C02: Snowball Fight (did not hack)

Friday, December 22, 2023 11:59 PM

Difficulty: Level 2
Visit Christmas Island and talk to Morcel Nougat about this great new game. Team up with another player and show Morcel how to win against Santa!

CONVERSATION w/ Elf, Morcel Nougat	**Morcel Nougat (Frosty's Beach)** Hey there, I'm Morcel Nougat, elf extraordinaire! You won't believe this, but we're on a magical tropical island called Christmas Island, and it even has snow! I'm so glad ChatNPT suggested we come here this year! Santa, some elves, and I are having a snowball fight, and we'd love you to join us. Santa's really good, so trust me when I say it's way more fun when played with other people. But hey, if you can figure out a way to play solo by tinkering with client side variables or parameters to go solo mode, go for it! There's also ways to make the elves' snowballs do no damage, and all kinds of other shenanigans, but you didn't hear that from me. Just remember, it's all about having fun and sharing the joy of the holiday season with each other. So, are you in? We'd really love your company in this epic snowball battle! gist/screenshot (https://gist.github.com/chrisjd20/93771da596ca5e49043f148a845c469f) ** ------- Response after completing challenge ------- ** You're like a snowball fighting ninja! A real-life legend. Can I have your autograph!? From <https://2023.holidayhackchallenge.com/badge?section=conversation&id=morcelnougat> **Santa (Frosty's Beach)** …. Now, why not start off your vacation with a snowball fight with Morcel, or check out my surf shack on the other end of the beach? However you decide to relax, be sure to soak in all the whimsical beauty of these magical islands, and enjoy the activities to the fullest! ** ------- Response after completing challenge ------- ** Congratulations! You are a true snowball fight champion and thank you so much for helping out Ginger Breddie! Oh, it feels like the warm and gentle winds are starting to pick up! The perfect time to head back to your boat and embark on an adventure to all the other whimsical places the Geese Islands have to offer! Safe travels my friend and thank you again for your help! From <https://2023.holidayhackchallenge.com/badge?section=conversation&id=santaapproach>
HINTS	**Snowball Super Hero** *From: Morcel Nougat* *Terminal: Snowball Hero* Its easiest to grab a friend play with and beat Santa but tinkering with client-side variables can grant you all kinds of snowball fight super powers. You could even take on Santa and the elves solo! From <https://2023.holidayhackchallenge.com/badge?section=hint> **Consoling iFrames** *From: Morcel Nougat* *Terminal: Snowball Hero* Have an iframe in your document? Be sure to select the right context before meddling with JavaScript. From <https://2023.holidayhackchallenge.com/badge?section=hint&id=hintSnowballHero2>

MY WORK AND ANSWER
I participated in snowball fight multiple times with no success. The elves and Santa were vicious! I was also unsuccessful in making modifications to the developer code work. I did eventually defeated the elves and Santa in game play with another player.

Reviewed the code in the game to determine which variables can be modified to aid in my defeating Santa and his elves.

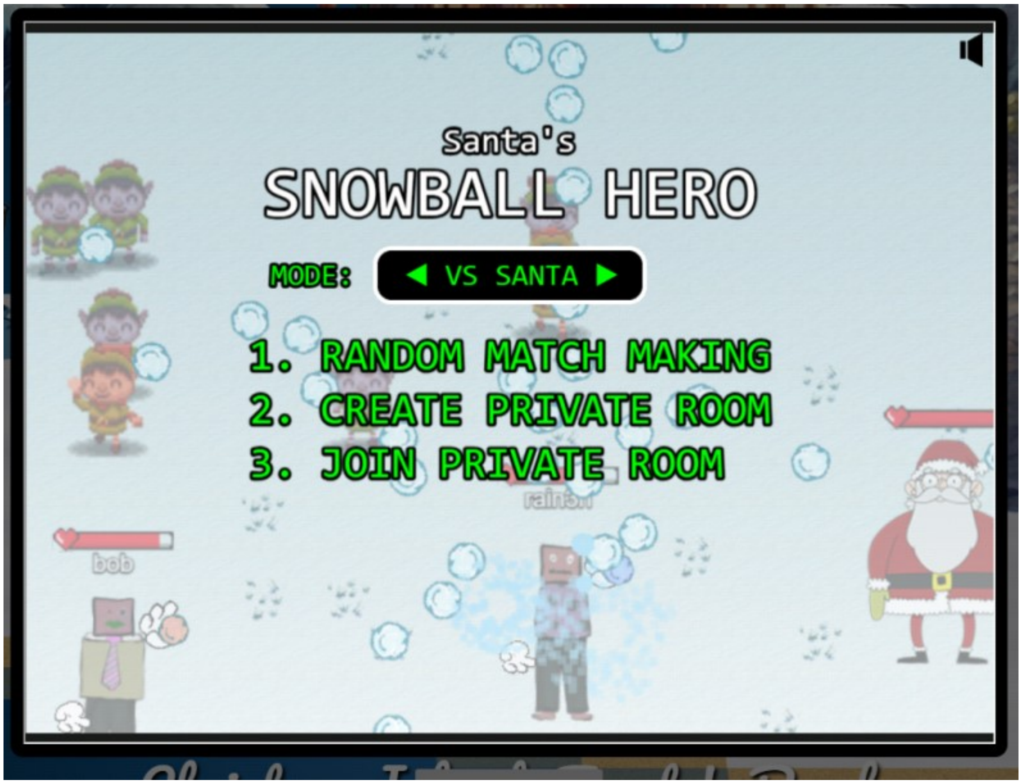
Before game play, I tried making changes on multiple occassions.

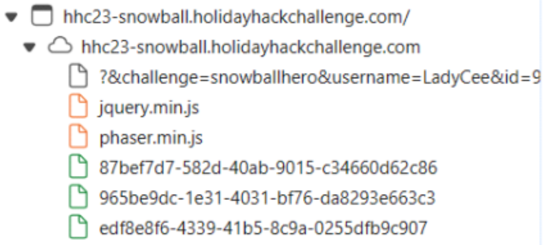
Edited variables associated with player to include player.throwDelay, player.health, and player.lastHealth.

Also, made edits to other variables such as snowballSpeed, elfThrowDelay, santaThrowDelay.

However, none of this worked so I bounced between jumping into games with at least one other player and hacking the code.

I enjoyed the snowball fight so eventually another player and I were able to defeat the elves and Santa.





```
▾ hhc23-snowball.holidayhackchallenge.com/
  ▾ hhc23-snowball.holidayhackchallenge.com
      ?&challenge=snowballhero&username=LadyCee&id=9
      jquery.min.js
      phaser.min.js
      87bef7d7-582d-40ab-9015-c34660d62c86
      965be9dc-1e31-4031-bf76-da8293e663c3
      edf8e8f6-4339-41b5-8c9a-0255dfb9c907
```

```
// ========== player stuff
player = createPlayerObject(playerDNA, starting_pos.x, starting_pos.y)
player.username = username
player.throwDelay = 300
player.moveVelocity = playersVelocity
player.throwTime = 0
player.isregistered = false
player.lastX = player.x
player.lastY = player.y
player.playerId = playerId
player.assigned_id = false
player.health = 50
player.lastHealth = player.health + 0
player.update = true
if (gameType === "free-for-all") {
player.ready = 1
} else {
player.ready = 0
}
player.isdefeated = 0
player.healthbar = this.add.image(player.x + player_healthbar_offset.x, player.y + player_healthbar_offset.y, 'healthbar')
player.healthbar.setFrame(0);
player.healthbar.setScale(1.5)
player.usernameText = gameSceneObject.add.text(player.x, player.healthbar.y + 6, username, textStyle);
player.usernameText.setOrigin(0.5, 0);
player.takehit = (dmg, owner_playerobj) => {
if (!player.isdefeated) {
player.health = Math.min( Math.max(Math.abs( player.health - dmg ), 0), 50)
if (player.health !== player.lastHealth) {
player.update = true
player.lastHealth = player.health + 0
player.healthbar.setFrame( Math.min(50 - player.health, 49) );
player.healthbar.setFrame( Math.min( Math.max(Math.abs( 50 - player.health ), 0), 49) )
if (player.health == 0) {
player.isdefeated = 1
if (gameType === 'free-for-all') {
setTimeout(function() {
ws.close()
window.location.reload();
}, playerRespawnTime)
} else {
stopTheGame = true
ws.close()
}
}
if (player.isdefeated) {
playerDeath(player)
setTimeout(function() {
if (ws.readyState === WebSocket.OPEN) {
ws.send(JSON.stringify({ a: 'd-' + assigned_id + '-' + owner_playerobj.assigned_id, i: playerId}));
}
}, sendRate+50)
}
}
}
}
player.entity_type = 'player'
player.walkingTween = this.tweens.add({
targets: player,
rotation: 0.1, // This is in radians. Adjust this value to get the desired effect.
ease: 'Sine.inOut',
yoyo: true, // Yoyo effect makes the animation play back and forth.
repeat: -1, // Repeat forever.
duration: 150,
paused: true // Start paused so it only plays when we move.
});
player.setOrigin(0.5,0.5)
player.flipX = true
cursors = {
upW: this.input.keyboard.addKey(Phaser.Input.Keyboard.KeyCodes.W),
upArrow: this.input.keyboard.addKey(Phaser.Input.Keyboard.KeyCodes.UP),
downS: this.input.keyboard.addKey(Phaser.Input.Keyboard.KeyCodes.S),
downArrow: this.input.keyboard.addKey(Phaser.Input.Keyboard.KeyCodes.DOWN),
leftA: this.input.keyboard.addKey(Phaser.Input.Keyboard.KeyCodes.A),
leftArrow: this.input.keyboard.addKey(Phaser.Input.Keyboard.KeyCodes.LEFT),
rightD: this.input.keyboard.addKey(Phaser.Input.Keyboard.KeyCodes.D),
rightArrow: this.input.keyboard.addKey(Phaser.Input.Keyboard.KeyCodes.RIGHT),
};
this.anims.create({
key: 'throw',
frames: this.anims.generateFrameNumbers('hand_sh', { start: 0, end: 13 }),
frameRate: 50,
repeat: 0,
hideOnComplete: false
});
setupPlayerHands.bind(this)(player, isme=true);
this.input.on('pointerdown', function (pointer) {
let nowt = Date.now()
if (Date.now() - player.throwTime > player.throwDelay && player.ready) {
player.throwTime = nowt
playerThrow(pointer)
}
}, this);
// ========== end of player stuff
```

From <https://hhc23-snowball.holidayhackchallenge.com/room/?username=LadyCee&roomId=23448b08f&roomType=public&gameType=co-op&id=d3170016-7e78-4ebe-b05a-1201b594fcd8&dna=ATATATTAATATATATATATTAATATATATATGCATTATAATATATATATATTAATATATATATATATGCATATATATCGATATATATATATATTAATATATATATATGCATATATATTA&singlePlayer=false>

Comments of Interest from other Players

It's a developer console challenge. You can win the snowball challenge in 2-player mode without hacking anything. You should unlock an achievement after completing the snowball challenge. If you see the Elf the Dwarf Victory message it should grant the achievement/completion as long as you played the game in the iframe inside the world.

CAUTION: The iframe is required; you have to run within the iframe so make sure you are in the right frame

Inspect the code in the game, look at the **console** and play with commands within the console. Think of words or phrases you might expect to be in game. Think about who you competing against and what you and all the other players might be called in the game.

- Use the Inspector / inspect in your browser to select the iframe, then it should be visible, i.e.
  Open <iframe title="challenge" src="https://hhc23-snowball.holidayhackchallenge.com?
  &amp;challenge=snowballhero&amp;username=ravhackxmas&amp;id=5989cd55-0a3a-4ec3-b601-d909f21fb0ec&amp;area=ci-frostysbeach&amp;location=29,16
  &amp;tokens=&amp;dna=ATATATTAATATATATATATATTAATATATATTACGGCCGATATATATATATATATATATATATATATTAATATGCCGATATATATATATTAATATATATATATATTACGATATATGC"></iframe>
- To complete in iframe solo window.location.href is your friend; window.location.href.replace (/foo/g,'bar')

Make chsnes and do it before clicking ready

- need to change the drop-down in console to the correct js file to affect
- Fiddle with the JS console for extra "help". Or find a way to get elf the dwarf to help you. He's a beast
- singlePlayer=false parameter in the url
  Debug christmasmagic.js
  - Right click on the .js file and click override content. The potential gotcha that got me earlier was another popup may appear asking where you want to store your overrides and you need to give chrome permission to write to the filesystem.
  - so I was able to get the URL to work separately but still not able to figure out the iframe part. blah!
  - it helps if you click the drop down windows on the console when attempting to change the variables

Look at the source code for the game - how the game is called, what values get passed to it and see where/how they are used in the code. Check the parameters passed to initiate the game; there's some parameters that you might be able to change. Once you've found out where to change it, change the value and hit enter to refresh the URL

- Review the URL and JS files ; you can plug a modified URL into that.
- Take a look at the hint provided as to interacting with iframes and ensuring you are in the right context.
- Parameters to change via browser console made the game much easier - can fly around quickly, snowballs don't damage me, and I can thrown them as fast as Will Ferrell in Elf. (This person gave himself a machine gun: I have a machine gun... ho ho ho)
  - Set the hitbox variable to 0,
  - Set damage to 0 --> look at Inspector
  - Player object that had a health (which loads from 14.1143.0) and
  - throwDelay parameters changing those

What I found strange is if I copy and paste the source code into text editor, it shows more than what the chrome browser displays
When opening up in developer tools, the script stops at var paramsdefault. However when you copy and paste the code in text editor it shows many more lines of hidden code underneith. it is as if it only prints 100 lines of a script and then nothing

Take it out of the console. I copy-pasted the URL I got from one of the request's headers (from the Network tab in dev tools) and ran that in the browser. The parameter to edit is there in the URL
Breakpoints did the trick

If people copy your link that you posted: (https://hhc23-snowball.holidayhackchallenge.com/room/?username=kindng&roomId=217b190dd&roomType=public&gameType=free-for-all&id=42e5421c-cbc6-47b9-8e22-37763ec892c6&dna=avatar9&singlePlayer=false) people can login and play as you!

- Kindngg fixed so this no longer works

I have spawned my clone and defeated elves with instant-kill and auto degraded health of Santa without hitting him with SnowBalls 😁 . I hope you will like my solution too ☺ https://www.youtube.com/watch?v=2pTYupvcXeE

accidentally inverted time and space by entering santa.NotReal=true;

If y'all can't edit, go read up on how google dev mode works with local caching because it took me a bit of searching before I realized how to make that part work. You can win and have it register your success once you get that part and then figure out how to use it.

Should the page show up in the "Sources" tab? Because the sources for "room" is completely empty for me.
Not working when you split to New window, try repeat without split

Ended up changing the score value to complete this one, but I wanted to know if someone would be willing to explain to me how the JWT exploit using burp is executed? I'm curious as to how it is completed
Got it!! did both kind of together, slowed down the elves and changed the code to win with just 1 instead of 75, with Burp

I assume there are 10 different solutions here ☺ If a change does not lead to the desired success, it may have happened too "late". Often it is also the difference between request and response that makes the difference.
 - Thanks, editing the javascript in the response body did it

basically ... you use the Intercept Options to modify the Responses, so you change your set-cookie to the value you want, or even the Response Body like a piece of JavaScript, but you need to setup your browser to not use proxy for the holidayhackchallange domain.