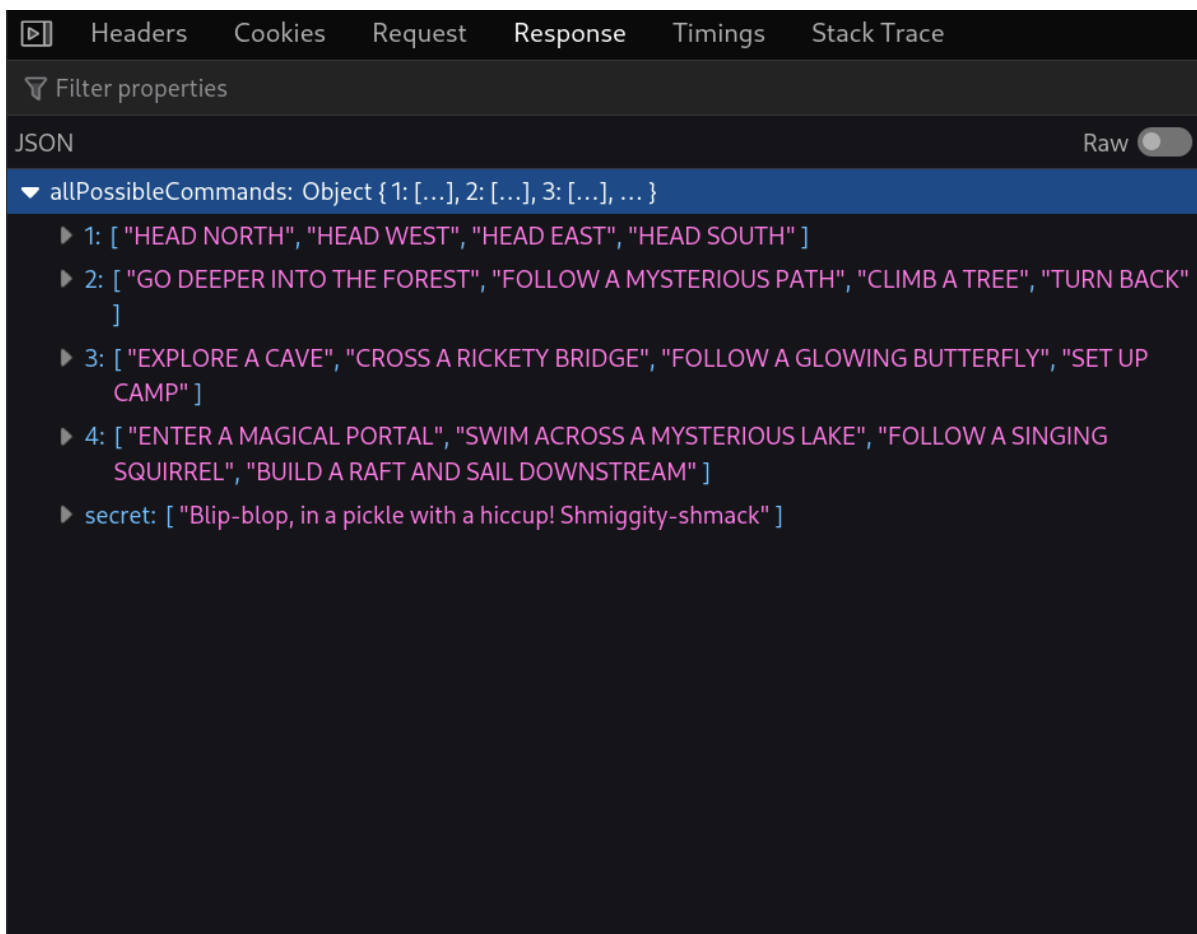
We can play the game but none of the option leads us to the flag

Solution

If we simply look at the developer's tool network tab and reload the page, we can see it makes a web request to the `options` endpoint

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms	80 ms	160 ms
200	GET	127.0.0.1:1337	/	document	html	1.65 kB	1.47 kB	1 ms		
204	GET	127.0.0.1:1337	commands.css	stylesheet	css	cached	1.59 kB	3 ms		
204	GET	127.0.0.1:1337	commands.js	script	js	cached	1.98 kB	3 ms		
204	GET	127.0.0.1:1337	terminal.css	stylesheet	css	cached	1.80 kB	2 ms		
204	GET	127.0.0.1:1337	main.js	script	js	cached	11.42 kB	4 ms		
204	GET	127.0.0.1:1337	game.js	script	js	cached	613 B	4 ms		
200	GET	127.0.0.1:1337	options	main.js:351 (fetch)	json	803 B	637 B	1 ms		
200	GET	127.0.0.1:1337	favicon.ico	FaviconLoader.sys.mjs:175 (i...	json	cached	33 B	0 ms		

Looking at the response of this endpoint. There is a secret command whose value is "Blip-blop, in a pickle with a hiccup! Shmiggity-shmack".



If we start the game and enter the secret value we get the flag.