

EG CTF 2023

Category: WEB

Challenge name: EVE

Points: 100

Challenge description:

Seriously, it's so easy. Even my grandma can do it!

Note: Submit flag with EG{}

Given Link: <https://eliteghost.tech/wall-e/>

Given Hints:

- 1. Who is EVE? Hackers always do their research!**
- 2. Function robots for web? I don't know, make some research dude!**

SOLUTION

Let's start by viewing the link provided.

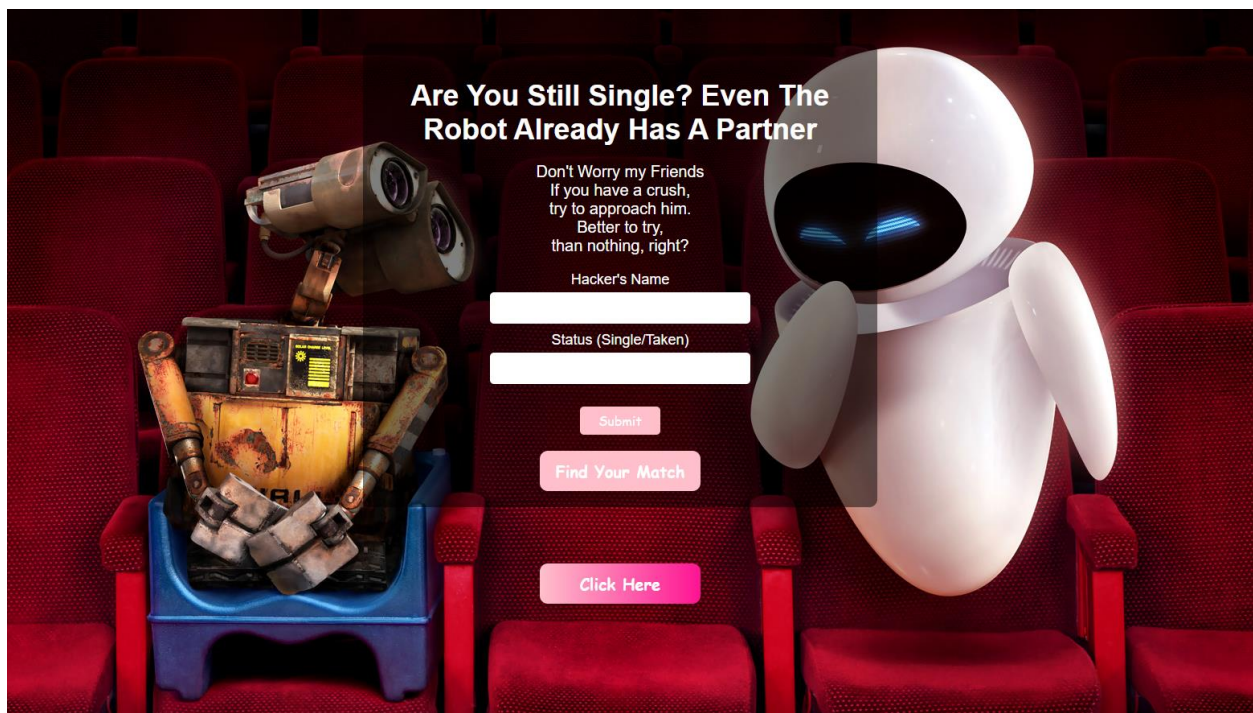


Figure 1 home view

Now let's inspect the webpage.

```
<title>Find Love Today</title>
<style>_</style>
<script data-avast-pam="y" type="text/javascript" name="AVAST_PAM_submitInjector">_</script>
<script data-avast-pam="y" type="text/javascript" name="AVAST_PAM_submitInjector">_</script>
</head>
<body id="main">
  <div class="card">
    <h1>Are You Still Single? Even The Robot Already Has A Partner</h1>
    <div class="price">_</div>
    <form class="AVAST_PAM_nonloginform">_</form> (flex)
    <a href="https://youtu.be/5ngWIDkPP3o">
      <button class="fancy-button fancy-button-1">Find Your Match</button>
    </a>
  </div>
  <style>_</style> == $0
  <p style="text-align: center;">
    <a href="https://linkedin.com/in/naqib-fitri">
      <button class="fancy-button fancy-button-2">Click Here</button>
    </a>
  </p>
</body>
</html>
```

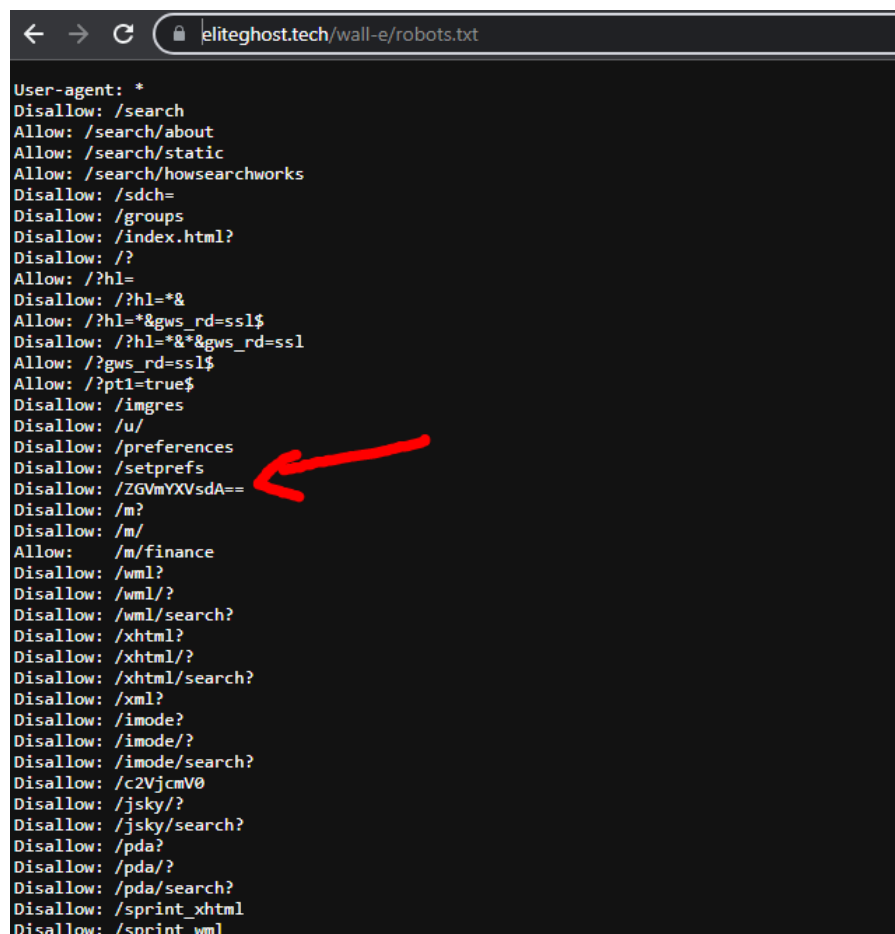
Figure 2 page source

The source code tells us a few things about the webpage, to summarize it

- Find your match button leads us to a YouTube video
- Click here button leads us to LinkedIn profile
- Submit button that doesn't lead anywhere in particular.

Basically, we found nothing in this source code. So, we going to move on to the next investigation. We now going to put Robots.txt in the URL. Which looks like this

<https://eliteghost.tech/wall-e/robots.txt>



```
← → ↻ eliteghost.tech/wall-e/robots.txt

User-agent: *
Disallow: /search
Allow: /search/about
Allow: /search/static
Allow: /search/howsearchworks
Disallow: /sdch=
Disallow: /groups
Disallow: /index.html?
Disallow: /?
Allow: /?hl=
Disallow: /?hl=*%
Allow: /?hl=*%gws_rd=ssl$
Disallow: /?hl=*%gws_rd=ssl$
Allow: /?gws_rd=ssl$
Allow: /?pt1=true$
Disallow: /imgres
Disallow: /u/
Disallow: /preferences
Disallow: /setprefs
Disallow: /ZGVmYXVsdA==
Disallow: /m?
Disallow: /m/
Allow: /m/finance
Disallow: /wml?
Disallow: /wml/?
Disallow: /wml/search?
Disallow: /xhtml?
Disallow: /xhtml/?
Disallow: /xhtml/search?
Disallow: /xml?
Disallow: /imode?
Disallow: /imode/?
Disallow: /imode/search?
Disallow: /c2VjcmV0
Disallow: /jsky/?
Disallow: /jsky/search?
Disallow: /pda?
Disallow: /pda/?
Disallow: /pda/search?
Disallow: /sprint_xhtml
Disallow: /sprint wml
```

Figure 3 robots.txt

Right off the bat we can see an encoded text. Decode it and we have

ZGVmYXVsdA== - Base64

“default”

Now we can try and use this decoded text in our URL which now looks like this

<https://eliteghost.tech/wall-e/default/>



Nothing here bro, go home

What did you expect?

Figure 4 scammed

Whoops, looks like we got the wrong page, let's retry again

```

Disallow: /cl2/ical/
Disallow: /coop/directory
Disallow: /coop/manage
Disallow: /trends?
Disallow: /trends/music?
Disallow: /trends/hottrends?
Disallow: /trends/viz?
Disallow: /trends/embed.js?
Disallow: /trends/fetchComponent?
Disallow: /trends/beta
Disallow: /trends/topics
Disallow: /musica
Disallow: /musicad
Disallow: /musicas
Disallow: /czNjcjN0MTMzNw==
Disallow: /musics
Disallow: /musicsearch
Disallow: /musicsp
Disallow: /musiclp
Disallow: /urchin_test/
Disallow: /movies?
Disallow: /wapsearch?
Allow: /safebrowsing/diagnostic
Allow: /safebrowsing/report_badware/
Allow: /safebrowsing/report_error/
Allow: /safebrowsing/report_phish/
Disallow: /reviews/search?
Disallow: /orkut/albums
Disallow: /cbk
Disallow: /recharge/dashboard/car
Disallow: /recharge/dashboard/static/
Disallow: /profiles/me
Allow: /profiles
Disallow: /s2/profiles/me

```

Figure 5 another one

Oh, we found another one, decode it and we have

czNjcjN0MTMzNw== - Base64

“s3cr3t1337”

Put this in the URL and we have another page which says nothing here, but I’m not buying it



What're you looking for? Nothing here!

Figure 6 white page

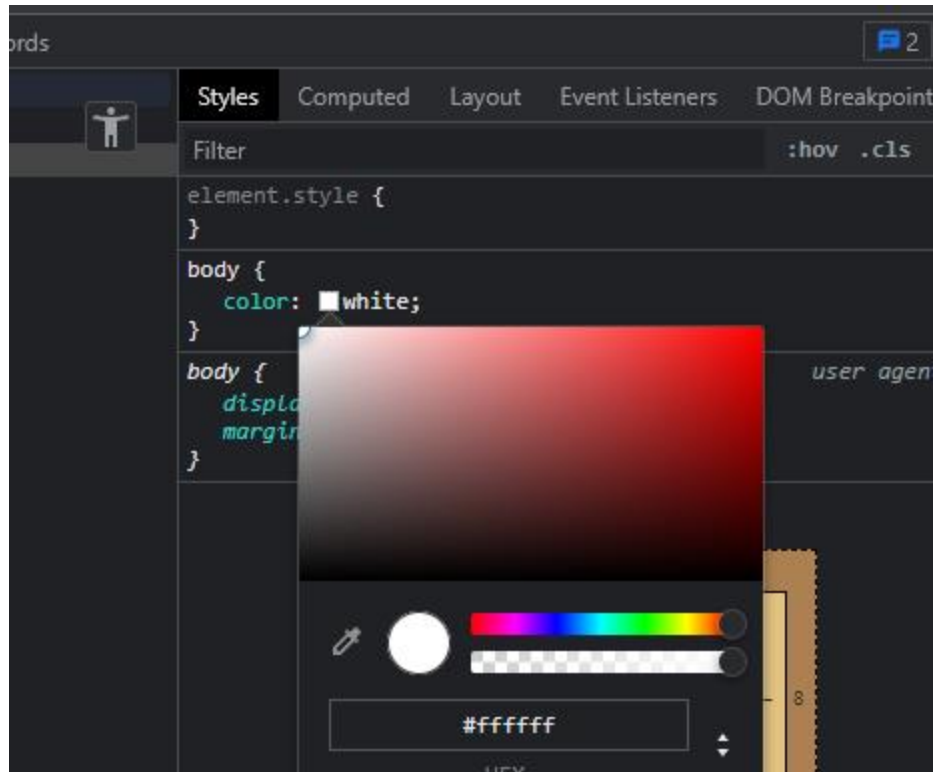


Figure 7 change style

Inspect the page, on styles change the color to black.

What're you looking for? Nothing here!

RUd7UjBCMhRTX1cxhEhfQjY0X1dhNV9Tb19GWE5fUjFHsFR9

Figure 8 flag revealed

Voila! We have some encoded text, decode it and we get the flag

EG{R0B0tS_W1tH_B64_Wa5_So_FXN_R1GHT}

Challenge name: Birthday

Points: 408

Challenge description:

I mean, EliteGhost was here since 10's. But what about eliteghost.tech?

Note: Submit flag with EG{}

Given Files: [present.zip](#)

Given Hints: none

SOLUTION

Let's start by visiting the eliteghost.tech

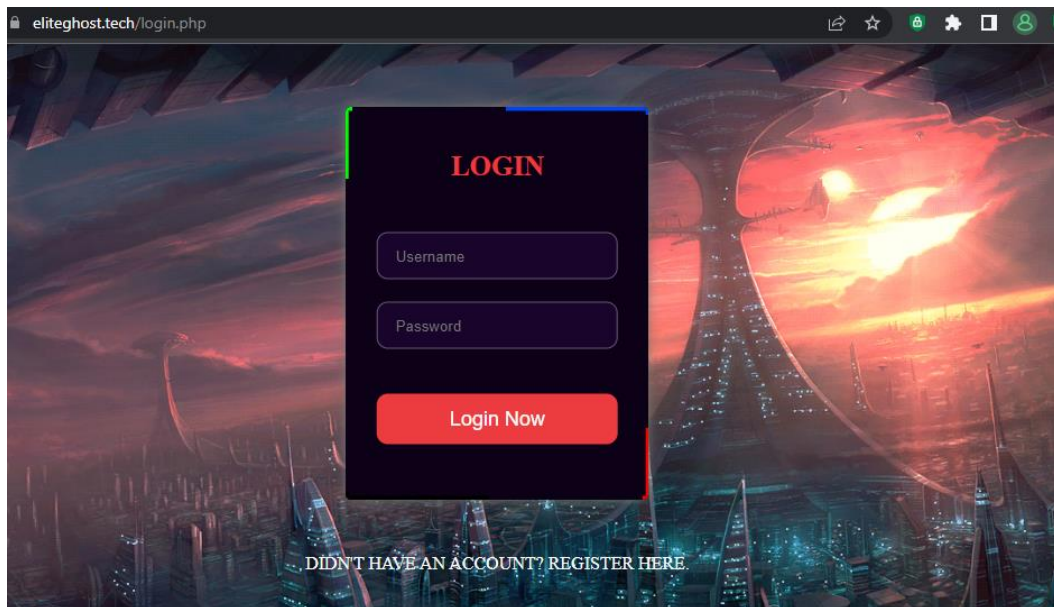


Figure 9 eliteghost site

From the description alone I think we could have a solid idea of the birthday of eliteghost.tech is going to be the password for our present.zip file. To do that we would want to use **whois**.

eliteghost.tech		Updated 5 days ago
Domain Information		
Domain:	eliteghost.tech	
Registrar:	Go Daddy, LLC	
Registered On:	2022-10-12	
Expires On:	2023-10-12	
Updated On:	2022-11-30	
Status:	ok	
Name Servers:	ns3.mudahhosting.com ns4.mudahhosting.com	
Registrant Contact		

Figure 10 whois info

Eliteghost.tech was created on 2022-10-12, now we have that info, we're going to use the pass to open our zip file



Figure 11 inside the zip file

After unzip we have a picture. If we zoomed in a little bit, we can see the flag is on top-center of the picture.



Figure 12 zoomed in

We have obtained the flag

EG{H4PPY_N3W_Y34R_CTF_2023}