C16: Elf Hunt (did not hack)

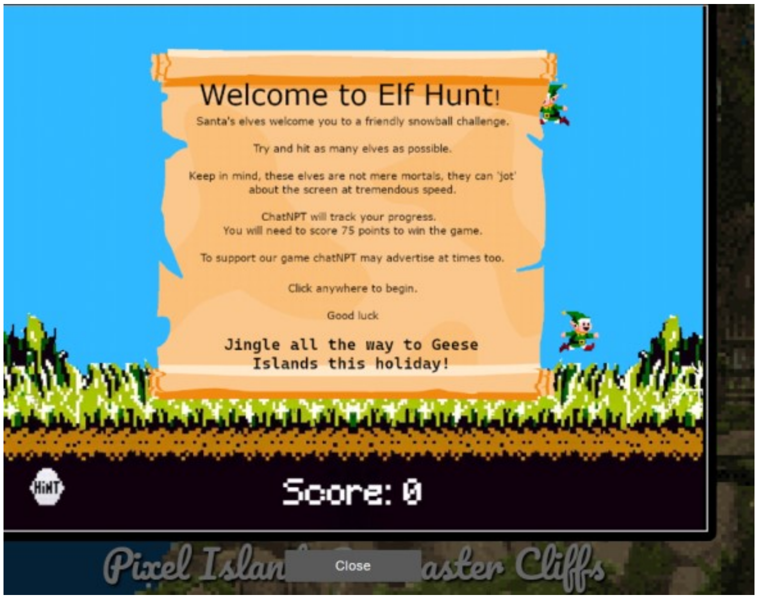
Saturday, December 23, 2023 4:54 PM

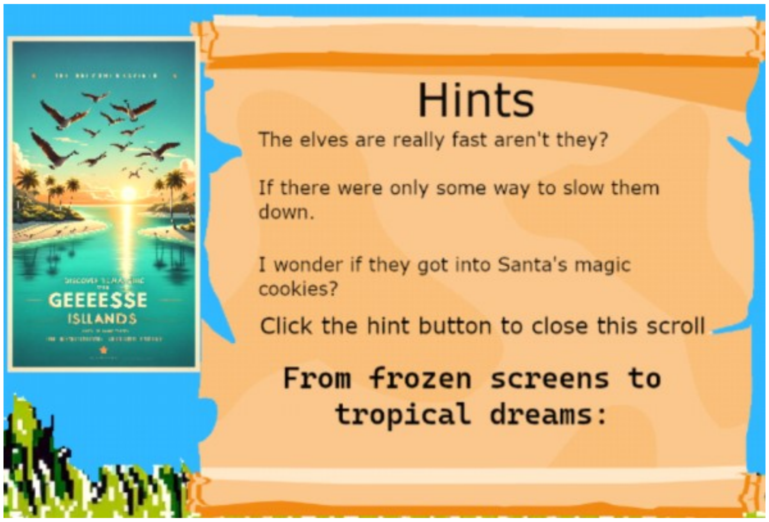
Difficulty: Level 3
Piney Sappington needs a lesson in JSON web tokens. Hack Elf Hunt and score 75 points.

CONVERSATION w/ Elf Piney Sappington	**Piney Sappington (Rainraster Cliffs)** Hey there, friend! Piney Sappington here. You look like someone who's good with puzzles and games. I could really use your help with this Elf Hunt game I'm stuck on. I think it has something to do with manipulating JWTs, but I'm a bit lost. If you help me out, I might share some juicy secrets I've discovered. Let's just say things around here haven't been exactly... normal. So, what do ya say? Are you in? Oh, brilliant! I just know we'll crack this game together. I can't wait to see what we uncover, and remember, mum's the word! Thanks a bunch! Keep your eyes open and your ears to the ground. From <https://2023.holidayhackchallenge.com/badge?section=conversation&id=pineysappington> ** ------- Response after completing challenge ------- ** Well done! You've brilliantly won Elf Hunt! I couldn't be more thrilled. Keep up the fine work, my friend! What have you found there? The Captain's Journal? Yeah, he comes around a lot. You can find his comms office over at Brass Buoy Port on Steampunk Island. From <https://2023.holidayhackchallenge.com/badge?section=conversation&id=pineysappington>
HINTS	**JWT Secrets Revealed** *From: Piney Sappington* *Terminal: Elf Hunt* Unlock the mysteries of JWTs with insights from PortSwigger's JWT Guide. From <https://2023.holidayhackchallenge.com/badge?section=hint&id=hintElfhunt>

MY WORK AND ANSWER

I played this game and won. It didn't take as long as others seemed to have indicated. I realized afterwards that I missed an opportunity to learn about JSON web tokens (JWTs). So I went back afterwards to look at the code to see where I could manipulate the code (my write-up for this part of the hack is in the table below). However, I did not attempt to test since I'd completed this challenge already.

After playing the game and winning, I returned to the game with the intent of looking for vulnerabilities and how they can be hacked to making winning easier. The welcome game screens hinted at being able to manipulate the scoring mechanism (i.e., ChatNPT will track your progress), cookies (regarding being able to slow down the elves). I also noted the comment about ChatNPT posting advertisements too - something to also explore.	 Welcome to Elf Hunt! Santa's elves welcome you to a friendly snowball challenge. Try and hit as many elves as possible. Keep in mind, these elves are not mere mortals, they can 'jot' about the screen at tremendous speed. ChatNPT will track your progress. You will need to score 75 points to win the game. To support our game chatNPT may advertise at times too. Click anywhere to begin. Good luck Jingle all the way to Geese Islands this holiday! Score: 0



Hints

The elves are really fast aren't they?

If there were only some way to slow them down.

I wonder if they got into Santa's magic cookies?

Click the hint button to close this scroll

From frozen screens to tropical dreams:

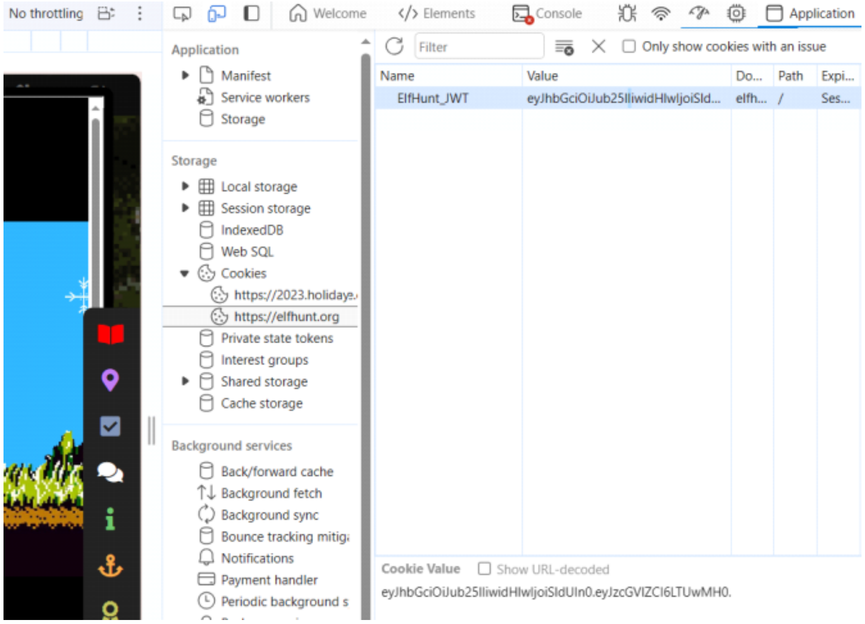
Inspecting the code and the application, I saw that the JWT, ElfHunt_JWT is parsed into three (3) parts where the 3rd part is missing

Using JWT IO to decode the cookie, it reveals the speed of the elves. The speed can be manipulated so that they would move slower and thereby make easier targets to hit.

- The default is 500; maybe change to 25 or 50.

Another option would be to trick the game into thinking I'd already defeated it but manipulating the score. I didn't explore where this change would be made but suspect there is a function that is tracking the score.

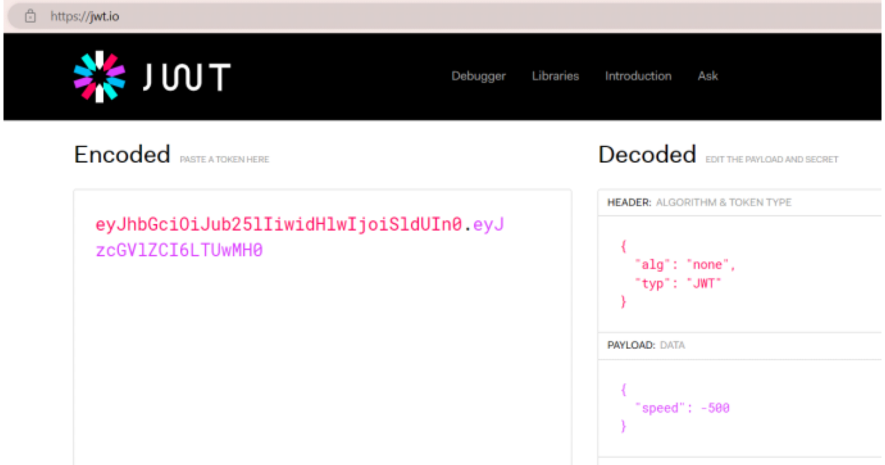
```
/js main code

function parseJwtPayload(token) {
  // Split the JWT into its three parts
  const parts = token.split('.');
  // The payload is the second part. We decode it from base64 and parse the JSON
  try {
    const decodedPayload = atob(parts[1]);
    const jsonObj = JSON.parse(decodedPayload);
    return jsonObj;
  } catch (e) {
    console.error('Failed to parse JWT payload', e);
    return null;
  }
}

function getCookie(name) {
  // This function will read the cookie by name
  const value = `; ${document.cookie}`;
  const parts = value.split(`; ${name}=`);
  if (parts.length === 2) return parts.pop().split(';').shift();
  return null;
}

function getDecodedJwtPayload(cookiename) {
  // This function retrieves the JWT from the cookie and decodes it
  const jwt = getCookie(cookiename);
  if (jwt) {
    return parseJwtPayload(jwt);
  } else {
    console.log('JWT not found');
    return null;
  }
}
```



Name	Value	Do...	Path	Expi...
ElfHunt_JWT	eyJhbGciOiJub25lIiwidHlwIjoiSld...	elfh...	/	Ses...

Cookie Value □ Show URL-decoded

eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJzcGVlZCI6LTUwMH0.



Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJzcGVlZCI6LTUwMH0
```

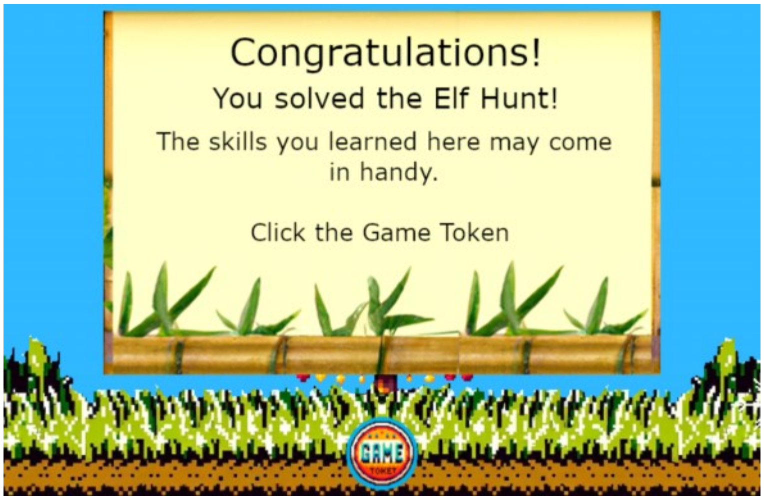
Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "none",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "speed": -500
}
```



Congratulations!

You solved the Elf Hunt!

The skills you learned here may come in handy.

Click the Game Token

Comments of Interest from other Players

design issues and flawed handling of JSON web tokens (JWTs) can leave websites vulnerable to a variety of high-severity attacks. As JWTs are most commonly used in authentication, session management, and access control mechanisms, these vulnerabilities can potentially compromise the entire website and its users.

Unlike with classic session tokens, all of the data that a server needs is stored client-side within the JWT itself.