
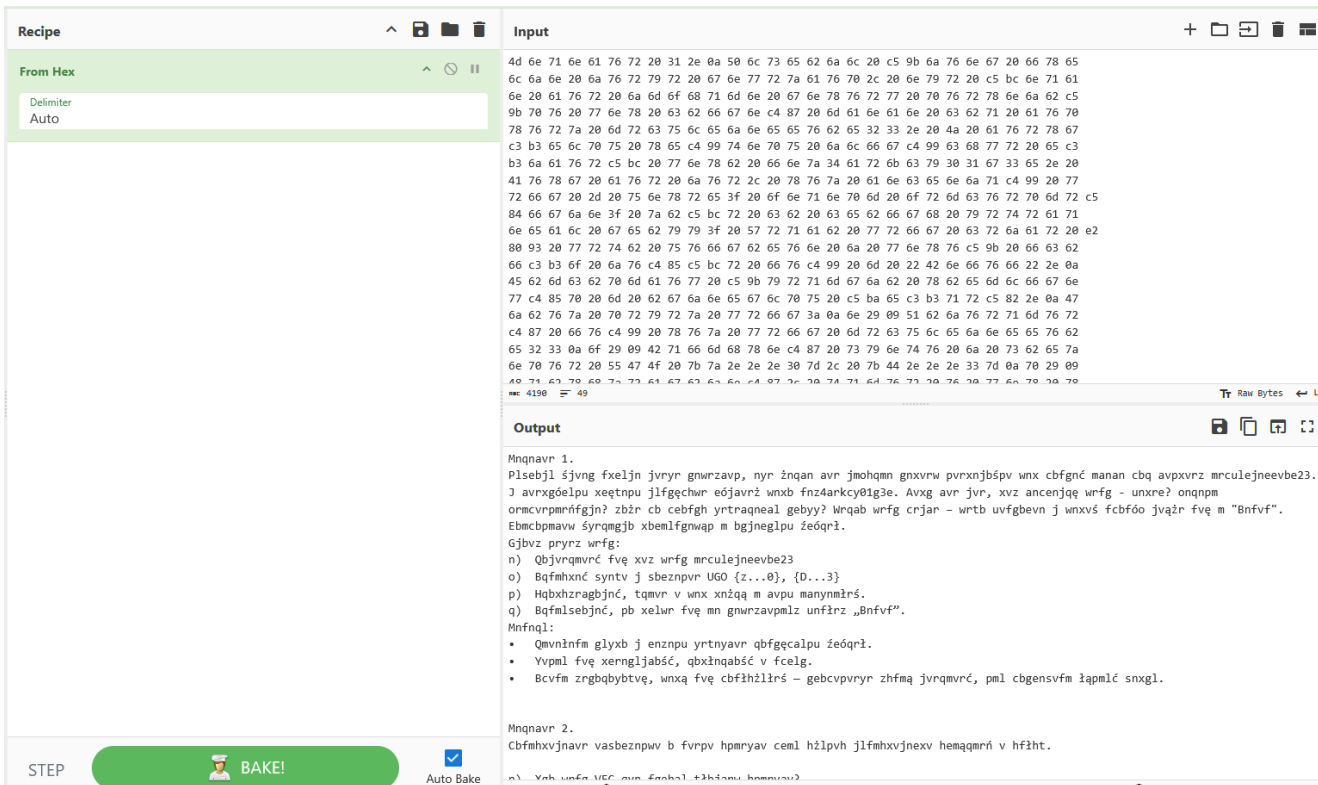


<p>POLITECHNIKA WROCŁAWSKA</p>  <p>Wydział Informatyki i Telekomunikacji</p>	<p>Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30</p>
<p align="center">CBESI0053G Informatyka śledcza – Laboratorium 6</p>	
<p>Prowadzący: mgr inż. Adrian Florek</p> <p>Data wykonania ćwiczenia: 07.04.2025</p> <p>Data oddania sprawozdania: 13.04.2025</p>	<p>Autor: 1. Gerard Błaszczuk</p>

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

Szyfr Cezara - koder/dekoder online

Zakoduj lub rozkoduj wiadomość Szyfrem Cezara w zależności od wybranego przesunięcia.

Przesunięcie:

13

Tekst:

Mnqnavr 1.

Plsebjl śjvng fxeljn jvryr gnwrzavp, nyr źnqan
avr jmoħqmn gnxvrw pvrxnjbśpv wnx cbfgńć
manan cbq avpxvrz mrculejneevbe23. J
avrxgóelpu xeętnpu jlfgęchwreójavrz wnxb
fnz4arkcy01q3e. Avxq avr jvr, xvz ancenjqę

Szyfr Cezara:

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

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:

- Dowiedzieć się kim jest zephyrwarrior23
- Odszukać flagi w formacie HTB {m...0}, {0...3}
- Udokumentować, gdzie i jak każdą z nich znalazłeś.
- 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.

- Kto jest ISP dla strony głównej uczelni?
- Jakie oprogramowanie serwerowe jest najczęściej występujące na PWR?
- Jaka najstarsza wersja oprogramowania serwerowego jest wciąż używana? Czy ma jakieś krytyczne podatności?
- Znajdź adres IP serwera gry.
- *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**

The screenshot shows a web browser with the address bar displaying `http://sam4nexpl01t3r.blogspot.com/2023/02/find-my-cv-here.html`. The page features a dark theme and a sidebar on the left with the user's profile picture and name 'sam4nexpl01t3r'. The main content area is titled 'FIND MY CV HERE!' and contains a resume for Samantha 'Zephyr' Williams. The resume includes contact information, a summary, education details (Bachelor of Science in Computer Science from UCLA), skills (C++, Java, Python, game development), and work experience (Game Developer).

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:

```
(kali㉿kali)-[/mnt/shared]
$ exiftool Samantha\ "Zephyr"\ Williams\ -\ CV\ (1\).pdf
ExifTool Version Number      : 13.00
File Name                    : Samantha "Zephyr" Williams - CV(1).pdf
Directory                   : .
File Size                    : 50 kB
File Modification Date/Time  : 2025:04:13 14:36:10-04:00
File Access Date/Time       : 2025:04:13 14:38:10-04:00
File Inode Change Date/Time  : 2025:04:13 14:36:53-04:00
File Permissions             : -rwxrwx---
File Type                   : PDF
File Type Extension         : pdf
MIME Type                   : application/pdf
Linearized                  : No
Page Count                  : 2
PDF Version                 : 1.5
Create Date                 : 0000:01:01 00:00:00
Producer                   :
Title                      :
Author                     : sam4nexpl01t3r
Creator                    :
Modify Date                 : 0000:01:01 00:00:00
Flag                       : HTB{met4d4t4_m1ghT_3xp053_1nf0}
Subject                    :
```

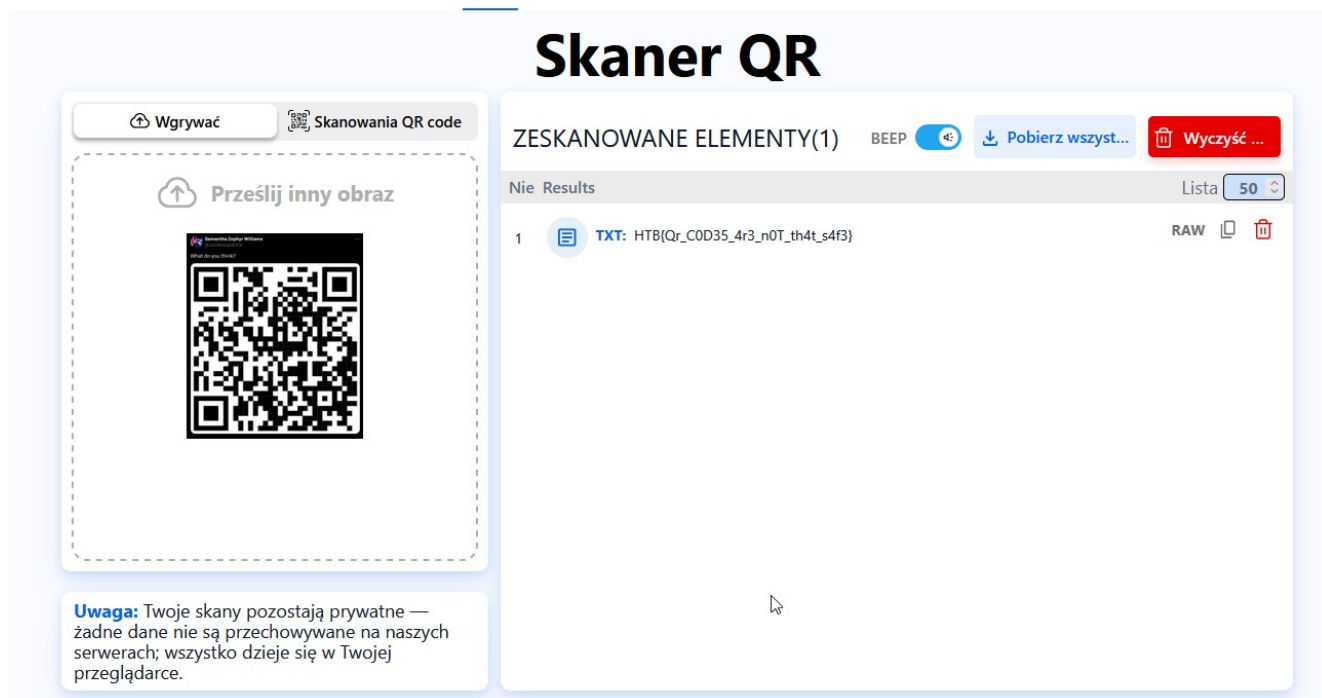
Rysunek 5: analiza CV narzędziem exiftool

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.**

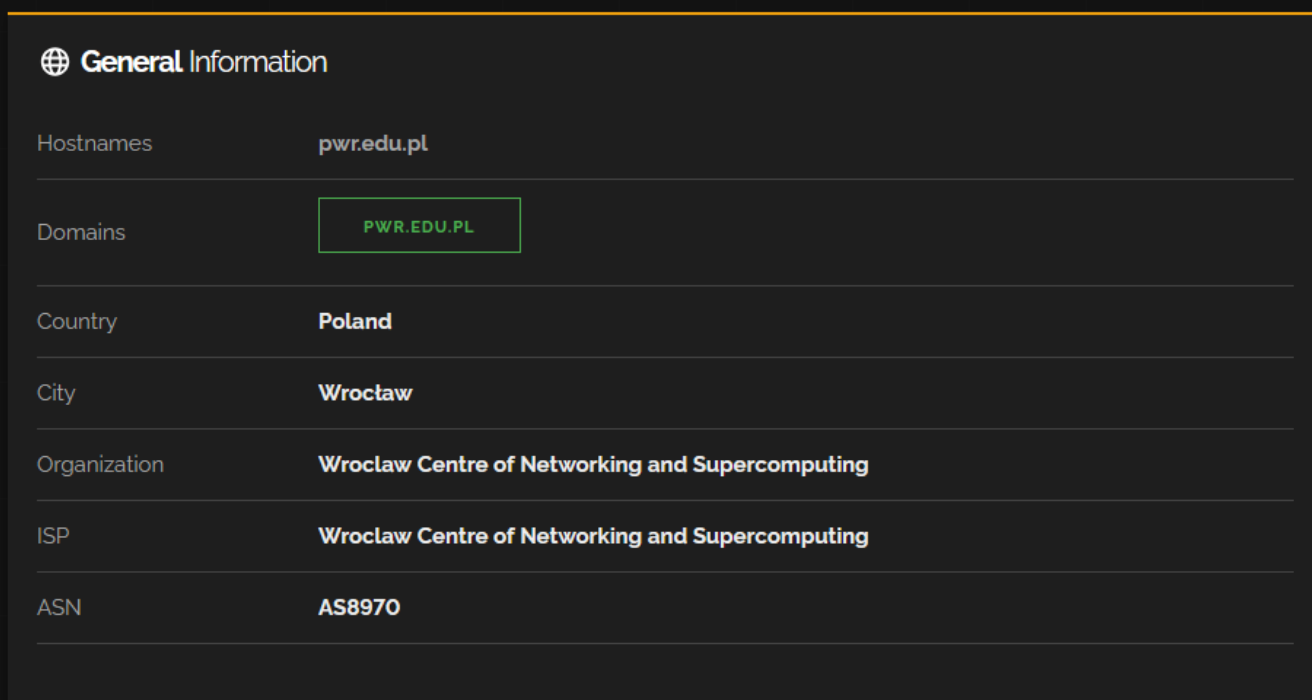
Obie strony na których znalazłem flagi są jedne z pierwszych, które pojawiają się po wpisaniu nazwy użytkownika w wyszukiwarkę. Przedmiot „Informatyka Śledcza” zobowiązuje do analizy plików odpowiednimi narzędziami, stąd znalezienie pierwszej flagi, druga nie była schowana szczególnie głęboko.

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 głównej uczelni?**



General Information	
Hostnames	pwr.edu.pl
Domains	PWR.EDU.PL
Country	Poland
City	Wrocław
Organization	Wrocław Centre of Networking and Supercomputing
ISP	Wrocław Centre of Networking and Supercomputing
ASN	AS8970

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

b) **Jakie oprogramowanie serwerowe jest najczęściej występujące na PWR?**

The screenshot shows the Censys search interface. On the left, a sidebar lists software products, with 'WebSocket++' at the top. The main area displays search results for the domain pwr.edu.pl. The results are organized by IP address, showing the operating system (e.g., Linux, Ubuntu) and the software products installed on the server. The results include:

- 156.17.39.166: WASK WROCMAN-EDU educational part of WASK network, Wroclaw, Poland (8970). Software products: remote-access, 22/SSH, 80/HTTP, 443/HTTP.
- 156.17.7.22 (informatyka.im.pwr.wroc.pl): Debian Linux, WASK WROCMAN-EDU educational part of WASK network, Wroclaw, Poland (8970). Software products: jquery, modernizr, zurb-foundation, 80/HTTP, 443/HTTP.
- 156.17.67.209 (gz-161.itcmp.pwr.wroc.pl): Ubuntu Linux, WASK WROCMAN-EDU educational part of WASK network, Wroclaw, Poland (8970). Software products: alpine.js, 80/HTTP, 443/HTTP.
- 156.17.7.47 (portal.im.pwr.edu.pl): WASK WROCMAN-EDU educational part of WASK network, Wroclaw, Poland (8970). Software products: 80/HTTP, 443/HTTP.
- 156.17.7.27 (studiuj.im.pwr.edu.pl): Debian Linux, WASK WROCMAN-EDU educational part of WASK network, Wroclaw, Poland (8970). Software products: bootstrap, grav, jquery, default-landing-page, 22/UNKNOWN, 80/HTTP, 443/HTTP.
- 156.17.9.40 (denali.kcir.pwr.edu.pl): Debian Linux, WASK WROCMAN-EDU educational part of WASK network, Wroclaw, Poland (8970). Software products: 22/UNKNOWN, 80/HTTP, 222/UNKNOWN, 443/HTTP, 6667/UNKNOWN, 8448/HTTP.

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) Znajdź adres IP serwera gry.

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