

LambdaMamba / CTFwriteups

Code Issues Pull requests Actions Projects Security Insights

**Files**

- main
- Go to file
- 1337UP\_2022
- UTCTF\_2022
- beginner
- cryptography
- forensics
- misc
- discord\_rules
- mid\_ctf\_survey
- osint\_full
- img
- README.md
- public\_panic
- public\_panic\_p2
- README.md
- VishwaCTF\_2022
- picoCTF\_2022
- .gitignore
- README.md

**CTFwriteups / UTCTF\_2022 / misc / osint\_full /**

Add file ...

**LambdaMamba** Fixed some format problems e349910 · 2 years ago History

Name	Last commit message	Last commit date
..		
img	Added writeup for UTCTF 2022 Osint Full	2 years ago
README.md	Fixed some format problems	2 years ago

**README.md**

## UTCTF 2022 Osint Full (Category: Misc)

The challenge is the following,

**Challenge** 96 Solves X

### Osint Full

797  
797

Find out the following information about EddKing6 The name of his dog? His favourite video game? His alma mater? His Role at his company? His favorite food? His Email?

The email will have the strings "blob" and "corp" in it any other email is out of scope. Deviant Art and Soundcloud are out of scope Then send him a carefully crafted phishing email including all the details.

Pls check spam if you don't see the reply email within 5 minutes. By Emma(@Emma on discord)

Flag Submit

We are given the username of the person we are targeting, which is `EddKing6`. It also mentions that the email should contain the strings `blob` and `corp`, so this is something we should be looking for when searching Ed King. Also, we will need to look for the following info:

- Name of his dog
- His favorite video game
- His alma master
- His role at his company
- Favorite food
- His email

It doesn't explicitly state which social media websites we are supposed to search except for DeviantArt and Soundcloud, so I started off with Twitter to get more clues about this person.

In fact, searching `EddKing6` on Twitter returned [this account](#).

We can see that the account was created on `February 2022` and that he runs `blob corp`, so we can be certain that this is the Edd King we are looking for.

**edd king**  
@eddking6  
I like hacking things and running blob corp  
Joined February 2022  
6 Following 3 Followers  
Not followed by anyone you're following

We can see that Edd King has posted the following tweets.

**eddking6 @eddking6 · Mar 2**  
Here's an example of a vulnerable web app I like to use for testing

**eddking6/vulnerable-web-app**

github.com  
GitHub - eddking6/vulnerable-web-app  
Contribute to eddking6/vulnerable-web-app development by creating an account on GitHub.

**eddking6 @eddking6 · Feb 28**  
I like to play FactorIO when I'm not busy being a #CISO

**eddking6 @eddking6 · Feb 28**  
#hacktheplanet

**eddking6 @eddking6 · Feb 28**  
Just made my twitter

From the tweet `I like to play FactorIO when I'm not busy being a #CISO`, we can see that he is a `CISO` and he plays `FactorIO`. However, I wasn't too sure what `FactorIO` was, so I did a Google Search and revealed that it was in fact a video game.

factorio

All Images Videos News Shopping More Tools

About 4,870,000 results (0.64 seconds)

<https://www.factorio.com> Factorio

Factorio is a game in which you build and maintain factories. You will be mining resources, researching technologies, building infrastructure, ...

[Blog](#) · [Download demo](#) · [Buy](#) · [Log in](#)

From the tweets alone, we have found the following so far:

- Name of his dog: ?
- His favorite video game: `FactorIO`
- His alma mater: ?
- His role at his company: `CISO`
- Favorite food: ?
- His email: ?

One of his tweets includes a link to [his Github's vulnerable web app respository](#).

**eddking6 / vulnerable-web-app** Public

Code Issues Pull requests Actions Projects Wiki Security Insights

master 1 branch 0 tags Go to file Add file Code

Edd King vulnerable web app 2a70ed6 13 days ago 1 commit

imgs	vulnerable web app	13 days ago
templates	vulnerable web app	13 days ago
Dockerfile	vulnerable web app	13 days ago
README.md	vulnerable web app	13 days ago
challenge.yml	vulnerable web app	13 days ago

**About**  
No description, website, or topics provided.

Readme 0 stars 1 watching 0 forks

**Releases**

[docker-compose.yml](#) vulnerable web app 13 days ago

[flag.txt](#) vulnerable web app 13 days ago

[main.py](#) vulnerable web app 13 days ago

[predict.py](#) vulnerable web app 13 days ago

[README.md](#)

## Among Us Predictor

Among Us CTF Web Hard 900

From the source code we know that the flag is stored in `flag.txt`. We're able to upload images which are then visible on the site. By reading the source code you can notice that there is no path validations on the exec url. We are then able to craft a python script that reads the flag file and prints it to stdio. We can then call the script by visiting `isss.io:5000/exec/imgs/flag.png`.

I did some searching on this repository, but couldn't find what I was looking for, so instead, I went to [his Github profile](#) from this vulnerable web app repository.

Edd King  
eddking6

I love walking my dog and eating Cacio e Pepe

2 followers • 0 following

Created 1 commit in 1 repository  
eddking6/DogFeedScheduler 1 commit

His profile bio says `I love walking my dog and eating Cacio e Pepe`. I wasn't too sure what `Cacio e Pepe` was, so I did a Google Search and revealed that it was a type of pasta.

Google search results for "cacio e pepe".

Images tab showing various photos of pasta dishes, including spaghetti with cheese and herbs.

Now we have found out that `Cacio e Pepe` is his favorite food. Now on his Github, he has another repository called [DogFeedScheduler](#) written in Go.

[eddking6 / DogFeedScheduler](#)

Code Issues Pull requests Actions Projects Wiki Security Insights

main 1 branch 0 tags Go to file Add file Code

**Edd King added email functionality** e76f938 13 days ago 3 commits

.gitignore	Initial commit	13 days ago
go.mod	added scheduler	13 days ago
go.sum	added scheduler	13 days ago
quickstart.go	added email functionality	13 days ago

No description, website, or topics provided.

0 stars 1 watching 0 forks

**Releases**  
No releases published

**Packages**  
No packages published

**Languages**  
Go 100.0%

Digging through the files, I found the following in [quickstart.go](#).

main DogFeedScheduler / quickstart.go / < Jump to v Go to file ...

**Edd King added email functionality** Latest commit e76f938 13 days ago History

0 contributors

61 lines (50 sloc) | 1.43 KB Raw Blame

```

1 package main
2
3 import (
4     "context"
5     "encoding/base64"
6     "io/ioutil"
7     "log"
8     "strings"
9
10    "golang.org/x/oauth2/google"
11    "google.golang.org/api/gmail/v1"
12    "google.golang.org/api/options"
13 )
14
15 func sendmail(srv gmail.Service, frommail string) {
16     temp := []byte("From: 'me'\r\n" +
17                 "reply-to: blobcorpiso@gmail.com\r\n" +
18                 "To: blobcorpiso@gmail.com\r\n" +
19                 "Subject: Feed Spot\r\n" +
20                 "remember to feed spot")

```

This shows us his email, which is `blobcorpiso@gmail.com` and his dog's name which is `Spot`.

From the tweets and Github, we have found the following so far:

- Name of his dog: `Spot`
- His favorite video game: `FactorIO`
- His alma master: ?
- His role at his company: `CISO`
- Favorite food: `Cacio a Pepe`
- His email: `blobcorpiso@gmail.com`

Now we just need his alma master. I assumed that the most likely place someone would list their alma master would be LinkedIn, so I went ahead and tried inputting his username `EddKing6` into the LinkedIn link like <https://www.linkedin.com/in/eddking6/>.

This brought us to [Edd King's LinkedIn](#). Here, we can see that his alma master is at `Texas A&M University`, and also confirms that his role at his company Blob Corp is `CISO`.

**Edd King** (He/Him)  
CISO at Blob Corp  
Austin, Texas, United States - [Contact info](#)

Connect Message More

**Activity**  
0 followers + Follow

Edd hasn't posted lately.

Last posted lately  
Edd's recent posts and comments will be displayed here.

Show all activity →

### Experience



CISO  
Blob Corp · Full-time

### Education



Texas A&M University

From the tweets, Github and LinkedIn, we have found the following:

- Name of his dog: Spot
- His favorite video game: FactorIO
- His alma mater: Texas A&M University
- His role at his company: CISO
- Favorite food: Cacio a Pepe
- His email: blobcorpciso@gmail.com

Now, the challenge says we need to send him a carefully crafted phishing email including all the details. I felt that just sending the information we found would be enough to get me the flag, but I decided to make it more believable by impersonating someone he might know.

Based on his Twitter, it seemed that he was pretty close to [Nichole Stephenson](#).

### edd king

@eddking6

I like hacking things and running blob corp

Joined February 2022

6 Following 3 Followers

Not followed by anyone you're following

Tweets

Tweets & replies

Media

Likes



Nichole Stephenson @Nichole48928026 · Mar 2  
Made Brownies



1

1

1

1



edd king @eddking6 · Mar 2  
Looks good!

1

1

1

1

So I decided to make a Gmail account that impersonates Nichole Stephenson.

Google

Create your Google Account

to continue to Gmail

First name  Last name

Username  @gmail.com

You can use letters, numbers & periods

Password  Confirm

Use 8 or more characters with a mix of letters, numbers & symbols

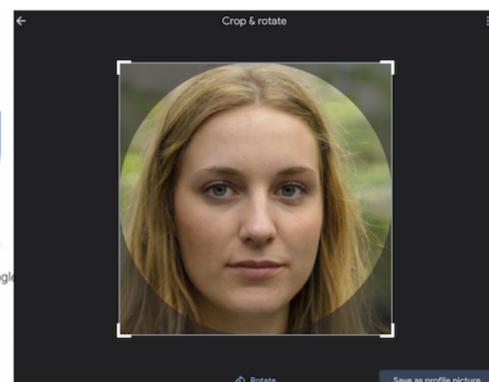
Show password



One account. All of Google working for you.

Sign in instead

Next



I wanted to make the phishing mail as believable as possible so I wrote an email to blobcorpciso@gmail.com saying that there is a company

I wanted to make the phishing mail as believable as possible, so I wrote an email to [blobcorpinfo@gmail.com](mailto:blobcorpinfo@gmail.com) saying that there is a company party that celebrates his achievements as a CISO, and embedded all the required information while trying to sound natural and believable.

## Important CISO business



Steph Nic <[blobsteph@gmail.com](mailto:blobsteph@gmail.com)>  
to blobcorpinfo ▾

Sat, Mar 12, 9:10 PM (3 days ago)



Dear Edd,

I made brownies and Cacio e Pepe this week, and I'm thinking to treat everyone at Blob Corp during this week's party to celebrate your achievements as a CISO!

Actually, I made so much that could feed everyone's family. I'll ask everyone to bring tupperwares so their kids can enjoy the brownies too. (Not for your furkid, Spot though! Since chocolate is poisonous to them haha)

I heard that the alumni from Texas A&M University are coming too? Any special preferences they might have regarding the brownie toppings and might anyone be allergic to Cacio e Pepe?

Also, I'll bring extra monitors & HDMI cables so we can all play FactorIO together at the party!

Let me know if there's anything else I should bring to the party!

Also, I need the password to log into the admin account so I can start set up an account for the guests that are coming.

Best regards,  
Nichole Stephenson

Reply

Forward

Then I received the flag after a few minutes of sending the email.

## Important CISO business



blobcorpinfo@gmail.com  
to me ▾

Sat, Mar 12, 9:11 PM (3 days ago)



Hi,  
The flag is `utf8{osint_is_fun}`

Reply

Forward

Here's another variation of the email I made which I thought might be interesting to share, where Nichole requests admin access to fix up the company's password reset system.

Important CISO business

blobcorpinfo@gmail.com

Important CISO business

Hi Edd King,

I am currently analysing the password reset functionality for the Blob Corp employees' accounts.

The current password reset questions look like this, and I'm using yours as an example:

Name: Edd King  
Position: CISO at Blob Corp  
Email: [blobcorpinfo@gmail.com](mailto:blobcorpinfo@gmail.com)

Where's your alma mater (Q1): Texas A&M University  
What's your favorite food (Q2): Cacio a Pepe  
What's your dog's name (Q3): Spot  
What's your favorite video game (Q4): FactorIO

These questions seem to be pretty weak as these info could be found online, so I'm planning to update the password reset questions and include multi-factor authentication.

Please give me the admin account password so I can update this functionality.

Regards,  
Nichole Stephenson

Thus, the flag is,

`utf8{osint_is_fun}`