



RAPORT Z OCENY BEZPIECZEŃSTWA

# Poligon CYRBER · środowisko testowe DVWA

<http://cyrber-dvwa-1/>

DATA: 2026-08-07

TRYB: MENS LIBER

ITERACJE: 17 · MODUŁY: 12 · CZAS: 7 min

## CRITICAL

14 wykrytych podatności

2

KRYTYCZNE

1

WYSOKIE

9

ŚREDNIE

2

NISKIE

POUFNE · WYŁĄCZNIE DO UŻYTKU AUTORYZOWANEGO

---

## SPIS TREŚCI

|           |                                |    |
|-----------|--------------------------------|----|
| <b>01</b> | Podsumowanie wykonawcze        | 4  |
| <b>02</b> | MISJA AUTONOMICZNA MENS        | 5  |
| <b>03</b> | PODATNOŚCI APLIKACJI WEBOWEJ   | 6  |
| <b>04</b> | WSTRZYKIWANIE SQL (SQLMAP)     | 6  |
| <b>05</b> | HTTPX                          | 7  |
| <b>06</b> | WALIDACJA DETEKCJI SIEM        | 7  |
| <b>07</b> | LOOT MISJI - PAMIĘĆ KILL-CHAIN | 7  |
| <b>08</b> | ITERUM - REPLAY MISJI          | 8  |
| <b>09</b> | PLAN NAPRAWCZY                 | 11 |

# PODSUMOWANIE DLA ZARZĄDU

Poligon CYRBER · środowisko testowe DVWA - 2026-08-07

|                                     |                                            |                                 |
|-------------------------------------|--------------------------------------------|---------------------------------|
| CEL<br><b>http://cyrber-dvwa-1/</b> | POZIOM RYZYKA<br><b>CRITICAL</b><br>90/100 | WYKRYTE PODATNOŚCI<br><b>14</b> |
|-------------------------------------|--------------------------------------------|---------------------------------|

## WYKRYTE PODATNOŚCI

|                       |                     |                     |                    |
|-----------------------|---------------------|---------------------|--------------------|
| <b>2</b><br>KRYTYCZNE | <b>1</b><br>WYSOKIE | <b>9</b><br>ŚREDNIE | <b>2</b><br>NISKIE |
|-----------------------|---------------------|---------------------|--------------------|

## WYMAGANE DZIAŁANIA

|                                                                  |
|------------------------------------------------------------------|
| <b>Natychmiast: naprawić 2 krytyczne podatności</b>              |
| <b>W ciągu 30 dni: zająć się 1 podatnością wysoką</b>            |
| <b>Ciągle: monitorować powierzchnię ataku przez CYRBER UMBRA</b> |

|                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------|
| SZACOWANY KOSZT NIEDZIAŁANIA<br>Średni koszt incydentu bezpieczeństwa w Europie: <b>€4.3M</b> (IBM Cost of a Data Breach 2024) |
|--------------------------------------------------------------------------------------------------------------------------------|

## 01 PODSUMOWANIE WYKONAWCZE

### Co odkryliśmy

Organizm CYRBER przeanalizował

system `http://cyrber-dvwa-1/`,

wykonując 17 iteracji w ciągu 7 min. Wykryliśmy **14 potencjalnych podatności**. Ogólny poziom ryzyka oceniamy jako **krytyczny - system zawiera podatności umożliwiające pełne przejęcie kontroli**.



■ CRITICAL 2 (14%) ■ HIGH 1 (7%) ■ MEDIUM 9 (64%) ■ LOW 2 (14%)

**Analiza AI:** Podczas testów penetracyjnych zidentyfikowaliśmy poważne luki w zabezpieczeniach aplikacji internetowej, które mogą umożliwić atakującemu przejęcie kontroli nad systemem, kradzież danych lub zakłócenie działalności. Wykryte podatności obejmują m.in. możliwość wykonania dowolnych komend, manipulację ścieżkami plików oraz ataki SQL Injection, co stwarza bezpośrednie zagrożenie dla poufności, integralności i dostępności danych firmy.

### Co może się stać, jeśli nic nie zrobimy

#### Command execution

MEDIUM

Co to znaczy dla Twojej firmy: Umożliwia atakującemu pełną kontrolę nad serwerem, co może prowadzić do całkowitego przejęcia infrastruktury IT.

#### Path Traversal

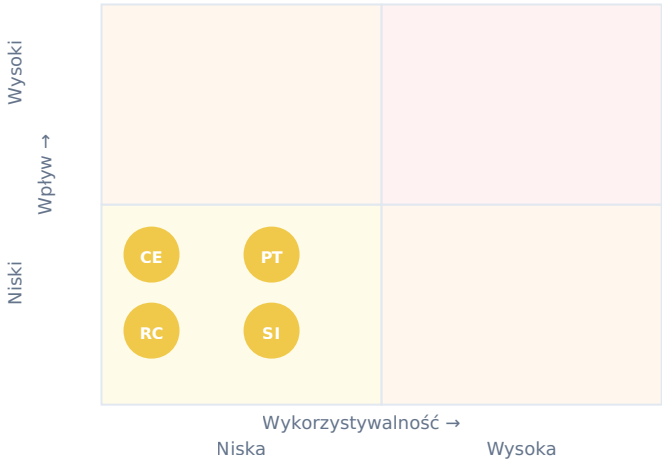
MEDIUM

Co to znaczy dla Twojej firmy: Ryzyko nieautoryzowanego dostępu do plików systemowych, co może skutkować ujawnieniem poufnych danych lub zakłóceniem działania aplikacji.

### Trzy kroki na najbliższe 30 dni

1. Natychmiast zaktualizuj aplikację i jej komponenty oprogramowania, aby usunąć krytyczną podatność SQL Injection (id) i inne krytyczne luki.
2. Wdrożenie mechanizmów walidacji i filtrowania danych wejściowych oraz ograniczenie uprawnień użytkowników w bazie danych, aby zapobiec atakom SQL Injection i Path Traversal.
3. Przeprowadź kompleksowy audyt bezpieczeństwa aplikacji oraz wdrożenie odpowiednich zabezpieczeń, takich jak Content Security Policy i ochrona przed Clickjacking, aby zminimalizować ryzyko powtórzenia się podobnych podatności.

MAPA CIEPŁA RYZYKA



**CE** = Command execution    **PT** = Path Traversal    **RC** = Reflected Cross Site Scripting    **SI** = SQL Injection

02 MISJA AUTONOMICZNA MENS

MODE

**LIBER**

ITERATIONS

**17**

MODULES

**12**

SYGNAŁY

**62**

DURATION

**7 min**

ZNALEZISKA WG MODUŁU



### 03 PODATNOŚCI APLIKACJI WEBOWEJ

#### Wapiti - 14 vulnerabilities

MEDIUM: 9

LOW: 5

| LEVEL                                     | VULNERABILITY                                                                                                                      | URL                                               | PARAMETER | WSTG                                       |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|-----------|--------------------------------------------|
| <b>MEDIUM</b>                             | <b>Command execution</b><br>Ryzyko biznesowe: Podatność może zostać wykorzystana do naruszenia bezpieczeństwa systemu              | /vulnerabilities/exec/                            | ip        | WSTG-INPV-12                               |
| <b>HIGH</b><br>CVSS 7.5<br>(HIGH)         | <b>Path Traversal</b><br>Ryzyko biznesowe: Atakujący może odczytać dowolne pliki z systemu                                         | /vulnerabilities/fi/                              | page      | WSTG-ATHZ-01                               |
| <b>MEDIUM</b>                             | <b>Reflected Cross Site Scripting</b><br>Ryzyko biznesowe: Podatność może zostać wykorzystana do naruszenia bezpieczeństwa systemu | /vulnerabilities/xss_r/, /vulnerabilities/csp/ +2 | name      | WSTG-INPV-01                               |
| <b>CRITICAL</b><br>CVSS 9.8<br>(CRITICAL) | <b>SQL Injection</b><br>Ryzyko biznesowe: Atakujący może uzyskać pełny dostęp do bazy danych                                       | /vulnerabilities/brute/, /vulnerabilities/sqli/   | username  | WSTG-INPV-05                               |
| <b>MEDIUM</b><br>CVSS 4.3<br>(MEDIUM)     | <b>Content Security Policy Configuration</b><br>Ryzyko biznesowe: Możliwe ataki XSS wstrzykujące złośliwy kod do stron             | /instructions.php                                 |           | WSTG-CONF-12, OSHP-Content-Security-Policy |
| <b>LOW</b>                                | <b>Clickjacking Protection</b><br>Ryzyko biznesowe: Użytkownik może zostać nakłoniony do kliknięcia w ukryte elementy              | /, /instructions.php                              |           | OSHP-X-Frame-Options                       |
| <b>MEDIUM</b><br>CVSS 4.3<br>(MEDIUM)     | <b>MIME Type Confusion</b><br>Ryzyko biznesowe: Przeglądarka może interpretować pliki jako kod wykonywalny                         | /, /instructions.php                              |           | OSHP-X-Content-Type-Options                |

### 04 WSTRZYKIWANIE SQL (SQLMAP)

**PODATNY** Parametry: id

05 HTTPX

PROBED HOSTS

LIVE HOSTS

TECHNOLOGIES

WEB SERVERS

9

1

3

1

DETECTED TECHNOLOGIES:

Apache HTTP Server:2.4.25

Debian

PHP

WEB SERVERS:

Apache/2.4.25 (Debian)

| STATUS | URL                     | TITLE                                                        | SERVER                 | TECHNOLOGIES                           |
|--------|-------------------------|--------------------------------------------------------------|------------------------|----------------------------------------|
| 200    | http://cyrber-dvwa-1:80 | Login :: Damn Vulnerable Web Application (DVWA) v1.10 *Devel | Apache/2.4.25 (Debian) | Apache HTTP Server:2.4.25, Debian, PHP |

06 WALIDACJA DETEKCJI SIEM

CYRBER wykonał 8 technik ATT&CK. ELS wykrył 2 (25.0%).

| Technika  | Opis                              | Status        |
|-----------|-----------------------------------|---------------|
| T1059     | Command and Scripting Interpreter | X NIEWIDOCZNA |
| T1059.007 | JavaScript                        | OK WYKRYTA    |
| T1083     | File and Directory Discovery      | X NIEWIDOCZNA |
| T1110     | Brute Force                       | X NIEWIDOCZNA |
| T1190     | Exploit Public-Facing Application | OK WYKRYTA    |
| T1505.003 | Web Shell                         | X NIEWIDOCZNA |
| T1592     | Gather Victim Host Information    | X NIEWIDOCZNA |
| T1595     | Active Scanning                   | X NIEWIDOCZNA |

KRYTYCZNE: ponad połowa technik niewidoczna dla SIEM. Priorytet: przegląd reguł detekcji.

07 LOOT MISJI - PAMIĘĆ KILL-CHAIN

Misja zebrała 2 węzłów loot (working memory kill-chain). Pieczęć TESTIMONIUM: 2/2. Podsumowania zredagowane - bez surowych sekretów.

Według rodzaju: session=2

| Rodzaj  | Etykieta                     | Cel                                              | Moduł      | Podsumowanie                                                                                                                          | Pieczęć |
|---------|------------------------------|--------------------------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------|---------|
| session | rce:ses-48859b7aa8f2         | http://cyrber-dvwa-1:80/vulnerabilities/fi/?page | cmdi_shell | [session] rce:ses-48859b7aa8f2 · via cmdi_shell · on http://cyrber-dvwa-1:80/vulnerabilities/fi/?page=file1.php · rce                 | ●       |
| session | real_access:ses-48859b7aa8f2 | http://cyrber-dvwa-1:80/vulnerabilities/fi/?page | cmdi_shell | [session] real_access:ses-48859b7aa8f2 · via cmdi_shell · on http://cyrber-dvwa-1:80/vulnerabilities/fi/?page=file1.php · real_access | ●       |

08 ITERUM - REPLAY MISJI

| <div><div>80</div><div>STEPS</div></div> <div><div>21</div><div>ITERATIONS</div></div> <div><div>447.6s</div><div>TOTAL TIME</div></div> |         |           |       |       |           |            |
|------------------------------------------------------------------------------------------------------------------------------------------|---------|-----------|-------|-------|-----------|------------|
| ITER                                                                                                                                     | FAZA    | MODUŁ     | GŁOWA | CZAS  | STATUS    | ZNALEZISKA |
| 1                                                                                                                                        | OBSERVE | -         | -     | 12.3s | ok        |            |
| 1                                                                                                                                        | THINK   | httpx     | RATIO | 5.5s  | ok        |            |
| 1                                                                                                                                        | ACT     | httpx     | RATIO | 3.3s  | completed | 1          |
| 1                                                                                                                                        | LEARN   | httpx     | RATIO | 3.4s  | completed | 1          |
| 2                                                                                                                                        | OBSERVE | -         | -     | 8.9s  | ok        |            |
| 2                                                                                                                                        | THINK   | web_crawl | RATIO | 4.8s  | ok        |            |
| 2                                                                                                                                        | ACT     | web_crawl | RATIO | 1.0s  | completed | 36         |
| 2                                                                                                                                        | LEARN   | web_crawl | RATIO | 867ms | completed | 36         |
| 3                                                                                                                                        | OBSERVE | -         | -     | 11.3s | ok        |            |
| 3                                                                                                                                        | THINK   | gobuster  | RATIO | 6.9s  | ok        |            |
| 3                                                                                                                                        | ACT     | gobuster  | RATIO | 634ms | completed |            |
| 3                                                                                                                                        | LEARN   | gobuster  | RATIO | 3.6s  | completed |            |
| 4                                                                                                                                        | OBSERVE | -         | -     | 9.1s  | ok        |            |
| 4                                                                                                                                        | THINK   | arjun     | RATIO | 6.5s  | ok        |            |
| 4                                                                                                                                        | ACT     | arjun     | RATIO | 2ms   | skipped   |            |
| 4                                                                                                                                        | LEARN   | arjun     | RATIO | 16ms  | skipped   |            |
| 5                                                                                                                                        | OBSERVE | -         | -     | 8.6s  | ok        |            |
| 5                                                                                                                                        | THINK   | dalfox    | RATIO | 4.6s  | ok        |            |
| 5                                                                                                                                        | ACT     | dalfox    | RATIO | 27.8s | completed | 2          |
| 5                                                                                                                                        | LEARN   | dalfox    | RATIO | 7.4s  | completed | 2          |
| 6                                                                                                                                        | OBSERVE | -         | -     | 7.8s  | ok        |            |
| 6                                                                                                                                        | THINK   | sqlmap    | RATIO | 5.0s  | ok        |            |
| 6                                                                                                                                        | ACT     | sqlmap    | RATIO | 18.2s | completed | 1          |
| 6                                                                                                                                        | LEARN   | sqlmap    | RATIO | 5.0s  | completed | 1          |
| 7                                                                                                                                        | OBSERVE | -         | -     | 9.0s  | ok        |            |
| 7                                                                                                                                        | THINK   | wapiti    | RATIO | 4.4s  | ok        |            |
| 7                                                                                                                                        | ACT     | wapiti    | RATIO | 78.3s | completed | 14         |
| 7                                                                                                                                        | LEARN   | wapiti    | RATIO | 3.0s  | completed | 14         |
| 8                                                                                                                                        | OBSERVE | -         | -     | 8.5s  | ok        |            |
| 8                                                                                                                                        | THINK   | lfi       | RATIO | 4.9s  | ok        |            |
| 8                                                                                                                                        | ACT     | lfi       | RATIO | 962ms | completed | 1          |
| 8                                                                                                                                        | LEARN   | lfi       | RATIO | 14.2s | completed | 1          |

|    |                |             |        |       |           |   |
|----|----------------|-------------|--------|-------|-----------|---|
| 9  | <b>OBSERVE</b> | -           | -      | 9.0s  | ok        |   |
| 9  | <b>THINK</b>   | file_upload | RATIO  | 5.7s  | ok        |   |
| 9  | <b>ACT</b>     | file_upload | RATIO  | 451ms | completed | 1 |
| 9  | <b>LEARN</b>   | file_upload | RATIO  | 4.4s  | completed | 1 |
| 10 | <b>OBSERVE</b> | -           | -      | 8.2s  | ok        |   |
| 10 | <b>THINK</b>   | csrf        | RATIO  | 4.9s  | ok        |   |
| 10 | <b>ACT</b>     | csrf        | RATIO  | 265ms | completed | 2 |
| 10 | <b>LEARN</b>   | csrf        | RATIO  | 3.6s  | completed | 2 |
| 11 | <b>OBSERVE</b> | -           | -      | 8.1s  | ok        |   |
| 11 | <b>THINK</b>   | brute_force | RATIO  | 5.0s  | ok        |   |
| 11 | <b>ACT</b>     | brute_force | RATIO  | 720ms | completed | 1 |
| 11 | <b>LEARN</b>   | brute_force | RATIO  | 4.4s  | completed | 1 |
| 12 | <b>OBSERVE</b> | -           | -      | 8.9s  | ok        |   |
| 12 | <b>THINK</b>   | stored_xss  | RATIO  | 4.8s  | ok        |   |
| 12 | <b>ACT</b>     | stored_xss  | RATIO  | 475ms | completed | 1 |
| 12 | <b>LEARN</b>   | stored_xss  | RATIO  | 4.2s  | completed | 1 |
| 13 | <b>OBSERVE</b> | -           | -      | 7.6s  | ok        |   |
| 13 | <b>THINK</b>   | cmdi_shell  | RATIO  | 6.0s  | ok        |   |
| 13 | <b>ACT</b>     | cmdi_shell  | RATIO  | 561ms | completed | 2 |
| 13 | <b>LEARN</b>   | cmdi_shell  | RATIO  | 9.6s  | completed | 2 |
| 14 | <b>OBSERVE</b> | -           | -      | 8.6s  | ok        |   |
| 14 | <b>THINK</b>   | commix      | RATIO  | 1ms   | ok        |   |
| 14 | <b>ACT</b>     | linpeas     | RATIO  | 0.0s  | skipped   |   |
| 15 | <b>OBSERVE</b> | -           | -      | 8.7s  | ok        |   |
| 15 | <b>THINK</b>   | commix      | RATIO  | 2ms   | ok        |   |
| 15 | <b>ACT</b>     | winpeas     | RATIO  | 0.0s  | skipped   |   |
| 16 | <b>OBSERVE</b> | -           | -      | 8.0s  | ok        |   |
| 16 | <b>THINK</b>   | commix      | RATIO  | 1ms   | ok        |   |
| 16 | <b>ACT</b>     | chisel      | RATIO  | 0.0s  | skipped   |   |
| 17 | <b>OBSERVE</b> | -           | -      | 7.9s  | ok        |   |
| 17 | <b>THINK</b>   | commix      | RATIO  | 1ms   | ok        |   |
| 17 | <b>ACT</b>     | lateral_sim | RATIO  | 0.0s  | skipped   |   |
| 18 | <b>OBSERVE</b> | -           | -      | 8.0s  | ok        |   |
| 18 | <b>THINK</b>   | commix      | RATIO  | 7ms   | ok        |   |
| 18 | <b>ACT</b>     | commix      | RATIO  | 56ms  | skipped   |   |
| 18 | <b>LEARN</b>   | commix      | RATIO  | 21ms  | skipped   |   |
| 19 | <b>OBSERVE</b> | -           | -      | 7.9s  | ok        |   |
| 19 | <b>THINK</b>   | post_ex     | ANIMUS | 5ms   | ok        |   |

|    |         |         |        |      |             |
|----|---------|---------|--------|------|-------------|
| 19 | ACT     | post_ex | ANIMUS | 0.0s | lex_blocked |
| 19 | LEARN   | post_ex | ANIMUS | 12ms | lex_blocked |
| 20 | OBSERVE | -       | -      | 7.5s | ok          |
| 20 | THINK   | post_ex | ANIMUS | 5ms  | ok          |
| 20 | ACT     | post_ex | ANIMUS | 0.0s | lex_blocked |
| 20 | LEARN   | post_ex | ANIMUS | 18ms | lex_blocked |
| 21 | OBSERVE | -       | -      | 7.9s | ok          |
| 21 | THINK   | post_ex | ANIMUS | 5ms  | ok          |
| 21 | ACT     | post_ex | ANIMUS | 0.0s | lex_blocked |
| 21 | LEARN   | post_ex | ANIMUS | 12ms | lex_blocked |

## 09 PLAN NAPRAWCZY

| POZIOM                                    | ZNALEZISKO                                                                                                                            | ZALECANE DZIAŁANIE                                                                     | TERMIN      | NAKŁAD   |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-------------|----------|
| <b>CRITICAL</b><br>CVSS 9.8<br>(CRITICAL) | <b>SQL Injection</b><br>Ryzyko biznesowe:<br>Atakujący może uzyskać pełny dostęp do bazy danych                                       | SQL Injection (DBMS: MariaDB) via injection in the parameter username                  | Natychmiast | 1-2 days |
| <b>HIGH</b><br>CVSS 7.5<br>(HIGH)         | <b>Path Traversal</b><br>Ryzyko biznesowe:<br>Atakujący może odczytać dowolne pliki z systemu                                         | Linux local file disclosure vulnerability via injection in the parameter page          | < 7 dni     | 1-2 days |
| <b>MEDIUM</b>                             | <b>Command execution</b><br>Ryzyko biznesowe:<br>Podatność może zostać wykorzystana do naruszenia bezpieczeństwa systemu              | Command execution via injection in the parameter ip                                    | < 30 dni    | 1-2 days |
| <b>MEDIUM</b>                             | <b>Reflected Cross Site Scripting</b><br>Ryzyko biznesowe:<br>Podatność może zostać wykorzystana do naruszenia bezpieczeństwa systemu | Reflected Cross Site Scripting vulnerability found via injection in the parameter name | < 30 dni    | 1-2 days |
| <b>MEDIUM</b><br>CVSS 4.3<br>(MEDIUM)     | <b>Content Security Policy Configuration</b><br>Ryzyko biznesowe:<br>Możliwe ataki XSS wstrzykujące złośliwy kod do stron             | CSP is not set                                                                         | < 30 dni    | < 1h     |
| <b>MEDIUM</b><br>CVSS 4.3<br>(MEDIUM)     | <b>MIME Type Confusion</b><br>Ryzyko biznesowe:<br>Przeglądarka może interpretować pliki jako kod wykonywalny                         | X-Content-Type-Options is not set                                                      | < 30 dni    | < 1h     |
| <b>LOW</b>                                | <b>Clickjacking Protection</b><br>Ryzyko biznesowe:<br>Użytkownik może zostać nakłoniony do kliknięcia w ukryte elementy              | X-Frame-Options is not set                                                             | < 90 dni    | < 1h     |