Autor: Ruxandra F. Olimid
Departamentul de Informatică, Universitatea din București

- Laborator Modul 4 -
Ethical hacking

Disclaimer: Pe parcursul acestui curs/laborator vi se vor prezenta diverse noțiuni de securitate informatică, cu scopul de a învăța cum să securizați sistemele. Toate noțiunile și exercițiile sunt prezentate în scop didactic, chiar dacă uneori se presupune să gândiți ca un adversar. Nu folosiți aceste tehnici în scopuri malițioase! Acestea pot avea consecințe legale în cazul comiterii unor infracțiuni, pentru care deveniți pe deplin răspunzători!

1. Google Gruyere

Google Gruyere este disponibil online [1]. Urmați tutorialul pentru a răspunde la următoarele cerințe.

Exercițiul 1.1. Porniți o instanță Gruyere (online sau local. **Atenție!** Pentru partea a doua a laboratorului aveți nevoie de o instanță locală). Urmați pașii din **Using Gruyere.** Creați un cont, adăugați un snippet și o poză de profil (icon), adăugați un fișier. Păstrați informațiile pentru că vă sunt necesare pentru următoarele exerciții.

Exercițiul 1.2. Urmați pașii din **File Upload XSS.** Creați și adăugați un fișier care permite rularea unui script.

Exercițiul 1.3. Urmați pașii din **Reflected XSS.** Găsiți un URL care să permită rularea unui script.

Exercițiul 1.4. Urmați pașii din **Stored XSS.** Adăugați un script care să deservească și altui utilizator.

Exercițiul 1.5. Urmați pașii din **Elevation of Privilege.** Transformați contul creat într-un cont de administrator.

Exercițiul 1.6. Urmați pașii din **Cookie Manipulation.** Obțineți un cookie pentru un alt cont.

Exercițiul 1.7. Urmați pașii din **XSRF Challenge.** Obțineți o modalitate de ștergere a înregistrărilor de tip snippet.

Exercițiul 1.8. Urmați (cel puțin una dintre) modalitățile de citire a bazei de date conform **Configuration Vulnerabilities.**

Exercițiul 1.9. Exemplificați orice altă vulnerabilitate a *Google Gruyere*.

2. ZAP

 Rulați *Google Gruyere* local. Pentru aceasta, urmați pașii din **Running locally**, tutorial disponibil online [1].

 Instalați *ZAP*, disponibil online [2]. Verificați după instalare dacă sunt există update-uri *(Help > Check for Updates)* - în caz contrar este posibil să întâmpinați erori la lansarea browser-ului. Pentru instalare, cât și pentru realizarea exercițiilor următoare, citiți cu atenție pașii din tutorialul [3], *day-1-day-4*.

Exercițiul 2.1. Realizați o scanare manuală a *Gruyere* lansat local. Verificati tab-urile *History* și *Alerts*. Explicați o vulnerabilitate la alegere.

Exercițiul 2.2. Folosiți *Manual Request Editor*. Gasiți request-ul de login, rulați din nou, manual, cererea de login, mai intai cu utilizatorul creat de dvs. și apoi cu niște credențiale oarecare (invalide). Observați diferența în tab-ul *Response*.

Exercițiul 2.3. Pornind de la un request de adăugare snippet, reluati request-ul în mod manual cu un alt snippet și verificati impactul. Ștergeți cookie-ul. Ce se întâmplă? Cum considerați acest comportament?

Exercițiul 2.4. Rulați un atac de tip *dictionary attack* pentru utilizatorul *Brie* folosind *fuzzing*. Adăugați în lista de parole parola corectă, găsită în **Exercițiul 1.8**.

3. CTF - Reverse Engineering

 Instalați *IDA Free*, disponibil online [4]. Folosiți *IDA Free* pentru rezolvarea următoarelor două probleme de tip *Capture-The-Flag (CTF)*.

Notă: Flag-urile pot fi recuperate și prin alte metode. Indiferent de metoda aleasă, trebuie să arătați cum le puteți găsi în IDA Free.

Dacă nu aveți deja, creați un cont pe platforma *CyberEDU* [5].

Exercițiul 3.1. Problema **yopass-go** este disponibilă pe platforma CyberEDU [6]

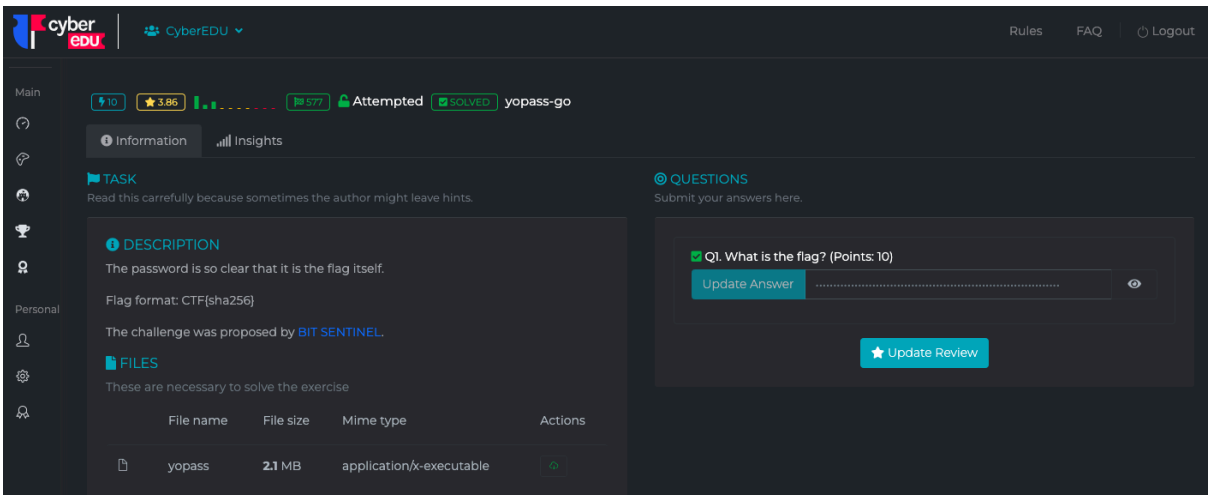

Fig.1. yopass-go [6]

Exercițiul 3.2. Problema **better-cat** este disponibilă pe platforma CyberEDU [7]:

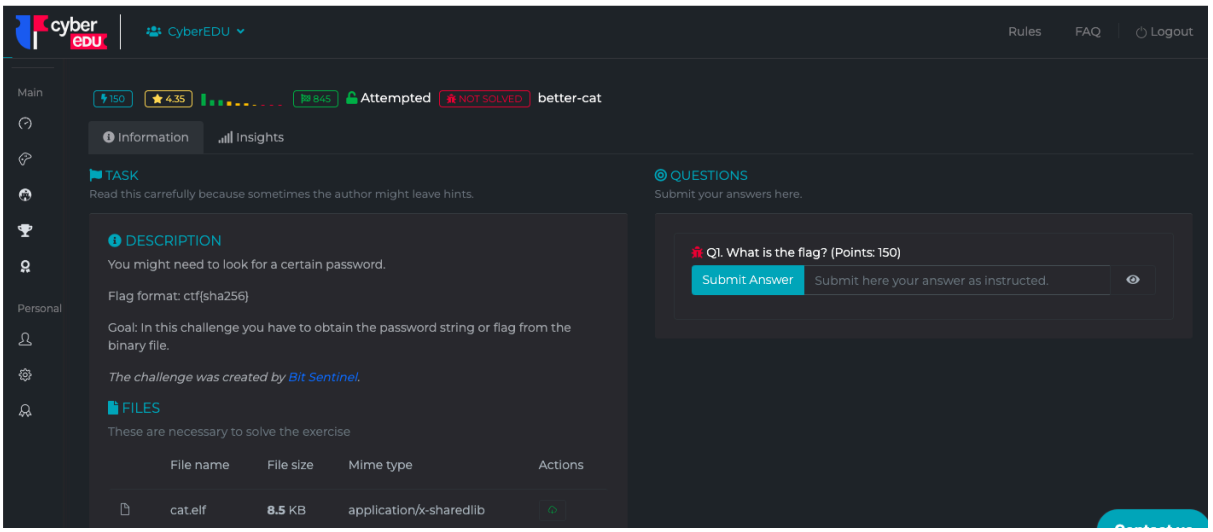

Fig.2. better-cat [7]

Referințe bibliografice

1. Google Gruyere. *Web application exploits and defenses.* Accesibil la: https://google-gruyere.appspot.com/ Ultima accesare: aprilie 2024.
2. Zed Attack Proxy (ZAP). Accesibil la: https://www.zaproxy.org/ Ultima accesare: aprilie 2024.
3. Mic Whitehorn. *Twelve Days of ZAPmas.* Accesibil la: https://www.secureideas.com/blog/twelve-days-of-zapmas-day-1-setting-up-zap Ultima accesare: aprilie 2024.
4. Hex-Rays. IDA Free. Accesibil la: https://hex-rays.com/ida-free/ Ultima accesare: aprilie 2024.
5. *CyberEDU*. Accesibil la: https://cyber-edu.co/ Ultima accesare: aprilie 2024.
6. BIT Sentinel. *yopass-go.* D-CTF 2020 Online. Tag: *Reverse Engineering*, Estimated Difficulty: *Entry Level*. Accesibil la: https://cyber-edu.co/ Ultima accesare: aprilie 2024.
7. BIT Sentinel. *yopass-go.* D-CTF 2020 Online. Tag: *Reverse Engineering*, Estimated Difficulty: *Entry Level*. Accesibil la: https://cyber-edu.co/ Ultima accesare: aprilie 2024.