POLITECHNIKA WROCŁAWSKA  Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30

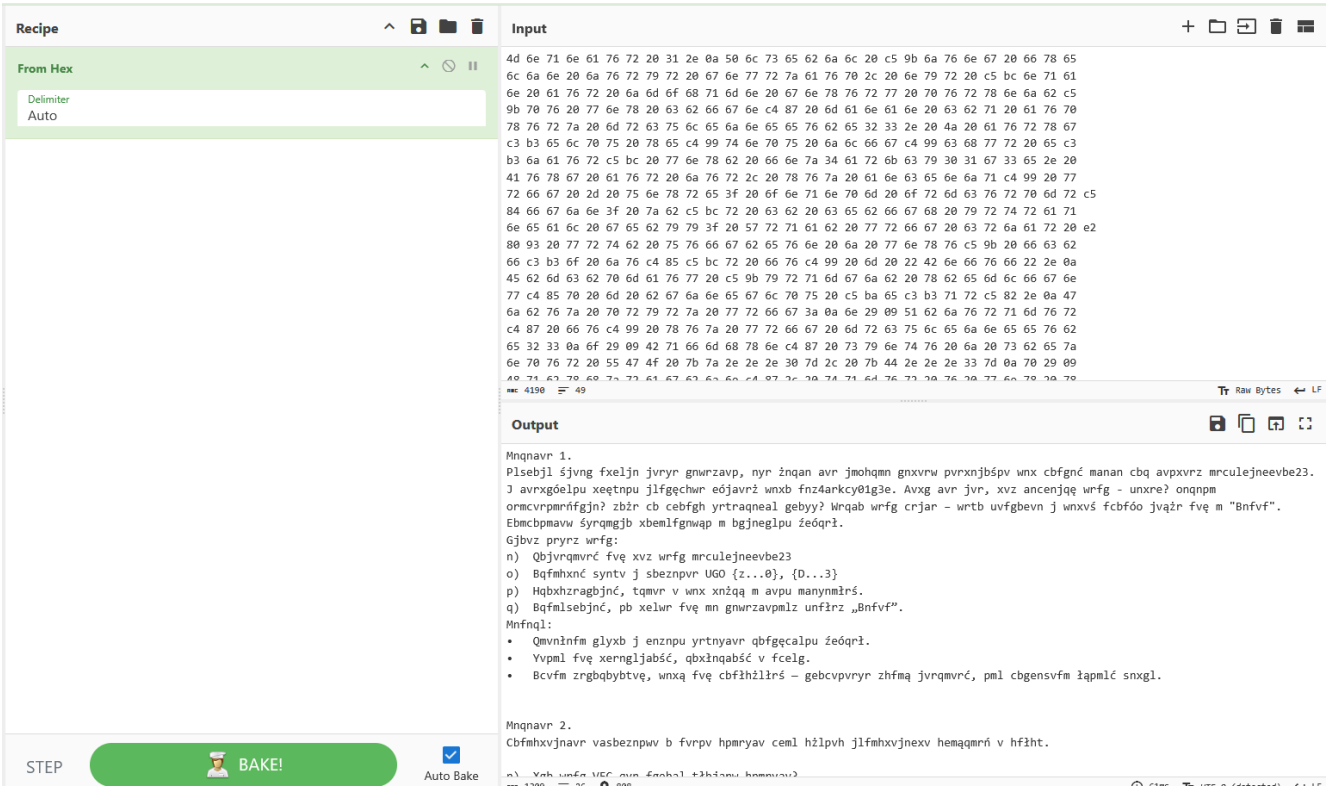
CBESI0053G Informatyka śledcza – Laboratorium 6

Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 07.04.2025	
Data oddania sprawozdania: 13.04.2025	

1. Cel ćwiczenia

Wyszukiwanie informacji na temat użytkowników i urządzeń sieciowych za pomocą ogólnodostępnych narzędzi pasywnych.

2. Odszyfrowanie instrukcji laboratoryjnej



Rysunek 1: odkodowanie z formatu hex; narzędzie CyberChef

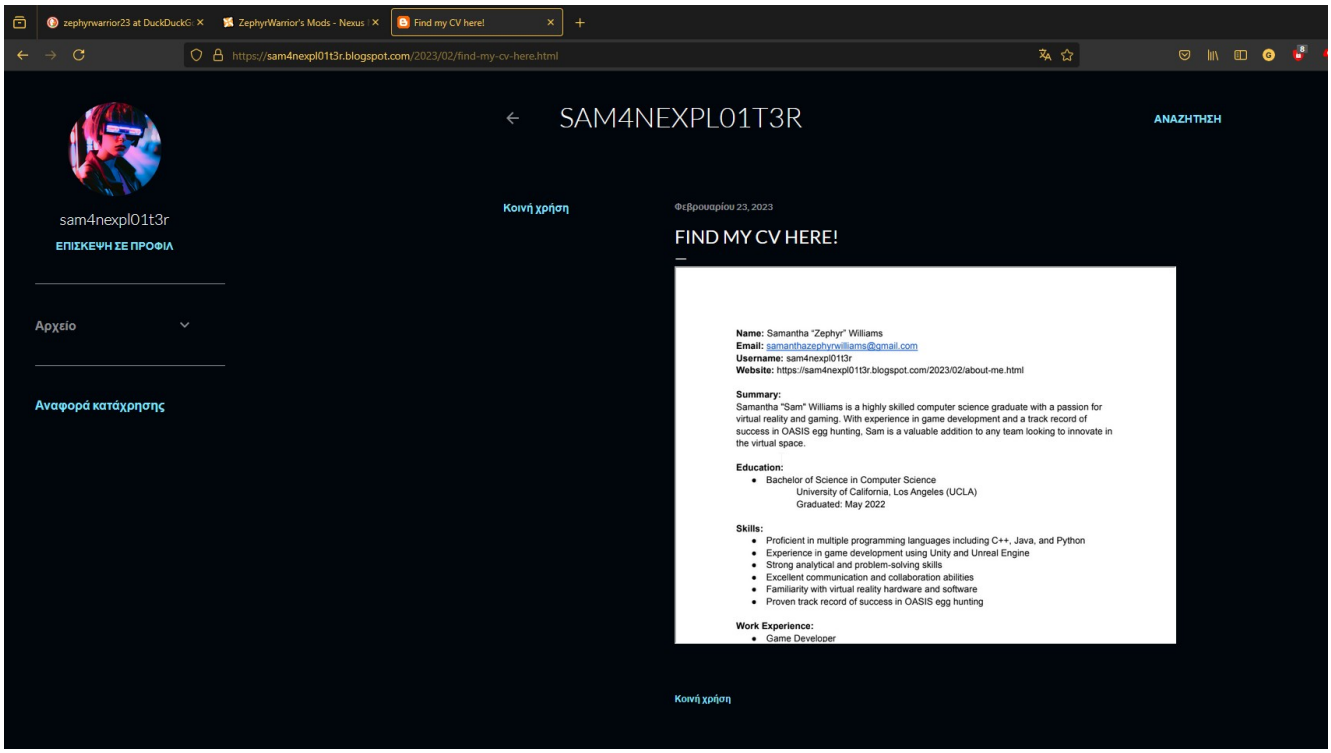
Rysunek 2: rozszyfrowanie szyfrem cezara; skalkuluj.pl

```
Zadanie 1.
Cyfrowy świat skrywa wiele tajemnic, ale żadna nie wzbudza takiej ciekawości jak postać znana pod nickiem zephyrwarrior23. W niektórych
kręgach występuje również jako sam4nexpl01t3r. Nikt nie wie, kim naprawdę jest - haker? badacz bezpieczeństwa? może po prostu legendarny
troll? Jedno jest pewne – jego historia w jakiś sposób wiąże się z "Oasis".
Rozpocznij śledztwo korzystając z otwartych źródeł.
Twoim celem jest:
a)      Dowiedzieć się kim jest zephyrwarrior23
b)      Odszukać flagi w formacie HTB {m...0}, {Q...3}
c)      Udokumentować, gdzie i jak każdą z nich znalazłeś.
d)      Odszyfrować, co kryje się za tajemniczym hasłem „Oasis”.
Zasady:
•       Działasz tylko w ramach legalnie dostępnych źródeł.
•       Liczy się kreatywność, dokładność i spryt.
•       Opisz metodologię, jaką się posłużyłeś – tropiciele muszą wiedzieć, czy potrafisz łączyć fakty.


Zadanie 2.
Poszukiwanie informacji o sieci uczelni przy użyciu wyszukiwarki urządzeń i usług.

a)      Kto jest ISP dla strony głownej uczelni?
b)      Jakie oprogramowanie serwerowe jest najczęściej występujące na PWR?
c)      Jaka najstarsza wersja oprogramowania serwerowego jest wciąż używana? Czy ma jakieś krytyczne podatności?
d)      Znajdz adres IP serwera gry.
e)      *Znajdź adresy IP konsol do gier podpiętych do sieci uczelni.


W zadaniach używamy tylko narzędzi pasywnych!
```

Rysunek 3: jawna treść instrukcji

3. Realizacja zadań laboratoryjnych

Zadanie 1. *Cyfrowy świat skrywa wiele tajemnic, ale żadna nie wzbudza takiej ciekawości jak postać znana pod nickiem zephyrwarrior23. W niektórych kręgach występuje również jako sam4nexpl01t3r. Nikt nie wie, kim naprawdę jest - haker? badacz bezpieczeństwa? może po prostu legendarny troll? Jedno jest pewne – jego historia w jakiś sposób wiąże się z "Oasis".*
Rozpocznij śledztwo korzystając z otwartych źródeł.
Twoim celem jest:
a) Dowiedzieć się kim jest zephyrwarrior23



Rysunek 4: CV badanej osoby; sam4nexpl01t3r.blogspot.com

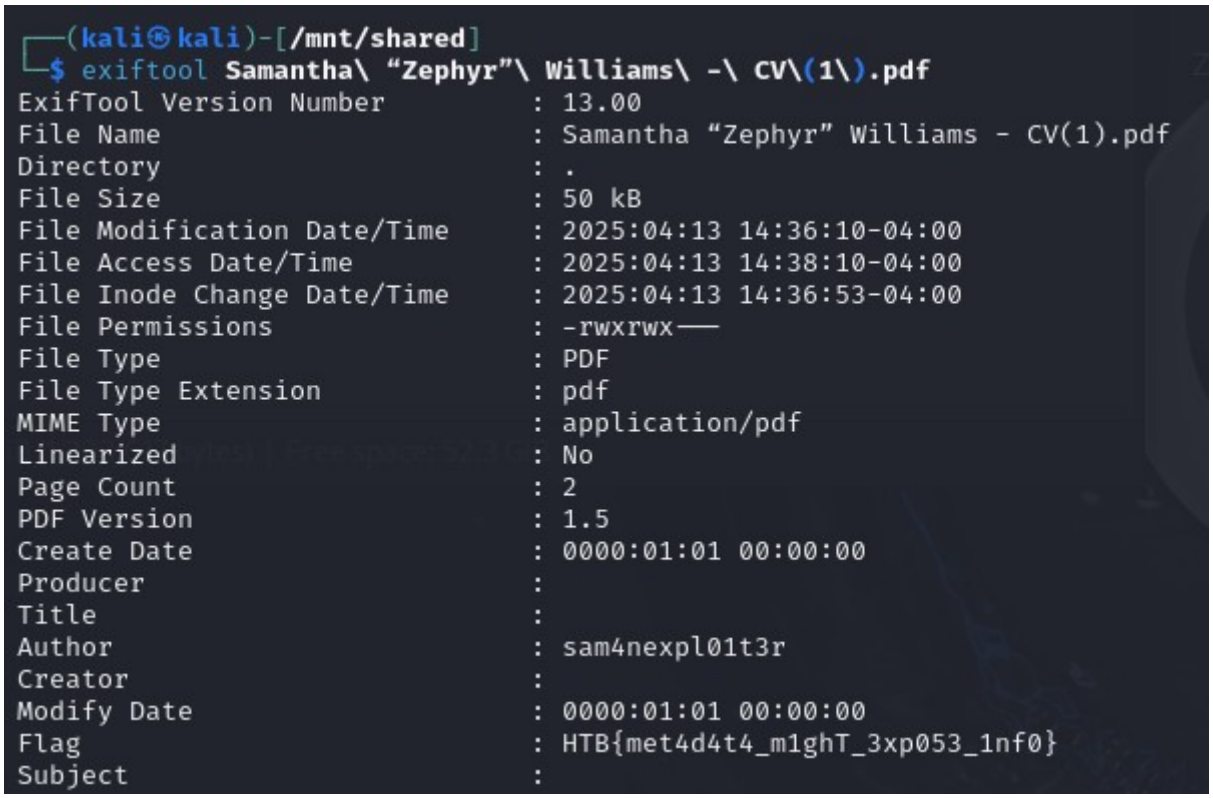
Z dokumentu można odczytać:
Name: Samantha “Zephyr” Williams

Email: samanthazephyrwilliams@gmail.com
Username: sam4nexpl01t3r

Tłumaczenie podsumowania: *Samantha „Sam” Williams jest wysoko wykwalifikowaną absolwentką informatyki, pasjonującą się rzeczywistością wirtualną i grami. Mając doświadczenie w tworzeniu gier i historię sukcesów w polowaniu na jajka OASIS, Sam jest cennym uzupełnieniem każdego zespołu, który chce wprowadzać innowacje w przestrzeni wirtualnej.*

b) Odszukać flagi w formacie HTB {m...0}, {Q...3}

Badając plik CV narzędziami do szczegółowej analizy plików znaleźć można:

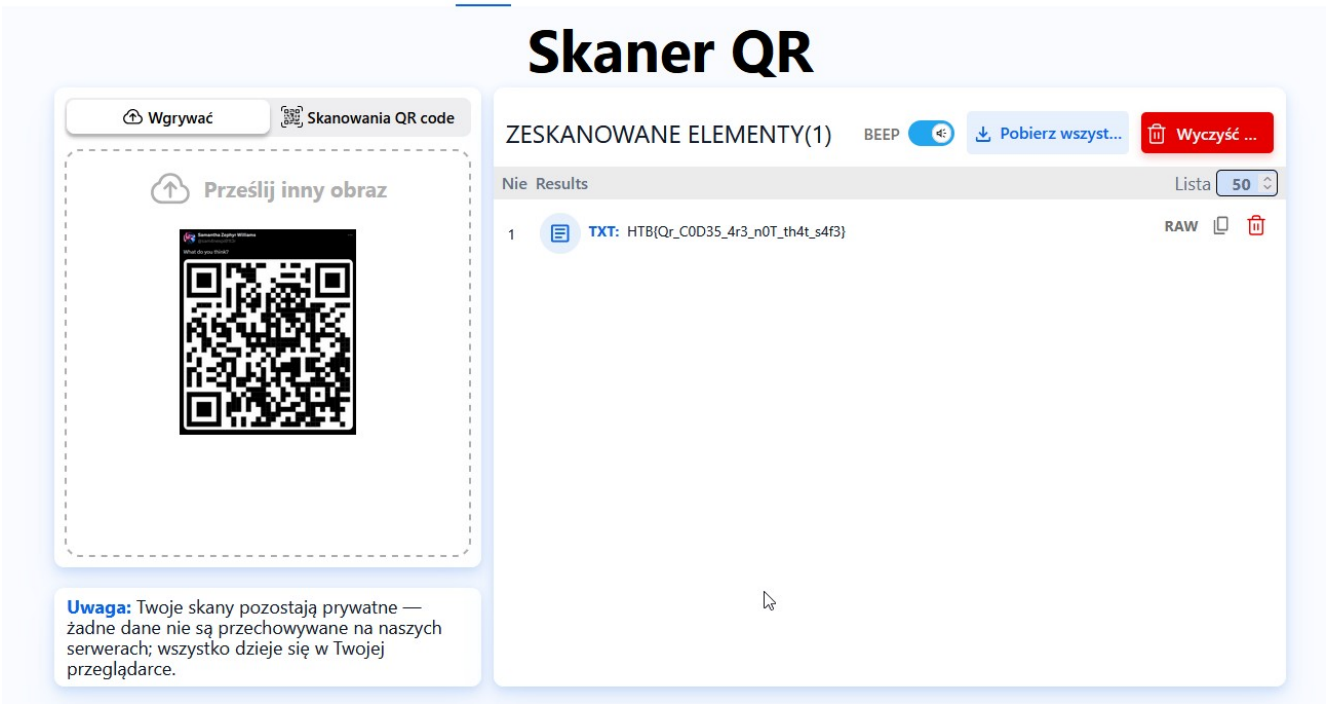


Rysunek 5: analiza CV narzędziem exiftool

Flaga: HTB{met4d4t4_m1ghT_3xp053_1nf0}

Wchodząc na profil użytkownika *sam4nexpl01t3r* na platformie „X” znaleźć można:

Rysunek 6: kod QR z profilu „X” użytkownika



Rysunek 7: odkodowanie kodu QR; https://qrscanner.net/pl

Flaga: HTB{Qr_C0D35_4r3_n0T_th4t_s4f3}

c) Udokumentować, gdzie i jak każdą z nich znalazłeś.

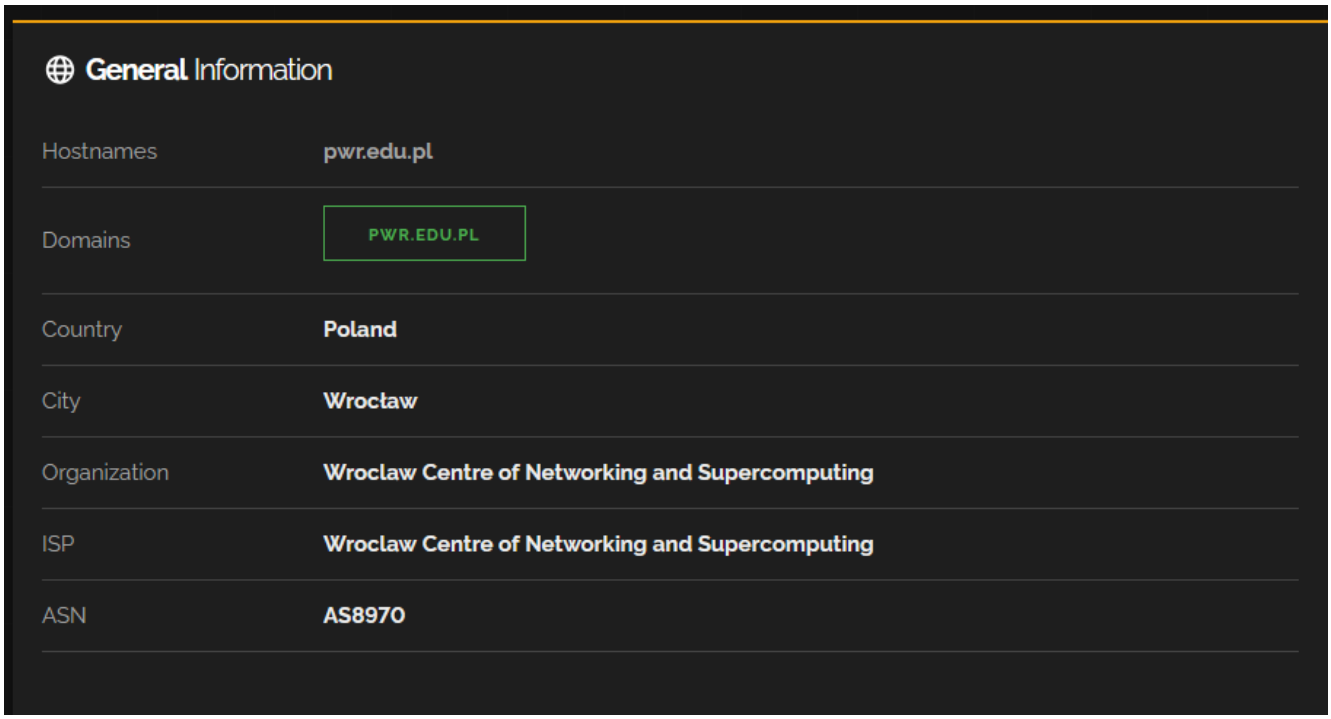
Obie strony na których znalazłem flagi są jedne z pierwszych, które pojawiają się po wpisaniu nazwy użytkownika w wyszukiwarkę. Przedmiot „Informatyka Śledcza” zobowiązuje do analizy plików odpowiednimi narzędziami, stąd znalezienie pierwszej flagi, druga nie była schowana szczególnie głęboko.

d) Odszyfrować, co kryje się za tajemniczym hasłem „Oasis”.

Według https://github.com/supermedium/gunters-of-oasis OASIS to akronim od: *Open and Super Immersive Simulation*

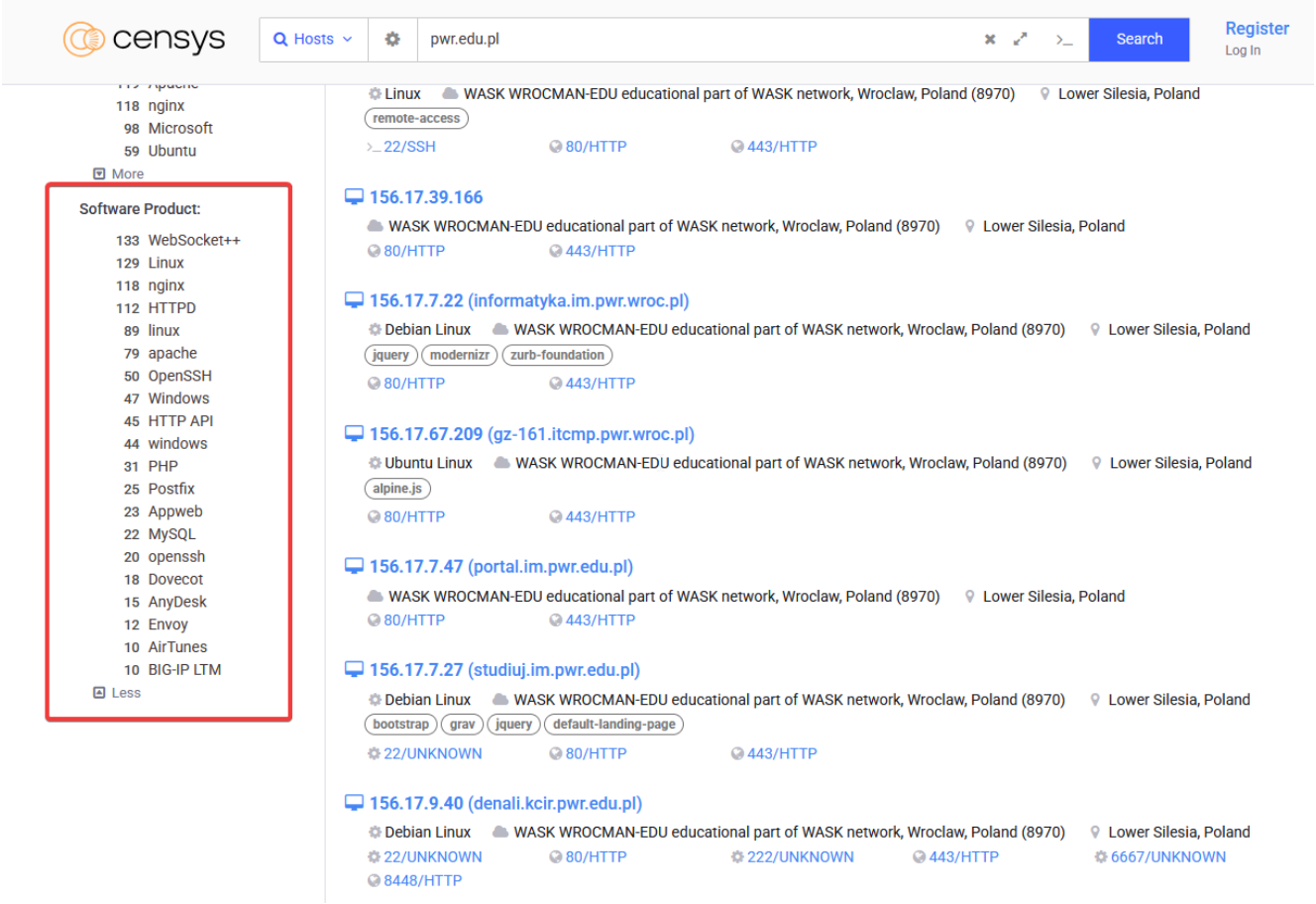
Zadanie 2. *Poszukiwanie informacji o sieci uczelni przy użyciu wyszukiwarki urządzeń i usług.*

a) Kto jest ISP dla strony głownej uczelni?



Rysunek 8: ISP - Wroclaw Centre of Networking and Supercomputing; shodan.io

b) Jakie oprogramowanie serwerowe jest najczęściej występujące na PWR?



Rysunek 9: WebSocket++; censys.io

c) Jaka najstarsza wersja oprogramowania serwerowego jest wciąż używana? Czy ma jakieś krytyczne podatności?

Najstarszą wersję jaką znalazłem to: WebSocket++ 0.8.1. Według security.snyk.io ta wersja jest narażona między innymi na ataki DoS, zalecane jest przejście do najnowszej wersji.

d) Znajdz adres IP serwera gry.

Nie udało mi się znaleźć takiego serwera, najpewniej jest to któreś urządzenie z podsieci: podsieci 156.17.228.0/24