

ctfIsMagic Write Up



OSINT

Rookie Mistake

CHALL

While preparing the CTF platform for Hackerclass, I accidentally pointed the CTF Compfest subdomain to the dev server before it was ready :(Hopefully no one noticed.... right?

Author: sl0ck

Technical Report

1. go to this website : <https://archive.org/web/>
2. Search for <https://ctf.compfest.id/>
3. You can find website snapshot on AUGUST 8, 2022 15:02:26, and click it
4. And you can find the flag in html comment section <!-- COMPFEST14{oh_noo_the_platform_got_leaked_in_dev?!?_669ff817a1} -->

Flag

COMPFEST14{oh_noo_the_platform_got_leaked_in_dev?!?_669ff817a1}

I forgot something important

CHALL

A few days back, I was going through my old stuff, and there's this one letter i found who's written by one of my classmates back in high school. Damn, I just realized then that it was a love letter. I wanted to contact her, but she changed her phone number when she moved abroad to Austria. Now, I only got her Facebook. If only I knew her email address :(

Can you help me get her phone number? Here's her Facebook link <https://www.facebook.com/profile.php?id=100082501329298>

Flag: COMPFEST14{+[2 Digit Country Code][10 Digit Number]}

Example: COMPFEST14{+621234567890}

No bruteforce is needed for this challenge.

Author: myticalCat

Technical Report

we go to the link of

https://www.facebook.com/vallaisonnayskala/?show_switched_toast=0&show_invite_to_follow=0&show_switched_tooltip=0&show_podcast_settings=0&show

we get the name of vallaisonnayskala then we search into the youtube.

we get this youtube <https://www.youtube.com/watch?v=N43xIF9WxD4>.

then because she live in austria, the country code must be +43 instead of russian country code.

From the youtube there's some contact number which we refers to vallaisonnayskala's number so we just put the number here

676510260

The rest number we just guessing by putting the number from 1 - 9 huehuehue.

Flag

COMPFEST14{+4367651026018}

MISC

SEAMULATOR

CHALL

My brother has a new hobby, making a game. Yesterday, he made a cool game named Seamulator. I tried to play it, and after I did 7 actions, my fish price was \$20,000. But I forgot which actions did I take.

nc 103.185.38.43 13000 nc 103.185.38.43 13001

Author: kilometer

Technical Report

1. after i check the program, i find : swim = x10, eat = +12, jump = x2
2. first point is 1 and target is 20000
3. so i use this combination [3,3,2,2,4,4,4] and i get 20000 point
4. after validate my answer with problem set i get the flag
COMPFEST14{s3amUlat0r_v3ry_e4sy_63e2c19257}

Flag

COMPFEST14{s3amUlat0r_v3ry_e4sy_63e2c19257}

WaifuDroid3

Chall

After so many successful attempts at enticing my waifu chatbot, I had to lock her up in my jail. I taught her various languages and now she only takes orders in a language that few people know how to speak well. This should be the final solution.

She's online as Nadenka#2595 on the Discord server, but only talking in DMs. This time it should be safe.

(Note: this challenge requires no automation. Please do not automate your Discord account as that is a violation of Discord's Terms of Service and may lead to the termination of your account)

Author: sl0ck

Technical Report

We download the app.js and as you can see we can analyze the function just like below

```

const Discord = require(`discord.js`);
const client = new Discord.Client();

const { secret } = require(`./secrets.js`);

const responses = {
  reticent: [ `Grrr`, `NO FLAG`, `No flag!`, `Нет флага`, `\u{1F47A}`, `no f
l a g`, `Ora ana bendera`, `Teu aya bendera` ],
  secret: secret
};

const isValid = (str) => {
  let allowedChars = [ `+`, `-`, `/`, `~`, `[`, `]`, `{`, `}`, `!` ];
  for(let chr of str) {
    if(!allowedChars.includes(chr)) return false;
  }
  return true;
};

const fetchResponse = (responseType) => {
  return responses[responseType][Math.floor(Math.random() *
responses[responseType].length)];
};

client.on(`message`, (msg) => {
  let user = msg.author;
  if(msg.channel.type !== `dm` || user === client.user) return;
  let content = msg.content;

  let response = fetchResponse(`reticent`);

  if(content.length > 766 || !isValid(content)) {
    return user.send(response);
  }

  try {
    content = eval(content);
  } catch(err) {
    content = ``;
  }

  if(content === `yes Flag`) {
    response = fetchResponse(`secret`);
  }

  user.send(response);
});

client.login(process.env.BOT_TOKEN);

```

it is requiring the token environment and discord.js module so to test the function i need to rewrite the function

```

const secret = "123"

const responses = {
  reticent: [`Grrr`, `NO FLAG`, `No flag!`, `Нет флага`, `\u{1F47A}`, `no flag`, `Ora ana bendera`, `Teu aya bendera`],
  secret: secret
};

const fetchResponse = (responseType) => {
  return responses[responseType][Math.floor(Math.random() * responses[responseType].length)];
};

const isValid = (str) => {
  if(/[^\+~\-\~\[\]\{\}\!]+\$/i.test(str)) {
    console.log("String is valid")
    return true;
  }
  return false;
};

const main = (msg) => {
  let content = msg;

  let response = fetchResponse(`reticent`);

  if(content.length > 766 || !isValid(content)) {
    console.log(`the length of content [${content.length}] msg not valid`);
    return response;
    // console.log(response);
  }

  try {
    content = eval(content);
  } catch(err) {
    content = ``;
  }

  if(content === `yes Flag`) {
    response = fetchResponse(`secret`);
  }

  console.log(response);
}

main("+");

```

It says that the true isValid is true. But I'm stuck for about I dunno maybe 4 hours
Then i just think that is i pass a function into the msg argument it'll get the flag.
So i just create the function that modify the content into yes Flag because there's an
if statement that says if statement that says yes Flag then we can call the method
of fetchResponse(secret) which what we want to get

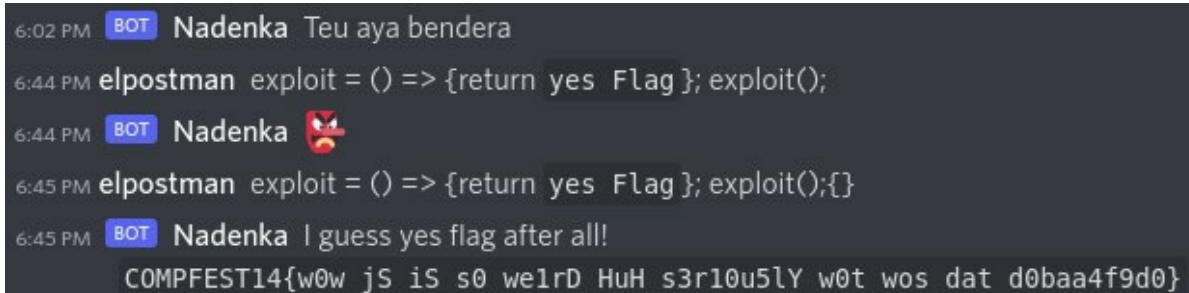
first i try to pass the function just like this.

```
exploit = () = {return `yes Flag`; exploit();}
```

but it won't work... So i just try to write using the curly braces at the end

```
exploit = () = {return `yes Flag`; exploit();{}}
```

just like below.



A screenshot of a chat window with a dark background. It shows a series of messages between a user named 'elpostman' and a bot named 'Nadenka'. The messages are as follows:
6:02 PM BOT Nadenka Teu aya bendera
6:44 PM elpostman exploit = () => {return yes Flag }; exploit();
6:44 PM BOT Nadenka 🤡
6:45 PM elpostman exploit = () => {return yes Flag }; exploit();{ }
6:45 PM BOT Nadenka I guess yes flag after all!
COMPFEST14{w0w_js_iS_s0_we1rD_HuH_s3r10u5lY_w0t_wos_dat_d0baa4f9d0}

Flag

COMPFEST14{w0w_js_iS_s0_we1rD_HuH_s3r10u5lY_w0t_wos_dat_d0baa4f9d0}