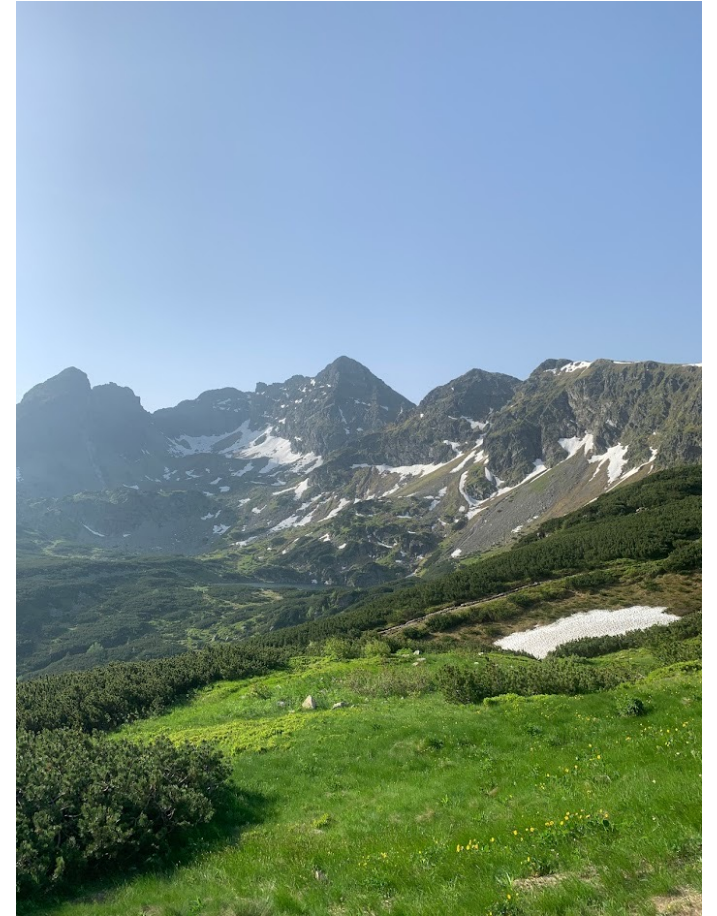


Szukanie dziur w całym, czyli o pentestach słów kilka

Krystian Powójski, Equinix

§ BIO

- Inżynier ds. bezpieczeństwa aplikacji w Equinix
- Absolwent PW
- Lubię góry i amatorsko gram w squash



§ Intro



Źródło: <https://www.theguardian.com/>

§ Pentesty – ale po co to komu?

- Znajdujemy błędy ktoś zacznie je wykorzystywać



Źródło: <https://www.britishairways.com/>



Źródło: <https://www.bloomberg.com/>



§ Pentesty – ale po co to komu?

- Testy bezpieczeństwa wykonujemy w ‘kontrolowanych’ warunkach



§ Whitebox vs Blackbox

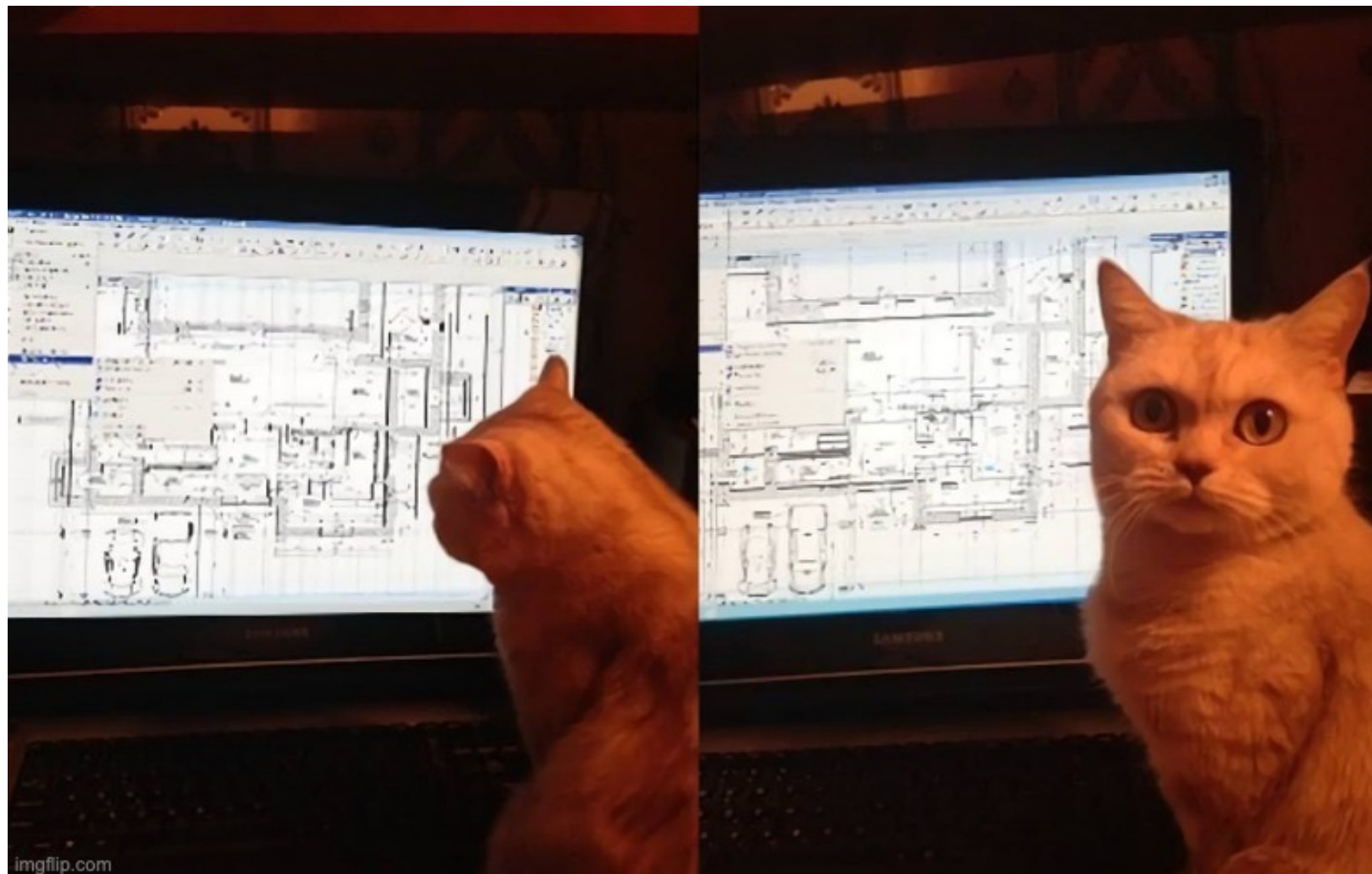


V S



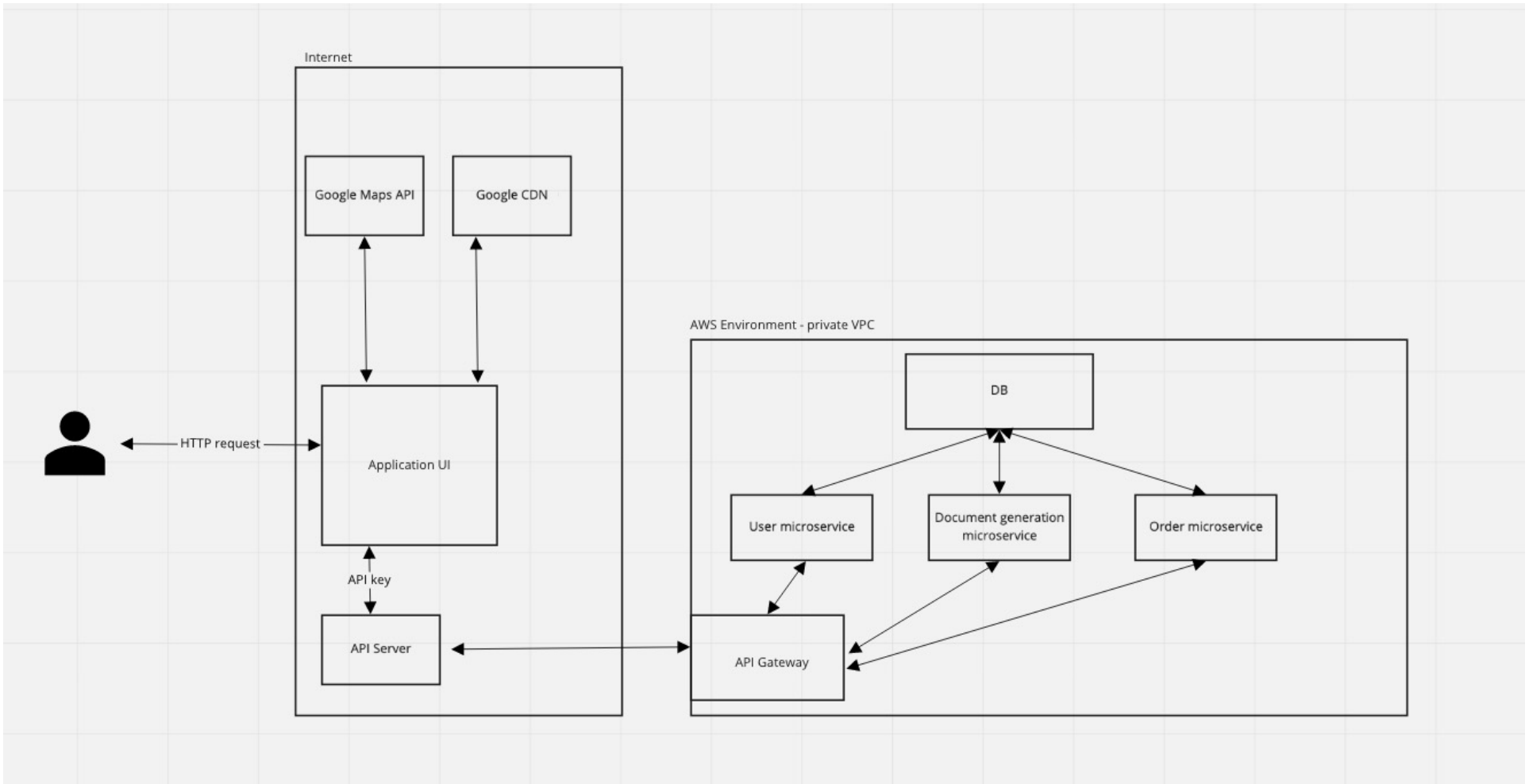
Źródło: <https://cdn.educba.com/>

§ Krok 1 - Analiza architektury



Źródło: <https://imgur.com>

§ Krok 1 - Analiza architektury



§ Krok 2 - Pentest

DEMO #1

§ Krok 2 - Pentest

DEMO #2

§ Krok 3 - Raportowanie



Źródło: <https://media.thegospelcoalition.org/>



EQUINIX

§ Krok 3 - Raportowanie

- Przykładowe raporty z testów bezpieczeństwa:
 - <https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>
 - <https://cdn.sekurak.pl/eventory-sample-pentest-report.pdf>
 - <https://protonmail.com/blog/wp-content/uploads/2021/07/securitum-protonmail-security-audit.pdf>
 - <https://github.com/juliocesarfort/public-pentesting-reports>
 - <https://hackerone.com/hacktivity>



§ Krok 4 - Retesty



Źródło: <https://imgur.com>

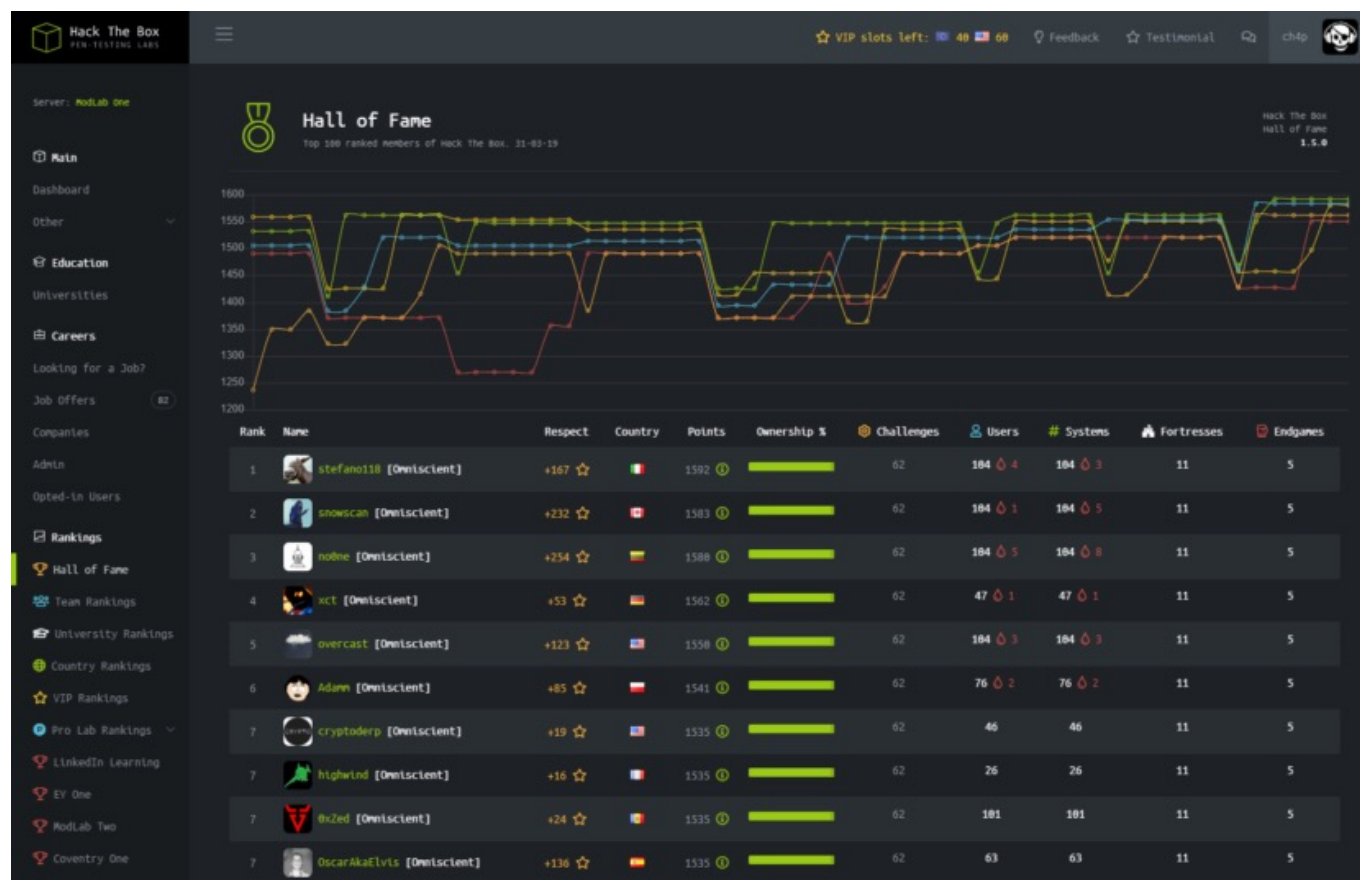
§ Skąd brać wiedzę?

- OWASP – <https://owasp.org/Top10/>
- Dokumentacja Mozilla MDN - <https://developer.mozilla.org/pl/>
- Portswigger Web Security Academy - <https://portswigger.net/web-security/dashboard>
- Dokumentacja RFC
- Twitter
-



§ Skąd brać wiedzę?

HackTheBox - <https://www.hackthebox.com/>



§ Skąd brać wiedzę – polecane książki

- Splątana sieć - Michał Zalewski (<https://www.amazon.pl/Tangled-Web-Securing-Modern-Applications/dp/1593273886/>)
- Web Application Hacker's Handbook – D. Stuttard & M. Pinto = (<https://www.amazon.pl/Web-Application-Hackers-Handbook-Discovering/dp/1118026470/>)
- Bezpieczeństwo Aplikacji Webowych – książka Sekurak'a (<https://sklep.sekurak.pl/product/view?id=1>)



§ Skąd brać wiedzę – programy Bug bounty

hackerone



bugcrowd



§ Pytania



EQUINIX

§ Źródła

Prezentacja oraz źródła https://github.com/kpoow/knbi_presentation