Politechnika Wrocławska

Analiza i eksploitacja podatności w DVWA

Politechnika Wrocławska

Spis treści

Politechnika Wrocławska

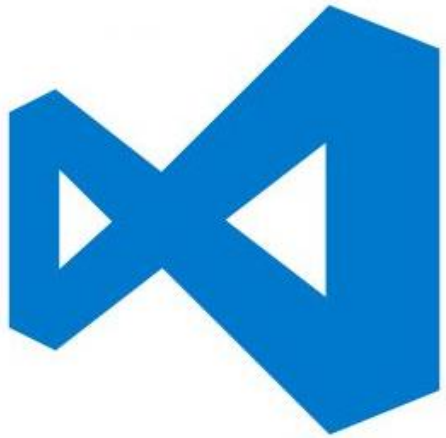
Cel projektu

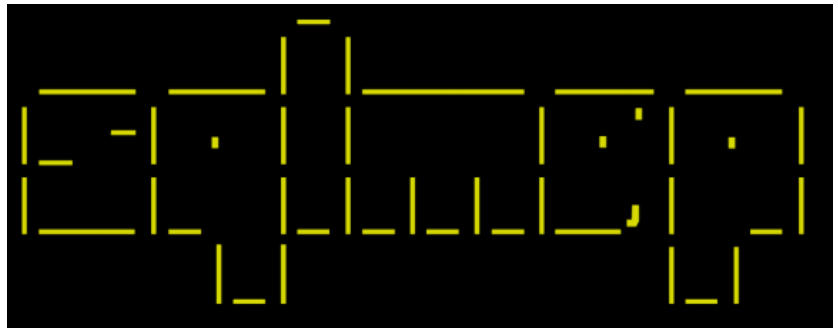
Celem naszego projektu była analiza i praktyczne wykorzystanie podatności zawartych w aplikacji DVWA. Skupiliśmy się na:

- Identyfikacji jak największej liczby podatności,
- Zrozumieniu mechanizmów ich działania,
- Opracowaniu skutecznych metod ich eksploitacji,
- Automatyzacji najważniejszych ataków przy użyciu własnych skryptów.

Politechnika Wrocławska

Środowisko testowe





Politechnika Wrocławska

Czym jest DVWA?

DVWA (Damn Vulnerable Web Application) to celowo podatna aplikacja internetowa napisana w PHP i MySQL.

Jej głównym celem jest nauka testowania zabezpieczeń aplikacji webowych w bezpiecznym, kontrolowanym środowisku.

Politechnika Wrocławska

Wykryte podatności

- Brute force
- Command Injection
- XSS – Stored
- XSS - Reflected
- XSS – DOM
- SQL Injection (zwykłe i blind)
- Open HTTP Redirect
- Cryptography
- CSP Bypass
- Weak Session IDs
- Authorization bypass
- CSRF
- File Inclusion (LFI/RFI)

Politechnika Wrocławska

Automatyzacja eksploitacji – przygotowanie

Każdy skrypt ataku zawiera:

- Zmienne konfiguracyjne (dane logowania, adresy URL)
- Funkcję login() – logowanie do DVWA z użyciem tokena
- Funkcję set_security_low() – ustawienie poziomu zabezpieczeń na "Low"

Dzięki temu:

- Środowisko testowe jest zawsze gotowe
- Eksploitacja działa automatycznie i spójnie
- Możemy szybko testować różne podatności bez ingerencji ręcznej

```python
import requests
from bs4 import BeautifulSoup
import subprocess

LOGIN_URL = "http://localhost/DVWA/login.php"
SECURITY_URL = "http://localhost/DVWA/security.php"
VULN_URL = "http://localhost/DVWA/vulnerabilities/sqli/"
USERNAME = "admin"
PASSWORD = "password"

session = requests.Session()

def login():
    print("[*] Logowanie do DVWA...")
    r = session.get(LOGIN_URL)
    soup = BeautifulSoup(r.text, "html.parser")
    token = soup.find("input", {"name": "user_token"})["value"]

    payload = {
        "username": USERNAME,
        "password": PASSWORD,
        "Login": "Login",
        "user_token": token
    }

    session.post(LOGIN_URL, data=payload)
    print(f"[+] Zalogowano na DVWA z danymi: {USERNAME} / {PASSWORD}")

def set_security_low():
    print("[*] Ustawianie poziomu zabezpieczeń na LOW...")
    r = session.get(SECURITY_URL)
    soup = BeautifulSoup(r.text, "html.parser")
    token = soup.find("input", {"name": "user_token"})["value"]

    payload = {
        "security": "low",
        "seclev_submit": "Submit",
        "user_token": token
    }

    r = session.post(SECURITY_URL, data=payload)
    if "Security level set to low" in r.text:
        print("[+] Poziom zabezpieczeń ustawiony na LOW.")
    else:
        print("[-] Nie udało się ustawić poziomu zabezpieczeń.")

```

Politechnika
Wrocławska

Live demo - podatności + dokumentacja

Politechnika Wrocławska

Podsumowanie

- **DVWA** to świetne środowisko do nauki ataków webowych w praktyce.
- Zidentyfikowano i wykorzystano **13 różnych podatności**, w tym SQL Injection, XSS, RFI, CSRF, itp.
- Automatyzacja pozwoliła na szybsze testy, powtarzalność, oraz skalowalność, przez co pełni ważną rolę w audycie bezpieczeństwa.
- Najczęstsze przyczyny luk to brak walidacji danych, słabe zarządzanie sesją, oraz brak zabezpieczeń jak CSP czy CSRF tokeny.
- Wykonanie projektu pomogło nam uzmysłowić, że nawet proste aplikacje są podatne, a zrozumienie mechanizmów ataku to podstawa skutecznej obrony.

Politechnika Wrocławska

Dziękujemy za uwagę!