OSINT Scenario Solutions

Introduction

The OSINT scenario in this case is NOT jeopardy style. This is a real life engagement scenario, so it should be approached as such. It aims to showcase how a real life forensics analysis are typically approached by professionals and how to cancel out excessive noise the artifacts tend to have in real life. That said, let's dive straight into the solution.

Note that all the "challenges" expecting answers were designed to be case insensitive, so it doesn't matter how you will provide the right answer. (security or SeCURitY, both will be correct)

Statement of Work

A statement of work is a document that is created between two companies – the supplier and the customer, which will provide services. The supplier in this case provides a service defined by the Statement of Work to the customer. A statement of work is considered a legal document and as such a breach of contract could result in fines or legal repercussions. That's why the statement of work should contain clearly defined expectations and limitations in case they are applicable.

The statement of work provided in the event was "SoW – OSINT Consulting Services 2025.docx".

BLIND SECURITY

Statement of Work

Blind Security ("Customer")	**CSCGR Pentesting Team ("Supplier")**
Kaykasou 19, Aristotelous 54044 Thessaloniki Greece	Athens University of West Attica 122 43 Greece
Email: accounts@blindsecurity.net Telephone: 240765432 VAT: 589552658	Email: your@team.email VAT: N/A
Contact: Petros Papadopoulos	Contact: Your-Team-Lead-Name

Solutions

OSINT

Question: What does OSINT stand for?

Answer: Open Source INTelligence

Explanation: Simple abbreviation.

OSINT Framework

Question: What is the most famous OSINT Framework called?

Answer: maltego

Explanation: Maltego is actually the tool not the framework, so there's a bit of a mistake in the question itself. Maltego is sometimes associated as a framework as well. In any case, it's the most popular **tool** out there.

OSINT Non-Profit

Question: What is the non-profit organization called which assists in missing persons cases and provides OSINT training?

Answer: tracelabs

Explanation: Trace Labs is a nonprofit organization whose mission is to accelerate the family reunification of missing persons while training members in the tradecraft of open source intelligence (OSINT).

Checkpoint – Review

Let's start by reviewing the statement of work. We have been given allowance to start working with the main webpage of the company (blindsecurity.net) and identify further company resources/associated employees. We cannot however target the websites and perform any type of active scanning. We are free however to perform passive scans on the websites and identified resources.

Scope of Work

The scope includes footprint analysis for all Blind Security related information and employees. The assessment can start with the below website:

Type	Applications	Endpoints
Main Website	BlindSec Main Website	blindsecurity.net

Scope Limitations

Identified websites and resources related to Blind Security or its employees shall not be pentested. Passive scans are allowed if deemed applicable.

Additionally, the following attacks are deemed out of scope and therefore are not permitted:

1. Denial of Service Attacks (DoS) and Distributed Denial of Services Attacks (DDoS)
2. Active scans on identified websites or resources of Blind Security or their employees. (dirbuster, gobuster, sqlmap, etc)

All other attacks not specified by Blind Security are permitted.

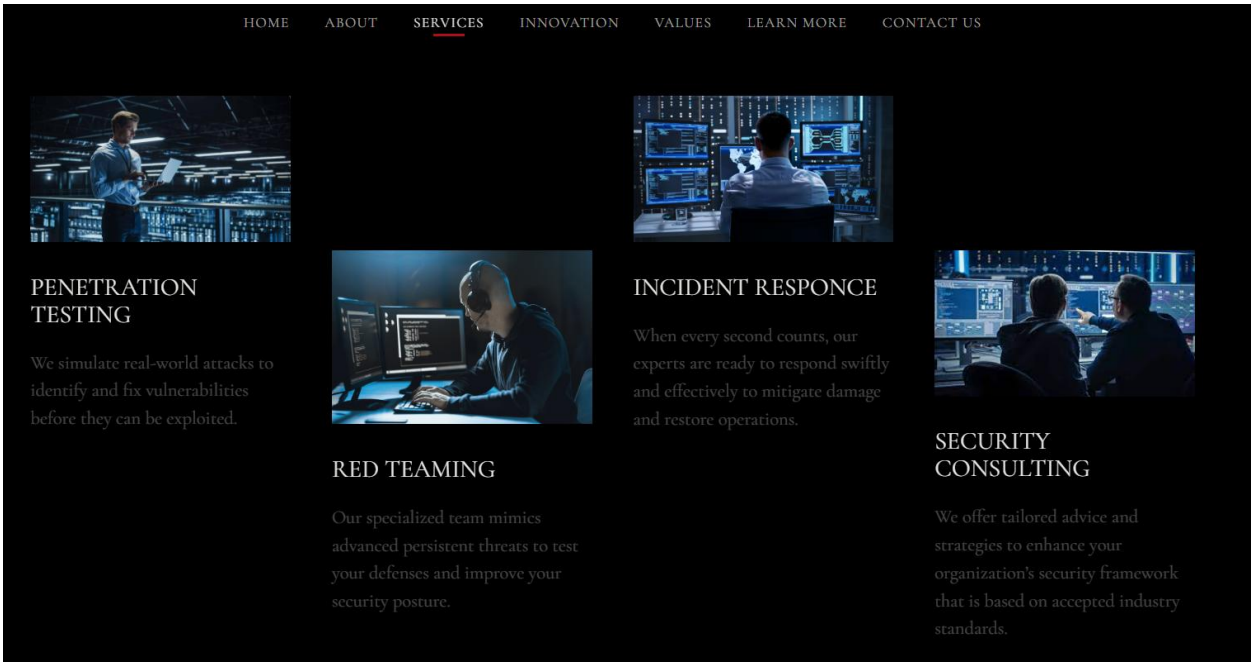
Services

Question: How many services does Blind Security provide?

Answer: 4

Explanation: Let's start by reviewing the main website of the company. In the frontpage we can see the 'Services' section on which they specifically list 4 offered services:

- Penetration Testing
- Red Teaming
- Incident Response
- Security Consulting



Employees

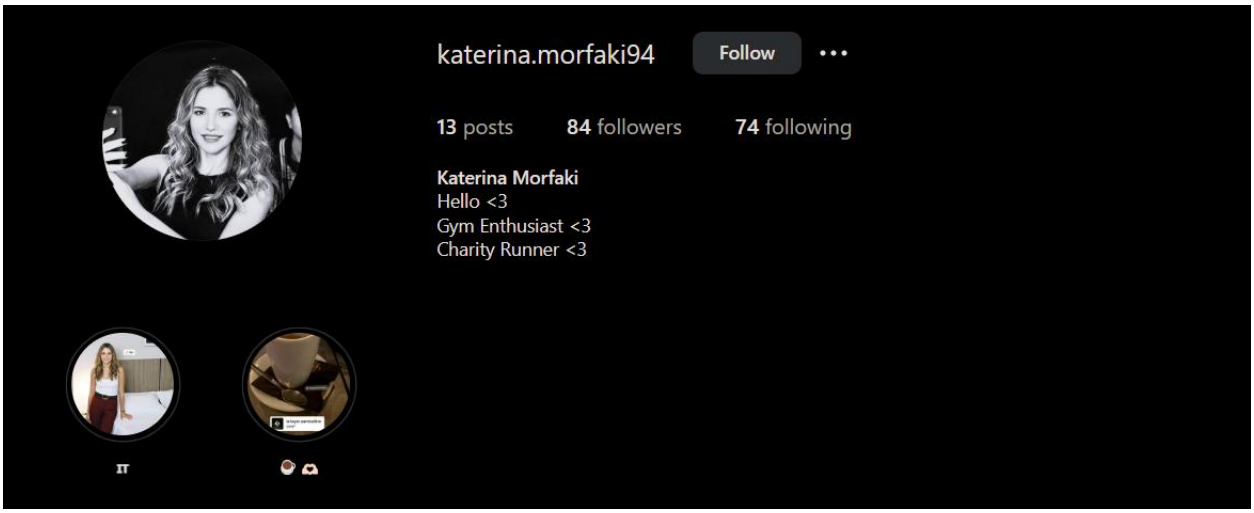
Question: How many team members does Blind Security have?

Answer:12

Explanation: Scrolling down to the “Values” part of the webpage we can notice there’s a button “Our Team” which redirects to “/team.html”. There we can count 12 people in the company. (Even though C-levels are not considered employees, for this example we will consider them as employees)

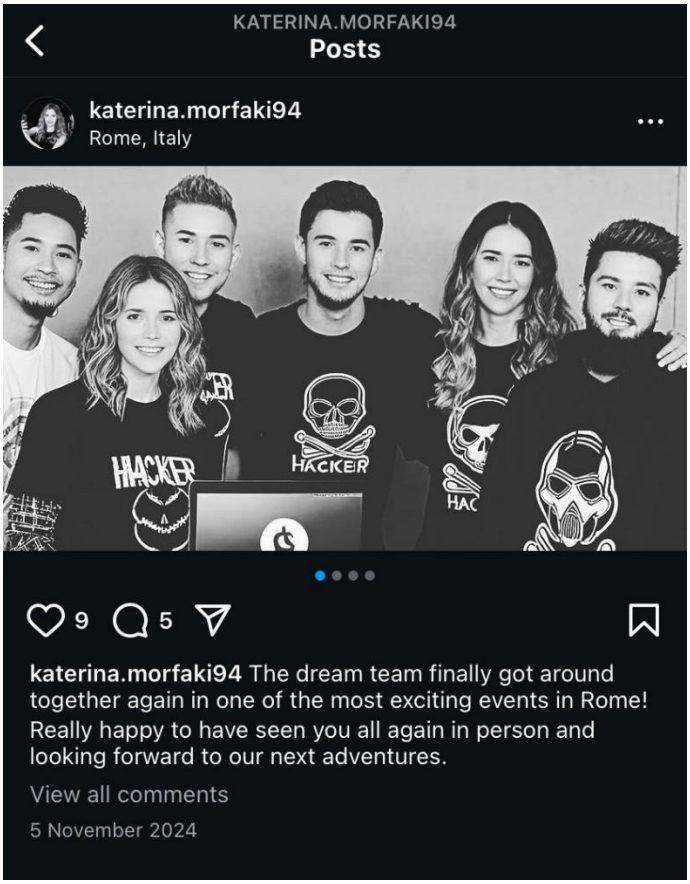
CheckPoint – OSINT

Before we proceed answering any further questions/flags, we need to perform some proper OSINT. Let’s start with Katerina’s account as proposed by the order of the challenges. After searching a bit for Katerina Morfaki on social media while keeping in mind her picture, we come across her Instagram profile:

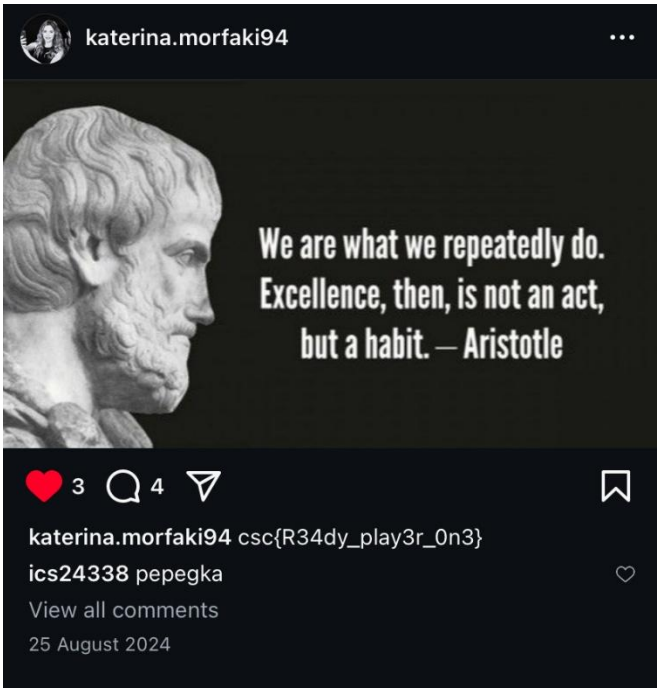


Apparently she loves going to the gym and is a charity runner. Probably a Cardio buff. Bruh,.. :D

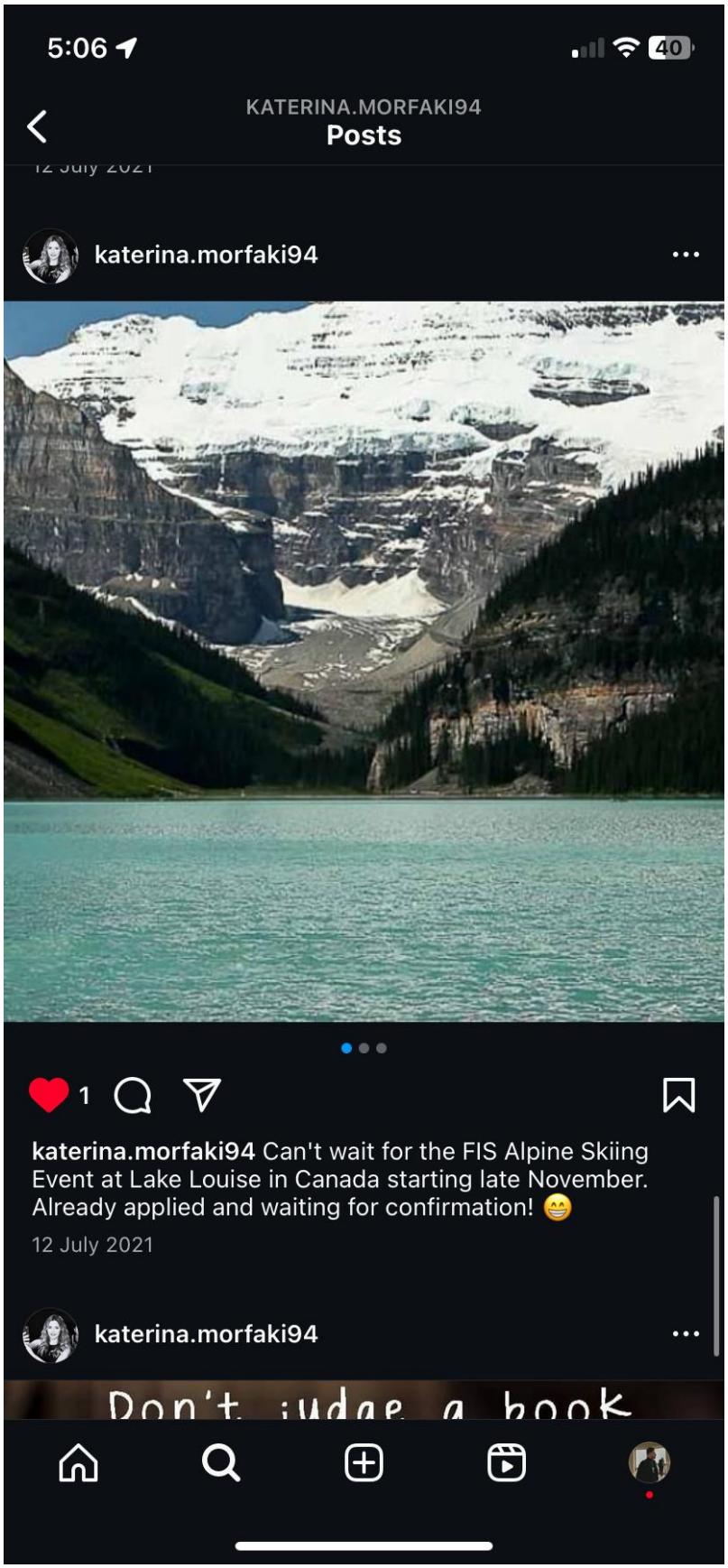
Going through her posts we notice she went to a cybersecurity conference – which we do not know yet, but we know it was in Rome. So we would look for specific security related conferences taking place in Rome later on. First, we focus on low hanging fruits.



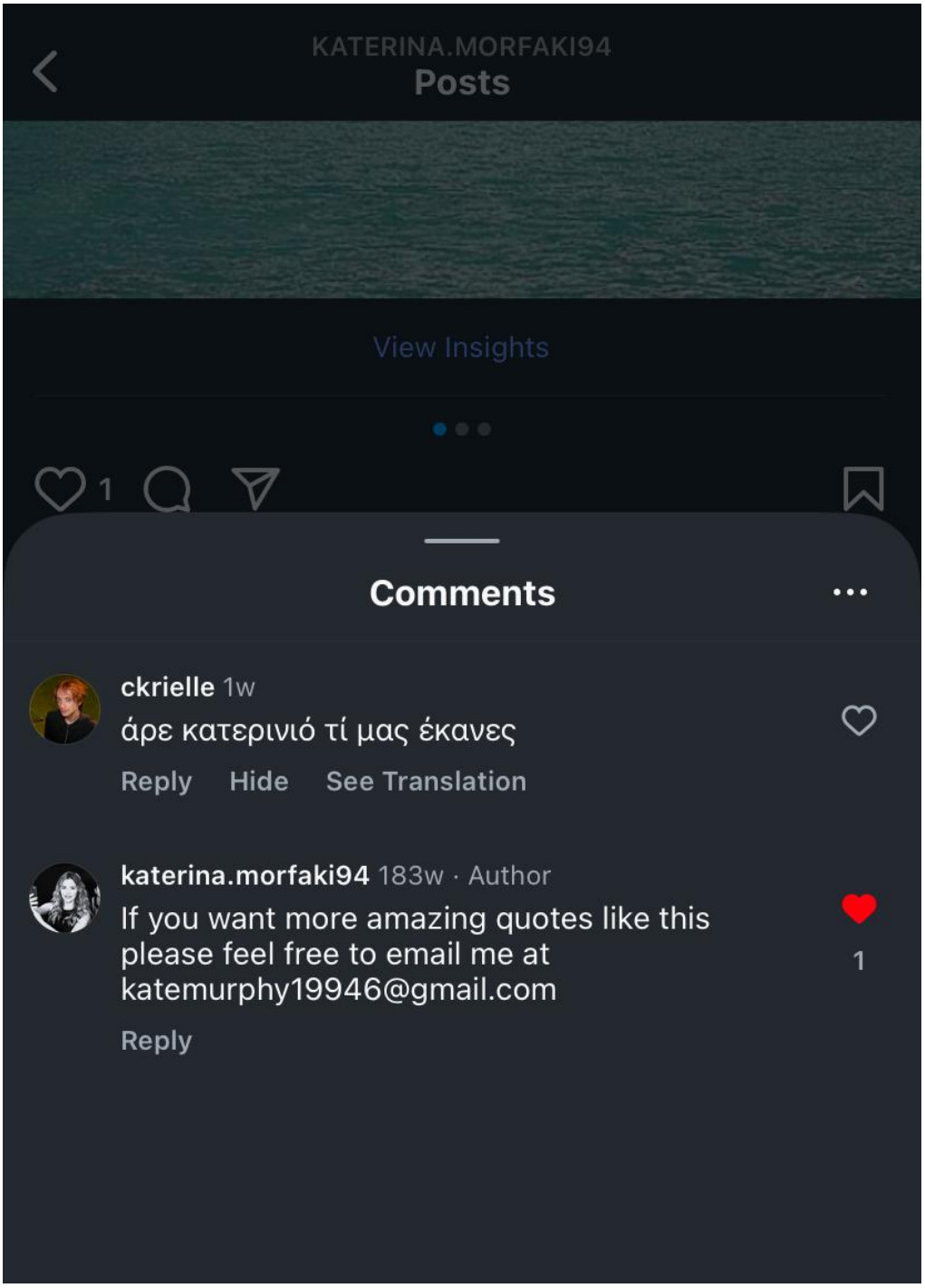
She apparently has a cat as another post indicates.. She also has some quotes. The first quote actually has the flag. (*Answer to Katerina Morfaki)



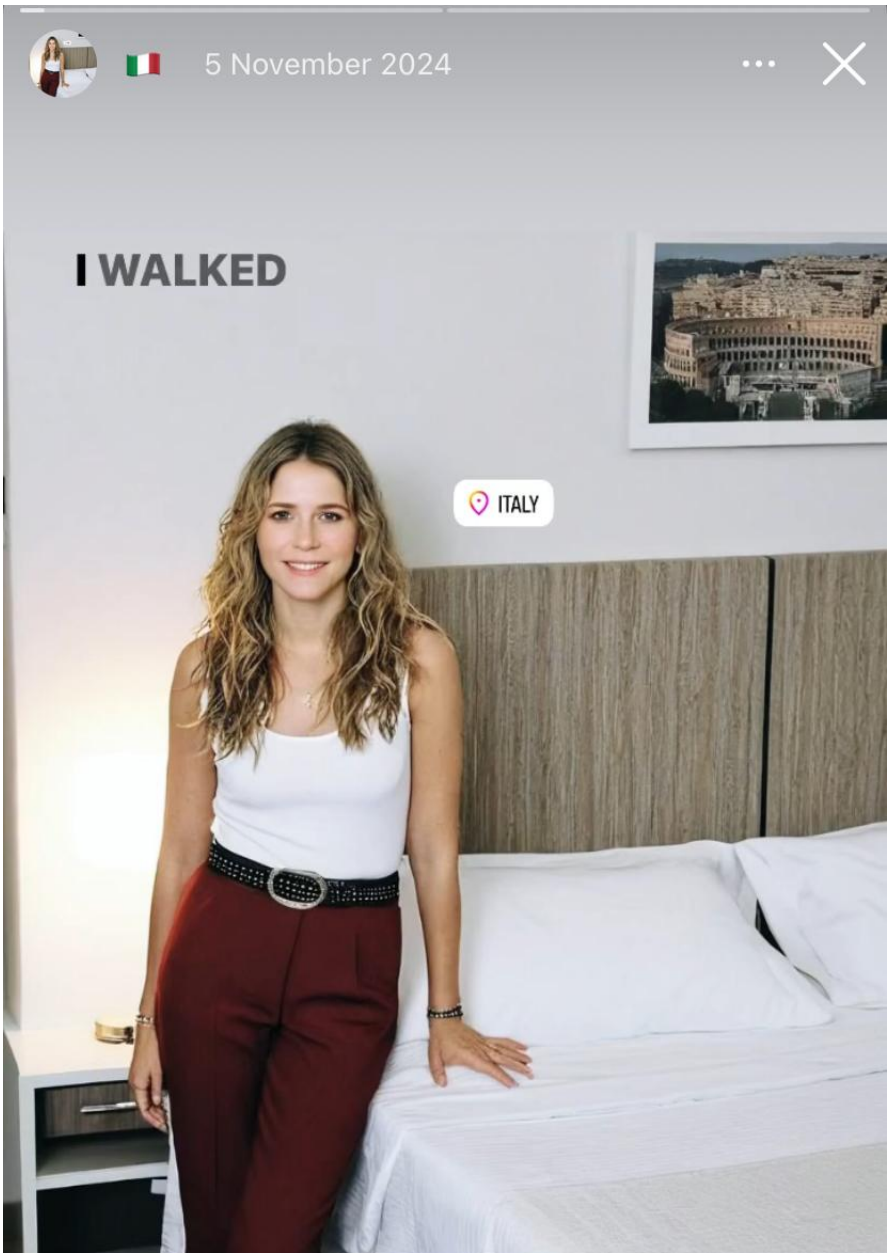
There are some other extra posts including some interesting info such as the FIS Alpine Skiing Event.



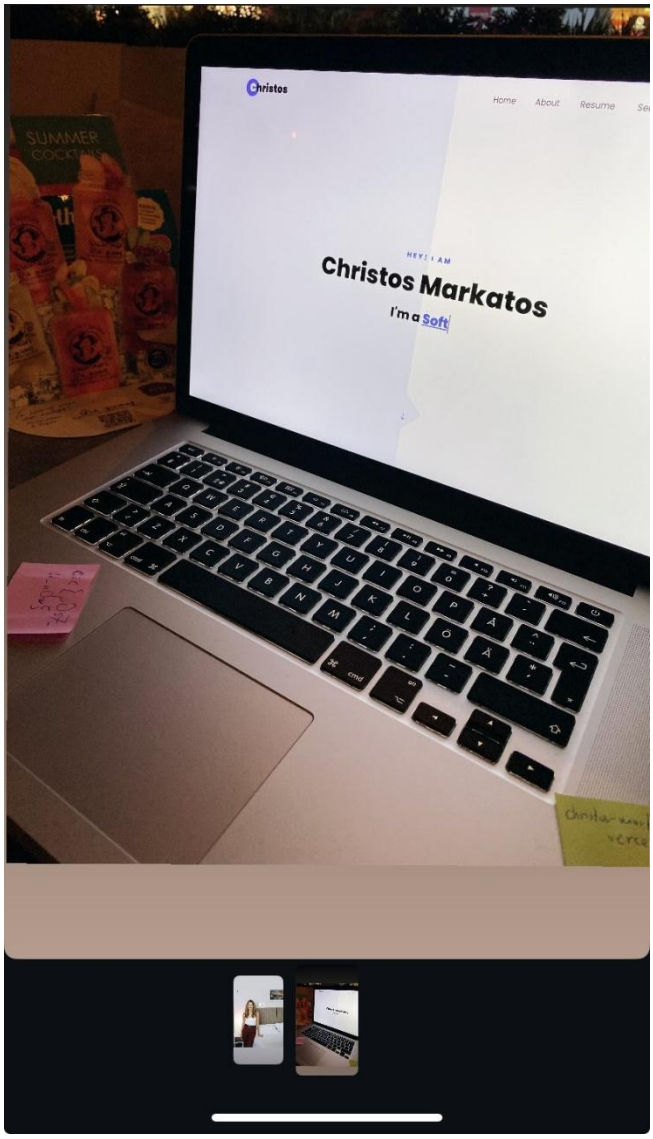
And the last post which contains her email address. (Note that in light of recent Instragram changes her email address was either redacted from the comment or her comment was not visible at all. Once this was identified the CSCGR team released her email in discord.) (*Answer to Katerina's Email)



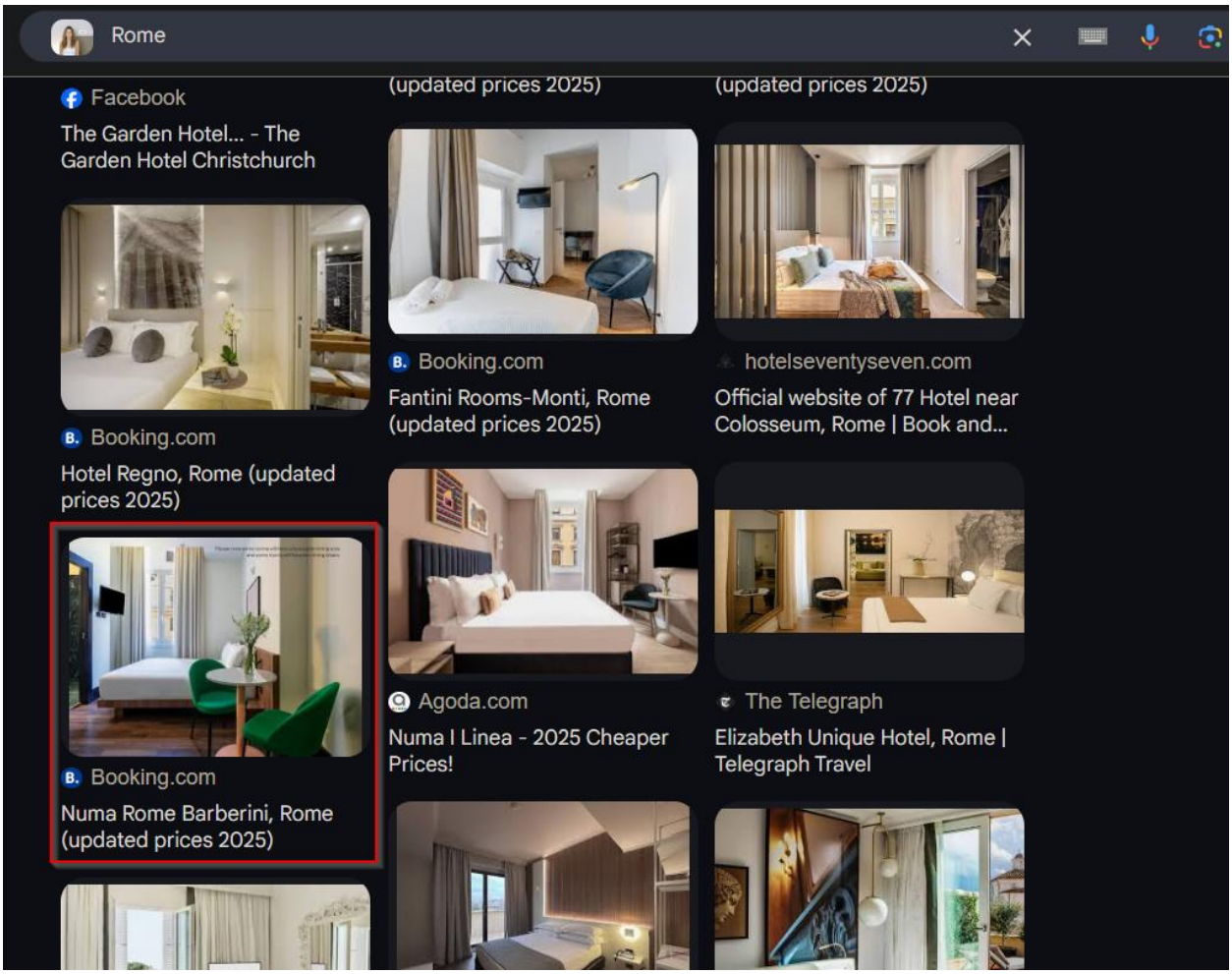
Examining her highlights, we can see a picture of her in a hotel room which we can tell is from Italy as per the location tag. We could use this to identify which hotel it was.



The next highlight is a story with her computer and some post its. Probably from the security conference in Rome she mentioned in the post as it's on the same highlight as her hotel. The post it notes is a flag – csc{p0s7_1t_n0w} (*Answer to Artifacts) and the other post has the following visible text – christos-mark and verce. We need to guess the rest.



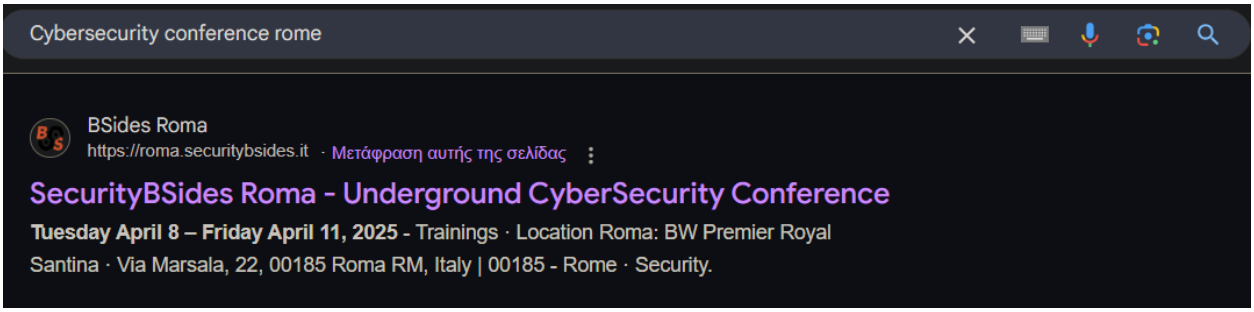
Time to see what other questions we can answer. Let's try to identify the hotel. The approach to this would be a reverse image search which we could use from her highlight. Let's try that.



Examining the rooms and details of what we have in the picture, we can tell the bed frame and picture on top of the bed match what we saw on Katerina's picture for one of the hotels listed in the results. – Numa Rome Barberini (*Answer to Katerina's Hotel) – **Note**: During the event, the hint of the word count was misleading due to an issue with the CTFd platform interpreting asterisks as bold text and therefore changed the number of letters suggested and did not match the right hotel, hence it went unsolved, even though multiple teams actually solved it.

What event could Katerina have visited? This one is an interesting one. There's multiple events in Italy. Let's look for specific events in Rome. Many exist but most

notably, with one of our sponsors equivalents 😉 -

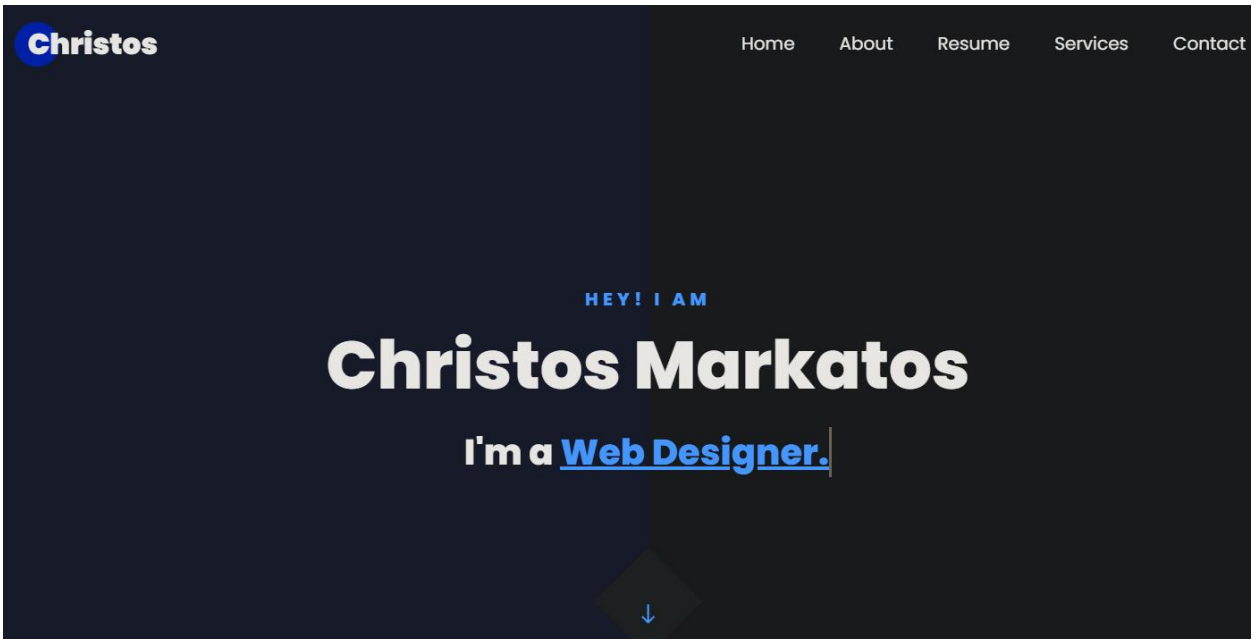


BSides Roma – (*Answer to Katerina's Event)

Time to move past Katerina and start looking at Christos Markatos. We know there's a hint for him – christos-mark and verce. This looks like a URL structure. We know we are also looking for a personal webpage. A common free provider to host your personal page is Vercel.app. Chances are that Chris is hosting his personal webpage on vercel and shared it with Katerina during the conference. Let's have a look and google for that.

christos-mark.vercel.app doesn't yield any results. Maybe he used his full name?

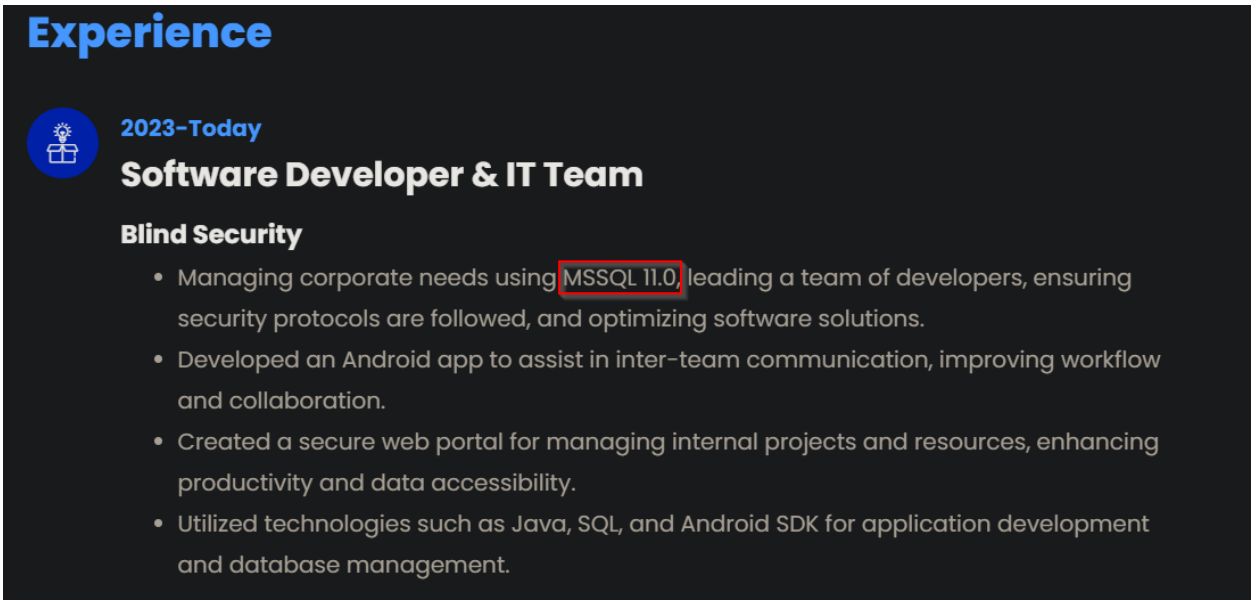
christos-markatos.vercel.app returns a webpage.



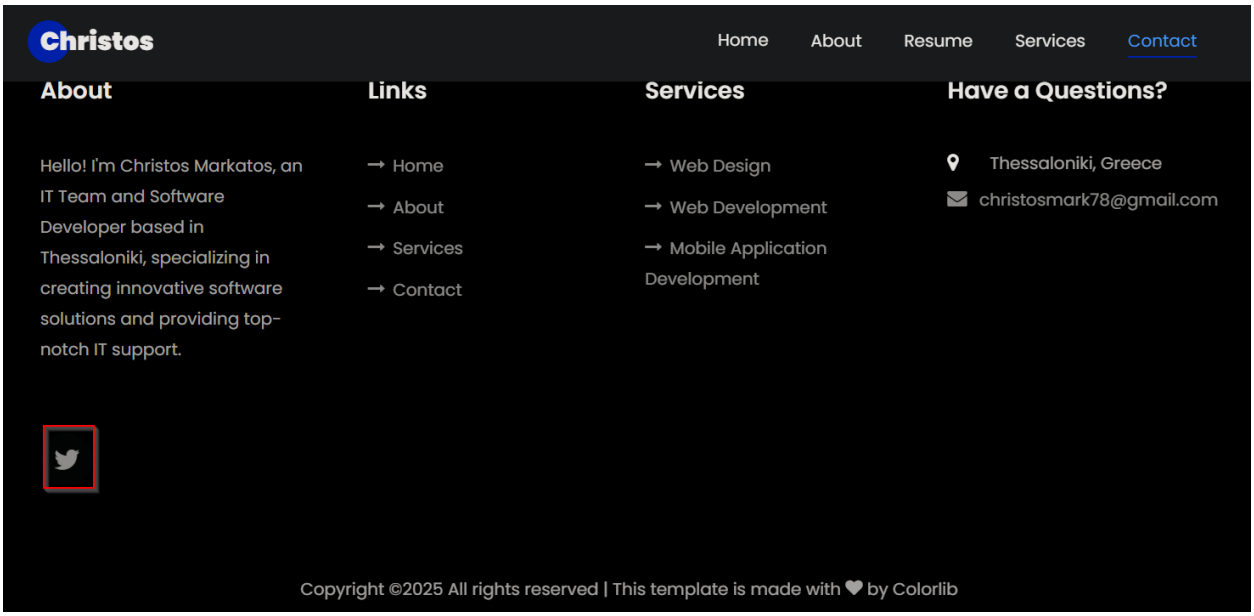
Let's investigate a bit. Actually hold up. While writing the write-up I encountered the flag. It's loading painfully slow, so let's use developer tools to get it instead.

(*Answer to Christos Markatos Personal Page)

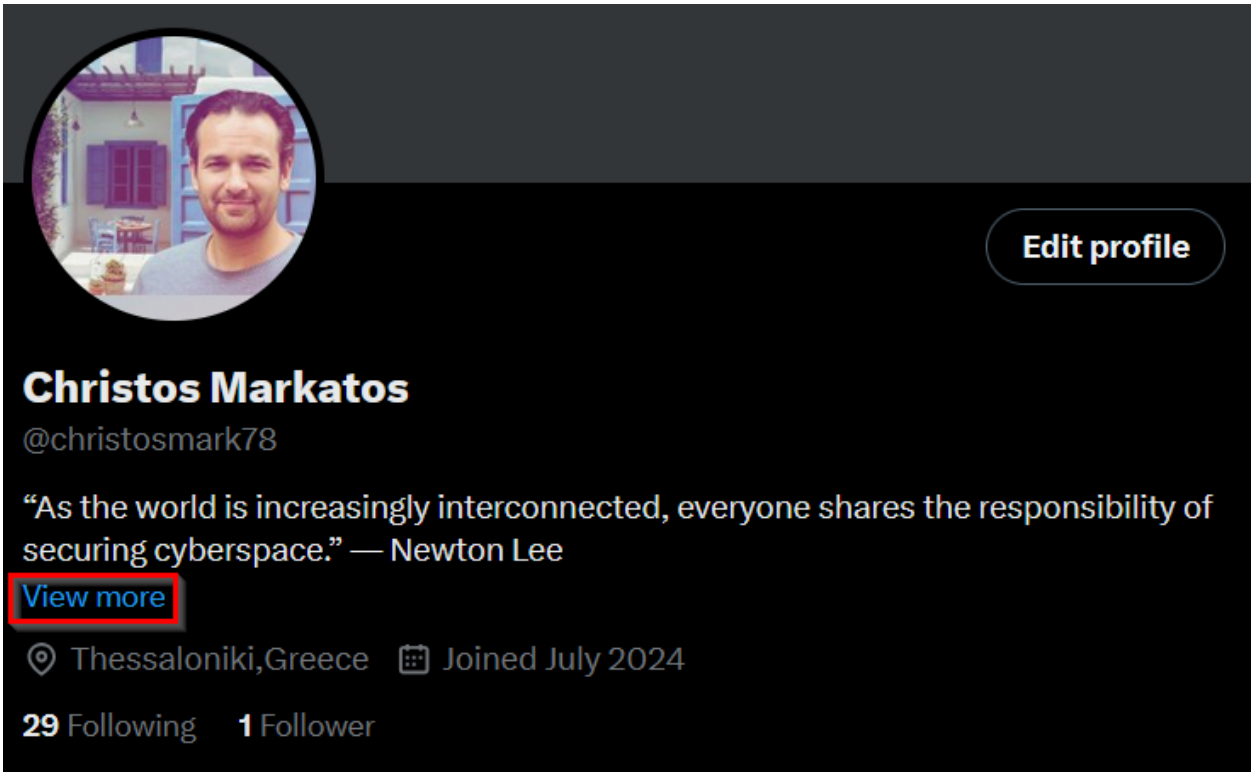
Further going down christos' page, we notice he has gained experience with MSSQL 11.0 while working for Blind Security. That's a good indicator that Blind Security is using MSSQL 11.0 for their systems.

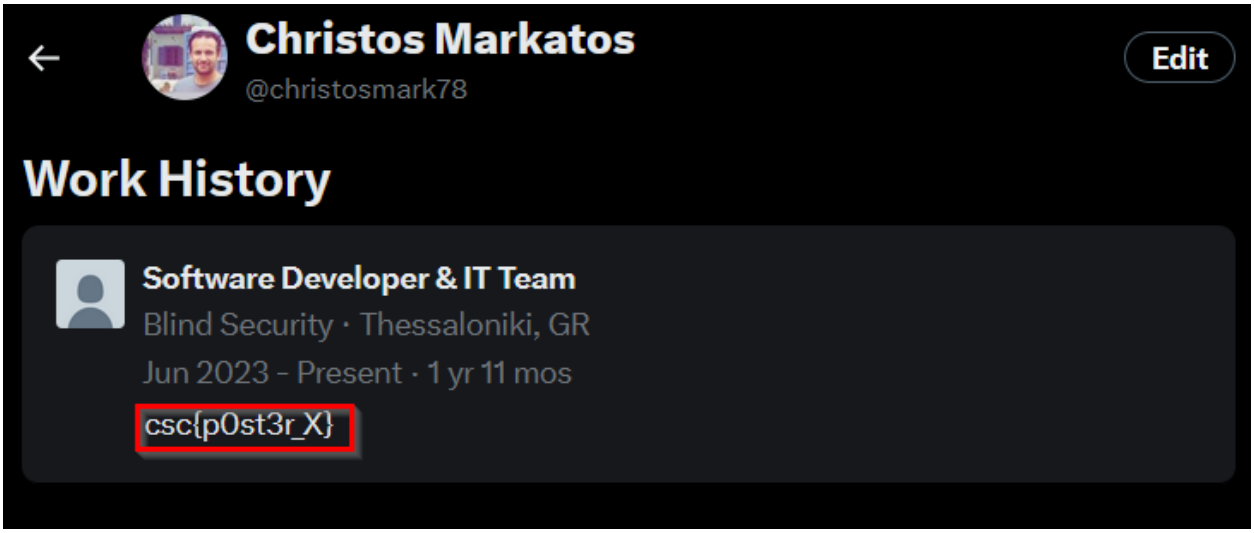


And finally, after scrolling all the way down, we finally see a twitter link linking us to chris' first social media account -

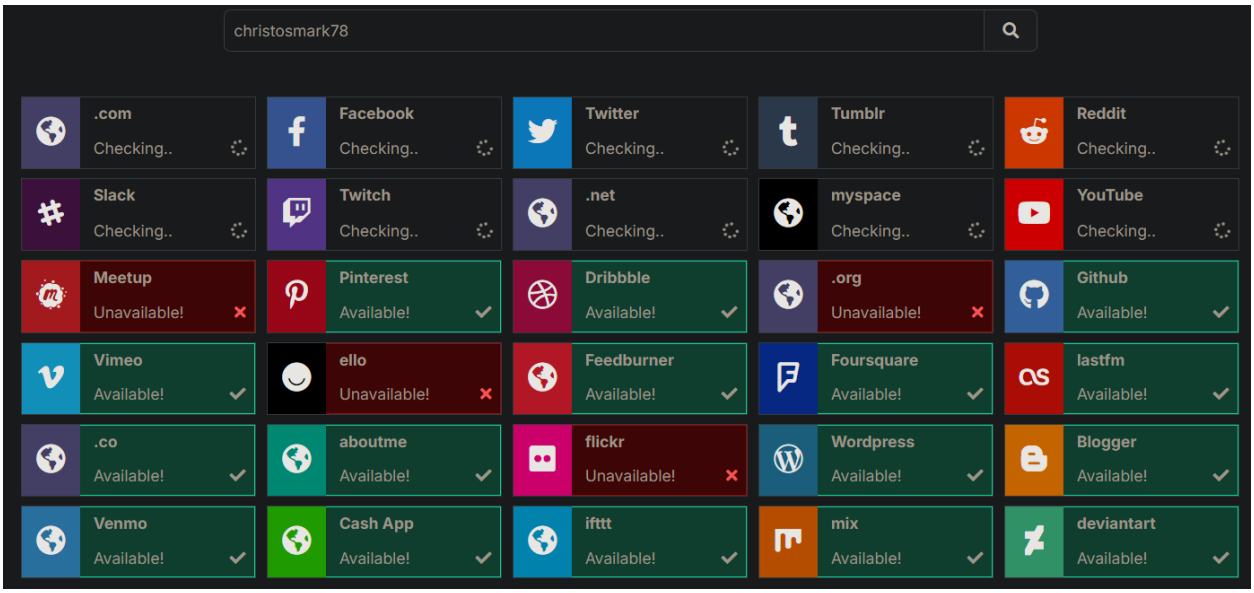


The first thing we notice as soon as we arrive on his page is a multitude of posts. We can go through them, but it doesn't look like there's a flag anywhere to be found. We have to be more creative than that. (There's a semi-newly implemented feature in X which allows users to add their professional experience and comments which is not yet visible on mobile devices using the app – at the time of the event and writing) Chris apparently uses it and has added the flag there.



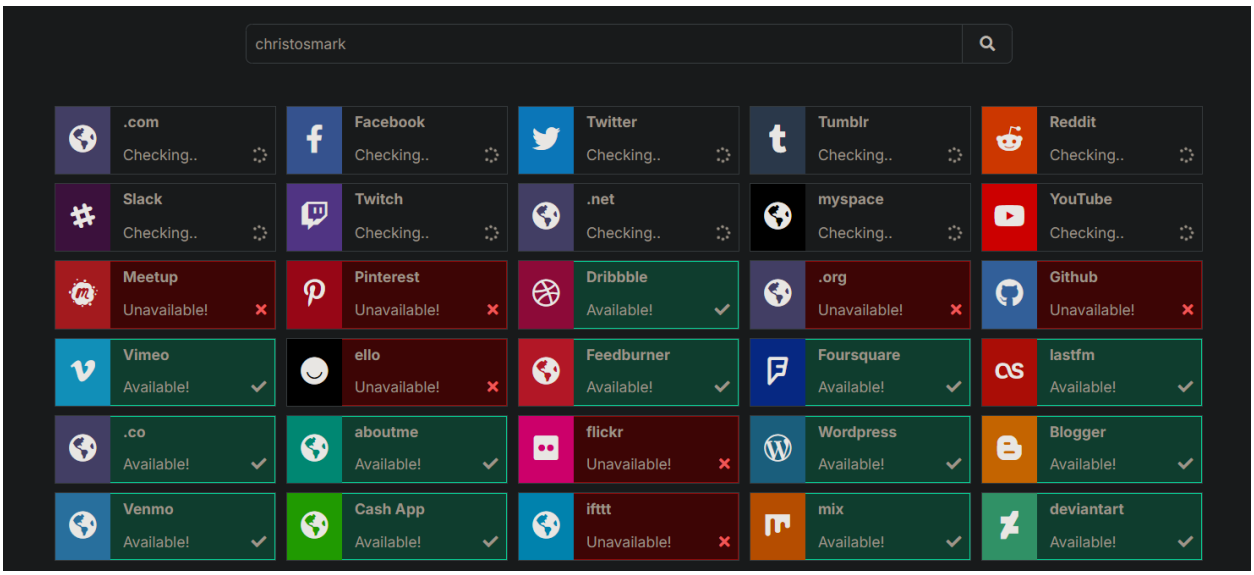


And as we know we’re looking for another social media, let’s try seeing if he reused his username on other platforms. I’m using namechkr.com to perform this operation.

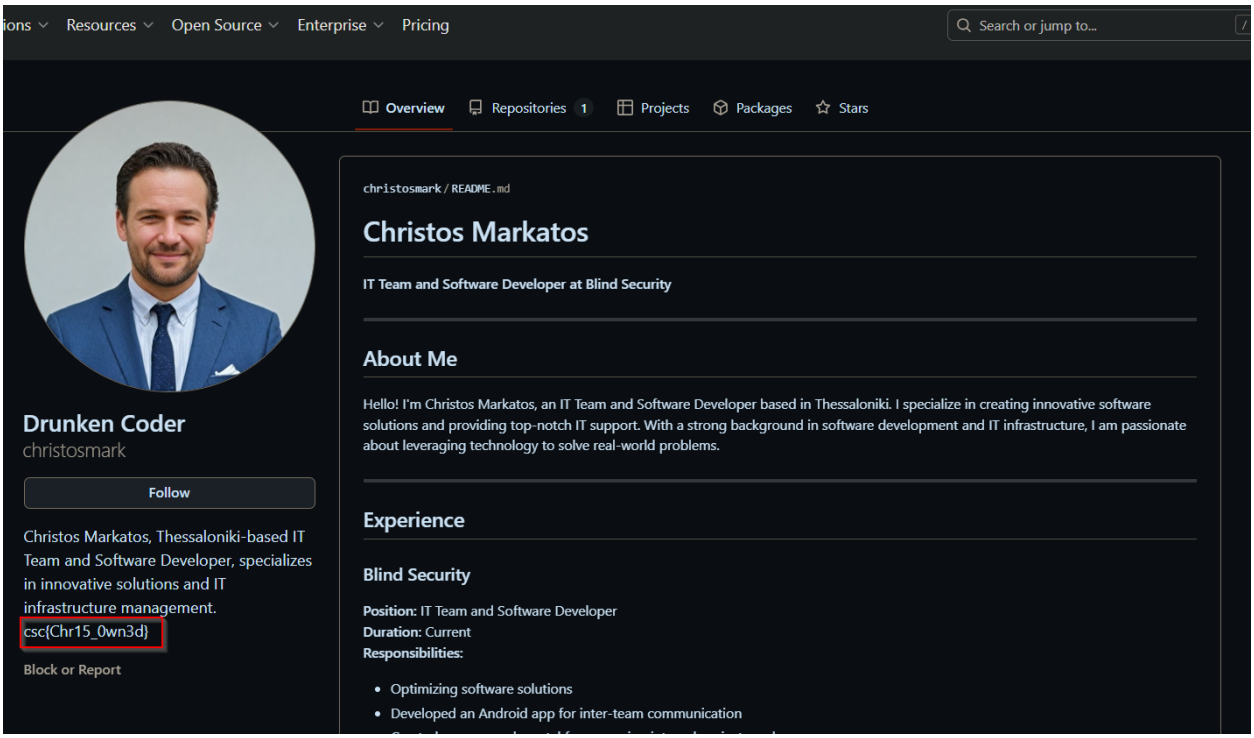


We see that he doesn't seem to have most things and what shows up is invalid, so maybe he didn't reuse his username exactly as it was. (Green (Available) means that the username is available for use – not currently in use; and red (Unavailable) means that the username is not available for use – currently in use.)

Let's try christosmark without the 78.



We notice that among a couple others, GitHub is also red now. Maybe that's it?



Yep that's it. (*Answer to Christos Markatos Social 2)

For the Social Engineering for Katerina you can use any type of information you'd like to create a believable phishing email. Just don't use random pretexts and make sure your pretext doesn't include absolutely everything as it might raise suspicion. There is a fine line of enough pretext and too much pretext. Additionally, try to utilize some psychological principles such as Scarcity, Urgency and Authority to create stress/belief to the victim, but make sure you do not overdo it that it screams "I'm trying to scam you". A perfect example can be found at the end of this writeup by BitMasters. (*Expectations for Social Engineering)

Software Versions

Question: Which type and version of database does Blind Security use?

Answer: MSSQL 11.0

Explanation: As explained above.

Katerina Morfaki

Question: Explore Katerina's social media and find the flag.
Answer: csc{R34dy_play3r_0n3}

Explanation: As explained above.

Christos Markatos Personal Page

Question: Find Christos' personal webpage.

Answer: csc{Y0u_F0unD_m3_0SIN7_M4st4R}

Explanation: As explained above.

Christos Markatos Social 1

Question: Look for Christos' first social media account.

Answer: csc{p0st3r_X}

Explanation: As explained above.

Christos Markatos Social 2

Question: Find Christos' second account.

Answer: csc{Chr15_0wn3d}

Explanation: As explained above.

Katerina’s Hotel

Question: On which hotel did Katerina stay for her security related trip?
Answer: Numa Rome Barberini

Explanation: As explained above.

Katerina’s Event

Question: Which security related event did Katerina participate in last year?

Answer: BSides Roma

Explanation: As explained above.

Artifacts

Question: Can you spot any interesting artifacts on her trip's post?

Answer: csc{p0s7_1t_n0w}

Explanation: As explained above.

Katerina’s Email

Question: What's Katerina's personal email?

Answer: katemurphy19946@gmail.com

Explanation: As explained above.

Social Engineering

Question: Try to trick Katerina into clicking a phishing email in her personal email. Use all the information you gathered so far from her social media profile to create a unique and believable phishing email. All email submissions will be verified manually so do your best to get the flag! :)

(Nigerian Prince attempts will be rejected)

Team's Best Response: BitMasters

Answer: **Subject**: 🏂 Confirmation Needed: Exclusive Ski Trip to the Alps – Limited Spots!

Body:

Hi Katerina,

We're reaching out because you're on the priority list for our Winter

Escape Ski Package in the Swiss Alps next month! As a past traveler (or

based on your interest in our partner resorts), we're offering you first

access to our last-minute openings for the April 10–17 trip.

Your selected preferences:

1. Luxury chalet accommodation (private hot tub!)
2. Off-piste guided tours
3. 10% loyalty discount

Act fast—only 3 spots remain!

To secure your place or adjust your booking, click here:

👉 Review Your Reservation

Note: This link expires in 24 hours. If you no longer wish to receive

offers, [unsubscribe here].

Cheers,

Sophie Laurent

Customer Experience Manager

Alpine Escape Getaways

📞 +41 22 345 6789 (9am–5pm CET)

P.S. Weather forecasts predict fresh powder all week—check the [trail conditions]!