Sprawozdanie

Temat pracy: **REKONESANS PASYWNY WZGLĘDEM DOMENY FACEIT.COM**

xxx

.....

(kierunek studiów)

xxx

.....

(przedmiot)

Student:

Hubert Makowski

Prowadzący zajęcia:

xxx

Warszawa 2024

Spis treści

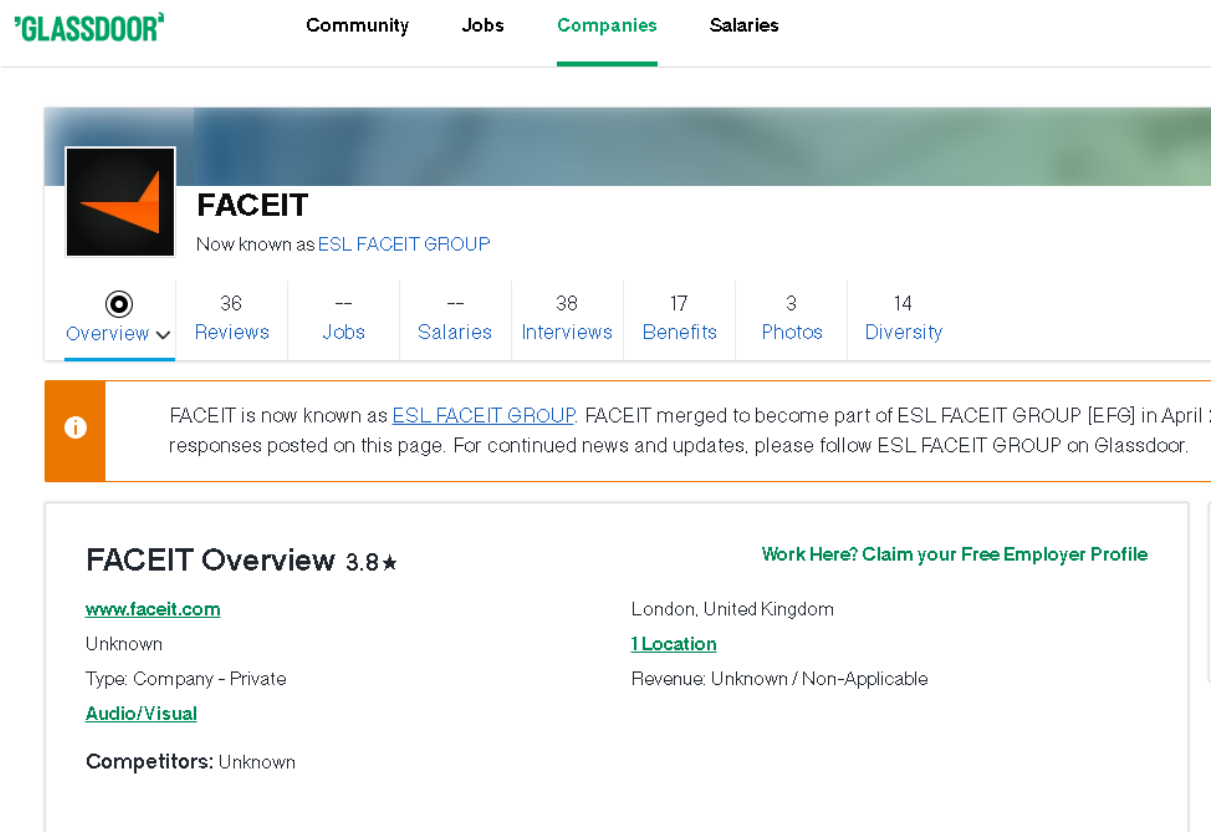
Uzasadnienie wyboru domeny 4
Dane ogólne dotyczące organizacji będącej właścicielem domeny 4
Serwery DNS obsługujące domenę 2
Ogólne dane dotyczące witryny domeny..... 32
Struktura domeny 41
Wykorzystywane systemy operacyjne, usługi sieciowe i aplikacje realizujące te usługi 52
Wykorzystywane technologie informatyczne 60
Pracownicy i osoby powiązane 105
Bezpieczeństwo 132
Stosowane urządzenia sieciowe..... 164
Inne rodzaje uzyskanych danych..... 167
Wnioski ogólne..... 176

1. Uzasadnienie wyboru domeny

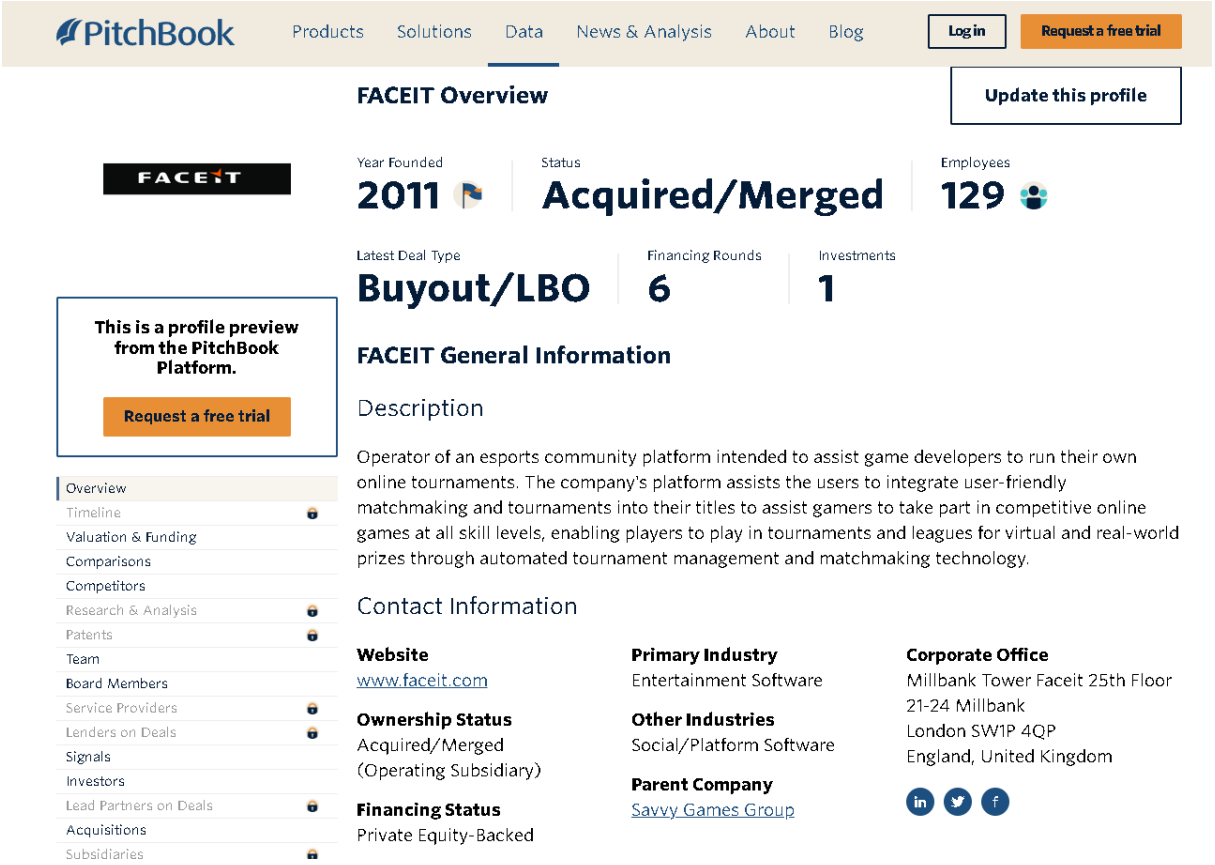
Zdecydowałem się na wybór domeny faceit.com, ponieważ w przeszłości korzystałem regularnie z usług domeny. Kilka lat temu dowiedziałem się o wycieku haseł z domeny faceit.com (menadżer haseł google), co wzbudziło moje zainteresowanie domeną i jej zabezpieczeniami.

2. Dane ogólne dotyczące organizacji będącej właścicielem domeny

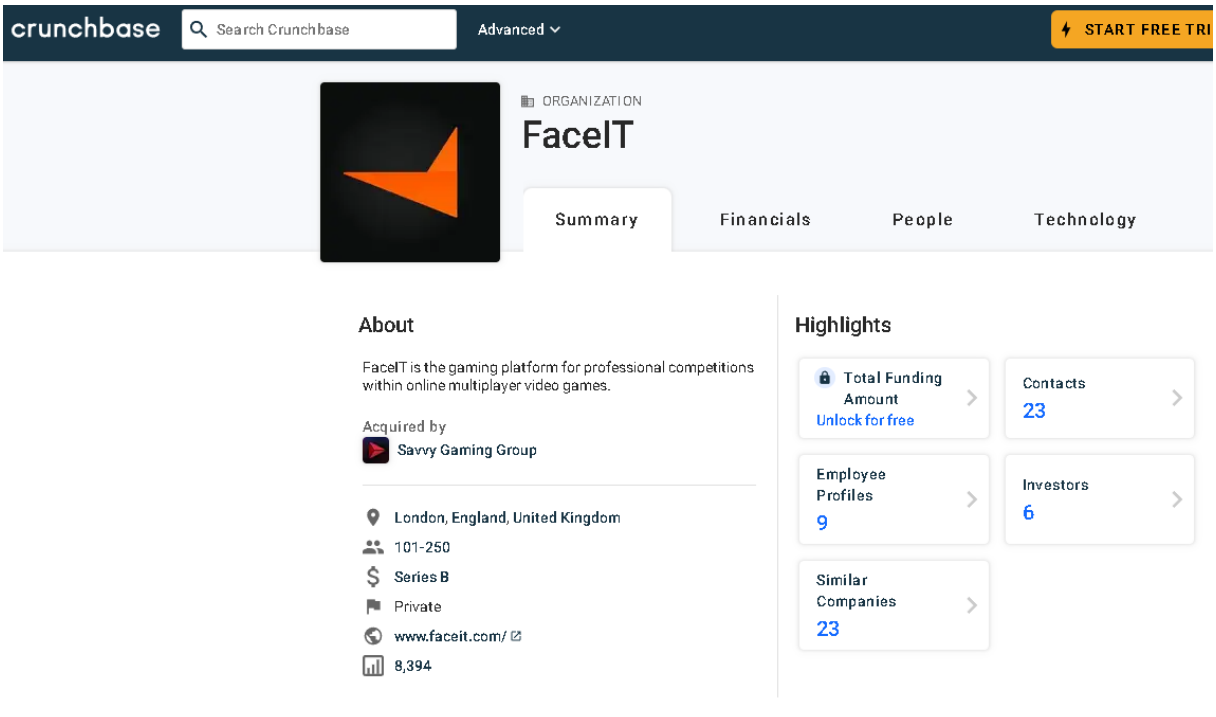
Organizacja Faceit jest właścicielem domeny faceit.com. Organizacja zajmuje się produkcją oprogramowania służącego do rozrywki online (głównie turnieje), a także produkcją wideo. Firma została założona w Londynie w 2011 roku. Organizacja ma swoją siedzibę w Milibank, Londyn, co widać na obrazach 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6.



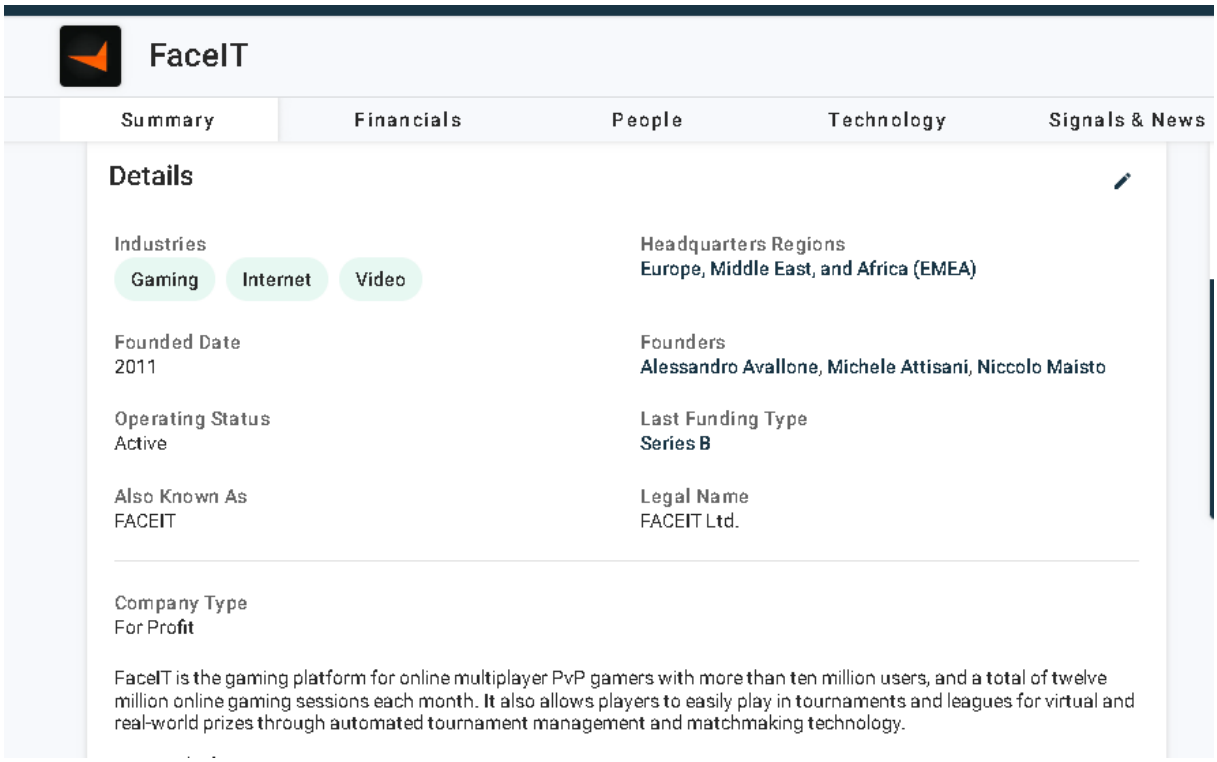
Obraz 2.1.1 ogólny zarys firmy Faceit, źródło glassdoor.co.uk, data wykonania zrzutu 10.01.2024 r.



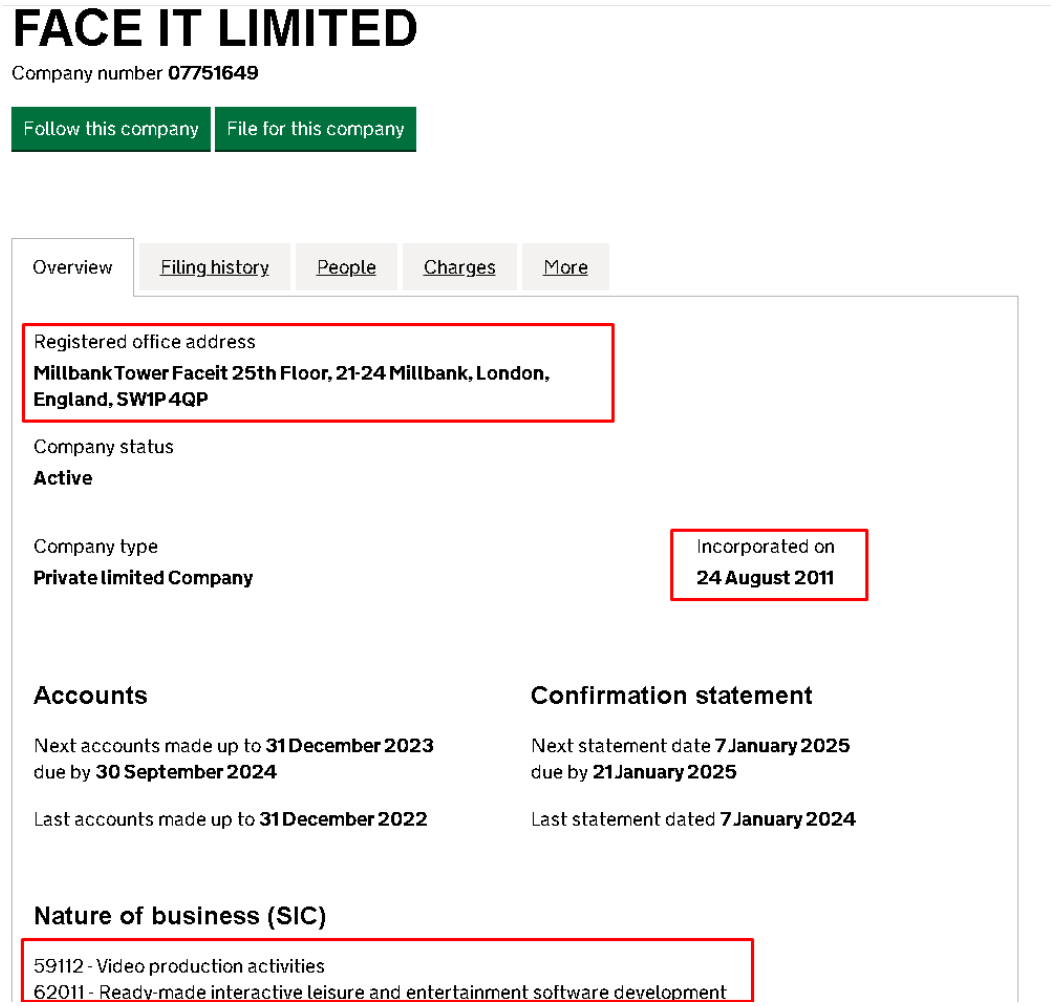
Obraz 2.1.2 ogólne dane na firmy Faceit, źródło pitchbook.com, data wykonania zrzutu 10.01.2024 r.



Obraz 2.1.3 ogólny zarys firmy Faceit, źródło crunchbase.com, data wykonania zrzutu 10.01.2024 r.



Obraz 2.1.4 ogólny zarys firmy Faceit, źródło crunchbase.com, data wykonania zrzutu 10.01.2024 r.



FACE IT LIMITED

Company number **07751649**

Follow this company | File for this company

Overview | Filing history | People | Charges | More

Registered office address
Millbank Tower Faceit 25th Floor, 21-24 Millbank, London, England, SW1P 4QP

Company status
Active

Company type
Private limited Company

Incorporated on
24 August 2011

Accounts

Next accounts made up to **31 December 2023**
due by **30 September 2024**

Last accounts made up to **31 December 2022**

Confirmation statement

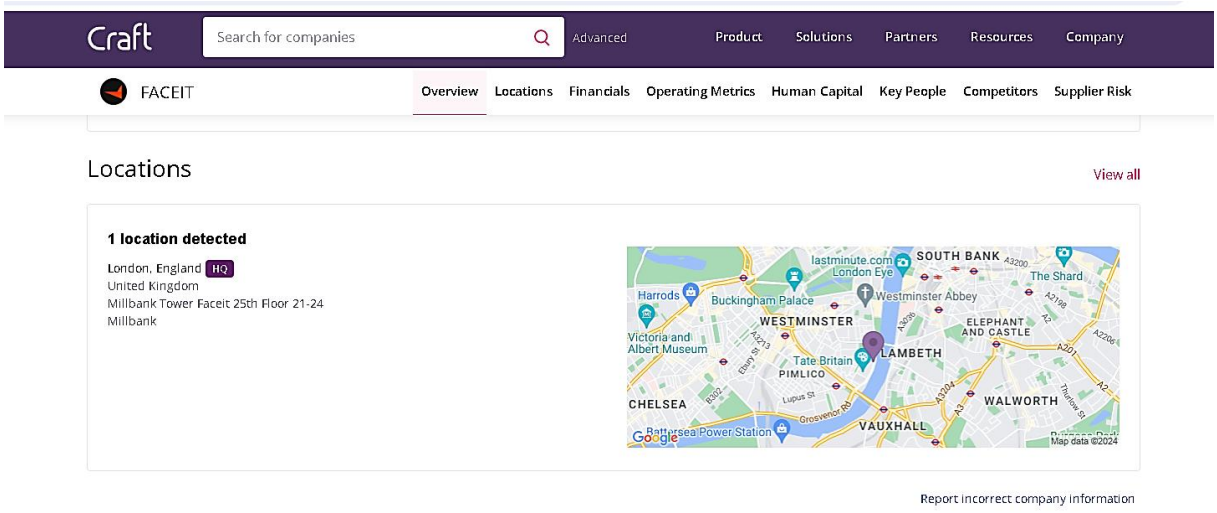
Next statement date **7 January 2025**
due by **21 January 2025**

Last statement dated **7 January 2024**

Nature of business (SIC)

59112 - Video production activities
62011 - Ready-made interactive leisure and entertainment software development

Obraz 2.1.5 dane firmy Faceit w brytyjskim rejestrze spółek, źródło gov.uk, data wykonania zrzutu 15.01.2024 r.



Craft | Search for companies | Advanced | Product | Solutions | Partners | Resources | Company

FACEIT | Overview | Locations | Financials | Operating Metrics | Human Capital | Key People | Competitors | Supplier Risk

Locations | View all

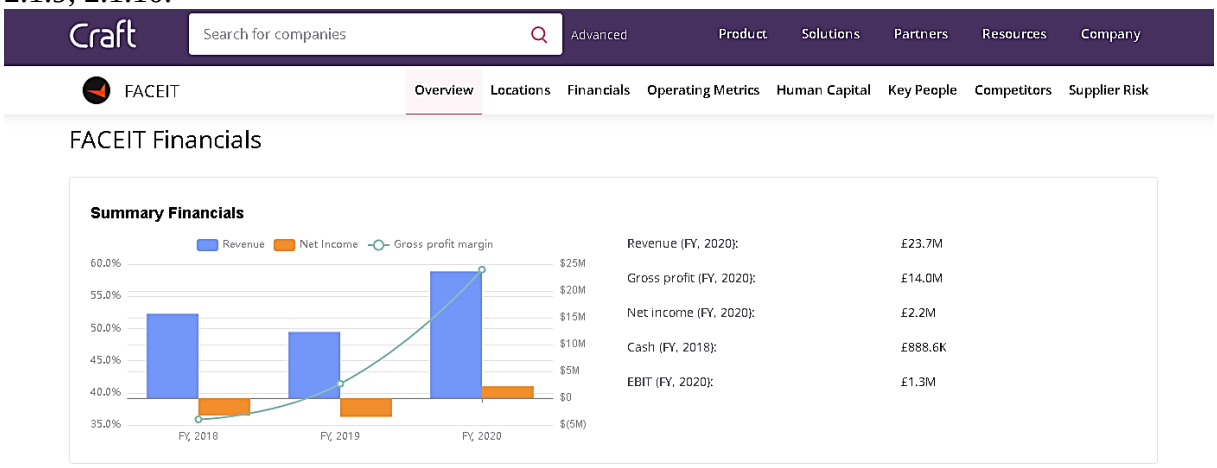
1 location detected

London, England HQ
United Kingdom
Millbank Tower Faceit 25th Floor 21-24
Millbank

Report incorrect company information

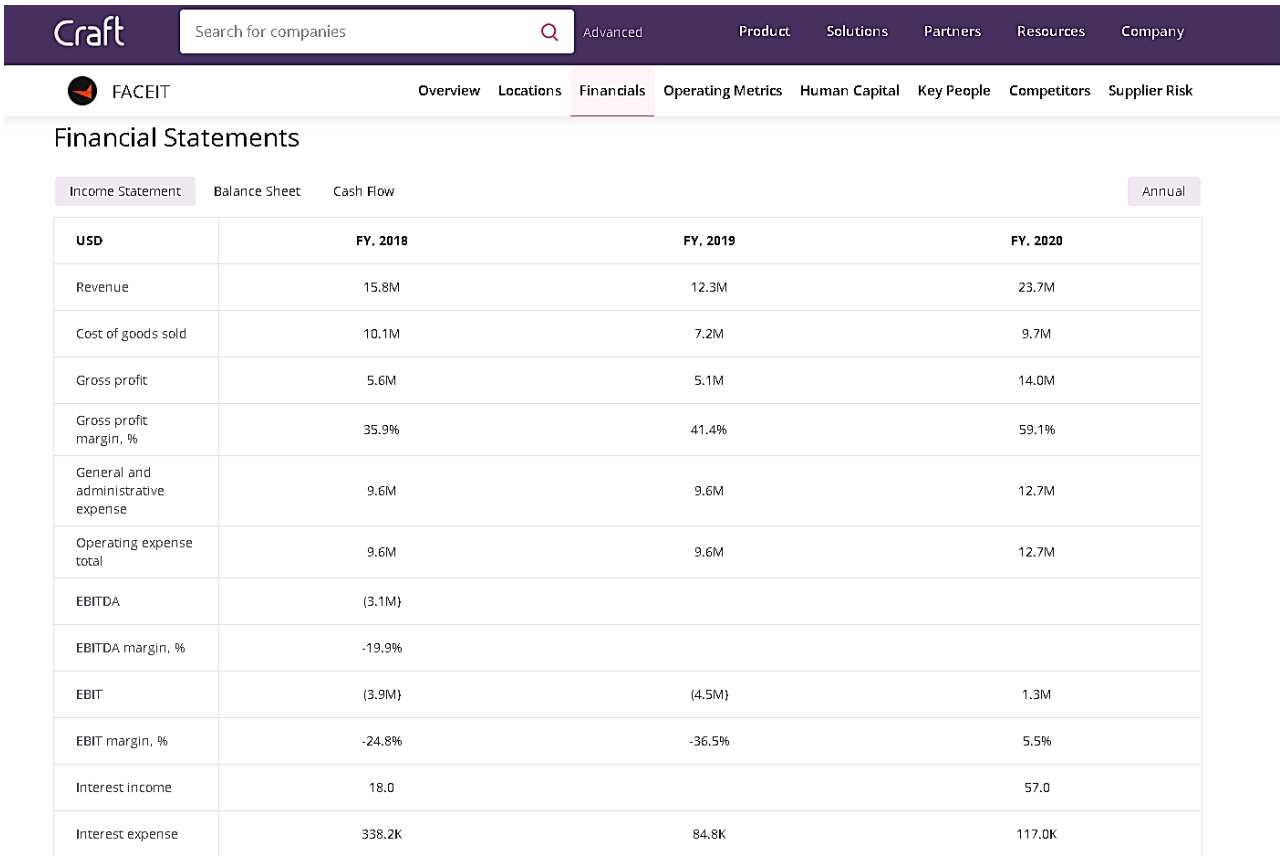
Obraz 2.1.6 ogólny zarys firmy Faceit, źródło craft.co, data wykonania zrzutu 10.1.2024 r.

Sprawozdania finansowe organizacji Faceit zostały przedstawione na obrazach 2.1.7, 2.1.8, 2.1.9, 2.1.10.



Obraz 2.1.7 roczne sprawozdania finansowe firmy Faceit za lata 2018-2020 (w funtach), w formie wykresu, źródło craft.co, data wykonania zrzutu 10.1.2024 r.

Obraz 2.1.8 pokazuje, że największy przychód firmy w okresie 3 lat między 2018-2020 przypada na rok 2020, co można wytłumaczyć pandemią i zwiększoną liczbą użytkowników gier online korzystającą z usług organizacji.



USD	FY, 2018	FY, 2019	FY, 2020
Revenue	15.8M	12.3M	23.7M
Cost of goods sold	10.1M	7.2M	9.7M
Gross profit	5.6M	5.1M	14.0M
Gross profit margin, %	35.9%	41.4%	59.1%
General and administrative expense	9.6M	9.6M	12.7M
Operating expense total	9.6M	9.6M	12.7M
EBITDA	(3.1M)		
EBITDA margin, %	-19.9%		
EBIT	(3.9M)	(4.5M)	1.3M
EBIT margin, %	-24.8%	-36.5%	5.5%
Interest income	18.0		57.0
Interest expense	338.2K	84.8K	117.0K

Obraz 2.1.8 szczegółowe roczne sprawozdania finansowe firmy Faceit za lata 2018-2020 (w funtach), źródło craft.co, data wykonania zrzutu 10.1.2024 r.

Z obrazu 2.1.9 można odczytać, że organizacja miała największy przyrost zasobów miedzy latami 2014-2015 (około 90-kronty wzrost zasobów).

Craft | Search for companies | Advanced | Product | Solutions | Partners | Resources | Company

FACEIT | Overview | Locations | Financials | Operating Metrics | Human Capital | Key People | Competitors | Supplier Risk

Financial Statements

Income Statement | Balance Sheet | Cash Flow | Annual

GBP	FY, 2012	FY, 2013	FY, 2014	FY, 2015	FY, 2016	FY, 2017	FY, 2018
Cash	80.7K	703.0	36.5K	9.0M	447.1K	4.2M	888.6K
Accounts Receivable	63.8K	69.2K	76.7K	387.5K	4.6M	424.3K	325.9K
Current Assets	144.5K	70.0K	113.2K	9.6M	5.8M	5.8M	2.3M
PP&E	1.7K	9.0K	4.9K	56.1K	583.1K	527.7K	562.8K
Total Assets	146.2K	79.0K	118.1K	9.9M	7.1M	8.1M	5.7M
Accounts Payable	43.1K	18.9K	162.6K	554.4K	883.5K	684.6K	1.8M
Current Liabilities	43.1K	18.9K	162.6K	1.5M	3.7M	5.1M	9.5M
Non-Current Liabilities						3.7M	
Total Liabilities	43.1K	18.9K	162.6K	1.5M	3.7M	8.8M	9.5M
Common Stock	20.5K	22.6K	23.8K	35.7K	34.4K	34.4K	34.5K
Retained Earnings		(346.6K)	(551.1K)	(1.3M)	(4.9M)	(9.1M)	(12.3M)
Total Equity	103.1K	60.1K	(44.5K)	8.4M	3.4M	(653.5K)	(3.8M)
Financial Leverage	1.4	1.3	-2.7	1.2	2.1	-12.4	-1.5

Obraz 2.1.9 szczegółowe roczne sprawozdania finansowe firmy Faceit za lata 2012-2018 (w funtach), źródło craft.co, data wykonania zrzutu 10.1.2024 r.

Z obrazu 2.1.10 można dowiedzieć się, że przychód firmy nie rośnie monotonicznie w latach 2015-2018.

Craft | Search for companies | Advanced | Product | Solutions | Partners | Resources | Company

FACEIT | Overview | Locations | Financials | Operating Metrics | Human Capital | Key People | Competitors | Supplier Risk

Learn more

Financial Statements

Income Statement | Balance Sheet | Cash Flow | Annual

GBP	FY, 2015	FY, 2016	FY, 2017	FY, 2018
Net Income	(721.7K)	(3.8M)	(4.3M)	(3.3M)
Cash From Operating Activities	147.3K	(6.1M)	1.2M	(2.2M)
Cash From Financing Activities	9.2M	(1.4M)	3.7M	28.2K
Net Change in Cash	9.0M	(8.5M)	3.8M	(3.4M)

Obraz 2.1.10 szczegółowe roczne sprawozdania finansowe firmy Faceit za lata 2015-2018 (w funtach), źródło craft.co, data wykonania zrzutu 10.1.2024 r.

W 2022 roku organizacja FACEIT została przejęta przez Savvy Games Group (SGG), spółkę holdingową należącą do Funduszu Inwestycji Publicznych Arabii Saudyjskiej, za łączną kwotę 1,5 miliarda dolarów, co widać na obrazach 2.2.1, 2.2.2. W ramach przejęcia obie firmy połączyły się i utworzyły grupę ESL FACEIT. Kontrowersja wzbudza fakt rzekomego zlecenia zabójstwa dziennikarza przez właściciela organizacji Savvy Games Group.

A year and a half ago, Savvy Games Group formed and acquired esports platforms ESL and Faceit in hopes of creating an esports powerhouse. Then Savvy, owned by Saudi Arabia's Public Investment Fund, also picked up a part of Vindex focused esports data and production.

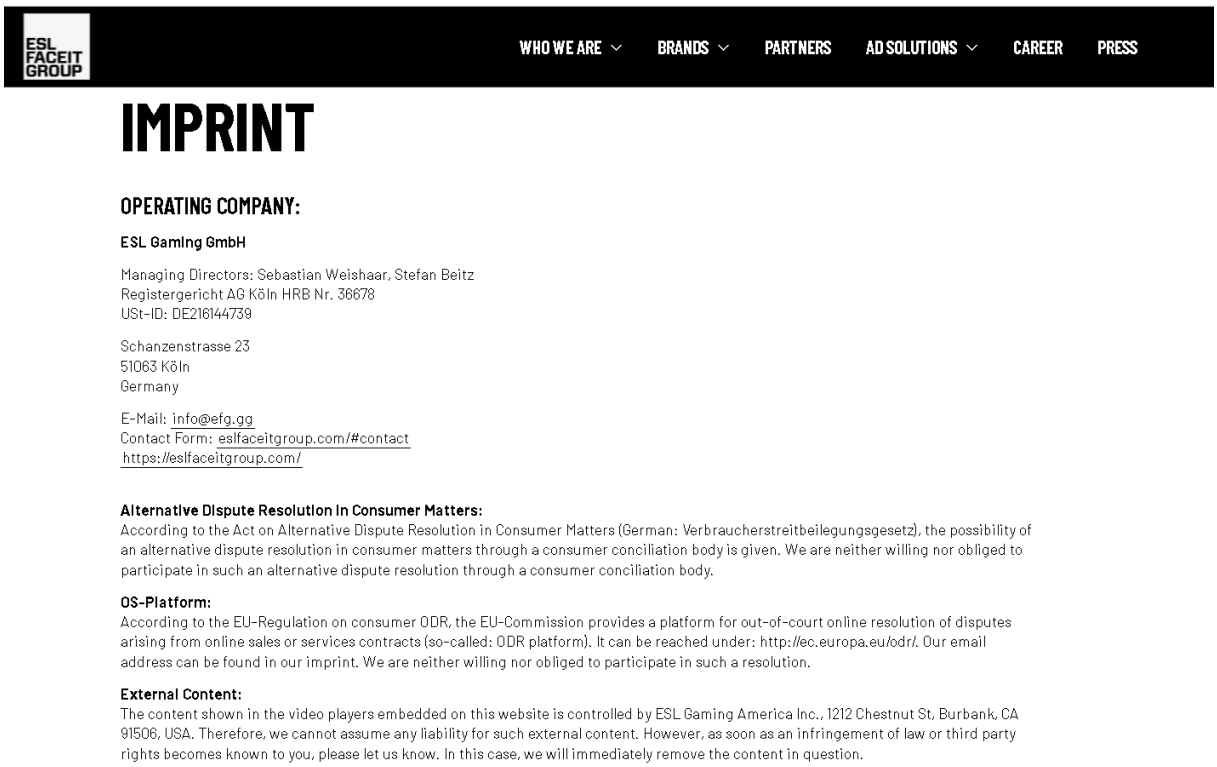
At Gamescom, I met with Ralf Reichert, chairman of ESL Faceit Group (EFG), and Michele Attisani, chief business development officer.

Obraz 2.2.1 opis przejęcia (fuzji) organizacji Faceit, źródło venturebeat.com, data wykonania zrzutu 15.01.2024 r.

There are additional headwinds on the political front, as Savvy and ESL Faceit are owned by the Saudi Arabia Public Investment Fund, headed by Saudi Crown Prince Mohammed Bin Salman, who was accused of orchestrating the murder of Washington Post writer Jamal Khashoggi in 2018. After an outcry from gamers in 2020, both Riot Games and Blast Premier pulled out of a Saudi project, as the Saudis have been accused, as they were with golf and soccer, of "sportwashing" human rights abuses.

Obraz 2.2.2 informacje o właścicielu Savvy, źródło venturebeat.com, data wykonania zrzutu 15.01.2024 r.

ESL FACEIT GROUP to organizacja mająca siedzibę w Kolonii, na ulicy Schanzenstrasse 22. Firma została założona w 2000 r., zajmuje się e-sport'em, grami, organizacją wydarzeń e-sportowych, produkcją telewizyjną, transmisja na żywo, co widać na obrazach 2.3.1, 2.3.2, 2.3.3, 2.3.4.



ESL FACEIT GROUP

WHO WE ARE BRANDS PARTNERS AD SOLUTIONS CAREER PRESS

IMPRINT

OPERATING COMPANY:

ESL Gaming GmbH

Managing Directors: Sebastian Weishaar, Stefan Beitz
Registergericht AG Köln HRB Nr. 36678
USt-ID: DE216144739

Schanzenstrasse 23
51063 Köln
Germany

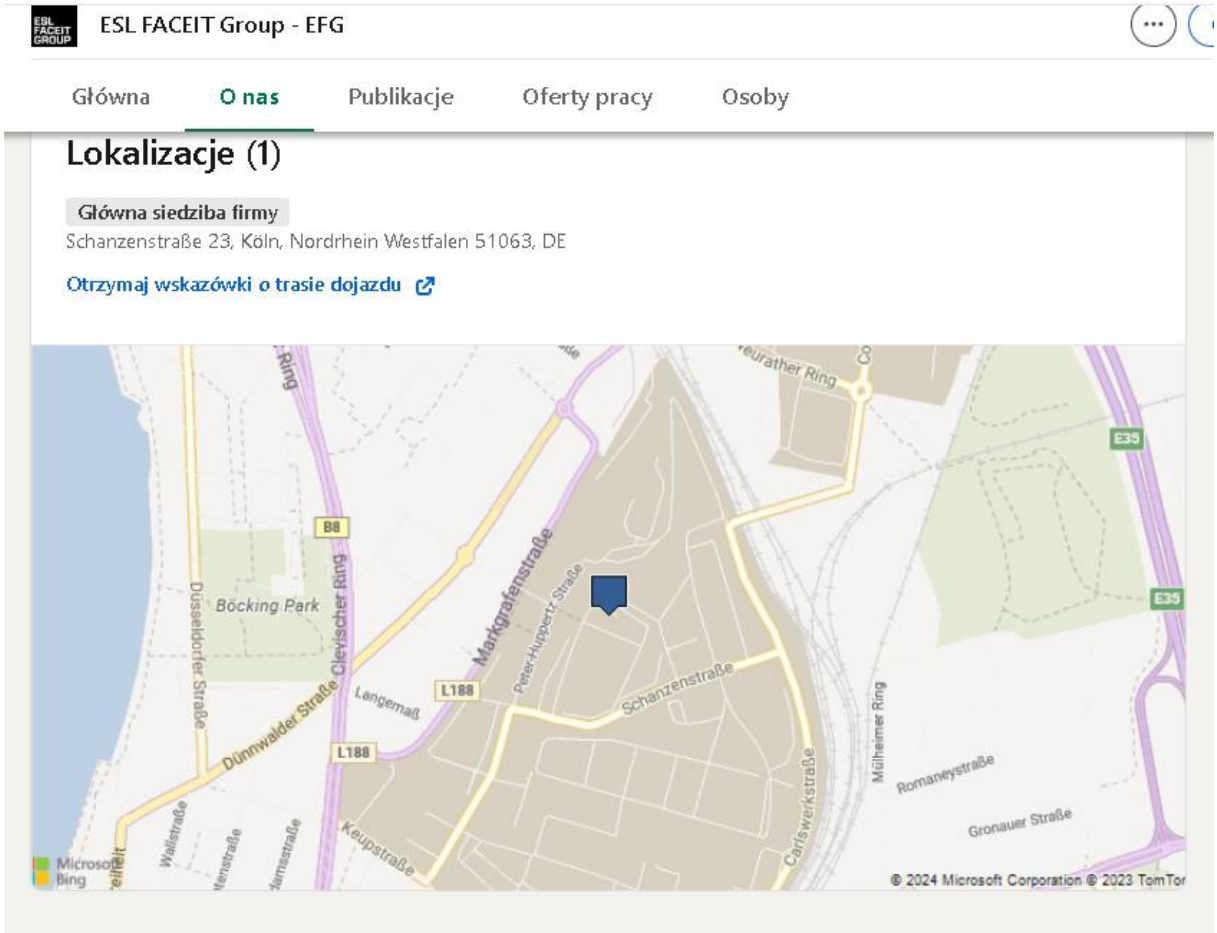
E-Mail: info@efg.gg
Contact Form: eslfaceitgroup.com/#contact
https://eslfaceitgroup.com/

Alternative Dispute Resolution in Consumer Matters:
According to the Act on Alternative Dispute Resolution in Consumer Matters (German: Verbraucherstreitbeilegungsgesetz), the possibility of an alternative dispute resolution in consumer matters through a consumer conciliation body is given. We are neither willing nor obliged to participate in such an alternative dispute resolution through a consumer conciliation body.

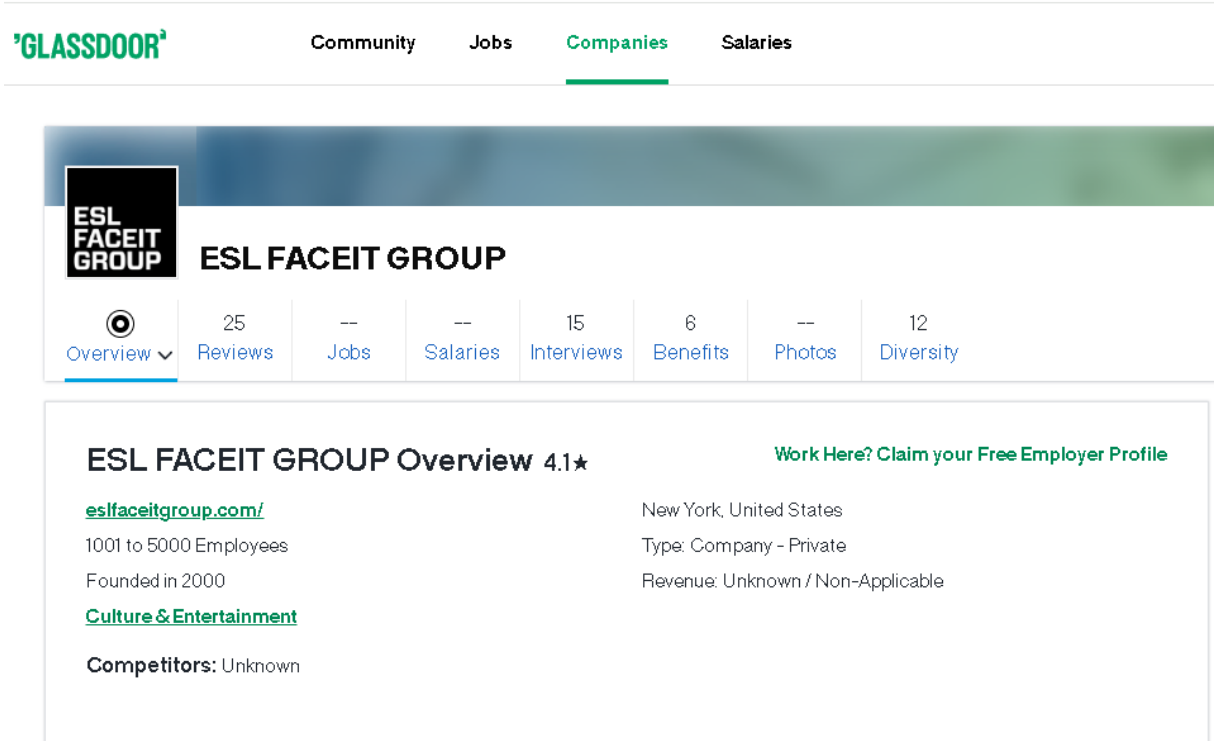
OS-Platform:
According to the EU-Regulation on consumer ODR, the EU-Commission provides a platform for out-of-court online resolution of disputes arising from online sales or services contracts (so-called: ODR platform). It can be reached under: http://ec.europa.eu/odr/. Our email address can be found in our imprint. We are neither willing nor obliged to participate in such a resolution.

External Content:
The content shown in the video players embedded on this website is controlled by ESL Gaming America Inc., 1212 Chestnut St, Burbank, CA 91506, USA. Therefore, we cannot assume any liability for such external content. However, as soon as an infringement of law or third party rights becomes known to you, please let us know. In this case, we will immediately remove the content in question.

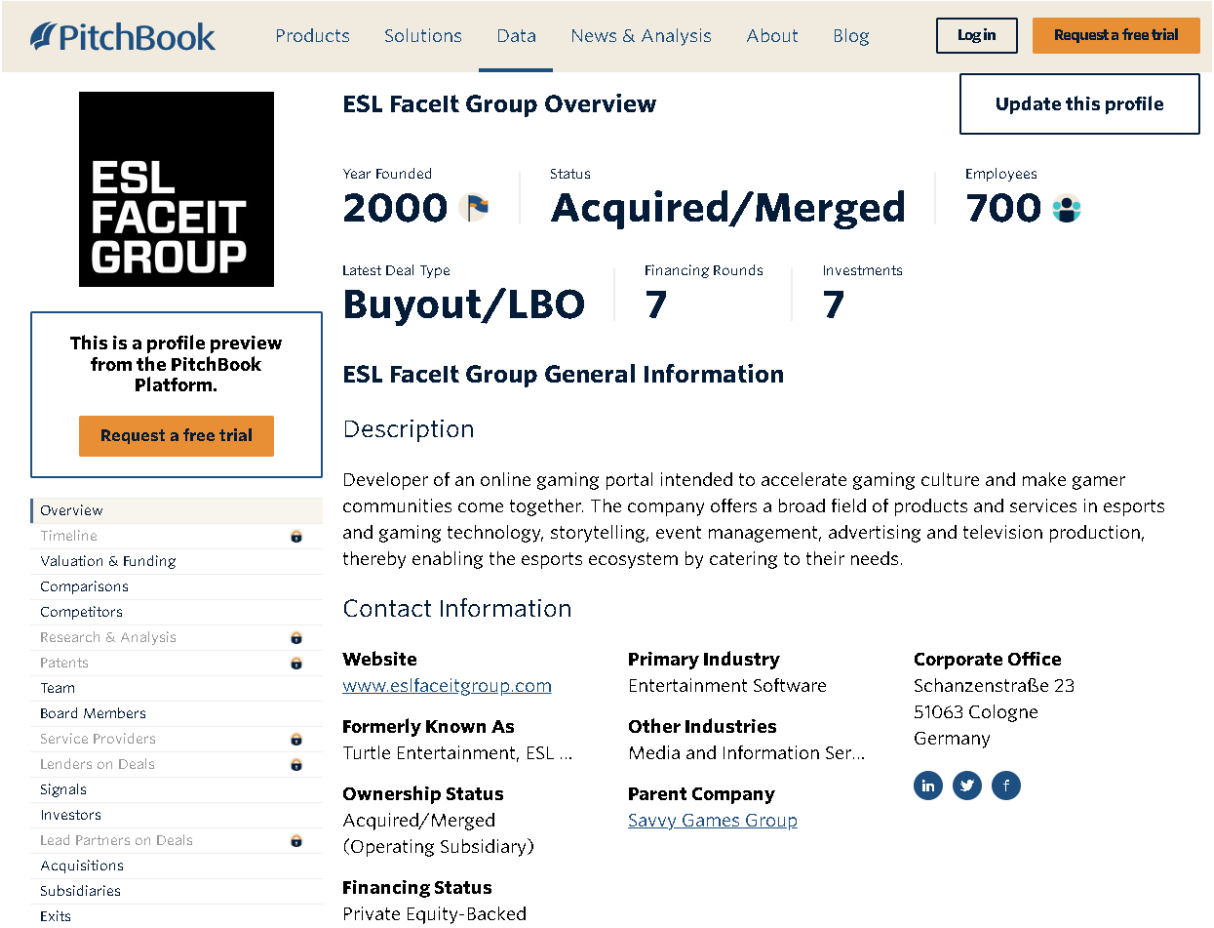
Obraz 2.3.1 informacje o organizacji ESL Gaming/ESL FACEIT GROUP, źródło eslfaceitgroup.com, data wykonania zrzutu 07.01.2024 r.



Obraz 2.3.2 siedziba organizacji ESL Gaming/ESL FACEIT GROUP na mapie, źródło linkedin.com, data wykonania zrzutu 07.01.2024 r.

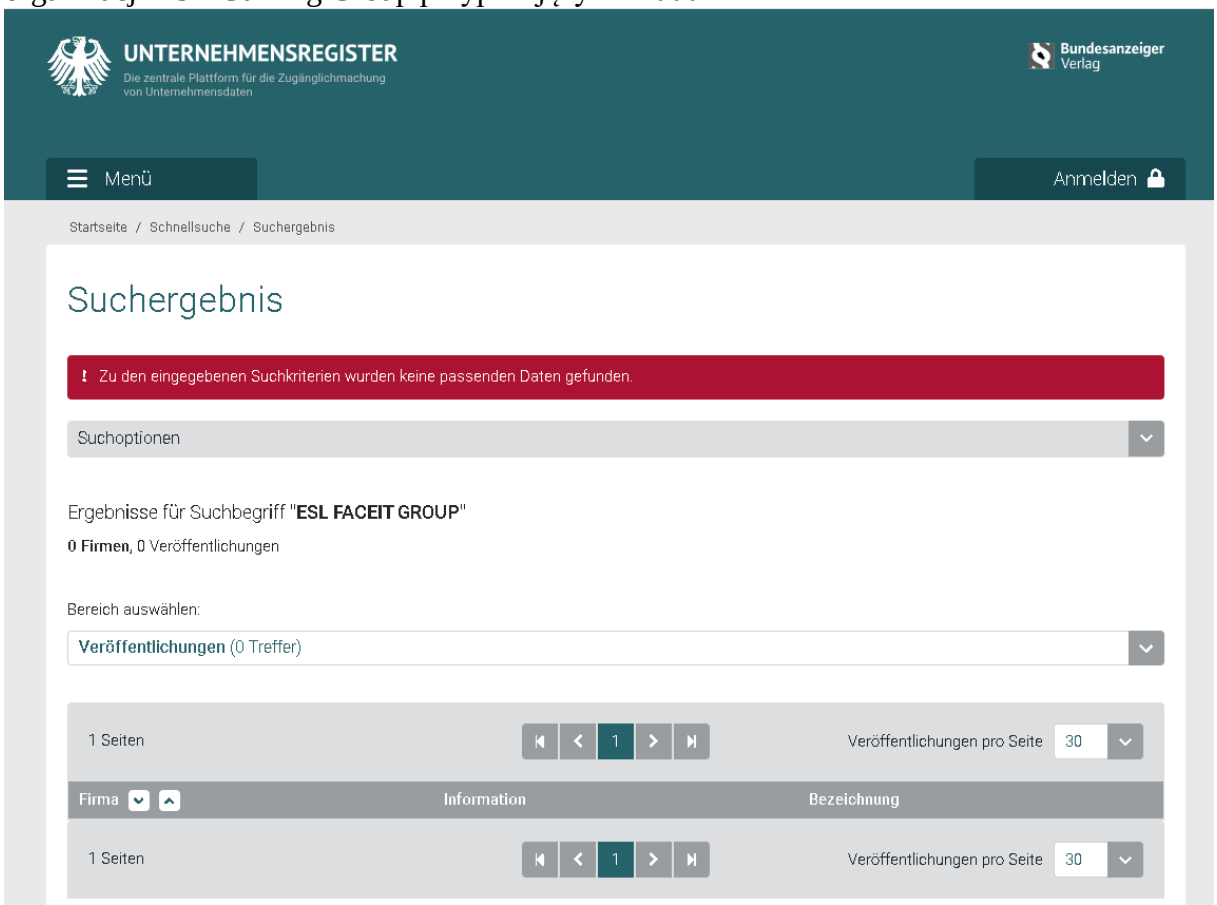


Obraz 2.3.3 ogólny zarys firmy ESL FACEIT GROUP, źródło glassdoor.co.uk, data wykonania zrzutu 10.01.2024 r.

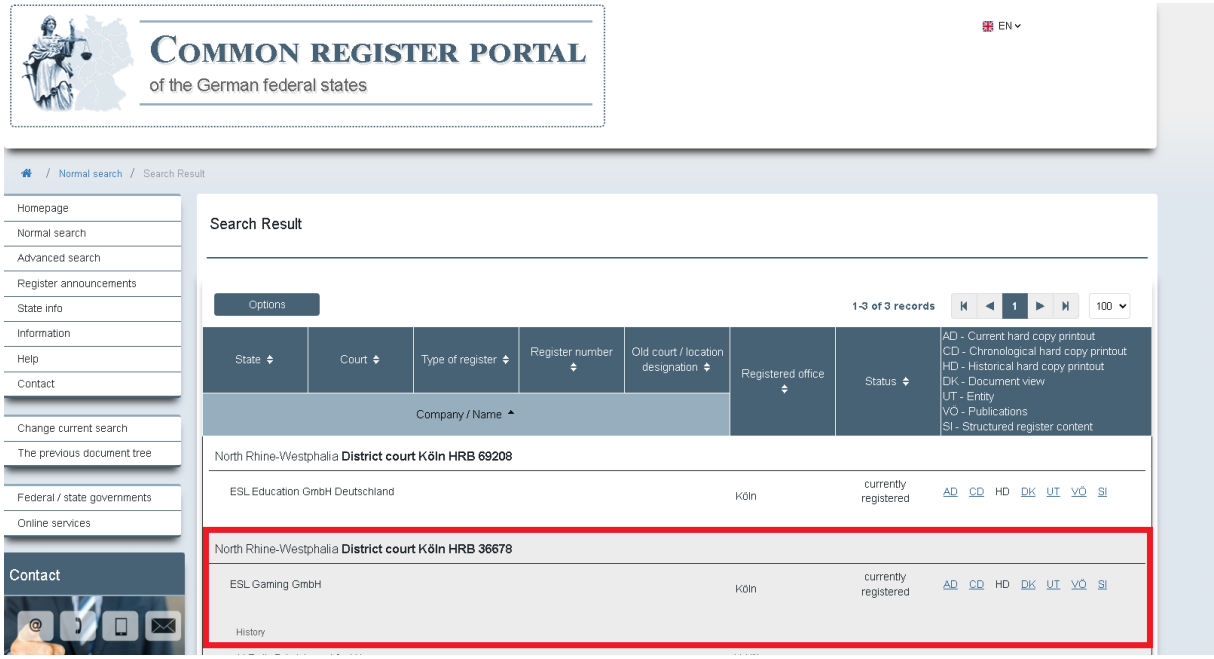


Obraz 2.3.4 ogólny zarys firmy ESL FACEIT GROUP, źródło pitchbook.com, data wykonania zrzutu 10.01.2024 r.

Brak wyników w niemieckim rejestrze firm dla frazy ESL FACEIT GROUP. Co ciekawe istnieje wpis o organizacji ESL Gaming, która uczestniczyła w fuzji w 2022 r. razem z organizacją Faceit opisaną powyżej (Obrazy 2.3.5, 2.3.6, 2.3.7). Siedziby organizacji ESL Gaming i ESL FACEIT GROUP są takie same. Zadziwiający jest fakt daty założenia organizacji ESL Gaming Group przypadający na 2000 r.



Obraz 2.3.5 wynik wyszukania firmy ESL FACEIT GROUP w niemieckim rejestrze spółek, źródło unternehmensregister.de, data wykonania zrzutu 10.01.2024 r.



Obraz 2.3.6 wynik wyszukania firmy ESL FACEIT GROUP w niemieckim rejestrze spółek, źródło en.justiz.de, data wykonania zrzutu 10.01.2024 r.

Handelsregister B des Amtsgerichts Köln	Abteilung B Wiedergabe des aktuellen Registerinhalts Abruf vom 10.01.2024 20:14	Nummer der Firma: **HRB 36678**
Abdruck	Seite 1 von 2	

1. Anzahl der bisherigen Eintragungen:

34

2. a) Firma:

ESL Gaming GmbH

b) Sitz, Niederlassung, inländische Geschäftsanschrift, empfangsberechtigte Person, Zweigniederlassungen:

Köln
Geschäftsanschrift: Schanzenstraße 23, 51063 Köln

c) Gegenstand des Unternehmens:

das Anbieten von redaktionellen Computerspiele Inhalten im Wesentlichen im Internet und in anderer Verbreitung, das Durchführen eines Online-Spielbetriebes im Internet und der Aufbau und Betrieb nationaler und internationaler Online-Spiele-Ligen, die Durchführung von Computer-Spiele-Veranstaltungen und -Turnieren sowie der An- und Verkauf, die Lizenzierung, Anmietung und Vermietung von Hard- und Software und von Lizenzen, die Lizenzierung von Rechten der Gesellschaft und der Betrieb einer Werbeagentur sowie die Vermarktung von eSports-Wettbewerben und -Inhalten der Gesellschaft selbst und von anderen eSports-Organisationen und -Inhalten.

3. Grund- oder Stammkapital:

146.136,00 EUR

4. a) Allgemeine Vertretungsregelung:

Ist nur ein Geschäftsführer bestellt, so vertritt er die Gesellschaft allein. Sind mehrere Geschäftsführer bestellt, so wird die Gesellschaft durch zwei Geschäftsführer gemeinsam vertreten.

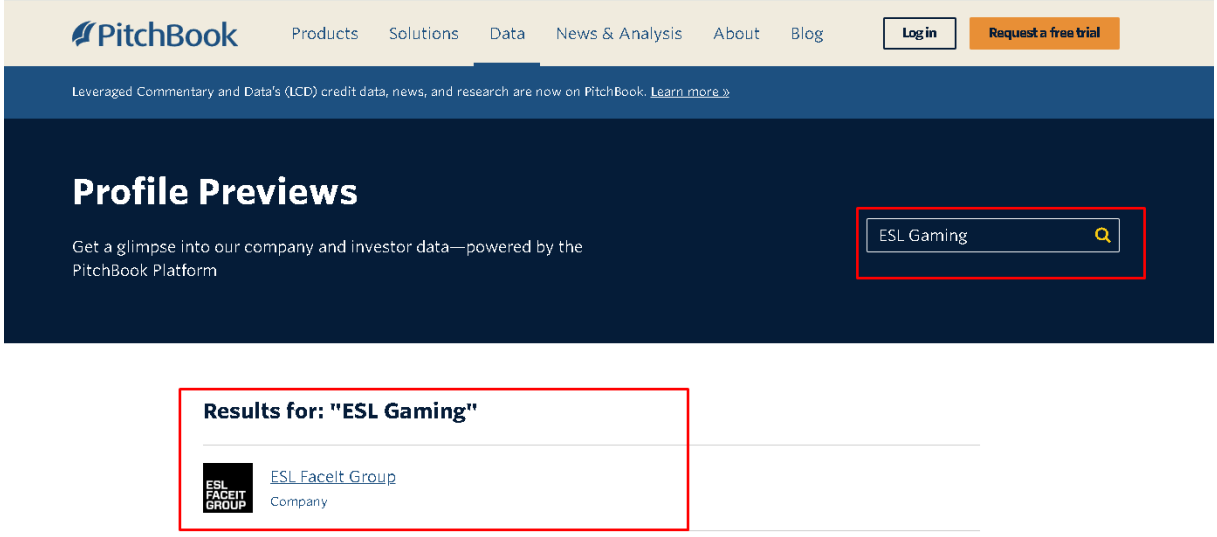
b) Vorstand, Leitungsorgan, geschäftsführende Direktoren, persönlich haftender Gesellschafter, Geschäftsführer, Vertretungsberechtigte und besondere Vertretungsbefugnis:

Geschäftsführer: Weishaar, Sebastian Frederic Constantin Alexander Philippe, Köln, *16.08.1983

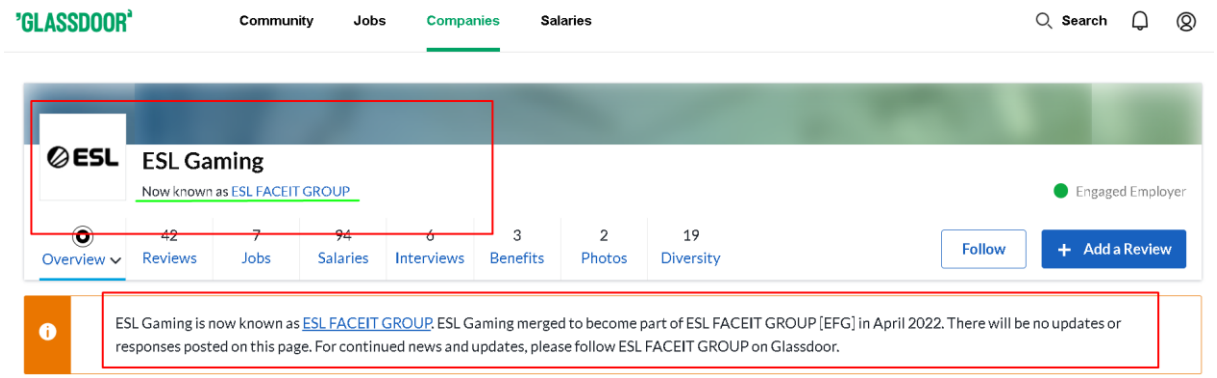
Mit der Befugnis im Namen der Gesellschaft mit sich als Vertreter eines Dritten Rechtsgeschäfte abzuschließen:
Geschäftsführer: Beitz, Stefan, München, *02.04.1980

Obraz 2.3.7 dane firmy ESL Gaming, źródło en.justiz.de, data wykonania zrzutu 10.01.2024 r.

Po wpisaniu frazy ESL Gaming w wyszukiwarce pitchbook(Obraz 2.3.8) wyświetla się organizacja ESL GAMING GROUP, co może świadczyć o tym, że organizacja ESL GAMING GROUP(taki sam adres siedziby, data założenia przypadająca na 2000 rok, a fuzja organizacji miała miejsce w 2022 r.) to tak naprawdę ESL Gaming po zmianie nazwy. Tą hipotezę potwierdza obraz 2.3.9.

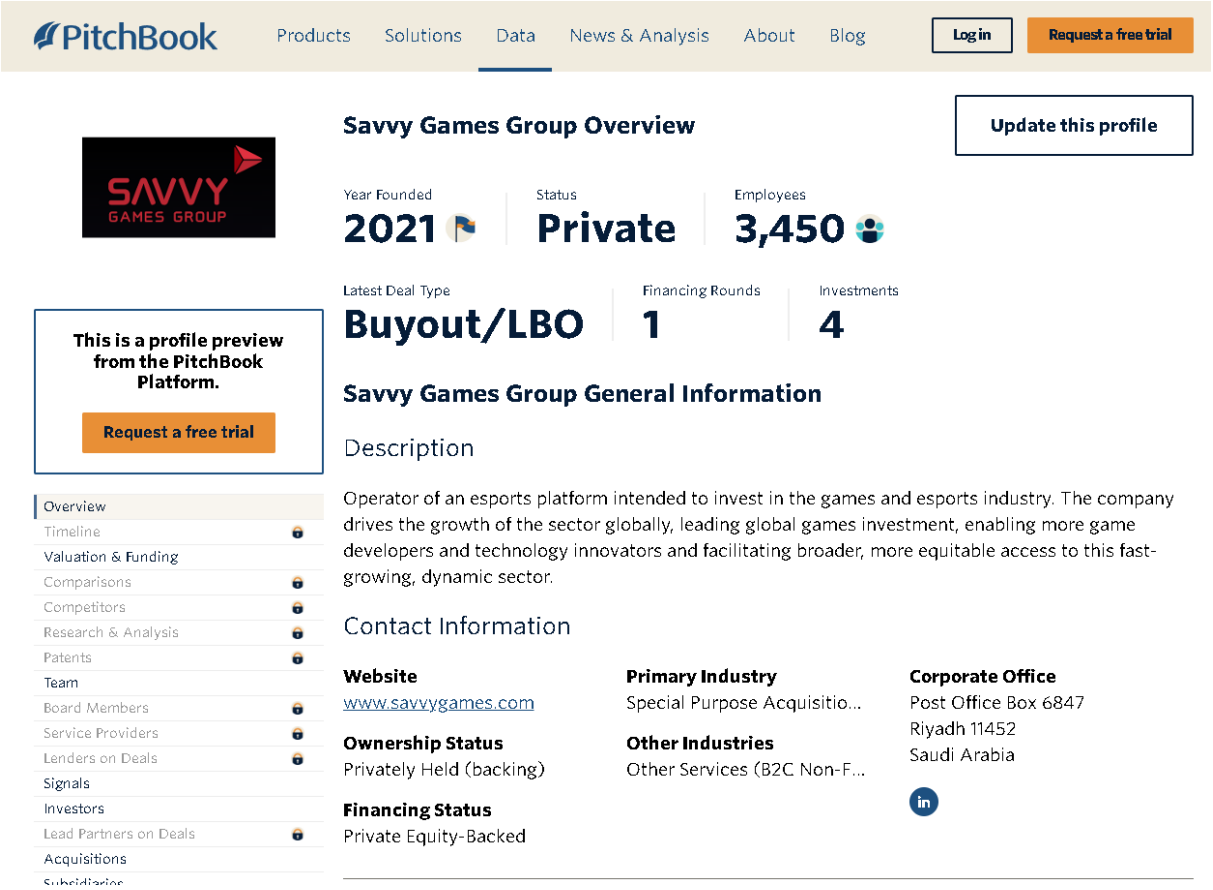


Obraz 2.3.8 wynik wyszukania firmy ESL Gaming, źródło pitchbook.com, data wykonania zrzutu 10.01.2024 r.

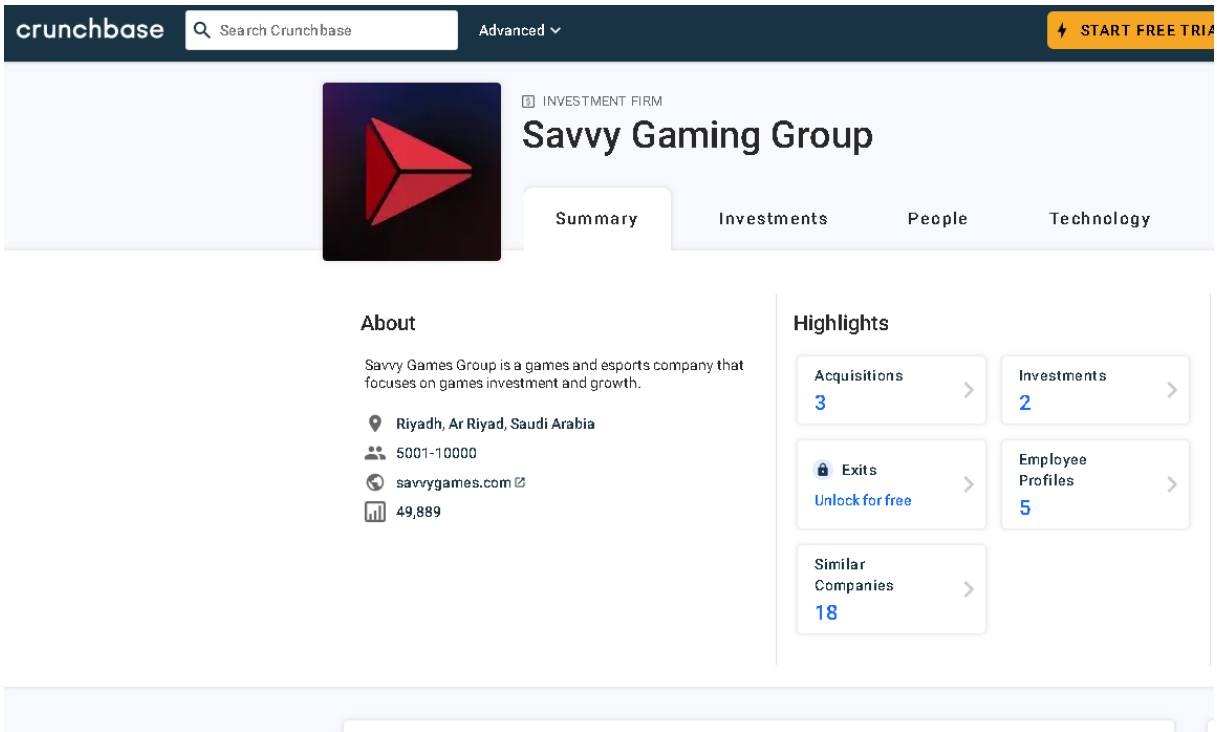


Obraz 2.3.9 dane firmy ESL Gaming, źródło glassdoor.co.uk, data wykonania zrzutu 10.01.2024 r.

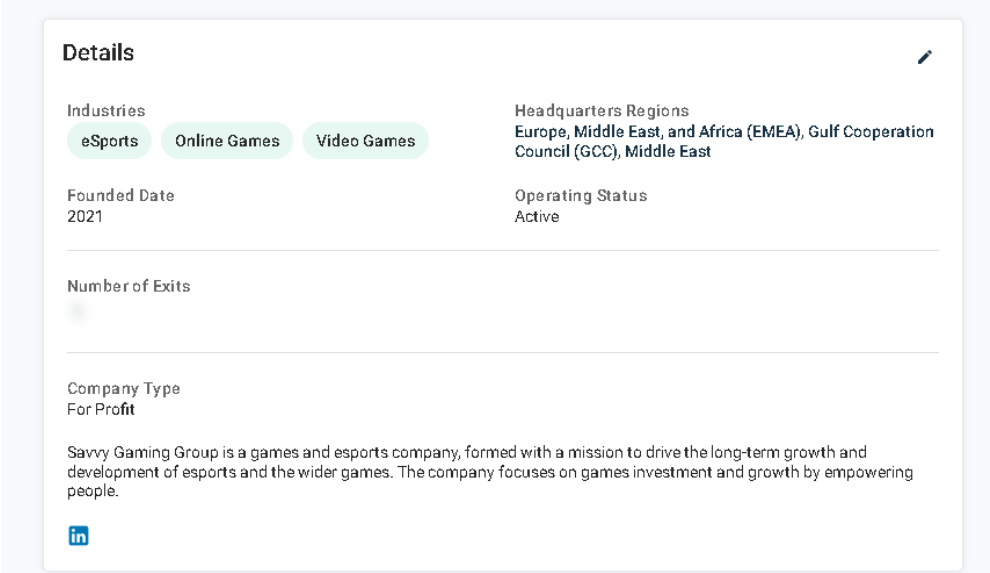
Savvy Games Group ma siedzibę w King Fahad Road, 6th Floor, 2.14 B, KAFD, Riyadh, SA. Organizacja zajmuje się esportem i promowaniem gier komputerowych, co potwierdzają obrazy 2.4.1, 2.4.2, 2.4.3, 2.4.4.



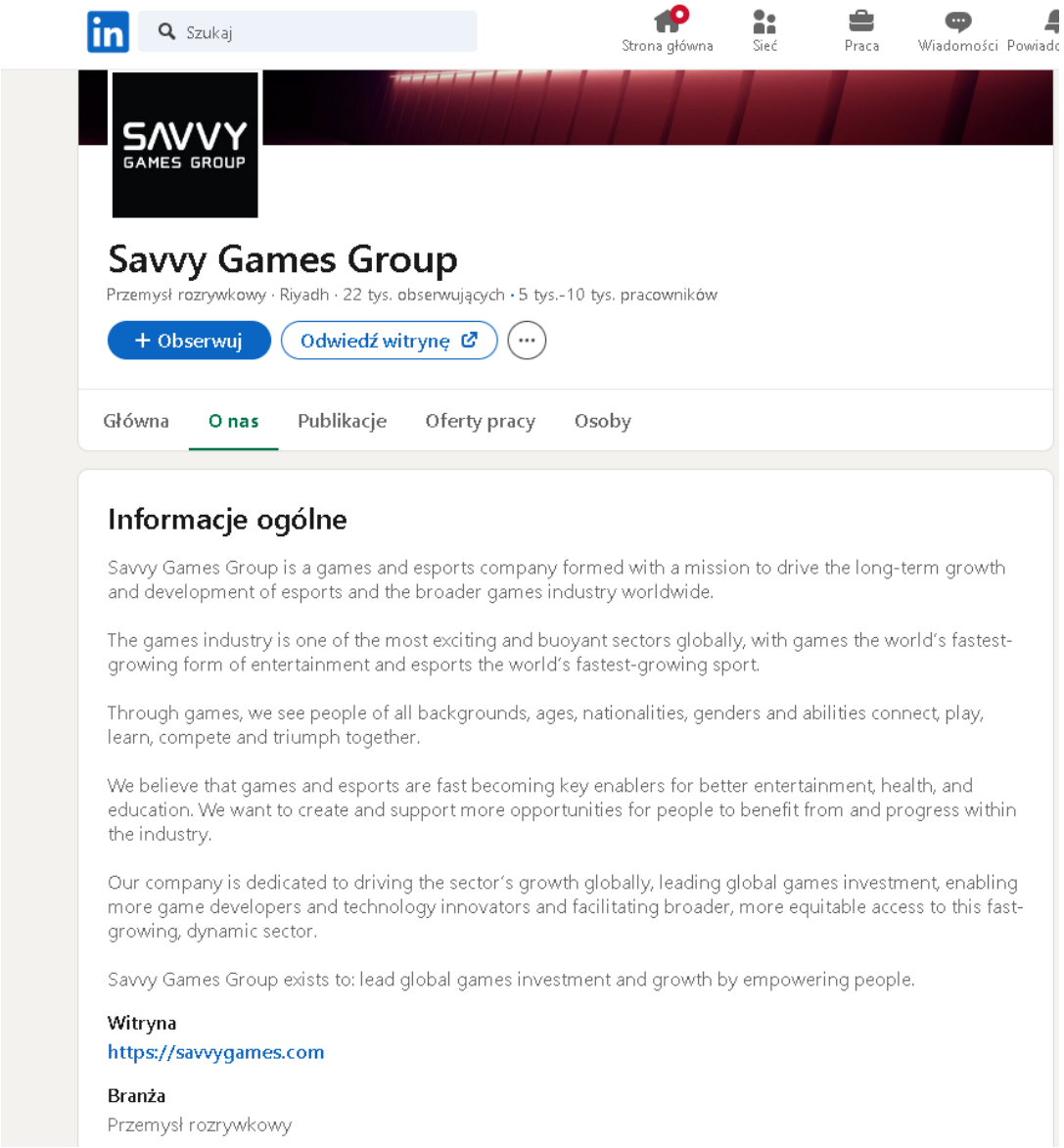
Obraz 2.4.1 ogólne dane firmy Savvy, źródło pitchbook.com, data wykonania zrzutu 10.01.2024 r.



Obraz 2.4.2 ogólne dane firmy Savvy, źródło crunchbase.com, data wykonania zrzutu 10.01.2024 r.



Obraz 2.4.3 ogólne dane firmy Savvy, źródło crunchbase.com, data wykonania zrzutu 10.01.2024 r.



Obraz 2.4.4 ogólne dane firmy Savvy, źródło linkedin.com, data wykonania zrzutu 10.01.2024 r.

Partnerzy biznesowi organizacji ESL FACEIT GROUP (do zebrania informacji o partnerach korzystano ze strony eslfaceitgroup.com), przykładowi partnerzy na obrazach 2.5.1, 2.5.2.

- Bayes Esports
- VTV-Cab
- IEM
- ASUS ROG
- GamingMalta Foundation
- Gravity Media
- EarlyGame
- Lenovo Legion
- Legendary Play
- Acer
- Gameloft
- Immutable X

- 343 Industries
- Google
- Gucci

Obraz 2.5.1 nagłówek artykułu dotyczącego współpracy Faceit z Google, źródło forbes.com, data wykonania zrzutu 10.1.2024 r.

Obraz 2.5.2 nagłówek artykułu dotyczącego współpracy Faceit z Gucci źródło forbes.com, data wykonania zrzutu 17.1.2024 r.

W zbieraniu danych do rozdziału 2 skorzystano ze stron takich jak linkedin.com, crunchbase.com, pitchbook.com, en.justiz.de, unternehmensregister.de, glassdoor.co.uk, eslfaceitgroup.com, venturebeat.com, craft.co, gov.uk które przedstawiono na obrazach 2.X.X. Z zebranych informacji można dowiedzieć się, że organizacje FACEIT, ESL FACEIT GROUP, Savvy Games Group zajmują się sektorem gier komputerowych. Każda z organizacji ma

siedziby w różnych krajach (Wielka Brytania, Niemcy, Arabia Saudyjska). Organizacje posiadają szeroką bazę parterów z branż technologicznych. Uzyskano z krajowych rejestrów informacje dotyczące adresów, typów działalności i sprawozdania finansowe organizacji.

3. Serwery DNS obsługujące domenę

Adresy serwerów dns obsługujących domenę faceit.com zostały wypisane przez narzędzia Kali'ego widoczne na obrazach 3.1.1, 3.2.1

```
┌──(kali㉿kali)-[~]
└─$ nslookup faceit.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   faceit.com
Address: 104.17.63.50
Name:   faceit.com
Address: 104.17.62.50
```

Obraz 3.1.1 wynik użycia narzędzia nslookup, system operacyjny Kali, data wykonania zrzutu 18.12.2023 r.

```
┌──(kali㉿kali)-[~]
└─$ dig faceit.com

; <<>> DiG 9.18.16-1-Debian <<>> faceit.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11328
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;faceit.com.                    IN      A

;; ANSWER SECTION:
faceit.com.             300     IN      A       104.17.62.50
faceit.com.             300     IN      A       104.17.63.50

;; Query time: 44 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Dec 13 15:21:01 EST 2023
;; MSG SIZE  rcvd: 71
```

Obraz 3.2.1 wynik użycia narzędzia dig, system operacyjny Kali, data wykonania zrzutu 13.12.2023 r.

Z obrazów 3.3.1, 3.3.2, 3.3.3 można dowiedzieć się, że dostawcą usług DNS dla domeny faceit.com jest Cloudflare (wykryto 6 adresów). Obsługą wiadomości email zarządzają serwery Google (3 adresy). Rozwiązywaniem nazwa dla protokołu IPv6 zarządza Cloudflare (wykryto 2 adresy).

faceit.com

General Information

Domain	faceit.com
Status	Active (last checked on 2023-12-09)
Top-level domain (TLD)	.com gTLD
Keyword	faceit
Active date	2012 or earlier
DomainRank	55/100
TrancoRank	11 479

Obraz 3.3.1 ogólne dane domeny faceit.com, źródło dnslytics.com, data wykonania zrzutu 10.12.2023r.

DNS records

NS Records	IP	Provider	ASN
jerry.ns.cloudflare.com used by 79 300 domains	108.162.193.182 (US)	Cloudflare, Inc. (US)	13335
	172.64.33.182 (US)	Cloudflare, Inc. (US)	13335
	173.245.59.182 (US)	Cloudflare, Inc. (US)	13335
	2606:4700:58::adf5:3bb6 (US)	Cloudflare, Inc. (US)	13335
	2803:f800:50::6ca2:c1b6 (CR)	Cloudflare, Inc. (US)	13335
	2a06:98c1:50::ac40:21b6 (US)	Cloudflare, Inc. (US)	13335
angela.ns.cloudflare.com used by 69 755 domains	108.162.192.65 (US)	Cloudflare, Inc. (US)	13335
	172.64.32.65 (US)	Cloudflare, Inc. (US)	13335
	173.245.58.65 (US)	Cloudflare, Inc. (US)	13335
	2606:4700:50::adf5:3a41 (US)	Cloudflare, Inc. (US)	13335
	2803:f800:50::6ca2:c041 (CR)	Cloudflare, Inc. (US)	13335
	2a06:98c1:50::ac40:2041 (US)	Cloudflare, Inc. (US)	13335

A/AAAA Records	Provider	ASN
104.17.62.50 (US) used by 1 domain	Cloudflare, Inc. (US)	13335
104.17.63.50 (US) used by 1 domain	Cloudflare, Inc. (US)	13335

Obraz 3.3.2 rekordy DNS domeny faceit.com, źródło dnslytics.com, data wykonania zrzutu 10.12.2023r.

A/AAAA Records	Provider	ASN
104.17.62.50 (US) used by 1 domain	Cloudflare, Inc. (US)	13335
104.17.63.50 (US) used by 1 domain	Cloudflare, Inc. (US)	13335

MX Records	IP	Provider	ASN
aspmx.l.google.com used by 15 645 253 domains	142.250.102.27 (US)	Google LLC (US)	15169
	2a00:1450:4025:401::1b (NL)	Google LLC (US)	15169
alt2.aspmx.l.google.com used by 15 348 195 domains	142.251.9.26 (US)	Google LLC (US)	15169
	2a00:1450:4025:c03::1b (PL)	Google LLC (US)	15169
alt1.aspmx.l.google.com used by 15 415 950 domains	209.85.202.27 (US)	Google LLC (US)	15169
	2a00:1450:4013:c16::1b (NL)	Google LLC (US)	15169

Obraz 3.3.3 rekordy DNS domeny faceit.com, źródło dnslytics.com, data wykonania zrzutu 10.12.2023r.

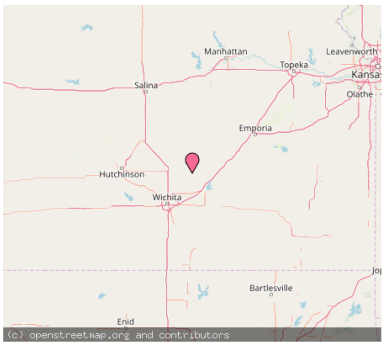
Z obrazów 3.3.1, 3.3.2, 3.3.3 można dowiedzieć się, że dostawcą usług DNS dla domeny faceit.com jest Cloudflare (wykryto 6 adresów). Obsługą wiadomości email zarządzają serwery Google (3 adresy). Rozwiązywaniem nazwa dla protokołu IPv6 zarządza Cloudflare (wykryto 2 adresy).

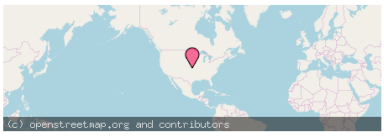
DNSlytics ip faceit.com

IP 104.17.62.50

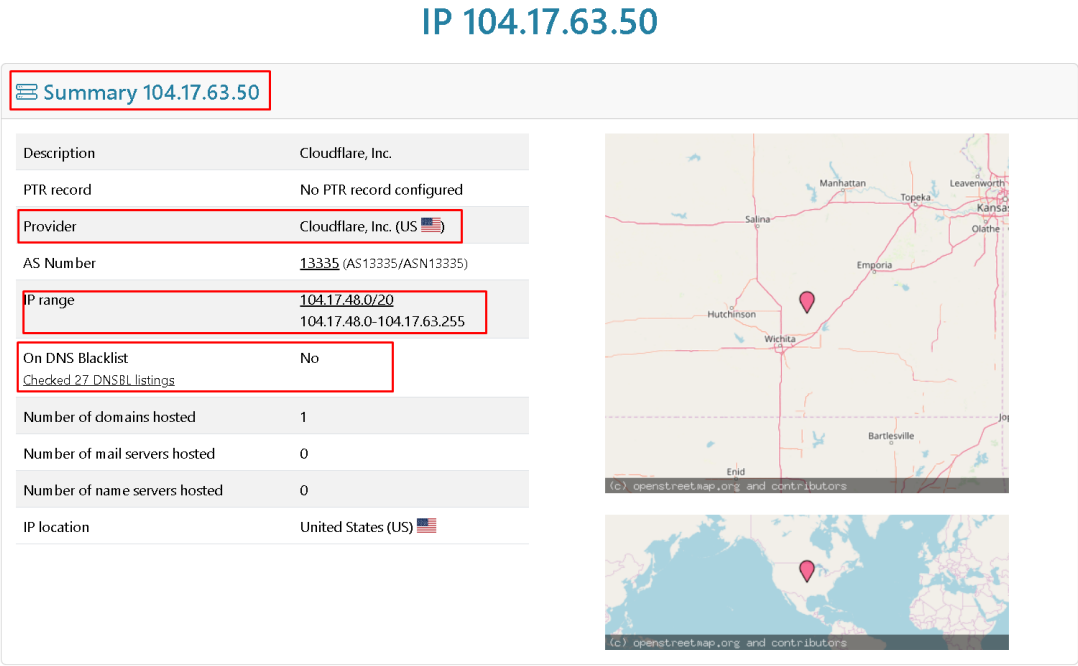
Summary 104.17.62.50

Description	Cloudflare, Inc.
PTR record	No PTR record configured
Provider	Cloudflare, Inc. (US)
AS Number	13335 (AS13335/ASN13335)
IP range	104.17.48.0/20 104.17.48.0-104.17.63.255
On DNS Blacklist Checked 27 DNSBL listings	No
Number of domains hosted	1
Number of mail servers hosted	0
Number of name servers hosted	0
IP location	United States (US)



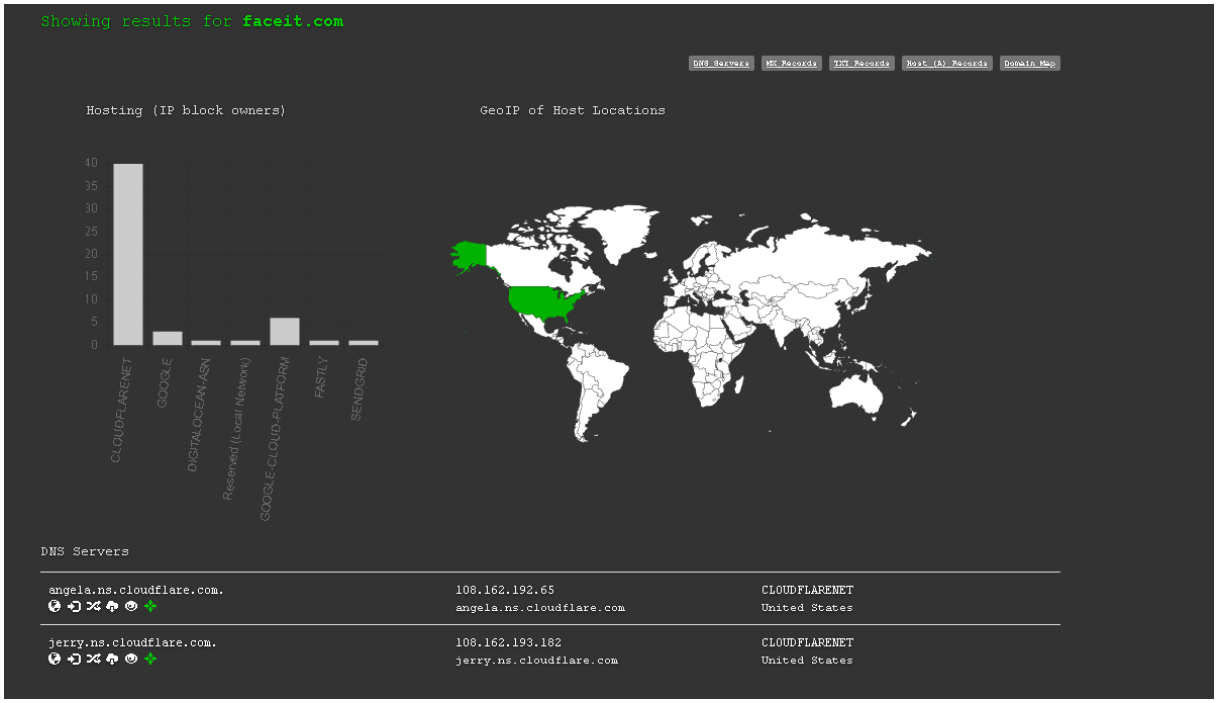


Obraz 3.3.4 ogólne dane domeny faceit.com, źródło dnslytics.com, data wykonania zrzutu 10.12.2023r.



Obraz 3.3.5 źródło dnslytics.com, data wykonania zrzutu 10.12.2023 r.

Z obrazów 3.4.1, 3.4.2 można dowiedzieć się, jakie serwery DNS obsługują domenę faceit.com. Znaleziono 2 serwery (hosting prowadzi Cloudflare) DNS i 3 rekordy MX (za hosting odpowiada Google).



Obraz 3.4.1 dane DNS domeny faceit.com, źródło dnsdumpster.com, data wykonania zrzutu 10.12.2023 r.

DNS Servers

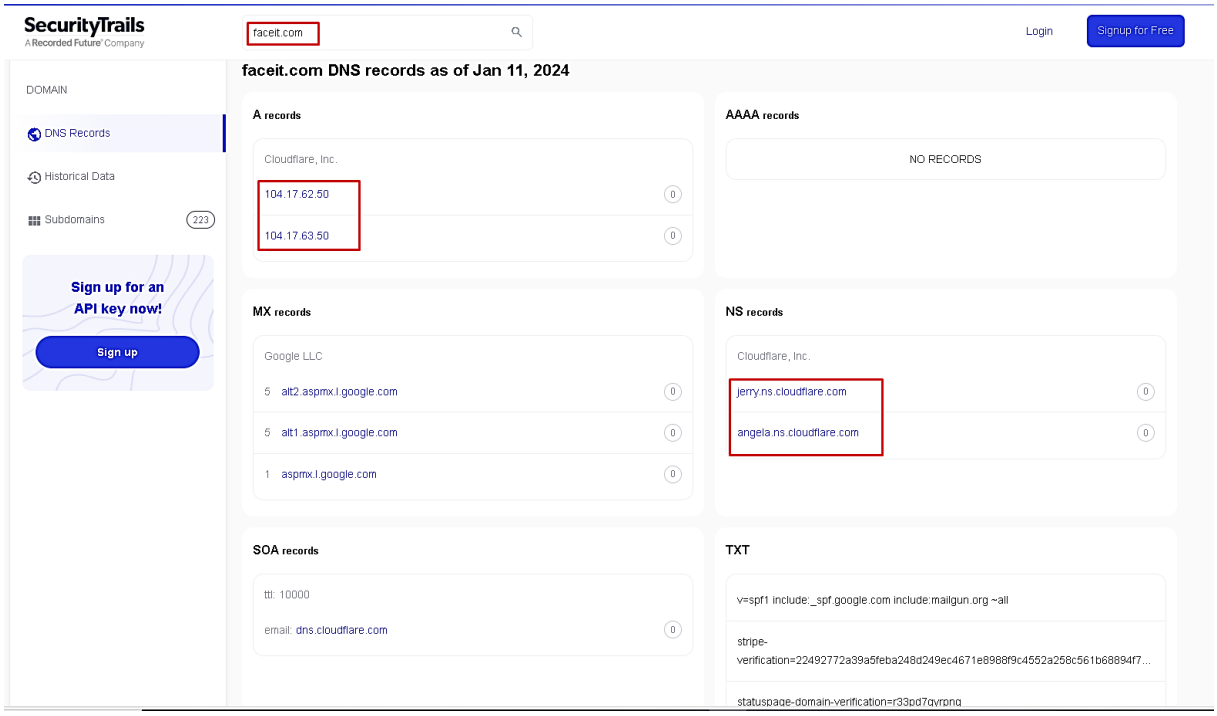
angela.ns.cloudflare.com.	108.162.192.65 angela.ns.cloudflare.com	CLOUDFLARENET United States
jerry.ns.cloudflare.com.	108.162.193.182 jerry.ns.cloudflare.com	CLOUDFLARENET United States

MX Records ** This is where email for the domain goes...

1 aspmx.l.google.com.	142.250.96.26 gg-in-f26.1e100.net	GOOGLE United States
5 alt1.aspmx.l.google.com.	142.250.112.26 ga-in-f26.1e100.net	GOOGLE United States
5 alt2.aspmx.l.google.com.	172.217.197.26 qa-in-f26.1e100.net	GOOGLE United States

Obraz 3.4.2 dane DNS domeny faceit.com, źródło dnsdumpster.com, data wykonania zrzutu 10.12.2023 r.

Z obrazu 3.5.1 można dowiedzieć się, jakie serwery DNS obsługują domenę faceit.com. Znaleziono 2 rekordy DNS i 3 rekordy MX i 1 rekord SOA.



Obraz 3.5.1 rekordy DNS domeny faceit.com, źródło securitytrails.com, data wykonania zrzutu 11.1.2024 r.

Z obrazów 3.6.1, 3.6.2 można dowiedzieć się, jakie serwery DNS obsługują domenę faceit.com. Znaleziono 2 serwery DNS.

DNS records

name	class	type	data	time to live
faceit.com	IN	HINFO	CPU: RFC8482 OS:	3600s (01:00:00)
faceit.com	IN	RRSIG	type covered: HINFO (13) algorithm: ECDSA Curve P-256 with SHA-256 (13) labels: 2 original ttl: 3600 (01:00:00) signature expiration: 2023-11-29 20:51:50Z signature inception: 2023-11-27 18:51:50Z key tag: 34505 signer's name: faceit.com signature: (512 bits) D4D6989AA1C53F0A7ACD2114E92C700F 9A405A8A2F1B1104B8628AA476232EBE 015797371C6F267C917F9B2FDF13C517 2334A0C7FD430C9FF174D285AC3CD677	3600s (01:00:00)
faceit.com	IN	NS	jerry.ns.cloudflare.com	86400s (1.00:00:00)
faceit.com	IN	NS	angela.ns.cloudflare.com	86400s (1.00:00:00)
50.63.17.104.in-addr.arpa	IN	HINFO	CPU: RFC8482 OS:	3600s (01:00:00)
17.104.in-addr.arpa	IN	NS	cruz.ns.cloudflare.com	4686s (01:18:06)
17.104.in-addr.arpa	IN	NS	kevin.ns.cloudflare.com	4686s (01:18:06)

-- end --

Obraz 3.6.1 rekordy DNS domeny faceit.com, źródło centralops.net, data wykonania zrzutu 12.12.2023 r.

faceit.com

Updated 5 days ago

Domain Information

Domain:	faceit.com
Registrar:	INWX GmbH
Registered On:	1996-06-27
Expires On:	2025-06-26
Updated On:	2023-09-20
Status:	clientTransferProhibited
Name Servers:	angela.ns.cloudflare.com jerry.ns.cloudflare.com

Registrant Contact

Country:	GB

Obraz 3.6.2 dane domeny faceit.com, źródło whois.com/whois/faceit.com, data wykonania zrzutu 12.12.2023 r.

Z obrazu 3.6.3 można dowiedzieć się, jakie serwery DNS obsługują domenę faceit.com. Znaleziono 2 serwery DNS i 3 rekordy MX i 1 rekord SOA.

Obraz 3.6.3 rekordy DNS domeny faceit.com, źródło shodan.io, data wykonania zrzutu 15.1.2024 r.

Z obrazów 3.6.4, 3.6.5 można dowiedzieć się, jakie serwery DNS obsługują domenę faceit.com (za hosting odpowiada Cloudflare). Dla każdego obrazu znaleziono te same serwery DNS. Większość z kluczowych pól jest zredagowana ze względu na prywatność. Data wygaśnięcia rejestracji nazwy domenowej przypada na połowę 2025 r., co można wykorzystać do przejęcia nazwy w przypadku braku przedłużenia przez obecnego właściciela.

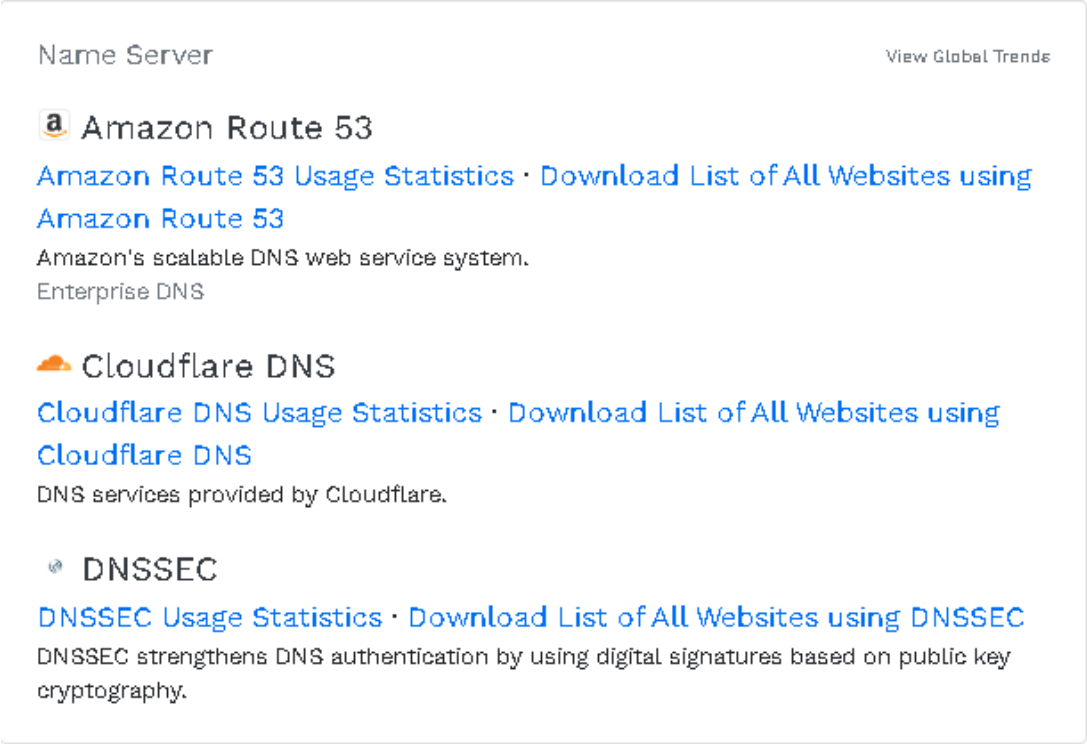
```
Registrar Registration Expiration Date: 2025-06-26T04:00:00Z
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: GB
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Name Server: jerry.ns.cloudflare.com
Name Server: angela.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: https://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-11-23T03:02:31Z <<<
```

Obraz 3.6.4 dane DNS domeny faceit.com, źródło whois.com/whois/faceit.com, data wykonania zrzutu 12.12.2023 r.

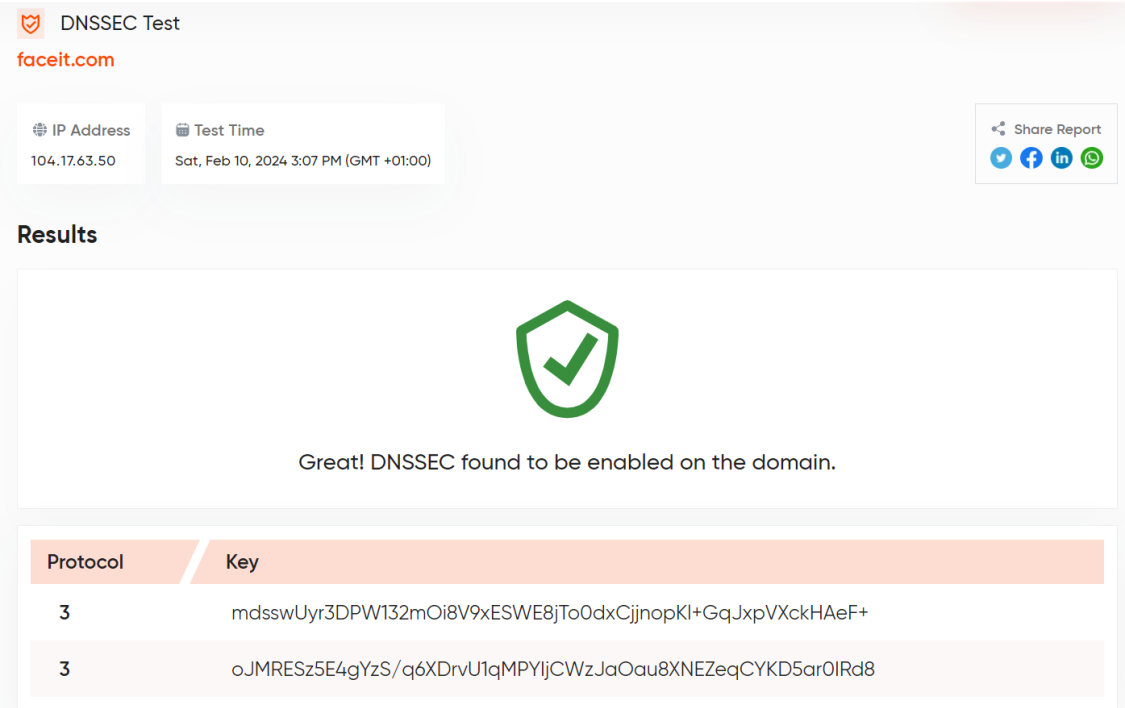
```
Name Server: jerry.ns.cloudflare.com
Name Server: angela.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: https://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-11-28T19:51:50Z <<<
```

Obraz 3.6.5 dane DNS domeny faceit.com, źródło centralops.net, data wykonania zrzutu 12.12.2023 r.

Z obrazów 3.7.1, 3.7.2 można dowiedzieć się, że serwery DNS obsługujące domenę faceit.com korzystają z zabezpieczeń DNSSEC (co chroni przed atakami DNS spoofing i DNS cache poisoning).



Obraz 3.7.1 dane DNS domeny faceit.com, źródło builtwith.com, data wykonania zrzutu 11.1.2024 r.

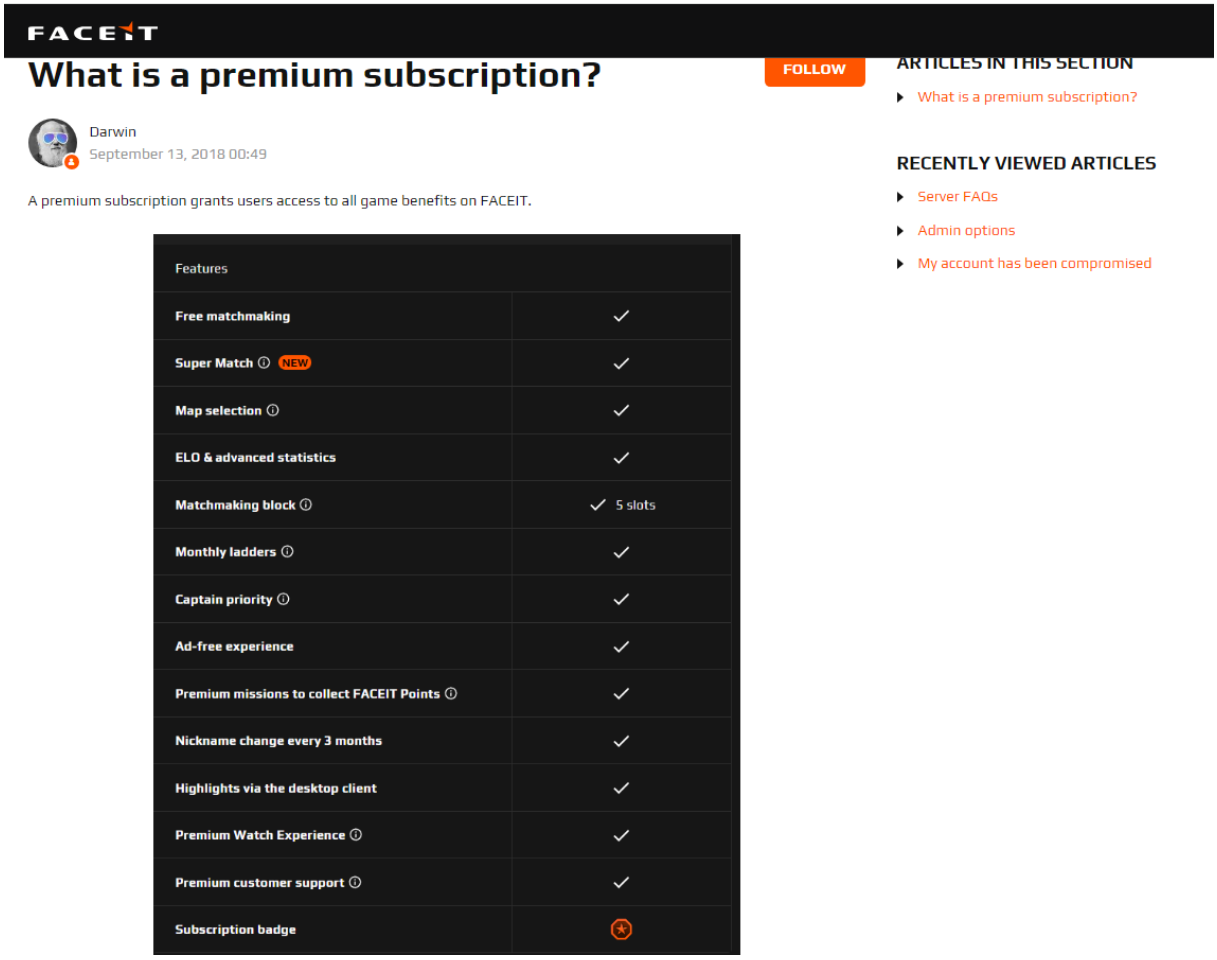


Obraz 3.7.2 wynik sprawdzenia rozszerzenia DNSSEC domeny faceit.com, źródło domsignal.com, data wykonania zrzutu 10.2.2024 r.

Do zebrania danych wykorzystano narzędzia dig, nslookup i strony dnsdumpster.com, dnslytics.com, centralops.net, whois.com, ipinfo.io, builtwith.com, shodan.io, securitytrails.com. Informacje dotyczące serwerów DNS zostały potwierdzone przez kilka narzędzi webowych i desktopowych, i nie wykazują rozbieżności między sobą. Serwery Cloudflare korzystają z zabezpieczeń DNNSEC. Domena jest obsługiwana przez 2 serwery DNS (hosting Cloudflare). Większość kluczowych informacji nie jest dostępna do odczytu z bazy Whois.

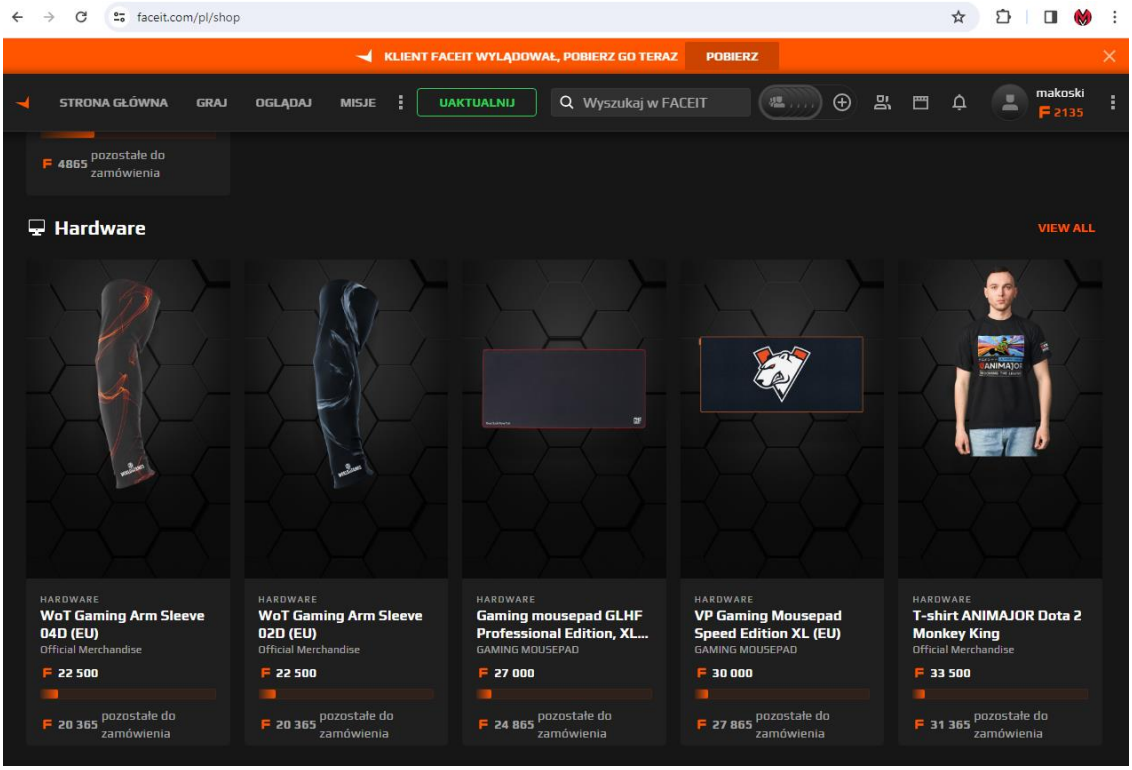
4. Ogólne dane dotyczące witryny domeny

Na obrazie 4.1.1 zaprezentowano korzyści płynące z zapisu do listy subskrypcyjnej dostępnej na witrynie. Subskrypcja umożliwia dostęp do zaawansowanych statystyk graczy, wybór mapy w grze (co może przynieść znaczące korzyści dla użytkownika). Jest to jedna z form dochodu organizacji.



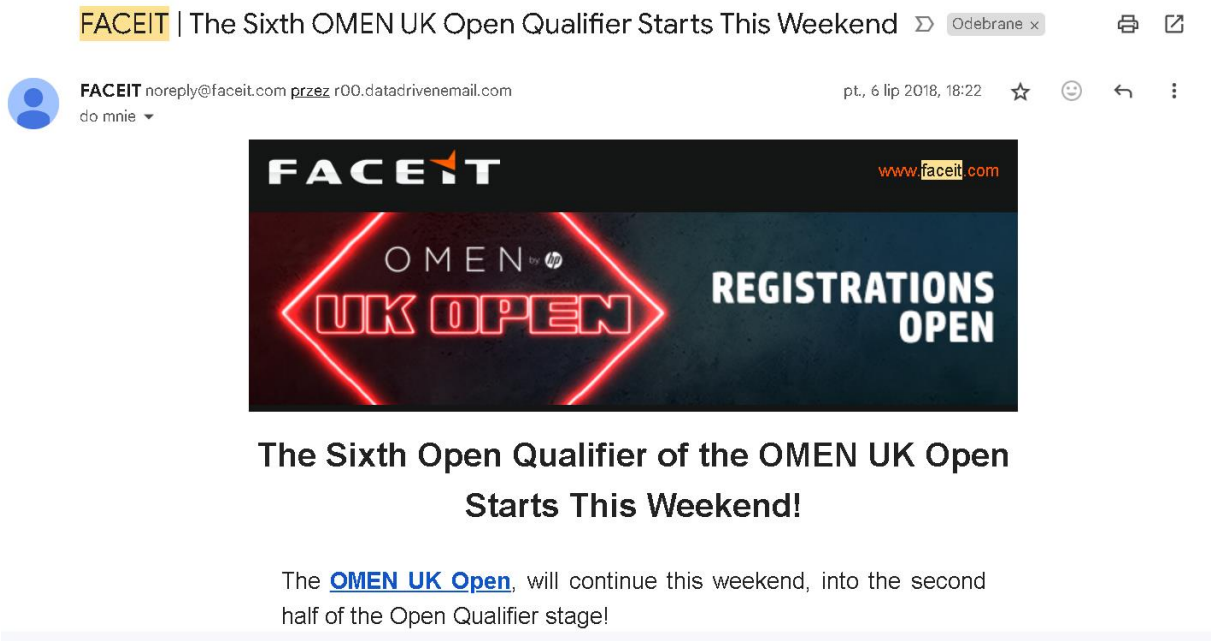
Obraz 4.1.1 lista subskrypcyjna witryny, źródło faceit.com, data wykonania zrzutu 5.12.2023 r.

Na obrazie 4.1.2 przedstawiono wygląd sklepu dostępnego na witrynie faceit. Waluta faceit może posłużyć do zakupu rzeczywistych przedmiotów (np. koszulki, sprzęt komputerowy, skórki). Użytkownik wygrywając turnieje zdobywa walutę, która może zamienić na rzeczywiste przedmioty. Organizacja w ten sposób zachęca użytkowników do spędzania jak największej liczby godzin na stronie faceit, co zwiększa jej ruch (może to służyć jako argument w negocjacjach z partnerami biznesowymi lub jako forma promocji) i przychody z reklam.



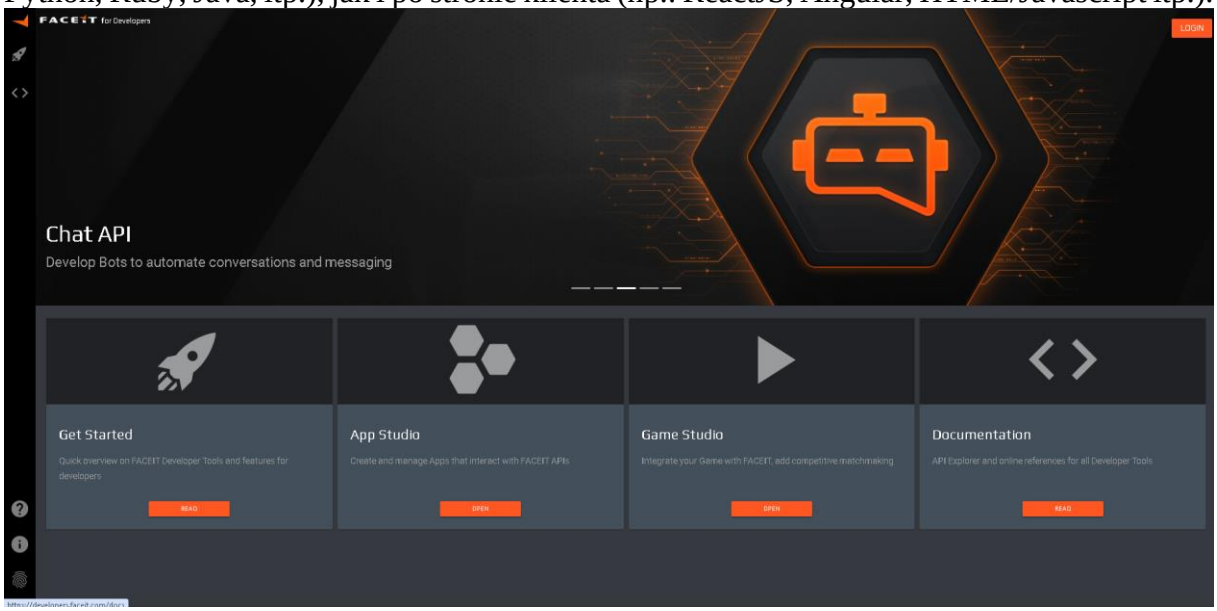
Obraz 4.1.2 sklep witryny, źródło faceit.com, data wykonania zrzutu 5.12.2023 r.

Na obrazie 4.1.3 przedstawiono wiadomość email otrzymaną od newslettera faceit. Informacje przekazywane przez newsletter zachęcają użytkowników do udziału w turniejach i zdobywania nagród w postaci wirtualnych skórek. Newsletter promuje także turnieje orgaznizowane dla profesjonalnych graczy i zachęca użytkowników do zakupu biletów na turnieje.



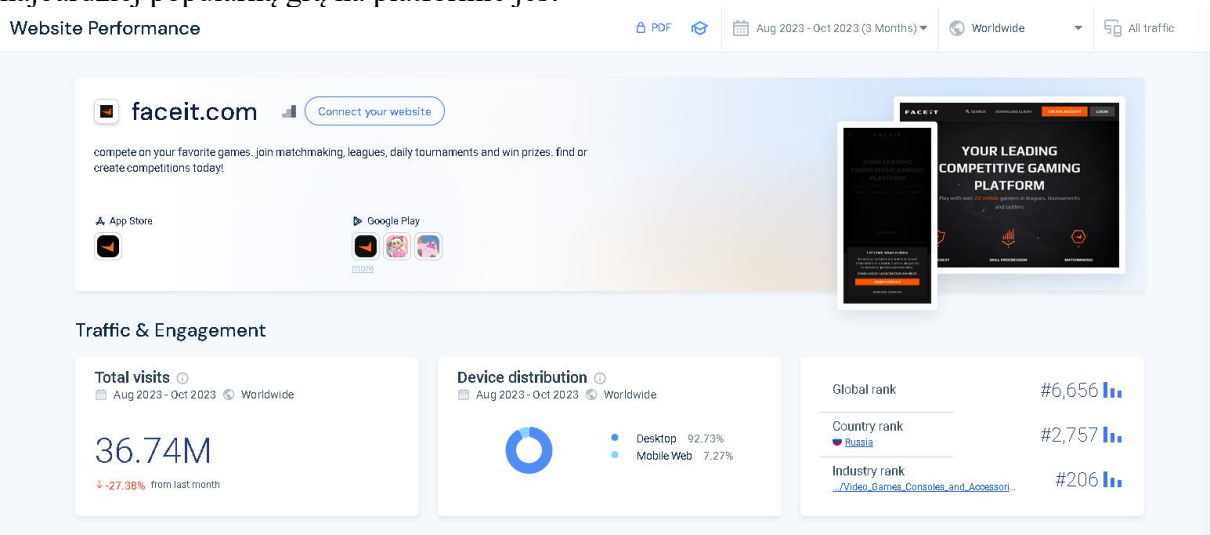
Obraz 4.1.3 wiadomość newsletter'a faceit, źródło gmail, data wykonania zrzutu 5.12.2023 r.

Witryna posiada interfejs dla developerów (obraz 4.1.4) umożliwiający tworzenie aplikacji, które wykorzystują dane Faceit i pozwalają na interakcje z graczami. Każda aplikacja może umożliwiać dostęp do interfejsów API danych, OAuth2, czatu. FACEIT Developer Tools współpracuje zarówno z technologiami i językami po stronie serwera (np.: Go Lang, NodeJS, Python, Ruby, Java, itp.), jak i po stronie klienta (np.: ReactJS, Angular, HTML/Javascript itp.).

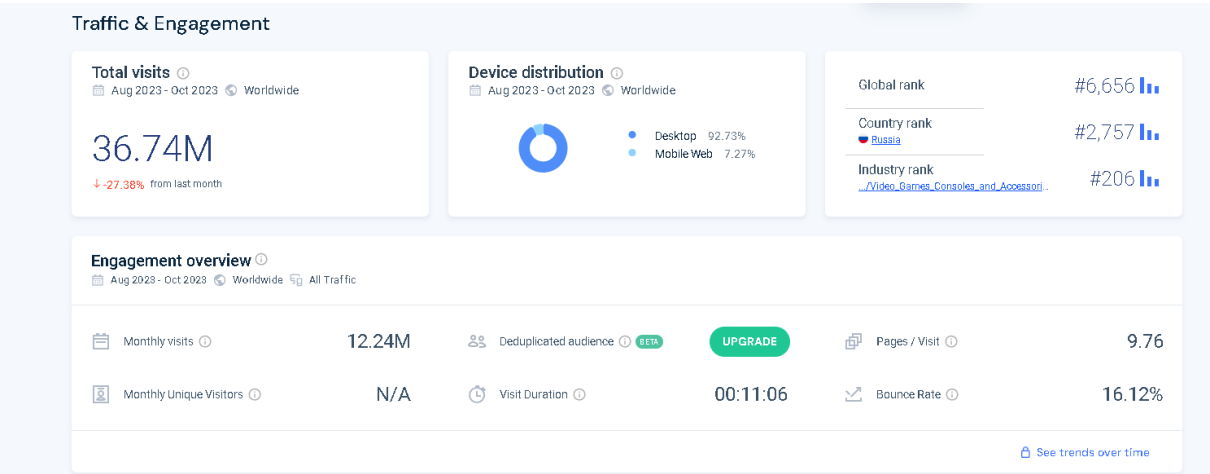


Obraz 4.1.4 interfejs dla developerów, źródło faceit.com, data wykonania zrzutu 10. 2.2024 r.

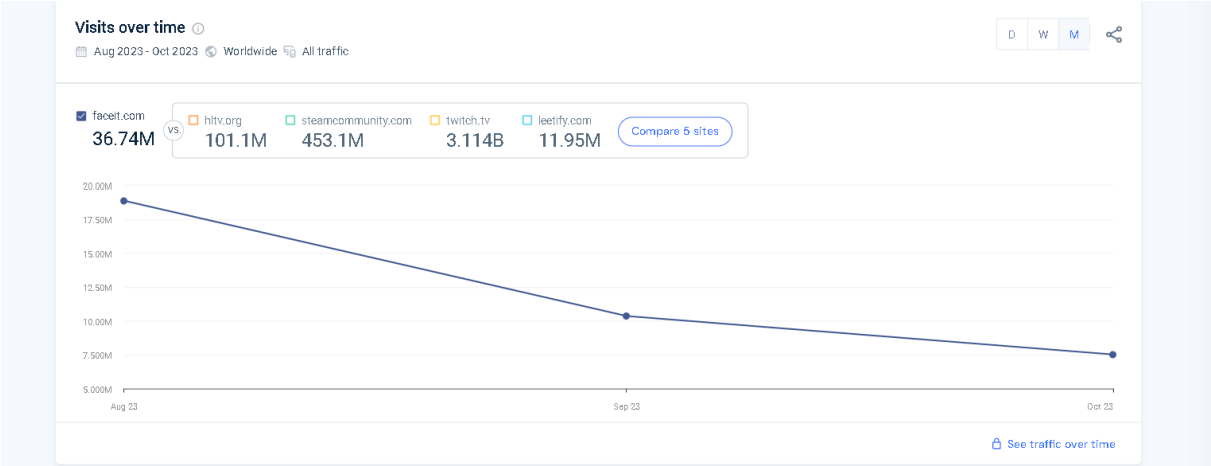
Z obrazów 4.2.1-4.2.8 można odczytać całkowitą liczbę wizyt na witrynie, udział urządzeń mobilnych/stacjonarnych w ruchu sieciowym, źródła pobrania aplikacji stacjonarnej, miejsce w światowym rankingu, czas trwania przebywania na stronie. Najwięcej odwiedzających stronę przypada na Rosję, na 3 miejscu jest Polska. Największy udział w ruchu strony mają mężczyźni poniżej 24 roku (prawie 40% całkowitego ruchu). Z danych statystycznych wynika, że najbardziej popularną grą na platformie jest



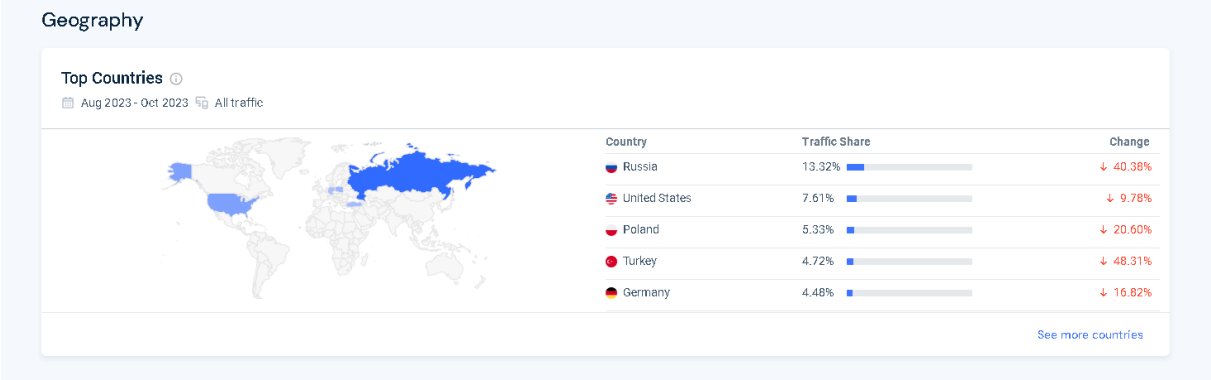
Obraz 4.2.1 dane statystyczne dotyczące odwiedzin witryny, źródło pro.similarweb.com, data wykonania zrzutu 15.12.2023 r.



Obraz 4.2.2 dane statystyczne dotyczące odwiedzin witryny, źródło pro.similarweb.com, data wykonania zrzutu 15.12.2023 r.

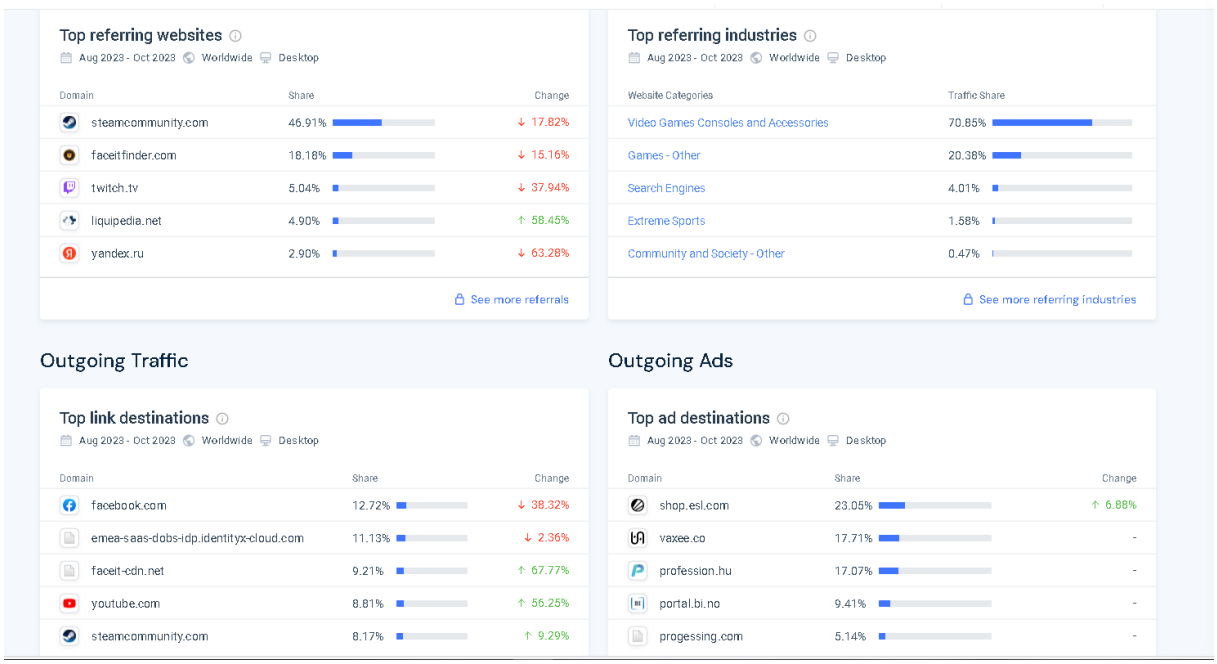


Obraz 4.2.3 dane statystyczne dotyczące odwiedzin witryny w czasie, źródło pro.similarweb.com, data wykonania zrzutu 15.12.2023 r.



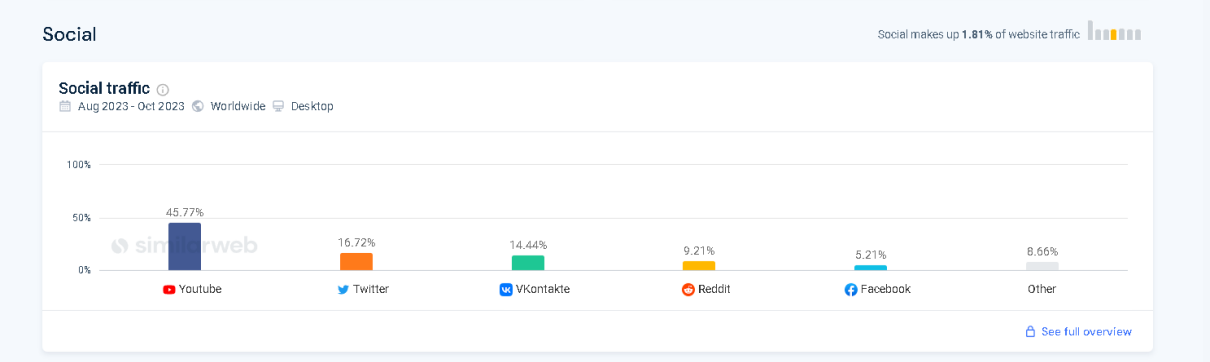
Obraz 4.2.4 procentowy udział odwiedzin witryny podzielony na narodowości odwiedzających, źródło pro.similarweb.com, data wykonania zrzutu 15.12.2023 r.

Na obrazie 4.2.5 zaprezentowano m.in. najczęściej występujące linki do zewnętrznych domen, najczęściej reklamy prowadzące do wskazanych domen, najczęściej wyszukiwane typy przedsiębiorstw.

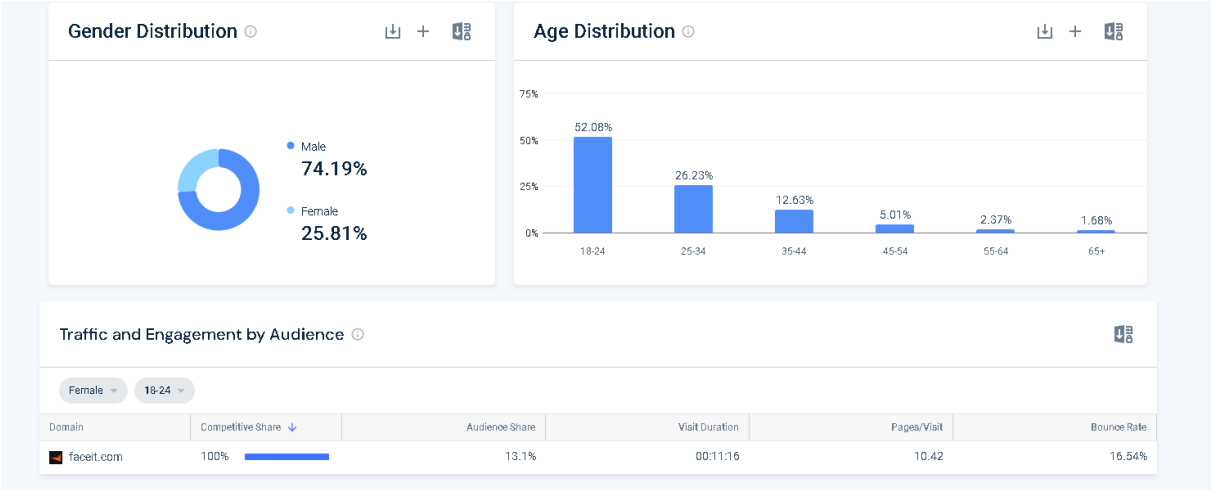


Obraz 4.2.5 dane statystyczne witryny takie jak przekierowania z reklam, źródło pro.similarweb.com, data wykonania zrzutu 15.12.2023 r.

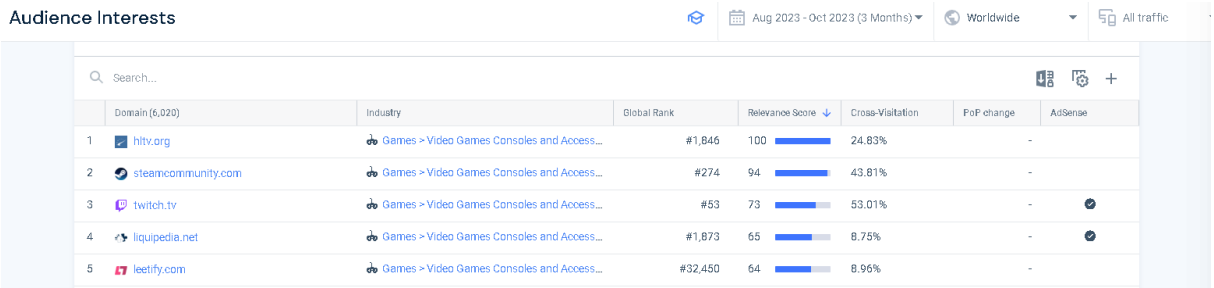
Na obrazie 4.2.6 zaprezentowano najczęściej odwiedzane social-media z witryny faceit (którymi są YouTube – kanał posiada 430 tyś subskrybentów i Twitter – blisko 300 tyś obserwujących).



Obraz 4.2.6 rozkład odwiedzanych social-media witryny, źródło pro.similarweb.com, data wykonania zrzutu 15.12.2023 r.



Obraz 4.2.7 podział na grupy wiekowe/płeć odwiedzających witrynę, źródło pro.similarweb.com, data wykonania zrzutu 15.12.2023 r.



Obraz 4.2.8 zainteresowania odwiedzających witrynę, źródło pro.similarweb.com, data wykonania zrzutu 15.12.2023 r.

Obraz 4.3.1 wskazuje na to, że domena cieszyła się największym zainteresowaniem w roku 2017. Od końca roku 2018 można zauważyć stabilizację ruchu domeny i nawet niewielki spadek przypadający na rok 2023.

Obraz 4.3.1 źródło semrush.com, data wykonania zrzutu 11.2.2024 r.

Z obrazu 4.3.2 można wnioskować, że najpopularniejszą grą platformy jest CS:GO (obecnie jest to prawdopodobnie CS:GO 2, jako następca CS:GO, co nie zostało jeszcze uwzględnione w trendach).

Organic Search Positions 11,934 — + Add to keyword list | Manage columns 11/16 | Export

Keyword	Intent	Position	SF	Traffic	Traffi...	Volume	KD %	URL	SERP	Updated
faceit	N	1	7	32.4K	58.26	40.5K	81	www.faceit.com/		1 day
face it	N	1	5	3.5K	6.32	4.4K	78	www.faceit.com/		3 days
faceit csgo	N	1	6	2.3K	4.17	2.9K	34	www.faceit.com/		Feb 05
faceit	N		7	1.3K	2.25	40.5K	81	www.faceit.com/		1 day
афсув	N	1	3	1K	1.87	1.3K	24	www.faceit.com/ru		1 day
faciet	N	1	8	704	1.26	880	77	www.faceit.com/		2 days
face it csgo	N	1	6	472	0.84	590	36	www.faceit.com/		Jan 29

Obraz 4.3.2 źródło semrush.com, data wykonania zrzutu 11.2.2024 r.

Z obrazu 4.3.3 wynika, że najczęściej żądanym typem danych jest typ text i podtyp html.

host faceit.com

Indexed on May 31, 2023.

Saved **4361 times** between December 27, 1996 and November 28, 2023.

MIME-types: Any MIME-types | Year Start: 1996 | Year End: 2023

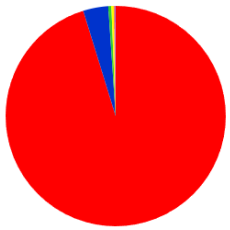
All | text | image | application | video

Summary on MIME-types Count

Quick search on MIME-types... << < 1 2 > >>

	Captures	URLs	New URLs
text/html	165 184	127 411	102 477
text/plain	6400	5270	5269
application/json	782	8	2
image/gif	582	555	457
image/jpeg	224	190	157
image/vnd.microsoft.icon	129	11	1
image/png	52	50	50
application/javascript	45	45	44
text/css	26	9	5
application/octet-stream	7	7	7

Captures



Explore faceit.com URLs

Obraz 4.3.3 źródło archive.org, data wykonania zrzutu 8.12.2023 r.

W zbieraniu danych do rozdziału 4 skorzystano z narzędzi takich jak semrush.com, archive.org pro.similarweb.com, a także usług dostępnych na stronie faceit.com. które przedstawiłem na rysunkach 4.2.1. Witryna świadczy usługi sklepu, zapisu na listy subskrypcyjne, newsletter i narzędzia dla developerów. W rozdziale przedstawiono dane statystyczne dotyczące popularności, intensywności modyfikacji. Największy odsetek ruch witryny stanowią mężczyźni w wieku 15-24, którzy interesują się sektorem gier komputerowych. Ruch

pochodzący z urządzeń mobilnych stanowi około 7%, co może powodować, że organizacja nie będzie inwestowała w technologie mobilne.

5. Struktura domeny

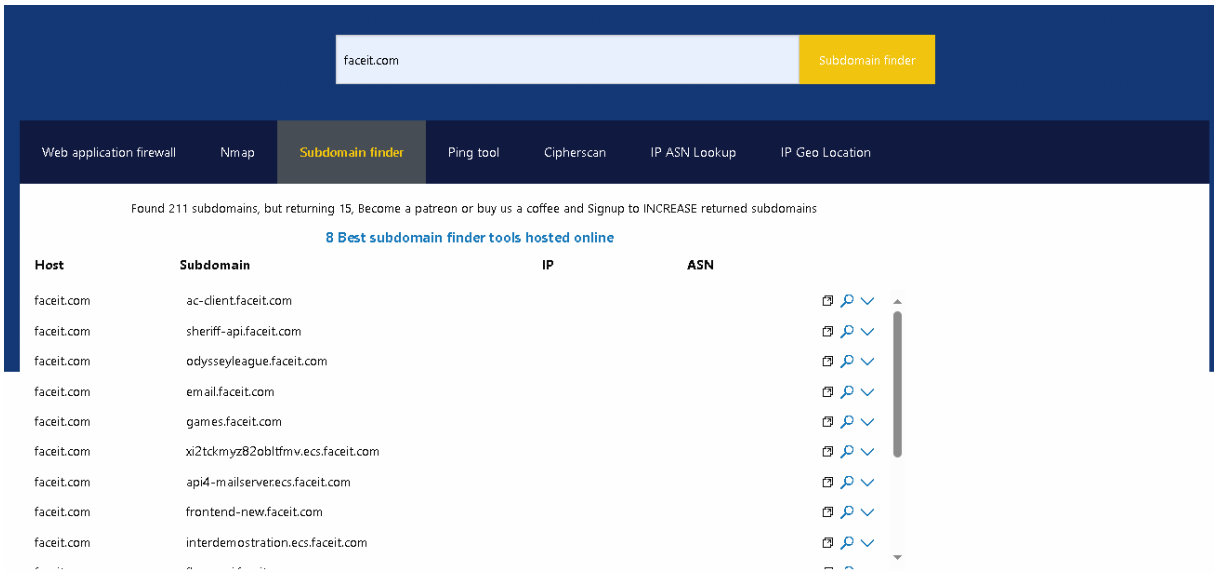
Na obrazie 5.1.1 przedstawiono część nazw poddomen domeny faceit.com. Po nazwach można wnioskować, że hosty obsługujące grę CS:GO znajdują w Europie Wschodniej, Azji Zachodniej.

Subdomains

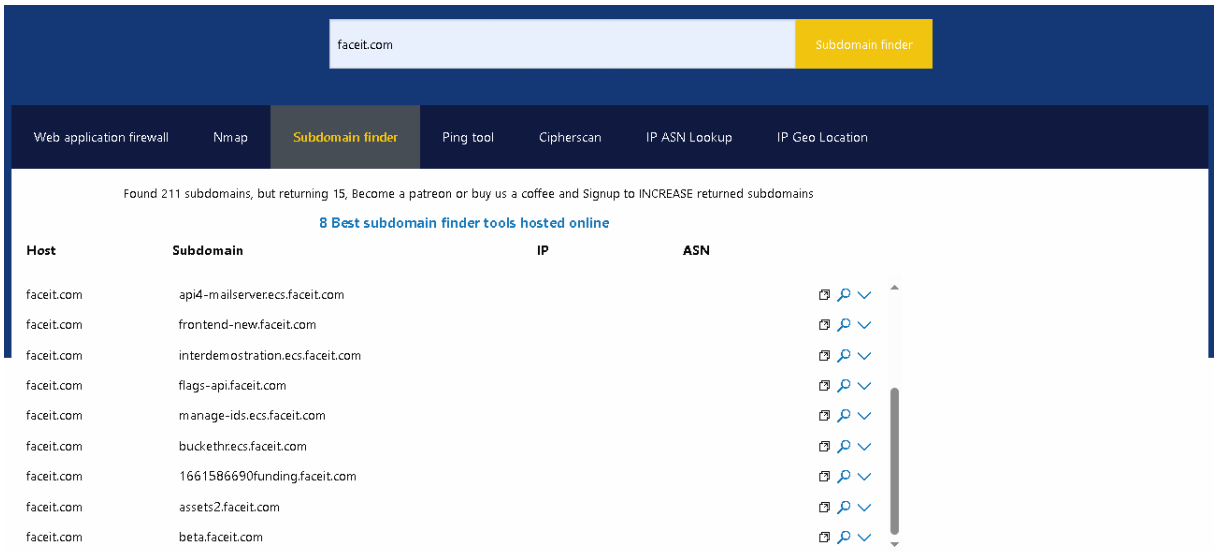
- _dmarc
- ac-api
- ac-api-external
- ac-backoffice
- ac-client
- ac-client-ws
- accounts
- achi
- ads
- advertise
- api
- backoffice
- beta
- blog
- cdn
- cdn-frontend
- chat-server
- corporate
- csgo-asia-east2-cluster
- csgo-europe-west1-cluster
- csgo-us-central1-cluster
- developers

Obraz 5.1.1 poddomeny domeny faceit.com, źródło shodan.io, data wykonania zrzutu 15.1.2024 r.

Na obrazach 5.2.1-5.2.2 przedstawiono nazwy poddomeny domeny faceit.com. Znaleziono domeny odpowiadające za mail, API.



Obraz 5.2.1 poddomeny domeny faceit.com, źródło nmmapper.com, data wykonania zrzutu 5.1.2024 r.



Obraz 5.2.2 poddomeny domeny faceit.com, źródło nmmapper.com, data wykonania zrzutu 5.1.2024 r.

Na obrazach 5.3.1-5.3.2 przedstawiono nazwy poddomeny domeny faceit.com (znaleziono 15 poddomen).

Hostnames matching faceit.com

▸ Search with another pattern?

15 results

Rank	Site	First seen	Netblock	OS	Site Report
1486	www.faceit.com	October 2014	Cloudflare, Inc.	Linux	
52100	accounts.faceit.com	July 2019	Cloudflare, Inc.	Linux	
76806	support.faceit.com	August 2016	Cloudflare, Inc.	Linux	
463235	clash.faceit.com	January 2023	Cloudflare, Inc.	Linux	
578142	cdn.faceit.com	Febuary 2016	Cloudflare, Inc.	Linux	
936171	faceit.com.ph	December 2022	Akamai Technologies, Inc.	unknown	
1116994	corporate.faceit.com	Febuary 2018	Cloudflare, Inc.	Linux	
1158287	drop-faceit.com	April 2023	Cloudflare, Inc.	Linux	

Obraz 5.3.1 poddomeny domeny faceit.com, źródło www.netcraft.com/solutions/other-solutions/internet-data-research/, data wykonania zrzutu 5.1.2024 r.

1168122	email.faceit.com	Febuary 2017	Google LLC	Linux	
1201757	esea-faceit.com	January 2023	Cloudflare, Inc.	unknown	
1205699	buff173-faceit.com	January 2023	Cloudflare, Inc.	unknown	
1209058	blast-premier-faceit.com	January 2023	Cloudflare, Inc.	unknown	
1289501	justice.faceit.com	Febuary 2020	Cloudflare, Inc.	Linux	
1455814	blastpremier-faceit.com		Cloudflare, Inc.	unknown	
1468071	faceit.com.pe	November 2022	Cloudflare, Inc.	unknown	

Obraz 5.3.2 poddomeny domeny faceit.com, źródło www.netcraft.com/solutions/other-solutions/internet-data-research/, data wykonania zrzutu 5.1.2024 r.

Na obrazie 5.4.1 przedstawiono nazwy poddomeny domeny faceit.com (znaleziono 10 poddomen). Nazwy często nawiązują do gier wspieranych na platformie. Największy ruch generuje strona www.faceit.com.

Organic Traffic Research

.domain.com/ | faceit.com | ANALYZE | ADD TO PROJECT | Data for: December 2023 | Currency: € EUR

Keywords | Ranking changes | Competitors | Competitor comparison | Traffic distribution by country | Pages | Subdomains

Search | FILTER | EXPORT

URL (18)	TRAFFIC SHARE	TOTAL TRAFFIC	TOTAL TRAFFIC COST	KEYWORDS TOTAL
www.faceit.com	96.21%	53.79K	€32.7K	24.46K
support.faceit.com	3.11%	1.74K	€9.45	3.75K
pro.faceit.com	0.38%	213	€5.57	664
replay.faceit.com	0.14%	76	€0.11	502
corporate.faceit.com	0.09%	51	€0.1	136
verify.faceit.com	0.03%	14	€0	51
r6collegiate.faceit.com	0.01%	8	€0	189
blog.faceit.com	0.01%	7	€0.05	396
accounts.faceit.com	0.01%	3	€0	3
clash.faceit.com	0.01%	3	€4.48	30

Obraz 5.4.1 poddomeny domeny faceit.com, źródło online.seranking.com, data wykonania zrzutu 5.1.2024 r.

Na obrazach 5.5.1-5.5.3 przedstawiono nazwy poddomeny domeny faceit.com.

Result of faceit.com

https://subdomainfinder.c99.nl/scans/2023-12-11/faceit.com

Scan date 2023-12-11 07:06:14
Domain Country: Worldwide (COM)
Subdomains found: 215
Most used IP: 104.17.62.50 (32x)

Whois Check | Check Status | Copy to clipboard | Download CSV | Download JSON

Subdomain	IP	Cloudflare
ac-api-external.faceit.com	104.17.62.50	
ac-api.faceit.com	104.17.63.50	
ac-backoffice.faceit.com	34.111.130.146	
ac-client-ws.faceit.com	104.17.62.50	
ac-client.faceit.com	34.102.217.190	
accounts.faceit.com	104.17.62.50	
achi.faceit.com	34.85.244.91	
ads.faceit.com	104.17.62.50	
advertise.faceit.com	104.17.62.50	
api.faceit.com	104.17.62.50	
backoffice.faceit.com	104.17.62.50	
beta.faceit.com	104.17.62.50	
blog.faceit.com	162.159.152.4	
corporate.faceit.com	162.159.135.42	
csgo-asia-east2-cluster.faceit.com	104.17.62.50	
csgo-europe-west1-cluster.faceit.com	104.17.63.50	

Obraz 5.5.1 poddomeny domeny faceit.com, źródło subdomainfinder.c99.nl, data wykonania zrzutu 11.12.2023 r.

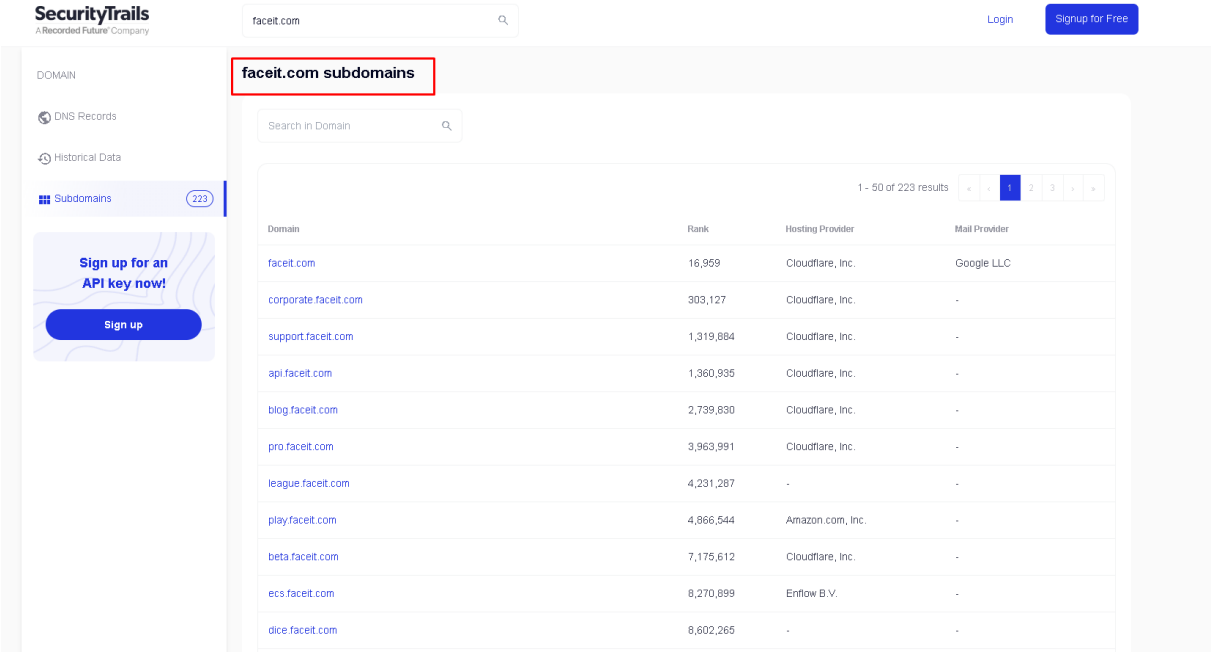
csgo-us-central1-cluster.faceit.com	104.17.62.50
developers.faceit.com	104.17.62.50
dota-bridge-web.faceit.com	104.17.62.50
ea-integration.faceit.com	104.17.62.50
ecs.faceit.com	89.106.200.1
edge.faceit.com	104.17.62.50
email.faceit.com	34.110.180.34
facebot-master.faceit.com	104.17.62.50
flick.faceit.com	89.106.200.1
fugly.faceit.com	104.17.62.50
game-integration.faceit.com	104.17.62.50
games.faceit.com	104.17.62.50
gwb.faceit.com	162.159.134.42
internal-frontend.faceit.com	10.136.0.10
justice.faceit.com	104.17.62.50
labs.faceit.com	104.17.62.50
labsportal.faceit.com	104.17.62.50
links.faceit.com	199.36.158.100
lol-integration.faceit.com	104.17.62.50
nino-blast-copenhagen-europe-west4-a-worker.faceit.com	34.90.86.4
nino-blast-copenhagen-europe-west4-b-worker.faceit.com	34.91.113.127
nino-red-bull-flick-helsinki-europe-north1-a-worker.faceit.com	34.88.158.250
nino-red-bull-flick-helsinki-europe-north1-b-worker.faceit.com	34.88.231.17
odysseyleague.faceit.com	89.106.200.1
open.faceit.com	104.17.62.50
ow2-integration.faceit.com	104.17.62.50

Obraz 5.5.2 poddomeny domeny faceit.com, źródło subdomainfinder.c99.nl, data wykonania zrzutu 11.12.2023 r.

payments-gateway.faceit.com	104.17.62.50
pro.faceit.com	162.159.134.42
r6collegiate.faceit.com	162.159.135.42
rainbow6.faceit.com	89.106.200.1
redbull-cms.faceit.com	104.17.62.50
redbullmeo.faceit.com	89.106.200.1
smite-integration.faceit.com	104.17.62.50
support.faceit.com	104.16.51.111
telekom-survey.faceit.com	168.119.247.17
upload-api.faceit.com	104.17.62.50
verify.faceit.com	162.159.134.42
vod-highlights.faceit.com	212.102.56.182
voice-callback.faceit.com	104.17.62.50
widgets.faceit.com	104.17.62.50
wot-integration.faceit.com	104.17.62.50
www.faceit.com	104.17.62.50

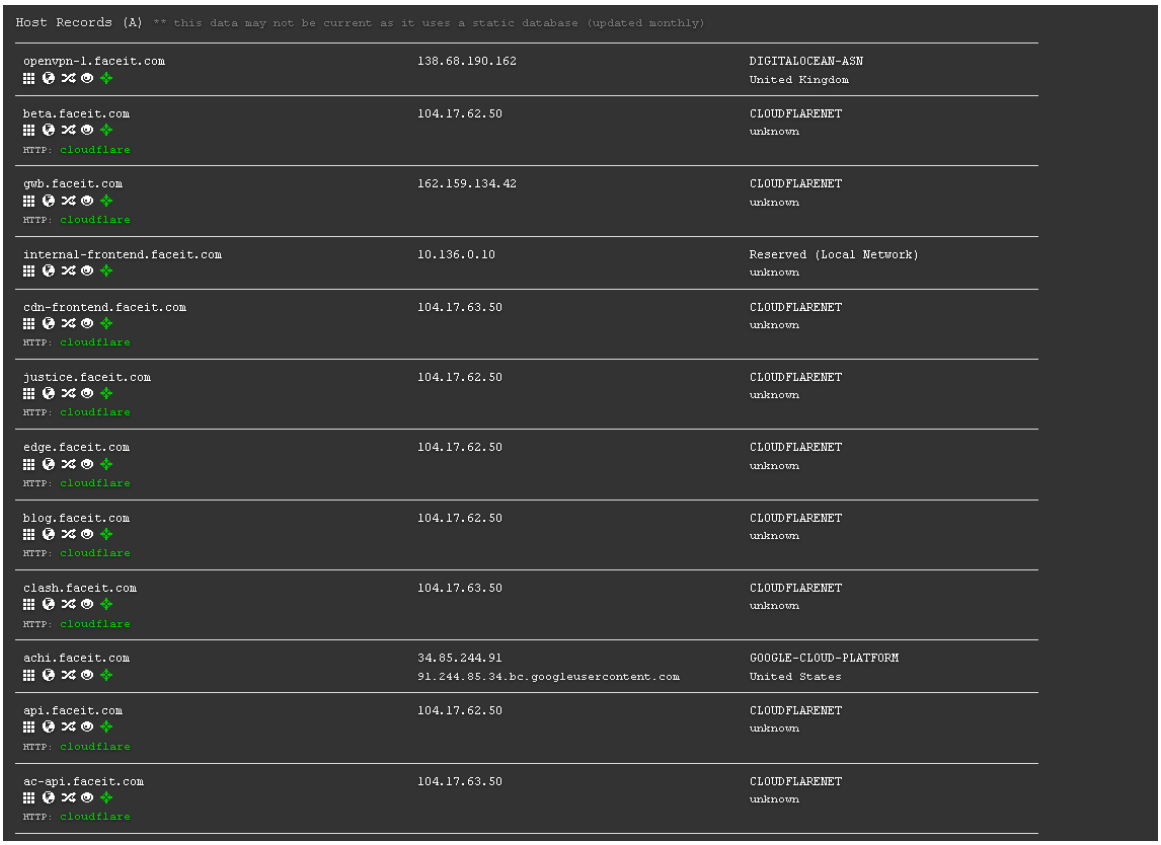
Obraz 5.5.3 poddomeny domeny faceit.com, źródło subdomainfinder.c99.nl, data wykonania zrzutu 11.12.2023 r.

Na obrazie 5.6.1 przedstawiono nazwy poddomeny domeny faceit.com (znaleziono 15 poddomen). Dostawcami hostingu są Cloudflare i Enflow, Amazon.



Obraz 5.6.1 poddomeny domeny faceit.com, źródło securitytrails.com, data wykonania zrzutu 11.1.2024 r.

Na obrazach 5.7.1-5.7.4 przedstawiono nazwy poddomeny domeny faceit.com. Dostawcami hostingu są Cloudflare i DigitalOcean, Google.



Obraz 5.7.1 poddomeny domeny faceit.com, źródło dnsdumpster.com, data wykonania zrzutu 10.12.2023 r.

ac-api.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
upload-api.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
match-api.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
fulfillment-api.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
labsportal.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
telekom.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
cdn.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
open.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
ea-integration.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
game-integration.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
smite-integration.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
lol-integration.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
wot-integration.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown

Obraz 5.7.2 poddomeny domeny faceit.com, źródło dnsdumpster.com, data wykonania zrzutu 10.12.2023 r.

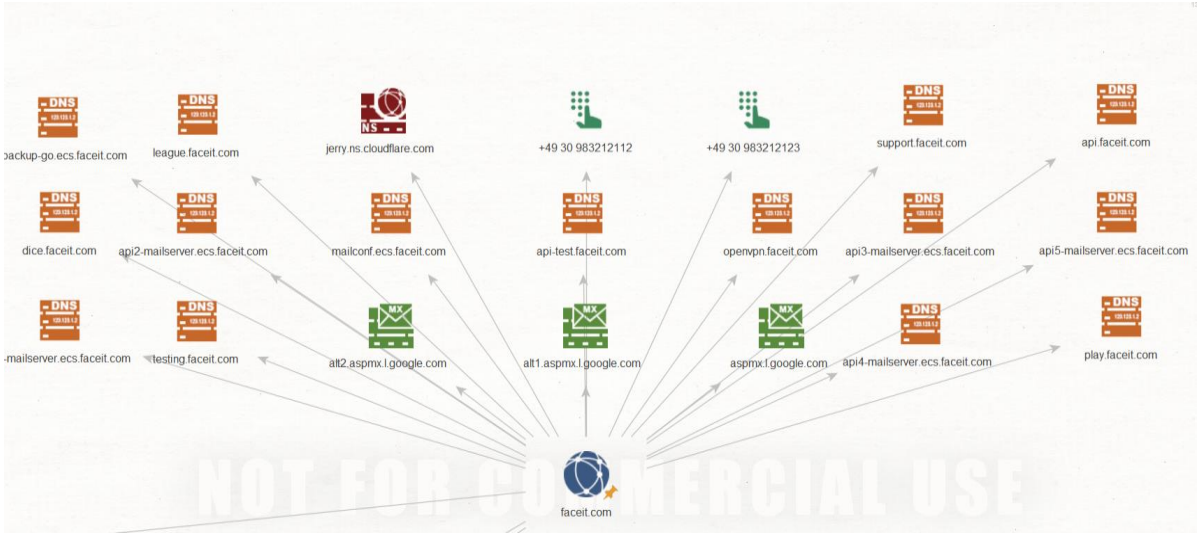
wot-integration.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
nino-red-bull-flick-helsinki-europe-northl-a-worker.faceit.com SSH: SSH-2.0-OpenSSH_7.4	34.88.158.250 250.158.88.34.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM Finland
nino-blast-copenhagen-europe-west4-a-worker.faceit.com SSH: SSH-2.0-OpenSSH_7.4	34.90.86.4 4.86.90.34.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM Netherlands
nino-red-bull-flick-helsinki-europe-northl-b-worker.faceit.com SSH: SSH-2.0-OpenSSH_7.4	34.88.231.17 17.231.88.34.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM Finland
nino-blast-copenhagen-europe-west4-b-worker.faceit.com SSH: SSH-2.0-OpenSSH_7.4	34.91.113.127 127.113.91.34.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM Netherlands
facebot-master.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
csgo-us-centrall-cluster.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
csgo-europe-westl-cluster.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
csgo-asia-east2-cluster.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
chat-server.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
labs.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
games.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown

Obraz 5.7.3 poddomeny domeny faceit.com, źródło dnsdumpster.com, data wykonania zrzutu 10.12.2023 r.

links.faceit.com HTTP: Varnish	199.36.158.100	FASTLY United States
developers.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
widgets.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
accounts.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
ingame-accounts.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
ac-client-ws.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
ac-client.faceit.com	34.102.217.190 190.217.102.34.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM United States
o2.o5.sg.dev.faceit.com	168.245.51.106 o66.sendgrid.yourtravelmates.com	SENDGRID United States
www.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
api-nginx.faceit.com HTTP: cloudflare	104.17.62.50	CLOUDFLARENET unknown
payments-gateway.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown
verify.faceit.com HTTP: cloudflare	162.159.134.42	CLOUDFLARENET unknown
fugly.faceit.com HTTP: cloudflare	104.17.63.50	CLOUDFLARENET unknown

Obraz 5.7.4 poddomeny domeny faceit.com, źródło dnsdumpster.com, data wykonania zrzutu 10.12.2023 r.

Na obrazie 5.8.1 przedstawiono diagram struktury domeny faceit (w tym serwery DNS). Narzędzie wykryło 3 poddomeny google odpowiedzialne za obsługę poczty.



Obraz 5.8.1 poddomeny domeny faceit.com, narzędzie maltego, data wykonania zrzutu 18.1.2024 r.

Na obrazie 5.9.1 przedstawiono część wyników otrzymanych przy enumeracji nazw poddomen. Hosty ze znalezionymi adresami ip zostały umieszczone w tabeli 5.1.

```
[*] Hosts found: 403
---------------------
*.faceit.com
0.ecs.faceit.com
01.ecs.faceit.com
0teixzygx.ecs.faceit.com
1.ecs.faceit.com
11.ecs.faceit.com
2.ecs.faceit.com
21.ecs.faceit.com
23.ecs.faceit.com
24.ecs.faceit.com
3.ecs.faceit.com
31.ecs.faceit.com
4.ecs.faceit.com
41.ecs.faceit.com
467zudfingppnolue.ecs.faceit.com
5.ecs.faceit.com
51.ecs.faceit.com
6.ecs.faceit.com
7.ecs.faceit.com
7ghbts63.ecs.faceit.com
8.ecs.faceit.com
8ncuejmxmntd26h3io4.ecs.faceit.com
9.ecs.faceit.com
API count exceeded - Increase Quota with Membership176×215×237×247.faceit.com
:176.215.237.247
ac-api-external.faceit.com
ac-api.faceit.com
ac-backoffice.faceit.com
ac-client-ws.faceit.com
ac-client.faceit.com
accounts.faceit.com
accounts.faceit.com:104.17.62.50
accounts.faceit.com:104.17.63.50
achi-test.faceit.com
achi.faceit.com
achi.faceit.com:34.85.244.91
achi.faceit.com:anticheat-producer-api-prod-vpc.us-east-1.elasticbeanstalk.co
m
achi.faceit.com:anticheat-producer-api-prod-vpc.us-east-1.elasticbeanstalk.co
m.
admin0-monitoring.ecs.faceit.com
admin1-monitoring.ecs.faceit.com
admin2-monitoring.ecs.faceit.com
admin3-monitoring.ecs.faceit.com
admin4-monitoring.ecs.faceit.com
admin5-monitoring.ecs.faceit.com
admin6-monitoring.ecs.faceit.com
admin7-monitoring.ecs.faceit.com
```

Obraz 5.9.1 poddomeny domeny faceit.com zebrane przy użyciu narzędzia theHarvester, data wykonania zrzutu 15.1.2024 r.

Tabela 5.1 zawiera informacje zebrane za pomocą narzędzia theHarvester, zapisano w niej nazwy hostów i adresy IPv4 jeśli zostały znalezione.

Tabela 5.1. Znalezione poddomeny przy użyciu narzędzia theHarvester.	
Nazwa Hosta	Adres IPv4 [jeśli znaleziono]
176x215x237x247.faceit.com	176.215.237.247
achi.faceit.com	34.85.244.91
blog.faceit.com	162.159.153.4
core-api.faceit.com	35.245.83.99
corporate.faceit.com	35.197.239.16
gwb.faceit.com	162.159.134.42
ingame-accounts.faceit.com	

links.faceit.com	199.36.158.100
nino-blast-copenhagen-europe-west4-a-worker.faceit.com	34.90.86.4
nino-blast-copenhagen-europe-west4-b-worker.faceit.com	34.91.113.127
nino-red-bull-flick-helsinki-europe-north1-a-worker.faceit.com	34.88.158.250
nino-red-bull-flick-helsinki-europe-north1-b-worker.faceit.com	34.88.231.17
o1.sg.t.faceit.com	168.245.46.230
o2.o5.sg.dev.faceit.com	168.245.51.106
openvpn-1.faceit.com	138.68.190.162
phpmyadmin.ecs.faceit.com	
redbull-cms.faceit.com	
sheriff-api.faceit.com	
telekom-survey.faceit.com	168.119.247.17
verify.faceit.com	

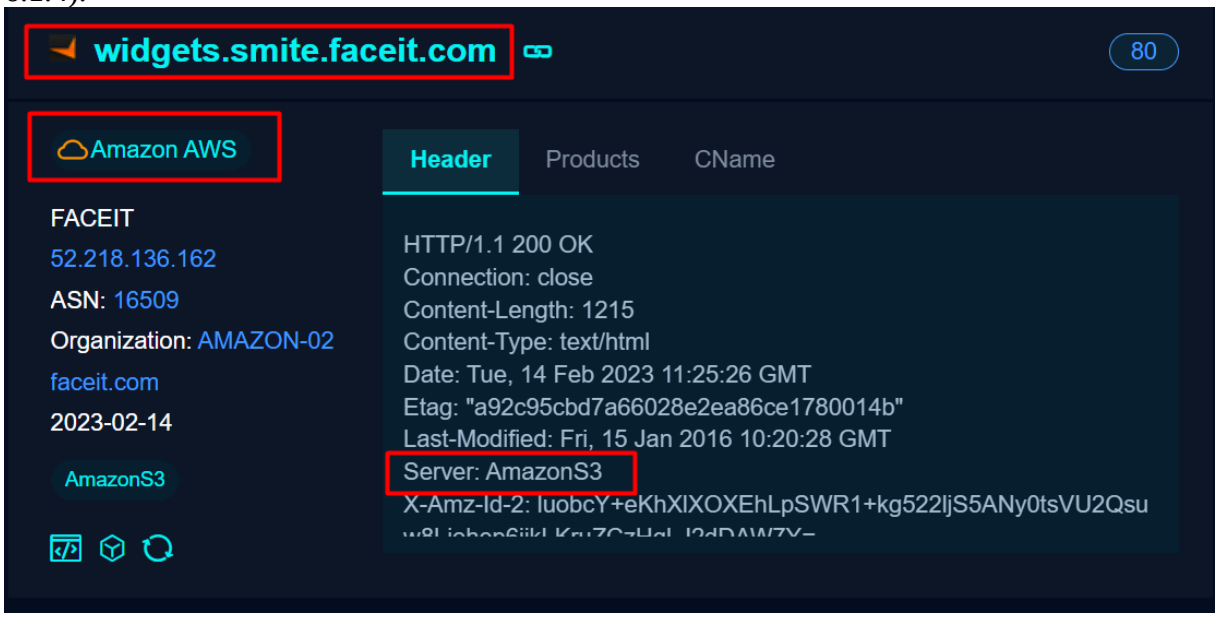
W zbieraniu danych do rozdziału 5 skorzystano z narzędzi takich jak theHarvester, maltego, subdomainfinder.c99.nl, online.seranking.com, nmmapper.com, shodan.io. Większość hostów domeny znajduje się w Stanach Zjednoczonych (San Francisco). Liczba znalezionych hostów w poddomenach wynosi ponad 400 (dane zdobyte przy użyciu theHarvester – wszystkich nie wymieniono). Dostawcami hostingu są Cloudflare, Google, DigitalOcean, Enflow, Amazon. Nazwy znalezionych hostów pochodzące z różnych narzędzi mają część wspólną.

6. Wykorzystywane systemy operacyjne, usługi sieciowe i aplikacje realizujące te usługi

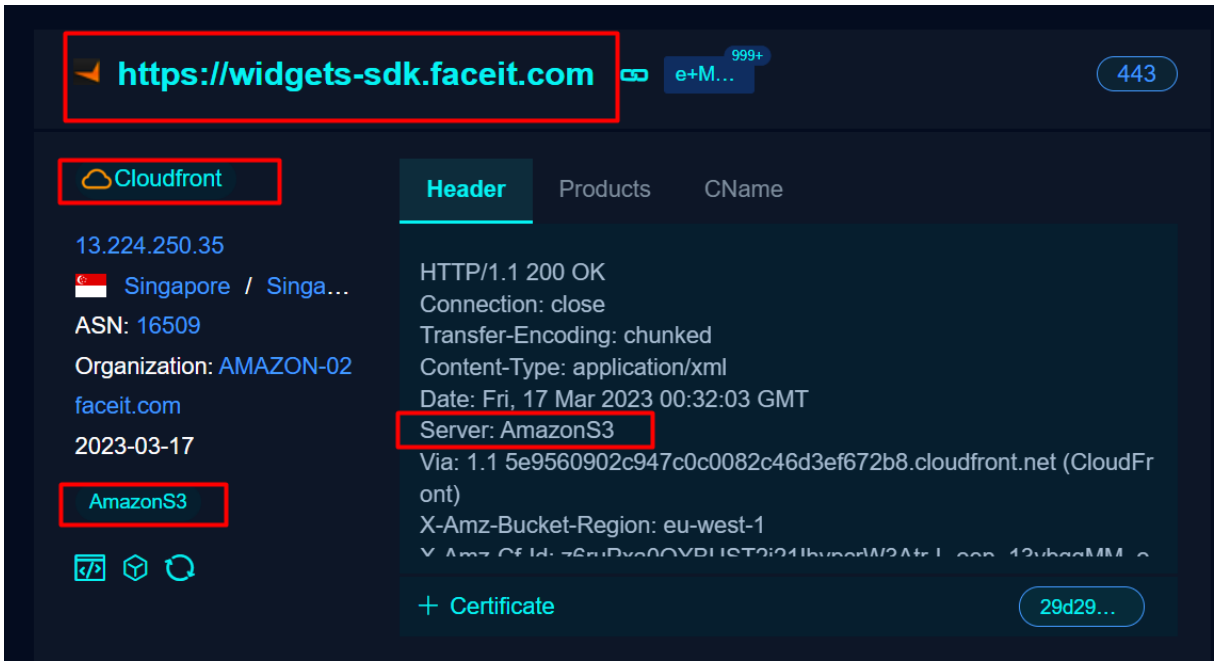
Strona znajduje się za chmurową usługą Cloudflare(obraz 6.1.1).

Obraz 6.1.1 rezultat sprawdzenia systemu operacyjnego serwera, źródło dnschecker.org, data wykonania zrzutu 17.1.2024 r.

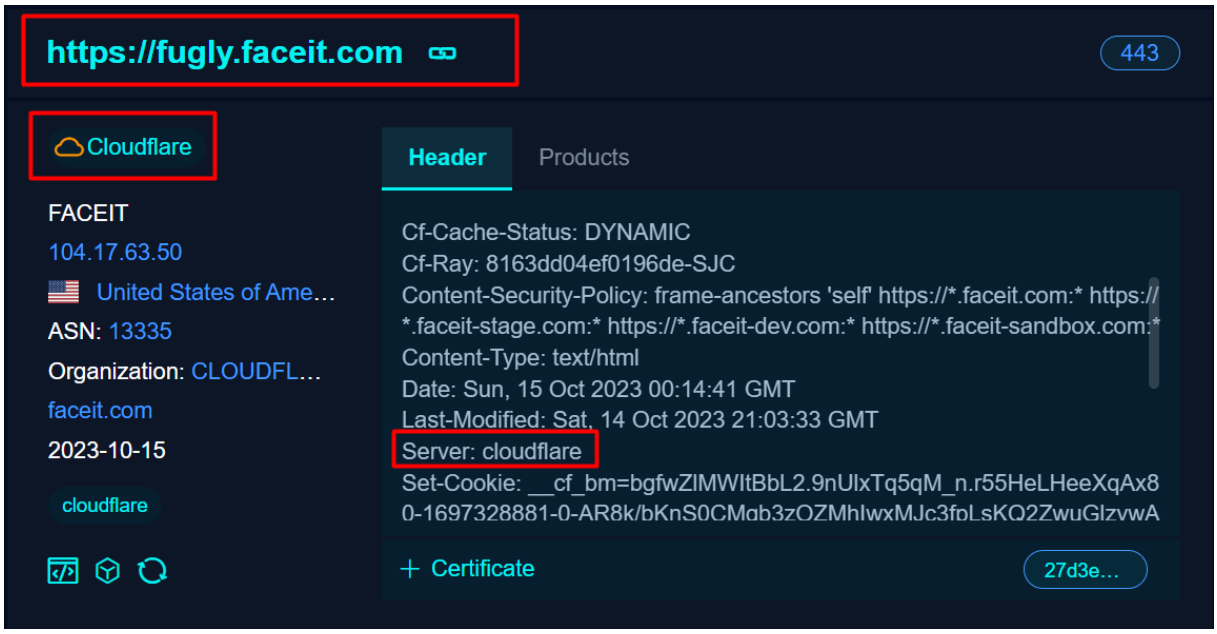
Hosty w poddomenach korzystają z chmurowych rozwiązań Amazona i Cloudflare. Hosty wykorzystują usługi organizacji Amazon takie jak Amazon S3 (przechowywanie danych, widoczne na obrazie 6.1.2) i Cloudfront (dostarczanie treści, widoczne na obrazie 6.1.3). Hosty korzystają z usług organizacji Cloudflare (zarządzanie DNS, hosting, widoczne na obrazie 6.1.4).



Obraz 6.1.2 ogólne informacje dla adresu 52.217.91.221 host widgets.smite.faceit.com, źródło en.fofa.info, data wykonana zrzutu 09.02.2024 r.



Obraz 6.1.3 ogólne informacje dla adresu 52.217.91.221 host widgets-sdk.faceit.com, źródło en.fofa.info, data wykonana zrzutu 09.02.2024 r.



Obraz 6.1.4 ogólne informacje dla hosta fugly-sdk.faceit.com, źródło en.fofa.info, data wykonana zrzutu 09.02.2024 r.

Na obrazach 6.2.1, 6.2.2 można dowiedzieć się, że poddomeny faceit.com są obsługiwane przez systemy operacyjne Linux – dystrybucja nieznana.

netcraft LEARN MORE REPORT FRAUD

Rank	Site	First seen	Netblock	OS	Site Report
1486	www.faceit.com	October 2014	unknown	Linux	
52100	accounts.faceit.com	July 2019	unknown	Linux	
76806	support.faceit.com	August 2016	unknown	Linux	
578142	cdn.faceit.com	Febuary 2016	unknown	Linux	
1116994	corporate.faceit.com	Febuary 2018	unknown	Linux	
1168122	email.faceit.com	Febuary 2017	unknown	Linux	
1289501	justice.faceit.com	Febuary 2020	unknown	Linux	

Obraz 6.2.1 rezultat sprawdzenia systemów operacyjnych poddomen, źródło netcraft.com, data wykonania zrzutu 17.1.2024 r.

Obrazy 6.3.2, 6.3.1, 6.3.3 wskazują na to, że host cdn.faceit.com jest obsługiwany przez system operacyjny Linux(dystrybucja Debian, wersja nieznana). Co więcej na systemie Linux działa usługa Apache w wersji 2.4.56 (obraz 6.3.1), a także MYSQL w wersji 8.0.35 (port 3306, obraz 6.3.2) i RedisLabs Redis w wersji nieznanej na procie 6379 (obsługa bazy danych NoSQL, obraz 6.3.3).

Downloads Pricing cdn.faceit.com Account

View Report Download Results Historical Trend View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out **everything you have access to.**

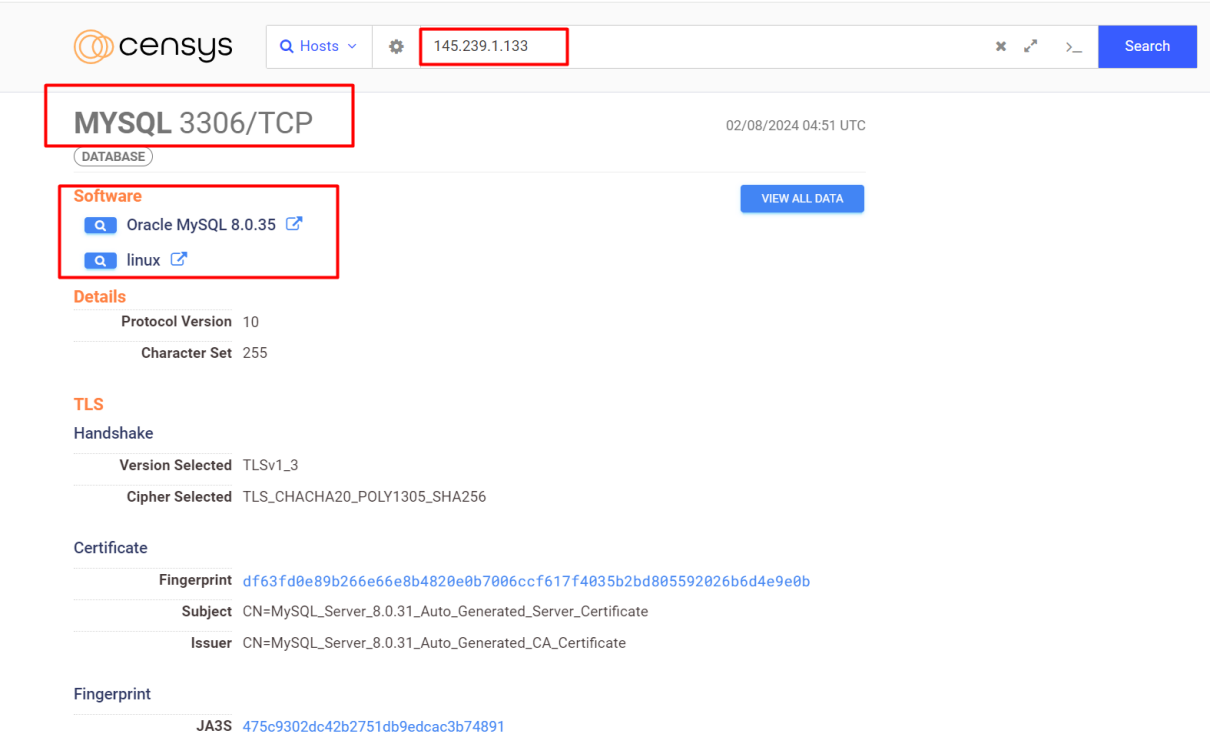
Redirecting to https://cdn.faceit.com/widgets/sso/index.html?client... 2024-01-22T03:04:36.015589

145.239.1.133
ns3084708.ip-145-239-1.eu
beta.memo.gg
OVH Dedicated Servers LIM
Germany, Frankfurt am Main

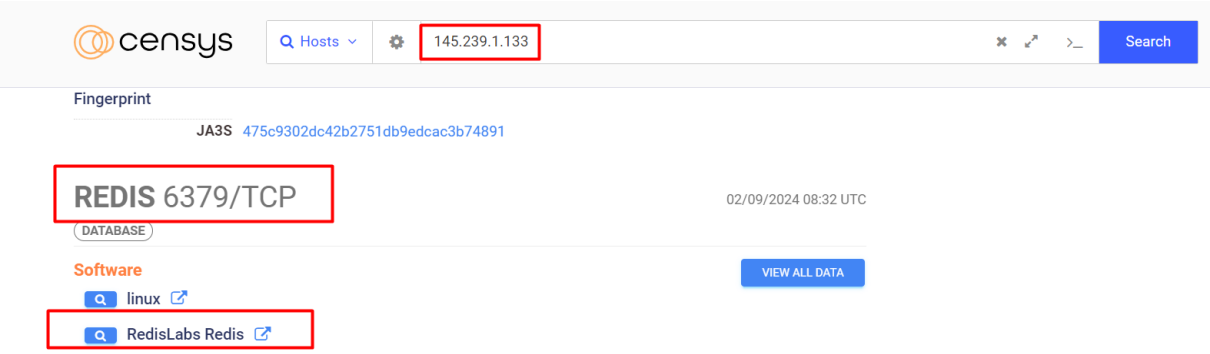
SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
beta.memo.gg
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 302 Found
Date: Mon, 22 Jan 2024 03:04:35 GMT
Server: Apache/2.4.56 (Debian)
Cache-Control: no-cache, private
Location: https://cdn.faceit.com/widgets/sso/index.html?client_id=1c865663-e1dc-425d
```

Obraz 6.3.1 ogólne informacje dla adresu 145.239.1.133 host cdn.faceit.com, źródło shodan.io, data wykonania zrzutu 09.02.2024 r.



Obraz 6.3.2 usługa działająca na porcie 3306 dla adresu 145.239.1.133 host cdn.faceit.com, źródło censys.io, data wykonania zrzutu 09.02.2024 r.



Obraz 6.3.3 usługa działająca na porcie 6379 dla adresu 145.239.1.133 host cdn.faceit.com, źródło censys.io, data wykonania zrzutu 09.02.2024 r.

Obraz 6.4.2 wskazuje na to, że systemem operacyjnym obsługującym hosta telekom-survey.faceit.com jest Ubuntu Linux 20.04. System udostępnia usługi na portach 80, 443 (serwer nginx wersja 1.18.0, obraz 6.4.1), port 22 usługa OpenSSH wersja 8.2p1 (obraz 6.4.2 i obraz 6.4.4), port 10011 Teamspeak (wersja nieznana, obraz 6.4.3).

// 80 / TCP -1356218440 | 2024-01-26T11:30:22.030980

nginx 1.18.0

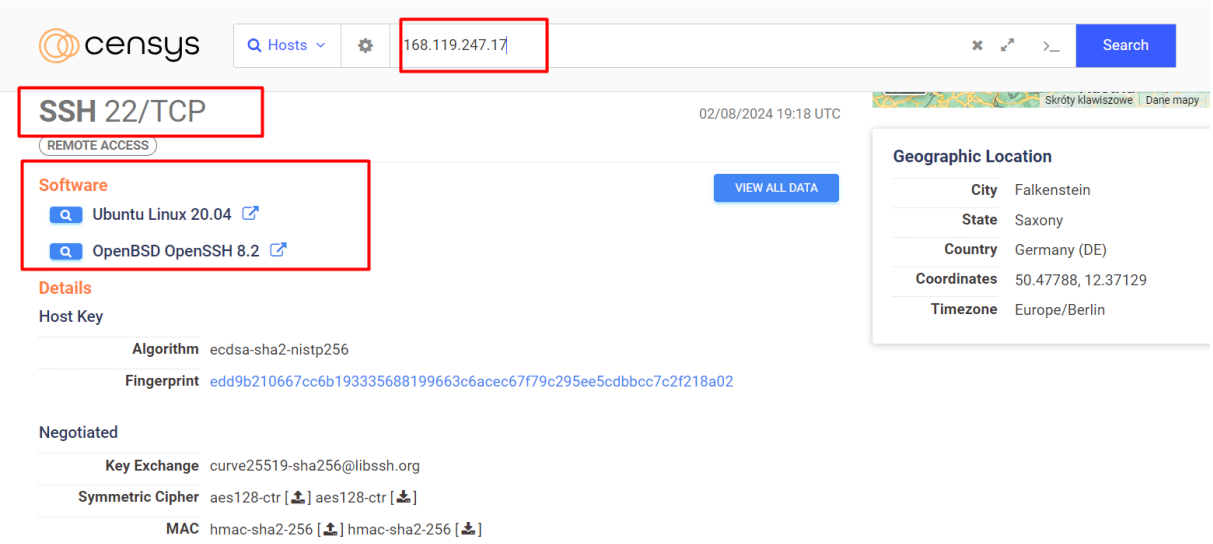
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 26 Jan 2024 11:30:21 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1885
Connection: keep-alive
X-Powered-By: Express
ETag: W/"75d-ZOB3eYXIFBhuxEYF/hoPSVIqQTM"
Set-Cookie: connect.sid=s%3A9CYdfKCSYSq_fLI8Z9SiCwZc91DaXrob.MZAJhYzYtAJ%2BRELRgdklw4RTdbURyS92qnz08eHE5
gw; Path=/; HttpOnly
```

// 443 / TCP -1356218440 | 2024-02-06T05:08:17.883739

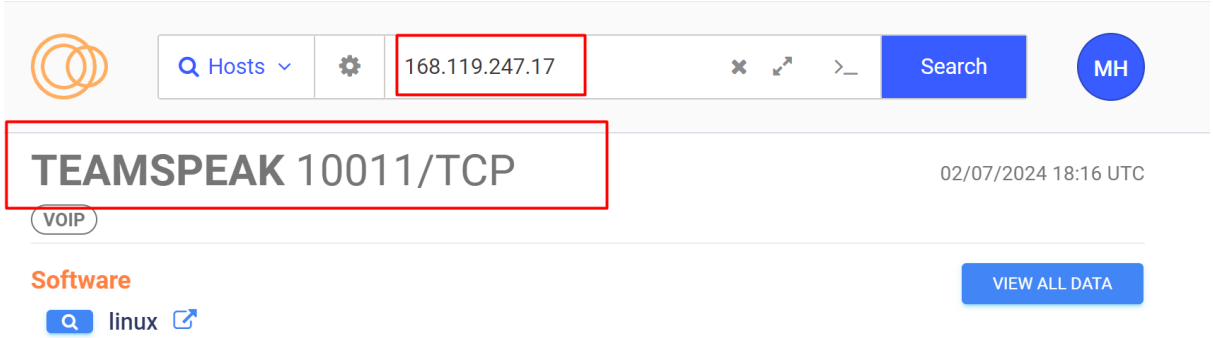
nginx 1.18.0

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 06 Feb 2024 05:08:17 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1885
Connection: keep-alive
X-Powered-By: Express
ETag: W/"75d-ZOB3eYXIFBhuxEYF/hoPSVIqQTM"
Set-Cookie: connect.sid=s%3AmWRyhIbWjvpQI_fDAP_pTTilWui3sT6T.Dc0Qhb%2B8Qn0kmuaPM79iamsHInpB58lKZhPAjFvkz
RY; Path=/; HttpOnly
```

Obraz 6.4.1 usługi działające na portach 443 i 80 dla hosta telekom-survey.faceit.com, źródło shodan.io, data wykonania zrzutu 09.02.2024 r.

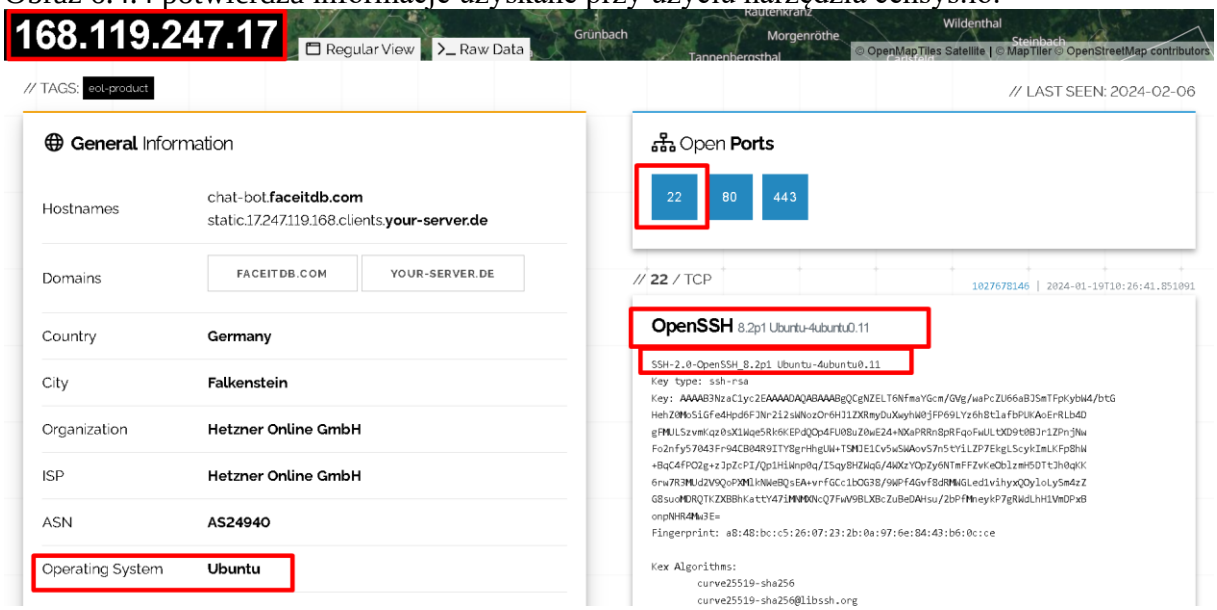


Obraz 6.4.2 usługa działająca na porcie 22(OpenSSH_8.2p1 Ubuntu-4ubuntu0.11) host telekom-survey.faceit.com, źródło censys.io, data wykonania zrzutu 09.1.2024 r.



Obraz 6.4.3 usługa działająca na porcie 10011 host telekom-survey.faceit.com, źródło censys.io, data wykonania zrzutu 09.1.2024 r.

Obraz 6.4.4 potwierdza informacje uzyskane przy użyciu narzędzia censys.io.



Obraz 6.4.4 ogólne informacje dla adresu 168.119.247.17 host telekom-survey.faceit.com, źródło censys.io

Obrazy 6.5.1, 6.5.2 wskazują, że na host corporate.faceit.com udostępnia usługi takie jak nginx, wersja nieznana (porty 80 i 443), a także SHH na porcie 2222 (wersja nieznana).

nginx

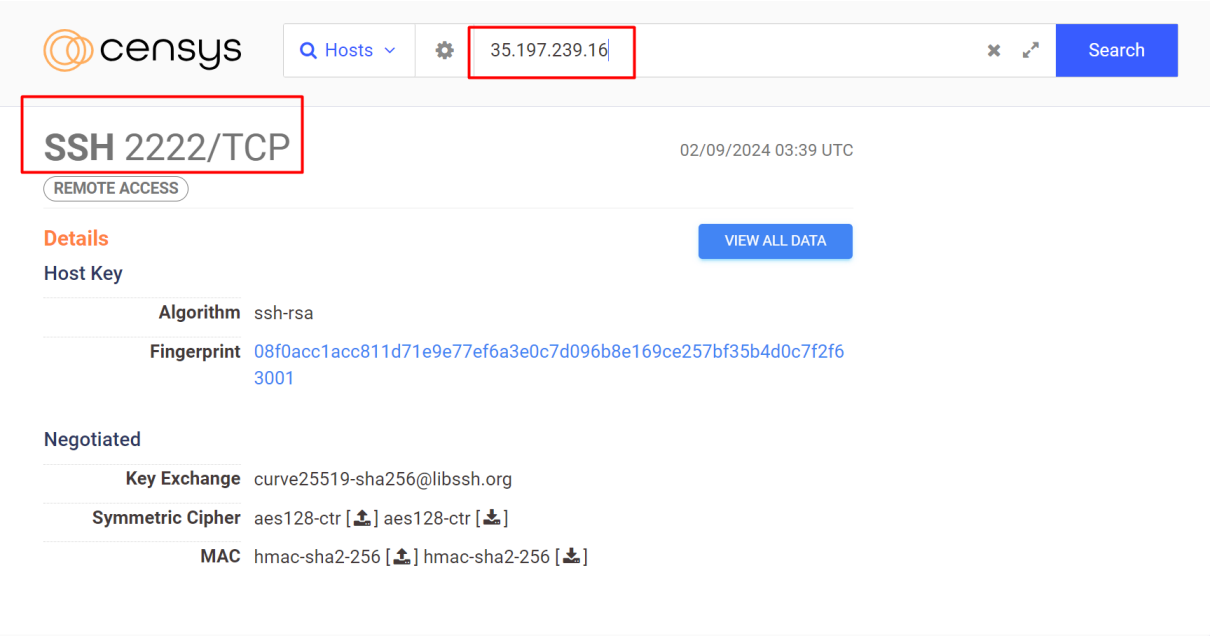
```
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Fri, 09 Feb 2024 07:08:14 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Keep-Alive: timeout=20
Location: https://www.cavagnagroup.com/
```

// **443** / TCP 25992354 | 2024-02-09T00:23:48.297653

nginx

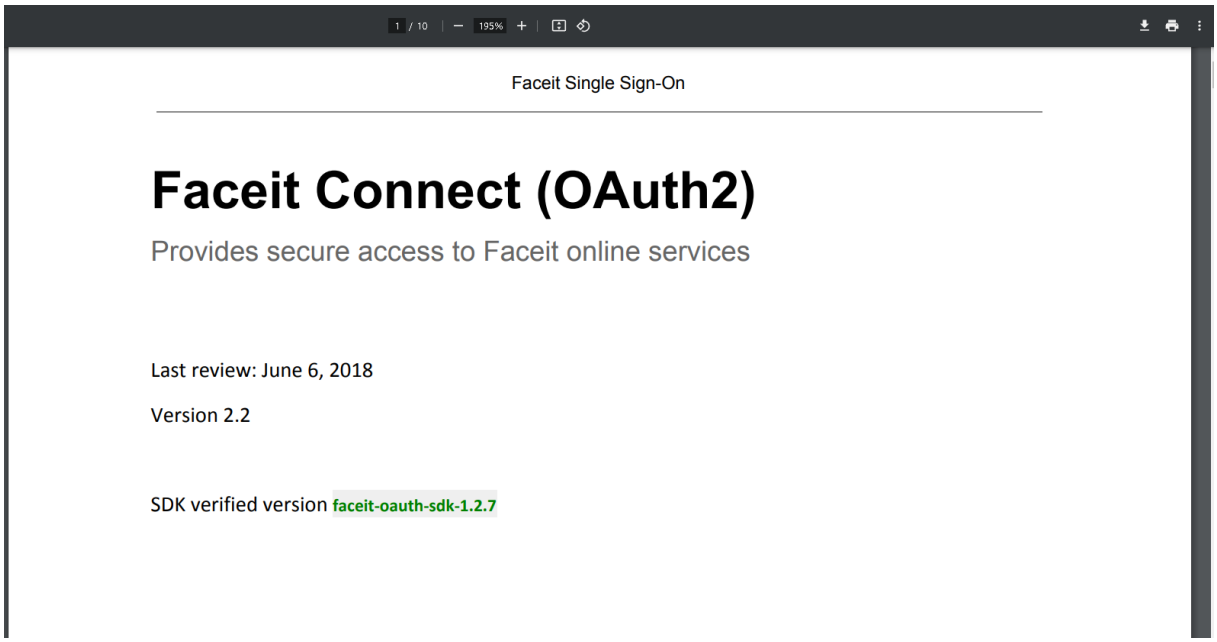
```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 09 Feb 2024 00:23:43 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 43299
Connection: keep-alive
Keep-Alive: timeout=20
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Link: <https://www.utbox.net/wp-json/>; rel="https://api.w.org/"
Link: <https://www.utbox.net/wp-json/wp/v2/pages/1045>; rel="alternate"; type="applica
tion/json"
Link: <https://www.utbox.net/>; rel=shortlink
X-Powered-By: WP Engine
X-Cacheable: SHORT
```

Obraz 6.5.1 usługa działająca na porcie 80 host corporate.faceit.com, źródło shodan.io, data wykonania zrzutu 15.1.2024 r.



Obraz 6.5.2 usługa działająca na porcie 2222 host corporate.faceit.com, źródło sensys.io, data wykonania zrzutu 9.2.2024 r.

Faceit wspiera protokół autoryzacji OAuth2 w celu korzystania z internetowych usług faceit (część dokumentu widoczna na obrazie 6.4.1).



Obraz 6.6.1 dokument opisujący protokół autoryzacji, źródło http://assets1.faceit.com/third_party/docs/Faceit_Connect.pdf, data wykonania zrzutu 11.1.2024 r.

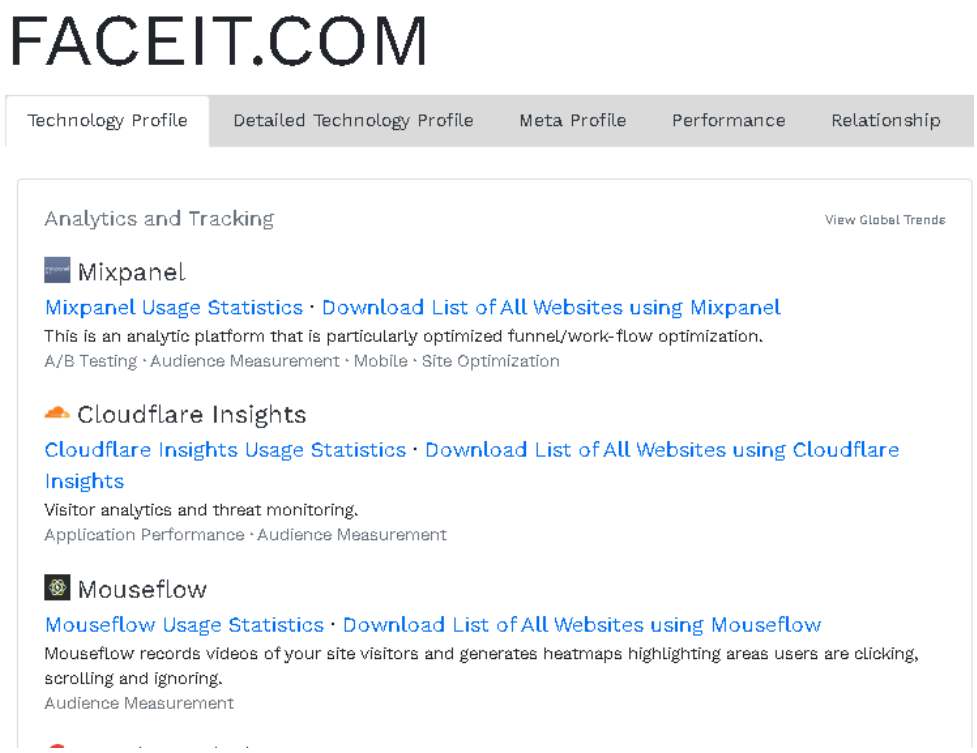
W zbieraniu danych do rozdziału 6 skorzystano z narzędzi takich jak shodan.io., builtwith.com, netcraft.com, dnschecker.org, censys.io. Z zebranych informacji wynika, że hosty domeny korzystają z systemu operacyjnego Linux (dystrybucje Debian i Ubuntu). Na hostach działają usługi takie jak nginx, Apache, OpenSHH, Teamspeak, RedisLabs Redis, MySQL, których część działa na licencji open-source. Faceit korzysta z protokołu OAuth2 w celu autoryzacji.

7. Wykorzystywane technologie informatyczne

Analityka i śledzenie [wybrane technologie] (część widoczna na obrazie 7.1.1)

- Cloudflare Insights
- Mixpanel
- Mouseflow
- Google Analytics
- Cloudflare Web Analytics
- Facebook Pixel

Cloudflare Web Analytics umożliwia monitorowanie i analizowanie ruchu na stronach internetowych hostowanych na platformie Cloudflare.



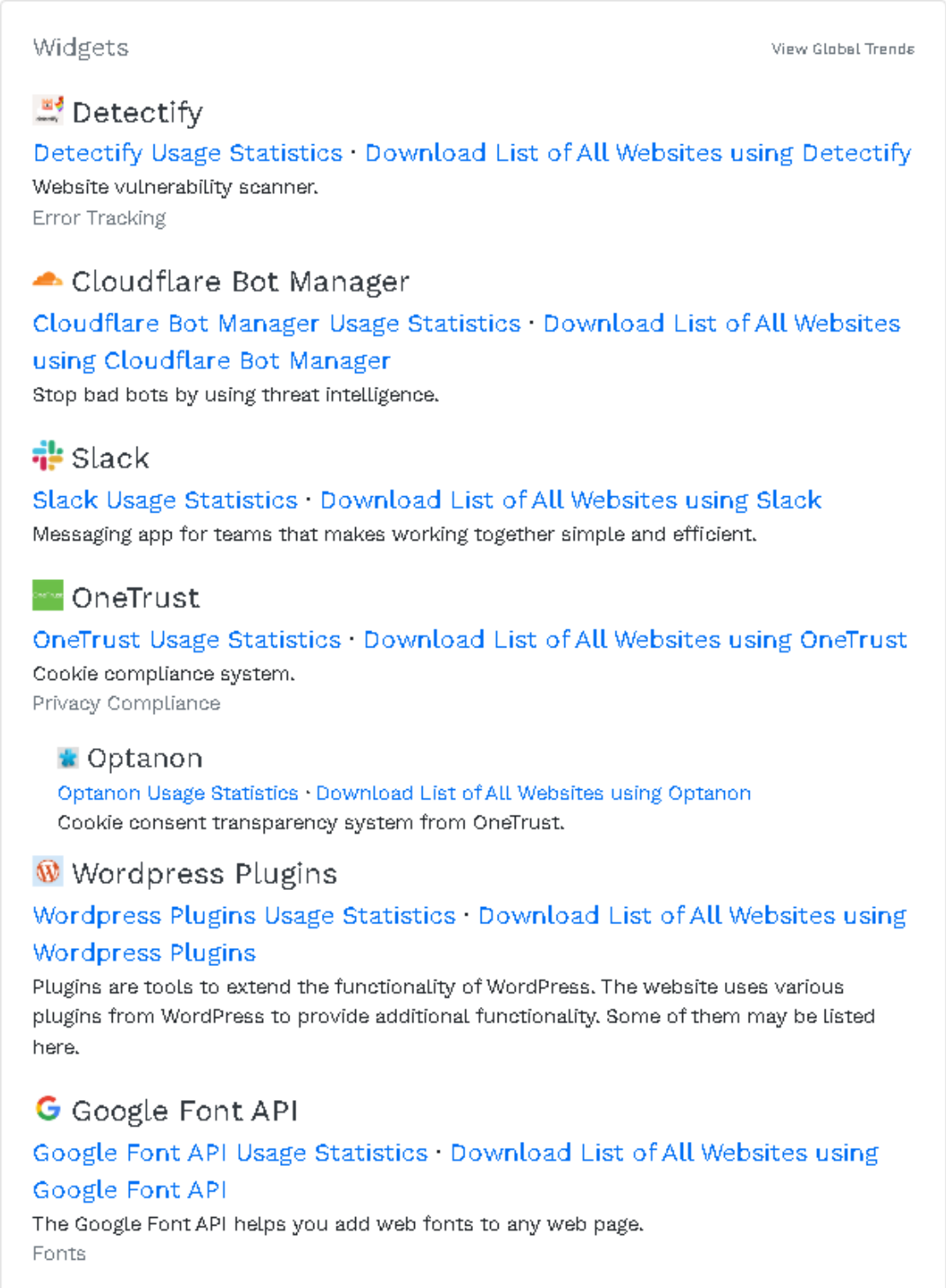
Obraz 7.1.1 wykorzystywane technologie śledzenia, źródło builtwith.com, data wykonania zrzutu 11.1.2024 r.

Widżety [wybrane elementy] (część widoczna na obrazie 7.1.2)

- Detectify
- Cloudflare Bot Manager
- Slack
- OneTrust
- Wordpress Plugins
- reCAPTCHA
- Google Font API
- CrUX Dataset

- Cloudflare Radar
- US Privacy User Signal Mechanism (Github)
- Global Privacy Control
- Cloudflare Turnstile

CrUX Dataset umożliwia segmentację danych na podstawie różnych kryteriów, takich jak kraj, urządzenie, typ połączenia internetowego i inne, co pozwala na dokładniejszą analizę i zrozumienie zachowań użytkowników.

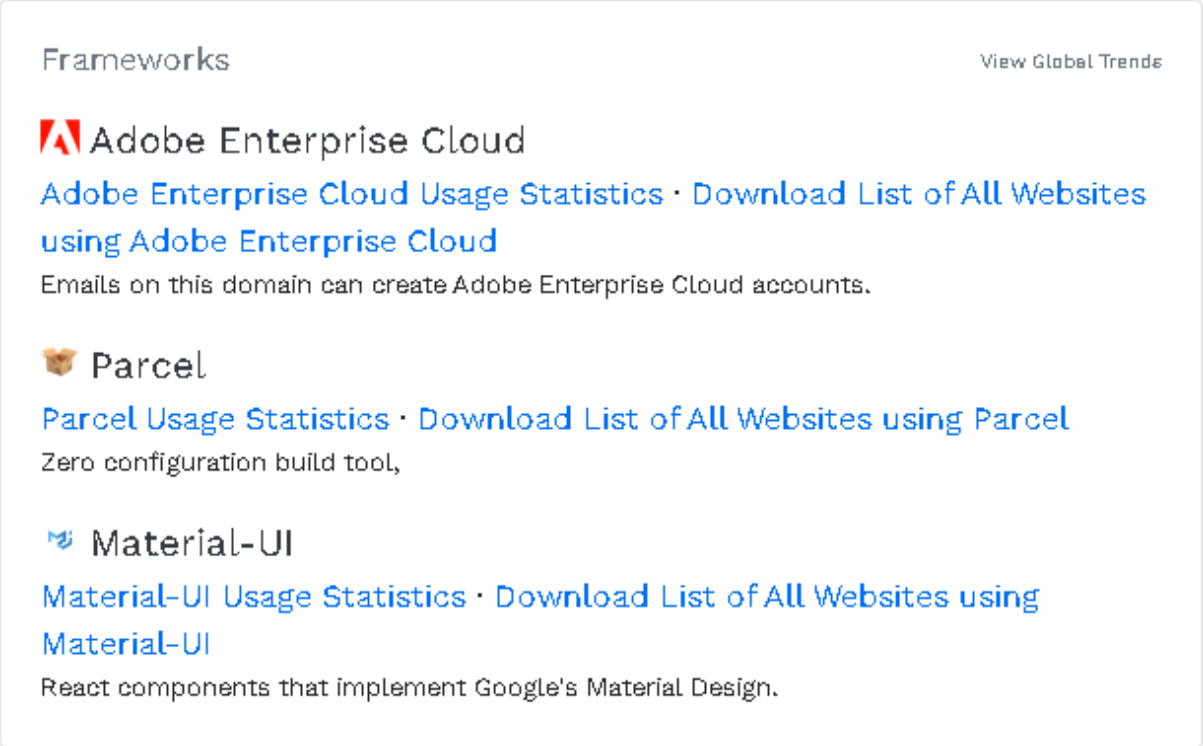


Obraz 7.1.2 wykorzystywane widżety, źródło builtwith.com, data wykonania zrzutu 11.1.2024 r.

Framworki [wybrane elementy] (część widoczna na obrazie 7.1.3)

- Adobe Enterprise Cloud
- Parcel
- Material-UI

Adobe Enterprise Cloud oferuje narzędzia do marketingu cyfrowego, takie jak Adobe Campaign, Adobe Target i Adobe Analytics, które umożliwiają personalizację doświadczeń klientów, zarządzanie kampaniami marketingowymi i analizę wyników działań marketingowych.

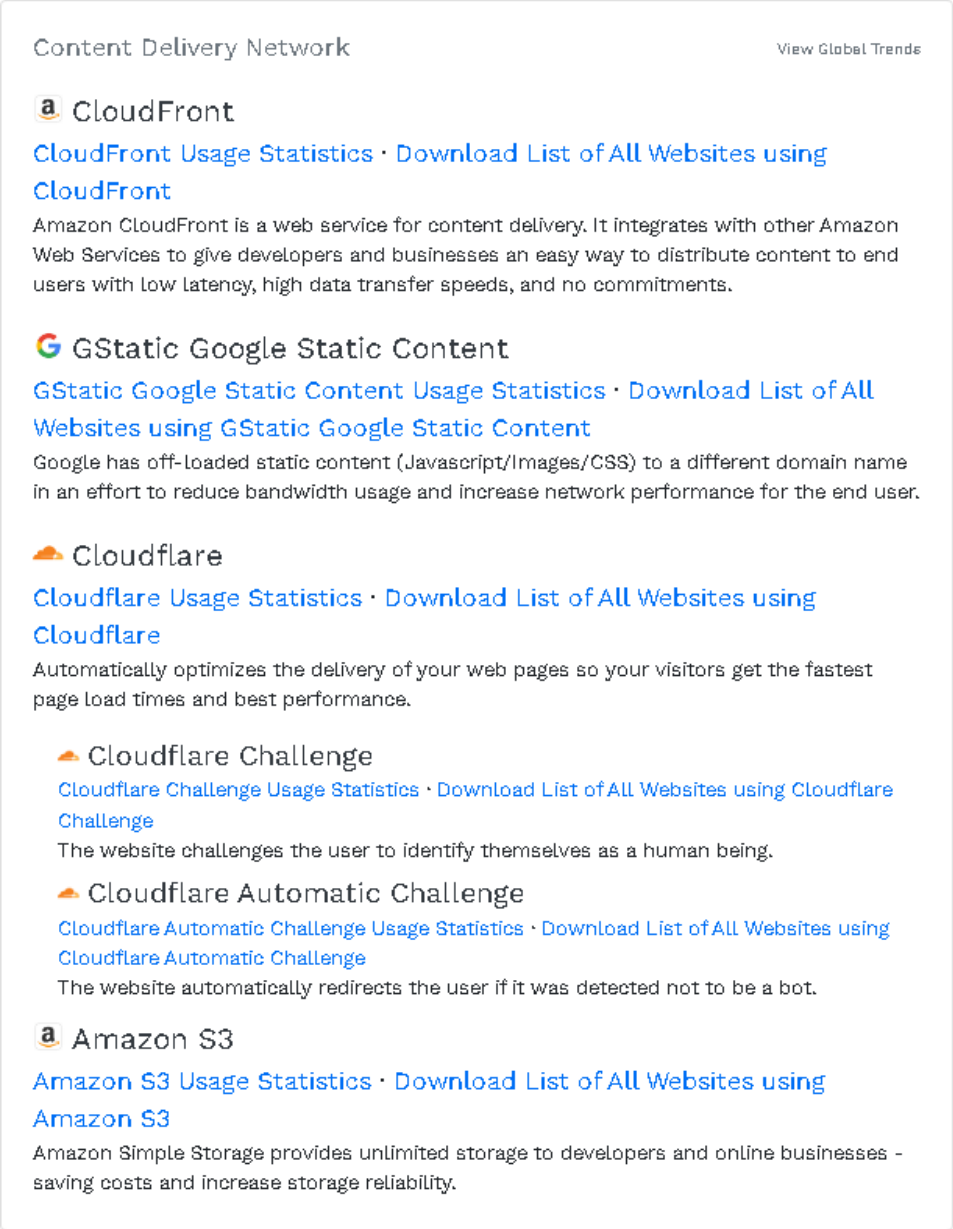


Obraz 7.1.3 wykorzystywane frameworki, źródło builtwith.com, data wykonania zrzutu 11.1.2024 r.

Sieć dostarczania treści (widoczne na obrazie 7.1.4)

- CloudFont
- Cloudflare
- Amazon S3

Faceit oferuje również szerokie wsparcie dla technologii CDN (Content Delivery Network), która przez rozproszoną sieć serwerów przechowywujących kopie treści internetowych umożliwiają szybkie i efektywne dostarczenie ich użytkownikom końcowym.

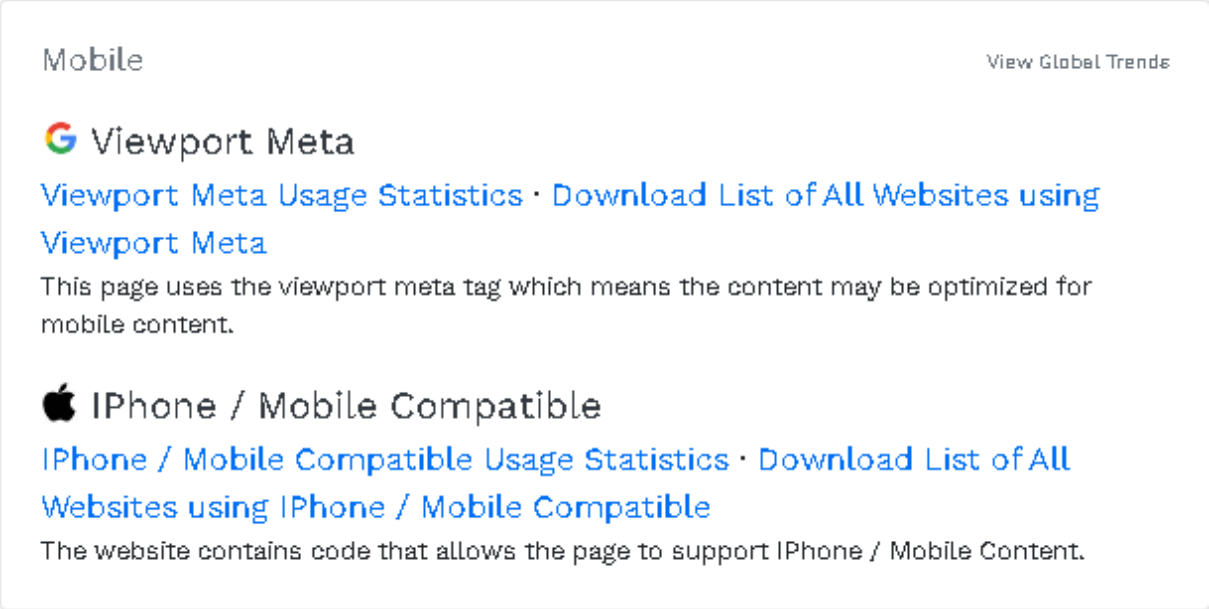


Obraz 7.1.4 wykorzystywane sieci dostarczania treści, źródło builtwith.com, data wykonania zrzutu 11.1.2024 r.

Rozwiązania mobilne (widoczne na obrazie 7.1.5)

- Viewport Meta
- IPhone / Mobile Compatible

Meta viewport to meta tag HTML używany na stronach internetowych do kontrolowania wyglądu i zachowania widoku strony na urządzeniach mobilnych.

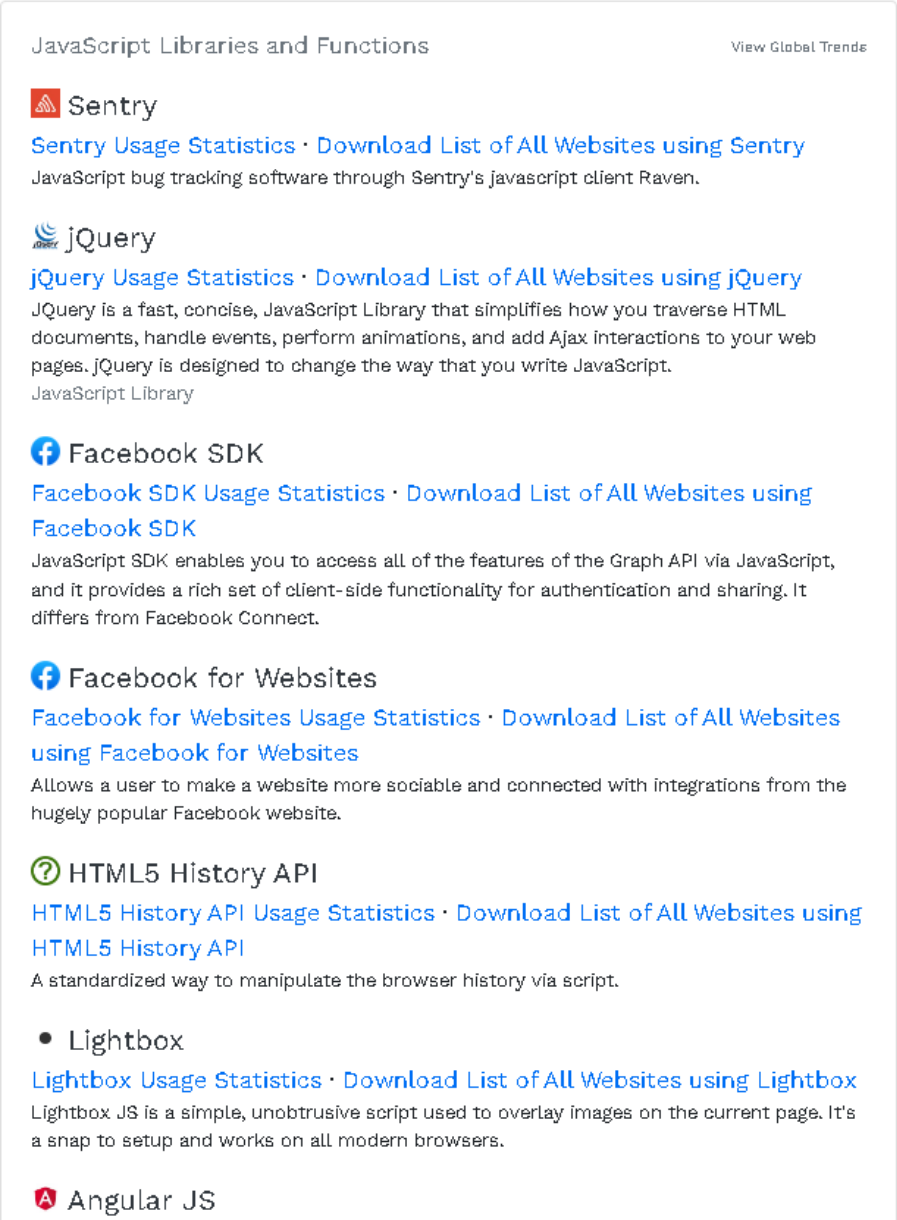


Obraz 7.1.5 wykorzystywane rozwiązania mobilne, źródło builtwith.com, data wykonania zrzutu 11.1.2024 r.

Biblioteki JavaScript i funkcje

- Sentry
- jQuery
- Facebook SDK
- Angular JS
- React
- Moment JS
- React Redux

Facebook SDK jest niezbędnym narzędziem dla deweloperów, którzy chcą zintegrować swoje aplikacje i witryny z platformą Facebook, aby zapewnić lepsze doświadczenia użytkownikom, promować swoje aplikacje.

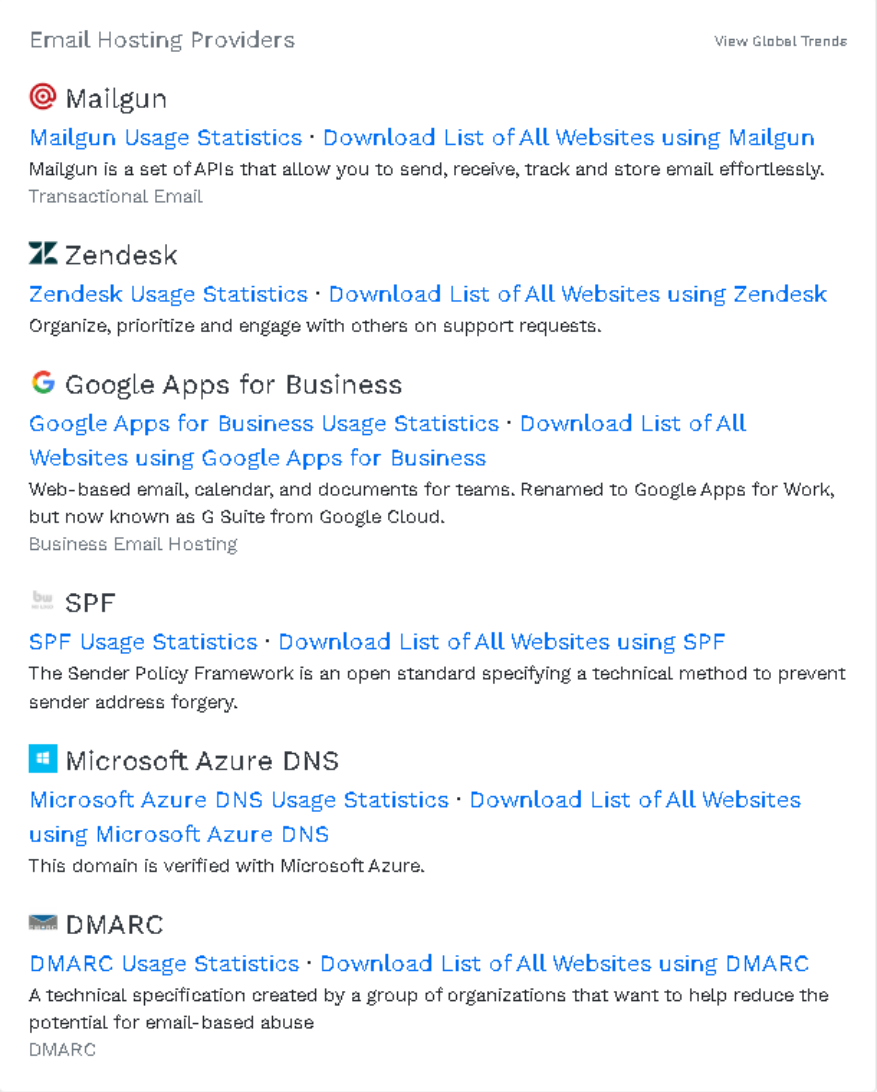


Obraz 7.1.6 wykorzystywane biblioteki javascript, źródło builtwith.com, data wykonania zrzutu 11.1.2024 r.

Dostawcy hostingu poczty e-mail

- Mailgun
- Zendesk
- SPF
- Microsoft Azure DNS
- DMARC
- SPF

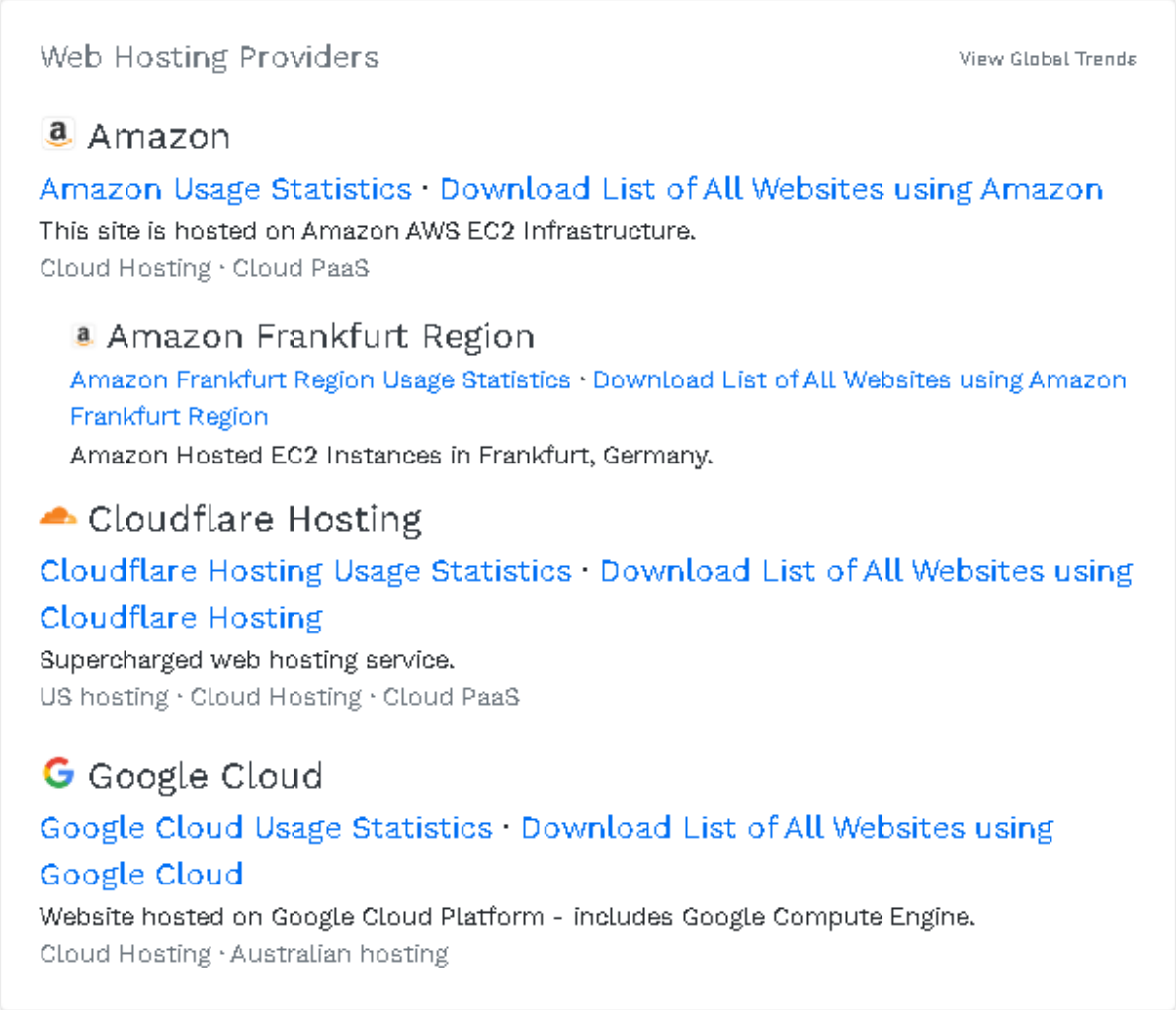
Kolejnymi istotnymi informacjami odnalezionymi przez witrynę builtwith.com jest zastosowanie zabezpieczenia SPF (Sender Policy Framework) i DMARC (Domain-based Message Authentication, Reporting, and Conformance). Pierwszy z nich ma chronić przed atakami typu ‘spoofing’ (używanie fałszywego adresu e-mail w celu podszywania się pod faktycznego nadwace), oraz uwierzytelnić adres email z którego wysyłane są przez nas wiadomości. Kolejne zabezpieczenie czyli DMARC ma za zadanie łączyć weryfikacje SPF oraz DKIM (DomainKeys Identified Mail) w związku z czym weryfikuje czy email pochodzi z prawidłowego serwera (SPF) oraz czy został podpisany cyfrowo (DKIM).



Obraz 7.1.7 dostawcy hostingu poczty email, źródło builtwith.com, data wykonania zrzutu 11.1.2024 r.

Platforma domyślnie wykorzystuje hosting AWS (Amazon Web Services, obraz 7.1.8), i zapewnia swoim klientom m.in. takie zabezpieczenia i usługi jak:

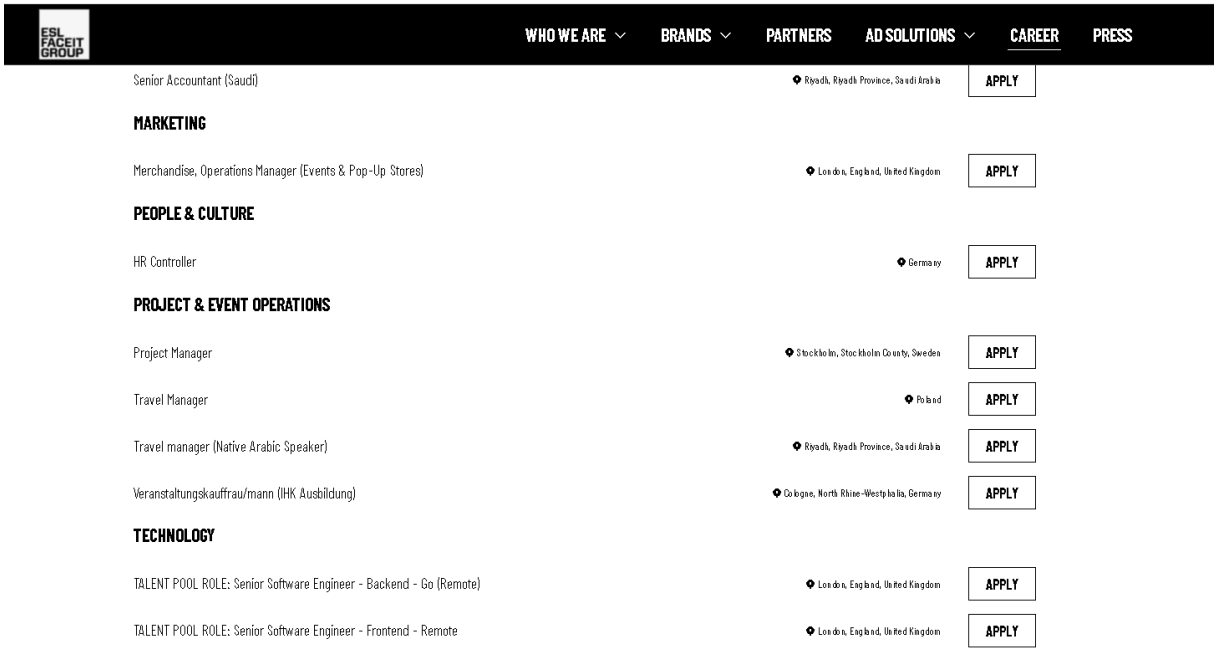
- Dwuetapowa weryfikacja
- Mechanizm Single Sign-On który umożliwia użytkownikom uzyskanie dostępu do wielu różnych systemów lub aplikacji (takich jak np. G Suite) za pomocą jednego zestawu poświadczeń
- Domyślne wbudowany certyfikat SSL
- Automatyczne backupy i aktualizacje.



Obraz 7.1.8 dostawcy usług hostingowych, źródło builtwith.com, data wykonania zrzutu 11.1.2024 r.

Z obrazów 7.2.1-7.2.7, 7.3.1, 7.4.1-7.4.4 wynika, że domena używa następujących technologii informatycznych:

- Go/Golang
- Mikroserwisy
- RESTful/gRPC
- Bazy danych NoSQL
- DOKCER
- React + Redux
- TypeScript
- Next.js
- SAP S/4HANA Public Cloud
- SAP Business Technology Platform
- Python
- Coupa, Salesforce with SAP
- MongoDB
- Redis
- Servers hosted on AWS, Google
- File stored using Dropbox



Obraz 7.2.1 oferty pracy organizacji ESL FACEIT GROUP, źródło eslfaceutgroup.com, data wykonania zrzutu 10.12.2023 r.

ESL FACEIT GROUP

WHO WE ARE BRANDS PARTNERS AD SOLUTIONS CAREER PRESS

REQUIREMENTS:

- Current commercial experience with Go/Golang on large scalable projects;
- Ability to design amazing distributed APIs and scheduled procedures;
- Experience working within a large Microservices environment;
- Excellent knowledge of RESTful/gRPC or APIs;
- Good understanding of Async communication;
- A passion for video games and esports is a plus;
- Proven experience working with NoSQL databases would be great;
- Ability to follow SOLID or DRY principles;
- Experience with Docker or Kubernetes;
- In-depth understanding of testing;
- Previous experience working on large complex applications.

BENEFITS:

- Flexible working environment;
- Work with the best tech available;
- Company book club, and gaming nights;
- Company (virtual) drinks session every Friday;
- Quarterly team outings;
- Your professional growth is important to us. We provide ongoing training opportunities;
- Best of all Free Premium FACEIT user account.

APPLY NOW

Obraz 7.2.2 oferty pracy organizacji ESL FACEIT GROUP, źródło eslfaceutgroup.com, data wykonania zrzutu 10.12.2023 r.

ESL FACEIT GROUP

WHO WE ARE BRANDS PARTNERS AD SOLUTIONS CAREER PRESS

to them. We're currently working on developing some crazy new features, but are always open to new exciting ideas our colleagues want to share.

REQUIREMENTS:

- Current commercial experience with React and Redux;
- Good demonstrable TypeScript experience;
- Experience with Websockets and real-time messaging;
- Desire to learn new technologies and frameworks;
- Previous experience working on large complex applications;
- A passion for videogames and esports is a plus.

We would get especially excited if you have experience with the following:

- Next.js
- Styled-components
- Webpack
- Internationalisation libraries (react-intl or react-i18next);
- Knowledge of React testing framework.

BENEFITS:

- Flexible working environment;
- Work with the best tech available;
- Company book club, and gaming nights;
- Company (virtual) drinks session every Friday;
- Quarterly team outings;
- Your professional growth is important to us. We provide ongoing training opportunities;
- Best of all Free Premium FACEIT user account.

APPLY NOW

Obraz 7.2.3 oferta pracy organizacji ESL FACEIT GROUP, źródło eslfaceutgroup.com, data wykonania zrzutu 10.12.2023 r.

ESL FACEIT GROUP

WHO WE ARE BRANDS PARTNERS AD SOLUTIONS CAREER PRE

At **EFG (ESL FACEIT Group)** we create worlds beyond gameplay, where players and fans become a community. We pride ourselves in having a corporate social responsibility which is that "IT'S NOT GG, UNTIL IT'S GG FOR ALL". Our passion, craft, and DNA are aligned to create and shape the world of esports, gaming tournaments, leagues, events, and holistic ecosystems through our millions of players, fans, and heroes, as well as through our people, and culture.

We are looking for a **SAP FI Consultant – 1st / 2nd Level** of the Finance and Controlling module of SAP S/4HANA Public Cloud who will be responsible in the Technology team for the efficient administration, optimization, and stability of our SAP landscape.

The primary purpose of the role is to leverage expertise in SAP S/4HANA Public Cloud to configure, maintain, troubleshoot, and support the organization's financial processes. This role plays a key part in enhancing the systems adoption, security, and compliance, ultimately contributing to the seamless operation of our SAP environment and enabling effective business processes within the Finance domain.

**Please note that we are happy to support remote work arrangements, fostering a collaborative and inclusive environment that values the diverse talents of our team members, regardless of their physical location.*

What will you do:

- Provide technical support for the SAP S/4 Hana public cloud modules, including troubleshooting and issue resolution for both end-users and technical team members.
- Support (manual) Interface of Business Partner (Update/Create Finance Master Data) – 1st Level
- Interpretation of finance data flows via CPI / BTP APIs
- Support the implementation or optimization of new features in the area of CPI-Integration (e.g. AP Down Payment Process, Amazon, etc.)
- Work closely with end-users and other stakeholders to understand and address their Finance related needs. This includes providing recommendations to improve the SAP S/4 Hana public cloud modules process and identifying areas for system optimization.
- Provide support for SAP S/4 Hana public cloud module-related requests, including assistance with user account management, system access, and defect resolution.
- Work with technical team members to identify and prioritize requests for system enhancements.
- Manage and maintain SAP S/4 Hana public cloud modules applications, including configuration and customization of the applications to meet the needs of the business.
- Collaborate with cross-functional teams to support program delivery efforts, including testing, training, and documentation. This includes working with the technical team to ensure that SAP S/4 Hana public cloud modules are properly integrated with other enterprise systems.
- Develop and maintain technical documentation related to SAP S/4 Hana public cloud modules. This includes creating functional specification documents and system documentation.
- Stay up to date with industry trends and best practices related to SAP S/4 Hana public cloud modules. This includes attending training sessions and conferences, as well as participating in professional development opportunities

Obraz 7.2.4 oferta pracy organizacji ESL FACEIT GROUP, źródło eslfaceutgroup.com, data wykonania zrzutu 10.12.2023 r.

ESL FACEIT GROUP

WHO WE ARE BRANDS PARTNERS AD SOLUTIONS CAREER PRESS

- Collaborate with cross-functional teams to support program delivery efforts, including testing, training, and documentation. This includes working with the technical team to ensure that SAP S/4 Hana public cloud modules are properly integrated with other enterprise systems.
- Develop and maintain technical documentation related to SAP S/4 Hana public cloud modules. This includes creating functional specification documents and system documentation.
- Stay up to date with industry trends and best practices related to SAP S/4 Hana public cloud modules. This includes attending training sessions and conferences, as well as participating in professional development opportunities

REQUIREMENTS:

What you will need:

- Minimum of 5 years of experience as an SAP Administrator, with a focus on the Finance and Controlling Module.
- Experience in SAP S/4HANA Public Cloud administration.
- Experience with SAP Business Technology Platform (BTP)
- Experience in integrating different Business Cloud Solutions (Coupa, Salesforce) with SAP
- Strong knowledge of SAP Finance and Controlling business processes.
- Experience in system configuration, optimization, and performance tuning.
- Solid understanding of SAP security principles and best practices.
- Knowledge of integration with other SAP modules and third-party systems.
- Familiar with Python as a programming language
- A basic understanding of BPMN

Firmly rooted in our values, EFG is an affirmative action employer that celebrates being an equal-opportunity workplace. Our unwavering commitment to fair employment extends to all individuals, regardless of their race, color, ancestry, religion, sex, national origin, age, sexual orientation, disability, citizenship, marital status, gender identity, or Veteran status.

APPLY NOW

Obraz 7.2.5 oferty pracy organizacji ESL FACEIT GROUP, źródło eslfaceutgroup.com, data wykonania zrzutu 10.12.2023 r.

ESL FACEIT GROUP

WHO WE ARE BRANDS PARTNERS AD SOLUTIONS CAREER PRESS

At **EFG (ESL FACEIT Group)** we create worlds beyond gameplay, where players and fans become a community. We pride ourselves in having a corporate social responsibility which is that "IT'S NOT GG, UNTIL IT'S GG FOR ALL". Our passion, craft, and DNA are aligned to create and shape the world of esports, gaming tournaments, leagues, events, and holistic ecosystems through our millions of players, fans, and heroes, as well as through our people, and culture.

We are looking for a **Senior SAP Public Cloud Administrator** of the Finance and Controlling module of SAP S/4HANA Public Cloud who will be responsible in the Technology team for the efficient administration, optimization, and stability of our SAP landscape.

The primary purpose of the role is to leverage expertise in SAP S/4HANA Public Cloud to configure, maintain, troubleshoot, and support the organization's financial processes. This role plays a key part in enhancing the systems adoption, security, and compliance, ultimately contributing to the seamless operation of our SAP environment and enabling effective business processes within the Finance domain.

**Please note that we are happy to support remote work arrangements, fostering a collaborative and inclusive environment that values the diverse talents of our team members, regardless of their physical location.*

What will you do:

- Provide technical support for the SAP S/4 Hana public cloud modules, including troubleshooting and issue resolution for both end-users and technical team members.
- Support (manual) Interface of Business Partner (Update/Create Finance Master Data) – 1st Level
- Interpretation of finance data flows via CPI / BTP APIs
- Support the implementation or optimization of new features in the area of CPI-Integration (e.g. AP Down Payment Process, Amazon, etc.)
- Work closely with end-users and other stakeholders to understand and address their Finance related needs. This includes providing recommendations to improve the SAP S/4 Hana public cloud modules process and identifying areas for system optimization.
- Provide support for SAP S/4 Hana public cloud module-related requests, including assistance with user account management, system access, and defect resolution.
- Work with technical team members to identify and prioritize requests for system enhancements.
- Manage and maintain SAP S/4 Hana public cloud modules applications, including configuration and customization of the applications to meet the needs of the business.
- Collaborate with cross-functional teams to support program delivery efforts, including testing, training, and documentation. This includes working with the technical team to ensure that SAP S/4 Hana public cloud modules are properly integrated with other enterprise systems.
- Develop and maintain technical documentation related to SAP S/4 Hana public cloud modules. This includes creating functional specification documents and system documentation.
- Stay up to date with industry trends and best practices related to SAP S/4 Hana public cloud modules. This includes attending training sessions and conferences, as well as participating in professional development opportunities

Obraz 7.2.6 oferta pracy organizacji ESL FACEIT GROUP, źródło eslfaceutgroup.com, data wykonania zrzutu 10.12.2023 r.

ESL FACEIT GROUP

WHO WE ARE BRANDS PARTNERS AD SOLUTIONS CAREER PRESS

- Provide support for SAP S/4 Hana public cloud module-related requests, including assistance with user account management, system access, and defect resolution.
- Work with technical team members to identify and prioritize requests for system enhancements.
- Manage and maintain SAP S/4 Hana public cloud modules applications, including configuration and customization of the applications to meet the needs of the business.
- Collaborate with cross-functional teams to support program delivery efforts, including testing, training, and documentation. This includes working with the technical team to ensure that SAP S/4 Hana public cloud modules are properly integrated with other enterprise systems.
- Develop and maintain technical documentation related to SAP S/4 Hana public cloud modules. This includes creating functional specification documents and system documentation.
- Stay up to date with industry trends and best practices related to SAP S/4 Hana public cloud modules. This includes attending training sessions and conferences, as well as participating in professional development opportunities

REQUIREMENTS:

What you will need:

- Minimum of 5 years of experience as an SAP Administrator, with a focus on the Finance and Controlling Module.
- Experience in SAP S/4HANA Public Cloud administration.
- Experience with SAP Business Technology Platform (BTP)
- Experience in integrating different Business Cloud Solutions (Coupa, Salesforce) with SAP
- Strong knowledge of SAP Finance and Controlling business processes.
- Experience in system configuration, optimization, and performance tuning.
- Solid understanding of SAP security principles and best practices.
- Knowledge of integration with other SAP modules and third-party systems.
- Familiar with Python as a programming language
- A basic understanding of BPMN

Firmly rooted in our values, EFG is an affirmative action employer that celebrates being an equal-opportunity workplace. Our unwavering commitment to fair employment extends to all individuals, regardless of their race, color, ancestry, religion, sex, national origin, age, sexual orientation, disability, citizenship, marital status, gender identity, or Veteran status.

APPLY NOW

Obraz 7.2.7 oferta pracy organizacji ESL FACEIT GROUP, źródło eslfaceutgroup.com, data wykonania zrzutu 10.12.2023 r.

11. INTERNATIONAL DATA TRANSFERS

It is possible that your personal information may be transferred outside of the EEA by third parties referred to in the policies as being the recipients of your data, and specifically your personal information may be transferred to other companies that belong to the same company group as FACEIT. We recommend that you refer to the privacy policies and/or terms and conditions of these third parties if you are concerned about your data being transferred outside the EEA.

Our databases are run using MongoDB, MySQL and Redis. Our servers are hosted AWS and Google. We use Digital Ocean to help us manage our cloud computing. Some files are stored using Dropbox.

Where we transfer your information outside of the EEA, we have agreements in place with those parties which include standard data protection clauses adopted by a data protection regulator and approved by the European Commission to ensure that appropriate safeguards are in place to protect your personal data. If you would like to find out more about these safeguards, please contact us at www.support.faceit.com.

Obraz 7.3.1 polityka prywatności faceit, źródło faceit.com, data wykonania zrzutu 10.12.2023 r.

Senior Data Engineer
ESL FACEIT Group - EFG · Wielka Bryta...

Łatwe aplikowanie | Zapisz | •••

EXPECTATIONS

- Serve as a leader in tech
  - Ask all the whys, relentlessly until you know your customer needs inside-out and know you're designing the right solution to the problems and not the other way around.
  - Partner with our stakeholders and serve as an internal consultant to foster the adoption of our data platform.
  - You contribute to the technical strategy of the team, and its execution through prioritization, and delivery management.
  - Set high standards across documentation, testing, resiliency, monitoring, and code quality. Enforce these standards by holding your team accountable.
  - You drive towards efficiencies and look for ways to simplify code, infrastructure and data models across the platform.
  - Inspire, teach and guide your fellow team members; lead design sessions, be there for a code review, take ownership of operational processes.
- Excel as Senior Engineer
  - Write well-rounded, reusable and documented code that captures the essential nature of the solution.
  - Decompose ambiguous and open-ended problems into solutions composed of multiple tooling.
  - Construct complex architectures tying multiple services and SaaS tooling together, leveraging a strong understanding of a cloud-based stack (AWS, GCP).
  - Drive towards efficiencies, lowering your cloud spend and tackling tech debt on a quarterly basis
- Personify our DNA
  - Exemplify the values we live by. Nurture a blameless culture. Know and care for your team members; inspire, and guide them to be the best that they can be.
  - Be the heart-first, people-first tech lead everyone wants to be around, because you have invested in building relationships.

Obraz 7.4.1 oferta pracy organizacji ESL FACEIT GROUP, źródło linkedin.com, data wykonania zrzutu 10.12.2023 r.

Senior Data Engineer
ESL FACEIT Group - EFG · Wielka Bryta...

Łatwe aplikowanie | Zapisz | •••

Experience

- Architecture
  - You've participated in shaping the architecture of a mature data platform, designed for different consumer types, and providing quantifiable business value.
  - You've run PoCs, planned large migrations of data and code, and participated in planning a roadmap multiple times before.
- Engineering Hands-On
  - You have hands-on experience in building resilient batch (Airflow, Fivetran) and streaming (Kafka, Kinesis, Dataflow) data pipelines at scale (> 1 TB/day)
  - You can advocate passionately for your tried-and-true best practices of CI/CD in data engineering (Github Actions, Jenkins)
  - You can build and maintain your own infrastructure through IaC (Terraform); you rely on DevOps expertise when needed
  - You have designed and implemented performant, reusable, and scalable data models (dbt) in cloud data warehouse (BigQuery, Snowflake)
  - You possess a comprehensive understanding of database design principles (star/snowflake schemas, data vault, normal forms) for effective and scalable data structures
  - You preach operational procedures from data and infrastructure observability (Monte Carlo, Datadog, Prometheus), alerting and incident management (PagerDuty, incident.io)
  - You know SQL & Python like the back of your hand
- Tech Leadership
  - You've served as a leader in technology in the past; you've made mistakes and learned from them.
  - You have interacted with a large community of stakeholders before; you understand the business use cases and can tailor your communication to ICs and Senior Management.

Obraz 7.4.2 oferta pracy organizacji ESL FACEIT GROUP, źródło linkedin.com, data wykonania zrzutu 10.12.2023 r.

S/4HANA (Solution) Consultant...
ESL FACEIT Group - EFG · Londyn, An...

Łatwe aplikowanie | Zapisz | •••

What will you do:

- Provide technical support for the SAP S/4 Hana public cloud modules, including troubleshooting and issue resolution for both end-users and technical team members.
- Support (manual) Interface of Business Partner (Update/Create Finance Master Data) - 1st Level
- Interpretation of finance data flows via CPI / BTP APIs
- Support the implementation or optimization of new features in the area of CPI-Integration (e.g. AP Down Payment Process, Amazon, etc.)
- Work closely with end-users and other stakeholders to understand and address their Finance related needs. This includes providing recommendations to improve the SAP S/4 Hana public cloud modules process and identifying areas for system optimization.
- Provide support for SAP S/4 Hana public cloud module-related requests, including assistance with user account management, system access, and defect resolution.
- Work with technical team members to identify and prioritize requests for system enhancements.
- Manage and maintain SAP S/4 Hana public cloud modules applications, including configuration and customization of the applications to meet the needs of the business.
- Collaborate with cross-functional teams to support program delivery efforts, including testing, training, and documentation. This includes working with the technical team to ensure that SAP S/4 Hana public cloud modules are properly integrated with other enterprise systems.
- Develop and maintain technical documentation related to SAP S/4 Hana public cloud modules. This includes creating functional specification documents and system documentation.
- Stay up to date with industry trends and best practices related to SAP S/4 Hana public cloud modules. This includes attending training sessions and conferences, as well as participating in professional development opportunities

Obraz 7.4.3 oferta pracy organizacji ESL FACEIT GROUP, źródło linkedin.com, data wykonania zrzutu 10.12.2023 r.

S/4HANA (Solution) Consultant...
ESL FACEIT Group - EFG · Londyn, An...

Łatwe aplikowanie | Zapisz | •••

Requirements

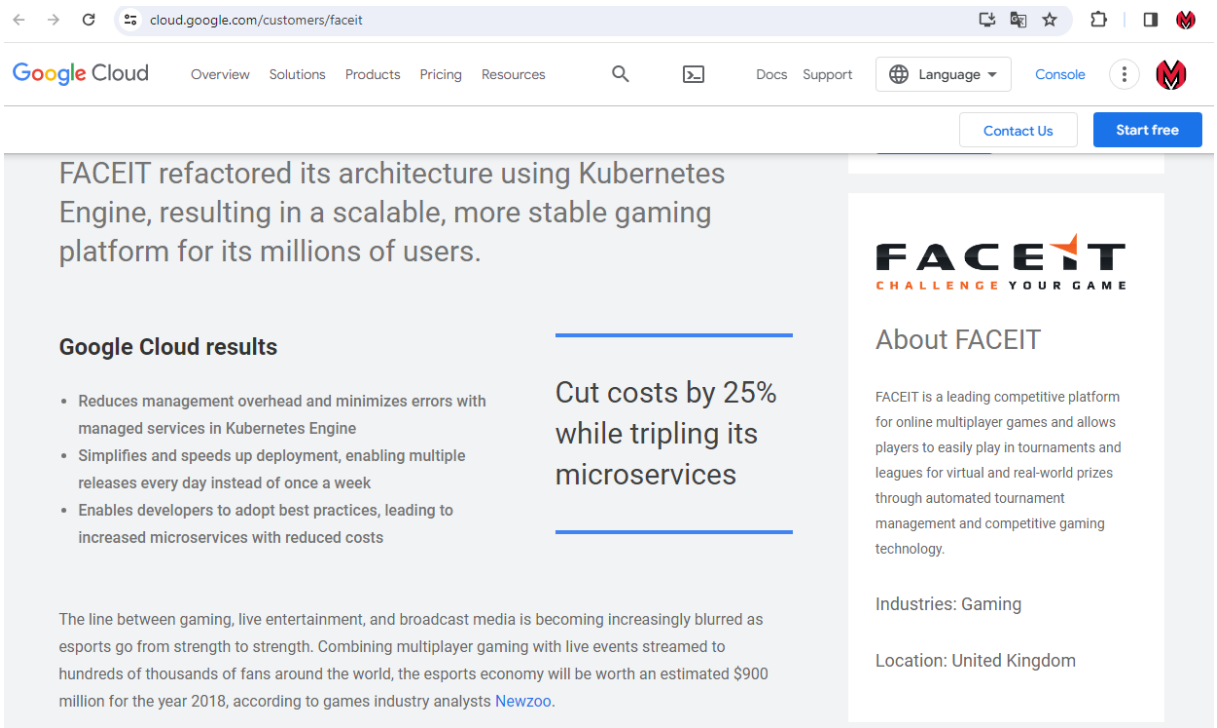
What you will need:

- Minimum of 5 years of experience as an SAP Administrator, with a focus on the Finance and Controlling Module.
- Experience in SAP S/4HANA Public Cloud administration.
- Experience with SAP Business Technology Platform (BTP)
- Experience in integrating different Business Cloud Solutions (Coupa, Salesforce) with SAP
- Strong knowledge of SAP Finance and Controlling business processes.
- Experience in system configuration, optimization, and performance tuning.
- Solid understanding of SAP security principles and best practices.
- Knowledge of integration with other SAP modules and third-party systems.
- Familiar with Python as a programming language
- A basic understanding of BPMN

Firmly rooted in our values, EFG is an affirmative action employer that celebrates being an equal-opportunity workplace. Our unwavering commitment to fair employment extends to all individuals, regardless of their race, color, ancestry, religion, sex, national origin, age, sexual orientation, disability, citizenship, marital status, gender identity, or Veteran status.

Obraz 7.4.4 oferta pracy organizacji ESL FACEIT GROUP, źródło linkedin.com, data wykonania zrzutu 10.12.2023 r.

Na obrazach 7.5.1-7.5.3 zaprezentowano, że domena używa technologii kubernetes, we współpracy z google. Kubernetes to otwarte oprogramowanie do zarządzania kontenerami, które umożliwia automatyzację wdrażania, skalowania i zarządzania aplikacjami kontenerowymi.



Obraz 7.5.1 dokument określający współpracę Faceit i Google, źródło cloud.google.com, data wykonania zrzutu 10.12.2023 r.

cloud.google.com/customers/faceit

Google Cloud Overview Solutions Products Pricing Resources Docs Support Language Console

Contact Us

FACEIT spent time planning its transition to Google Cloud so as not to incur any unnecessary downtime. With Jetstack's help, the company migrated its infrastructure within two months, with no disruption to its users. The core of FACEIT's new architecture was Kubernetes Engine, to simplify the creation and management of Kubernetes clusters.

"With Kubernetes Engine, we just don't have to worry about the infrastructure," says Emanuele. "By the time we've got our laptops out, any problems have already been resolved automatically and our job is to go through the logs and diagnose what went wrong."

The company used Container Registry to store and manage its container images and Cloud Storage to hold and help secure static assets such as images and configuration files. Google Stackdriver gave FACEIT the ability to monitor its system in depth. Separately, the stateful services that FACEIT needed ran on Compute Engine instances which are scaled up and down automatically when needed.

With the migration complete, FACEIT has found the new way of deploying much easier than before, when everything had to be set up manually. "We had to log in to the UI and manually copy over settings between browser windows for new releases, hoping that we hadn't made any mistakes," says Bradley. "Now we have a single config file for each service. We can just modify that, version it, and it works without having to go anywhere near the UI."

This model of infrastructure as code has made deployment far less prone to mistakes, and if there are ever any problems, they are now much easier to fix. According to Bradley, this has led to a much more stable platform with happier customers and partners. "We don't get woken up in the middle of the night anymore!" he says.

Obraz 7.5.2 dokument określający współpracę Faceit i Google, źródło linkedin.com, data wykonania zrzutu 10.12.2023 r.

A stable solution for today, a solid foundation for tomorrow

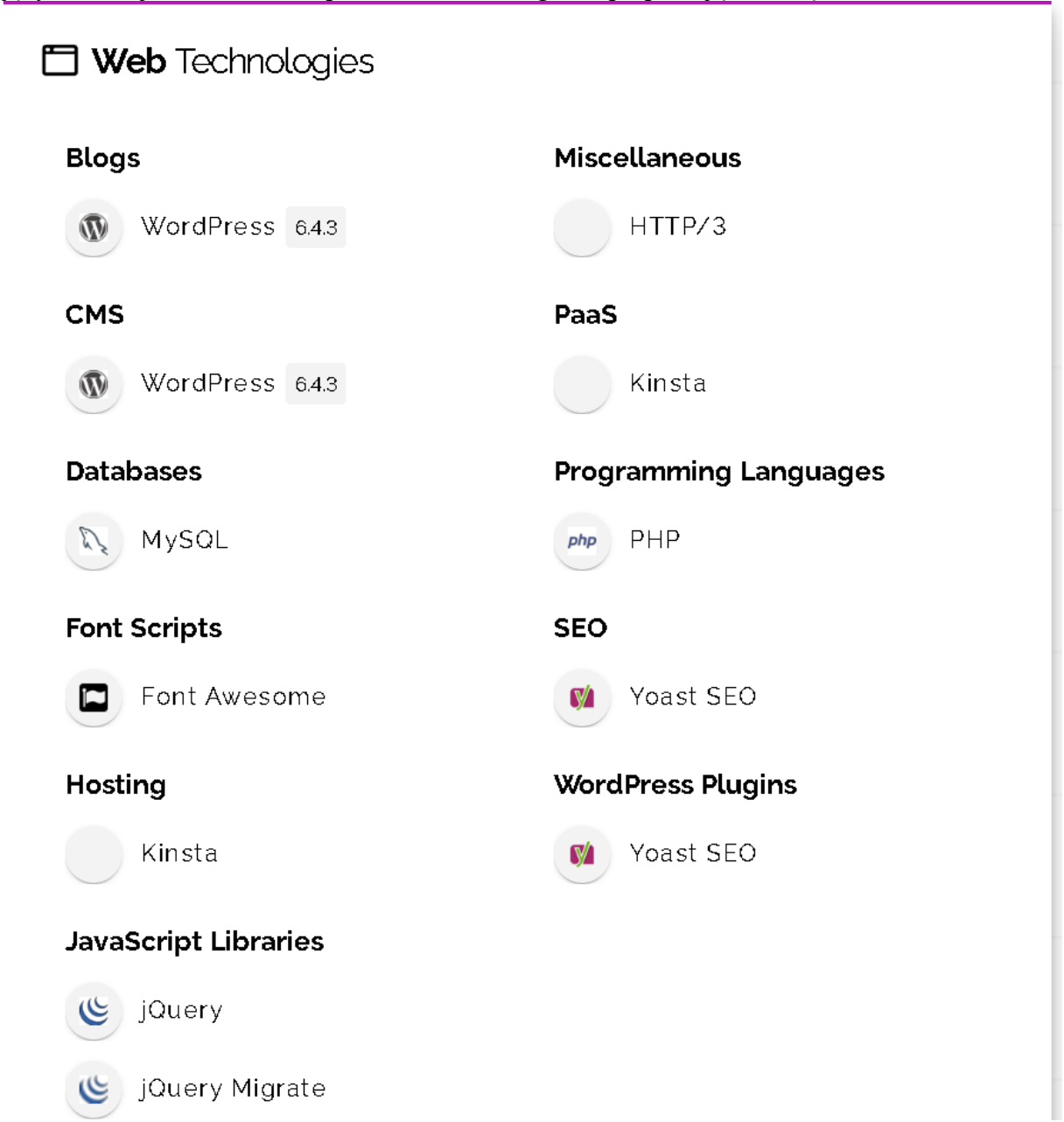
After the move to Google Cloud, FACEIT has continued to grow and grow, with season 6 of its biannual esports Championship Series (ECS), the most popular Counter-Strike: Global Offensive league in the world, being broadcast to 250,000 viewers exclusively on YouTube. The aftermath of an event like that shows off the scaling capabilities of the new infrastructure, as keen gamers log in to play the games they've just been watching causing large spikes in traffic.

FACEIT's quest for newer and better ways of working has not stopped. FACEIT is currently exploring BigQuery and Cloud Dataflow to optimize its data pipelining processes as well as Cloud Pub/Sub to replace its existing messaging service. For Emanuele, all this is possible because of the new atmosphere created by the move to Google Cloud.

"We're looking to make things even faster and reduce the complexity of the code even further," he says. "It comes down to having a solid foundation from which to build. If we hadn't reconfigured the infrastructure and adopted best practices, we couldn't think about doing any of this."

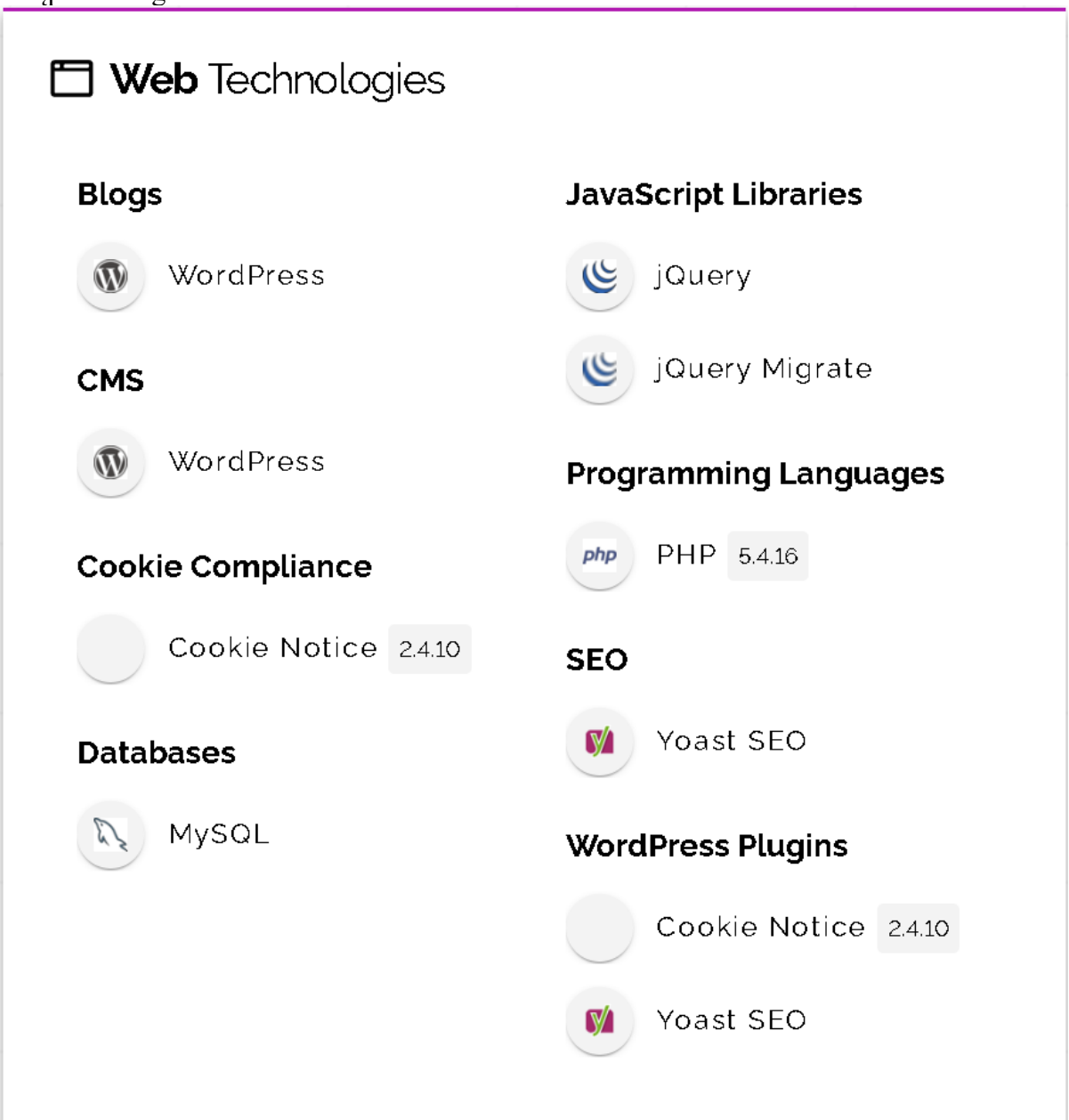
Obraz 7.5.3 dokument określający współpracę Faceit i Google, źródło linkedin.com, data wykonania zrzutu 10.12.2023 r.

Na obrazie 7.6.1 przedstawiono technologie wykorzystywane na stronie r6collegiate.faceit.com. WordPress w wersji 6.4.3 zostanie w rozdziale 9 sprawdzony pod kątem podatności. Występowanie bazy MySQL, systemu zarządzania treścią WordPress i języka PHP jest zrozumiałe, ponieważ technologie współpracują ze sobą.



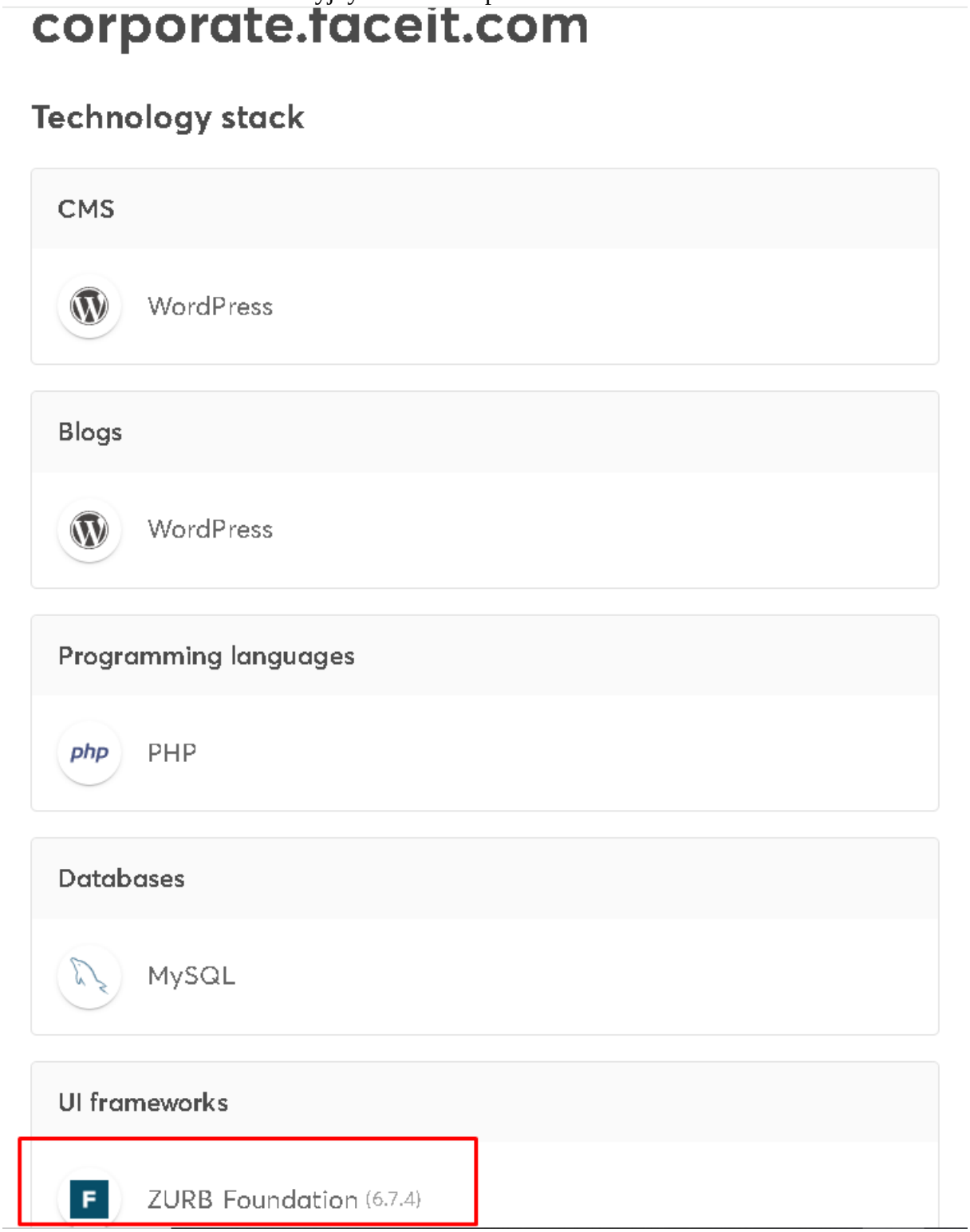
Obraz 7.6.1 Technologie informatyczne wykorzystywane przez hosta r6collegiate.faceit.com, źródło shodan.io, data wykonania zrzutu 07.02.2024 r.

Na obrazach 7.7.1, 7.7.2 przedstawiono technologie wykorzystywane na stronie corporate.faceit.com. Cookie Notice w wersji 2.4.10, PHP w wersji 5.4.16, Yoast Seo v21.5, core-js 3.25.5, jQuery v3.7.1 zostaną w rozdziale 9 sprawdzone pod kątem podatności. jQuery to szybka, mała i funkcjonalna biblioteka JavaScript. Umożliwia uproszczenie operacji takich jak przeszukiwanie dokumentu HTML, obsługa zdarzeń, animacje i interakcje Ajax. Mając na uwadze wykorzysywanie przez orgazniacje React i Angular, jQuery może w przyszłości zostać zastąpiane Angular'em lub React'em.



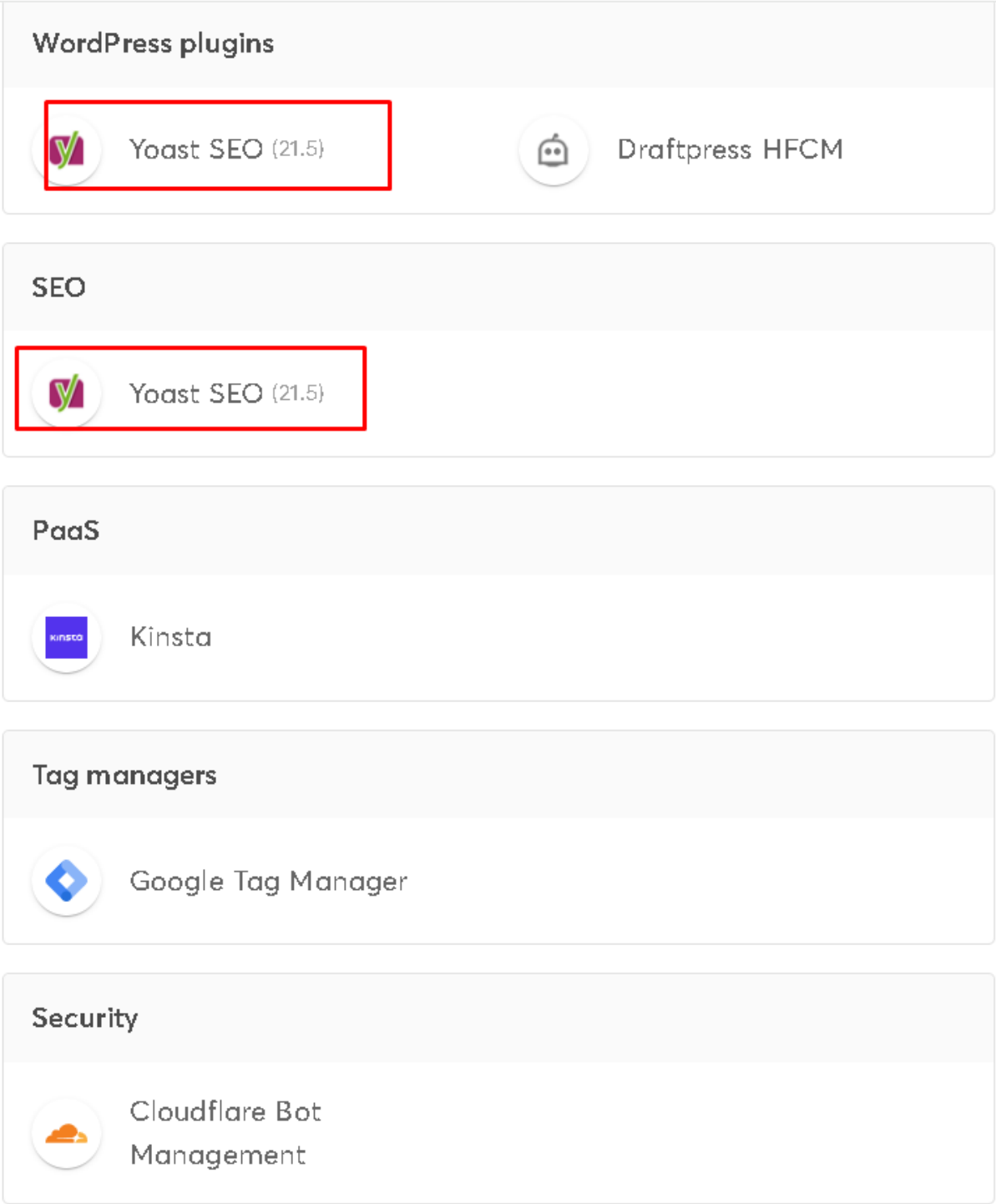
Obraz 7.7.1 Technologie informatyczne wykorzystywane przez poddomenę corporate.faceit.com, źródło shodan.io, data wykonania zrzutu 07.02.2024 r.

Zurb Foundation to konkurencyjny do Bootstrap framework CSS.

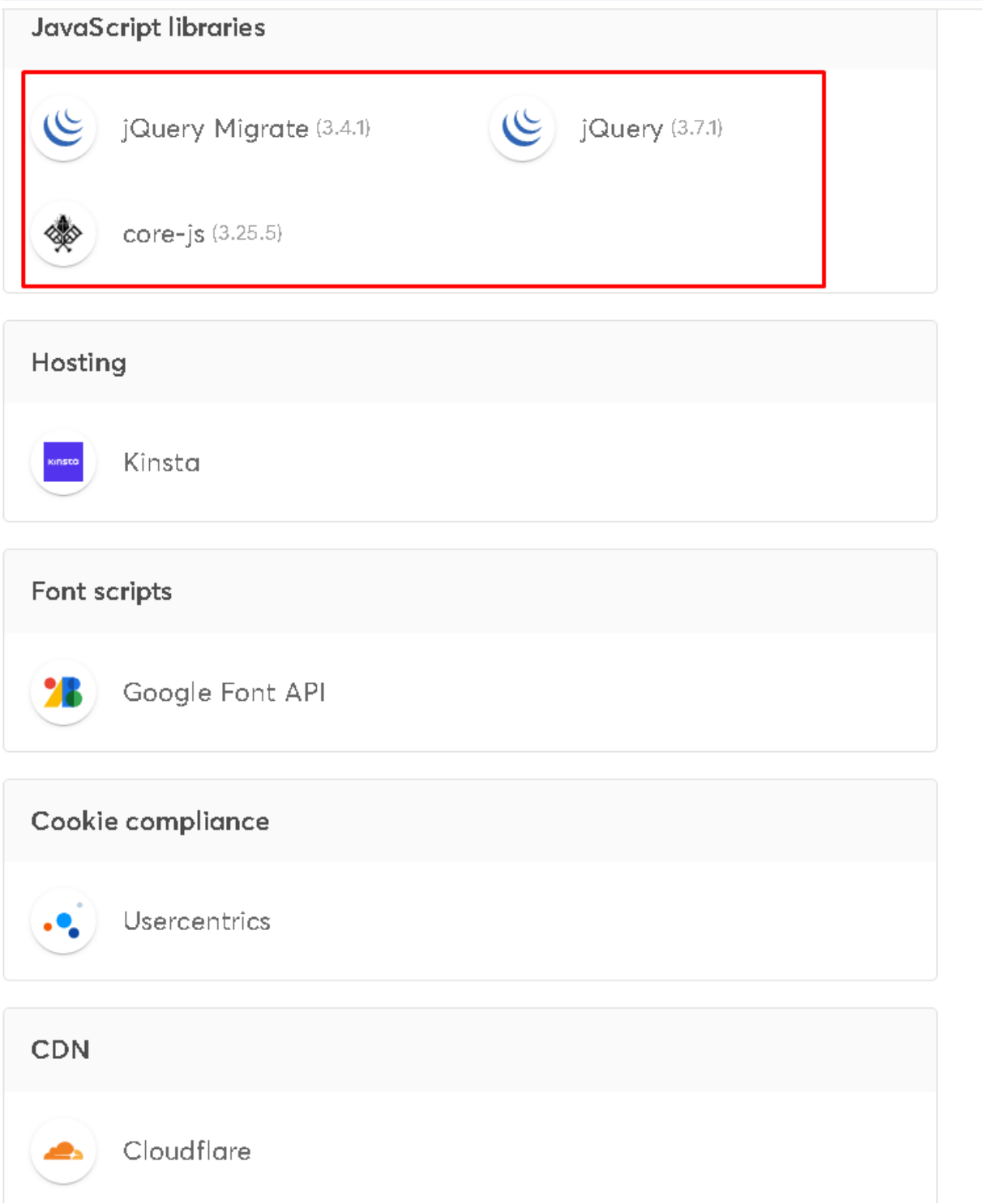


Obraz 7.7.2 wykorzystywane technologie strona corporate.faceit.com. wappalyzer.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.

Cloudflare Bot Management zapewnia narzędzia do ochrony witryn przed szkodliwymi botami, a także do optymalizacji działania i korzystania z przydatnych botów, takich jak boty wyszukiwarek.

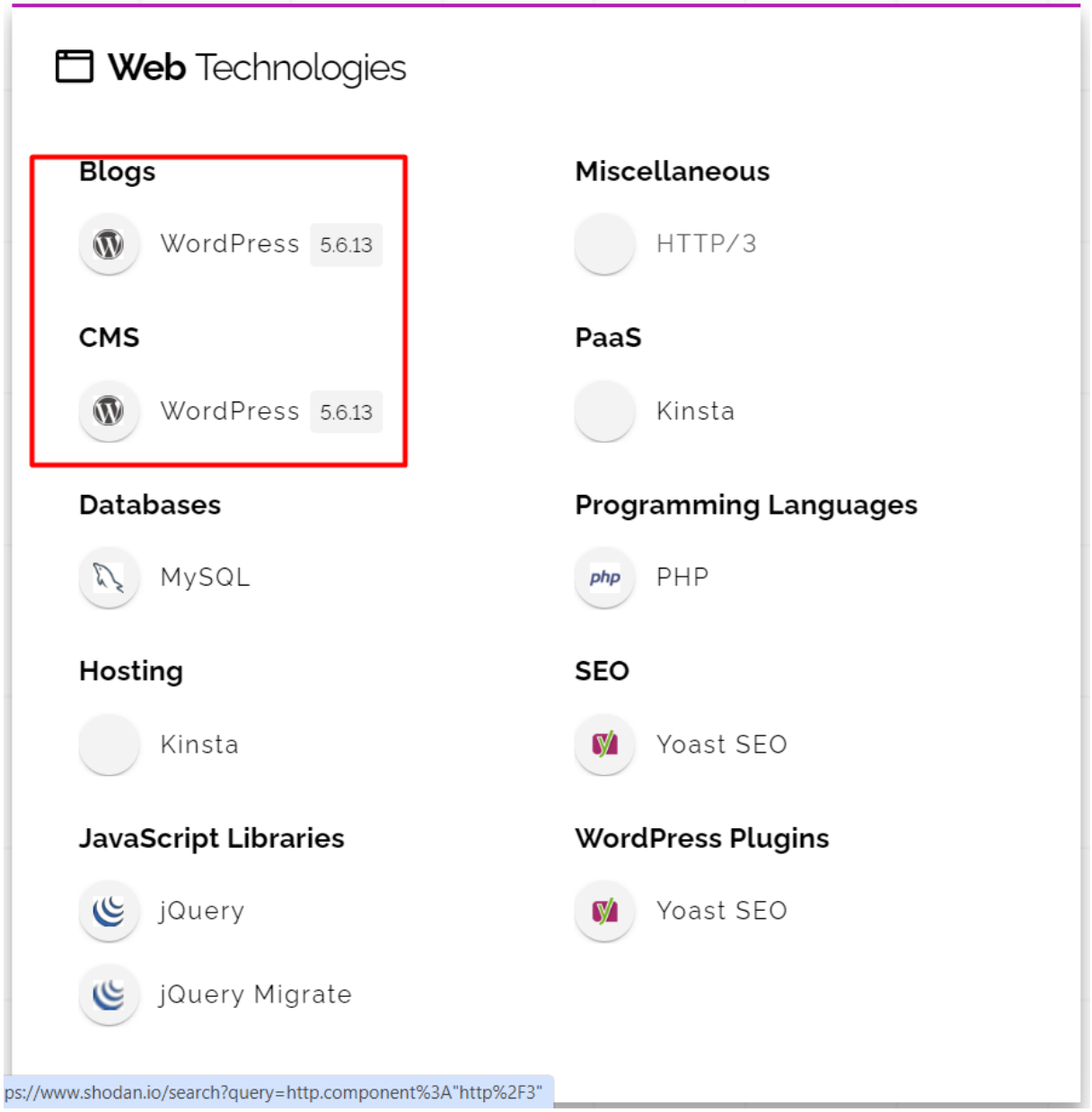


Obraz 7.7.3 wykorzystywane technologie strona corporate.faceit.com. wappalyzer.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.



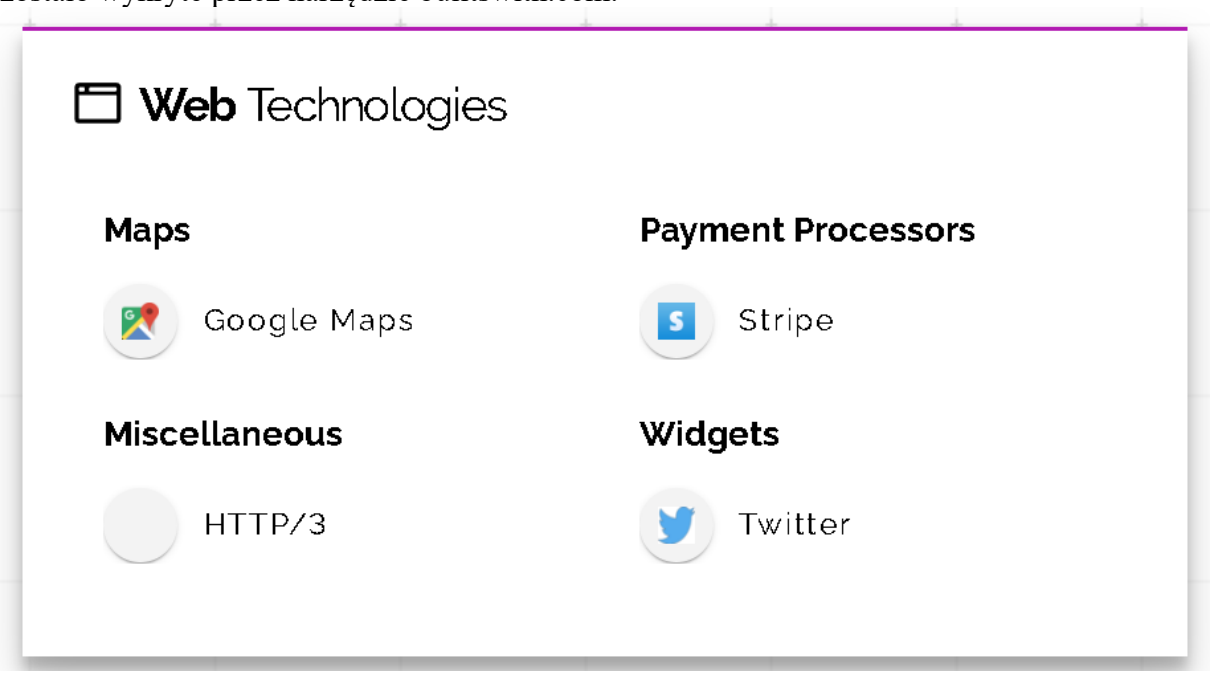
Obraz 7.7.4 wykorzystywane technologie strona corporate.faceit.com. wappalyzer.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.

Na obrazie 7.8.1 przedstawiono technologie wykorzystywane na stronie gwb.faceit.com. WordPress w wersji 5.6.13 zostanie w rozdziale 9 sprawdzony pod kątem podatności. Kinsta PaaS to zaawansowana i wydajna platforma hostingowa zaprojektowana specjalnie dla użytkowników WordPressa, zapewniająca wysoką wydajność, bezpieczeństwo.

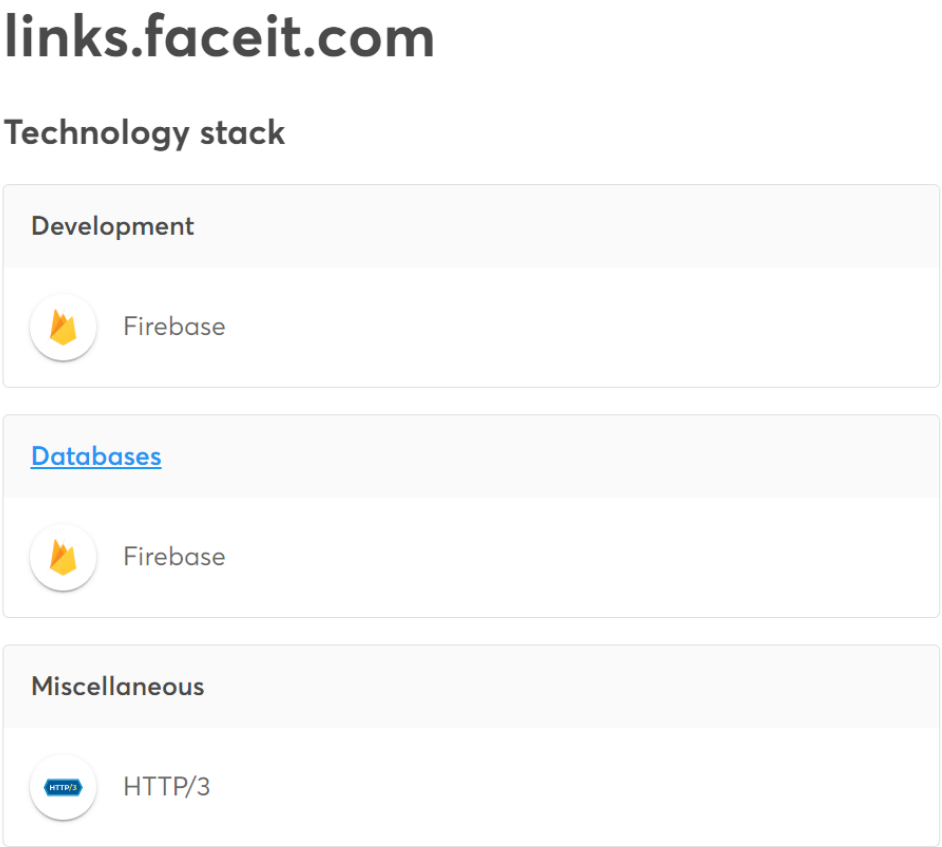


Obraz 7.8.1 Technologie informatyczne wykorzystywane przez poddomenę gwb.faceit.com, źródło shodan.io, data wykonania zrzutu 07.02.2024 r.

Na obrazach 7.9.1, 7.9.2 przedstawiono technologie wykorzystywane na stronie links.faceit.com. Narzędzie wappalyzer.com wykryło używanie bazy danych firebase, co nie zostało wykryte przez narzędzie builtswith.com.

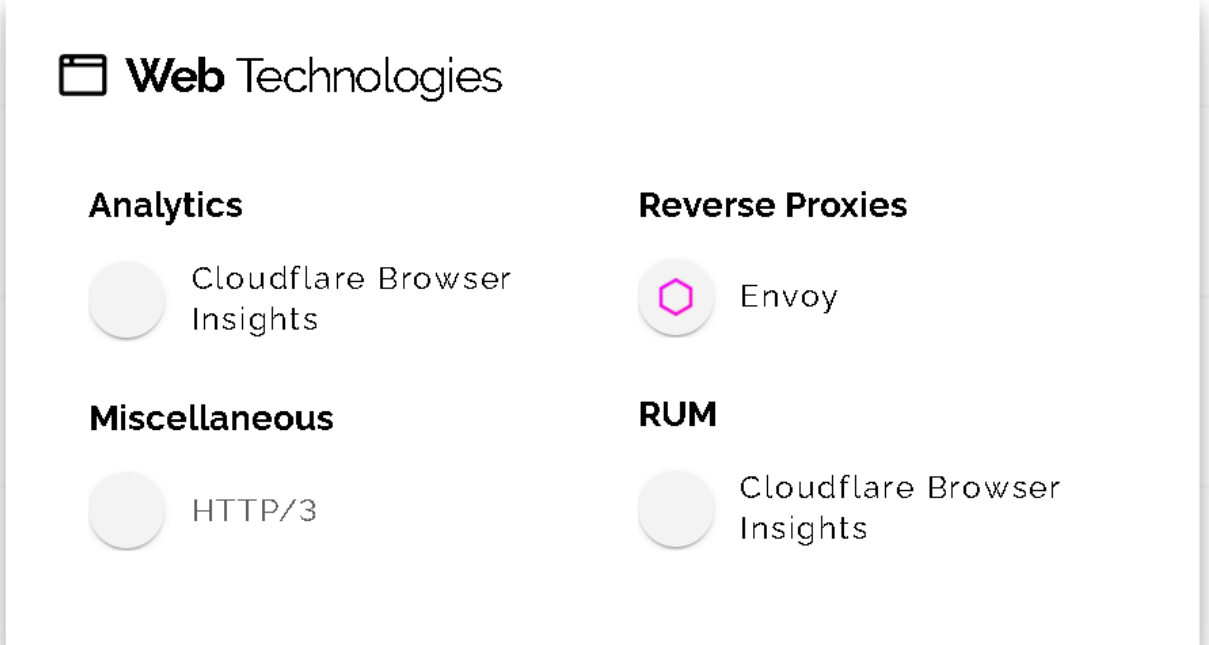


Obraz 7.9.1 Technologie informatyczne wykorzystywane przez poddomenę links.faceit.com, źródło shodan.io, data wykonania zrzutu 07.02.2024 r.



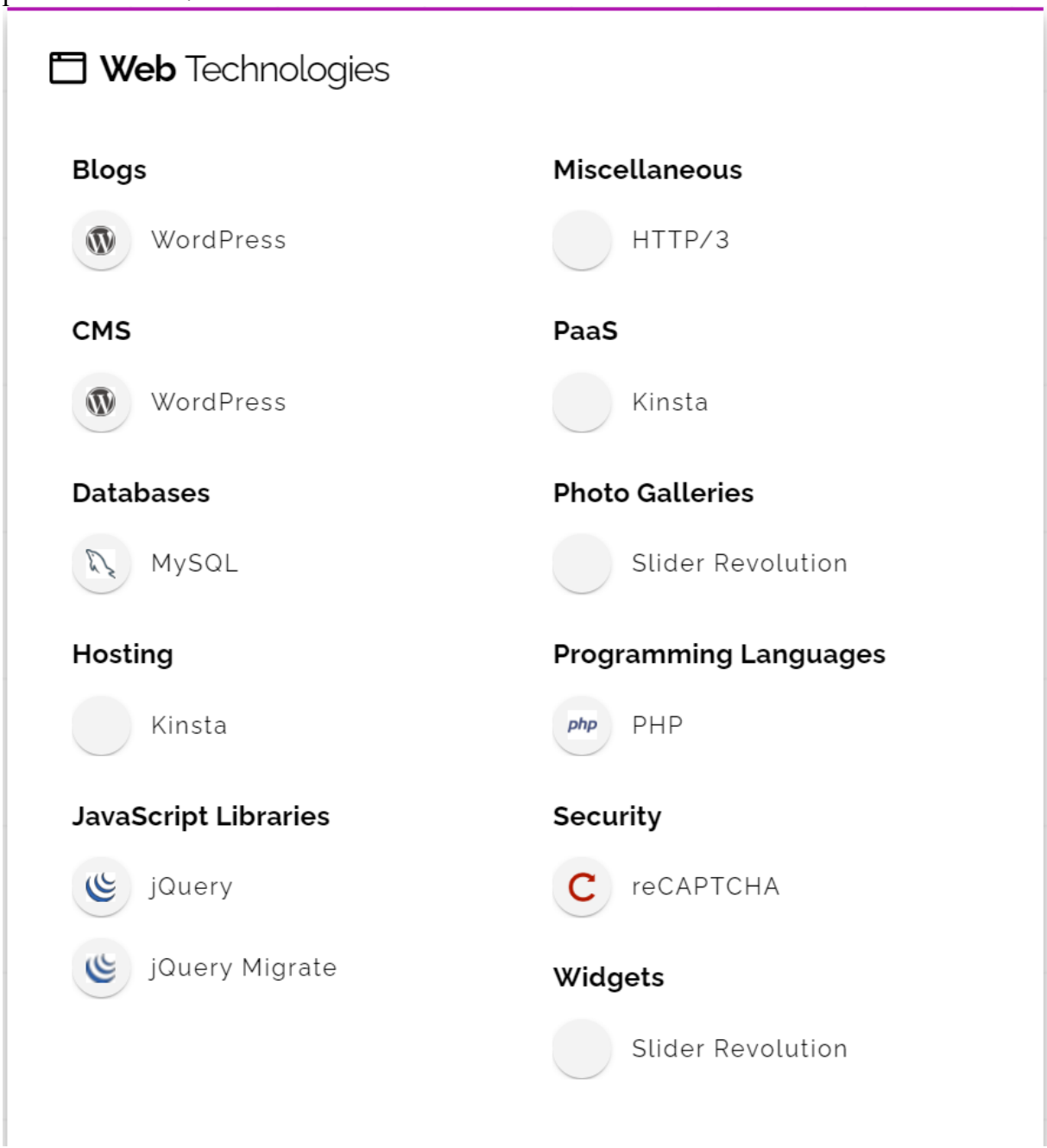
Obraz 7.9.2 Technologie informatyczne wykorzystywane przez poddomenę links.faceit.com, źródło wappalyzer.com, data wykonania zrzutu 09.02.2024 r.

Na obrazie 7.10.1 przedstawiono technologie wykorzystywane na stronie sheriff-api.faceit.com. Envoy Proxy jest często wykorzystywany w kontekście architektur opartych na mikroserwisach, kontenerach oraz w środowiskach chmurowych, co jak najbardziej ma zastosowanie do poddomen faceit.com, które są oparte o te architektury.



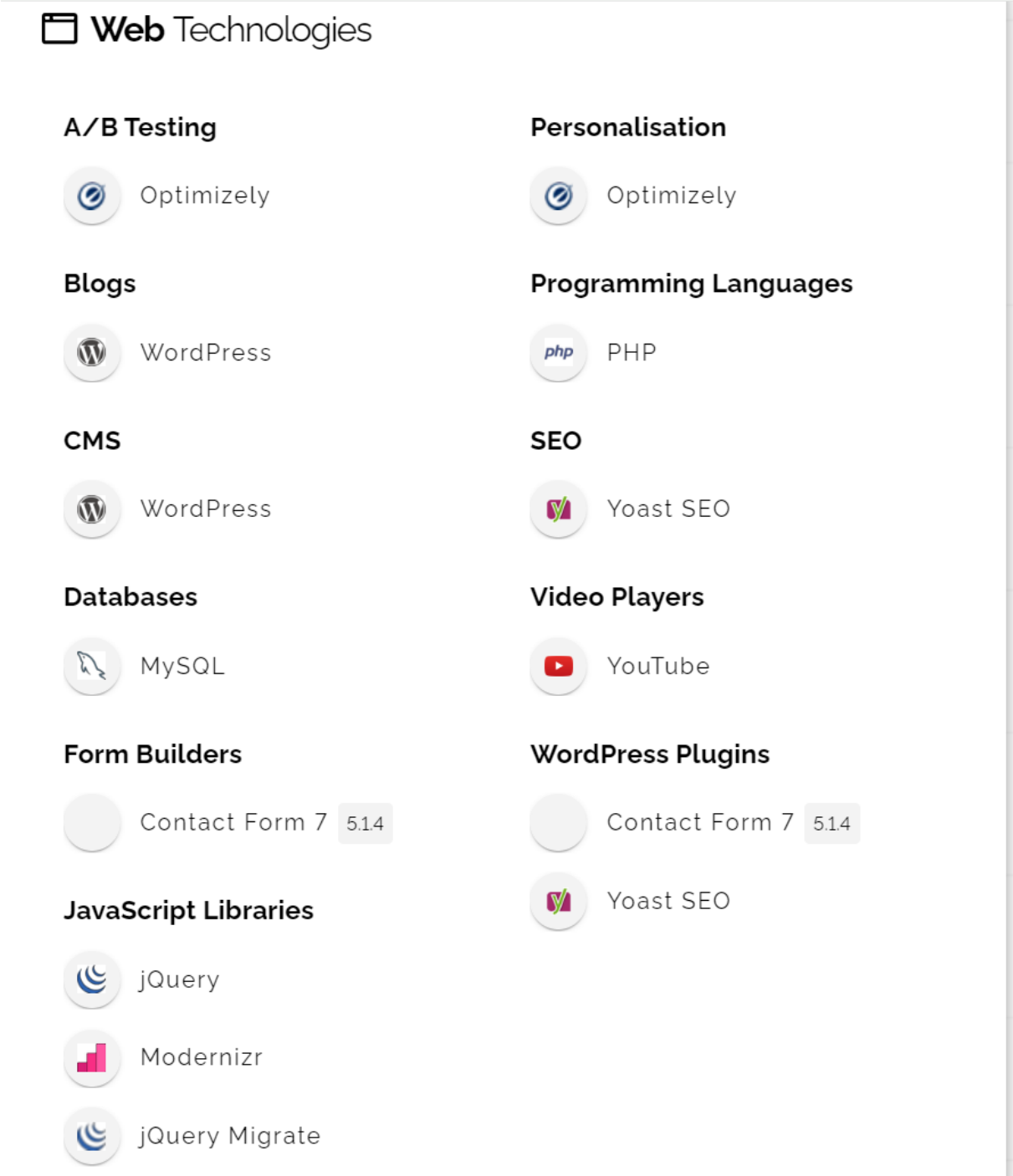
Obraz 7.10.1 Technologie informatyczne wykorzystywane przez poddomenę sheriff-api.faceit.com, źródło shodan.io, data wykonania zrzutu 07.02.2024 r.

Na obrazie 7.11.1 przedstawiono technologie wykorzystywane na stronie verify.faceit.com. ReCAPTCHA jest często używana, ponieważ jest skutecznym narzędziem w walce z automatycznymi botami i spamem. Slider Revolution jest często używany przez projektantów i deweloperów stron internetowych, aby wzmocnić wrażenia wizualne użytkowników, promować treści.



Obraz 7.11.1 Technologie informatyczne wykorzystywane przez poddomenę verify.faceit.com, źródło shodan.io, data wykonania zrzutu 07.02.2024 r.

Na obrazie 7.12.1 przedstawiono technologie wykorzystywane na stronie blog.faceit.com. Core-js w wersji 3.30.2 zostanie w rozdziale 9 sprawdzony pod kątem podatności. Optimizely pozwala organizacjom przeprowadzać eksperymenty w celu zrozumienia, które wersje ich stron internetowych lub funkcji są najbardziej skuteczne w przyciąganiu użytkowników.



Obraz 7.12.1 Technologie informatyczne wykorzystywane przez poddomenę blog.faceit.com, źródło shodan.io, data wykonania zrzutu 07.02.2024 r.

blog.faceit.com

Technology stack

Blogs

Medium

Programming languages

Node.js

GraphQL

Reverse proxies

Envoy

Security

reCAPTCHA

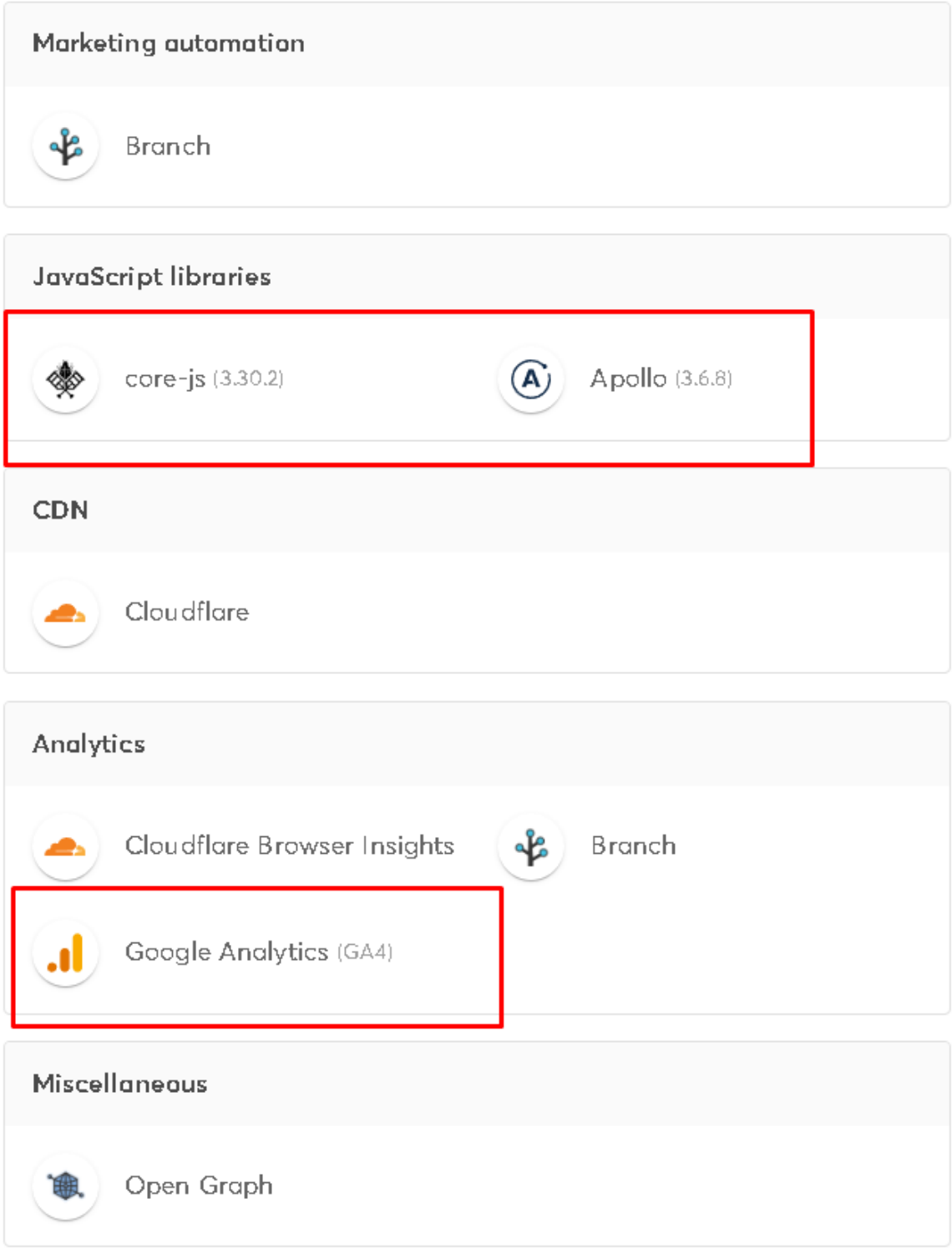
Cloudflare Bot Management

RUM

Cloudflare Browser Insights

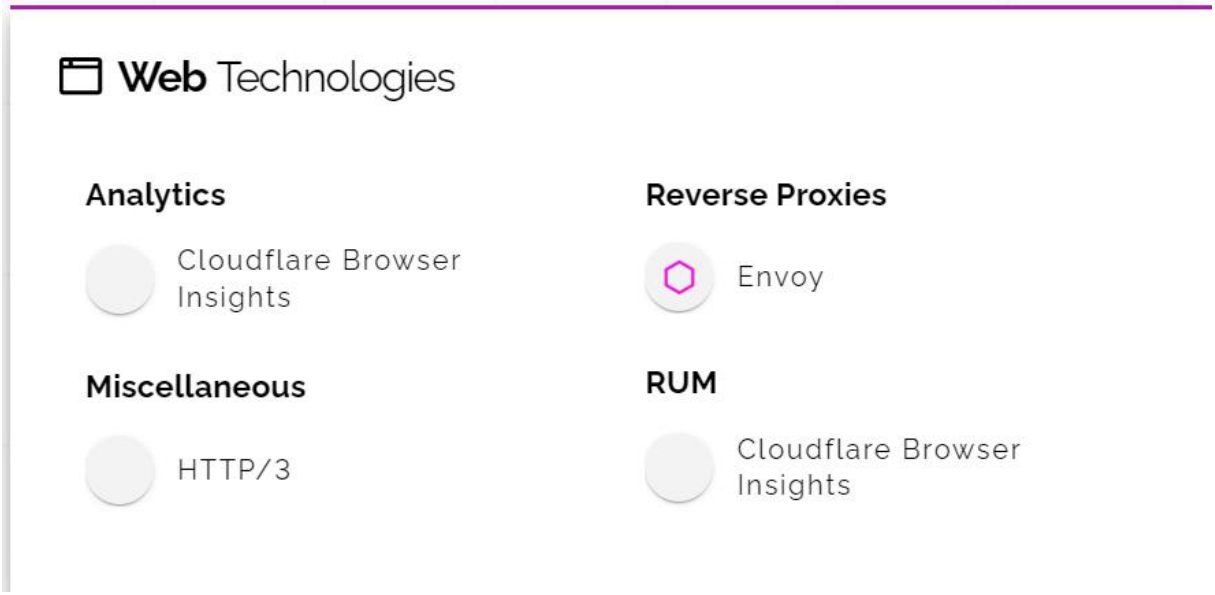
Obraz 7.12.2 wykorzystywane technologie strona blog.faceit.com. wappalyzer.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.

Branch Analytics jest szczególnie przydatne dla prowadzenia kampanii marketingowych w aplikacjach mobilnych.



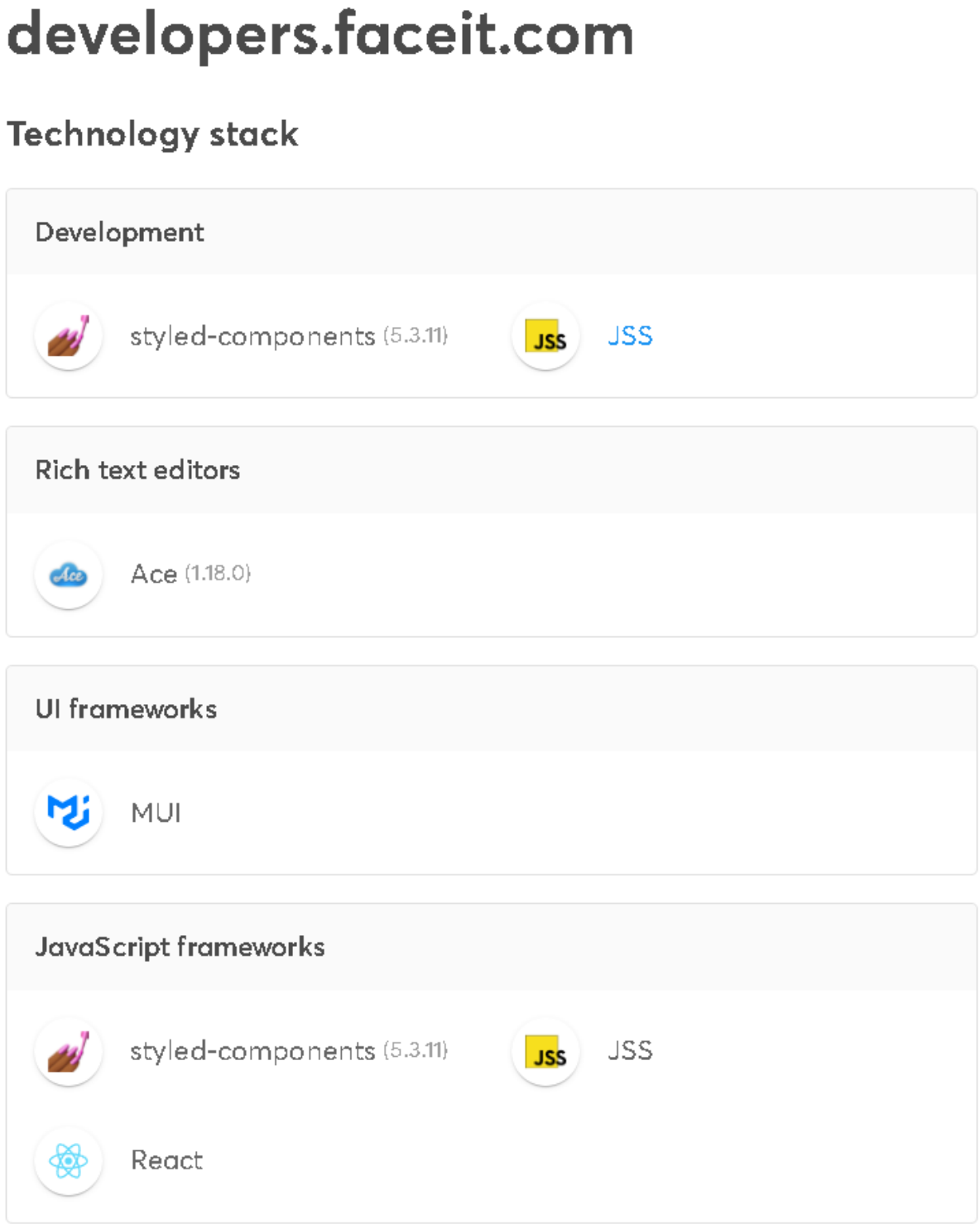
Obraz 7.12.3 wykorzystywane technologie strona blog.faceit.com. wappalyzer.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.

Na obrazie 7.13.1 przedstawiono technologie wykorzystywane na stronie ingame-accounts.faceit.com.

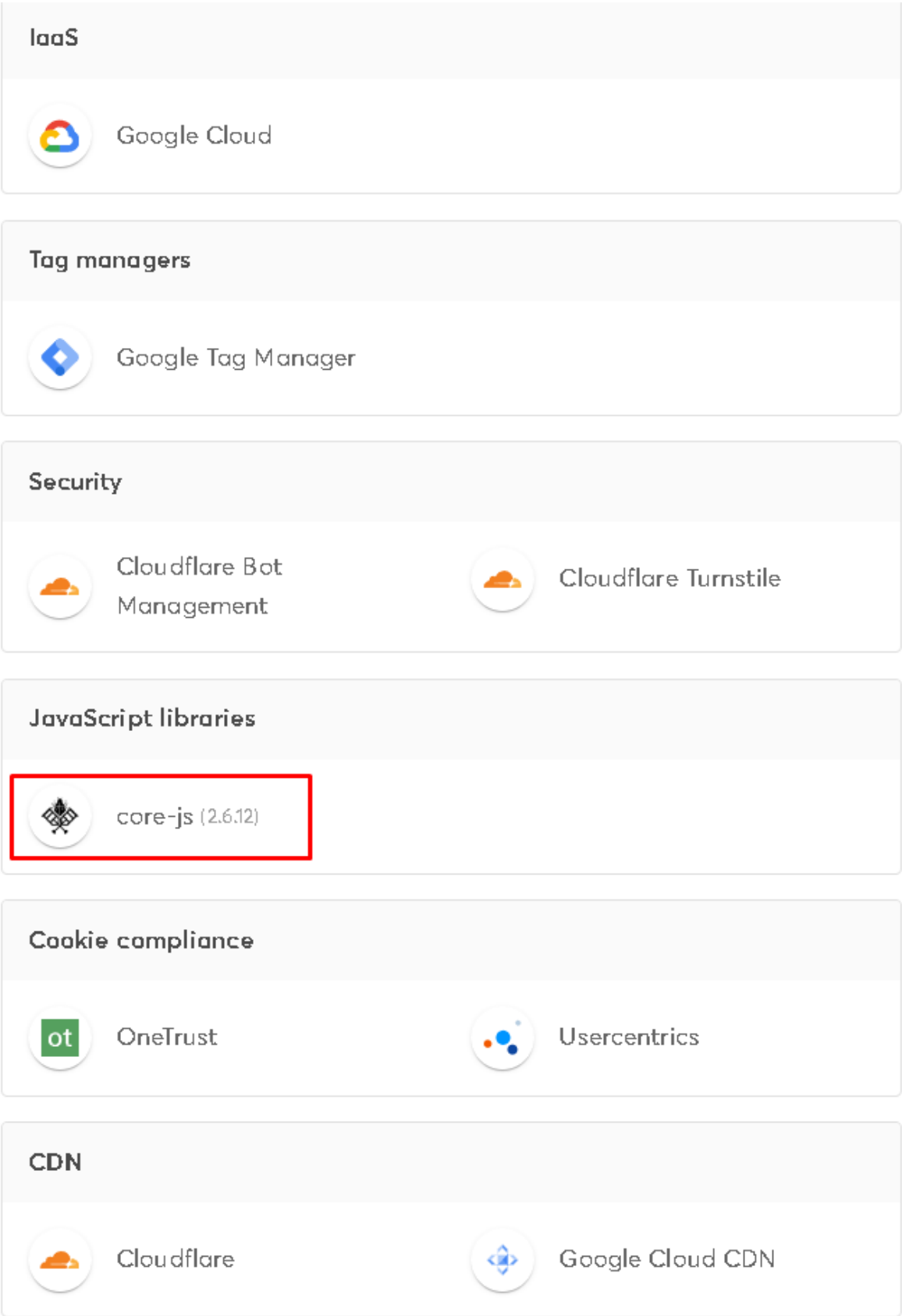


Obraz 7.13.1 Technologie informatyczne wykorzystywane przez poddomenę ingame-accounts.faceit.com, źródło shodan.io, data wykonania zrzutu 07.02.2024 r.

Na obrazie 7.13.1 przedstawiono technologie wykorzystywane na stronie developers.faceit.com. Core-js w wersji 2.6.12, Styled-Components v5.3.13 zostaną w rozdziale 9 sprawdzone pod kątem podatności. MUI jest zbudowany na bazie Reacta, co oznacza, że jest łatwo integrowalny z aplikacjami opartymi na React.

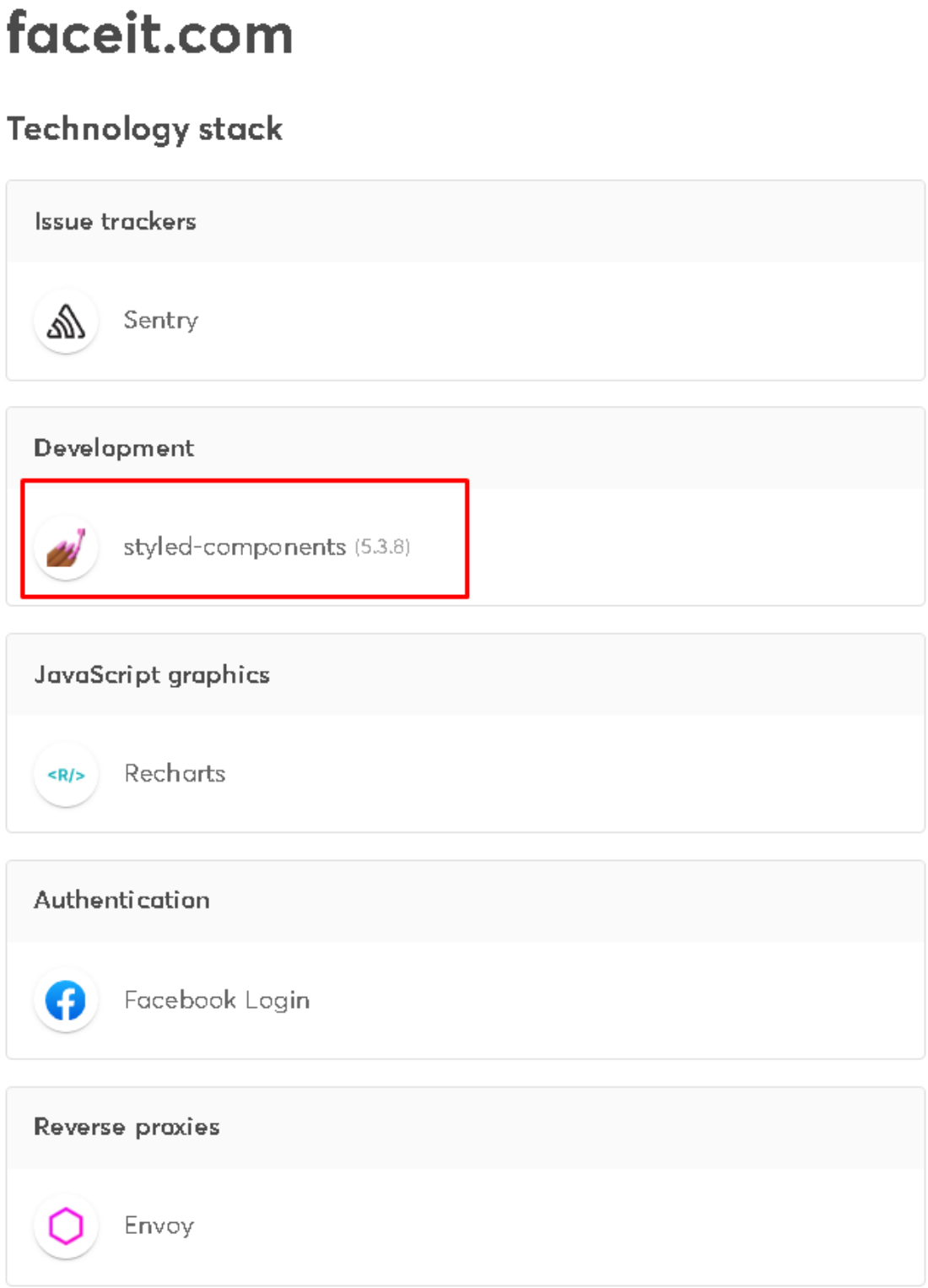


Obraz 7.13.1 wykorzystywane technologie strona developers.faceit.com. wappalyzer.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.



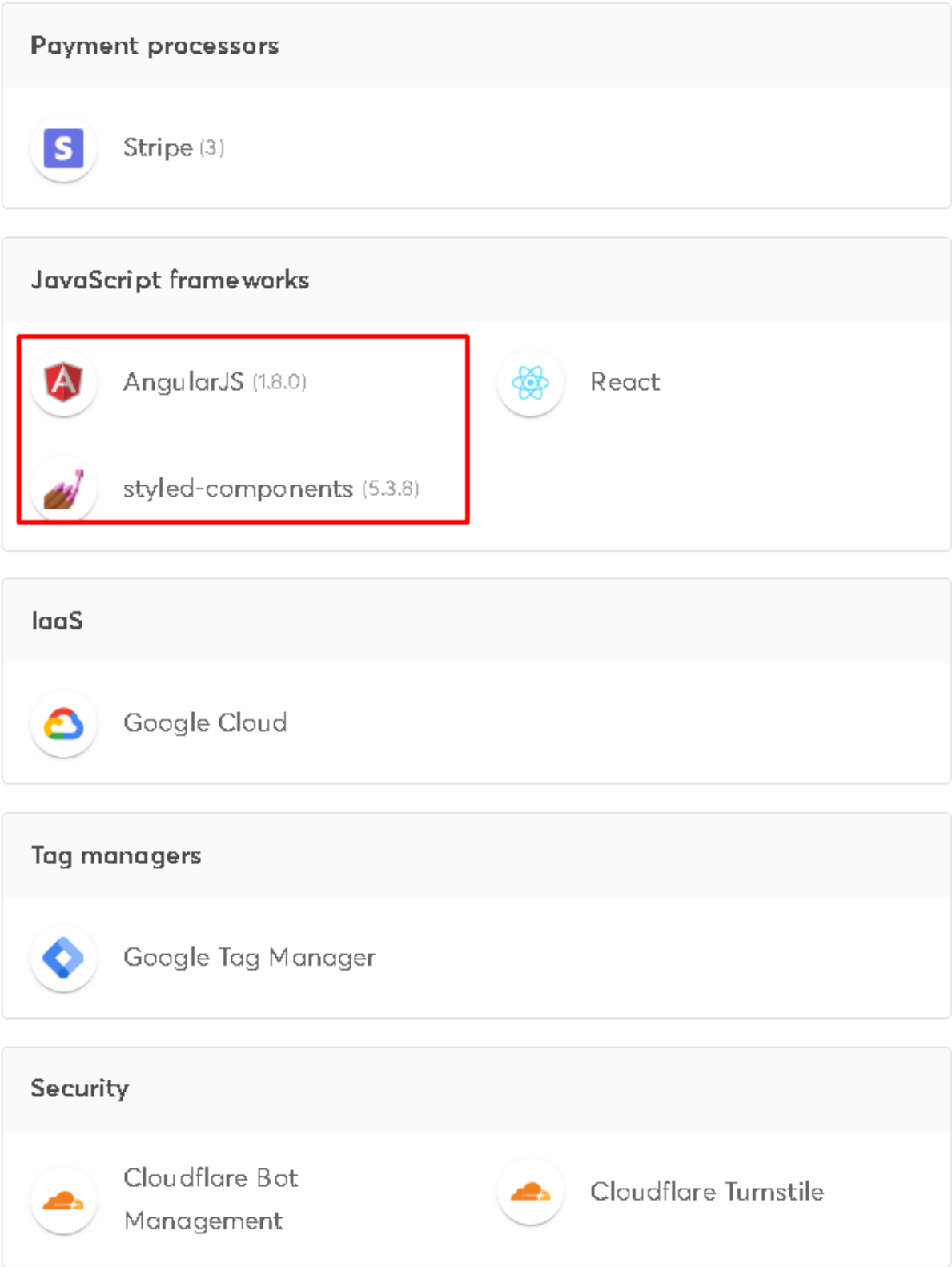
Obraz 7.13.2 wykorzystywane technologie strona developers.faceit.com. wappalyzer.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.

Na obrazach 7.14.1-7.14.4 przedstawiono technologie wykorzystywane na stronie faceit.com. Lodash v4.17.21, jQuery v3.5.1, core-js v3.27.0, Styled-components v5.3.8, Angular v1.8.0 zostaną w rozdziale 9 sprawdzone pod kątem podatności. Sentry to platforma monitorowania wyjątków i błędów w aplikacjach, która pomaga deweloperom śledzić, debugować i naprawiać problemy w swoich kodach.



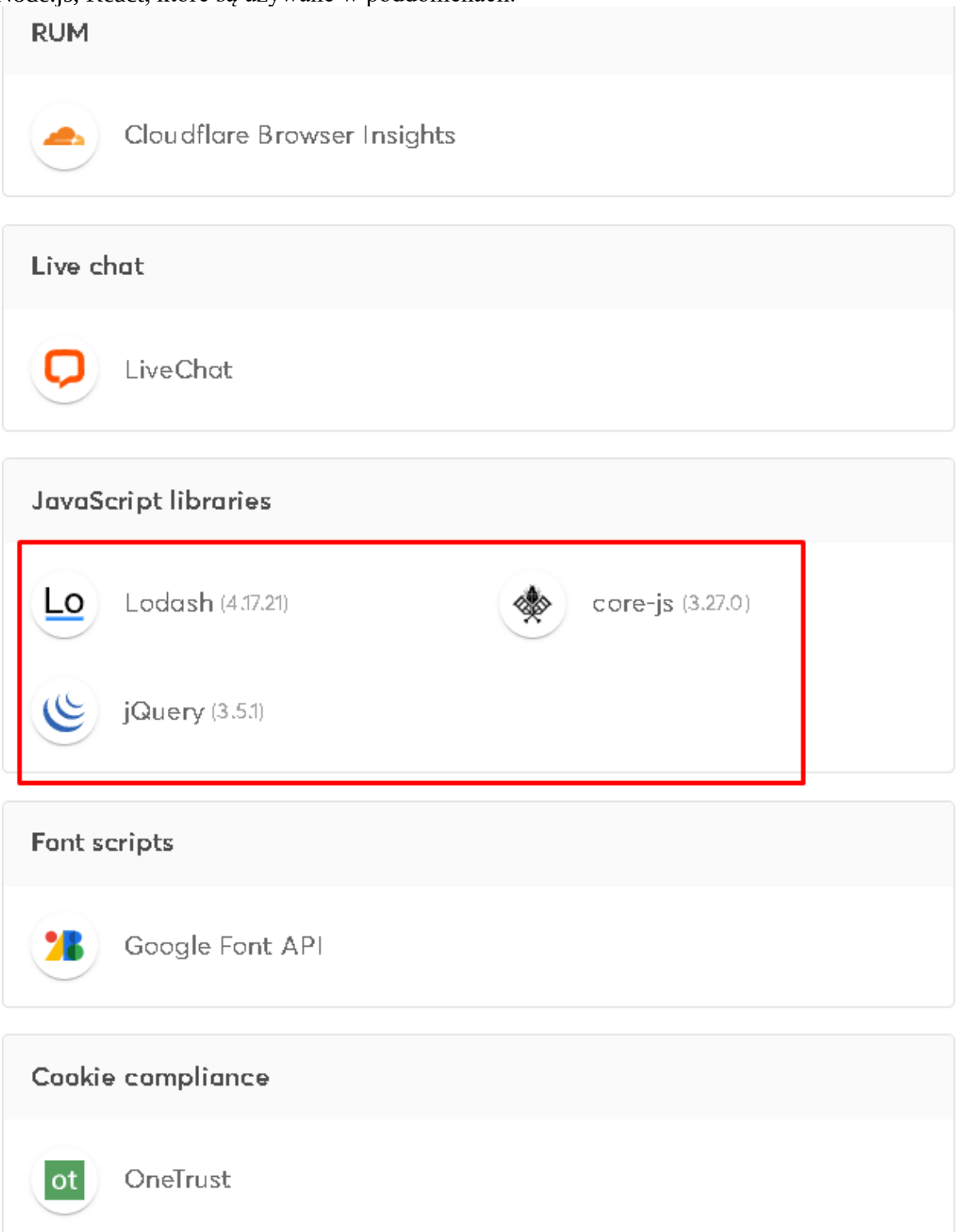
Obraz 7.14.1 wykorzystywane technologie strona faceit.com, źródło wappalyzer.com, data wykonania zrzutu 08.02.2024 r.

Płatności Stripe zapewniają wysoki poziom bezpieczeństwa transakcji, w tym zgodność z wymogami PCI DSS oraz obsługę autoryzacji dwuetapowej.

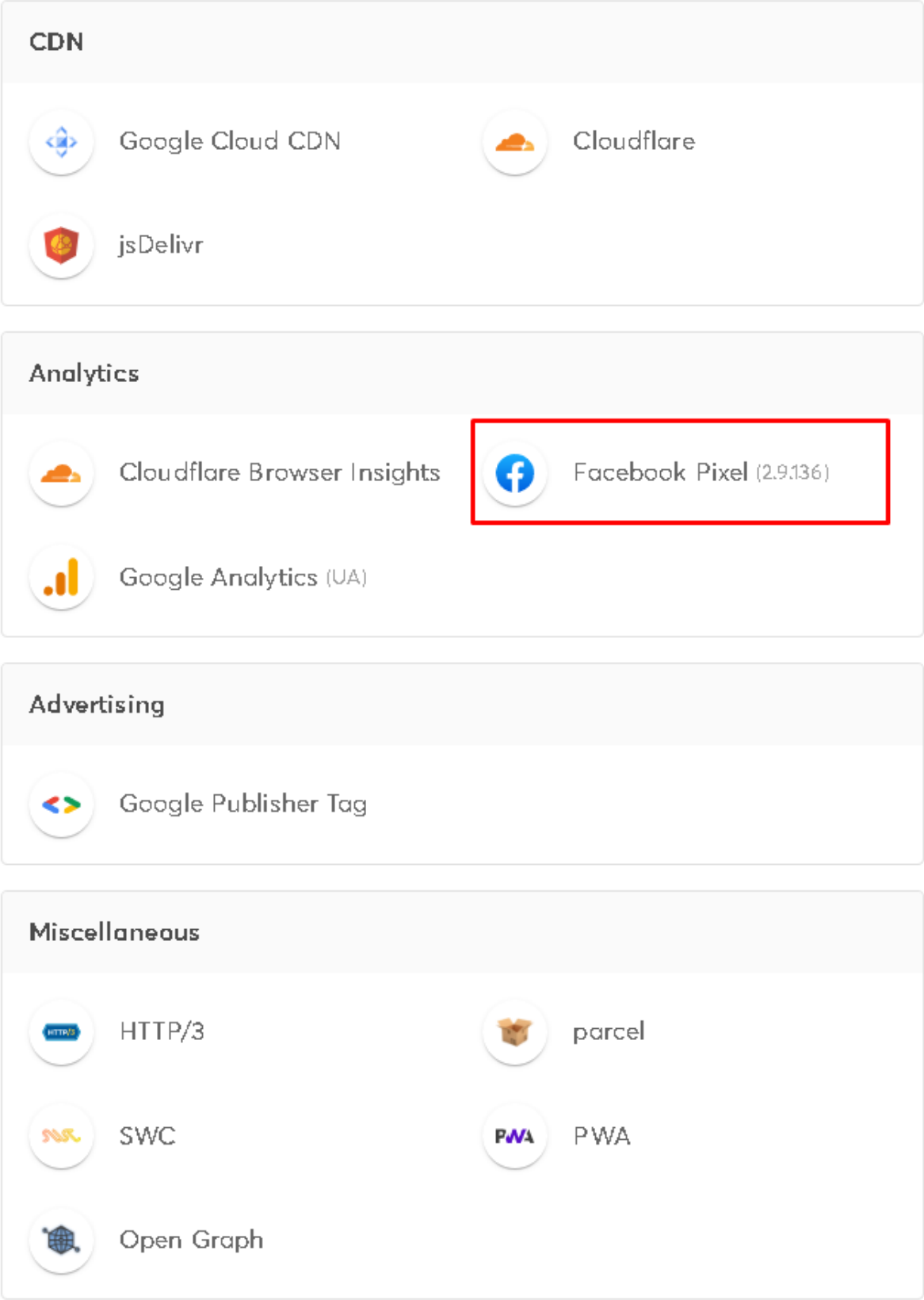


Obraz 7.14.2 wykorzystywane technologie strona faceit.com, źródło wappalyzer.com, data wykonania zrzutu 08.02.2024 r.

Lodash jest kompatybilny z wieloma różnymi środowiskami JavaScript, takimi jak środowiska Node.js, React, które są używane w poddomenach.

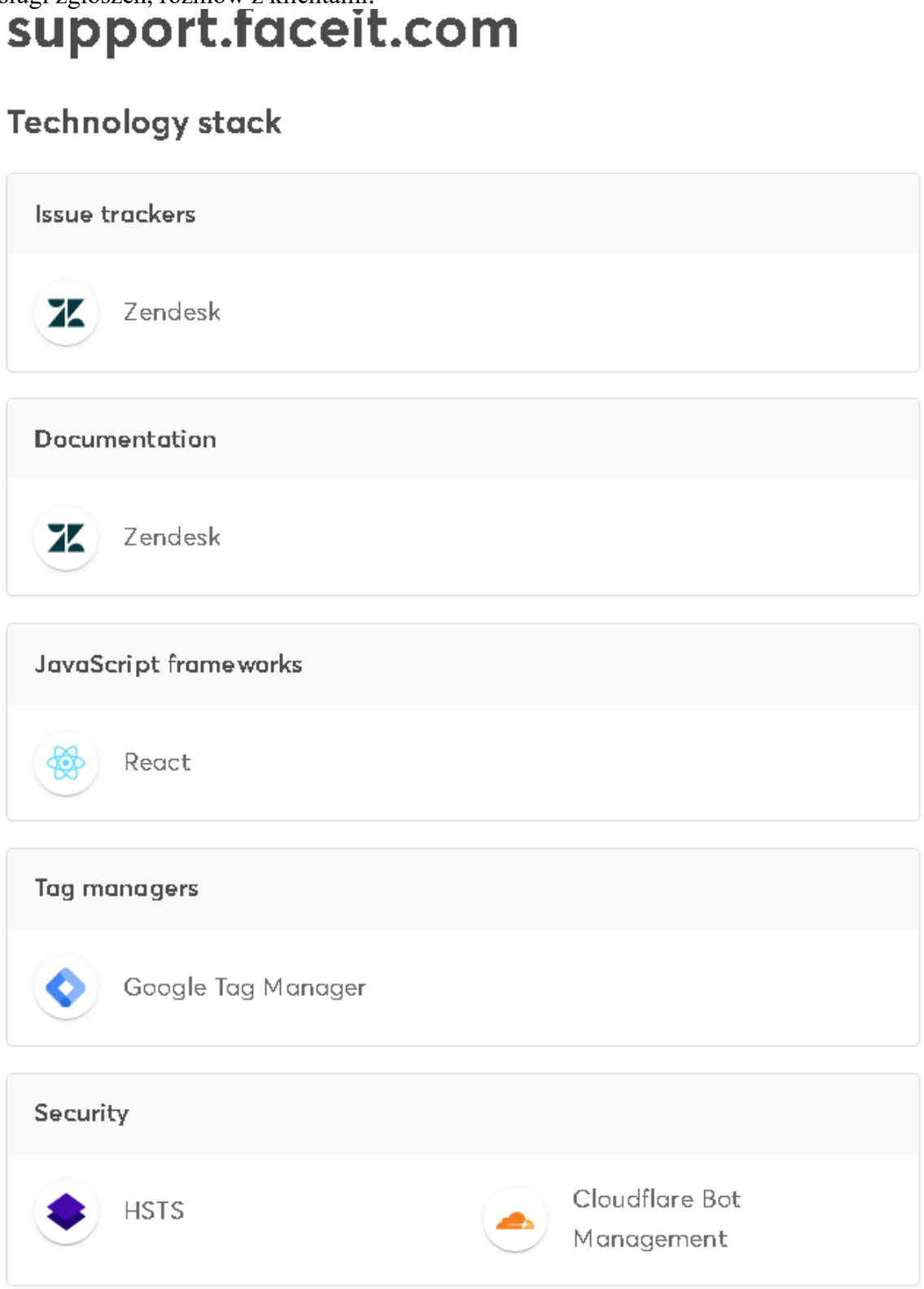


Obraz 7.14.3 wykorzystywane technologie strona faceit.com, źródło wappalyzer.com, data wykonania zrzutu 08.02.2024 r.

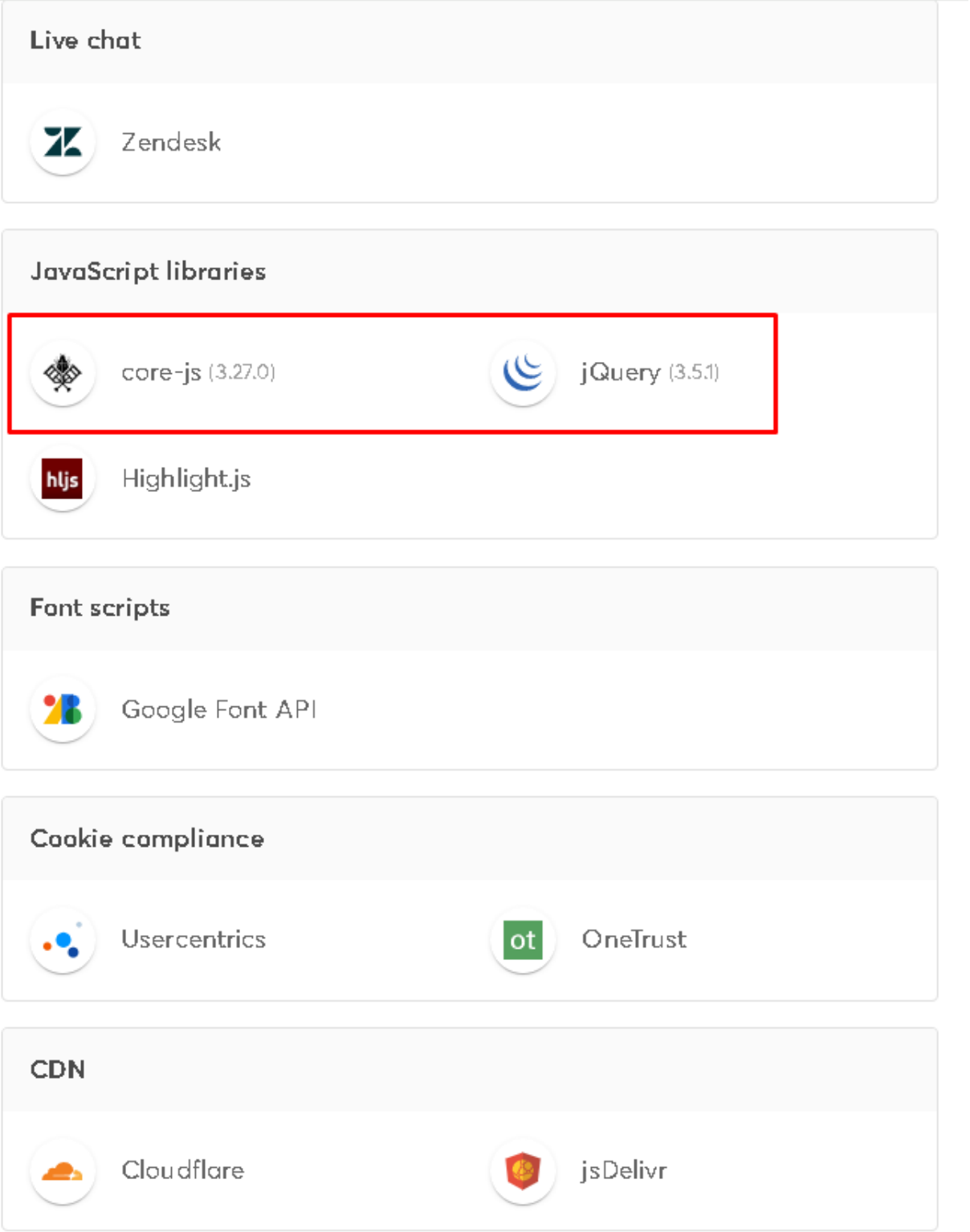


Obraz 7.14.4 wykorzystywane technologie strona faceit.com, źródło wappalyzer.com, data wykonania zrzutu 08.02.2024 r.

Na obrazach 7.15.1, 7.15.2 przedstawiono technologie wykorzystywane na stronie support.faceit.com. jQuery v3.5.1, core-js v3.27.0 zostaną w rozdziale 9 sprawdzone pod kątem podatności. HSTS wymusza użycie protokołu HTTPS zamiast HTTP podczas komunikacji między klientem a serwerem. Zendesk zarządza obsługą klienta, która oferuje narzędzia do obsługi zgłoszeń, rozmów z klientami.



Obraz 7.15.1 wykorzystywane technologie strona support.faceit.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.



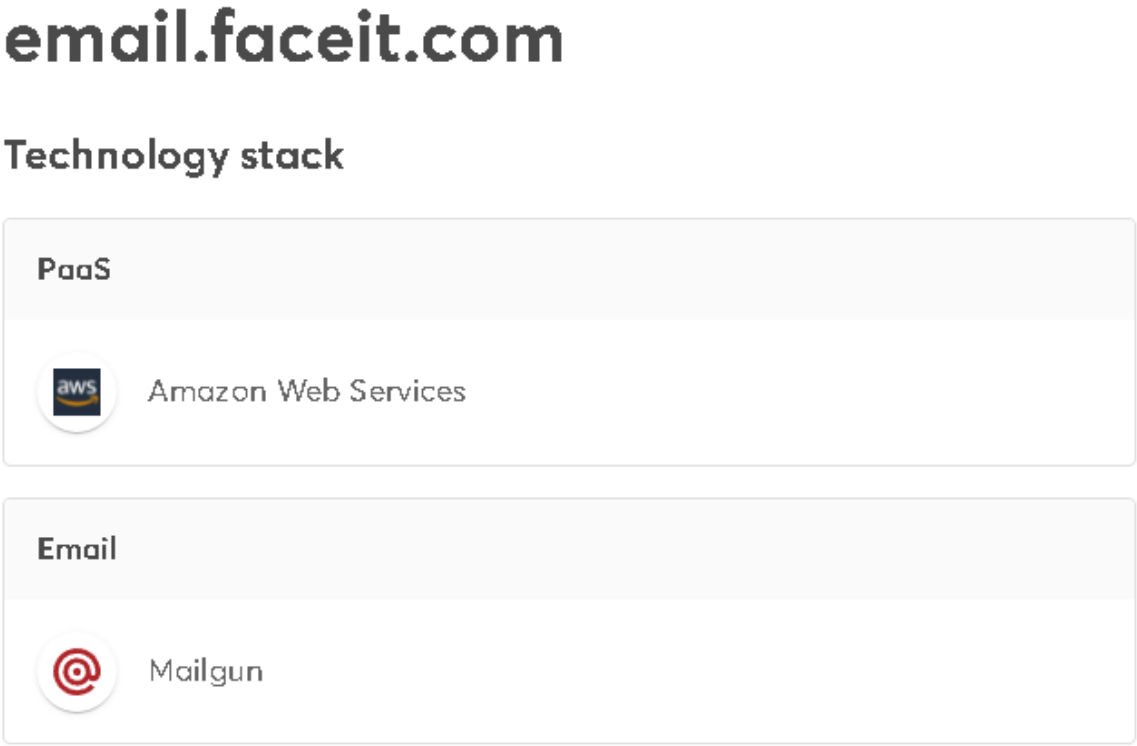
Obraz 7.15.2 wykorzystywane technologie strona support.faceit.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.

Na obrazie 7.16.1 przedstawiono technologie wykorzystywane na stronie pro.faceit.com. Lodash v4.17.21, jQuery Migrate v3.4.1, Yoast Seo v21.7 zostaną w rozdziale 9 sprawdzone pod kątem podatności.

Name	Version
WordPress	-
Cloudflare	-
Usercentrics	-
MySQL	-
Google Font API	-
Kinsta	-
jQuery	-
jQuery Migrate	3.4.1
Schema.org	-
Twitter Cards	-
HTTP/3	-
Open Graph	-
PHP	-
Yoast SEO	21.7
Cloudflare SSL	-
Google Tag Manager	-

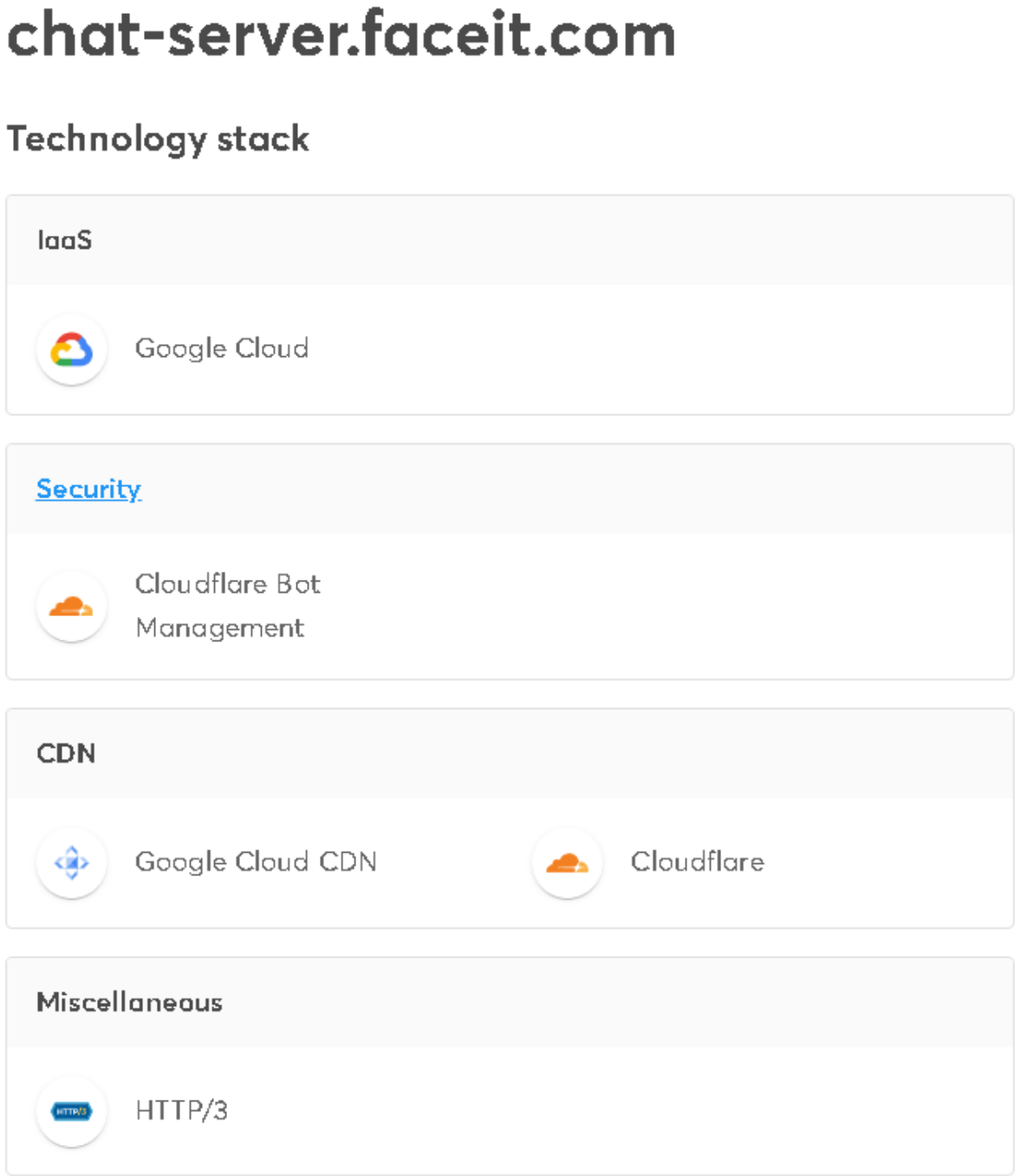
Obraz 7.16.1 wykorzystywane technologie strona pro.faceit.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.

Na obrazie 7.17.1 przedstawiono technologie wykorzystywane na stronie email.faceit.com. Dzięki Mailgun, można skutecznie komunikować się z klientami poprzez wysyłanie spersonalizowanych i ukierunkowanych wiadomości e-mail



Obraz 7.17.1 wykorzystywane technologie strona email.faceit.com. wappalyzer.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.

Na obrazach 7.14.1-7.14.4 przedstawiono technologie wykorzystywane na stronie chat-server.faceit.com.

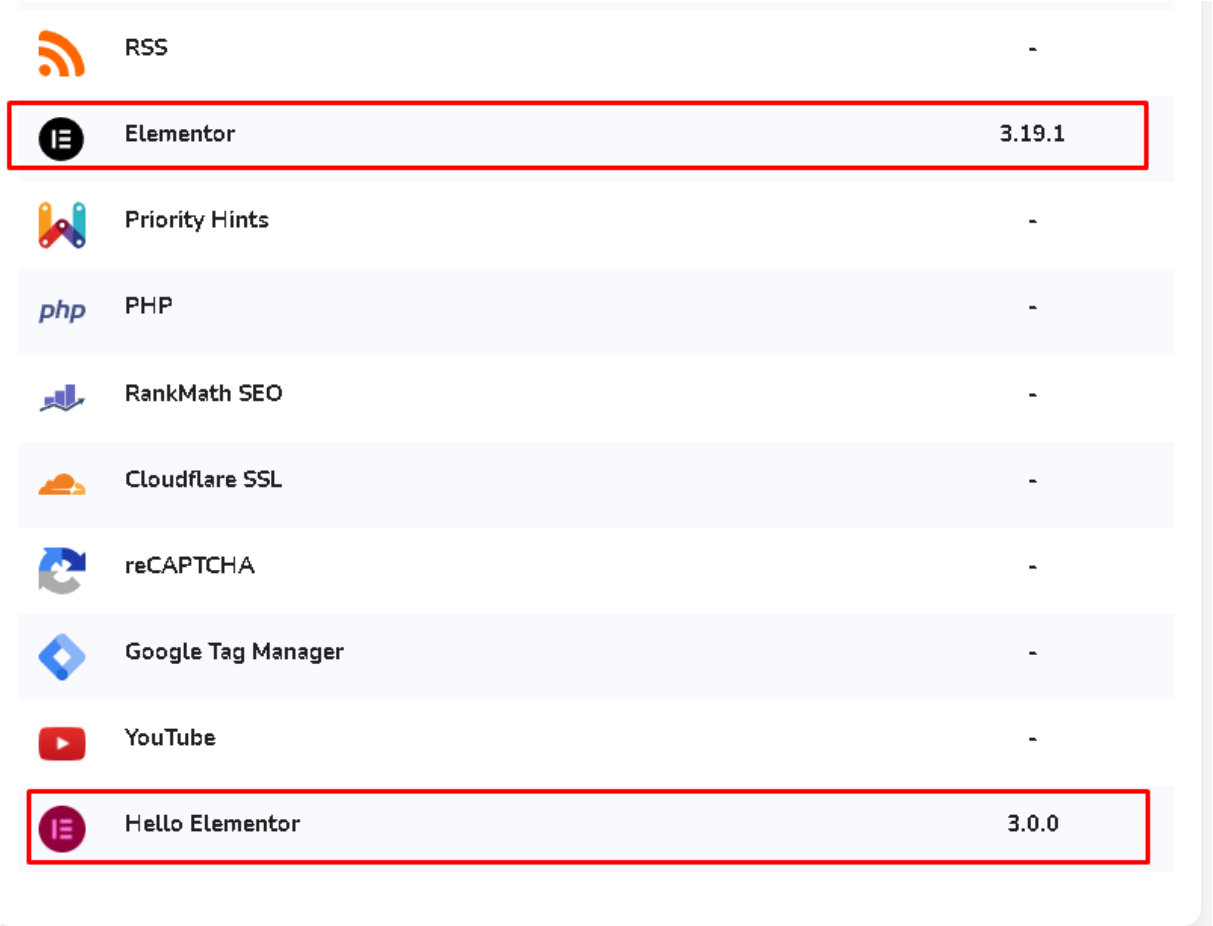


Obraz 7.18.1 wykorzystywane technologie strona chat-server.faceit.com. wappalyzer.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.

Na obrazach 7.19.1, 7.19.2 przedstawiono technologie wykorzystywane na stronie ads.faceit.com. WordPress v6.4.3, jQueryMigrate v3.4.1, Elementor v3.19.1 zostaną w rozdziale 9 sprawdzone pod kątem podatności.

Name	Version
Linkedin Ads	-
Linkedin Insight Tag	-
WordPress	6.4.3
Cloudflare	-
Usercentrics	-
MySQL	-
Font Awesome	-
Kinsta	-
jQuery	-
jQuery Migrate	3.4.1
Swiper	-
Schema.org	-
Twitter Cards	-
HTTP/3	-
Open Graph	-

Obraz 7.19.1 wykorzystywane technologie strona ads.faceit.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.



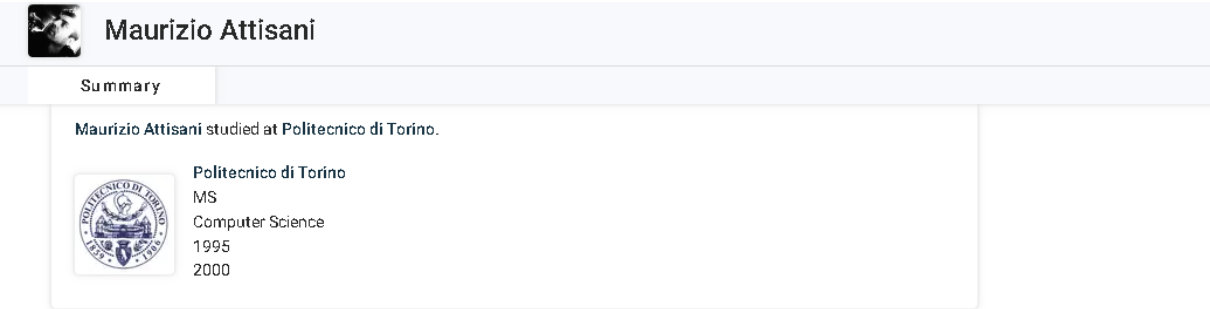
Obraz 7.19.2 wykorzystywane technologie strona ads.faceit.com, źródło seomator.com, data wykonania zrzutu 08.02.2024 r.

W zbieraniu danych do rozdziału 7 skorzystano ze stron takich jak linkedin.com, builtwith.com, cloud.google.com, eslfaceutgroup.com, faceit.com, seomator.com, wappalyzer.com. Domena korzysta z znaczącej liczby technologii, od farmeworków frontendowych do kontenerów. Sprawdzając technologie wykorzystywane przez każdą poddomenę nie natrafiono na wykorzystanie technologii Go/Golang, Next.js, Python, MongoDB, Moment JS, które zostały zebrane przy użyciu narzędzia builtswith.com, chociaż z pewnością nie sprawdzono wszystkich poddomen. Faceit korzysta zarówno z baz NoSQL (Redis) jak i SQL (MySQL). Poddomeny wykorzystują bibliotekę JavaScript Stripe w celu wykonania płatności. Witryny wykorzystują stabilną infrastrukturę AWS. Na podstawie wykorzystanych narzędzi i technik wykryto również elementy odpowiedzialne za bezpieczeństwo, takie jak zabezpieczenia mailowe w postaci rekordu SPF oraz protokołu DMARC. Wykorzystywane frameworki frontendowe Angular i Ract sugerują, że organizacja kładzie nacisk na przyjazny interfejs graficzny użytkownika. Sprawdzone poddomeny korzystają z rozwiązań otwartoźródłowych/wolnego oprogramowania takiego jak MySQL i WordPress.

8. Pracownicy i osoby powiązane

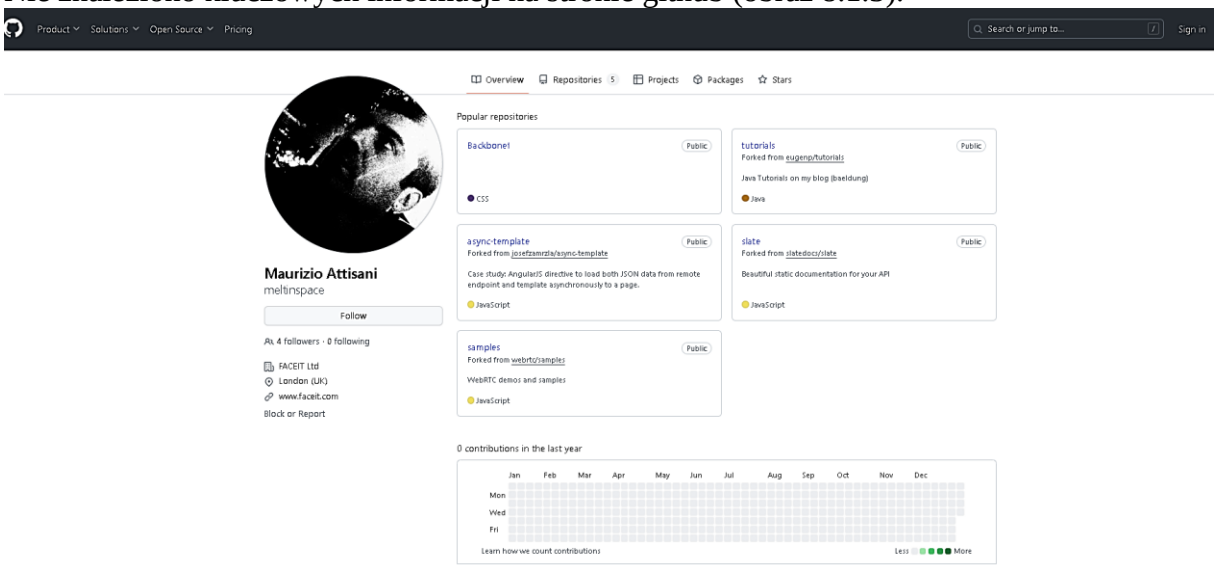
Maurizio Attisani – CTO ESL FACEIT. Urodził się w Turynie we Włoszech, gdzie ukończył inżynierię komputerową na Politechnice. Karierę zawodową rozpoczął we Włoszech w obszarze Web Intelligence. W 2006 roku przeniósł się do Stanów Zjednoczonych (San Francisco), a od 2015 roku do Wielkiej Brytanii (Londyn). Anioł biznesu i menedżer w branży Gaming i Esports, inwestuje w start-upy z dużym potencjałem i doskonałym kapitałem ludzkim. Należą do nich MindX Ltd, przeniesiona z rundy początkowej do wyjścia z HireVue Inc (Sequoia, TCV, The Carlyle Group). Więcej informacji zaprezentowano na obrazach 8.1.1-8.1.6,

Obraz 8.1.1 informacje o Maurizio Attisani, źródło clubdeglinvestitori.it, data wykonania zrzutu 10.1.2024 r.



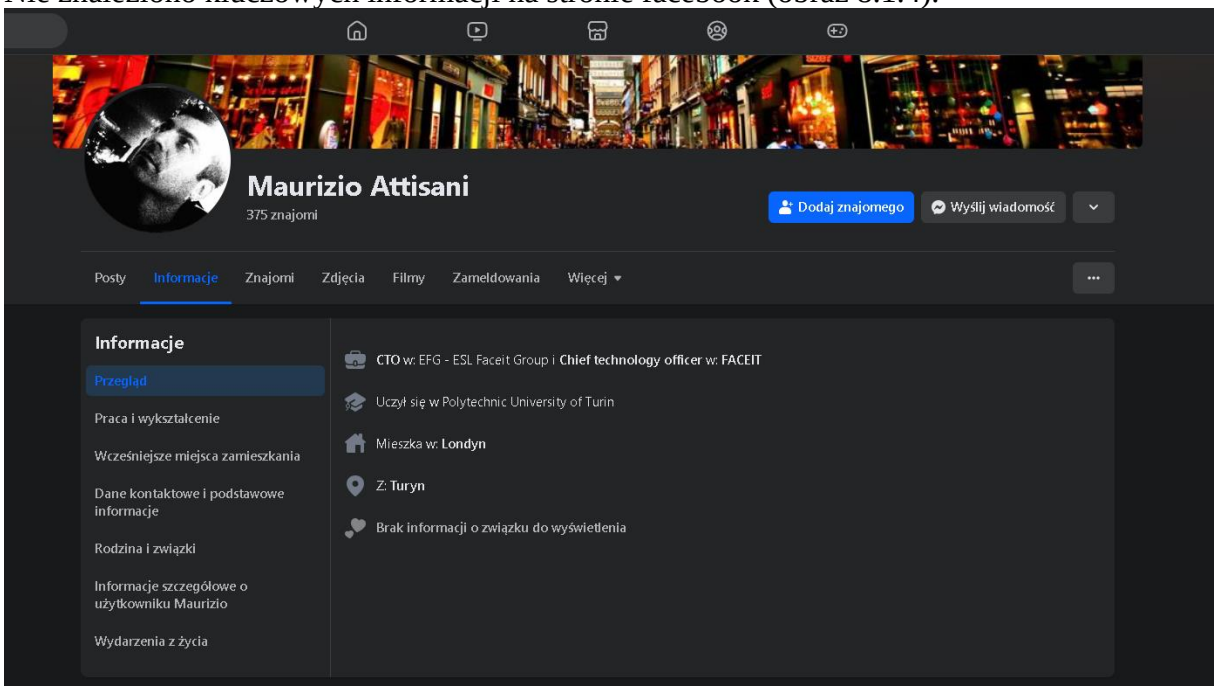
Obraz 8.1.2 informacje o Maurizio Attisani , źródło linkedin.com, data wykonania zrzutu 10.1.2024 r.

Nie znaleziono kluczowych informacji na stronie github (obraz 8.1.3).

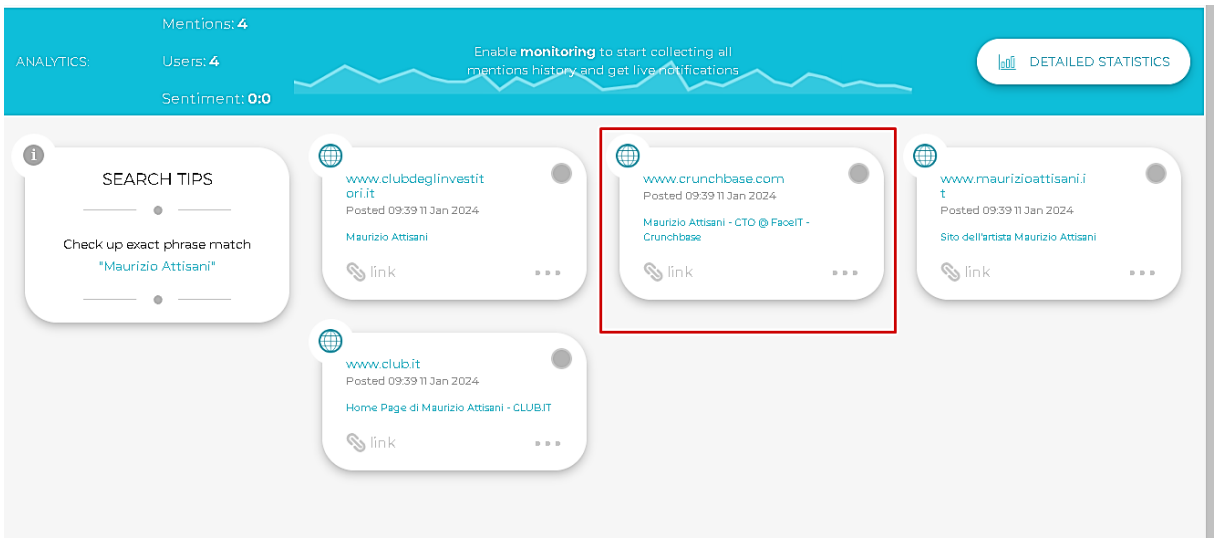


Obraz 8.1.3 strona Github Maurizio Attisani, źródło github.com, data wykonania zrzutu 10.1.2024 r.

Nie znaleziono kluczowych informacji na stronie facebook (obraz 8.1.4).

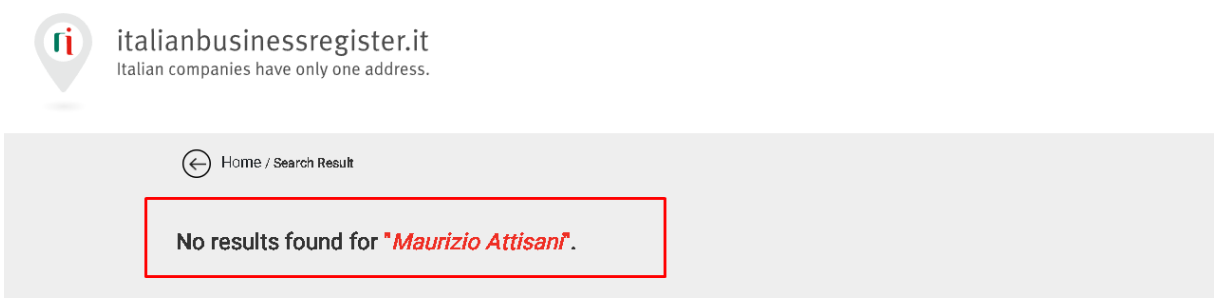


Obraz 8.1.4 strona Facebook Maurizio Attisani, źródło facebook.com, data wykonania zrzutu 10.1.2024 r.



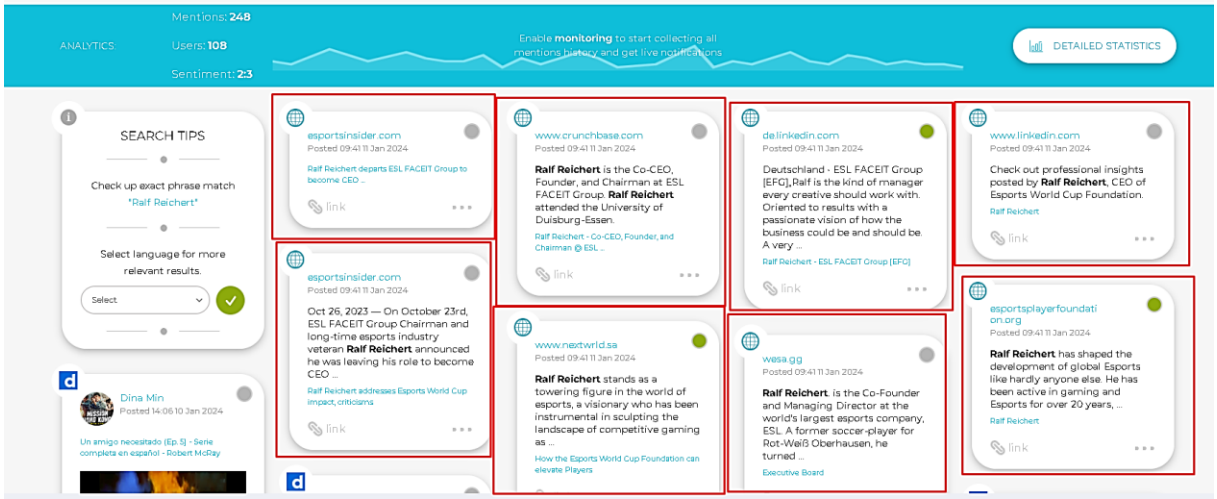
Obraz 8.1.5 rezultat wyszukania Maurizio Attisani w social-searcher.com, data wykonania zrzutu 10.1.2024 r.

Brak zarejestrowanej działalności na terenie Włoch(obraz 8.1.6).



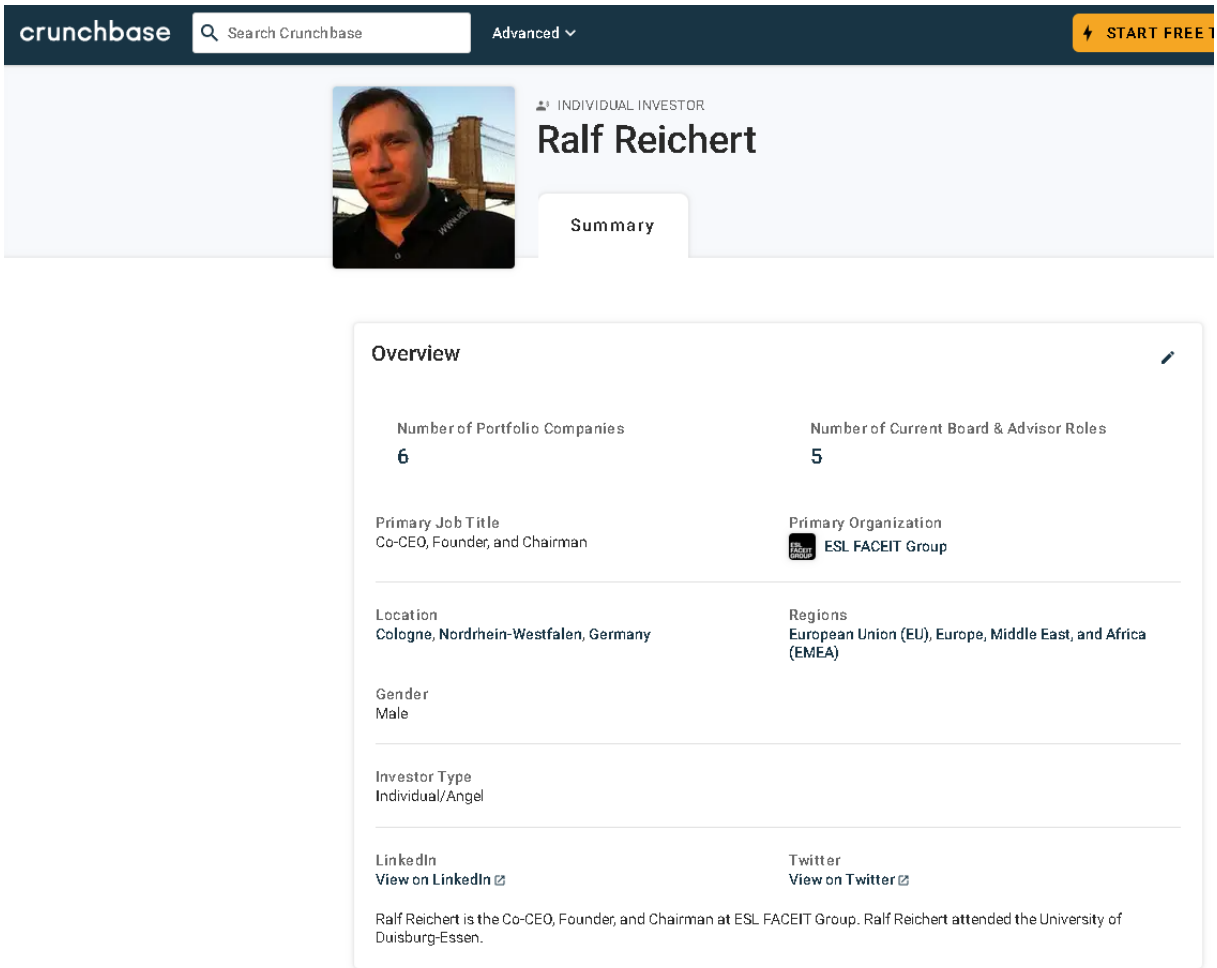
Obraz 8.1.6 rezultat wyszukania Maurizio Attisani w włoskim rejestrze przedsiębiorców, źródło italianbusinessregister.it, data wykonania zrzutu 15.1.2024 r.

Ralf Reichert – CEO w Esports World Cup Fundation, obecnie zamieszkuje Kolonie. Ukończył ekonomie na Uniwersytecie w Duisburg-Essen. Szczegółowe informacje przedstawiono na obrazach 8.2.1-8.2.9.



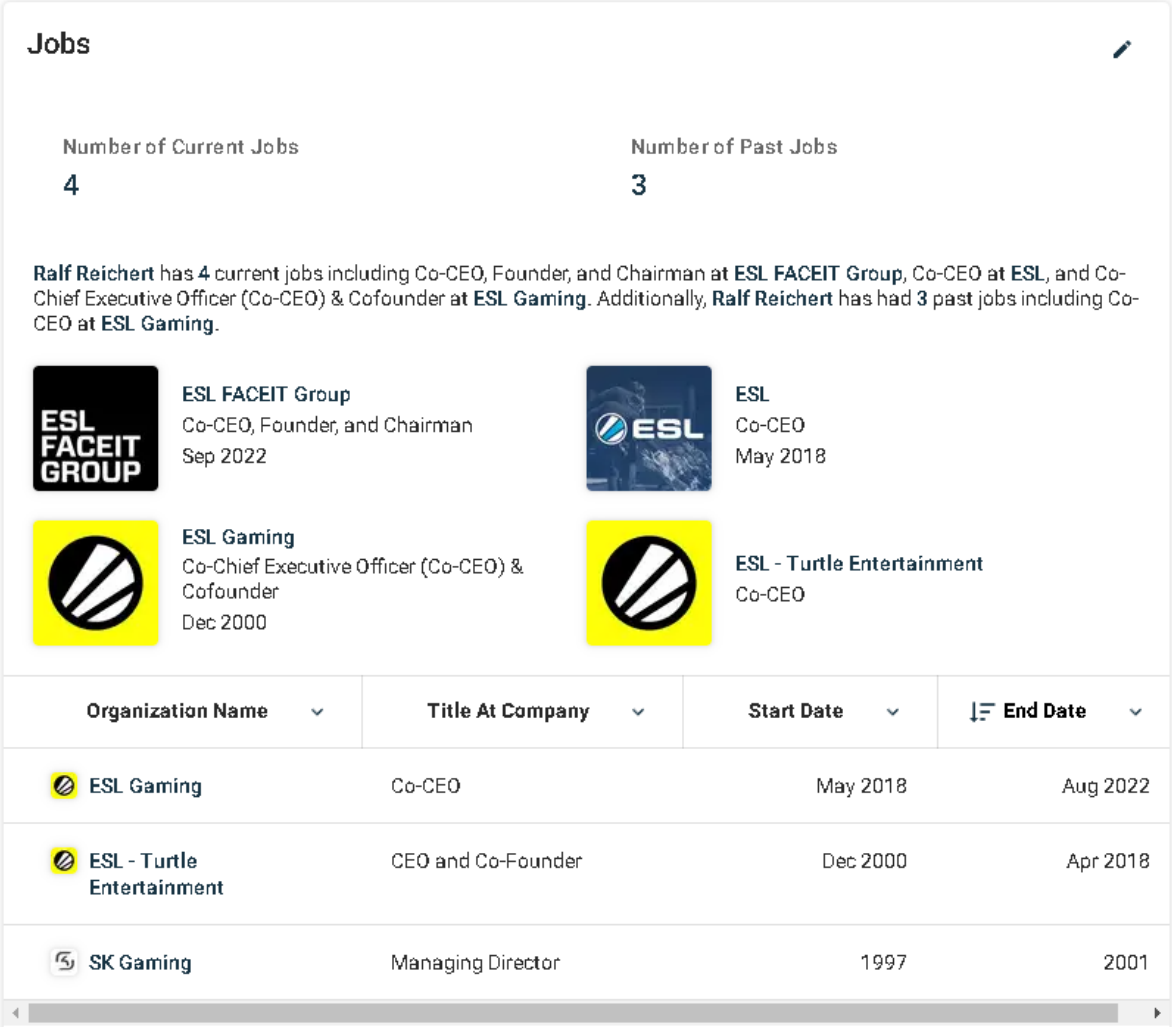
Obraz 8.2.1 rezultat wyszukania Ralf Reichert w social-searcher.com, data wykonania zrzutu 10.1.2024 r.

Obraz 8.2.2 ogłoszenie Ralf'a Reichert'a CEO, źródło social-searcher.com, data wykonania zrzutu 10.1.2024 r.



Obraz 8.2.3 informacje ogólne o Ralf Reichert, źródło crunchbase.com, data wykonania zrzutu 10.1.2024 r.

Obraz 8.2.4 informacje ogólne o Ralf Reichert, źródło crunchbase.com, data wykonania zrzutu 10.1.2024 r.



Jobs

Number of Current Jobs
4

Number of Past Jobs
3

Ralf Reichert has **4** current jobs including Co-CEO, Founder, and Chairman at **ESL FACEIT Group**, Co-CEO at **ESL**, and Co-Chief Executive Officer (Co-CEO) & Cofounder at **ESL Gaming**. Additionally, **Ralf Reichert** has had **3** past jobs including Co-CEO at **ESL Gaming**.

ESL FACEIT Group
Co-CEO, Founder, and Chairman
Sep 2022

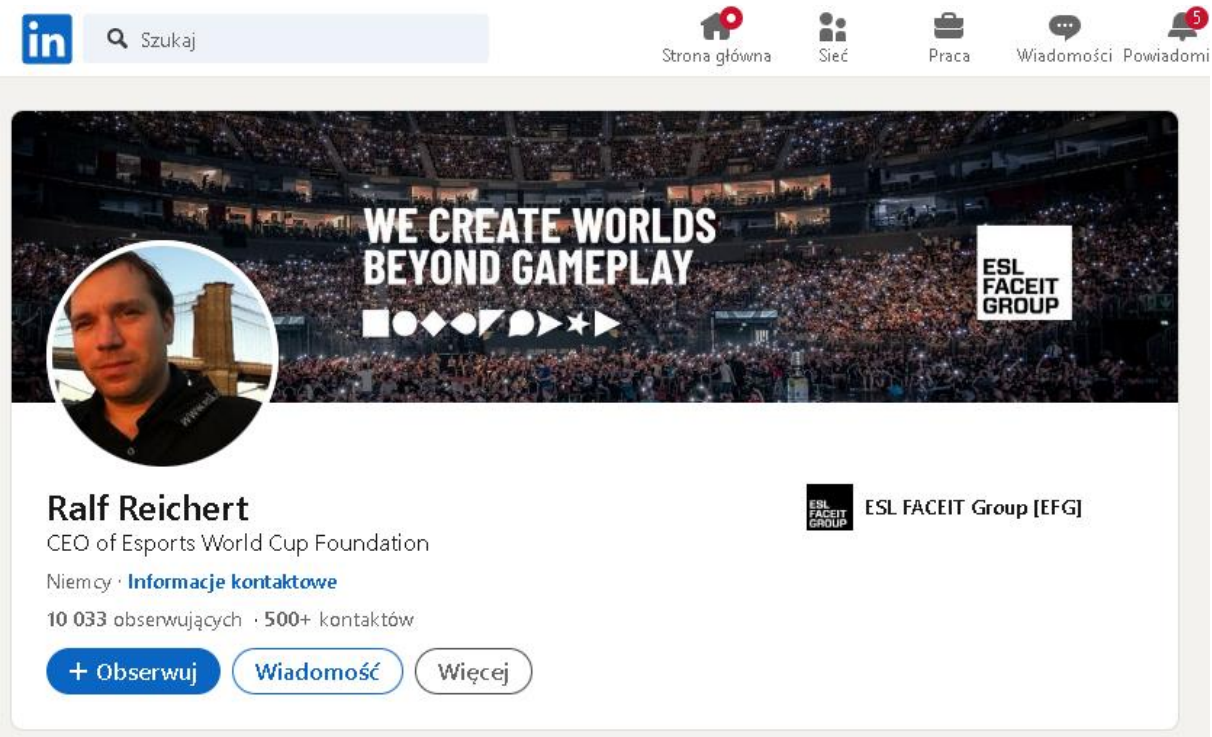
ESL
Co-CEO
May 2018

ESL Gaming
Co-Chief Executive Officer (Co-CEO) & Cofounder
Dec 2000

ESL - Turtle Entertainment
Co-CEO

Organization Name	Title At Company	Start Date	End Date
ESL Gaming	Co-CEO	May 2018	Aug 2022
ESL - Turtle Entertainment	CEO and Co-Founder	Dec 2000	Apr 2018
SK Gaming	Managing Director	1997	2001

Obraz 8.2.5 informacje ogólne o Ralf Reichert, źródło linkedin.com, data wykonania zrzutu 10.1.2024r.

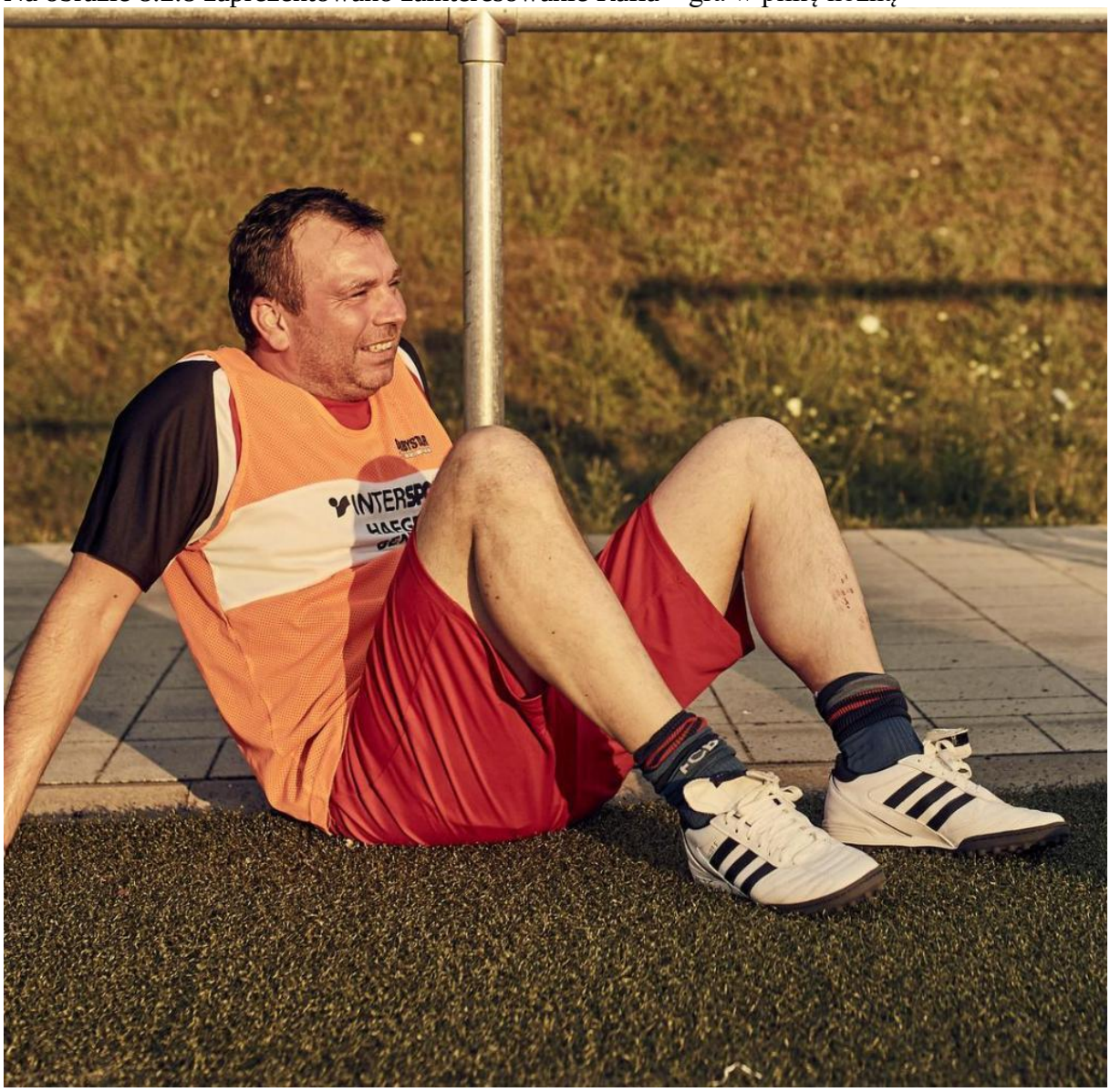


Obraz 8.2.6 informacje ogólne o Ralf Reichert, źródło linkedin.com, data wykonania zrzutu 10.1.2024r.

Obraz 8.2.7 wskazuje na współpracę grupy ESL FACEIT GROUP z marką mercedes, której nie uwzględniono w rozdziale 2.

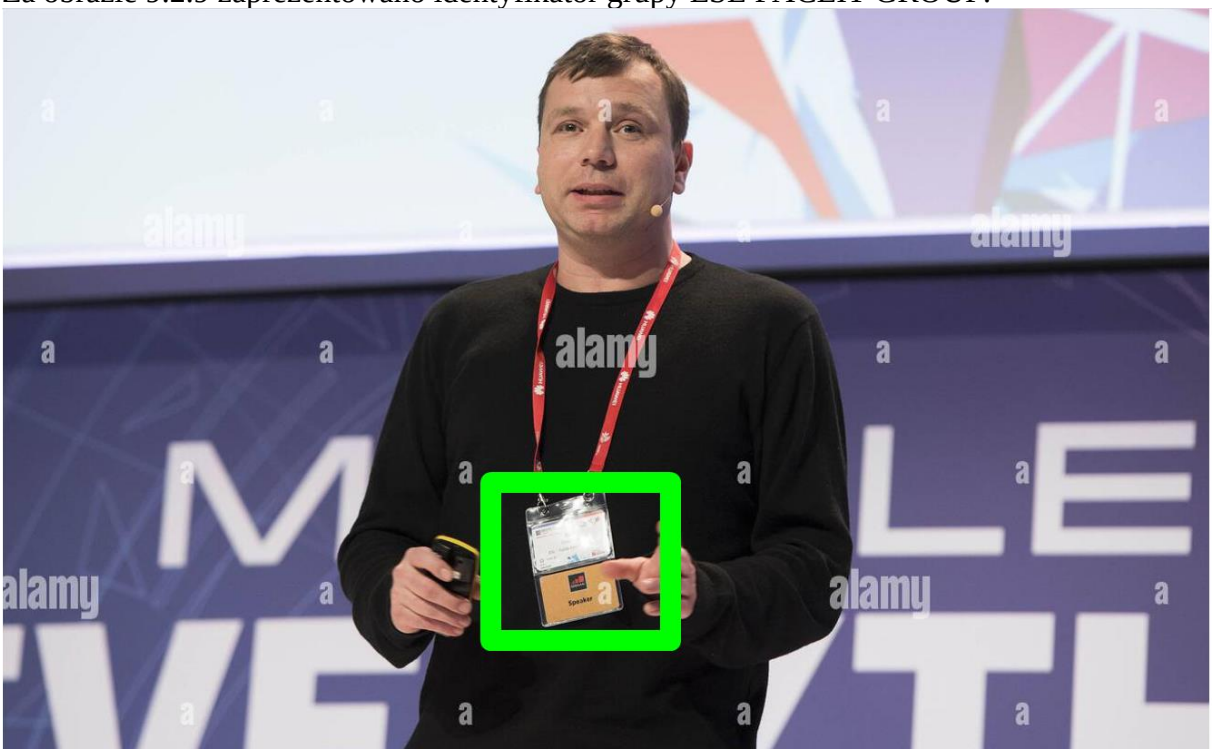
Obraz 8.2.7 Ralf Reichert na konferencji, źródło google.com, data wykonania zrzutu 18.1.2024 r.

Na obrazie 8.2.8 zaprezentowano zainteresowanie Rafla – gra w piłkę nożną



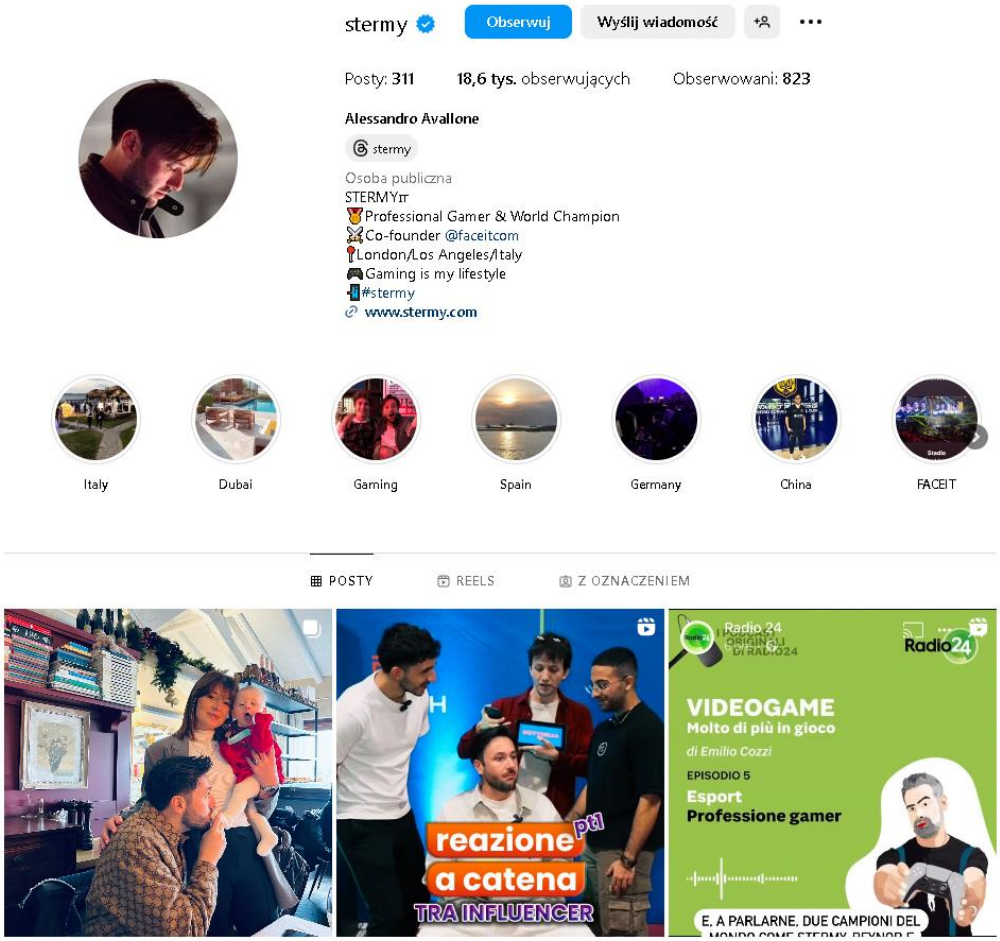
Obraz 8.2.8 zainteresowania Ralf Reichert, źródło welt.de, data wykonania zrzutu 18.1.2024 r.

Za obrazie 9.2.9 zaprezentowano identyfikator grupy ESL FACEIT GROUP.

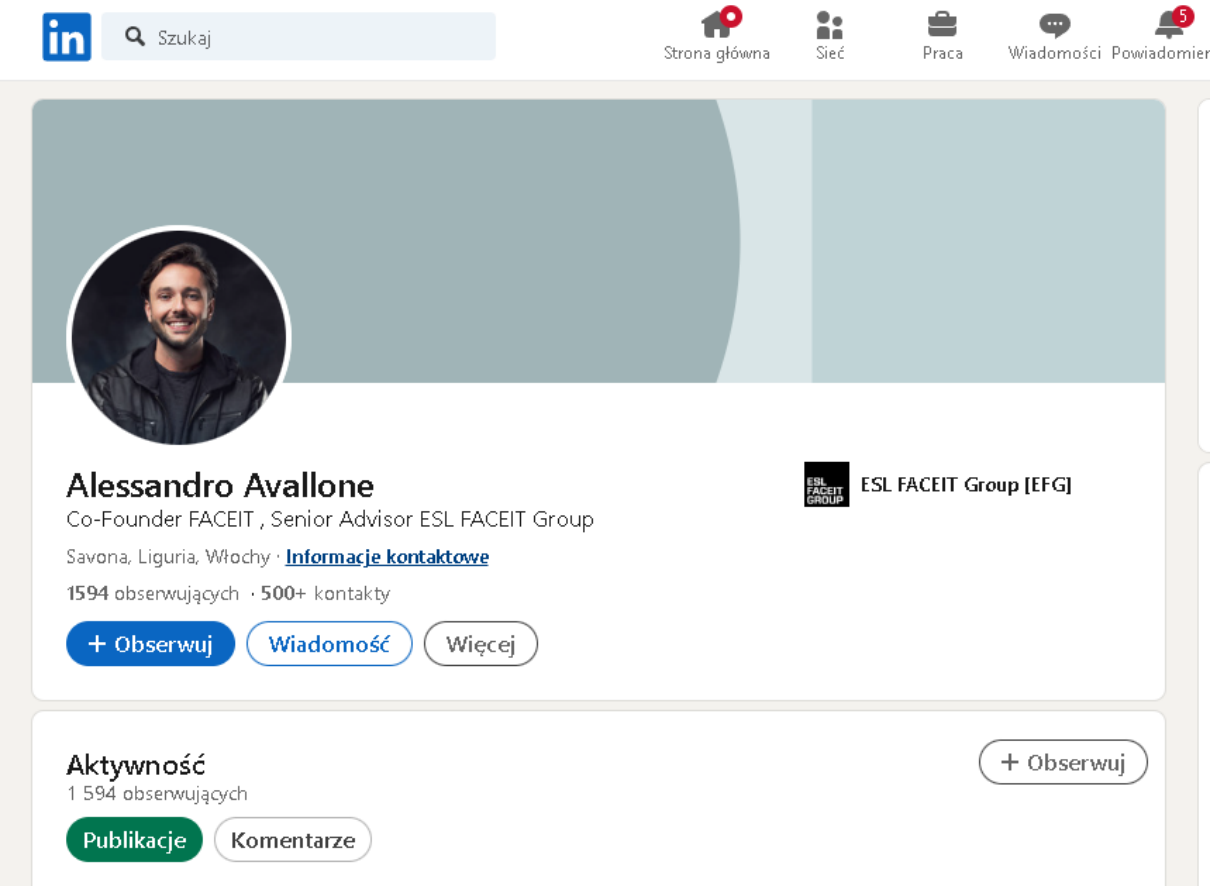


Obraz 8.2.9 Ralf Reichert na konferencji, źródło alamy.com, data wykonania zrzutu 18.1.2024 r.

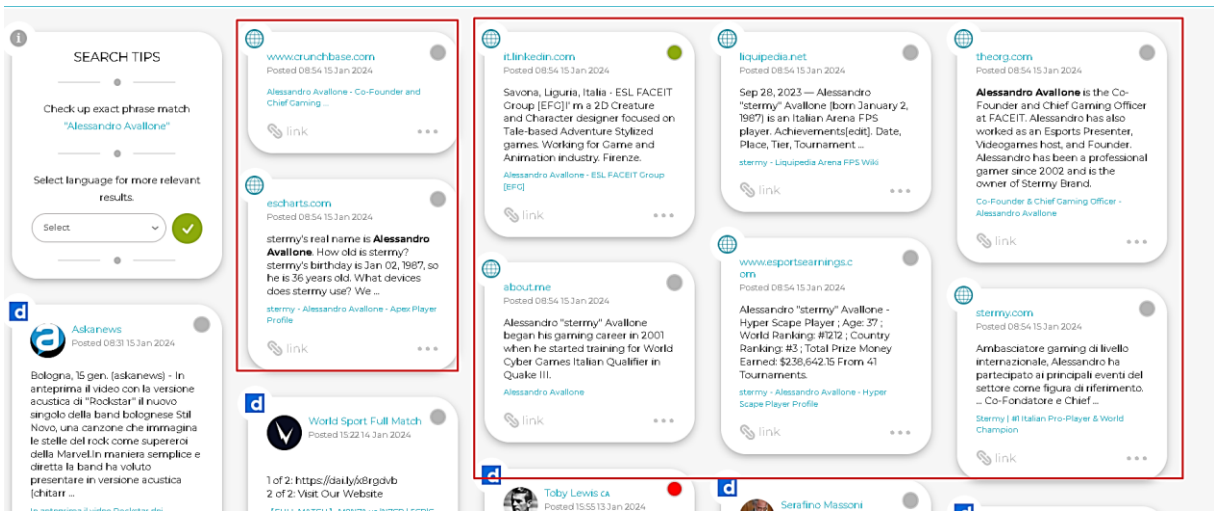
Alessandro Avallone - Co-Founder FACEIT. Były profesjonalny gracz Quake, FIFA. Mianuje się najlepszym włoskim graczem e-sportowym. Laureat licznych turniejów komputerowych. Szczegółowe informacje przedstawiono na obrazach 8.3.1-8.3.11. Po przejrzeniu konta Instagram nie znaleziono kluczowych informacji mających wpływ na dalsze etapy rekonesansu (obraz 8.3.1).



Obraz 8.3.1 social-media Alessandro Avallone, źródło instagram.com, data wykonania zrzutu 10.1.2024 r.

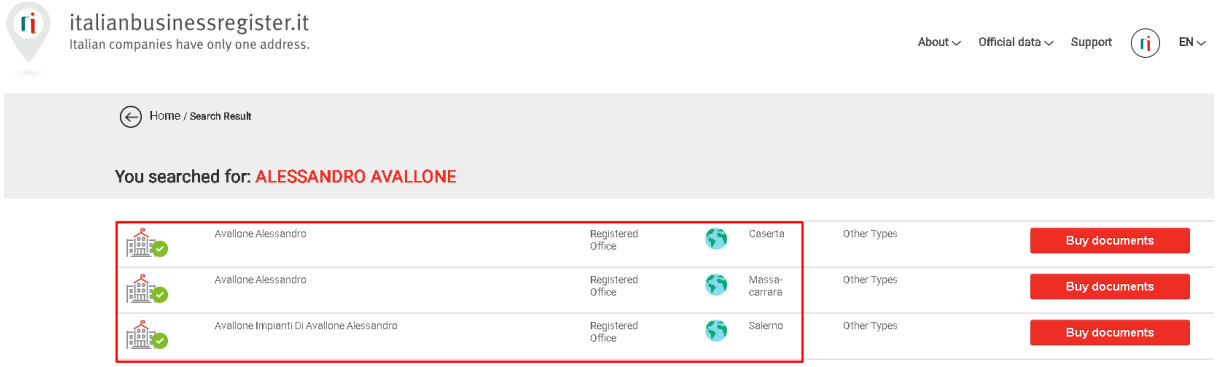


Obraz 8.3.2 informacje ogólne o Alessandro Avallone źródło linkedin.com, data wykonania zrzutu 10.1.2024 r.

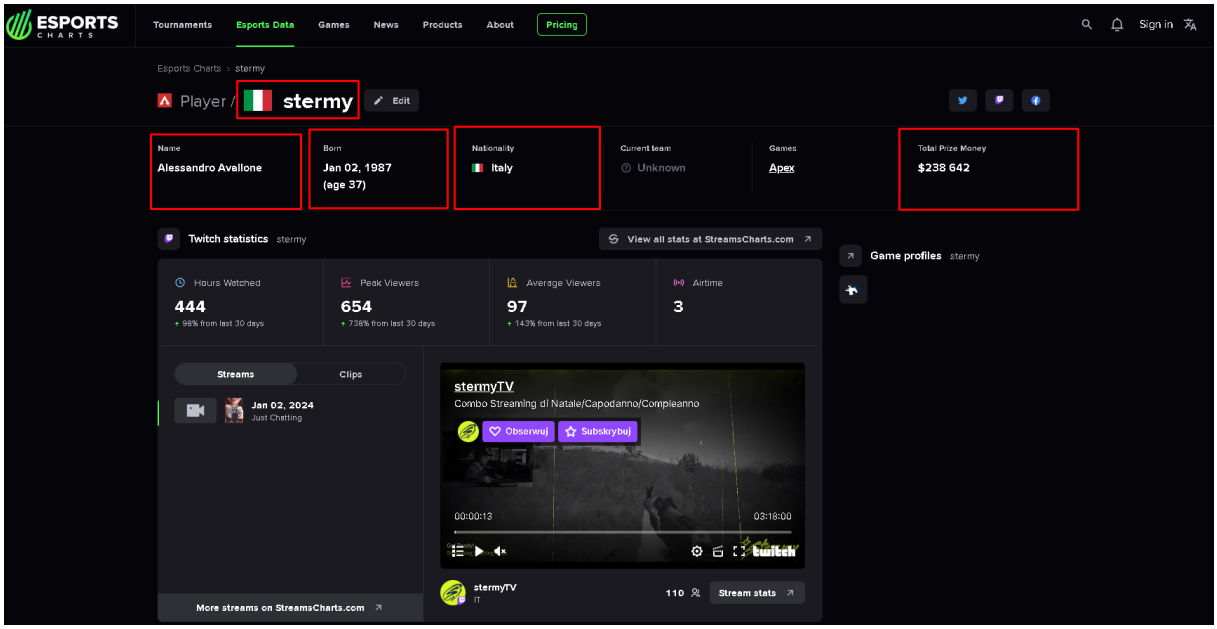


Obraz 8.3.3 wynik wyszukania Alessandro Avallone w social-searcher.com, data wykonania zrzutu 15.1.2024 r.

Obraz 8.3.4 wskazuje na brak zrejestrowanej działalności gospodarczej na osobę Alessandro Avallone.



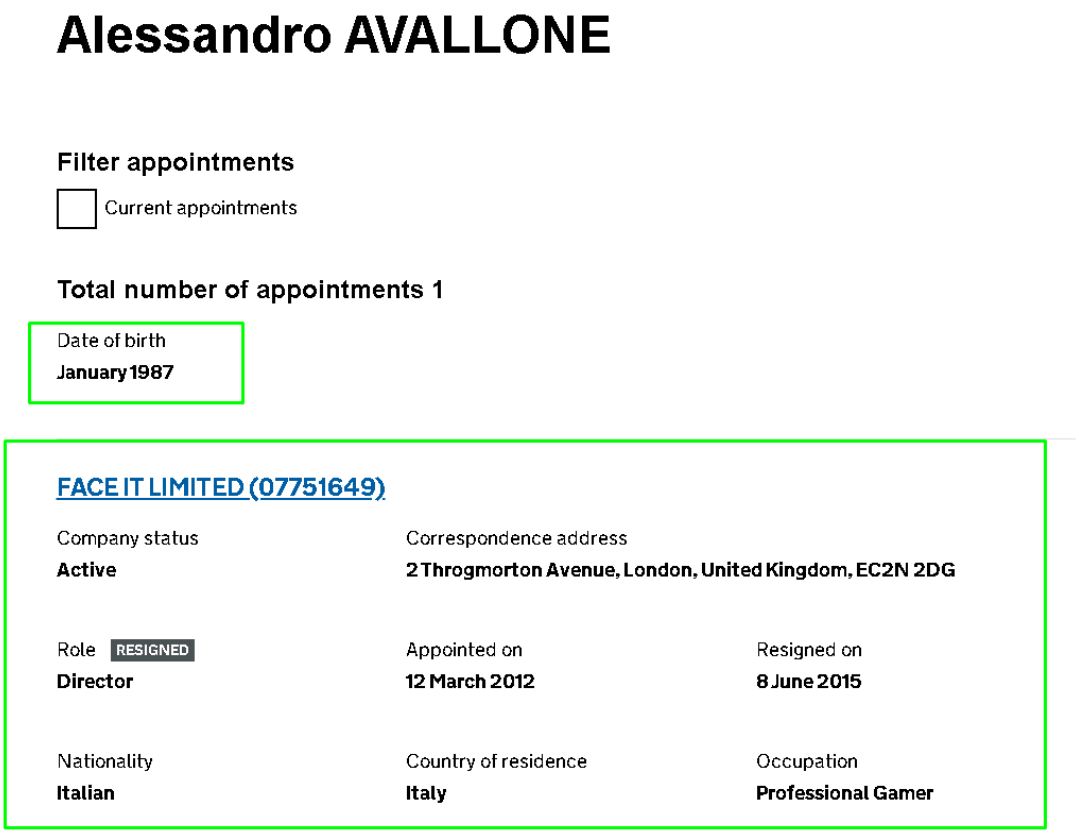
Obraz 8.3.4 wynik wyszukania Alessandro Avallone w włoskim rejestrze przedsiębiorców, źródło italianbusinessregister.it, data wykonania zrzutu 15.1.2024 r.



Obraz 8.3.5 informacje o karierze e-sportowej Alessandro Avallone, źródło escharts.com, data wykonania zrzutu 15.1.2024 r.

Obrazy 8.3.6-8.3.8 wskazują na zarejestrowane działalności na osobę Alessandro Avallone na terenie Wielkiej Brytanii.

Obraz 8.3.6 wynik wyszukania Alessandro Avallone w brytyjskim rejestrze przedsiębiorców, źródło gov.uk, data wykonania zrzutu 15.1.2024 r.



Obraz 8.3.7 informacje o działalności gospodarczej Alessandro Avallone, źródło gov.uk, data wykonania zrzutu 15.1.2024 r.

Alessandro AVALLONE

Filter appointments

☐ Current appointments

Total number of appointments 1

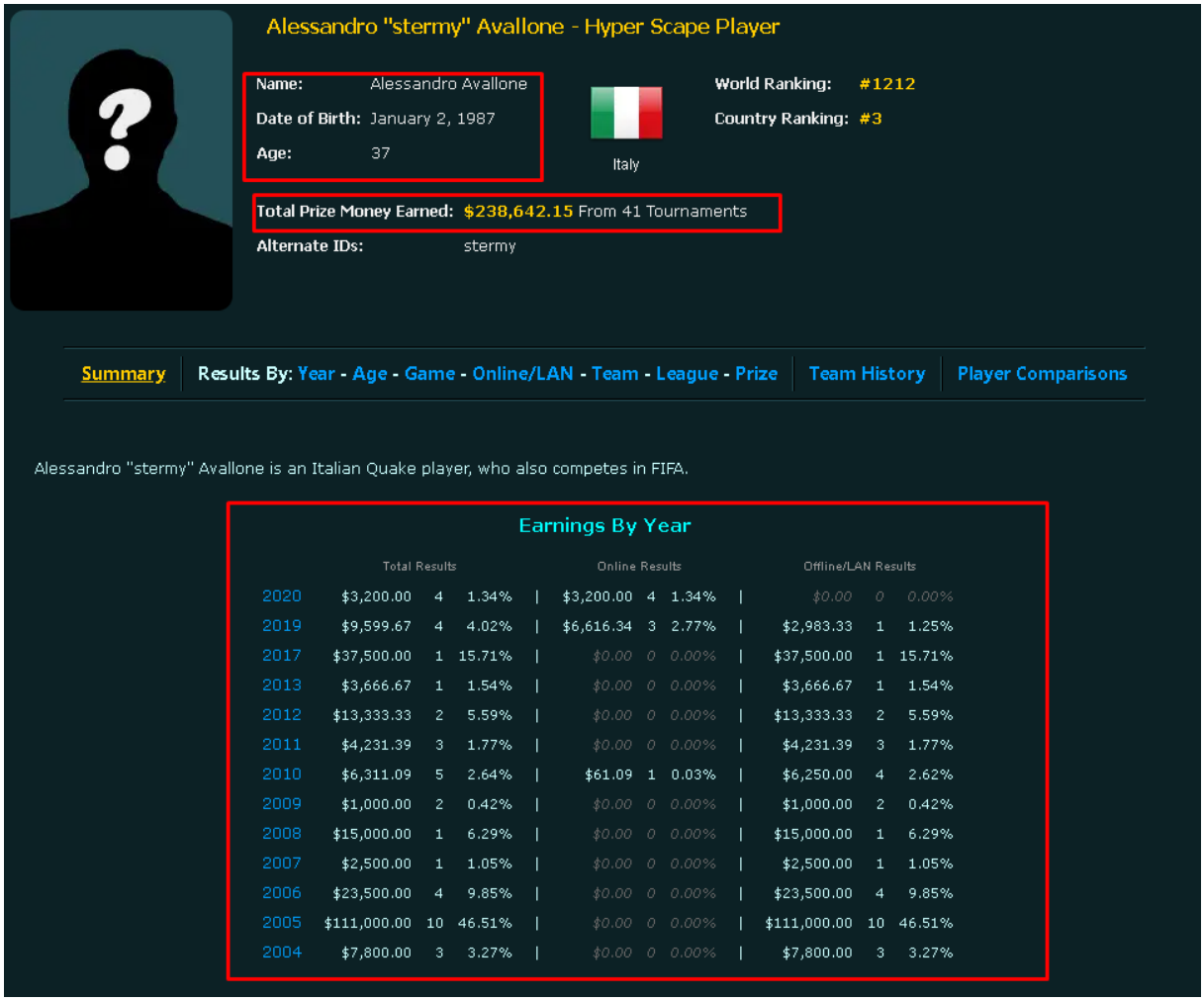
Date of birth
January 1987

STERMY LIMITED (10457595)

Company status	Correspondence address	
Dissolved	**C/O Mercer & Hole, 21 Lombard Street, London, United Kingdom, EC3V 9AH**	
Role	Appointed on	
Director	**2 November 2016**	
Nationality	Country of residence	Occupation
Italian	**United Kingdom**	**Professional Gamer**

Obraz 8.3.8 informacje o działalności gospodarczej Alessandro Avallone, źródło gov.uk, data wykonania zrzutu 15.1.2024 r.

Obrazy 8.3.9-8.3.11 prezentują bogatą karierę zawodnika esportowego i przychody z turniejów.



Alessandro "stermy" Avallone - Hyper Scape Player

Name: Alessandro Avallone
Date of Birth: January 2, 1987
Age: 37

Italy

World Ranking: #1212
Country Ranking: #3

Total Prize Money Earned: $238,642.15 From 41 Tournaments
Alternate IDs: stermy

Summary | Results By: Year - Age - Game - Online/LAN - Team - League - Prize | Team History | Player Comparisons

Alessandro "stermy" Avallone is an Italian Quake player, who also competes in FIFA.

Earnings By Year

	Total Results			Online Results			Offline/LAN Results		
2020	$3,200.00	4	1.34%	$3,200.00	4	1.34%	$0.00	0	0.00%
2019	$9,599.67	4	4.02%	$6,616.34	3	2.77%	$2,983.33	1	1.25%
2017	$37,500.00	1	15.71%	$0.00	0	0.00%	$37,500.00	1	15.71%
2013	$3,666.67	1	1.54%	$0.00	0	0.00%	$3,666.67	1	1.54%
2012	$13,333.33	2	5.59%	$0.00	0	0.00%	$13,333.33	2	5.59%
2011	$4,231.39	3	1.77%	$0.00	0	0.00%	$4,231.39	3	1.77%
2010	$6,311.09	5	2.64%	$61.09	1	0.03%	$6,250.00	4	2.62%
2009	$1,000.00	2	0.42%	$0.00	0	0.00%	$1,000.00	2	0.42%
2008	$15,000.00	1	6.29%	$0.00	0	0.00%	$15,000.00	1	6.29%
2007	$2,500.00	1	1.05%	$0.00	0	0.00%	$2,500.00	1	1.05%
2006	$23,500.00	4	9.85%	$0.00	0	0.00%	$23,500.00	4	9.85%
2005	$111,000.00	10	46.51%	$0.00	0	0.00%	$111,000.00	10	46.51%
2004	$7,800.00	3	3.27%	$0.00	0	0.00%	$7,800.00	3	3.27%

Obraz 8.3.9 informacje o karierze e-sportowej Alessandro Avallone, źródło esportsearnings.com, data wykonania zrzutu 15.1.2024 r.

ALESSANDRO AVALLONE

Alessandro "stermy" Avallone began his gaming career in 2001 when he started training for World Cyber Games Italian Qualifier in Quake III. One year later stermy won the same qualifier, earning a chance to compete with the very best at the World Cyber Games Finals in Korea. At the age of 15 he had vaulted to the top level of players in the world and was one of the youngest players to ever participate in the World Cyber Games.

Through 2003 stermy continued to compete in Quake III and dominated the International First Person Shooter circuit where he gained a reputation as one of the most talented duelers in Europe.

In 2004 Alessandro switched to Painkiller, the newest FPS Game at that time. His 2nd place finish at the Electronic Sports World Cup in France that year confirmed his position as one of the best PainKiller players in the world.

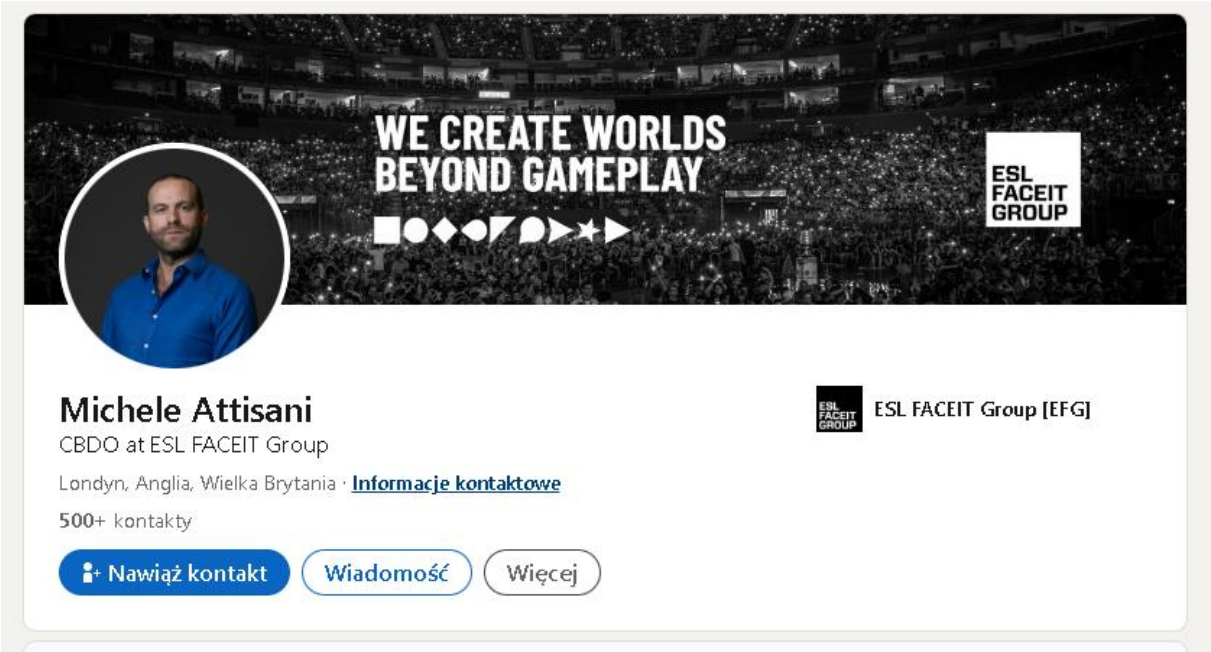
Obraz 8.3.10 informacje o karierze e-sportowej Alessandro Avallone, źródło about.me/stermy, data wykonania zrzutu 15.1.2024 r.

The CPL World Tour in 2005 gave him the opportunity to compete in locations around the world against the very best. As one of the most consistent players throughout the world tour he placed 3rd in the Championship Final event, one of the most exciting and highly viewed tournaments in history. His $70,000 prize for this event ranks among the highest paydays in competitive video game history and gave him international exposure.
Switching to Quake 4 in 2006, Stermy competed in the World Series of Video Games circuit, taking 1st place at the inaugural event in Louisville, Kentucky. His impressive play continued as he fought his way to the finals in the two following WSVG events.
Showing versatility, Alessandro was the first player chosen to play FIFA at the Championship Gaming Series (CGS) initial draft and has competed for the San Francisco Optx team for the last 2 seasons.
As Team Captain, Stermy lead his team an impressive 2nd place in the the CGS World Finals of 2008, winning $150.000.

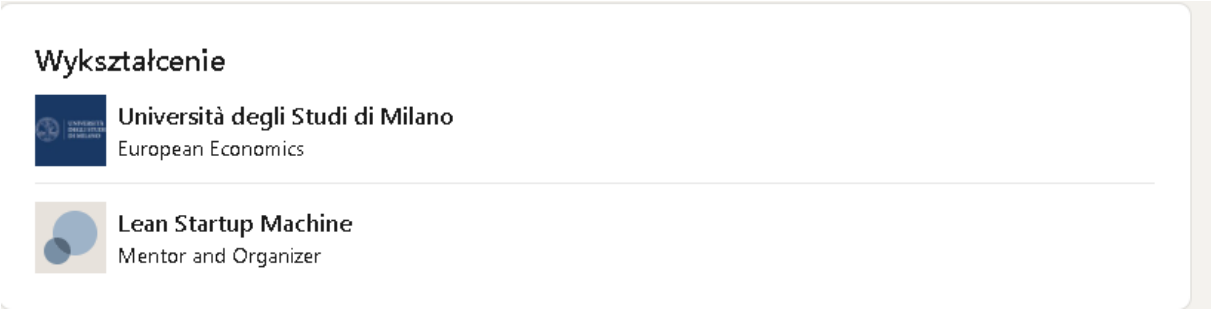
Stermy, now 23 years old, was born and still lives in Andora, Italy, a small town near Genoa. He is a gifted athlete who once considered playing professional soccer before committing to a professional video gaming career. In addition to his gaming success, his winning smile and outgoing personality has made him a global star.

Obraz 8.3.11 informacje o karierze e-sportowej Alessandro Avallone, źródło about.me/stermy, data wykonania zrzutu 15.1.2024 r.

Michele Attisani - CBDO w ESL FACEIT Group, ukończył Uniwersytet w Mediolanie na kierunku ekonomia. Posiada stronę joneslanglasalle.com (zajmującą się m.in. nieruchomościami). Profesjonalny gracz przez ponad 20 lat. Współpracował z wieloma firmami z indeksu Fortune 500. Szczegółowe informacje zaprezentowano na obrazach 8.4.1-8.4.6.



Obraz 8.4.1 informacje ogólne o Michele Attisani, źródło linkedin.com, data wykonania zrzutu 10.1.2024 r.



Obraz 8.4.2 informacje ogólne o Michele Attisani, źródło linkedin.com, data wykonania zrzutu 15.1.2024 r.

Na obrazie 8.4.3 zaprezentowano konto przedsiębiorcy zarejestrowanego na terenie Wielkiej Brytanii.

Michele ATTISANI

Filter appointments

☐ Current appointments

Total number of appointments 1

Date of birth
October 1985

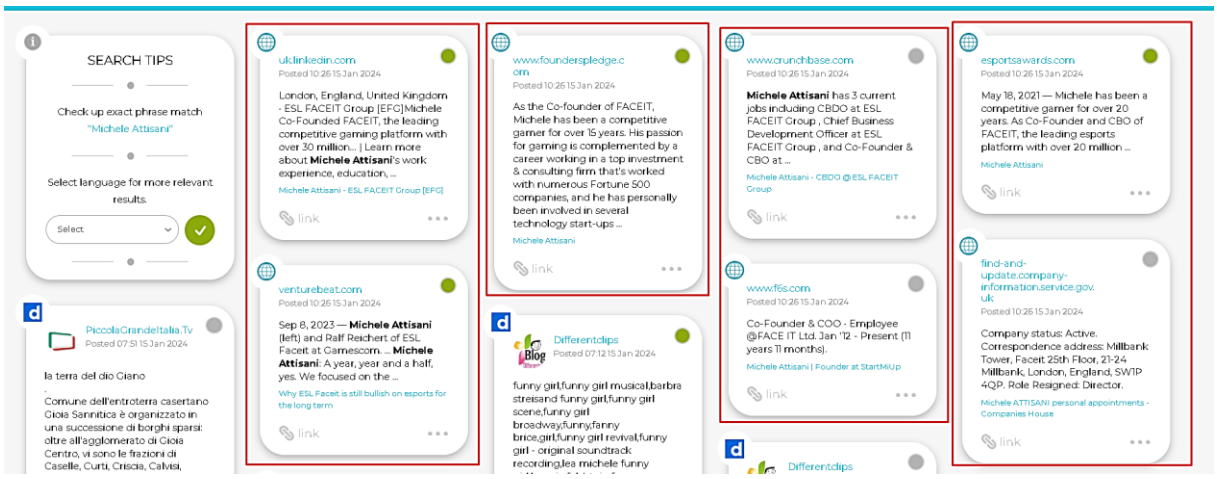
FACE IT LIMITED (07751649)

Company status	Correspondence address
Active	**Millbank Tower, Faceit 25th Floor, 21-24 Millbank, London, England, SW1P 4QP**

Role RESIGNED	Appointed on	Resigned on
Director	**12 March 2012**	**20 April 2022**

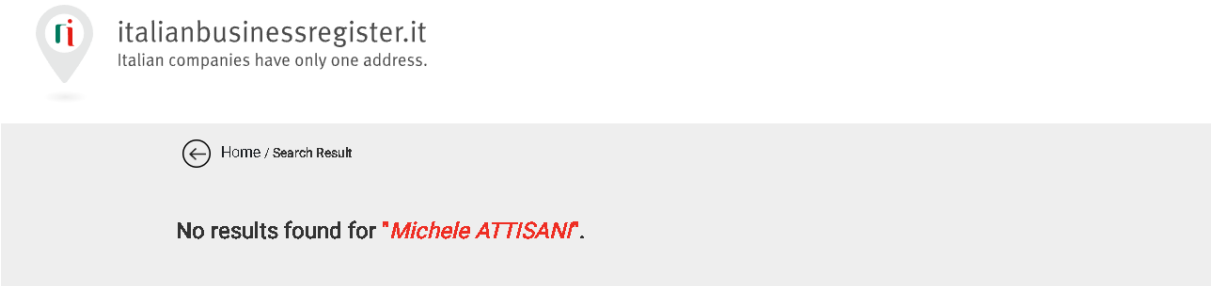
Nationality	Country of residence	Occupation
Italian	**United Kingdom**	**None**

Obraz 8.4.3 informacje o działalności gospodarczej Michele Attisani, źródło gov.uk, data wykonania zrzutu 15.1.2024 r.

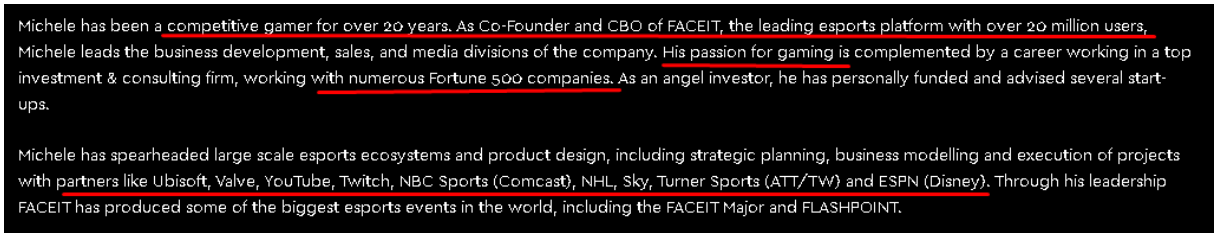


Obraz 8.4.4 wynik wyszukania Michele Attisani w social-searcher.com, data wykonania zrzutu 15.1.2024 r.

Obraz 8.4.5 nie wskazuje nie działalność gospodarczą prowadzoną na terenie Włoch.



Obraz 8.4.5 rezultat wyszukania Michele Attisani w włoskim rejestrze przedsiębiorców, źródło italianbusinessregister.it, data wykonania zrzutu 15.1.2024 r.

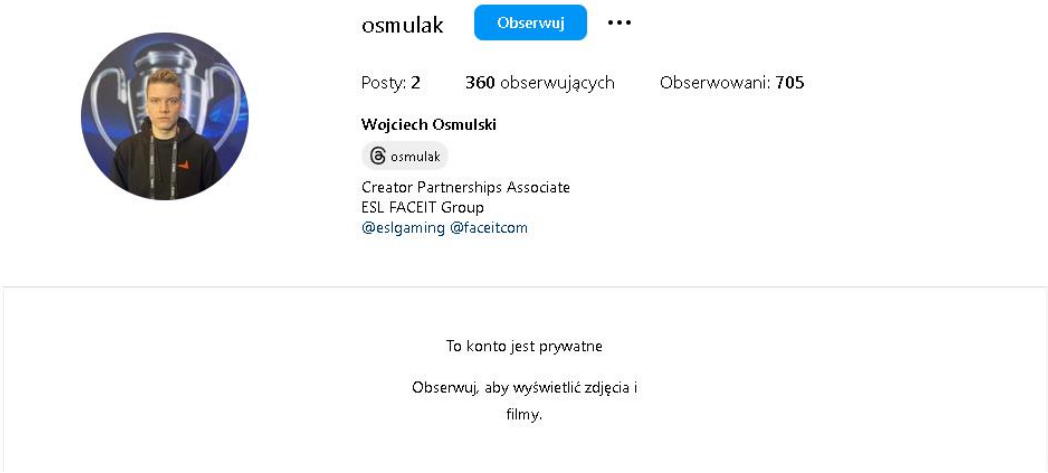


Michele has been a competitive gamer for over 20 years. As Co-Founder and CBO of FACEIT, the leading esports platform with over 20 million users, Michele leads the business development, sales, and media divisions of the company. His passion for gaming is complemented by a career working in a top investment & consulting firm, working with numerous Fortune 500 companies. As an angel investor, he has personally funded and advised several start-ups.

Michele has spearheaded large scale esports ecosystems and product design, including strategic planning, business modelling and execution of projects with partners like Ubisoft, Valve, YouTube, Twitch, NBC Sports (Comcast), NHL, Sky, Turner Sports (ATT/TW) and ESPN (Disney). Through his leadership FACEIT has produced some of the biggest esports events in the world, including the FACEIT Major and FLASHPOINT.

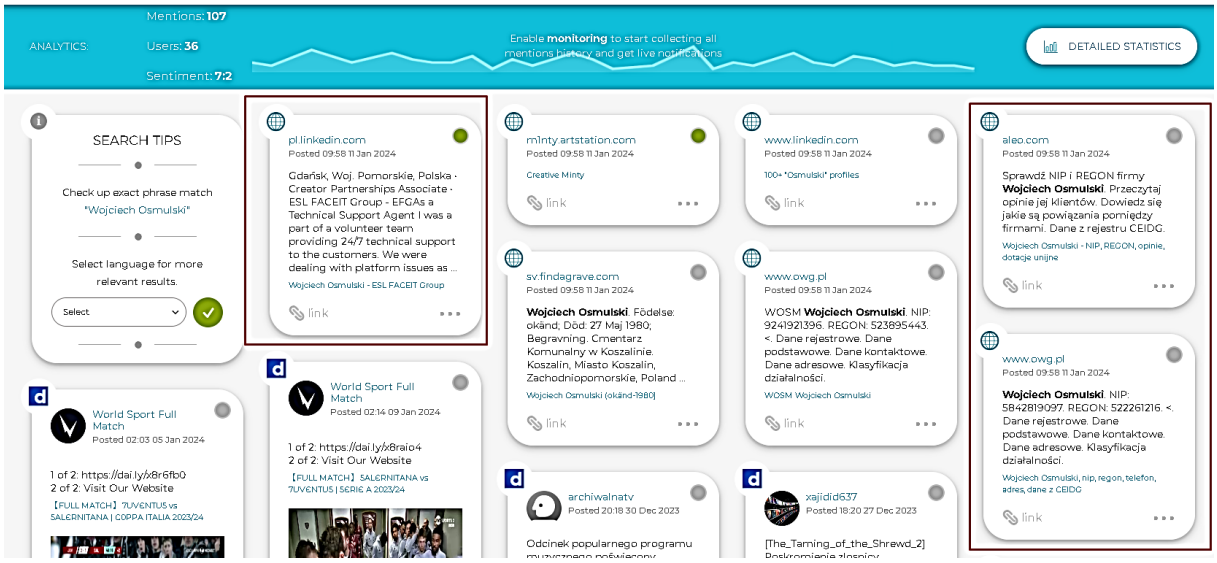
Obraz 8.4.6 informacje ogólne o Michele Attisani, źródło esportsawards.com, data wykonania zrzutu 15.1.2024 r.

Wojciech Osmulski Intern Frontend Developer w ESL FACEIT Group. Ukończył Polsko-Japońska Akademia Technik Komputerowych w Warszawie (obrazy 8.5.1-8.5.3).



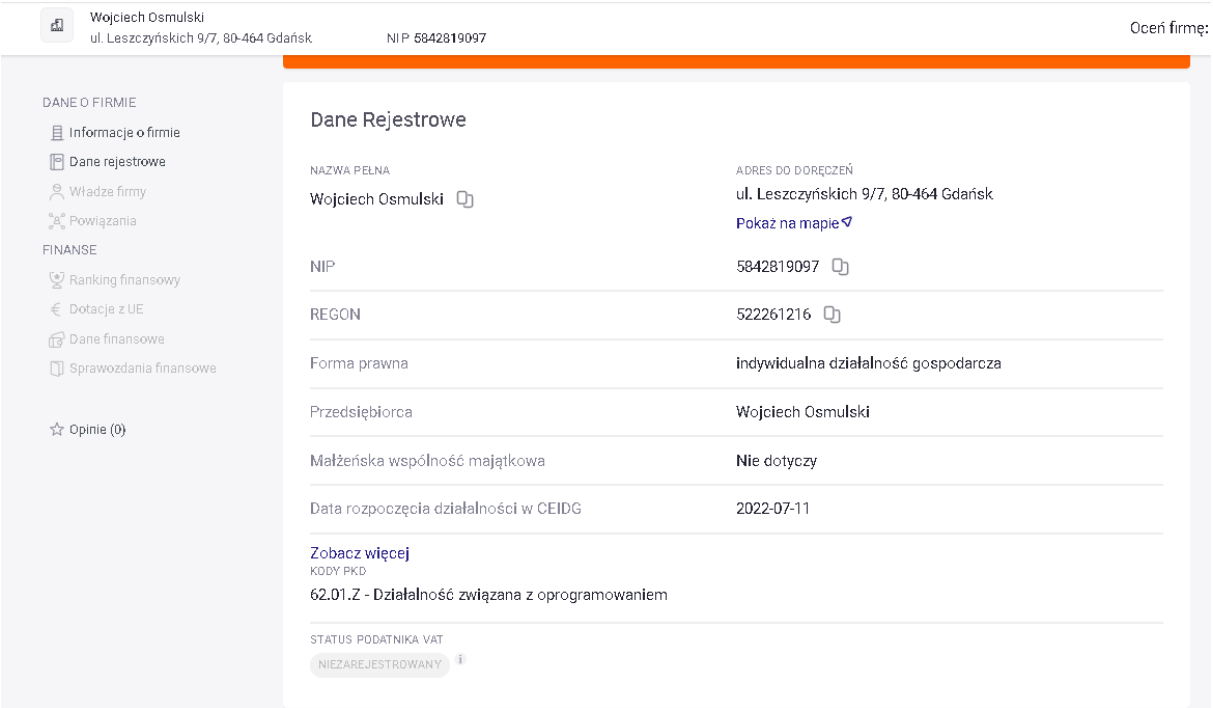
Obraz 8.5.1 social-media Wojciecha Osmulskiego, źródło instagram.com, data wykonania zrzutu 10.1.2024 r.

Obraz 8.5.2 informacje ogólne o Wojciechu Osmulskim, źródło linkedin.com, data wykonania zrzutu 10.1.2024 r.



Obraz 8.5.3 rezultat wyszukania Wojciecha Osmulskiego w social-searcher.com, data wykonania zrzutu 10.1.2024 r.

Adres firmy i zamieszkanie Wojciecha Osmulskiego podane w rejestrze CEIDG (obrazy 8.5.4-8.5.6) zgadzają się z danymi zamieszkania na linkedin.



Obraz 8.5.4 rezultat wyszukania Wojciecha Osmulskiego w polskim rejestrze przedsiębiorców, źródło aleo.com, data wykonania zrzutu 11.1.2024 r.

FIRMA Z: REJESTR CEIDG

Dane podstawowe

Imię:	Wojciech
Nazwisko:	Osmulski
Firma przedsiębiorcy:	Wojciech Osmulski
NIP:	5842819097
REGON:	522261216
Forma prawna:	CEIDG - Osoby fizyczne prowadzące działalność gospodarczą

Obraz 8.5.5 rezultat wyszukania Wojciecha Osmulskiego w polskim rejestrze przedsiębiorców, źródło owg.pl, data wykonania zrzutu 11.1.2024 r.

Klasyfikacja działalności

Działalność przeważająca wg PKD

Kod PKD	Nazwa
62.01.Z	Działalność związana z oprogramowaniem

Działalność wg PKD

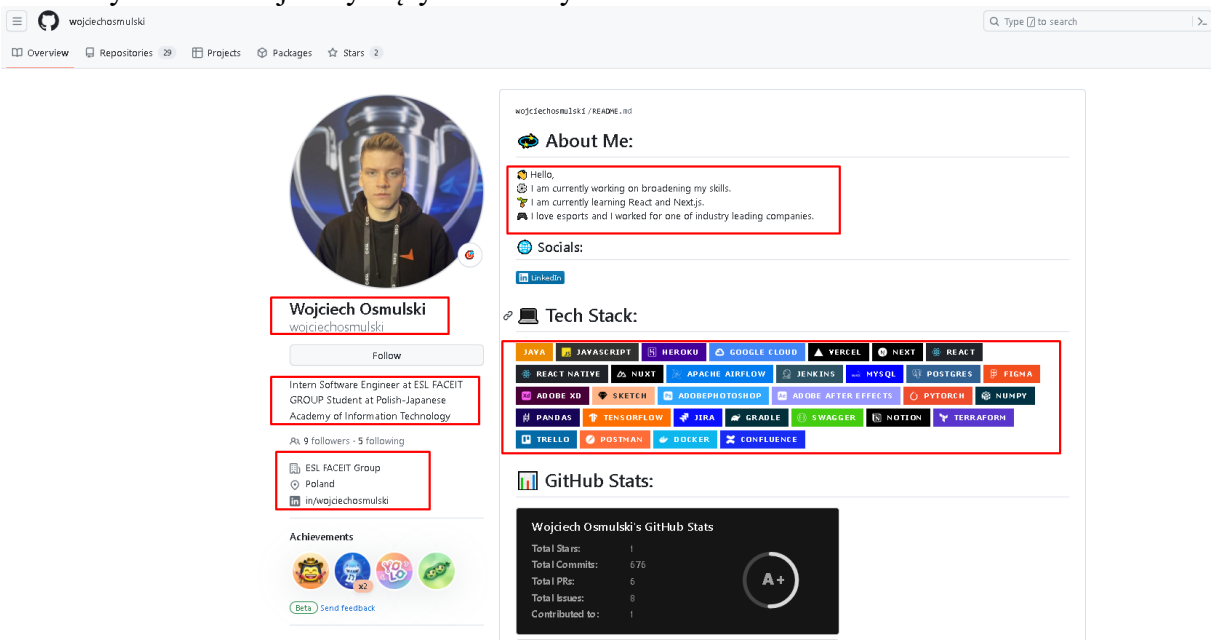
Kod PKD	Nazwa
62.01.Z	Działalność związana z oprogramowaniem

Dane dodatkowe

Data rozpoczęcia wykonywania działalności gospodarczej:	2022-07-11
Data zawieszenia wykonywania idywidualnej działalności:	2022-09-30
Data wznowienia wykonywania indywidualnej działalności:	-
Data zaprzestania wykonywania działalności gospodarczej:	-
Data wykreślenia wpisu z rejestru:	-
Małżeńska wspólnota majątkowa:	-

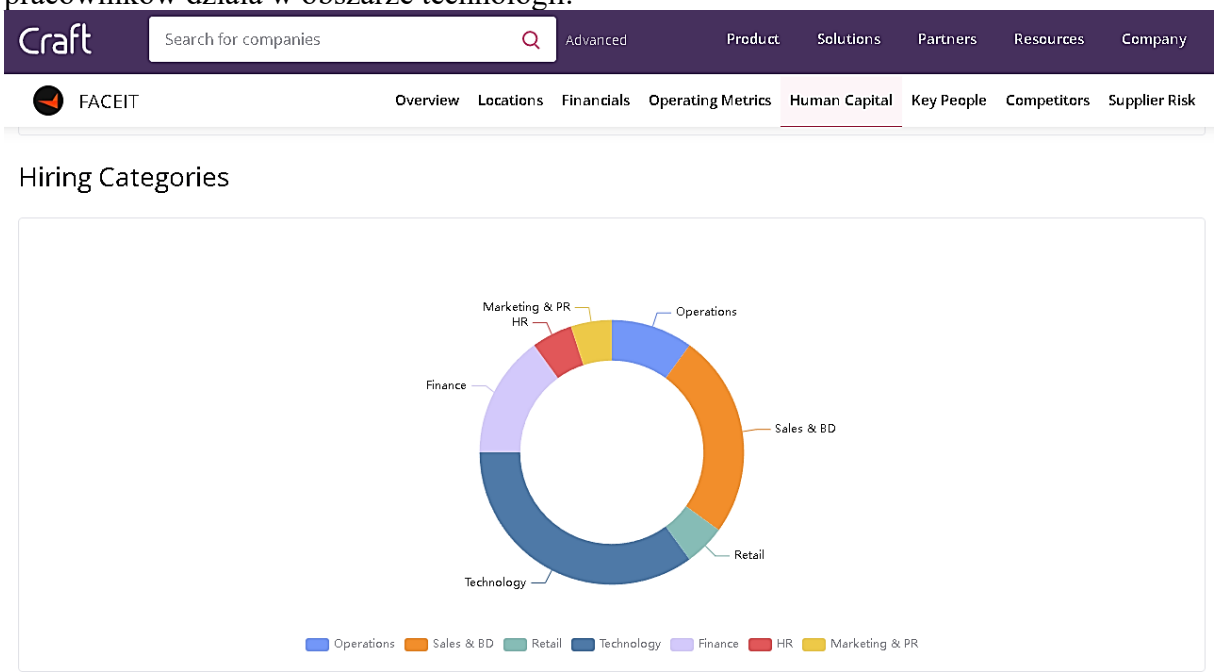
Obraz 8.5.6 rezultat wyszukania Wojciecha Osmulskiego w polskim rejestrze przedsiębiorców, źródło owg.pl, data wykonania zrzutu 11.1.2024 r.

Na obrazie 8.5.7 przedstawiono konto github programisty. W repozytoriach nie znaleziono kluczowych informacji dotyczących domeny faceit.com.



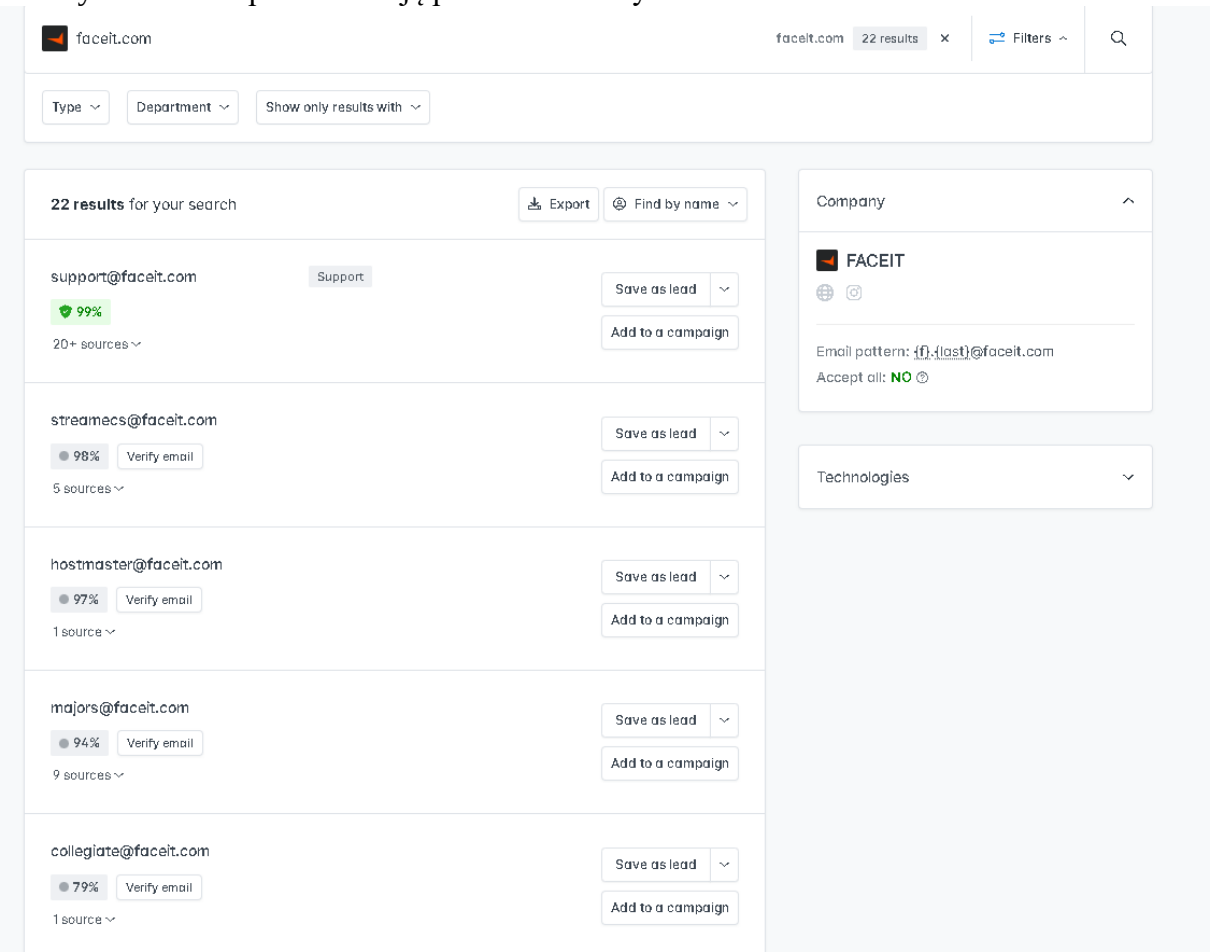
Obraz 8.5.7 strona Github Wojciecha Osmulskiego, źródło owg.pl, data wykonania zrzutu 17.1.2024 r.

Na obrazie 8.6.1 zaprezentowano strukturę zatrudnienia w firmie Faceit – większość pracowników działa w obszarze technologii.

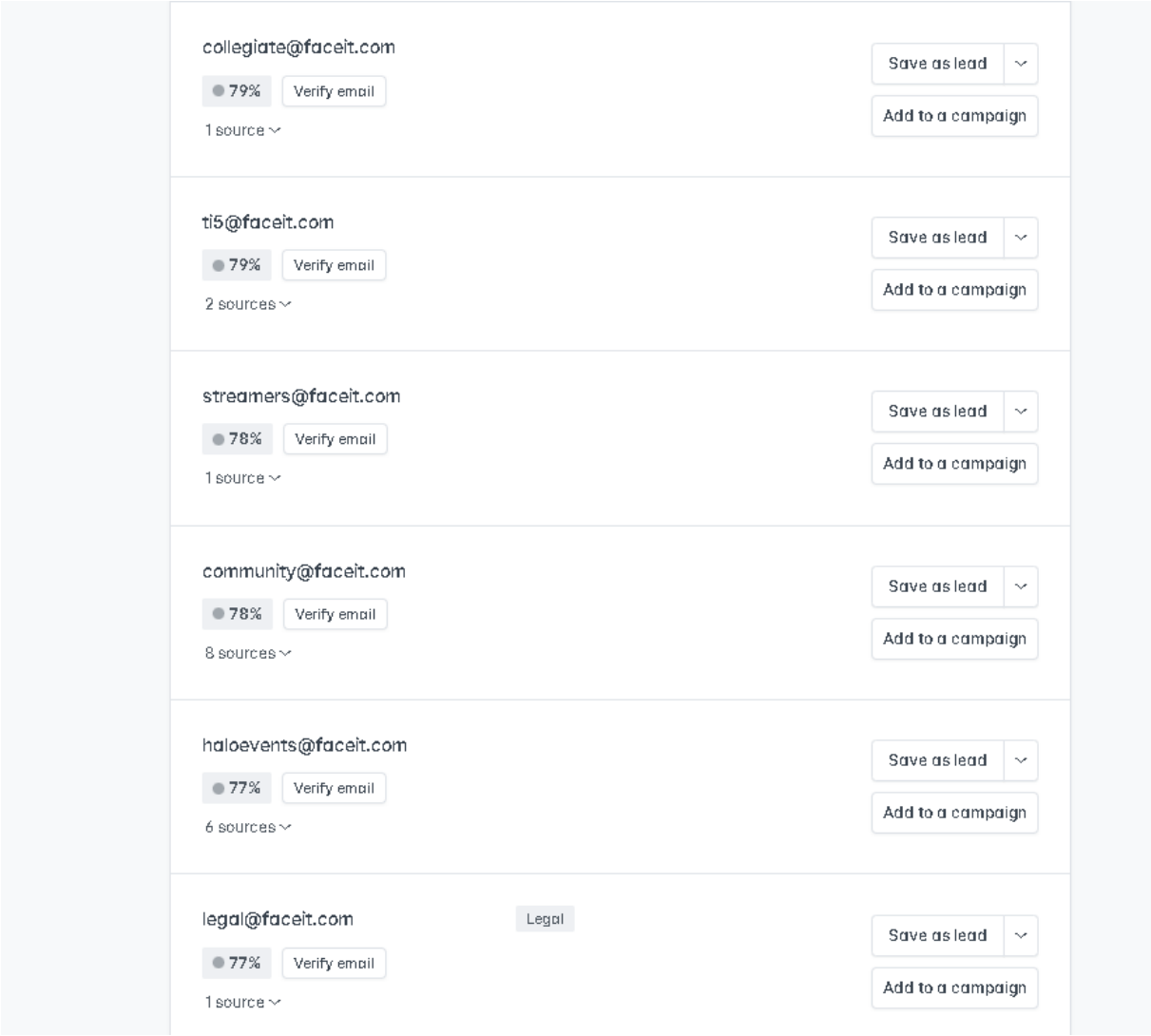


Obraz 8.6.1 struktura zatrudnienia w firmie Faceit, źródło craft.co,data wykonania zrzutu 10.1.2024 r.

Obrazy 8.7.1-8.7.2 przedstawiają publiczne adresy email.

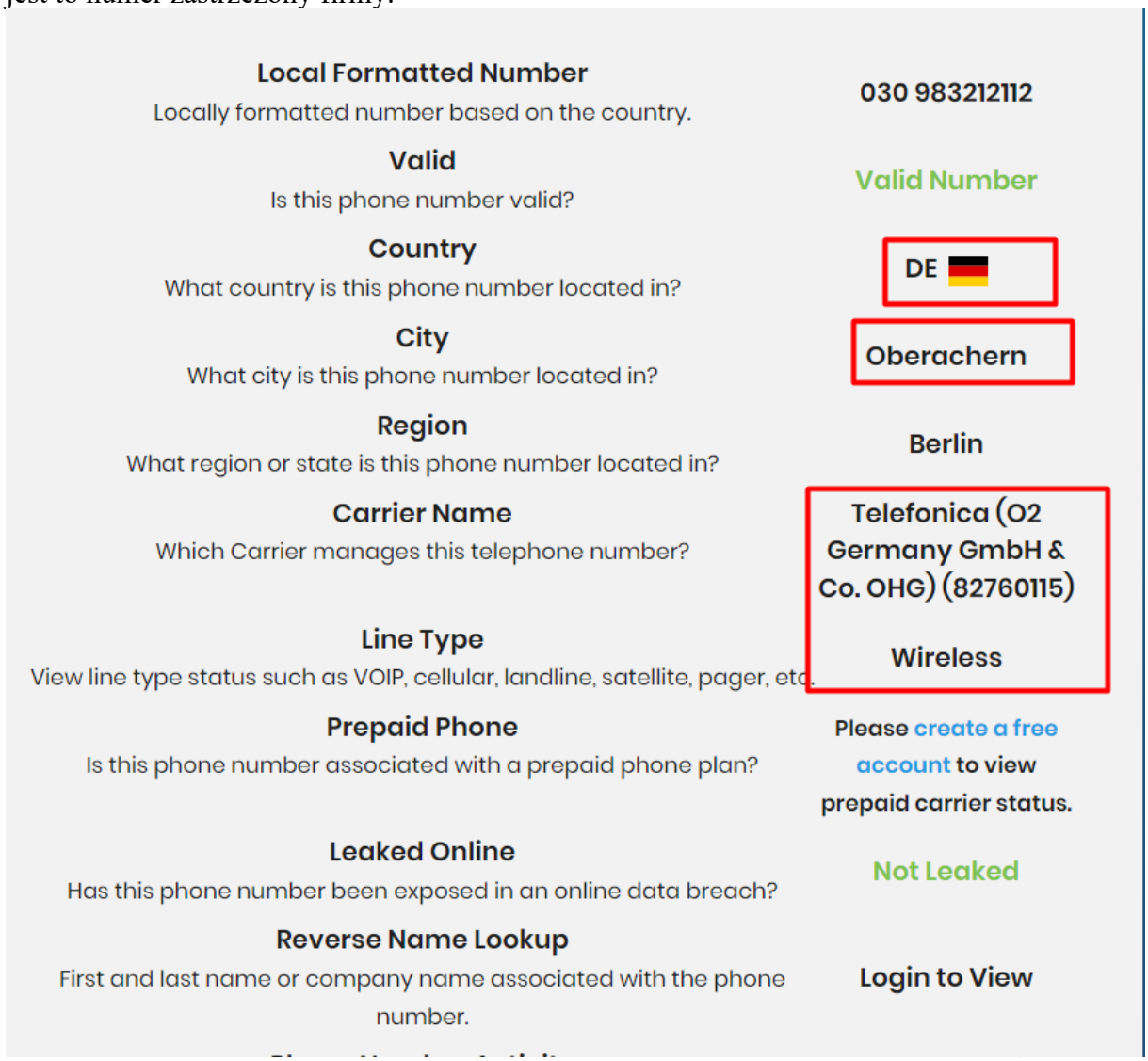


Obraz 8.7.1 publiczne adresu email domeny faceit.com, źródło hunter.io, data wykonania zrzutu 13.12.2023 r.



Obraz 8.7.2 publiczne adresu email domeny faceit.com, źródło hunter.io, data wykonania zrzutu 13.12.2023 r.

Na obrazie 8.8.1 sprawdzono numer telefonu wykryty przez narzędzie maltego. Miasto Oberachern nie jest siedzibą firmy ESL FACEIT GROUP, zatem nie można podejrzewać, że jest to numer zastrzeżony firmy.



Obraz 8.8.1 sprawdzenie numeru telefonu, źródło ipqualityscore.com, data wykonania zrzutu 10.2.2024 r.

W zbieraniu danych do rozdziału 8 skorzystano ze stron takich jak linkedin.com, hunter.io, owg.pl, aleo.com, instagram.com, esportsawards.com, italianbusinessregister.it, gov.uk, about.me/stermy, esportsearnings.com, escharts.com, social-searcher.com, facebook.com, crunchbase.com, github.com, clubdeglinvestitori.it. Nie udało znaleźć się prywatnych adresów e-mail pracowników. Znaleziono prywatne konto programisty jak i jego rekord w polskim rejestrze przedsiębiorców. W rozdziale 5 narzędzie maltego wykryło 2 numery telefonów których prefiksem jest numer 49 identyfikujący je z numerem zarządzanym przez organizacje niemieckie.

9. Bezpieczeństwo

Na obrazach 9.1.1-9.1.4 przedstawiono podatności dla języka PHP w wersji 5.4.16 (który jest używany przez stronę corporate.faceit.com) umożliwiające m.in. zdalne wykonanie kodu.

PHP 5.4/5.5/5.6 - 'Unserialize()' Use-After-Free

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
38125	N/A	TAOGUANG CHEN	DOS	PHP	2015-09-09

EDB Verified: ✕ Exploit: / {} Vulnerable App:

```
Use After Free Vulnerabilities in unserialize()

Taoguang Chen <[@chtg](http://github.com/chtg)>
Write Date: 2015.7.31
Release Date: 2015.9.4

Multiple use-after-free vulnerabilities were discovered in unserialize() with Serializable class that can be abused for leaking arbitrary memory blocks or execute
arbitrary code remotely.

Affected Versions
------------
Affected is PHP 5.6 < 5.6.12
Affected is PHP 5.5 < 5.5.28
Affected is PHP 5.4 < 5.4.44
```

Obraz 9.1.1 podatność dla języka PHP, źródło exploit-db.com, data wykonania zrzutu 07.02.2024r.

PHP 5.4/5.5/5.6 - SplObjectStorage 'Unserialize()' Use-After-Free

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
38122	2015-6834	TAOGUANG CHEN	DOS	PHP	2015-09-09

EDB Verified: ✓ Exploit: / {} Vulnerable App:

```
Yet Another Use After Free Vulnerability in unserialize() with SplObjectStorage

Taoguang Chen <[@chtg](http://github.com/chtg)>
Write Date: 2015.8.27
Release Date: 2015.9.4

A use-after-free vulnerability was discovered in unserialize() with SplObjectStorage object's deserialization and crafted object's __wakeup() magic method that can be
abused for leaking arbitrary memory blocks or execute arbitrary code remotely.

Affected Versions
------------
Affected is PHP 5.6 < 5.6.13
Affected is PHP 5.5 < 5.5.29
Affected is PHP 5.4 < 5.4.45
```

Obraz 9.1.2 podatność dla języka PHP, źródło exploit-db.com, data wykonania zrzutu 07.02.2024r.

PHP 5.4/5.5/5.6 - SplDoublyLinkedList 'Unserialize()' Use-After-Free

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
38120	2015-6834	TAOGUANG CHEN	DOS	PHP	2015-09-09

EDB Verified: ✓ Exploit: / {} Vulnerable App:

```
Yet Another Use After Free Vulnerability in unserialize() with SplDoublyLinkedList

Taoguang Chen <[@chtg](http://github.com/chtg)> -
Write Date: 2015.8.27
Release Date: 2015.9.4

A use-after-free vulnerability was discovered in unserialize() with SplDoublyLinkedList object's deserialization and crafted object's __wakeup() magic method that can
be abused for leaking arbitrary memory blocks or execute arbitrary code remotely.

Affected Versions
------------
Affected is PHP 5.6 < 5.6.13
Affected is PHP 5.5 < 5.5.29
Affected is PHP 5.4 < 5.4.45
```

Obraz 9.1.3 podatność dla języka PHP, źródło exploit-db.com, data wykonania zrzutu 07.02.2024r.

Vulnerability Details : CVE-2019-9641

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.

Obraz 9.1.4 podatności dla języka PHP, źródło sca.analysiscenter.veracode.com

Baza danych spamu nie wykazała , że wskazany adres IP znajduje się na czarnej liście (obrazy 9.2.1, .9.2.2).

Obraz 9.2.1 sprawdzenie bazy danych spamu, źródło dnsdbl.com, data wykonania zrzutu 11.1.2024 r.

Obraz 9.2.2 sprawdzenie bazy danych spamu, źródło dnsdbl.com, data wykonania zrzutu 11.1.2024 r.

Baza danych spamu (mxtoolbox.com) nie wykazała , że wskazany adres IP znajduje się na czarnej liście z sprawdzanych 92 list (obrazy 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5).

Checking **faceit.com** which resolves to **104.17.62.50** against **92** known blacklists...
Listed **0** times with **1** timeouts

	Blacklist	Reason	TTL	ResponseTime	
OK	ivmURI			10	
OK	Nordspam DBL			0	
OK	SEM FRESH			31	
OK	SEM URI			31	
OK	SEM URIRED			31	
OK	SORBS RHSBL BADCONF			0	
OK	SORBS RHSBL NOMAIL			0	
OK	Spamhaus DBL			0	
OK	SURBL multi			0	
OK	0SPAM			44	
OK	0SPAM RBL			44	
OK	Abuse.ro			122	
OK	Abusix Mail Intelligence Blacklist			0	
OK	Abusix Mail Intelligence Domain Blacklist			0	
OK	Abusix Mail Intelligence Exploit list			0	
OK	Anonmails DNSBL			101	
OK	BACKSCATTERER			0	
OK	BARRACUDA			11	
OK	BLOCKLIST.DE			0	
OK	CALIVENT			11	
OK	CYMRU BOGONS			31	

Obraz 9.3.1 sprawdzenie bazy danych spamu, źródło mxtoolbox.com, data wykonania zrzutu 11.1.2024 r.

OK	DAN TOR			255	
OK	DAN TOREXIT			255	
OK	DNS SERVICIOS			112	
OK	DRMX			214	
OK	DRONE BL			21	
OK	FABELSOURCES			11	
OK	HIL			11	
OK	HIL2			11	
OK	Hostkarma Black			65	
OK	IBM DNS Blacklist			11	
OK	ICMFORBIDDEN			122	
OK	IMP SPAM			11	
OK	IMP WORM			11	
OK	INTERSERVER			21	
OK	ivmSIP			0	
OK	ivmSIP24			0	
OK	JIPPG			162	
OK	KEMPTBL			0	
OK	KISA			193	
OK	Konstant			10	
OK	LASHBACK			0	
OK	LNSGBLOCK			10	
OK	LNSGBULK			10	
OK	LNSGMULTI			10	

Obraz 9.3.2 sprawdzenie bazy danych spamu, źródło mxtoolbox.com, data wykonania zrzutu 11.1.2024 r.

OK	LNSGOR			10	
OK	LNSGSRC			10	
OK	MADAVI			213	
OK	MAILSPIKE BL			65	
OK	MAILSPIKE Z			65	
OK	MSRBL Phishing			21	
OK	MSRBL Spam			81	
OK	NETHERRELAYS			10	
OK	NETHERUNSURE			10	
OK	NIXSPAM			10	
OK	Nordspam BL			10	
OK	ORVEDB			122	
OK	PSBL			0	
OK	RATS Dyna			0	
OK	RATS NoPtr			0	
OK	RATS Spam			0	
OK	RBL JP			0	
OK	RSBL			121	
OK	s5h.net			13	
OK	SCHULTE			13	
OK	SEM BACKSCATTER			34	
OK	SEM BLACK			34	

Obraz 9.3.3 sprawdzenie bazy danych spamu, źródło mxtoolbox.com, data wykonania zrzutu 11.1.2024 r.

OK	SERVICESNET			23	
OK	SORBS BLOCK			0	
OK	SORBS DUHL			0	
OK	SORBS HTTP			0	
OK	SORBS MISC			0	
OK	SORBS NEW			0	
OK	SORBS SMTP			0	
OK	SORBS SOCKS			10	
OK	SORBS SPAM			10	
OK	SORBS WEB			13	
OK	SORBS ZOMBIE			10	
OK	SPAMCOP			10	
OK	Spamhaus ZEN			10	
OK	SPFBL DNSBL		259200	121	
OK	Suomispam Reputation			101	
OK	SWINOG			10	
OK	TRIUMF			3	
OK	TRUNCATE			20	
OK	UCEPROTECTL1			0	
OK	UCEPROTECTL2			0	
OK	UCEPROTECTL3			0	
OK	Woodys SMTP Blacklist			0	
OK	ZapBL			77	
TIMEOUT	NoSolicitado			0	Ignore

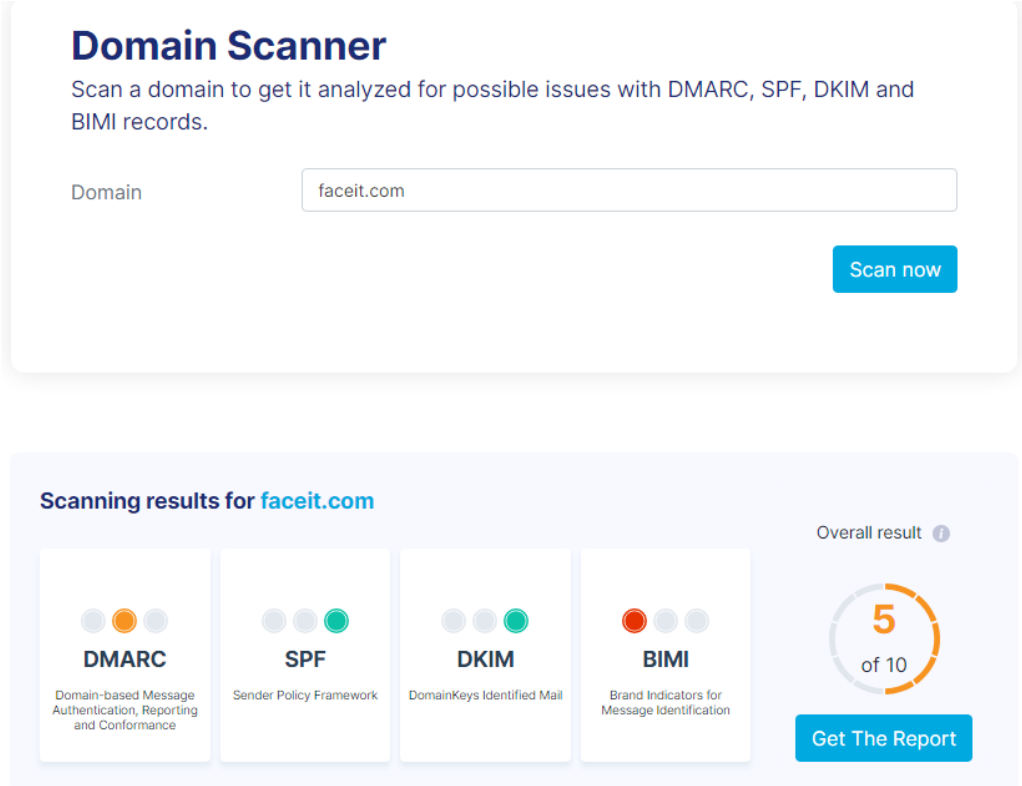
Obraz 9.3.4 sprawdzenie bazy danych spamu, źródło mxtoolbox.com, data wykonania zrzutu 11.1.2024 r.

Checking 104.17.63.50 against 83 known blacklists...
Listed 0 times with 1 timeouts

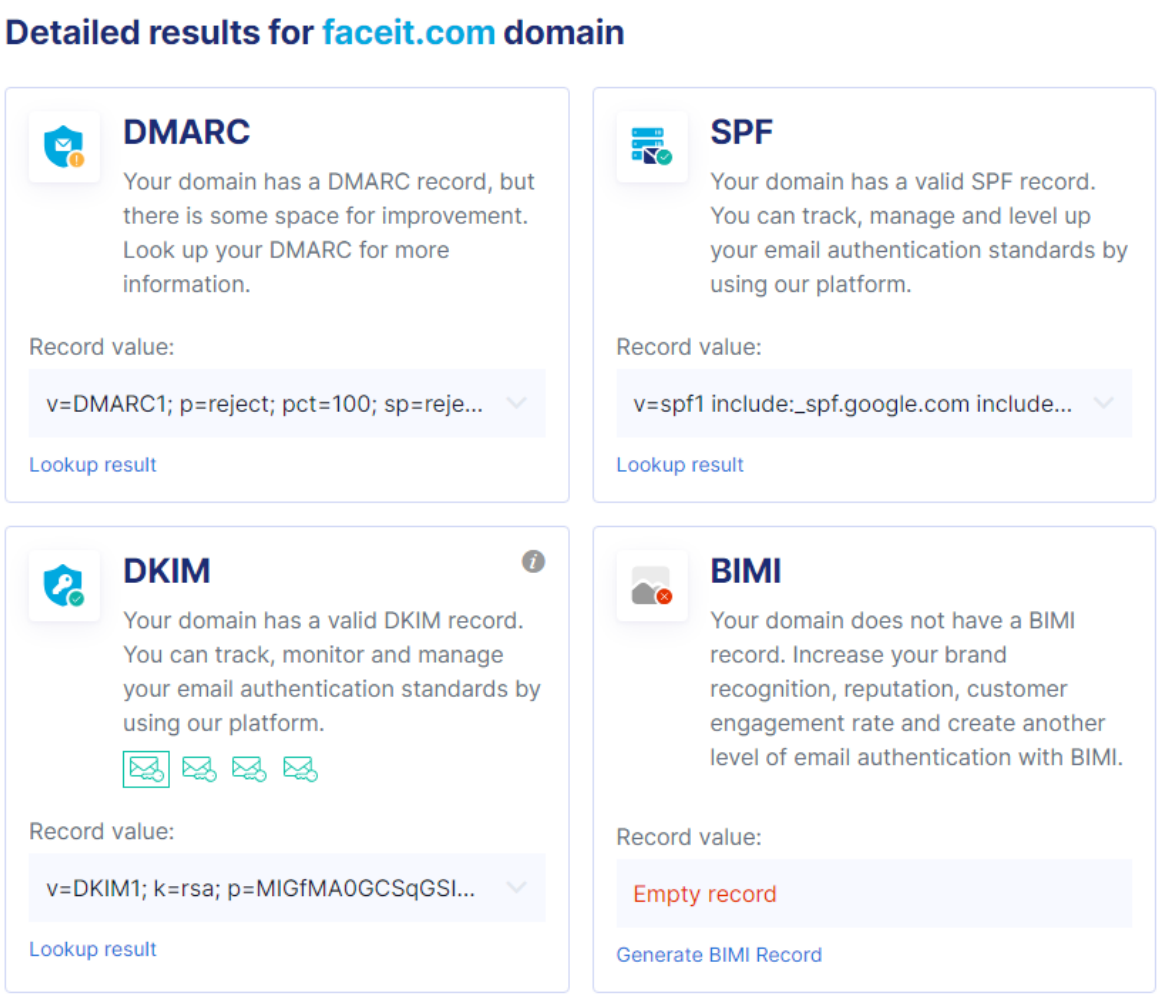
	Blacklist	Reason	TTL	ResponseTime	
OK	0SPAM			42	
OK	0SPAM RBL			42	
OK	Abuse.ro			119	
OK	Abusix Mail Intelligence Blacklist			0	
OK	Abusix Mail Intelligence Domain Blacklist			0	
OK	Abusix Mail Intelligence Exploit list			10	
OK	Anonmails DNSBL			109	
OK	BACKSCATTERER			11	
OK	BARRACUDA			11	
OK	BLOCKLIST.DE			10	
OK	CALIVENT			11	
OK	CYMRU BOGONS			32	
OK	DAN TOR			270	
OK	DAN TOREXIT			270	
OK	DNS SERVICIOS			109	
OK	DRMX			206	
OK	DRONE BL			21	
OK	FABELSOURCES			11	
OK	HIL			1	

Obraz 9.3.5 sprawdzenie bazy danych spamu , źródło mxtoolbox.com, data wykonania zrzutu 15.1.2024 r.

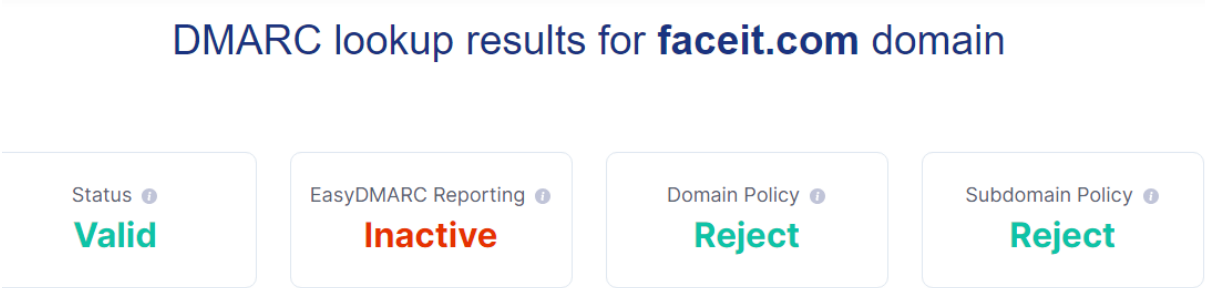
Obrazy 9.4.1-9.4.4 wskazują, że strona faceit.com posiada rekordy DMARC, SPF, DKIM. Narzędzie wskazuje na możliwość poprawki – dodanie rekordu BIMI w celu uwierzytelniania adresów email.



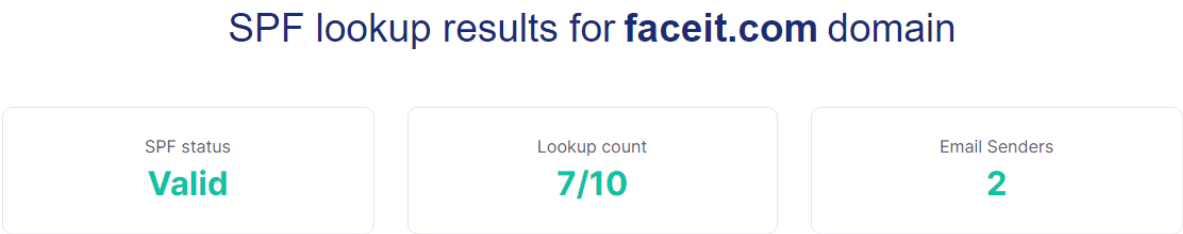
Obraz 9.4.1 raport skanu domeny faceit.com, źródło easydmarc.com, data wykonania zrzutu 11.1.2024 r.



Obraz 9.4.2 raport skanu domeny faceit.com, źródło easydmarc.com, data wykonania zrzutu 11.1.2024 r.

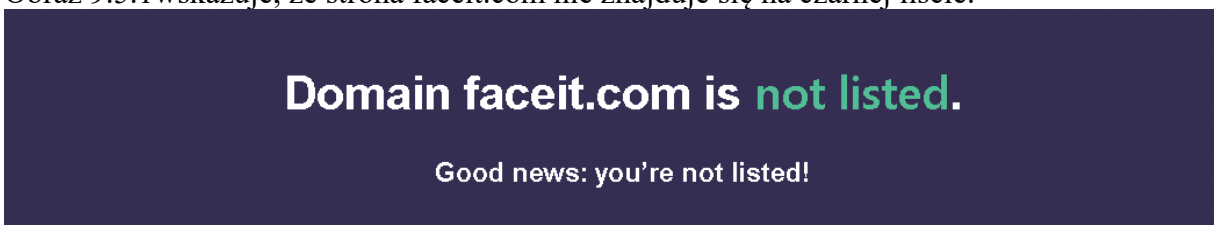


Obraz 9.4.3 raport skanu domeny faceit.com, źródło easydmarc.com, data wykonania zrzutu 11.1.2024 r.



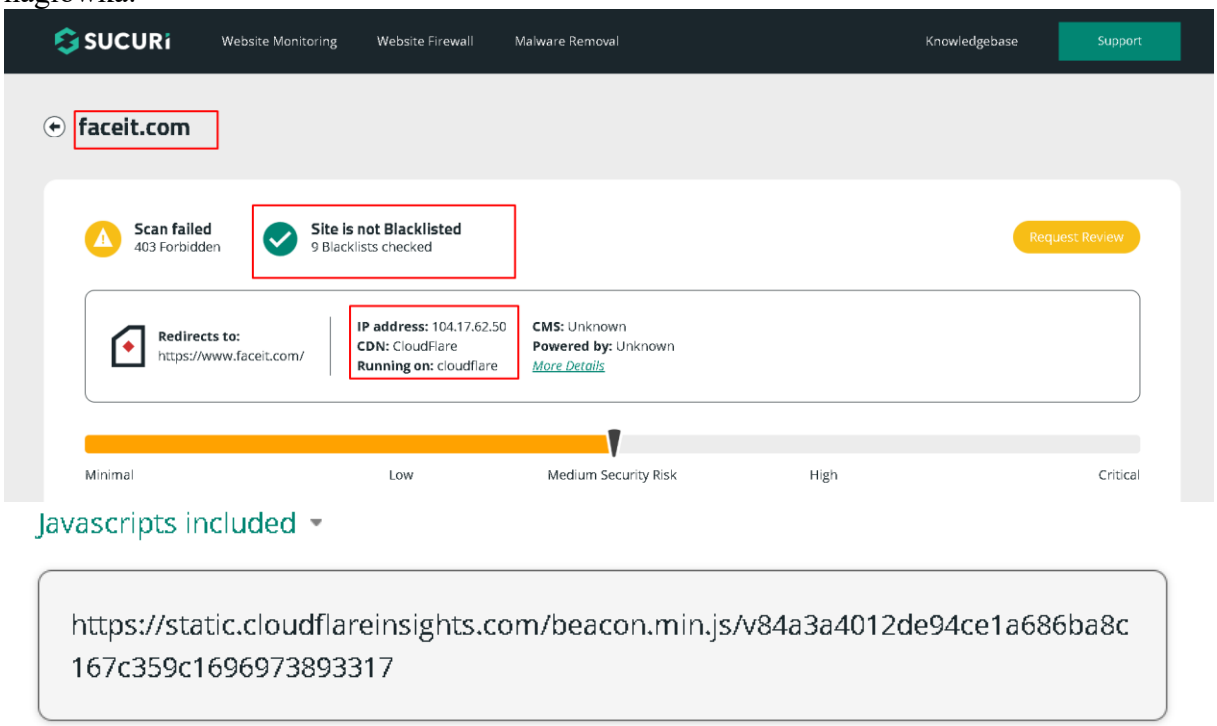
Obraz 9.4.4 raport skanu domeny faceit.com, źródło easydmarc.com, data wykonania zrzutu 11.1.2024 r.

Obraz 9.5.1wskazuje, że strona faceit.com nie znajduje się na czarnej liście.

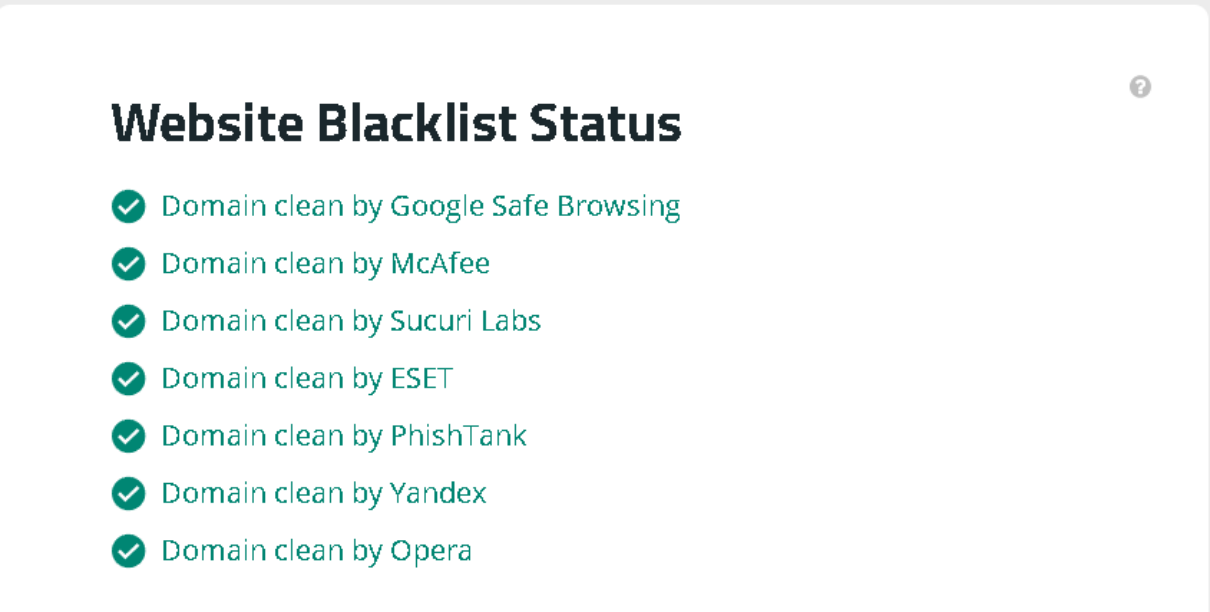


Obraz 9.5.1 sprawdzenie bazy danych spamu, źródło lookup.abusix.com, data wykonania zrzutu 15.1.2024 r.

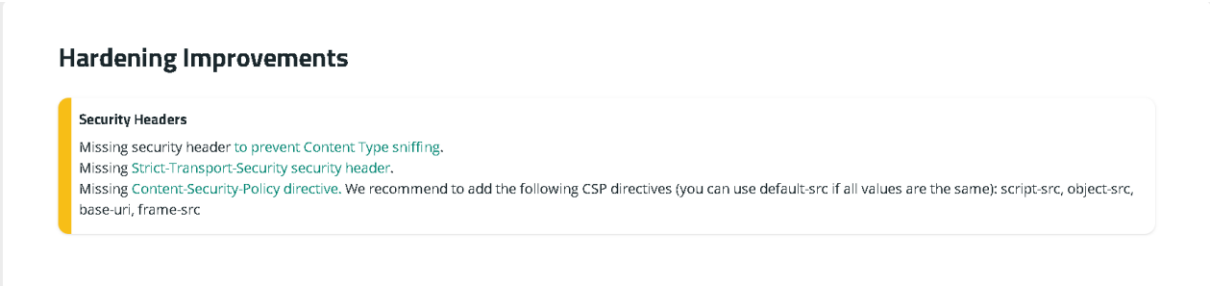
Obrazy 9.6.1-9.6.3 wskazują, że strona faceit.com nie znajduje się na czarnej liście (sprawdzono 9 czarnych list, m.in. Google safe browsing). Narzędzie wskazuje na możliwość poprawki – dodanie zabezpieczenia nagłówka w celu zabezpieczenia przed podsłuchem nagłówka.



Obraz 9.6.1 raport wygenerowany przez sitecheck.sucuri.net, data wykonania zrzutu 15.1.2024 r., domena nie jest na czarnej liście

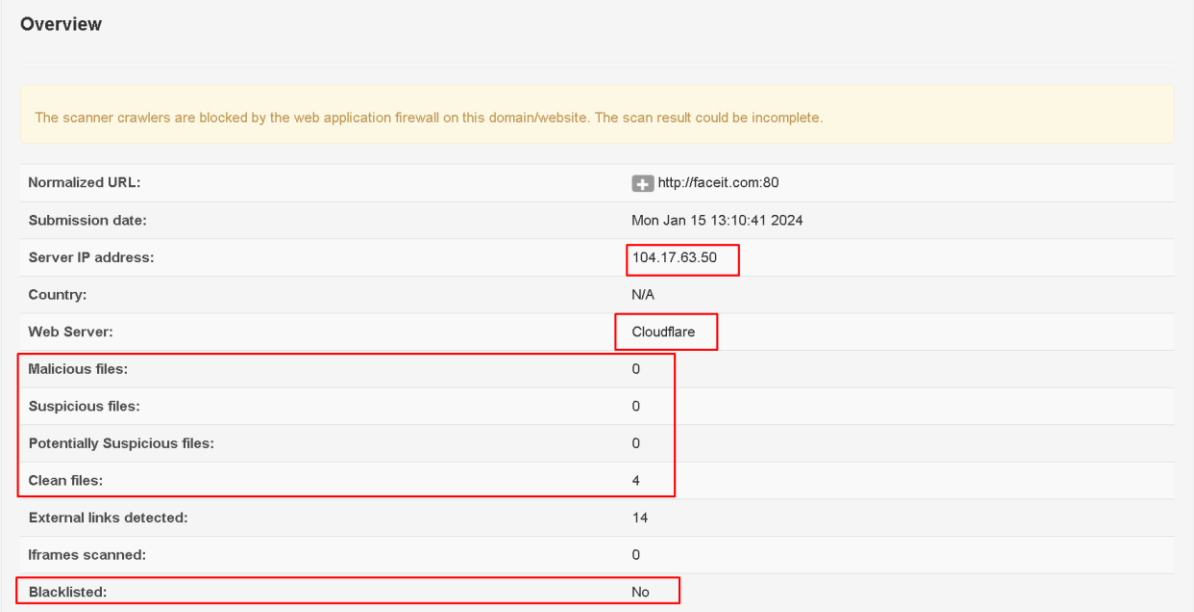


Obraz 9.6.2 sprawdzenie bazy danych spamu, źródło sitecheck.sucuri.net, data wykonania zrzutu 15.1.2024 r., domena nie jest na czarnej liście



Obraz 9.6.3 sprawdzenie nagłówka HTTP, źródło sitecheck.sucuri.net, data wykonania zrzutu 15.1.2024 r.

Analiza plików dostępna na obrazach 9.7.1-9.7.3 nie wykazała złośliwych plików udostępnianych przez stronę faceit.com. Ponadto strona nie znajduje się na czarnej liście bazy.



Obraz 9.7.1 raport wygenerowany przez scanner.pcrisk.com, data wykonania zrzutu 15.1.2024 r.

Clean files: 4

/#

Severity:	Clean
Reason:	No significant issues detected.
Details:	File is clean.
File size[byte]:	5977
File type:	HTML
MD5:	6A96EA10BE8AD4D35B49A2AD875A3E28
Scan duration[sec]:	0.129

/cdn-cgi/styles/cf.errors.ie.css

Severity:	Clean
Reason:	No significant issues detected.
Details:	File is clean.
File size[byte]:	3429
File type:	INI
MD5:	B6664BE34FA5F99C65E55E8D721CB511
Scan duration[sec]:	0.052

Obraz 9.7.2 sprawdzenie plików pod kątem bezpieczeństwa, źródło scanner.pcrisk.com, data wykonania zrzutu 15.1.2024 r.

/cdn-cgi/styles/cf.errors.css

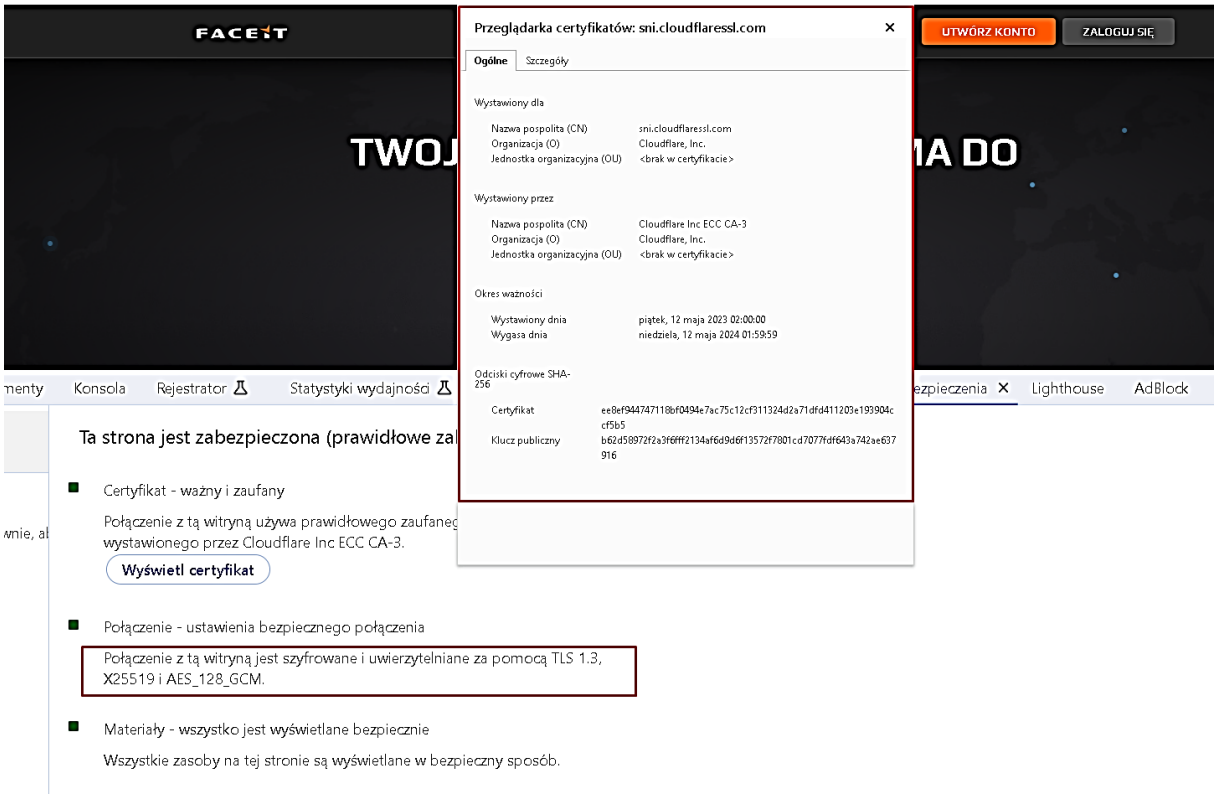
Severity:	Clean
Reason:	No significant issues detected.
Details:	File is clean.
File size[byte]:	24132
File type:	INI
MD5:	A1CEDC21F16B5A97114857154FAB35E9
Scan duration[sec]:	0.199

/cdn-cgi/challenge-platform/scripts/jsd/main.js

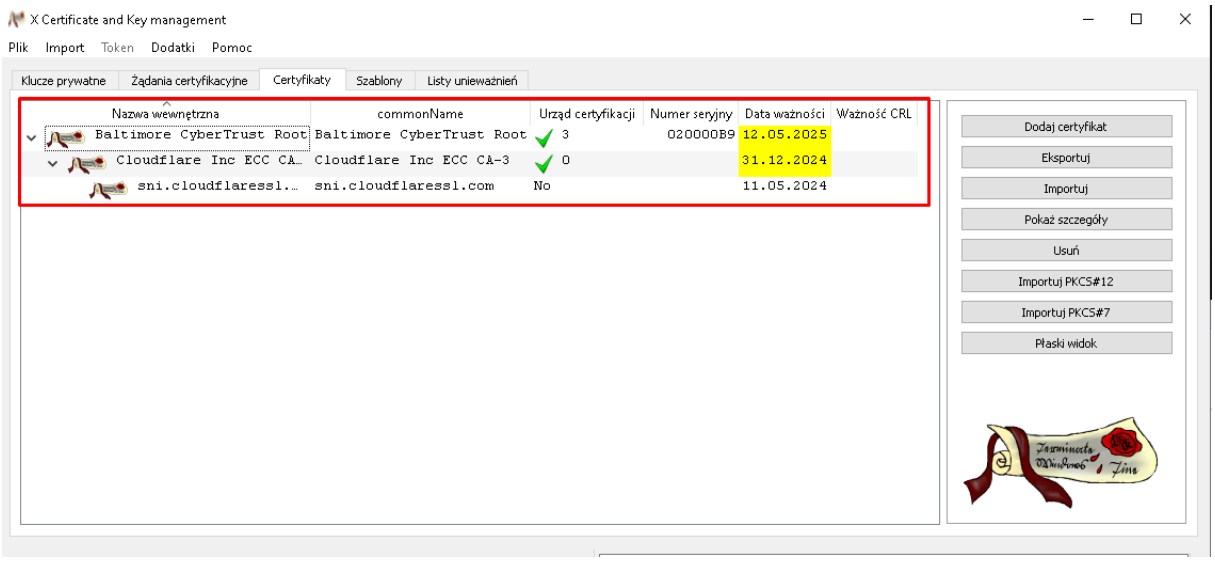
Severity:	Clean
Reason:	No significant issues detected.
Details:	File is clean.
File size[byte]:	7432
File type:	ASCII
MD5:	C7310818DE35048668FF81B15D5D2E04
Scan duration[sec]:	1.495

Obraz 9.7.3 sprawdzenie plików pod kątem bezpieczeństwa, źródło scanner.pcrisk.com, data wykonania zrzutu 15.1.2024 r.

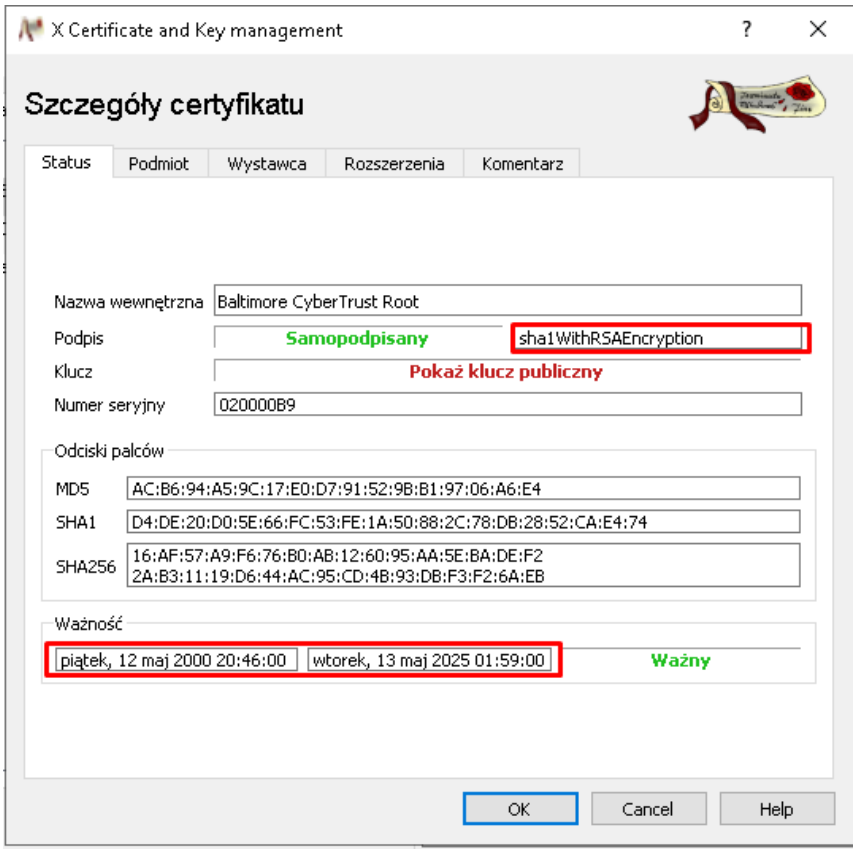
Pobrane certyfikaty ze strony faceit.com zostały zaimportowane do narzędzia XCA. Interesujące jest to, że root certyfikat został wystawiony na 25 lat (Amazon zaleca obecnie 10 lat). Podpis na root certyfikacie korzysta z funkcji SHA-1 (w 2017 r. wygenerowano 2 pliki o takim samym skrócie SHA-1).



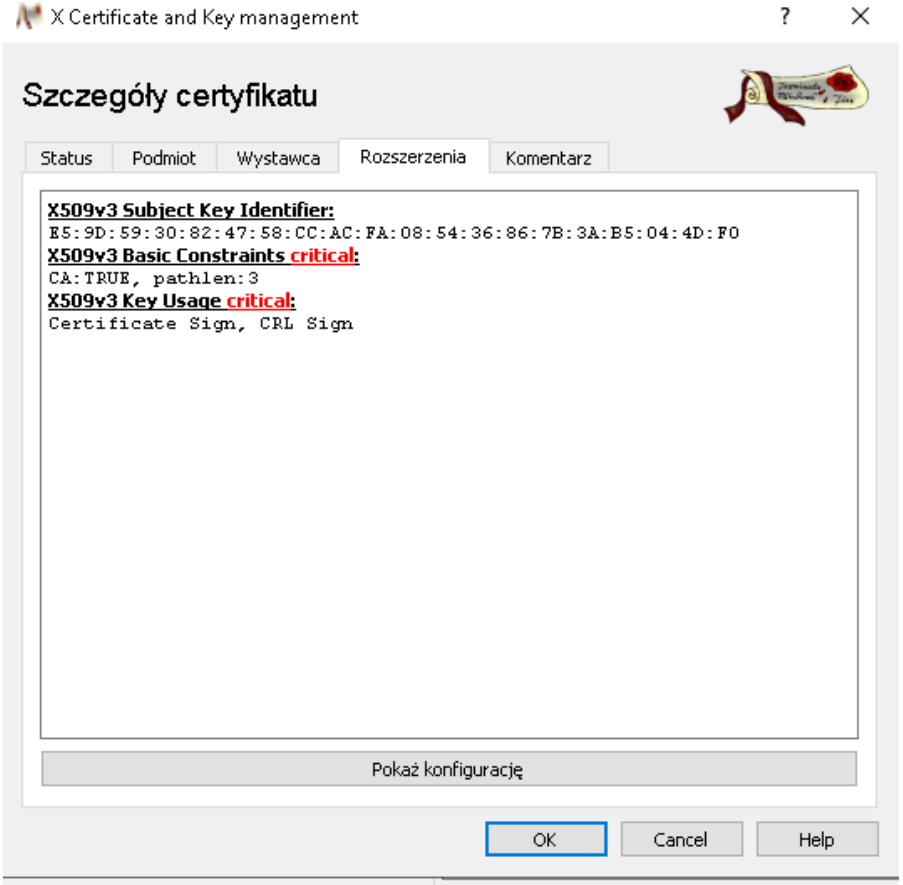
Obraz 9.8.1 certyfikat strony faceit.com, data wykonania zrzutu 11.1.2024 r.



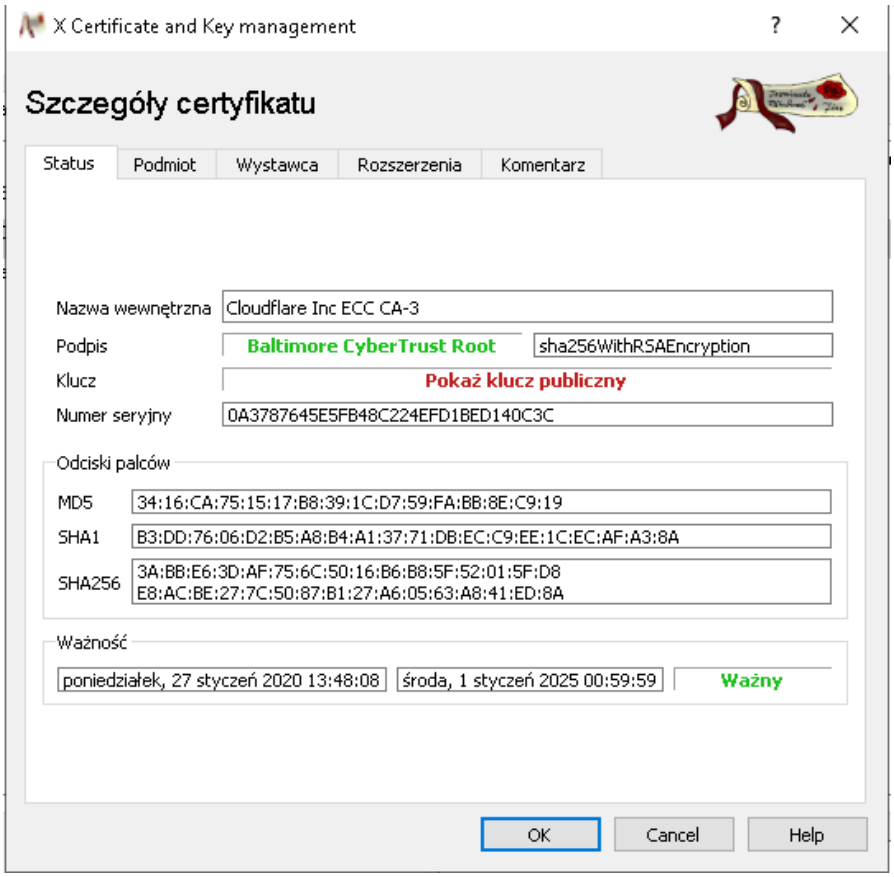
Obraz 9.8.2 certyfikaty strony faceit.com, narzędzie XCA, data wykonania zrzutu 11.1.2024 r.



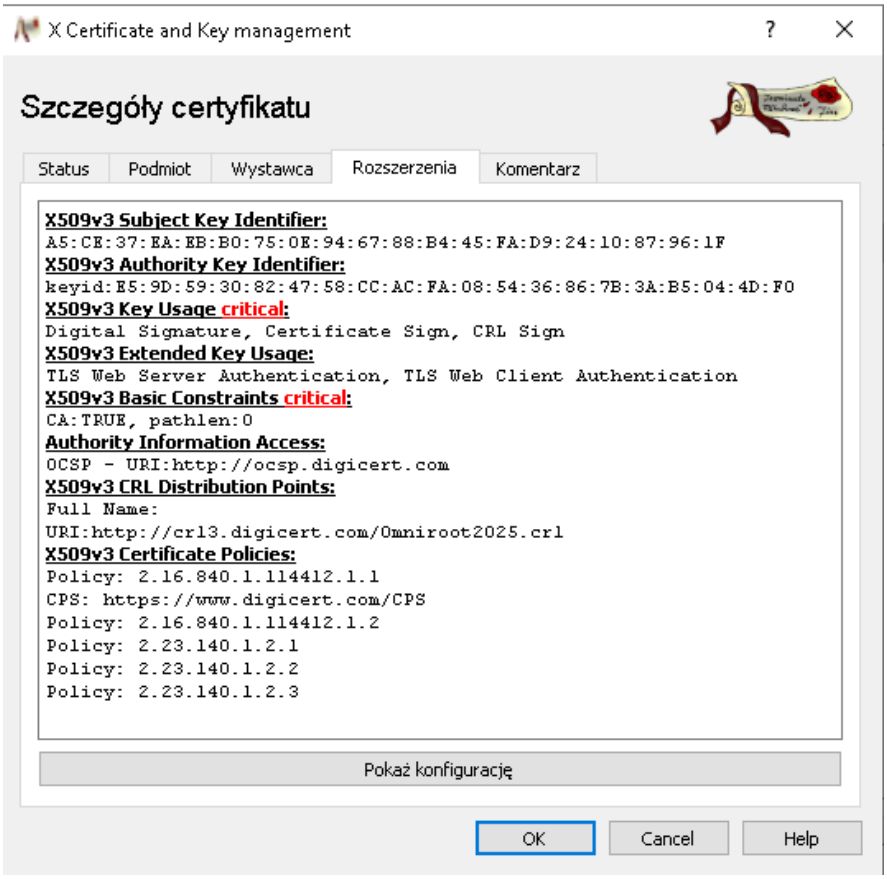
Obraz 9.8.3 certyfikat strony faceit.com, narzędzie XCA, data wykonania zrzutu 11.1.2024 r.



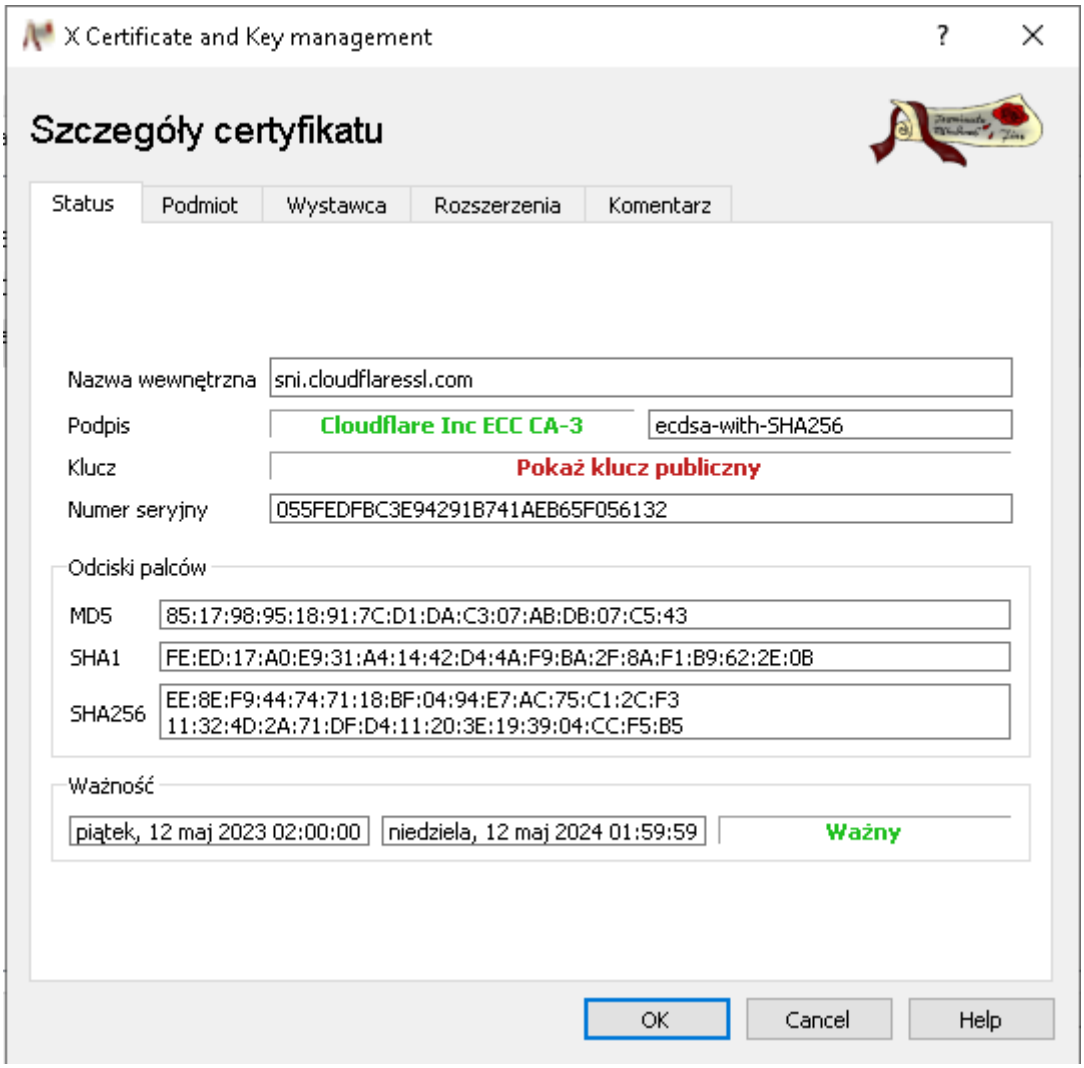
Obraz 9.8.4 certyfikat strony faceit.com, narzędzie XCA, data wykonania zrzutu 11.1.2024 r.



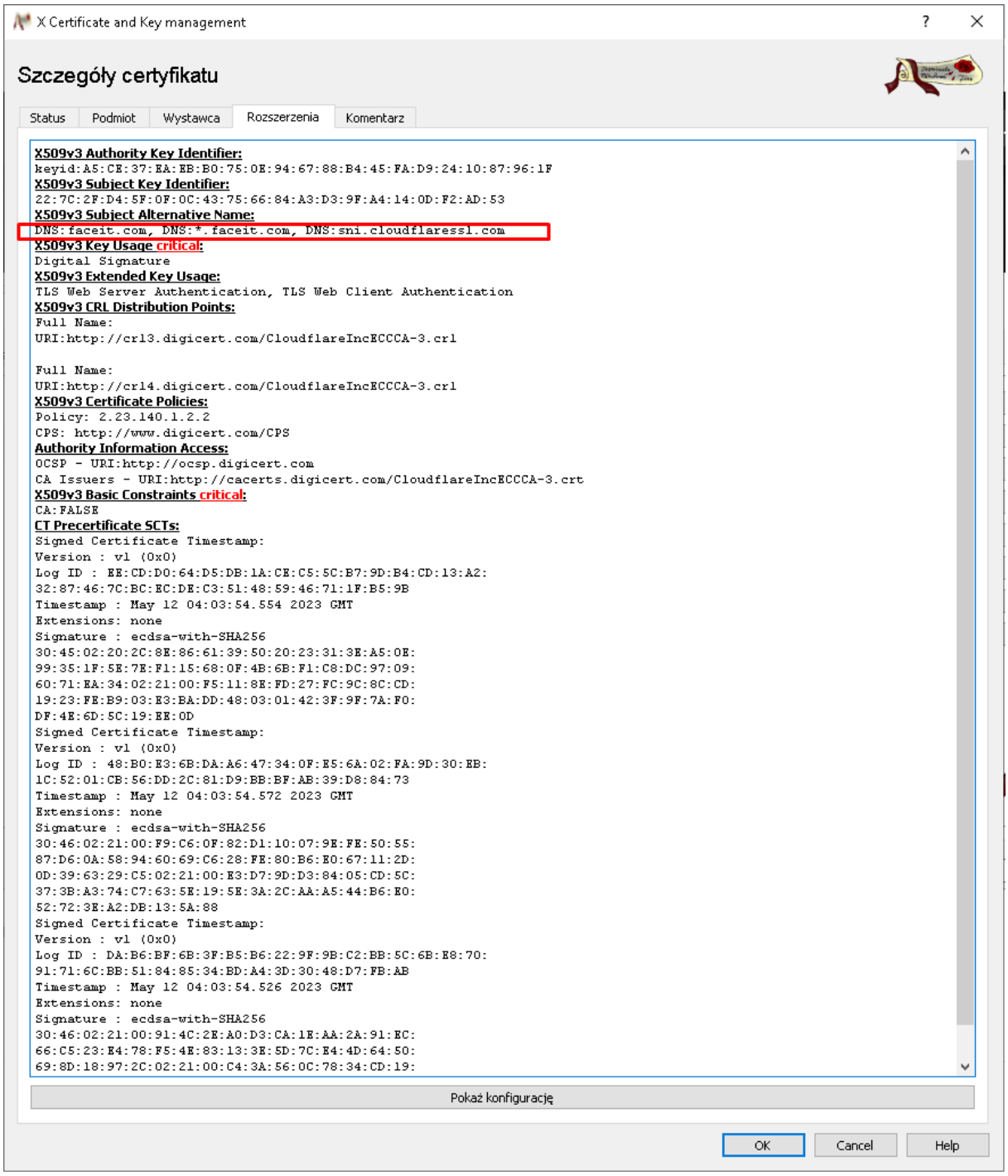
Obraz 9.8.5 certyfikat strony faceit.com, narzędzie XCA, data wykonania zrzutu 11.1.2024 r.



Obraz 9.8.6 certyfikat strony faceit.com, narzędzie XCA, data wykonania zrzutu 11.1.2024 r.

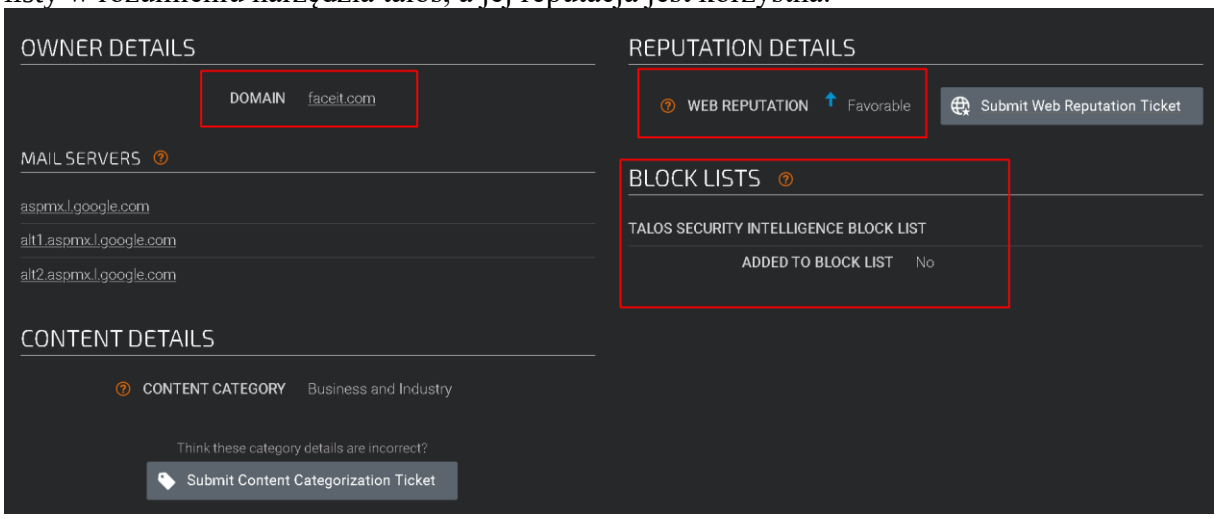


Obraz 9.8.7 certyfikat strony faceit.com, narzędzie XCA, data wykonania zrzutu 11.1.2024 r.



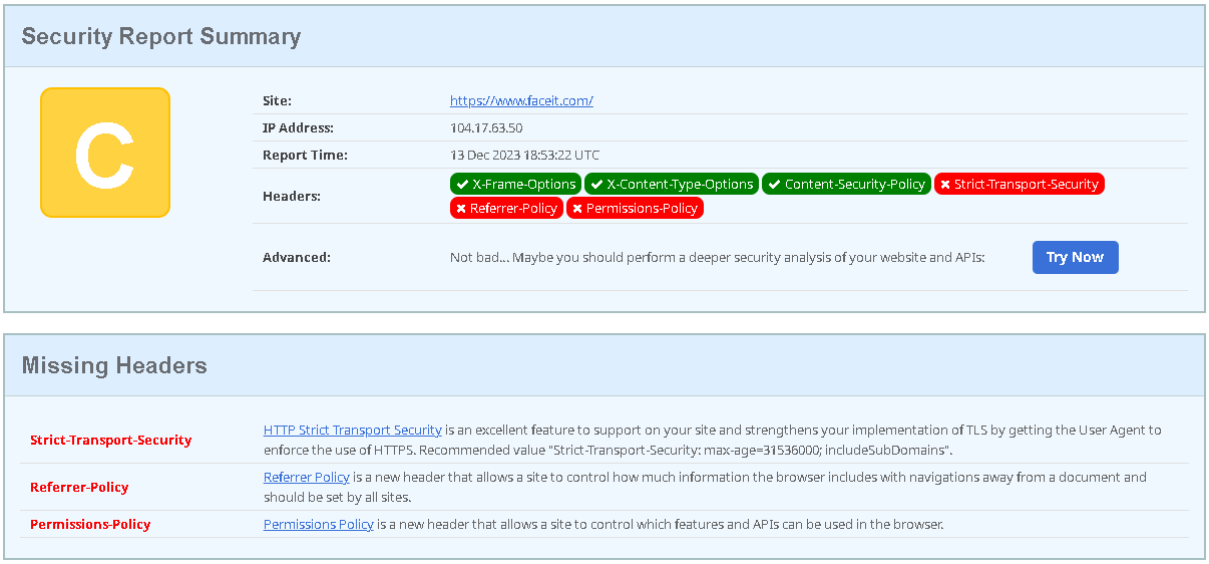
Obraz 9.8.8 certyfikat strony faceit.com, narzędzie XCA, data wykonania zrzutu 11.1.2024 r.

Na obrazie 9.10.1 zaprezentowano, że domena faceit.com nie została dodana do zablokowanej listy w rozumieniu narzędzia talos, a jej reputacja jest korzystna.



Obraz 9.10.1 raport dotyczący domeny wygenerowany przez talosintelligence.com, data wykonania zrzutu 17.1.2024 r.

Analiza nagłówków http strony www.faceit.com widoczna na obrazach 9.11.1-9.11.3 nie wykazała krytycznych uchybień od normy.



Obraz 9.11.1 sprawdzenie nagłówka, źródło securityheaders.com, data wykonania zrzutu 13.12.2023 r.

Raw Headers

HTTP/2	200
date	Wed, 13 Dec 2023 18:53:22 GMT
content-type	text/html
last-modified	Wed, 13 Dec 2023 13:29:53 GMT
vary	Accept-Encoding
x-frame-options	SAMEORIGIN
x-content-type-options	nosniff
content-security-policy	frame-ancestors *'self'* https://*.faceit.com:*
x-envoy-upstream-service-time	0
via	1.1 google
alt-svc	h3=":443"; ma=86400
cf-cache-status	DYNAMIC
set-cookie	__cf_bm=PwEnu7D5S07vfMcV.mh_hi8uNkdWe5srcbEQ_sDsXdE-1702493602-1-AeFrG/I1Z1Ol6y5r5BvlWBU9K3osg9IfvwIcKZYsfivkfZGjTT5fc+U9W7fstl1e3T/lh3K5VRm1M2Z3qrP2mLqE0h8uOIN0Ckexp2hrf9QQ; path=/; expires=Wed, 13-Dec-23 19:23:22 GMT; domain=.faceit.com; **HttpOnly**; **Secure**; **SameSite**=None
set-cookie	_cfuvid=3URoOD8t59xBVmbdKtGdYdCLNC5E2e2XlYp3KwMZpNo-1702493602856-0-604800000; path=/; domain=.faceit.com; **HttpOnly**; **Secure**; **SameSite**=None
server	cloudflare
cf-ray	835068d93a0dfa9e-SJC
content-encoding	gzip

Upcoming Headers

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Obraz 9.12.2 sprawdzenie nagłówka, źródło securityheaders.com, data wykonania zrzutu 13.12.2023 r.

Additional Information

x-frame-options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking.
x-content-type-options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
content-security-policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. Analyse this policy in more detail. You can sign up for a free account on Report URI to collect reports about problems on your site.
server	Server value has been changed. Typically you will see values like "Microsoft-IIS/8.0" or "nginx 1.7.2".

Obraz 9.12.3 sprawdzenie nagłówka, źródło securityheaders.com, data wykonania zrzutu 13.12.2023 r.

Podatności dla hosta gwb.faceit.com zostały przedstawione na obrazach 9.13.1, 9.13.2. Znalezione podatności dotyczą wyłącznie języka PHP. Nie znaleziono wersji PHP z której korzysta gwb.faceit.com, zatem nie można stwierdzić, czy te podatności mogą zostać wykorzystane.

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2022-31629	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications.
CVE-2022-31628	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.
CVE-2019-9641	7.5 An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.

Obraz 9.13.1 podatności dla hosta gwb.faceit.com, źródło shodan.io, data wykonania zrzutu 07.02.2024 r.

CVE-2015-4603	10.0 The exception::getTraceAsString function in Zend/zend_exceptions.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to execute arbitrary code via an unexpected data type, related to a "type confusion" issue.
CVE-2015-4602	10.0 The __PHP_Incomplete_Class function in ext/standard/incomplete_class.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.
CVE-2015-4601	10.0 PHP before 5.6.7 might allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in (1) ext/soap/php_encoding.c, (2) ext/soap/php_http.c, and (3) ext/soap/soap.c, a different issue than CVE-2015-4600.
CVE-2015-4600	10.0 The SoapClient implementation in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in the (1) SoapClient::__getLastRequest, (2) SoapClient::__getLastResponse, (3) SoapClient::__getLastRequestHeaders, (4) SoapClient::__getLastResponseHeaders, (5) SoapClient::__getCookies, and (6) SoapClient::__setCookie methods.
CVE-2015-4599	10.0 The SoapFault::__toString method in ext/soap/soap.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information, cause a denial of service (application crash), or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

Obraz 9.13.2 podatności dla hosta gwb.faceit.com, źródło shodan.io, data wykonania zrzutu 07.02.2024 r.

Podatności dla hosta telekom-survey.faceit.com dotyczące protokołu ALPACA (może zostać wykorzystane na serwerze nginx v1.18.0), HTTP/2, i serwera nginx (podatność przedstawiona na obrazie 9.13.4) zostały przedstawione na obrazie 9.13.3.

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

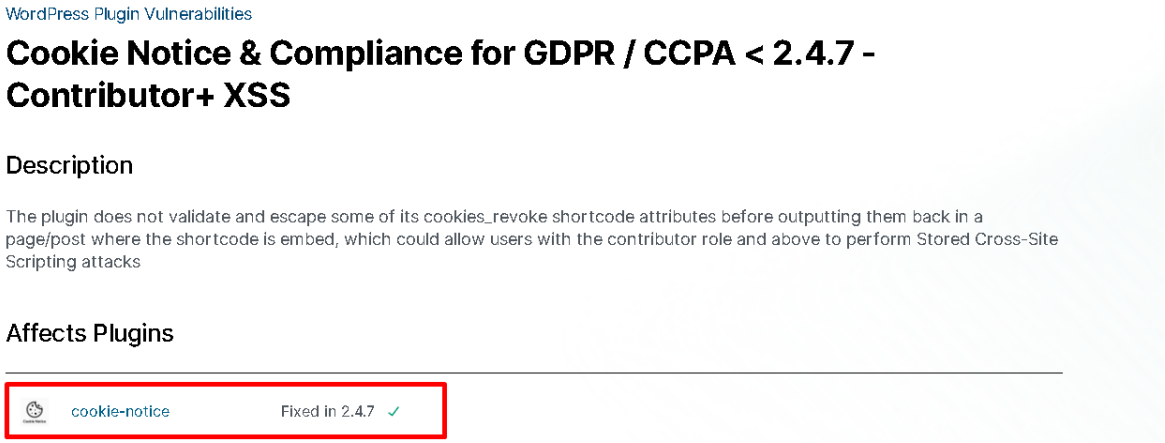
CVE-2023-44487	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.
CVE-2021-3618	5.8 ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.
CVE-2021-23017	6.8 A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

Obraz 9.13.3 podatności dla hosta telekom-survey.faceit.com, źródło shodan.io

Znaleziono podatność (umożliwiającą przeprowadzenie ataku DOS) dla serwera nginx w wersji 1.18.0 (dla hosta telekom-survey.faceit.com).

Obraz 9.13.4 podatności dla Nginx 1.18.0, źródło exploit-db.com, data wykonania zrzutu 07.02.2024 r.

Nie znaleziono podatności pluginu Wordpress Cookie Notice w wersji 2.4.10 (dla hosta corporate.faceit.com). Ostatnia podatność została wykryta dla wersji 2.4.7 – obraz 9.14.1.



Obraz 9.14.1 podatności dla pluginu wordpress – cookie notice, źródło wpscan.com, data wykonania zrzutu 07.02.2024 r.

Dla Wordpress w wersji 5.6.13 (dla hosta gwb.faceit.com) znaleziono 1 niezałataną podatność – obraz 9.14.3. Dla Wordpress w wersji 6.4.3 (dla hosta r6collegiate.faceit.com) nie znaleziono podatności – obraz 9.14.2.

WordPress 6.4 Vulnerabilities

Version released on 2023-11-07

↓ Download tar

↓ Download zip

Published	Title	Fixed in	CVSS
2024-01-30	WordPress < 6.4.3 - Deserialization of Untrusted Data	✓ Fixed in 6.4.3	8.5 (high)
2024-01-30	WordPress < 6.4.3 - Admin+ PHP File Upload	✓ Fixed in 6.4.3	6.6 (medium)
2023-12-06	WP 6.4-6.4.1 - POP Chain	✓ Fixed in 6.4.2	8.1 (high)

Obraz 9.14.2 podatności dla wordpress, źródło wpscan.com, data wykonania zrzutu 07.02.2024 r.

WordPress Vulnerabilities

WP <= 6.2 - Unauthenticated Blind SSRF via DNS Rebinding

Description

WordPress is affected by an unauthenticated blind SSRF in the pingback feature. Because of a TOCTOU race condition between the validation checks and the HTTP request, attackers can reach internal hosts that are explicitly forbidden.

Proof of Concept

```
https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/
```

Affects WordPress

6.1.1	No known fix ✕
6.1	No known fix ✕
4.1.37	No known fix ✕
4.1.36	No known fix ✕
4.1.35	No known fix ✕
4.1.34	No known fix ✕

Obraz 9.14.3 podatność dla wordpress, źródło wpscan.com, data wykonania zrzutu 07.02.2024 r.

Znaleziono podatności (umożliwiające przeprowadzenie ataku DOS) dla serwera Apache w wersji 2.4.56 (dla hosta cdn.faceit.com), co przedstawiono na obrazach 9.14.4, 9.14.5.

BUG Apache2, 2.4.56, is vulnerable to CVE-2023-31112, CVE-2023-43622 and CVE-2023-45802

rejected #51281: Utworzony przez Knight Chang. Ostatnia aktualizacja 20.12.2023 09:55. Assign to me DZIAŁANIE PLIKI RELACJE (1)

The version of Apache httpd installed on the remote host is prior to 2.4.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.58 advisory.

- mod_macro buffer over-read: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57. Acknowledgements: finder: David Shoon (github/davidshoon) (CVE-2023-31122)

- Apache HTTP Server: DoS in HTTP/2 with initial windows size 0: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known slow loris attack pattern. This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57. Users are recommended to upgrade to version 2.4.58, which fixes the issue.
Acknowledgements: (CVE-2023-43622)

- Apache HTTP Server: HTTP/2 stream memory not redaimed right away on RST: When a HTTP/2 stream was reset (RST frame) by a dient, there was a time window were the request's memory resources were not redaimed immediately. Instead, de-allocation was deferred to connection dose. A dient could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection dose, all resources were redaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test dient. During normal HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection doses or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.
Acknowledgements: (CVE-2023-45802)

Obraz 9.14.4 podatności dla Apache 2.4.56, źródło community.openproject.org, data wykonania zrzutu 07.02.2024 r.

low: Apache HTTP Server: DoS in HTTP/2 with initial windows size 0 (CVE-2023-43622)

An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern.

This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout.

This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57.

Users are recommended to upgrade to version 2.4.58, which fixes the issue.

Acknowledgements:

- finder: Prof. Sven Dietrich (City University of New York)
- finder: Isa Jafarov (City University of New York)
- finder: Prof. Heejo Lee (Korea University)
- finder: Choongin Lee (Korea University)

Reported to security team	2023-09-15
Update 2.4.58 released	2023-10-19
Affects	<=2.4.57

Obraz 9.14.5 podatności dla Apache 2.4.56, źródło httpd.apache.org, data wykonania zrzutu 07.02.2024 r.

Znaleziono 1 niezałataną podatność (umożliwiającą przeprowadzenie ataku MitM) dla OpenSHH w wersji 8.2p1 (dla hosta telekom-survey.faceit.com), co przedstawiono na obrazach 9.14.6, 9.14.7

Vulnerabilities in OpenSSH 8.2p1

Multiple vulnerabilities in OpenSSH 19 Dec, 2023
Medium Patched

Remote code execution in OpenSSH ssh-agent 20 Jul, 2023
Medium Patched

Multiple vulnerabilities in OpenSSH 04 Oct, 2022
Low Patched

Amazon Linux AMI update for openssh 19 Feb, 2022
Low Patched

Privilege escalation in OpenSSH 26 Sep, 2021
Low Patched

Remote code execution in OpenSSH client 14 Mar, 2021
Medium Patched

MitM attack in OpenSSH client 30 Jul, 2020
Medium Not Patched

Security restrictions bypass in OpenSSH 27 May, 2020
Low Patched

Obraz 9.14.6 podatności dla OpenSSH 8.2p1, źródło cybersecurity-help.cz, data wykonania zrzutu 07.02.2024 r.

Openbsd » Openssh » 8.2 : Security Vulnerabilities, CVEs,

cpe:2.3:a:openbsd:openssh:8.2:*:*:*:*:*:*:*

Published in: ≡ 2024 January February

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

Copy

CVE-2023-38408

The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

Max CVSS	9.8
Published	2023-07-20
Updated	2023-12-22
EPSS	3.00%

CVE-2020-15778

** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

Max CVSS	7.8
Published	2020-07-24
Updated	2023-02-24
EPSS	0.29%

CVE-2020-12062

** DISPUTED ** The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the

Max CVSS	7.5
Published	2020-06-01
Updated	2020-06-04
EPSS	0.11%

Obraz 9.14.7 podatności dla OpenSSH 8.2p1, źródło cvedetails.com, data wykonania zrzutu 07.02.2024 r.

Znaleziono podatności (umożliwiające przeprowadzenie ataku DOS) dla serwera MySQL w wersji 8.0.35 (dla hosta cdn.faceit.com), co zostało zaznaczone na obrazach 9.15.1-9.15.3.

Vulnerability Details : CVE-2024-20985

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Published 2024-01-16 22:15:45 Updated 2024-02-02 17:27:12 Source Oracle

View at NVD, CVE.org

Vulnerability category: Denial of service

Exploit prediction scoring system (EPSS) score for CVE-2024-20985

Probability of exploitation activity in the next 30 days: 0.04%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 11 % EPSS Score History EPSS FAQ

CVSS scores for CVE-2024-20985

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	2.8	3.6	secalert_us@oracle.com

Obraz 9.15.1 podatności dla MySQL wersja 8.0.35, źródło cvedetails.com, data wykonania zrzutu 09.02.2024 r.

Vulnerability Details : CVE-2024-20973

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Published 2024-01-16 22:15:44 Updated 2024-02-02 17:22:05 Source Oracle

View at NVD, CVE.org

Vulnerability category: Denial of service

Exploit prediction scoring system (EPSS) score for CVE-2024-20973

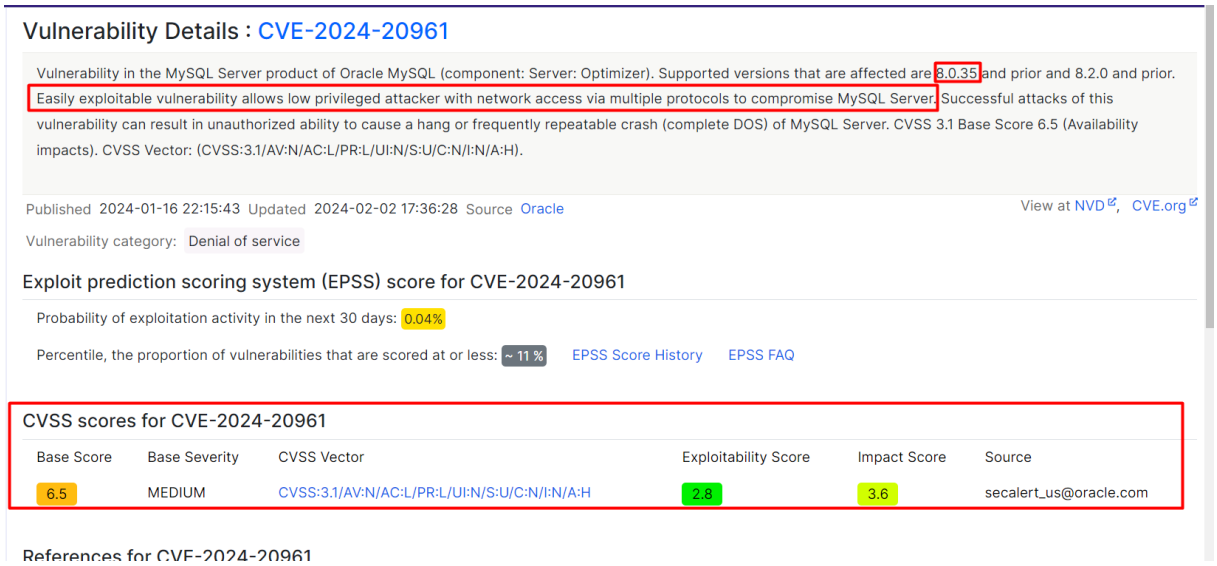
Probability of exploitation activity in the next 30 days: 0.04%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 11 % EPSS Score History EPSS FAQ

CVSS scores for CVE-2024-20973

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	2.8	3.6	secalert_us@oracle.com

Obraz 9.15.2 podatności dla MySQL wersja 8.0.35, źródło cvedetails.com, data wykonania zrzutu 09.02.2024 r.



Vulnerability Details : CVE-2024-20961

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Published 2024-01-16 22:15:43 Updated 2024-02-02 17:36:28 Source Oracle

View at NVD, CVE.org

Vulnerability category: Denial of service

Exploit prediction scoring system (EPSS) score for CVE-2024-20961

Probability of exploitation activity in the next 30 days: 0.04%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 11 % EPSS Score History EPSS FAQ

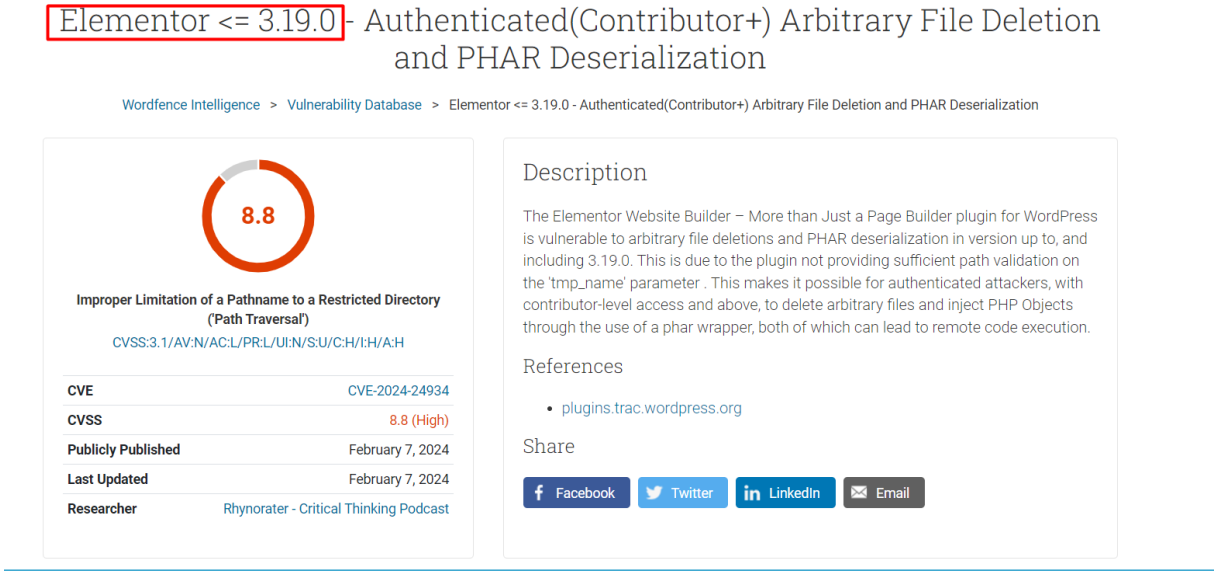
CVSS scores for CVE-2024-20961

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	2.8	3.6	secalert_us@oracle.com

References for CVE-2024-20961

Obraz 9.15.3 podatności dla MySQL wersja 8.0.35, źródło cvedetails.com, data wykonania zrzutu 09.02.2024 r.

Nie znaleziono podatności dla wersji 3.19.1 (dla hosta ads.faceit.com) pluginu Elementor. Ostatnia podatność została opublikowana 7 lutego 2024 r., co zaprezentowano na obrazie 9.16.1.



Elementor <= 3.19.0 - Authenticated(Contributor+) Arbitrary File Deletion and PHAR Deserialization

Wordfence Intelligence > Vulnerability Database > Elementor <= 3.19.0 - Authenticated(Contributor+) Arbitrary File Deletion and PHAR Deserialization

8.8

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE	CVE-2024-24934
CVSS	8.8 (High)
Publicly Published	February 7, 2024
Last Updated	February 7, 2024
Researcher	Rhynorater - Critical Thinking Podcast

Description

The Elementor Website Builder – More than Just a Page Builder plugin for WordPress is vulnerable to arbitrary file deletions and PHAR deserialization in version up to, and including 3.19.0. This is due to the plugin not providing sufficient path validation on the 'tmp_name' parameter . This makes it possible for authenticated attackers, with contributor-level access and above, to delete arbitrary files and inject PHP Objects through the use of a phar wrapper, both of which can lead to remote code execution.

References

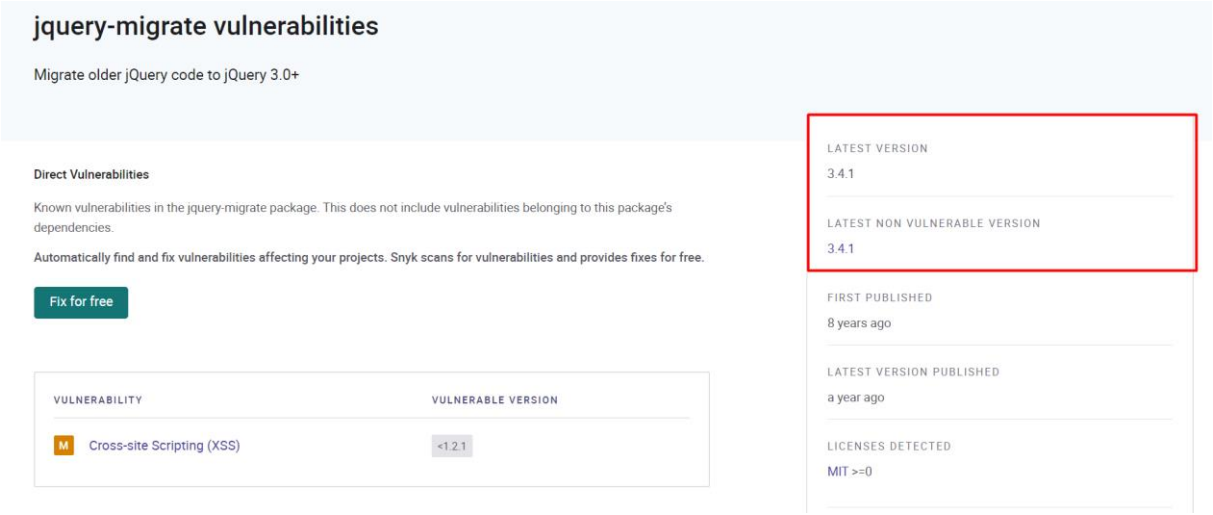
- plugins.trac.wordpress.org

Share

Facebook Twitter LinkedIn Email

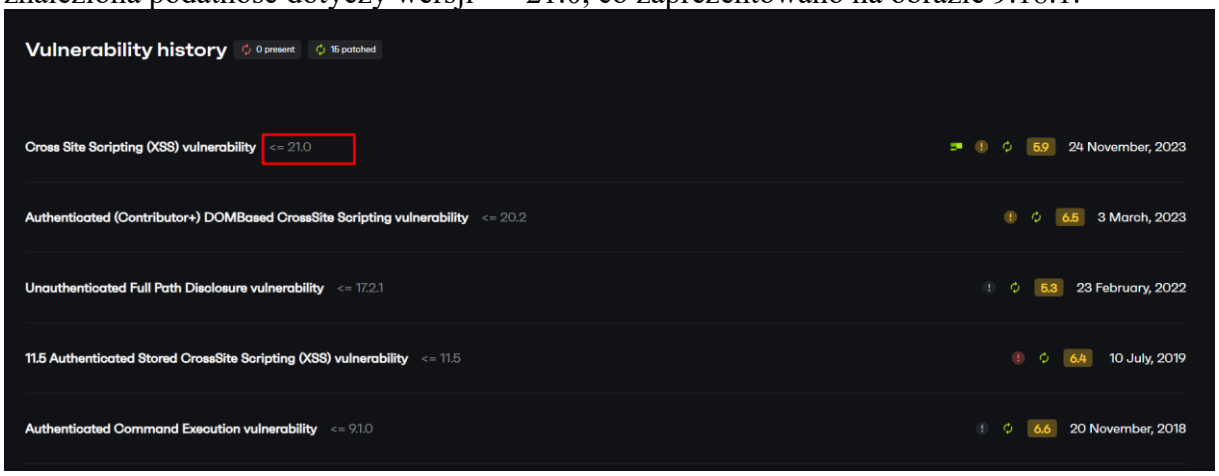
Obraz 9.16.1 podatność dla pluginu Elementor, źródło wordfence.com, data wykonania zrzutu 09.02.2024 r.

Nie znaleziono podatności dla jQuery-migrate w wersji 3.4.1 (dla stron ads.faceit.com, pro.faceit.com, corporate.faceit.com) na dzień 09.02.2024 r., co zaprezentowano na obrazie 9.17.1.



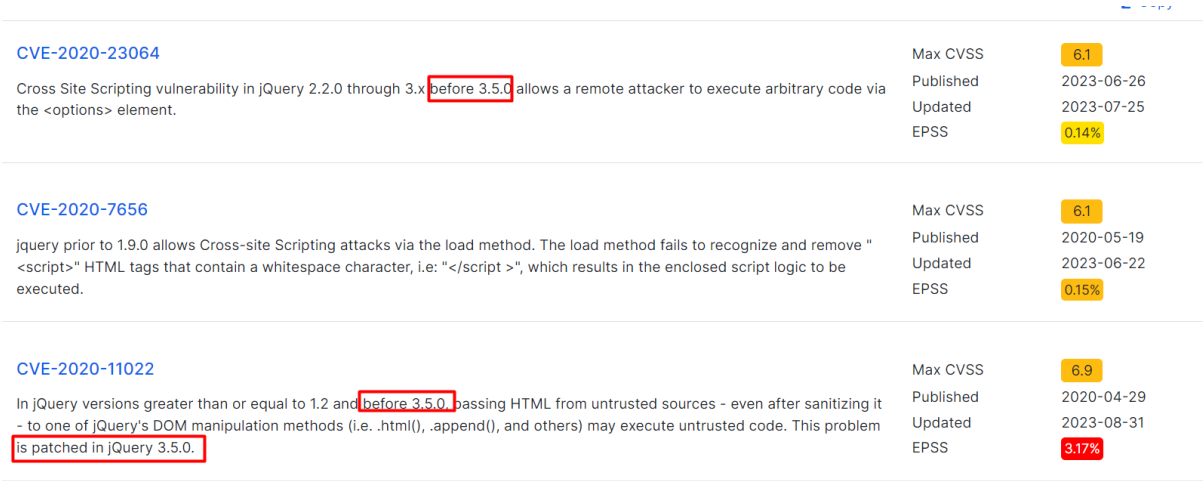
Obraz 9.17.1 podatność dla jQuery-migrate, źródło security.snyk.io, data wykonania zrzutu 09.02.2024r.

Nie znaleziono podatności dla Yoast Seo (dla strony pro.faceit.com) w wersji 21.7. Ostatnia znaleziona podatność dotyczy wersji <= 21.0, co zaprezentowano na obrazie 9.18.1.



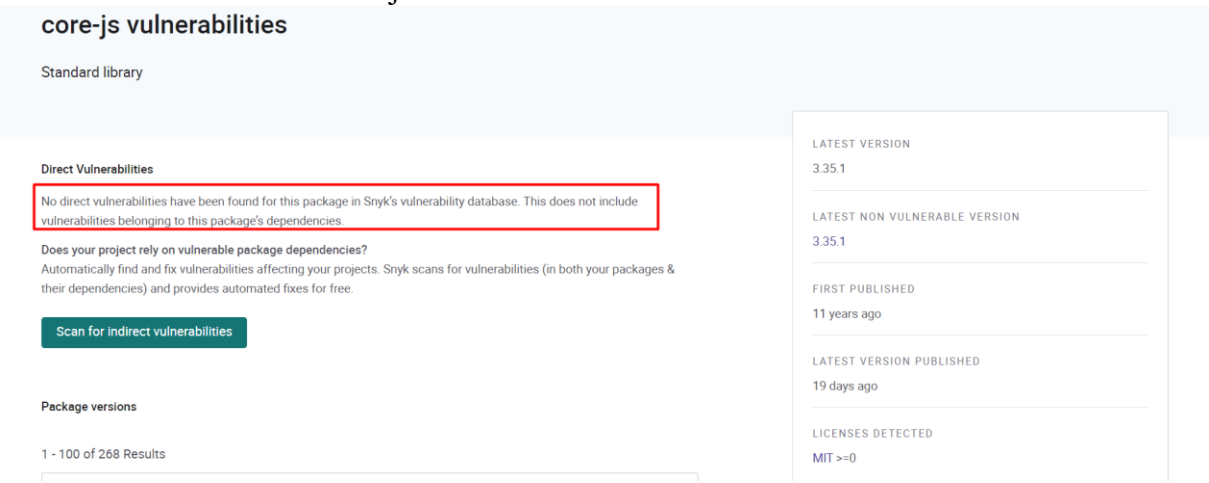
Obraz 9.18.1 podatność dla Yoast SEO, źródło patchstack.com, data wykonania zrzutu 09.02.2024 r.

Nie znaleziono podatności dla jQuery w wersji 3.5.1 (dla stron faceit.com i suport.faceit.com) ani dla wersji 3.7.1 (dla strony corporate.faceit.com). Ostatnie znaleziono podatności dotyczą wersji < 3.5.0, co zaprezentowano na obrazie 9.20.1.



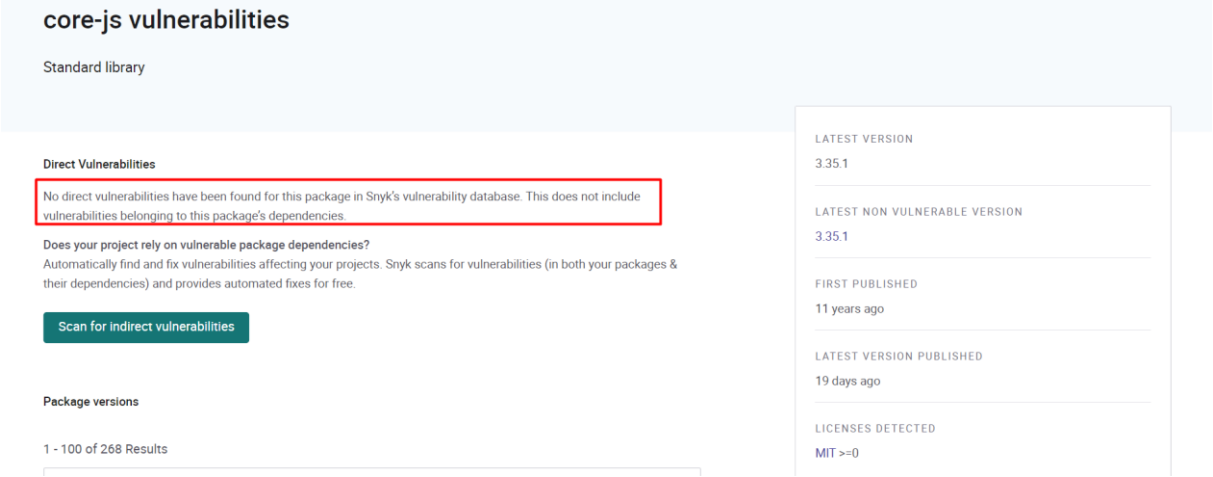
Obraz 9.20.1 podatność dla jQuery, źródło cvedetails.com, data wykonania zrzutu 09.02.2024 r.

Nie znaleziono podatności dla core-js w wersji 3.27.0 (dla stron faceit.com i suport.faceit.com), a także dla wersji 2.6.12 (dla strony developers.faceit.com) na co wskazuje Obraz 9.21.1. Należałoby jednak użyć nowej wersji core-js, ponieważ wersja 3.27.0 core-js została opublikowana w grudniu 2022 roku, a najnowsza wersja została opublikowana w styczniu 2024 roku i nie doszło do aktualizacji.



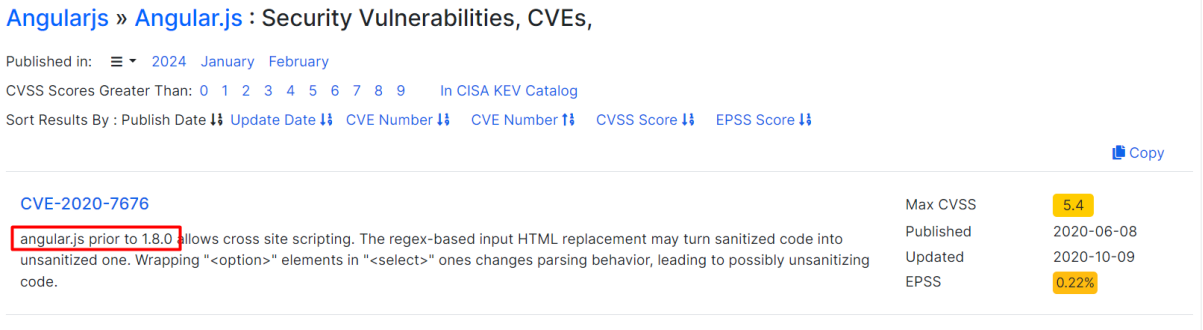
Obraz 9.21.1 podatność dla core-js, źródło security.snyk.io, data wykonania zrzutu 09.02.2024 r.

Nie znaleziono podatności dla core-js w wersji 3.30.2 (dla strony blog.faceit.com), co pokazano na obrazie 9.22.1). Należałoby jednak użyć nowej wersji core-js, ponieważ wersja 3.30.2 core-js została opublikowana w maju 2023 roku, a najnowsza wersja została opublikowana w styczniu 2024 roku i nie doszło do aktualizacji.



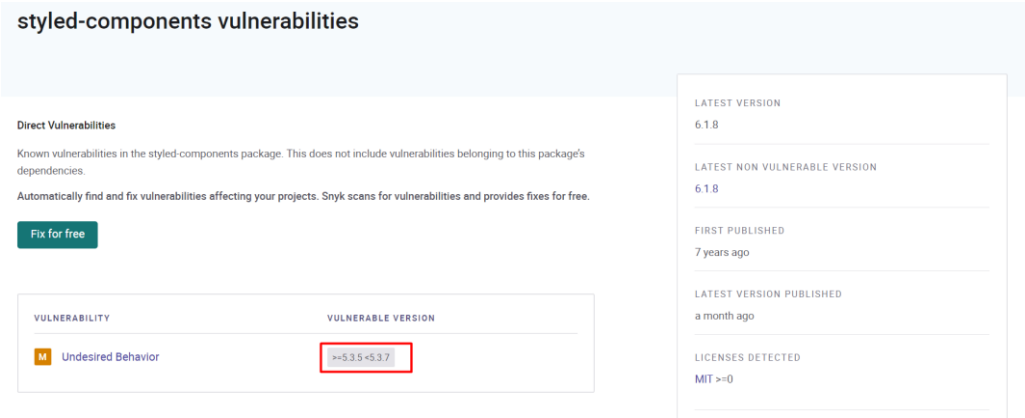
Obraz 9.22.1 podatność dla core-js, źródło security.snyk.io, data wykonania zrzutu 09.02.2024 r.

Nie znaleziono podatności dla Angular (dla hosta faceit.com) w wersji 1.8.0. Ostatnia znaleziona podatność dotyczy wersji < 1.8.0, co zaprezentowano na obrazie 9.23.1.



Obraz 9.23.1 podatność dla Angular, źródło cvedetails.com, data wykonania zrzutu 09.02.2024 r.

Nie znaleziono podatności dla styled-components (dla hosta faceit.com) w wersji 5.3.8. Ostatnia znaleziona podatność dotyczy wersji < 5.3.7, co zaprezentowano na obrazie 9.24.1. Należałoby jednak użyć nowej wersji styled-components, ponieważ wersja 5.3.8 styled-components została opublikowana w marcu 2023 roku, a najnowsza wersja została opublikowana w styczniu 2024 roku i nie doszło do aktualizacji.



Obraz 9.24.1 podatność dla styled-components, źródło security.snyk.io, data wykonania zrzutu 09.02.2024 r.

Nie znaleziono podatności dla Lodash (dla strony faceit.com) w wersji 4.17.21. Ostatnia znaleziona podatność dotyczy wersji < 4.17.21, co zaprezentowano na obrazie 9.25.1.

Obraz 9.25.1 podatność dla Lodash, źródło cvedetails.com, data wykonania zrzutu 09.02.2024 r.

Nie znaleziono podatności dla ZURB Foundation (dla strony corporate.faceit.com) w wersji 6.7.4. Ostatnia znaleziono podatność obejmuje wersję do 5.5.3, co zaprezentowano na obrazie 9.26.1.

Obraz 9.26.1 podatność dla ZURB Foundation, źródło vuldb.com, data wykonania zrzutu 09.02.2024 r.

POLITYKA PRYWATNOŚCI(TAJNOŚCI) [wybrane elementy], oparta na informacjach dostępnych na stronie faceit.com (przykładowy obraz 9.13.1).

Przetwarzane dane

- Adres email
- Data urodzenia
- Imię i nazwisko
- Stały adres zamieszkania
- Numer telefonu
- Dane karty kredytowej lub inne dane dotyczące płatności

Przy rejestracji/logowaniu do usług online, zbierane są następujące informacje:

- Rodzaj używanego urządzenia;
- Adres IP;
- Szczegóły geolokalizacji, w tym region, kraj, stan, miasto;
- rodzaj używanej przeglądarki;

Gromadzone dane osobowe, obejmują:

- Adres IP i MAC;
- Dostawca usług internetowych;
- Identyfikator konsoli;
- System operacyjny i wersja urządzenia;
- Marka, marka i model urządzenia;
- Typ, wersja i język przeglądarki;

Dane mogą być udostępnianie stronom trzecim wyłącznie w sposób opisany w niniejszej Polityce prywatności:

- Członkom grupy, personelowi, dostawcom lub podwykonawcom.
- W przypadku fuzji lub przejęcia. Jeśli dojdzie do fuzji, przejęcia lub sprzedaży całości lub części jej aktywów, zostaną wysłane wiadomości do konta.

W wiadomościach z poczty elektronicznej z 2022 r. nie znalazły się informacje o przejęciu/fuzji co było wymagane i jawnie napisane w polityce prywatności.

2. INFORMATION WE MAY COLLECT ABOUT YOU

We collect and process the following information which may include your personal data.

Information provided when you register with our Online Services

("Registration Information")

In order to access restricted sections of the Website and install a Client, you are required to providing the following information:

- Username;
- Email;
- Password;
- Country;
- Date of birth;
- First Name; and
- Last Name.

Obraz 9.13.1 polityka prywatności faceit.com, data wykonania zrzutu 17.12.2023 r.

W zbieraniu danych do rozdziału 9 skorzystano ze stron takich jak faceit.com, vuldb.com, cvedetails.com, security.snyk.io, patchstack.com, wordfence.com, cybersecurity-help.cz, httpd.apache.org, community.openproject.org, exploit-db.com, wpscan.com, shodan.io, securityheaders.com, talosintelligence.com, scanner.pcrisk.com, sitecheck.sucuri.net, lookup.abusix.com, easydmarc.com, mxtoolbox.com, dnsdbl.com, sca.analysiscenter.veracode, aplikacja XCA. Technologie takie jak WordPress, Styled-Components, Angular, core-js, jQuery, Yoast Seo, jQuery-migrate, usługi MySQL, nginx, OpenSSH, Apache, PHP nie zostały zaktualizowane do najnowszych wersji na dzień 10.02.2024 r. Technologie Elementor, Cookie Notice zostały zaktualizowane do najnowszych wersji na dzień 10.02.2024 r. Według baz danych spamu domena faceit.com nie znajduje się

na żadnej z czarnych list. Znaleziono podatności dla wykorzystywanych wersji serwera nginx, Apache, MySQL, OpenSSH, WordPress, PHP.

10.Stosowane urządzenia sieciowe

ESL FACEIT GROUP

WHO WE ARE BRANDS PARTNERS AD SOLUTIONS CAREER PRESS

At **EFG (ESL FACEIT Group)** we create worlds beyond gameplay, where players and fans become a community. We pride ourselves in having a corporate social responsibility which is that "IT'S NOT GG, UNTIL IT'S GG FOR ALL". Our passion, craft, and DNA are aligned to create and shape the world of esports, gaming tournaments, leagues, events, and holistic ecosystems through our millions of players, fans, and heroes, as well as through our people, and culture.

We are looking for a **Senior SAP Public Cloud Administrator** of the Finance and Controlling module of SAP S/4HANA Public Cloud who will be responsible in the Technology team for the efficient administration, optimization, and stability of our SAP landscape.

The primary purpose of the role is to leverage expertise in SAP S/4HANA Public Cloud to configure, maintain, troubleshoot, and support the organization's financial processes. This role plays a key part in enhancing the systems adoption, security, and compliance, ultimately contributing to the seamless operation of our SAP environment and enabling effective business processes within the Finance domain.

**Please note that we are happy to support remote work arrangements, fostering a collaborative and inclusive environment that values the diverse talents of our team members, regardless of their physical location.*

What will you do:

- Provide technical support for the SAP S/4 Hana public cloud modules, including troubleshooting and issue resolution for both end-users and technical team members.
- Support (manual) Interface of Business Partner (Update/Create Finance Master Data) – 1st Level
- Interpretation of finance data flows via CPI / BTP APIs
- Support the implementation or optimization of new features in the area of CPI-Integration (e.g. AP Down Payment Process, Amazon, etc.)
- Work closely with end-users and other stakeholders to understand and address their Finance related needs. This includes providing recommendations to improve the SAP S/4 Hana public cloud modules process and identifying areas for system optimization.
- Provide support for SAP S/4 Hana public cloud module-related requests, including assistance with user account management, system access, and defect resolution.
- Work with technical team members to identify and prioritize requests for system enhancements.
- Manage and maintain SAP S/4 Hana public cloud modules applications, including configuration and customization of the applications to meet the needs of the business.
- Collaborate with cross-functional teams to support program delivery efforts, including testing, training, and documentation. This includes working with the technical team to ensure that SAP S/4 Hana public cloud modules are properly integrated with other enterprise systems.
- Develop and maintain technical documentation related to SAP S/4 Hana public cloud modules. This includes creating functional specification documents and system documentation.
- Stay up to date with industry trends and best practices related to SAP S/4 Hana public cloud modules. This includes attending training sessions and conferences, as well as participating in professional development opportunities

Obraz 10.1.1 oferty pracy ESL FACEIT GROUP, źródło eslfaceutgroup.com, data wykonania zrzutu 10.12.2023 r.

ESL FACEIT GROUP

WHO WE ARE BRANDS PARTNERS AD SOLUTIONS CAREER PRESS

- Provide support for SAP S/4 Hana public cloud module-related requests, including assistance with user account management, system access, and defect resolution.
- Work with technical team members to identify and prioritize requests for system enhancements.
- Manage and maintain SAP S/4 Hana public cloud modules applications, including configuration and customization of the applications to meet the needs of the business.
- Collaborate with cross-functional teams to support program delivery efforts, including testing, training, and documentation. This includes working with the technical team to ensure that SAP S/4 Hana public cloud modules are properly integrated with other enterprise systems.
- Develop and maintain technical documentation related to SAP S/4 Hana public cloud modules. This includes creating functional specification documents and system documentation.
- Stay up to date with industry trends and best practices related to SAP S/4 Hana public cloud modules. This includes attending training sessions and conferences, as well as participating in professional development opportunities

REQUIREMENTS:

What you will need:

- Minimum of 5 years of experience as an SAP Administrator, with a focus on the Finance and Controlling Module.
- Experience in SAP S/4HANA Public Cloud administration.
- Experience with SAP Business Technology Platform (BTP)
- Experience in integrating different Business Cloud Solutions (Coupa, Salesforce) with SAP
- Strong knowledge of SAP Finance and Controlling business processes.
- Experience in system configuration, optimization, and performance tuning.
- Solid understanding of SAP security principles and best practices.
- Knowledge of integration with other SAP modules and third-party systems.
- Familiar with Python as a programming language
- A basic understanding of BPMN

Firmly rooted in our values, EFG is an affirmative action employer that celebrates being an equal-opportunity workplace. Our unwavering commitment to fair employment extends to all individuals, regardless of their race, color, ancestry, religion, sex, national origin, age, sexual orientation, disability, citizenship, marital status, gender identity, or Veteran status.

APPLY NOW

Obraz 10.1.2 oferty pracy ESL FACEIT GROUP, źródło eslfaceutgroup.com, data wykonania zrzutu 10.12.2023 r.

S/4HANA (Solution) Consultant...
ESL FACEIT Group - EFG · Londyn, An...

Łatwe aplikowanie | Zapisz | •••

What will you do:

- Provide technical support for the SAP S/4 Hana public cloud modules, including troubleshooting and issue resolution for both end-users and technical team members.
- Support (manual) Interface of Business Partner (Update/Create Finance Master Data) - 1st Level
- Interpretation of finance data flows via CPI / BTP APIs
- Support the implementation or optimization of new features in the area of CPI-Integration (e.g. AP Down Payment Process, Amazon, etc.)
- Work closely with end-users and other stakeholders to understand and address their Finance related needs. This includes providing recommendations to improve the SAP S/4 Hana public cloud modules process and identifying areas for system optimization.
- Provide support for SAP S/4 Hana public cloud module-related requests, including assistance with user account management, system access, and defect resolution.
- Work with technical team members to identify and prioritize requests for system enhancements.
- Manage and maintain SAP S/4 Hana public cloud modules applications, including configuration and customization of the applications to meet the needs of the business.
- Collaborate with cross-functional teams to support program delivery efforts, including testing, training, and documentation. This includes working with the technical team to ensure that SAP S/4 Hana public cloud modules are properly integrated with other enterprise systems.
- Develop and maintain technical documentation related to SAP S/4 Hana public cloud modules. This includes creating functional specification documents and system documentation.
- Stay up to date with industry trends and best practices related to SAP S/4 Hana public cloud modules. This includes attending training sessions and conferences, as well as participating in professional development opportunities

Obraz 10.1.3 oferty pracy ESL FACEIT GROUP, źródło linkedin.com, data wykonania zrzutu 10.12.2023 r.

S/4HANA (Solution) Consultant...
ESL FACEIT Group - EFG · Londyn, An...
Łatwe aplikowanie Zapisz •••

Requirements

What you will need:

- Minimum of 5 years of experience as an SAP Administrator, with a focus on the Finance and Controlling Module.
- Experience in SAP S/4HANA Public Cloud administration.
- Experience with SAP Business Technology Platform (BTP)
- Experience in integrating different Business Cloud Solutions (Coupa, Salesforce) with SAP
- Strong knowledge of SAP Finance and Controlling business processes.
- Experience in system configuration, optimization, and performance tuning.
- Solid understanding of SAP security principles and best practices.
- Knowledge of integration with other SAP modules and third-party systems.
- Familiar with Python as a programming language
- A basic understanding of BPMN

Firmly rooted in our values, EFG is an affirmative action employer that celebrates being an equal-opportunity workplace. Our unwavering commitment to fair employment extends to all individuals, regardless of their race, color, ancestry, religion, sex, national origin, age, sexual orientation, disability, citizenship, marital status, gender identity, or Veteran status.

Obraz 10.1.4 oferty pracy ESL FACEIT GROUP, źródło linkedin.com, data wykonania zrzutu 10.12.2023 r.

W zbieraniu danych do rozdziału 10 skorzystano z narzędzi takich jak linkedin.com, eslfaceutgroup.com. które przedstawiono na obrazach 10.1.1-10.1.4. Nie znaleziono modelów, producentów używanych urządzeń sieciowych. Domena korzysta z chmury do świadczenia usług – Amazon(Amazon AWS) i Cloudflare(Cloudflare) co zostało wskazane na obrazach w rozdziale 6 na obrazach 6.1.1-6.1.4.

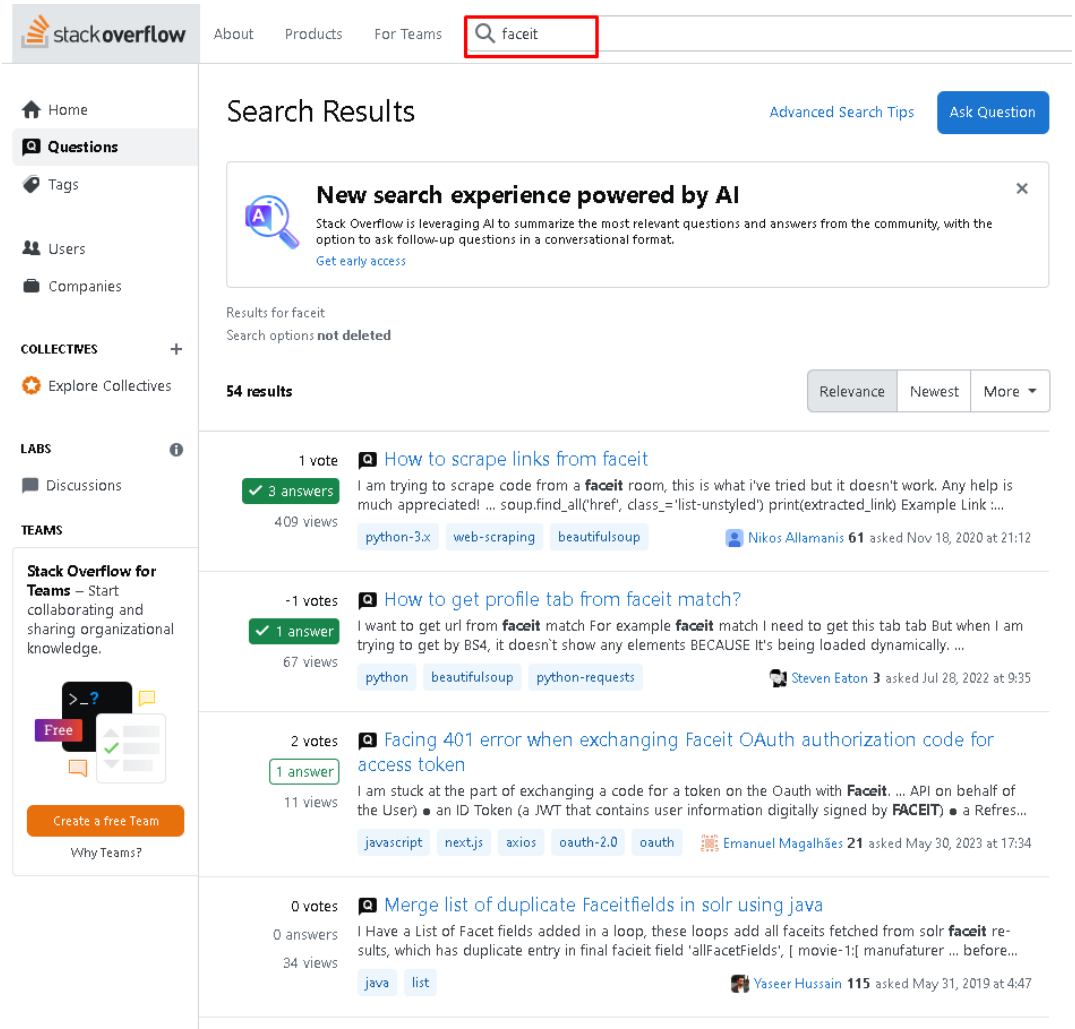
11.Inne rodzaje uzyskanych danych

Analiza kodu źródłowego nie wykazała znaczących informacji z zakresu danych kontaktowych do programistów. Jedyna interesująca informacja to skrypty wykorzystywane na stronie widoczne na obrazie 11.1.1.

```
Elementy  Konsola  Rejestrator  Statystyki wydajności  Źródła  Sieć  Wydajność  Pamięć  Aplikacja
<meta name="fragment" content="!">
<meta name="viewport" content="width=device-width,initial-scale=1">
<link rel="preconnect" href="https://api.faceit.com">
<link rel="preconnect" href="https://cdn.faceit.com">
<link rel="manifest" href="/manifest.json">
<script async src="https://www.googletagmanager.com/gtm.js?id=GTM-MMCLV43" id="gtm-js"></script>
<script src="https://connect.facebook.net/en_US/sdk.js?hash=696bf9b…" async crossorigin="anonymous"></script>
<script async src="https://connect.facebook.net/en_US/fbevents.js" id="metaPixel"></script>
<script async src="//securepubads.g.doubleclick.net/tag/js/gpt.js"></script>
<script async src="//imasdk.googleapis.com/js/sdkloader/ima3.js"></script>
<script>window.prerenderReady=!1</script>
<script>window.faceit={buildVersion:"1737-1704907063",appVersion:"f22be5c"}</script>
<script type="text/javascript">var _sf_startpt=(new Date).getTime()</script>
<link rel="shortcut icon" href="favicon.ico">
```

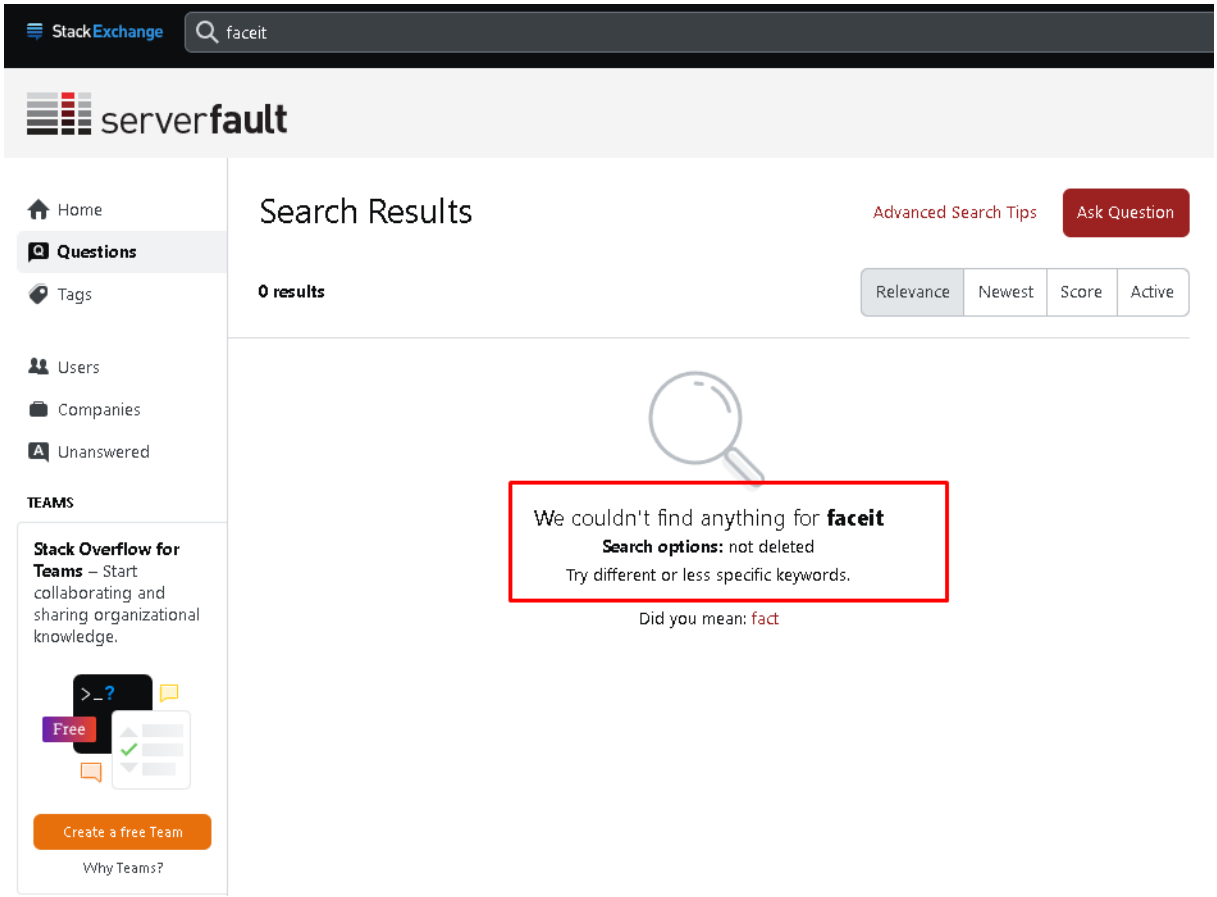
Obraz 11.1.1 wykorzystywane skrypty na stronie faceit.com, data wykonania zrzutu 11.1.2024 r.

Żaden 54 wyników zapytania na stronie stackoverflow widocznych na obrazie 11.2.1 nie zawiera informacji, który mają istotne znaczenie dla rekonesansu. Zwykle były to odwołania do Faceit Development Kit.

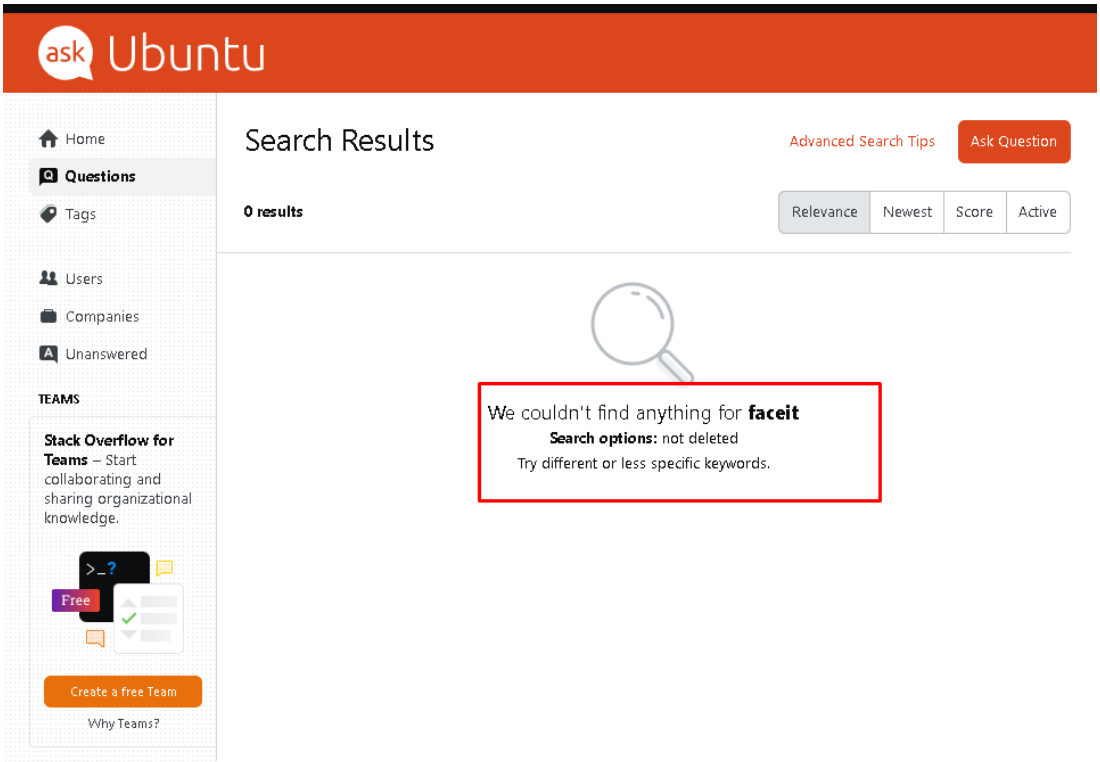


Obraz 11.2.1 rezultat wyszukania frazy faceit na stackoverflow.com, data wykonania zrzutu 11.1.2024r.

Przeglądając fora dyskusyjne – serverfault, ubuntuask widocznych na obrazach 11.2.2, 11.2.3 nie znaleziono żadnych wątków dotyczących frazy „faceit” czy „faceit.com”.

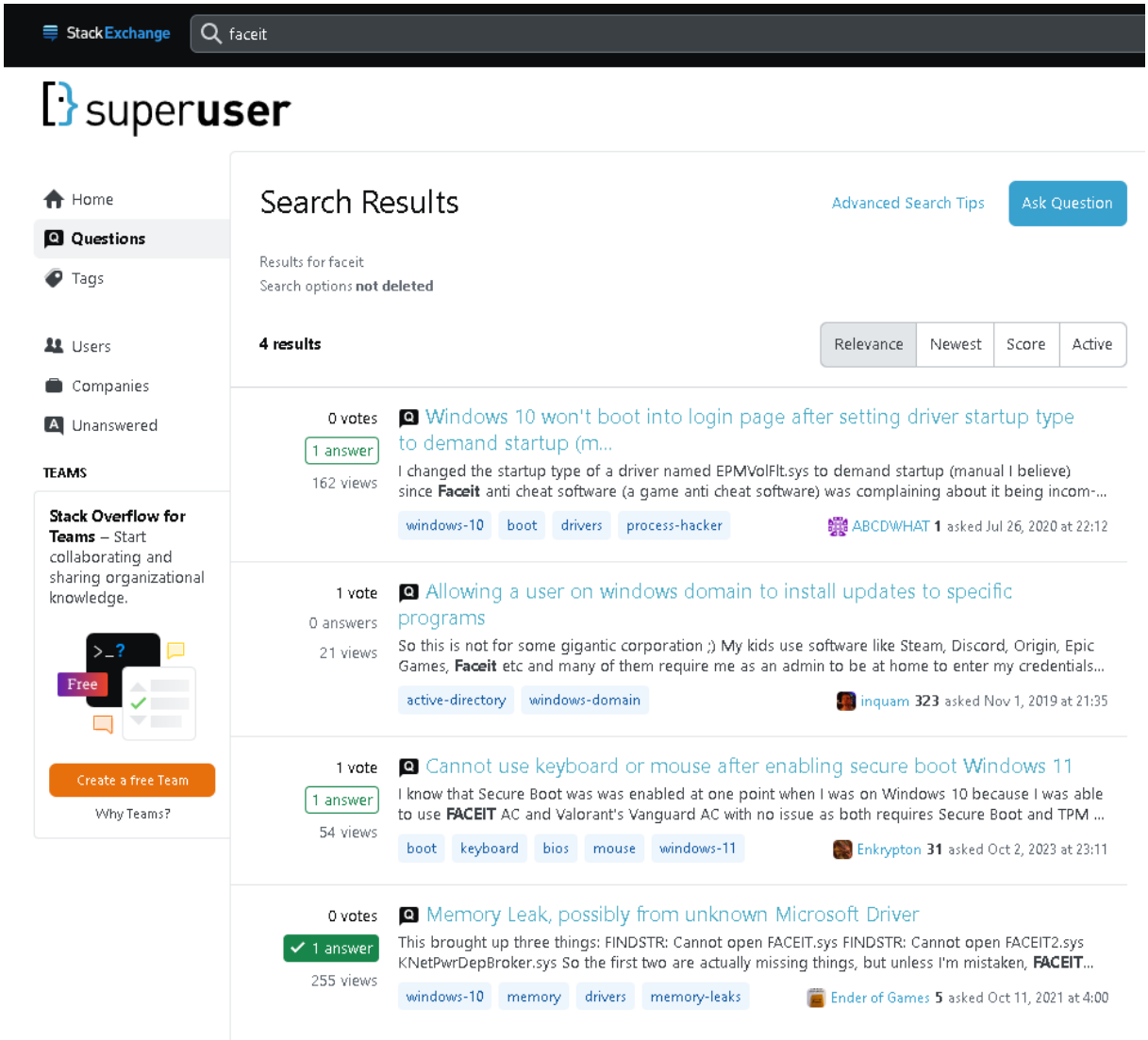


Obraz 11.2.2 rezultat wyszukania frazy faceit w serverfault.com, data wykonania zrzutu 11.1.2024 r.



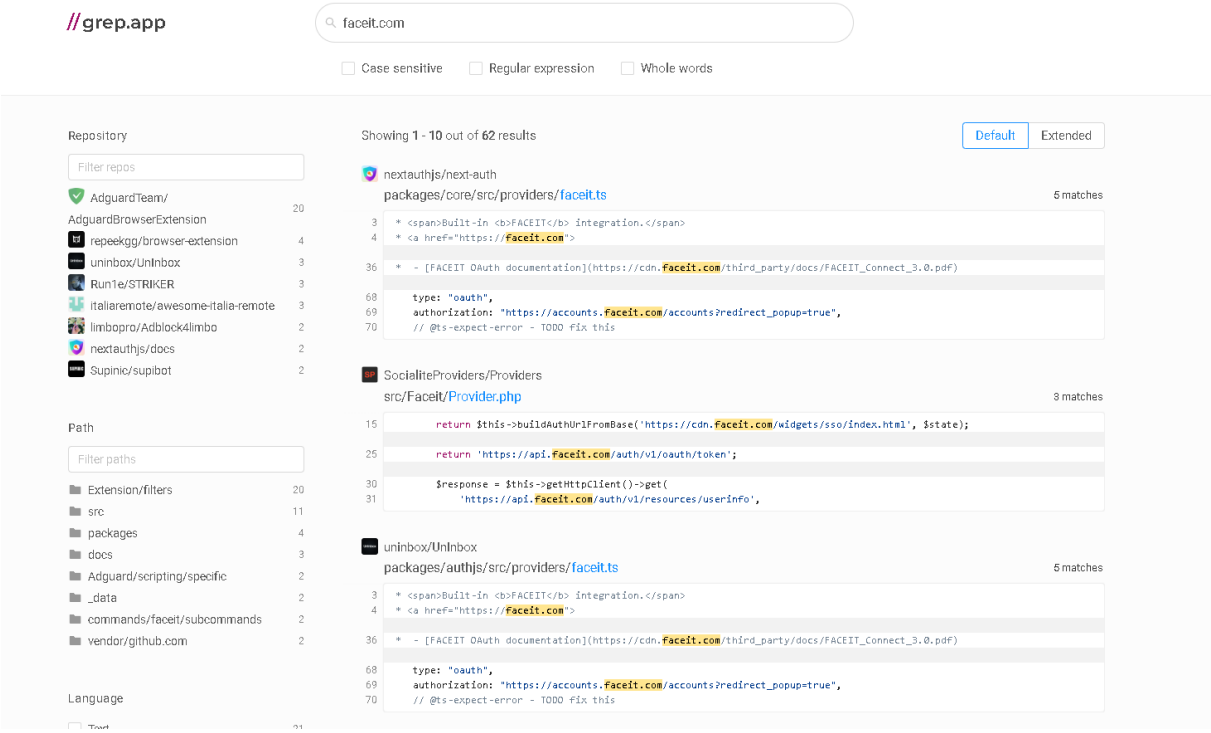
Obraz 11.2.3 rezultat wyszukania frazy faceit w askubuntu.com, data wykonania zrzutu 11.1.2024 r.

Wyniki znalezione na forum superuser widoczne na obrazie 11.2.4 dotyczyły m.in. plików systemowych nazwanych faceit.sys. Żaden z 4 rezultatów nie zawierał kluczowych informacji.



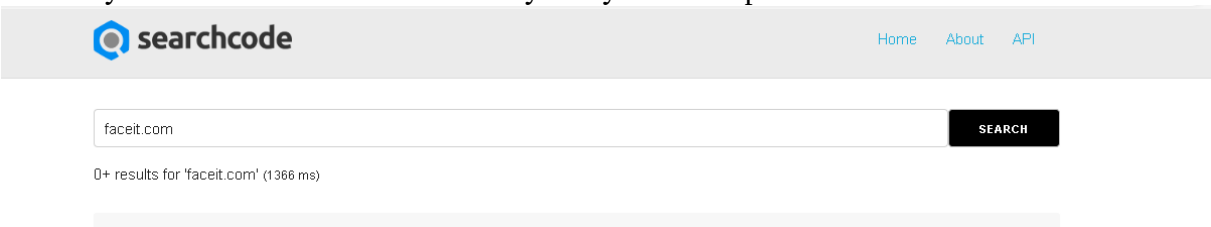
Obraz 11.2.4 rezultat wyszukania frazy faceit w superuser.com, data wykonania zrzutu 11.1.2024 r.

Po przejrzeniu 63 fragmentów kodów widocznych na obrazie 11.2.5 nie stwierdzono, że zawierają one interesujące informacje. Przeważnie były to odwołania do development KIT udostępnianego przez faceit.



Obraz 11.2.5 rezultat wyszukania frazy faceit w grepp.app, data wykonania zrzutu 11.1.2024 r.

Dla frazy faceit.com nie znaleziono żadnych wyników co potwierdza obraz 11.3.1.

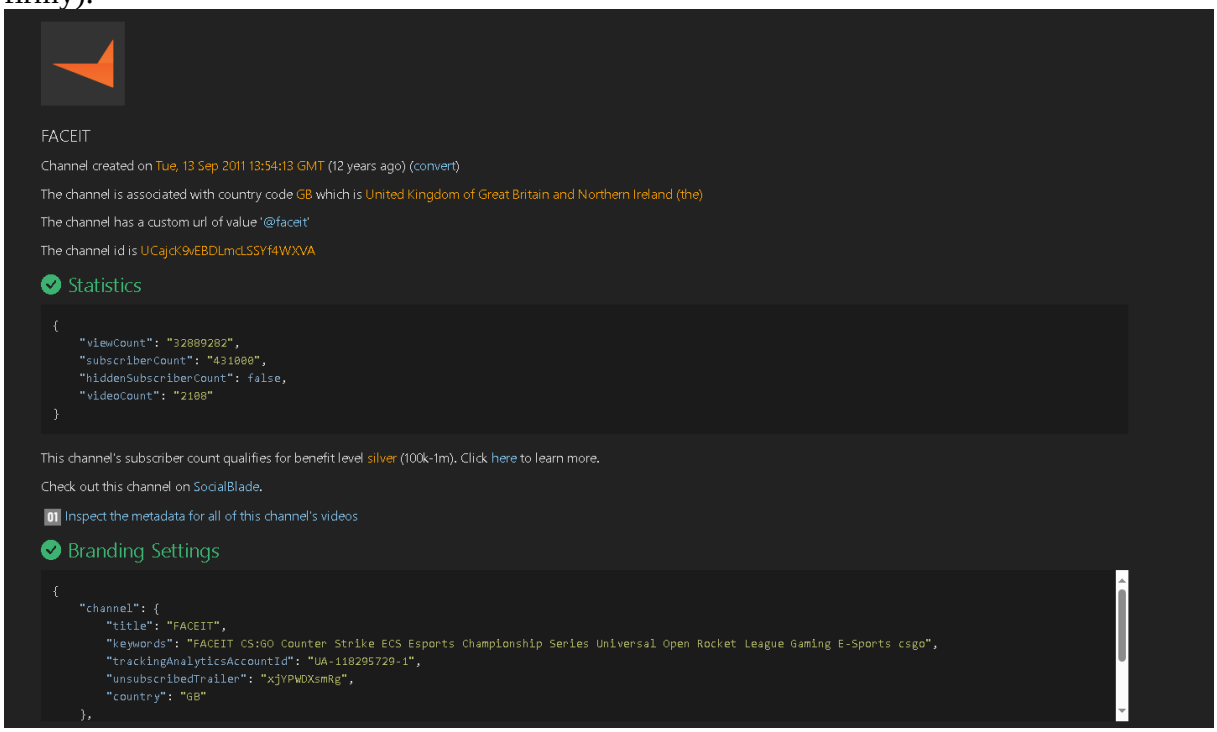


Obraz 11.3.1 rezultat wyszukania frazy faceit w searchcode.com, data wykonania zrzutu 13.12.2023 r.

Zawartość pliku robots.txt znajdująca się na obrazie 11.4.1 zawiera standardowe dyrektywy pozwalające robotom indeksować katalogi.

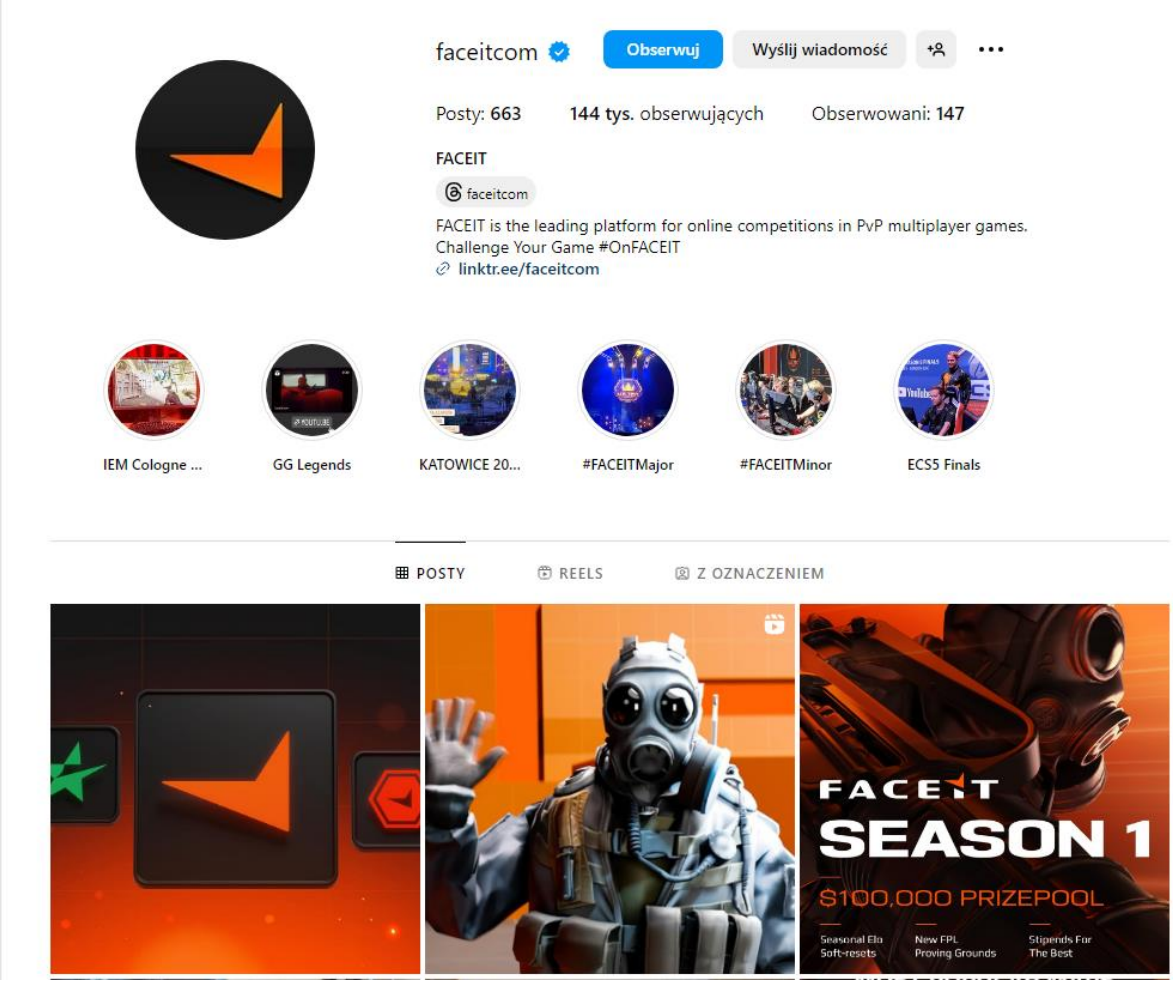
Obraz 11.4.1 zawartość pliku robots.txt, źródło faceit.com, data wykonania zrzutu 13.12.2023 r.

Przeglądając metadane kanału faceit widoczne na obrazie 11.5.1 nie natrafiono na informacje, które nie zostały już zapisane w poprzednich rozdziałach (np. zakres działania firmy, położenie firmy).



Obraz 11.5.1 sprawdzenie matadanych kanału YouTube Faceit, źródło mattw.io/youtube-metadata/, data wykonania zrzutu 10.1.2024 r.

Przeglądając media społecznościowe organizacji widoczne na obrazie 11.5.2 nie spostrzeżono istotnych informacji (media społecznościowe faceit służą wyłącznie do komunikacji z klientami, nie można tam znaleźć nawet informacji o parterach biznesowych, wyłącznie miejsca organizowania wydarzeń e-sportowych).



Obraz 11.5.2 social-media organizacji Faceit, źródło instagram.com, data wykonania zrzutu 10.1.2024r.

Na obrazach 11.6.1, 11.6.2 przedstawiono dane kontaktowe do administratorów zarządzających serwerami dns, z których usług korzysta domena faceit.com

Network Whois record

Queried **whois.arin.net** with "**n 104.17.63.50**"...

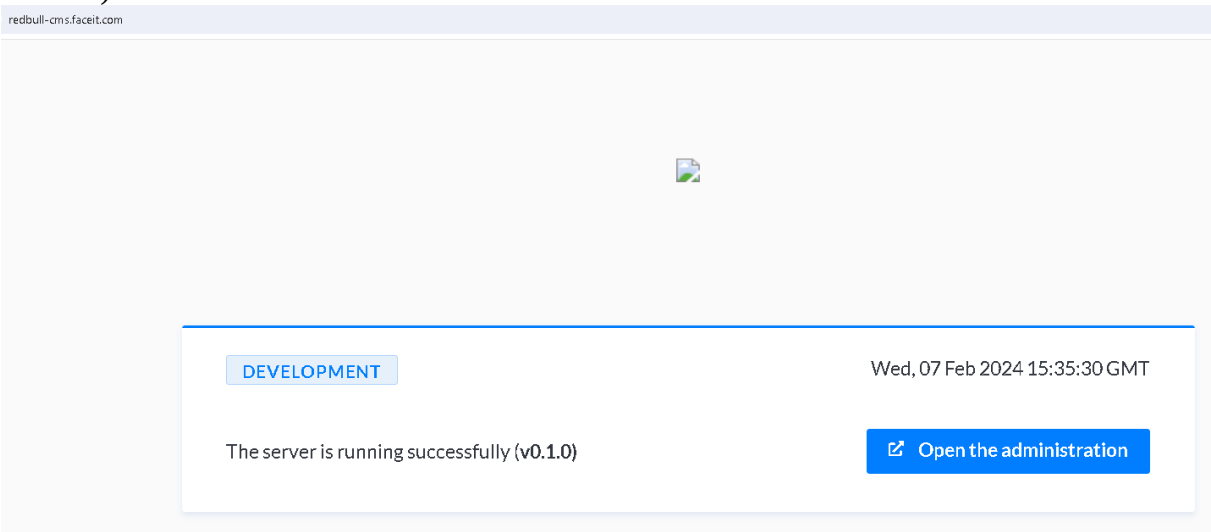
```
NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2021-05-26
Comment:        All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Ref:            https://rdap.arin.net/registry/ip/104.16.0.0


OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
Updated:        2021-07-01
Ref:            https://rdap.arin.net/registry/entity/CLOUD14


OrgNOCHandle: CLOUD146-ARIN
OrgNOCName:   Cloudflare-NOC
OrgNOCPhone:  +1-650-319-8930
OrgNOCEmail:  noc@cloudflare.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN

OrgRoutingHandle: CLOUD146-ARIN
OrgRoutingName:   Cloudflare-NOC
OrgRoutingPhone:  +1-650-319-8930
OrgRoutingEmail:  noc@cloudflare.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN

OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:  abuse@cloudflare.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:  rir@cloudflare.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN
```

Obraz 11.6.1 wyszukanie w bazie whois, źródło centralops.net, data wykonania zrzutu 12.12.2023 r.

```
OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:  abuse@cloudflare.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:  rir@cloudflare.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

RNOCHandle: NOC11962-ARIN
RNOCName:   NOC
RNOCPhone:  +1-650-319-8930
RNOCEmail:  noc@cloudflare.com
RNOCRef:    https://rdap.arin.net/registry/entity/NOC11962-ARIN

RAbuseHandle: ABUSE2916-ARIN
RAbuseName:   Abuse
RAbusePhone:  +1-650-319-8930
RAbuseEmail:  abuse@cloudflare.com
RAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

RTechHandle: ADMIN2521-ARIN
RTechName:   Admin
RTechPhone:  +1-650-319-8930
RTechEmail:  rir@cloudflare.com
RTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN
```

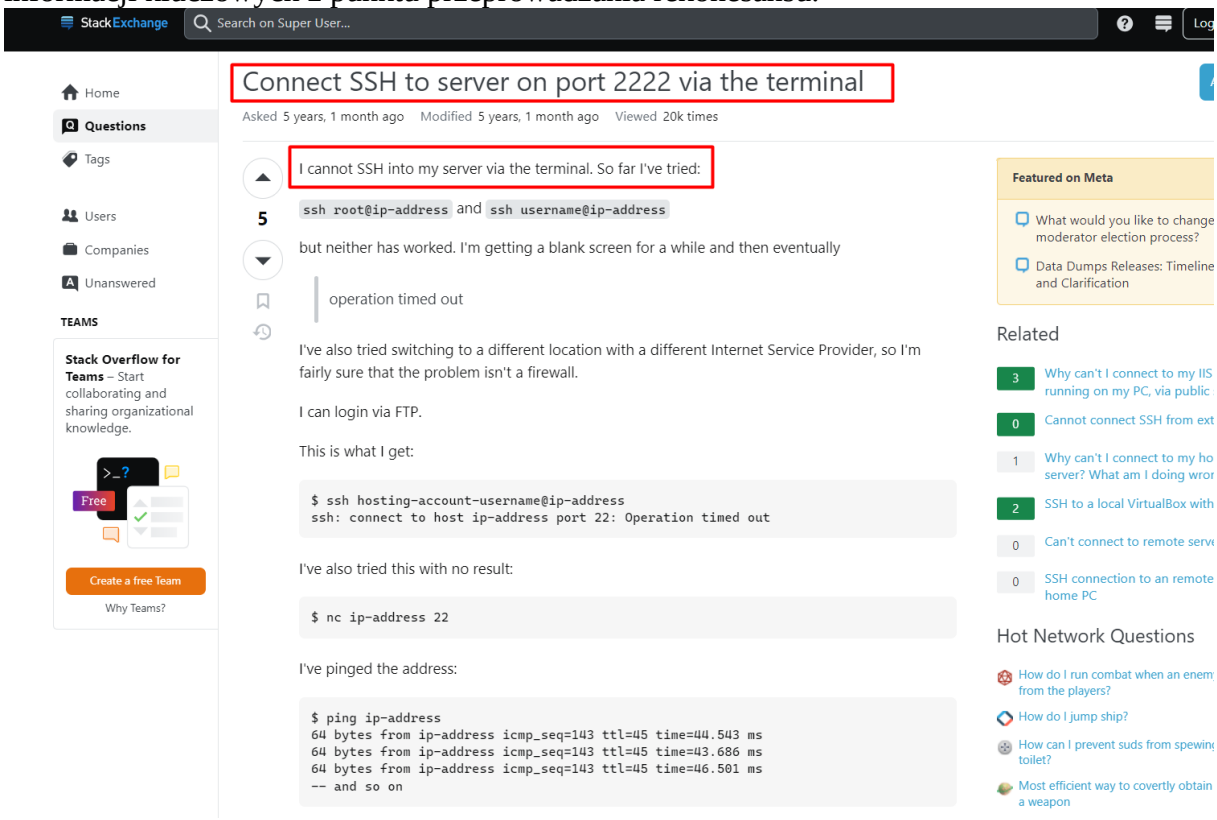
Obraz 11.6.2 wyszukanie w bazie whois, źródło centralops.net, data wykonania zrzutu 12.12.2023 r.

Pod adresem redbull-cms.faceit.com znajduje się interfejs przeznaczony dla administratorów (Obraz 11.7.1). Oczywiście próba otworzenia panelu kończy się niepowodzeniem – brak uprawnień. Interfejs informuje, że serwer w wersji 0.1.0 działa (nie udało się zidentyfikować serwera).



Obraz 11.7.1 potencjalny panel sterowania administratora dostępny pod adresem redbull-cms.faceit.com

Na obrazie 11.8.1 zaprezentowano pytanie użytkownika serwisu SuperUser o połączenie się z SSH na porrcie 2222 (na tym porcie jest udostępniona usługa SHH dla hosta faceit.com). Po przejrzeniu konta użytkownika i wątku widocznego na obrazie 11.8.1 nie spostrzeżono informacji kluczowych z punktu przeprowadzania rekonesansu.



Obraz 11.8.1 zapytanie w serwisie SuperUser

W zbieraniu danych do rozdziału 1 skorzystano z narzędzi takich jak instagram.com, mattw.io, faceit.com, grepp.app, superuser, askubuntu.com, serverfault, stackoverflow. Mimo rozbudowanych social mediów organizacji (YouTube, Instagram) nie znaleziono interesujących informacji mających wpływ na kolejne etapy rekonesansu.

12.Wnioski ogólne

Do przeprowadzenia rekonesansu pasywnego zostały użyte narzędzia dostępne w głównej mierze przez przeglądarkę internetową. Skorzystano również z kilku aplikacji desktopowych, czy narzędzi dostępnych w systemie Kali. Zgromadzono dane dotyczące organizacji, wykorzystywanych technologii, adresów, usługi sieciowe, wykorzystywane systemy operacyjne. Najwięcej kluczowych informacji zgromadzono w rozdziałach dotyczących serwerów DNS oraz struktury domeny, a także bezpieczeństwa i stosowanych usług sieciowych/systemów. Nie znaleziono prywatnych adresów email pracowników organizacji, modelów/typów urządzeń sieciowych, znaczących incydentów bezpieczeństwa. Wykryto podatności dla wykorzystywanych technologii czy usług sieciowych. Słabym punktem organizacji mogą być poglądy szerokich kręgów społecznych wobec współpracy z Arabską organizacją, której właściciel jest posądzany o morderstwo. Przeglądając prywatne konta pracowników nie znaleziono kluczowych informacji, jednak warto przyjrzeć się publicznym rejestrom przedsiębiorców Polskich i Brytyjskich, które zawierają wpisy o pracownikach organizacji. Do dalszych etapów rekonesansu przydatne są z pewnością informacje o tym, że usługi domeny są obsługiwane przez systemy operacyjne Linux. Czytając wpisy na forach dyskusyjnych nie można natrafić na przydatne informacje dotyczące infrastruktury domeny. Social media organizacji nie zawierają żadnych wycieków haseł zapisanych na kartkach, stosowanych urządzeniach sieciowych, umiejscowieniu kluczowej infrastruktury dla przetwarzania danych i prowadzenia procesów biznesowych. Nie znaleziono żadnych informacji na temat wycieku haseł, o którym poinformował google password manager i co było głównym powodem wyboru domeny.