



RAPORT Z OCENY BEZPIECZEŃSTWA

Raport przykładowy · środowisko testowe DVWA

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

DATA: 2026-08-17

TRYB: MENS LIBER

ITERACJE: 21 · MODUŁY: 13 · CZAS: 13 min

CRITICAL

15 wykrytych podatności

2

KRYTYCZNE

1

WYSOKIE

9

ŚREDNIE

3

NISKIE

5

INFO

POUFNE · WYŁĄCZNIE DO UŻYTKU AUTORYZOWANEGO

SPIS TREŚCI

01	Podsumowanie wykonawcze	4
02	MISJA AUTONOMICZNA MENS	5
03	PODATNOŚCI APLIKACJI WEBOWEJ	6
04	ENUMERACJA KATALOGÓW (GOBUSTER)	7
05	HTTPX	7
06	WALIDACJA DETEKCY SIEM	7
07	LOOT MISJI - PAMIĘĆ KILL-CHAIN	8
08	ITERUM - REPLAY MISJI	9
09	PLAN NAPRAWCZY	12

PODSUMOWANIE DLA ZARZĄDU

Raport przykładowy · środowisko testowe DVWA - 2026-08-17

CEL	POZIOM RYZYKA	WYKRYTE PODATNOŚCI
http://cyrber-dvwa-1/	CRITICAL 90/100	15

WYKRYTE PODATNOŚCI

2 KRYTYCZNE	1 WYSOKIE	9 ŚREDNIE	3 NISKIE
-----------------------	---------------------	---------------------	--------------------

WYMAGANE DZIAŁANIA

Natychmiast: naprawić 2 krytyczne podatności
W ciągu 30 dni: zająć się 1 podatnością wysoką
Ciągle: monitorować powierzchnię ataku przez CYRBER UMBRA

SZACOWANY KOSZT NIEDZIAŁANIA
Średni koszt incydentu bezpieczeństwa w Europie: €4.3M (IBM Cost of a Data Breach 2024)

01 PODSUMOWANIE WYKONAWCZE

Co odkryliśmy

Organizm CYRBER

przeanalizował system

`http://cyrber-dvwa-1/` , wykonując 21 iteracji w ciągu 13 min. Wykryliśmy **15 potencjalnych podatności**. Ogólny poziom ryzyka oceniamy jako **krytyczny** - system zawiera podatności umożliwiające pełne przejęcie kontroli.



Analiza AI: Podczas testów penetracyjnych zidentyfikowano poważne luki w zabezpieczeniach aplikacji internetowej, które mogą prowadzić do naruszenia poufności, integralności i dostępności danych. Znalaziono szereg podatności, które umożliwiają atakującym przejęcie kont, kradzież danych oraz zakłócenie działania systemu. Konieczne jest natychmiastowe wdrożenie działań naprawczych, aby zminimalizować ryzyko cyberataków.

Co może się stać, jeśli nic nie zrobimy

Command execution

MEDIUM

Co to znaczy dla Twojej firmy: Atakujący może uzyskać pełną kontrolę nad serwerem, co prowadzi do kradzieży danych, instalacji złośliwego oprogramowania lub zakłócenia działalności.

Path Traversal

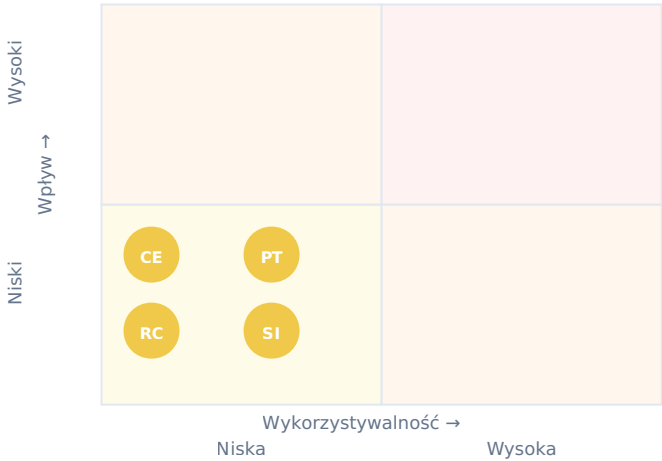
MEDIUM

Co to znaczy dla Twojej firmy: Atakujący może odczytać dowolne pliki z systemu

Trzy kroki na najbliższe 30 dni

1. Natychmiast zaktualizować i zabezpieczyć aplikację przed wykonaniem poleceń systemowych, wstrzykiwaniem SQL oraz atakami XSS.
2. Wdrożyć odpowiednie nagłówki bezpieczeństwa (np. CSP, X-Frame-Options) w celu ochrony przed atakami typu clickjacking i MIME Type Confusion.
3. Przeprowadzić audyt kodu i testy penetracyjne po wdrożeniu poprawek, aby potwierdzić skuteczność wprowadzonych zmian.

MAPA CIEPŁA RYZYKA



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

02 MISJA AUTONOMICZNA MENS

MODE

LIBER

ITERATIONS

21

MODULES

13

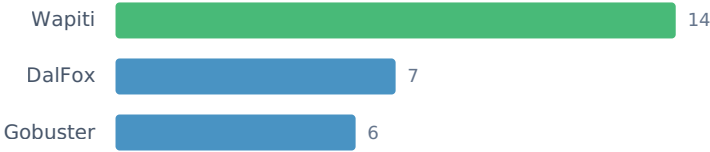
SYGNAŁY

71

DURATION

13 min

ZNALEZISKA WG MODUŁU



03 PODATNOŚCI APLIKACJI WEBOWEJ

Wapiti - 14 vulnerabilities

MEDIUM: 9

LOW: 5

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

04 ENUMERACJA KATALOGÓW (GOBUSTER)

ŚCIEŻKA	STATUS	RYZYSKO	UWAGA	ROZMIAR
index.php	200 (dostępny publicznie)	LOW		3947
.htpasswd	403 (zablokowany - warto sprawdzić)	INFO	Blocked but present - verify access control	316
.htaccess	403 (zablokowany - warto sprawdzić)	INFO	Blocked but present - verify access control	316
.hta	403 (zablokowany - warto sprawdzić)	INFO		311
help	301 (przekierowanie)	INFO		349
source	301 (przekierowanie)	INFO		351

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 9 technik ATT&CK. ELS wykrył 0 (0.0%).

Technika	Opis	Status
T1059	Command and Scripting Interpreter	X NIEWIDOCZNA
T1059.007	JavaScript	X NIEWIDOCZNA
T1083	File and Directory Discovery	X NIEWIDOCZNA
T1090	Proxy	X NIEWIDOCZNA
T1110	Brute Force	X NIEWIDOCZNA
T1190	Exploit Public-Facing Application	X NIEWIDOCZNA
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-a89c20b1fc4d	http://cyerber-dvwa-1/vulnerabilities/fi/?page=in	cmdi_shell	[session] rce:ses-a89c20b1fc4d · via cmdi_shell · on http://cyerber-dvwa-1/vulnerabilities/fi/?page=include.php · rce	●
session	real_access:ses-a89c20b1fc4d	http://cyerber-dvwa-1/vulnerabilities/fi/?page=in	cmdi_shell	[session] real_access:ses-a89c20b1fc4d · via cmdi_shell · on http://cyerber-dvwa-1/vulnerabilities/fi/?page=include.php · real_access	●

08 ITERUM - REPLAY MISJI

80 STEPS 21 ITERATIONS 758.4s TOTAL TIME						
ITER	FAZA	MODUŁ	GŁOWA	CZAS	STATUS	ZNALEZISKA
1	OBSERVE	-	-	14.2s	ok	
1	THINK	httpx	RATIO	15.7s	ok	
1	ACT	httpx	RATIO	7.1s	completed	1
1	LEARN	httpx	RATIO	5.2s	completed	1
2	OBSERVE	-	-	17.0s	ok	
2	THINK	dalfox	RATIO	6.9s	ok	
2	ACT	dalfox	RATIO	76.6s	completed	7
2	LEARN	dalfox	RATIO	60.1s	completed	7
3	OBSERVE	-	-	15.5s	ok	
3	THINK	sqlmap	RATIO	5.9s	ok	
3	ACT	sqlmap	RATIO	24.8s	completed	
3	LEARN	sqlmap	RATIO	3.5s	completed	
4	OBSERVE	-	-	14.5s	ok	
4	THINK	web_crawl	RATIO	4.8s	ok	
4	ACT	web_crawl	RATIO	790ms	completed	35
4	LEARN	web_crawl	RATIO	925ms	completed	35
5	OBSERVE	-	-	16.1s	ok	
5	THINK	gobuster	RATIO	9.0s	ok	
5	ACT	gobuster	RATIO	1.7s	completed	6
5	LEARN	gobuster	RATIO	983ms	completed	6
6	OBSERVE	-	-	13.3s	ok	
6	THINK	arjun	RATIO	5.7s	ok	
6	ACT	arjun	RATIO	3.2s	completed	
6	LEARN	arjun	RATIO	3.1s	completed	
7	OBSERVE	-	-	13.0s	ok	
7	THINK	wapiti	RATIO	5.4s	ok	
7	ACT	wapiti	RATIO	140.9s	completed	14
7	LEARN	wapiti	RATIO	1.4s	completed	14
8	OBSERVE	-	-	13.2s	ok	
8	THINK	lfi	RATIO	5.8s	ok	
8	ACT	lfi	RATIO	3.4s	completed	1
8	LEARN	lfi	RATIO	4.4s	completed	1

9	OBSERVE	-	-	13.5s	ok	
9	THINK	file_upload	RATIO	4.8s	ok	
9	ACT	file_upload	RATIO	419ms	completed	1
9	LEARN	file_upload	RATIO	7.2s	completed	1
10	OBSERVE	-	-	12.9s	ok	
10	THINK	csrf	RATIO	5.2s	ok	
10	ACT	csrf	RATIO	528ms	completed	2
10	LEARN	csrf	RATIO	957ms	completed	2
11	OBSERVE	-	-	12.9s	ok	
11	THINK	brute_force	RATIO	4.8s	ok	
11	ACT	brute_force	RATIO	1.1s	completed	1
11	LEARN	brute_force	RATIO	25.1s	completed	1
12	OBSERVE	-	-	11.6s	ok	
12	THINK	stored_xss	RATIO	4.3s	ok	
12	ACT	stored_xss	RATIO	1.1s	completed	1
12	LEARN	stored_xss	RATIO	17.1s	completed	1
13	OBSERVE	-	-	10.8s	ok	
13	THINK	cmdi_shell	RATIO	4.7s	ok	
13	ACT	cmdi_shell	RATIO	502ms	completed	2
13	LEARN	cmdi_shell	RATIO	7.5s	completed	2
14	OBSERVE	-	-	10.4s	ok	
14	THINK	commix	RATIO	1ms	ok	
14	ACT	linpeas	RATIO	0.0s	skipped	
15	OBSERVE	-	-	13.7s	ok	
15	THINK	commix	RATIO	0.0s	ok	
15	ACT	winpeas	RATIO	0.0s	skipped	
16	OBSERVE	-	-	12.2s	ok	
16	THINK	commix	RATIO	1ms	ok	
16	ACT	chisel	RATIO	0.0s	skipped	
17	OBSERVE	-	-	11.6s	ok	
17	THINK	commix	RATIO	1ms	ok	
17	ACT	lateral_sim	RATIO	0.0s	skipped	
18	OBSERVE	-	-	12.6s	ok	
18	THINK	commix	RATIO	9ms	ok	
18	ACT	commix	RATIO	579ms	skipped	
18	LEARN	commix	RATIO	16ms	skipped	
19	OBSERVE	-	-	11.8s	ok	
19	THINK	post_ex	ANIMUS	9ms	ok	

19	ACT	post_ex	ANIMUS	4ms	lex_blocked
19	LEARN	post_ex	ANIMUS	27ms	lex_blocked
20	OBSERVE	-	-	13.3s	ok
20	THINK	post_ex	ANIMUS	6ms	ok
20	ACT	post_ex	ANIMUS	0.0s	lex_blocked
20	LEARN	post_ex	ANIMUS	15ms	lex_blocked
21	OBSERVE	-	-	11.3s	ok
21	THINK	post_ex	ANIMUS	3ms	ok
21	ACT	post_ex	ANIMUS	0.0s	lex_blocked
21	LEARN	post_ex	ANIMUS	14ms	lex_blocked

09 PLAN NAPRAWCZY

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