OWASP Juice Shop - CTF

Jakub Łomzik, Natalia Staroń

Plan prezentacji

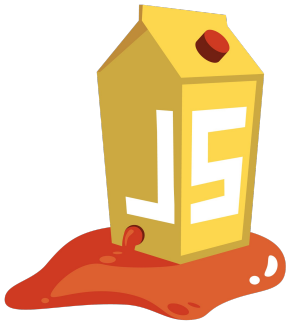
1. OWASP
2. Juice Shop
3. CTF
4. OWASP Top 10
5. Podsumowanie podatności
6. Zadania

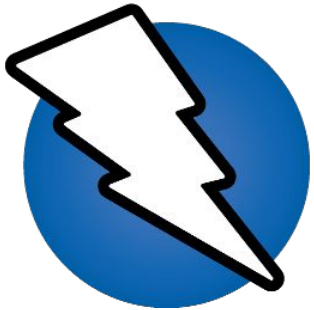
Czym jest OWASP?

- **Open Web Application Security Project** - społeczność internetowa powstała w 2001 r. prowadzona przez OWASP Foundation. Zajmuje się tworzeniem powszechnie dostępnych artykułów, dokumentacji, narzędzi i technologii w zakresie bezpieczeństwa aplikacji webowych. Celem organizacji jest **zwiększenie bezpieczeństwa oprogramowania**.

Projekty OWASP

- Amass
- Juice Shop
- Top Ten
- ZAP (Zed Attack Proxy)
- … jeszcze 234 inne





Czym jest Juice Shop?

Juice Shop

- niezabezpieczona aplikacja webowa
- kursy bezpieczeństwa, CTFy, testowanie narzędzi
- podatności z projektu **OWASP Top Ten** spotykane w realnych sytuacjach
- **JavaScript**: Node.js, Express, Angular
- “Saftladen” ⟶ “Juice shop”

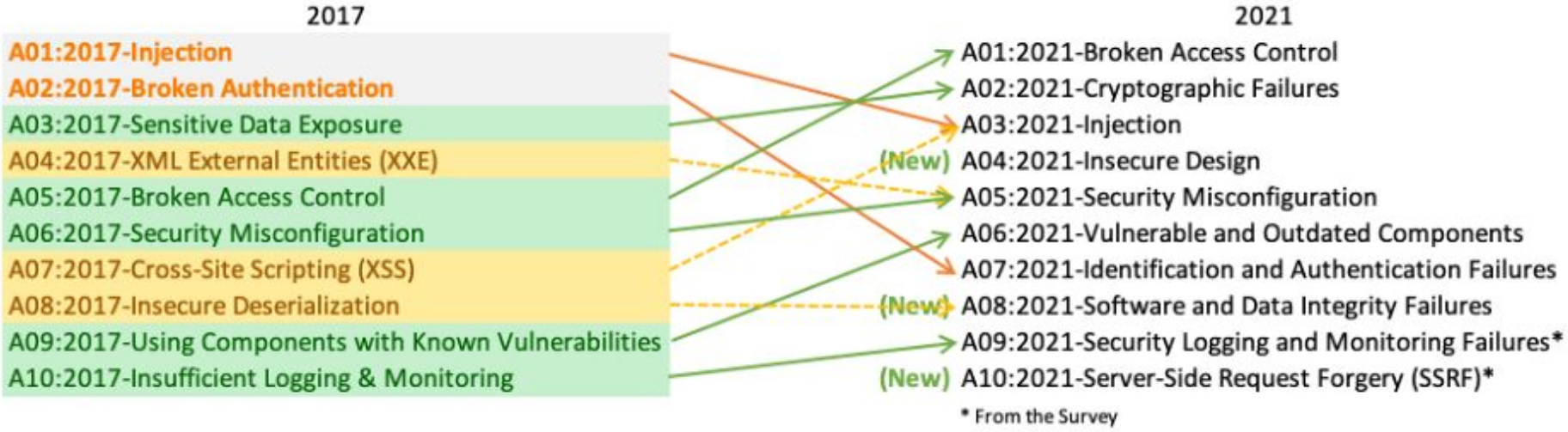
Czym jest CTF?

CTF - Capture the Flag

- kategorie:
  - Jeopardy
  - Attack - Defense
- wydarzenia:
  - Insomni'hack
  - GoogleCTF
  - DEF CON
- strony internetowe:
  - tryhackme.com
  - hackthebox.eu

Hack In The Box Security Conference

OWASP Top 10



Zmiany pomiędzy edycjami 2017 i 2021

Broken Access Control

- dostęp do danych poza uprawnieniami
- Cross-Site Request Forgery (CSRF)
- Server-Side Request Forgery (SSRF)
- Cross-Site Scripting (XSS)
- XML External Entity (XXE)

Injection

- przesłanie zapytania w formie złośliwego kodu
- SQL Injection
- HTML Injection
- OS command Injection
- Server-Side Template Injection (SSTI)

CVE-2021-44228 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

QUICK INFO

CVE Dictionary Entry:
CVE-2021-44228
NVD Published Date:
12/10/2021
NVD Last Modified:
01/12/2022
Source:
Apache Software Foundation

NIST NVD - baza danych podatności

Podsumowanie podatności

- SQL Injection
- HTML Injection
- Server-Side Template Injection (SSTI)
- Cross-Site Request Forgery (CSRF)
- Server-Side Request Forgery (SSRF)
- Cross-Site Scripting (XSS)
- XML External Entity (XXE)
- Heartbleed

Zadania

Źródła

- https://owasp.org/
- https://owasp.org/www-project-top-ten/
- https://owasp.org/Top10/A01_2021-Broken_Access_Control/
- https://owasp.org/Top10/A03_2021-Injection/
- https://pwning.owasp-juice.shop/part1/ctf.html
- https://pwning.owasp-juice.shop/appendix/solutions.html

Dziękujemy za uczestnictwo