Files

main

Go to file t

- 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

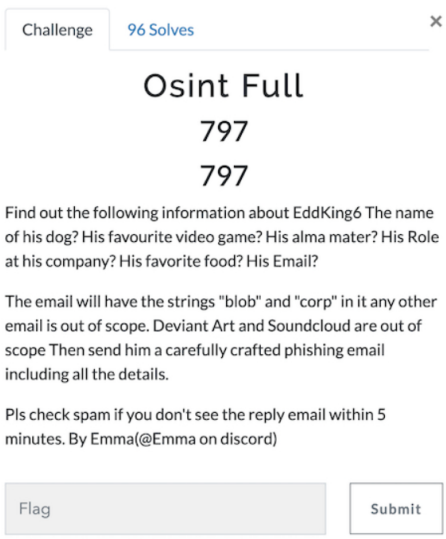
LambdaMamba Fixed some format problems e349910 · 2 years ago History

| 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,



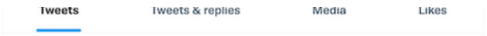

We are given the username of the person we are targeting, which is `EddKing6`. It also mentions that the email should contain the strings `blob` and `corp`, so this is something we should be looking for when searching Ed King. Also, we will need to look for the following info:

- 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.

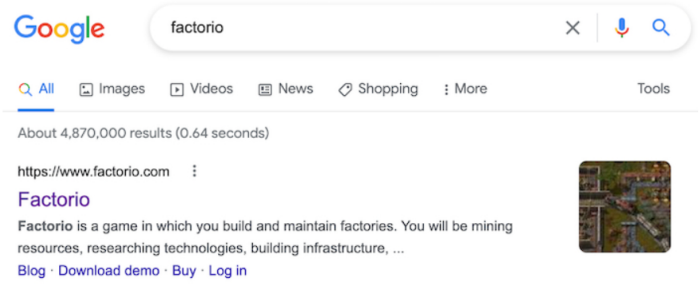
In fact, searching `EddKing6` on Twitter returned this account.

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.




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

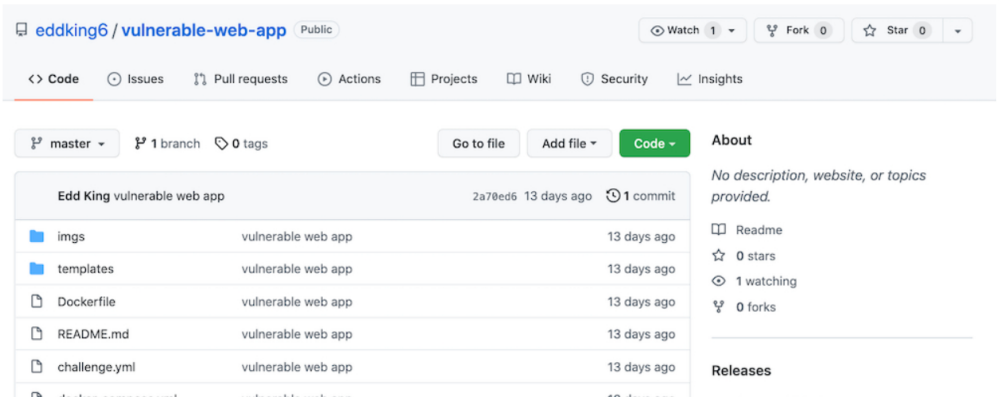

From the tweet `I like to play FactorIO when I'm not busy being a #CISO`, we can see that he is a `CISO` and he plays `FactorIO`. However, I wasn't too sure what `FactorIO` was, so I did a Google Search and revealed that it was in fact a video game.

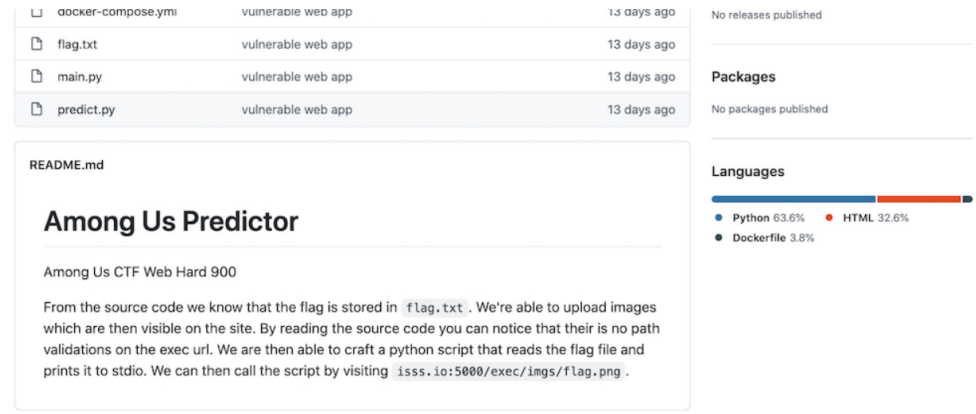



From the tweets alone, we have found the following so far:

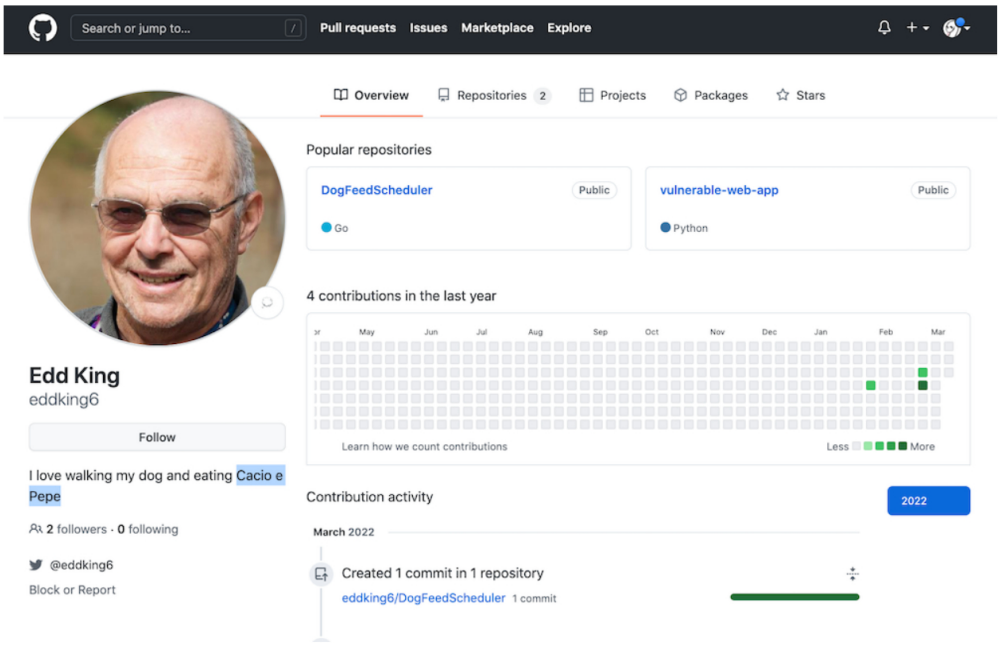
- Name of his dog: ?
- His favorite video game: `FactorIO`
- His alma master: ?
- His role at his company: `CISO`
- Favorite food: ?
- His email: ?

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

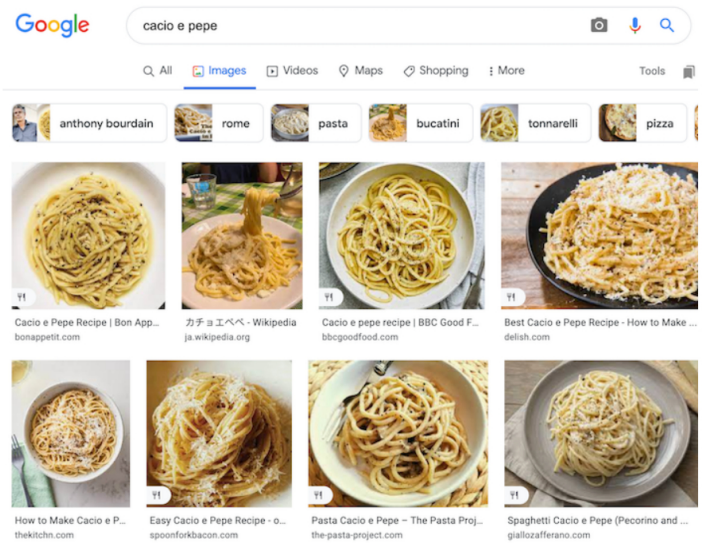




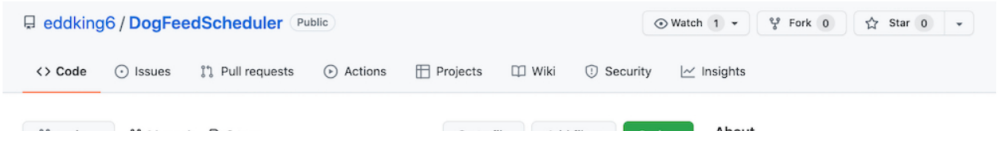

I did some searching on this repository, but couldn't find what I was looking for, so instead, I went to his Github profile from this vulnerable web app repository.

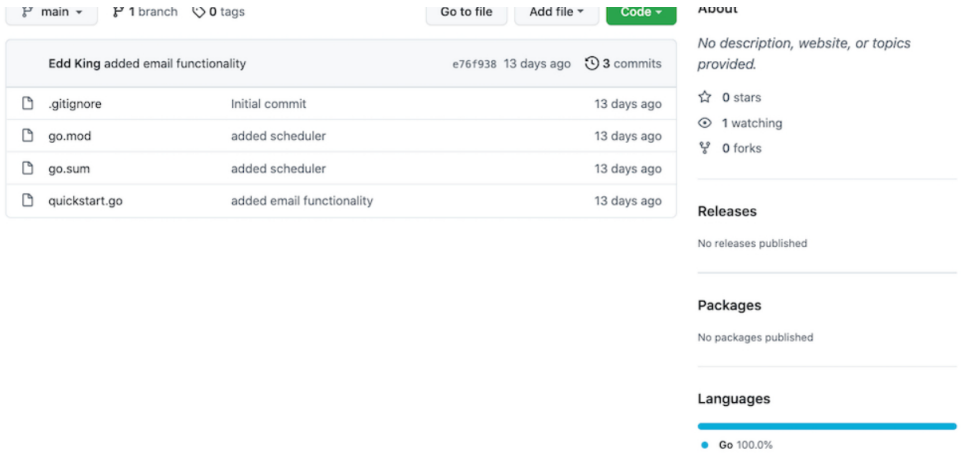



His profile bio says `I love walking my dog and eating Cacio e Pepe`. I wasn't too sure what `Cacio a Pepe` was, so I did a Google Search and revealed that it was a type of pasta.

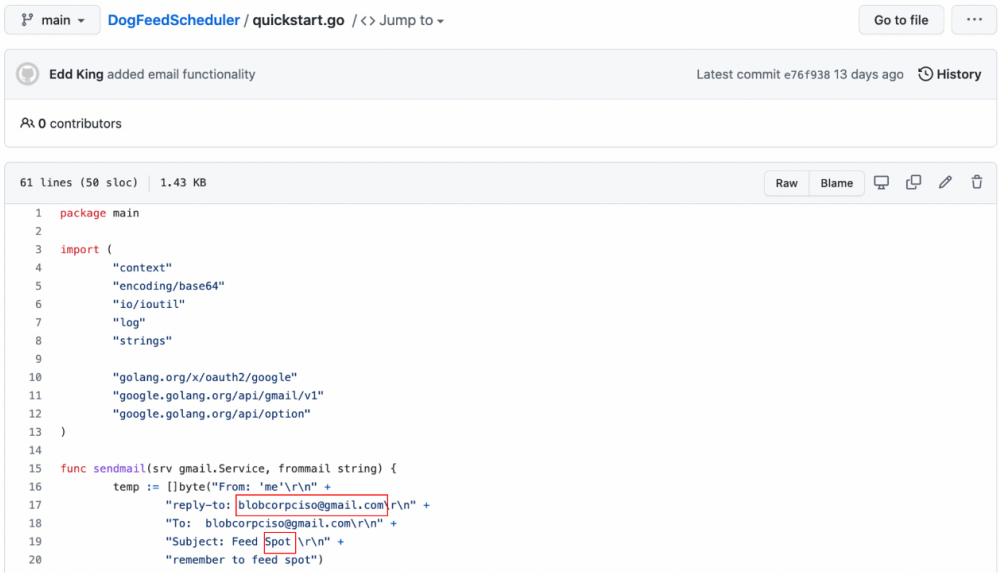



Now we have found out that `Cacio e Pepe` is his favorite food. Now on his Github, he has another repository called DogFeedScheduler written in Go.






Digging through the files, I found the following in quickstart.go.



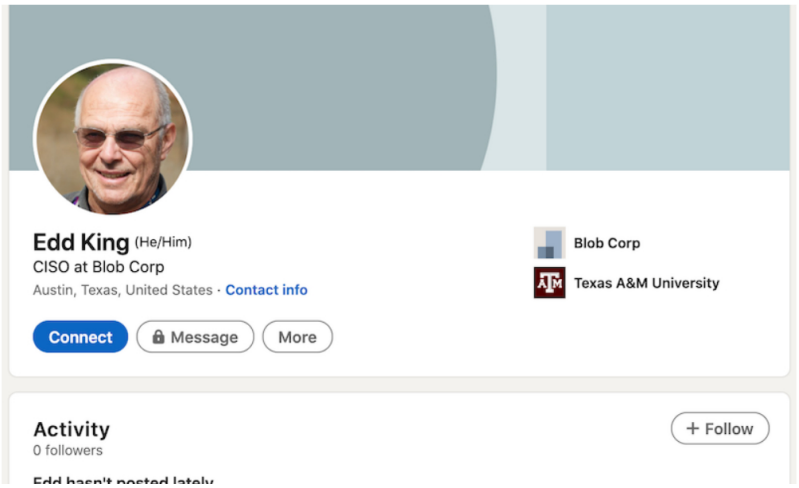

This shows us his email, which is `blobcorpciso@gmail.com` and his dog's name which is `Spot`.

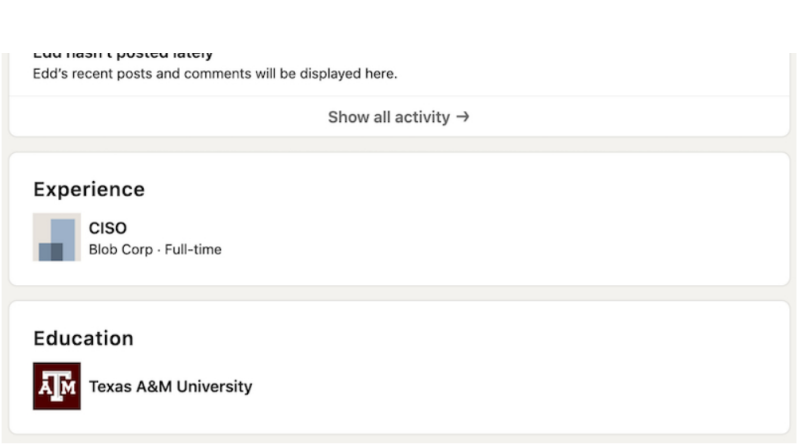
From the tweets and Github, we have found the following so far:

- 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: `blobcorpciso@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`.



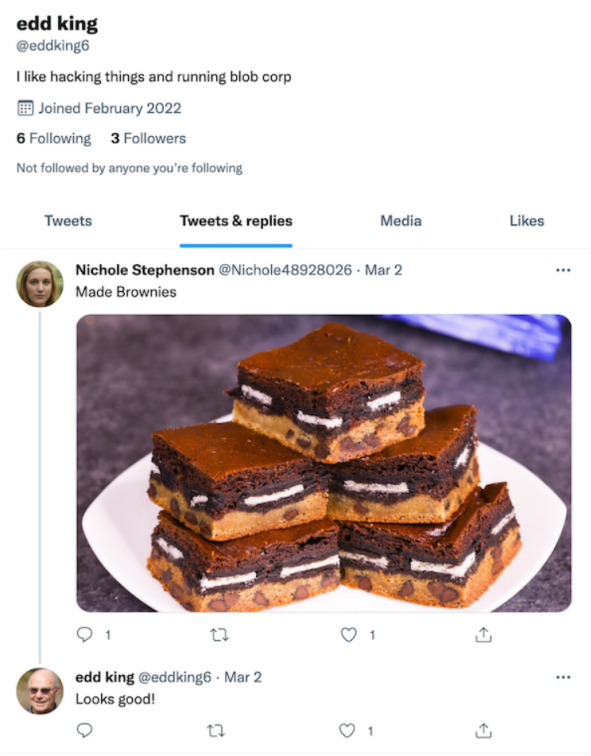



From the tweets, Github and Linkedin, we have found the following:

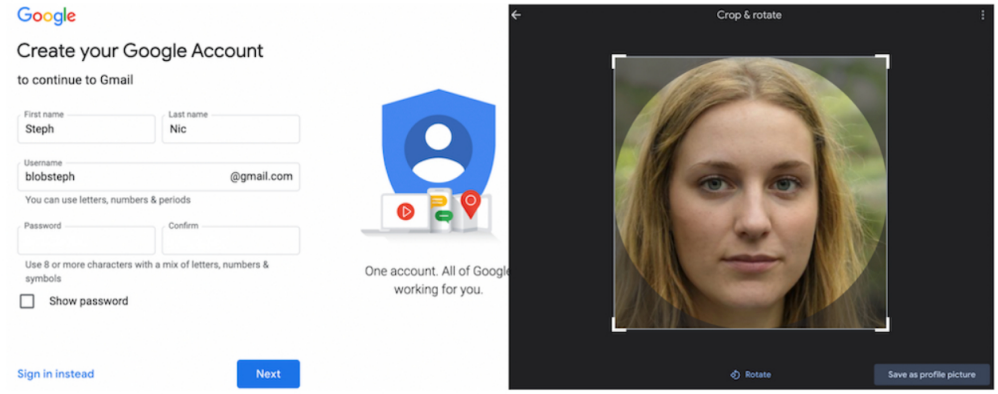
- Name of his dog: `Spot`
- His favorite video game: `FactorIO`
- His alma master: `Texas A&M University`
- His role at his company: `CISO`
- Favorite food: `Cacio a Pepe`
- His email: `blobcorpciso@gmail.com`

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.

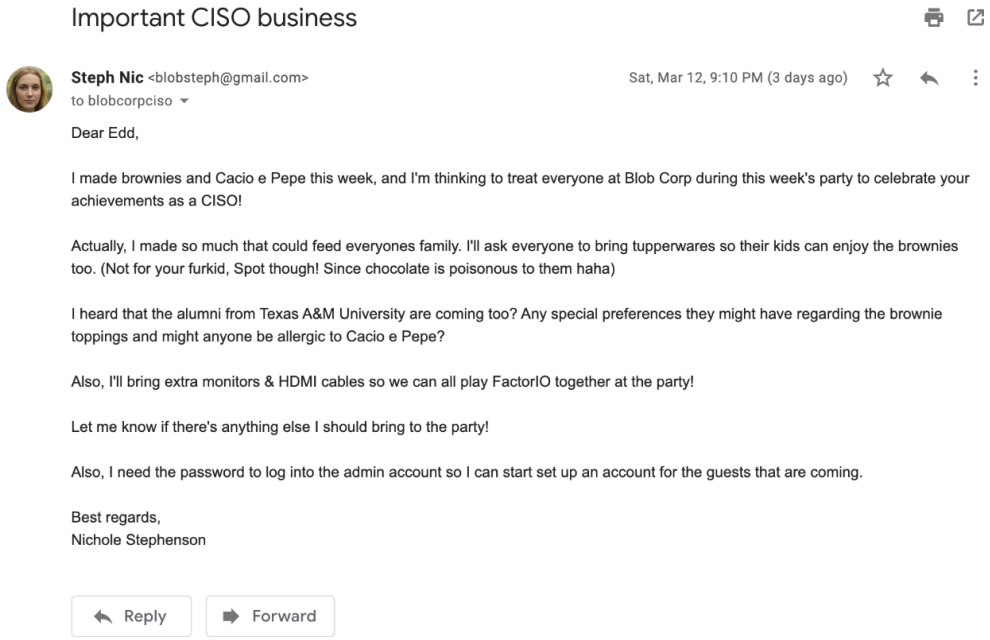



So I decided to make a Gmail account that impersonates Nichole Stephenson.




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 [redacted] 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> Sat, Mar 12, 9:10 PM (3 days ago)
to blobcorpciso

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 everyones 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!

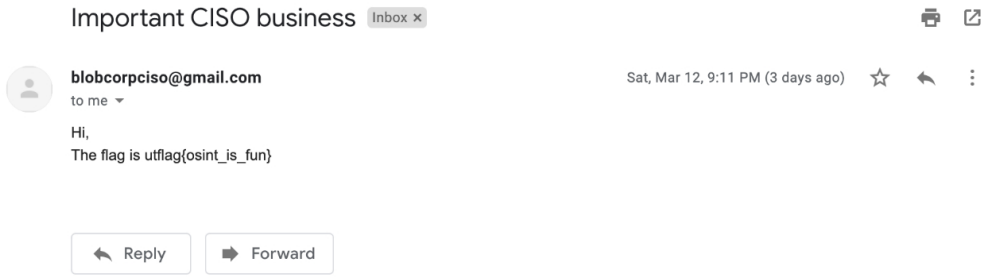
Let me know if there's anything else I should bring to the party!

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.



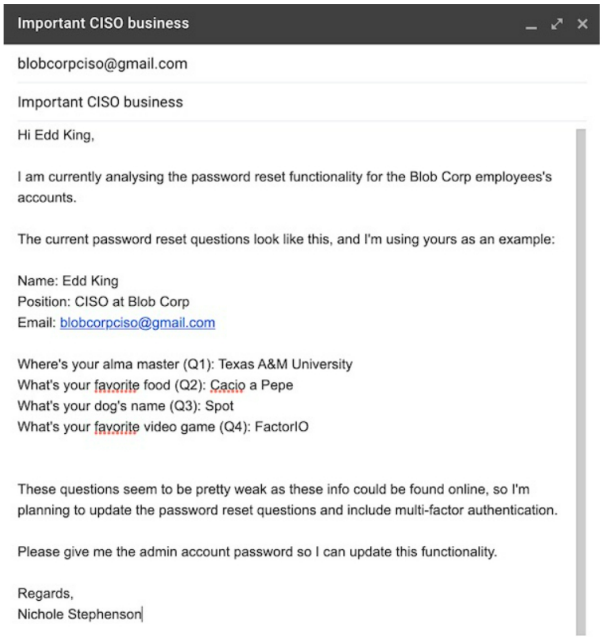
Important CISO business Inbox ×

**blobcorpciso@gmail.com** Sat, Mar 12, 9:11 PM (3 days ago)
to me

Hi,
The flag is utflag{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

blobcorpciso@gmail.com

Important CISO business

Hi Edd King,

I am currently analysing the password reset functionality for the Blob Corp employees's 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: blobcorpciso@gmail.com

Where's your alma master (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,

`utflag{osint_is_fun}`