

UNIVERSITATEA DIN BUCUREȘTI

FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ

SPECIALIZAREA MATEMATICĂ-INFORMATICĂ

LUCRARE DE LICENȚĂ

Web Application Vulnerability Scanner

COORDONATOR ȘTIINȚIFIC: ABSOLVENT:

Conf. Dr. RUXANDRA OLIMID NĂIBOIU TEODOR

BUCUREȘTI, IUNIE 202

Cuprins

[Introducere 5](#_Toc73728328)

[Capitolul 1. Tehnologii și Instrumente 7](#_Toc73728329)

[1.1 Python 7](#_Toc73728330)

[1.2 Requests 7](#_Toc73728331)

[1.3 Urllib 8](#_Toc73728332)

[1.3.1 Urllib.parse 8](#_Toc73728333)

[1.3.2 Urllib.request 8](#_Toc73728334)

[1.4 BeautifulSoup4 8](#_Toc73728335)

[1.4.1 BeautifulSoup 8](#_Toc73728336)

[1.5 SSL 9](#_Toc73728337)

[1.6 Socket 9](#_Toc73728338)

[1.7 Subprocess 10](#_Toc73728339)

[1.8 Threading 10](#_Toc73728340)

[1.9 Tkinter 10](#_Toc73728341)

[1.10 OS 11](#_Toc73728342)

[1.11 Re 11](#_Toc73728343)

[1.12 ConfigParser 11](#_Toc73728344)

[1.13 Metasploitable 2 12](#_Toc73728345)

[1.13.1 DVWA 12](#_Toc73728346)

[1.14 Alte tehnologii utilizate 13](#_Toc73728347)

[Capitolul 2. Vulnerabilitățile aplicațiilor web 14](#_Toc73728348)

[2.1 Injections 14](#_Toc73728350)

[2.1.1 SQL Injections 15](#_Toc73728351)

[2.1.2 NOSQL Injections 15](#_Toc73728352)

[2.1.3 OS Command Injection 16](#_Toc73728353)

[2.2 Broken Authentication 16](#_Toc73728354)

[2.2.1 Credential stuffing 16](#_Toc73728355)

[2.2.2 Session attacks 18](#_Toc73728356)

[2.3 Sensitive Data Exposure 19](#_Toc73728357)

[2.4 XML External Entities (XXE) 19](#_Toc73728358)

[2.5 Broken Access Control 20](#_Toc73728359)

[2.6 Security Misconfiguration 20](#_Toc73728360)

[2.7 Cross-Site Scripting (XSS) 21](#_Toc73728361)

[2.7.1 Reflected XSS 21](#_Toc73728362)

[2.7.2 Stored XSS 21](#_Toc73728363)

[2.7.3 DOM XSS 22](#_Toc73728364)

[Capitolul 3. Arhitectura aplicației și implementarea testelor 23](#_Toc73728365)

[3.1 Parsarea variabilelor din fișierul de configurare 23](#_Toc73728367)

[3.2 Clasa LoginTests 24](#_Toc73728368)

[3.3 Clasa OtherUser 27](#_Toc73728369)

[3.4 Clasa GUI 28](#_Toc73728370)

[3.5 Clasa Scanner 32](#_Toc73728371)

[3.5.1 Extragerea informațiilor 34](#_Toc73728372)

[3.5.2 Aplicarea testelor asupra informațiilor 38](#_Toc73728373)

[1. References 43](#_Toc73728374)

**Abstract**

Proiectul care urmează să fie prezentat în această lucrare este o aplicație software de tipul *scanner* destinată dezvoltatorilor de siteuri web și persoanelor care se ocupă cu testarea și asigurarea securității și integrității acestora. *Scannerul* are ca scop indetificarea și raportarea breșelor de securitate găsite în procesul de testare automată numită și *scanare*. Utilizatorii aplicației pot interacționa diferit cu aceasta în funcție de sistemul de operare pe care aceștia aleg să execute scanarea. Pe sistemele Windows aplicația dispune de un *graphical user interface* (GUI) cu care utilizatorul poate interacționa, toate informațiile despre folosirea *scannerului* fiind puse la dispoziție de către interfață. Pe sistemele Linux aplicația trebuie folosită prin intermediul unui terminal, toată interacțiunea fiind realizată exclusiv prin linia de comandă. Odată ce utilizatorul introduce datele aplicației pe care acesta dorește să o supună testării, tot ce rămâne de făcut este să pornească scanarea și să aștepte raportul generat. La final aplicația printează informații cu privire la raport și ghidează utilizatorul către fișierele generate pentru vizualizarea rezultatelor detaliate.

Din cauza diversității metodelor de implementare ale unei aplicații web, acestea sunt predispuse la mici erori de proiectare. Aceste erori cauzează, în majoritatea cazurilor, apariția vulnerabilităților în sistemele care manageriază aceste aplicații. Este nevoie de astfel de unelte care să ajute la depistarea și rezolvarea acestor erori într-un interval cât mai scurt de timp.

# Introducere

Securitatea este, simplu spus, libertatea fata de risc sau pericol [1]. Fiind una dintre nevoile fundamentale umane, oamenii și-au dedicat o lungă perioadă din viață în căutarea a noi metode inovative și eficiente pentru a combate pericolele născute fie din natură, cum ar fi eventimentele meteorologice, animalele, virusurile și bacteriile, fie născocite chiar de aproapele lui. Astfel, cu timpul, am fost nevoiți să ne adăpostim în locuințe confecționate în asa fel încât acestea să asigure protecție față de orice pericol provenit din exteriorul acestora. Pe măsură ce evoluăm ca specie, această nevoie de protecție crește proporțional cu riscurile cauzate de avansul, atât tehnologic cât și evoluționar al omului.

Foarte asemănătoare nouă este și evoluția securității informației. Am observat cum imediat după apariția internetului a fost nevoie de metode nemaiîntâlnite de a ne proteja informațiile și datele personale, păstrate până în acel moment în seifuri sau în locații bine păzite. Apariția internetului ne-a deschis, deci, porțiile către o noua lume mai conectată și cu o mulțime de noi posibilități dar și noi pericole, noi riscuri asociate acestei invenții.

Astăzi securitatea informației, sau securitatea cibernetică, joacă un rol extrem de important în buna funcționare a societății. Ea se definește ca diverse procese și practici ce au rolul de a proteja rețele, *device-uri*, programe și date în fața atacurilor, distrugerilor sau a accesului neautorizat [2].

Recent am fost martorii unui atac cibernetic de tipul *Ransomware* care a avut ca țintă “Colonial Pipeline”, o rețea de distrubuție de combustibil aflată în partea de Est a Statelor Unite. Atacul a cauzat o scădere a aprovizionării stațiilor de alimentare cu combustibil, având astfel un impact ridicat asupra economiei zonei afectate, producând daune de milioane de dolari și instaurând o panică generală în rândul cetățenilor [3]. Observăm astfel impactul dezastruos pe care o breșă de securitate îl poate avea atât pe plan politic și economic cât și psihologic.

Am văzut mai sus un singur tip de atac cibernetic, în realitate există o mulțime de astfel de atacuri de diferite forme și cu diferite intenții. Unele dintre ele sunt cauzate de conflicte politice, economice, iar altele din simplul motiv de a demonstra abilitățiile atacatorilor. O bună parte dintre aceste atacuri țintesc aplicațiile Web, cunoscute și sub numele de *siteuri web.* O aplicație web este un program care utilizează un *browser web* și metode *web* pentru a îndeplinii diverse atribuții pe internet [4]. Din cauza frecventelor interacțiuni umane cu aceste aplicații, riscul ca ele să devină ținta atacurilor cibernetice este unul foarte ridicat, astfel specialiștii în securitate cibernetică au investit timp și efort sporit în scopul securizării lor.

Securizarea aplicațiilor *web* este, pe zi ce trece, din ce în ce mai importantă. În fiecare zi zeci de milioane de persoane își încredințează atăt datele persoanale căt și confidențialitatea acestor aplicații, sarcina de a asigura această confidențialitate fiind pe umerii dezvoltatoriilor acestor *aplicații.* Totuși pe zi ce trece se descoperă noi vulnerabilități și noi atacuri din care un număr ridicat de oameni are de suferit. Așadar, dezvoltatorii și analiștii în securitate nu pot face față acestor atacuri fiind nevoie de un efort proactiv în securizarea aplicațiilor. Chiar și așa, din cauza numărului ridicat de metode intruzive, un dezvoltator este predispus să piardă din atenție un detaliu care se poate dovedi un punct critic în cazul realizării unui astfel de atac. Deci este nevoie de unelte din ce în ce mai performante și mai eficiente prin care astfel de catastrofe să fie evitate.

Acum că am definit conceptul de *aplicație web* este timpul să ne familiarizăm cu metodele prin care o astfel de aplicație este supusă testelor de siguranță înainte ca aceasta să fie disponibilă publicului. În mod normal, pentru a evita un atac, testerul se asigură că aplicația îndeplinește niște norme de securitate standard definite de OWASP [5].

Așadar în capitolele care urmează am să prezint o aplicație destinată în principal dezvolatorilor dar și testerilor, care are ca scop automatizarea proceselor de testare definite de OWASP și încapsularea lor într-o aplicație software. Interesul pentru această temă este datorat curiozității, cât și pasiunii mele pentru securitatea cibernetica, în special pentru securitatea *aplicațiilor web.* Astfel am decis să creez un program care să usureze procesul de securizare al aplicației și să minimizeze timpul petrecut practicând testele manual și erorile umane apărute pe parcursul acestora.

Consider că realizarea acestei lucrări a fost o provocare din care am reusit să-mi aprofundez cunoștiințele despre domeniul securitații și cred că rezultatul poate fi folosit de oricine dorește să dezvolte sau să testeze o *aplicațe web.*

# Capitolul 1. Tehnologii și Instrumente

Proiectul este realizat utilizând limbajul de programare Python. În cadrul acestui proiect am folosit diverse module. Un modul este un fișier Pyhon cu diverse definiții și instrucțiuni. Printre cele mai importante module folosite se numără modulul *requests,* folosit pentru a comunica cu *aplicația web*, modulul *urllib* folosit pentru manipularea adreselor *web*, modulul *BeautifulSoup4* pentru extragerea informațiilor, și alte module utile despre care urmează să vorbim în subcapitolele următoare.

## Python

Pyhon este un limbaj de programare util pentru aproape orice aplicație. Este un limbaj interpretat, orientat pe obiect cu o colecție vastă de module și o sintaxa atragătoare. Datorită asemănării lui cu limbajul *bash* și capacității sale de a executa o multitudine de operații des întâlnite în securitatea cibernetica, cât și a colecției impresionante de module special create pentru *Penetration Testing*, Pyhon a fost mereu limbajul preferat de inginerii de securitate și testeri.

Poate cel mai important avantaj al limbajului Pyhon în acest domeniu îl reprezintă rapiditatea cu care pot fi rezolvate problemele, implementarea codului și rezolvarea erorilor fiind mult mai rapidă în comparație cu alte limbaje de programare.

## Requests

Requests este un modul Python care permite utilizatorului să interacționeze cu *request-urile* de tip *Hypertext Transfer Protocol* (HTTP) într-un mod simplu și rapid. Un *request* este o acțiune realizată asupra unei resurse aflate la o anumită adresa *web,* cu alte cuvinte, este o cale intermediară care transportă informații între client (sau *browser*) și server. Tipurile de *request-uri* variază în funcție de scopul acestora. În total există un număr de nouă tipuri de astfel de *request-uri* dar cele mai importante și cele pe care le-am folosit în dezvoltarea acestei lucrări sunt: GET, POST, PUT, DELETE [6].

GET este folosită pentru a obține date de la server.

DELETE șterge o anumită resursă specificată în *request*.

PUT este metoda folosită pentru a modifica reprezentăriile unei stări existente, cu o reprezentare nouă, definită în procesul de *request*.

POST este metoda specifică pentru a trimite date noi către server. Poate fi folosită pentru a actualiza și a crea noi date pe server.

## Urllib

Urllib este un modul care are în componența lui două module importante pe care le-am folosit.

### Urllib.parse

Modulul urllib.parse este folosit pentru manipularea și modificarea *Uniform Resource Locator* (URL). Cu ajutorul acestui modul, putem fragmenta, combina și extrage fragmente din URL-uri [7].

### Urllib.request

Modulul urllib.request definește instrucțiuni de cod utile pentru accesarea și interacțiunea cu metodele HTTP. Modulul ne furnizează un mod de comunicare puțin mai avansat decât modulul *requests* [8].

## BeautifulSoup4

Din componența modulului BeautifulSoup4 am folosit modulul cu acelasi nume, adică BeautifulSoup [9].

### BeautifulSoup

Modulul BeautifulSoup este cel mai folosit modul în Pyhon pentru preluarea informațiilor din paginile *web.* În principal am folosit acest modul drept metodă de extragere a diverselor părți componente din codul sursă al paginii *web.* Este eficient în preluarea datelor de tipul HTTP și *Extensible Markup Language* (XML).

## SSL

Modulul SSL (*Secure Sockets Layer)* este un modul care permite accesul la TLS (*Transport Layer Security).* Pentru ca datele noastre *online* să fie securizate este nevoie de protocoale criptografice care să codeze aceste date în secvențe de litere și cifre aleatoare și indescifrabile pentru om. Protocolul SSL folosește un sistem de criptare cu două chei, o cheie publică și o cheie privată. Pentru decodarea mesajului este nevoie de ambele chei, astfel doar persoanele autorizate pot să aibă acces la datele criptate în mesajul transmis.

Acest modul se foloseste pentru interacțiunea cu certificatul de securitate al aplicației *web*, cunoscut și sub numele de *SSL Certificate.* Un astfel de certificate asigură utilizatorii că transferul datelor dintre *browserul* lor și aplicația *web* se realizează printr-un canal criptat, astfel datele fiind protejate și confidențiale.

Folosit împreuna cu modulul *socket* acest modul poate obține informații detaliate despre certificatele SSL [10].

## Socket

Modulul socket definește o gama largă de procedee care au ca scop conectarea a două noduri de rețea pentru a favoriza comunicarea între ele.  
Procesul prin care două noduri de rețea realizează o conexiune este usor explicat daca ne imaginăm că un nod așteaptă un răspuns de la un nod care încearcă să comunice cu acesta. Acest proces simulează o conexiune între un client și un server.

Un socket definește un *endpoint* într-o rețea, astfel, socketul crează un canal bidirecțional de comunicare folosindu-se de adresa *Internet Protocol* (IP) și de un port deschis pe aplicație. Un *endpoint* este un *device* conectat la o rețea. [11].

## Subprocess

Un proces este definit ca un program care se află în execuție. Astfel de procese sunt controlate de *Central Processing Unit* (CPU) și reprezintă o mulțime de calcule efectuate de procesor (CPU) într-un interval foarte scurt de timp. Aceste procese se află într-o continuă execuție secvențială, astfel, un program execută mereu un singur proces.

Modulul Subprocess este folosit pentru a crea, a distruge sau a interacționa cu aceste procese. Așadar utilizăm acest modul pentru a interacționa direct cu diverse programe, prin intermediul unei altei aplicații, procesul nou creat fiind integrat în *firul* principal de execuție.

Definim un *fir* de execuție drept un set de astfel de procese care sunt executate pe rand și într-o ordine bine definită și determinată de CPU [12].

## Threading

Un *thread* este o modalitate prin care putem executa mai multe procese în același timp. Putem să asemănăm *thread-urile* cu mai multe programe care rulează concomitent și independent unele față de altele. În aplicațiile în care avem nevoie ca mai multe instrucțiuni să fie executate în același timp și în care există riscul ca execuția unei bucăți de cod să blocheze execuția alteia, creăm astfel de *fire de execuție* care fragmenează instrucțiunile programului și comunică cu CPU pentru a aloca memorie separată pentru *firul de execuție* folosit [13].

## Tkinter

Modulul Tkinter este o suită populară de unelte folosite pentru a crea interfețe grafice.

Tkinter a fost construit cu scopul de a oferi simplitate și diversitate în alcătuirea unei interfațe grafice cât mai atrăgătoare și intuitive.

Structura Tkinter este realizată dintr-o fereastră simplă, dar ușor customizabilă prin metode implicite, astfel adaugarea unui buton, unei liste de conținut sau mesajelor de ajutor poate fi realizată în doar câteva linii de cod. Asupra ferestrei simple, se aplica diverse modificări și funcționlități care, utilizând modului *threading,* rulează în paralel cu execuția din spatele interfeței grafice, oferind astfel o interacțiune placută între utilizator și aplicație.

Pe lângă modului Tkinter, sunt des întâlnite și modulele PyQt5, Kivy, wxPython, PyFrosm, utilitatea lor fiind dată de scopul aplicației [14].

## OS

Prin intermediul modulului OS putem interacționa eficient cu sistemul de operare pe care rulează aplicația. Acest modul este indispensabil în interacțiunea cu fișiere, căi sau pentru diversele modificări pe care putem să le aducem acestora. Avantajul folosirii acestui modul este dat de transparența față de sistemul de operare. Sintaxa modulului comunică eficient cu sistemul de operare indiferent de sistemul pe care acesta rulează. Spre exemplu sintaxa *os.stat(path)* returnează informații despre calea dată ca argument indiferent dacă aceasta este o cale a sistemului *Windows* sau a sistemului *Unix* [15]*.*

## Re

Numele modulului Re este un acronim pentru *Regular expression*. Re este un set de caractere speciale (*patttern-uri)* folosit pentru căuta și a potrivi diverse șiruri de caractere care îndeplinesc regula definită în expresia specială (*regular expression).*

Un exemplu de o astfel de regulă este *“ \d.\* ”* care,aplicată pe șirul *“Ana are 5 mere”,* găsește subșirul “*5 mere”.* Acest modul este util în extragerea informațiilor de orice formă din orice șir de caractere [16].

## ConfigParser

Este o practică standard ca majoritatea aplicațiilor să folosească un fișier de configurare pentru a oferi flexibilitate și libertate utilizatorului. Pentru a exista comunicare între un astfel de fișier și codul aplicației, este nevoie de o metodă prin care limbajul de programare să comunice cu limbajul din fișierul de configurare.

Modulul ConfigParser oferă posibilitatea de a accesa astfel de fișiere de forma *nume\_fișier.ini* și de a traduce datele astfel încât limbajul aplicației să le înțeleagă. În felul acesta datele variabile sunt ușor de configurat de oricine, crescând potențialul aplicației pentru o gamă mai largă de utilizări.

## Metasploitable 2

Metasploitable 2 este o versiune de Ubuntu Linux, alcătuită special din cod nesecurizat, fiind astfel o colecție de servicii vulnerabile din punctul de vedere al securitații. Principalul scop al acestui sistem este de a pune la dispoziție un mediu sigur, închis, care să faciliteze practicile comune de testare, de învățare și de practicare a diverselor metode sau ustensile folosite în procesul învățării conceptelor de securitate cibernetică.

Sistemul conține nenumărate vulnerabilițăți adaugate intenționat sau neintenționat pentru a putea susține aproape orice tip de abordare și pentru a oferi totodată un mediu legal în care profesioniștii dar și persoanele interesate pot să exerseze și să capete mai multe cunoștiințe.

Datorită faptului că aplicația are la baza un sistem Linux, regăsim pe aceasta un server *web,* care susține o mică suită de aplicații web vulnerabile, fiecare cu numele ei reprezentativ. Printre aplicațiile vulnerabile se află aplicația *Damn Vulnerable Web App* (DVWA) care conține o colecție variată de vulnerabilități comune și des întalnite pe *site-urile web* [17].

### DVWA

DVWA este aplicația preferată pentru testarea conceptelor securității *web* datorită numărului ridicat de vulnerabilități existente pe aceasta și interfeței orientative. Aplicația este folosită nu doar de profesioniști, ci și de studenți, profesori, persoane interesate de securizarea aplicațiilor web sau dezvoltatori care caută un loc în care să-și testeze aplicațiile software fără a le face publice sau a încălca legea.

Am ales această aplicație atât datorită numărului ridicat de vulnerabilități cât și tehnologiilor pe care le pune la dispoziție, reușind să mimeze foarte bine aplicațiile *web* des întâlnite zi de zi. Prezența unui număr ridicat de vulnerabilități ofera o arie mai mare de acoperire pentru testele care urmează să fie făcute pe situații reale, atunci când atât tipul cât si numărul de vulnerabilițăti prezente într-o aplicație o să difere.

## Alte tehnologii utilizate

Alte module care merită menționate și care au ajutat la implementarea acestui proiect sunt module auxiliare, cu scop utilitar, care fie eficientizează programul din punctul de vedere al complexității, fie îndeplinesc mici atribuții.

Modulul *queue* care este folositor pentru implementarea unei cozi de diverse evenimente. În cazul acestui proiect, modul *queue* a eficientizat procesul prin care se testa validitatea unui șir de caractere, astfel, mai multe șiruri de caractere citite dintr-un fișier au fost încărcate și reținute în memorie prin intermediul unei astfel de cozi.

Modulul *datetime* ne oferă acces la datele calendaristice și timp. Cu ajutorul acestui modul am manipulat date de forma *ore:minute:secunde* și am reușit să aplic operații de scădere sau adunare a unor perioade de timp asupra datelor de forma specificată anterior.

Modulul *nmap* este o implementare a uneltei folosite pentru analizarea rețelelor care poartă același nume. *Network Mapper* (nmap) este folosit în special pentru maparea arhitecturii unei rețele și pentru detalierea servicilor și *host-urilor* care comunică pe aceasta. Un *host* reprezintă un calculator conectat la o rețea. Am folosit *nmap* pentru analizarea adresei IP a aplicației *web*.

Modulul *ctypes* este un modul care ne oferă tipuri de date compatibile cu limbajul C. Acest modul este folositor atunci când vrem să oprim execuția unui thread.

Modulul *shutil* oferă acces la operații de tip *high-level* pe fișiere. Aceste operații sunt ștergerea și copierea. Acest modul a fost implementat pentru a șterge fișierele temporare, create în timpul execuției.

Modulul *webbrowser* este un modul care interacționează și controlează *browserul* implicit al sistemului. Cu ajutorul acestui modul am implementat metode prin care utilizatorul poate vedea explicații detaliate disponibile pe internet cu privire la vulnerabilitățile descoperite și testate de *scanner*.

# Capitolul 2. Vulnerabilitățile aplicațiilor web

Înainte să vorbesc despre implementarea și arhitectura aplicației este nevoie să fixăm câteva noțiuni importante pe care le-am pus în practică în dezvoltarea acesteia. În acest capitol am să explic ce este o vulnerabilitate web, de câte tipuri sunt ele și cum afectează buna funcționare a unui *site web,* urmând ca în capitolul următor să explic detaliat abordarea pentru detecția acestora.

O vulnerabilitate web este o slăbiciune sau o configurare greșită a anumitor funcționalități pe care o aplicație web le îndeplinește. Uneori aceste vulnerabilități sunt abuzate de persoane rău intenționate care reușesc să preia controlul asupra aplicației pentru a obține date confidențiale în diverse scopuri personale, numim aceste persoane *hackeri* sau atacatori. În funcție de modul în atacatorii reușesc să obțina acces la resursele securizate ale aplicației web, se disting diferite tipuri de astfel de vulnerabilități.

OWASP Top Ten este documentul oficial în care sunt consemnate tipurile de riscuri la care *aplicațiile* *web* sunt supuse și tacticile de detecție și neutralizare ale acestora. Atât dezvoltatorii cât și *penetration* *testerii* urmăresc îndrumările și tehnicile însemnate în document pentru a se asigura că arhitectura *aplicațiilor web* îndeplinește ultimele standarde de securitate. Acest proiect a fost realizat conform abordărilor și metodelor menționate și documentate în lista *Web Security Testing Guide* (WSTG) din cadrul proiectului OWASP [18].

În subcapitolele care urmează am să menționez trăsăturile fiecărui tip de vulnerabilități testate și integrate în acest proiect. Pentru fiecare categorie au fost implementate diferite abordări de testare care urmează să fie detaliate în capitolul urmator.



## Injections

Tipul *Injections* reprezintă vulnerabilitățile care au la bază nesanitizarea *inputurilor* din aplicație. Acestea apar atunci cand un șir de instrucțiuni provenit din exterior este interpretat ca parte din codul aplicație, astfel instrucțiunea în cauză execută acțiuni nedorite cu potențial dăunator și intrusiv. Putem găsi acest tip de vulnerabilitate în orice cămp care primește date de la utilizator.

Cele mai populare tipuri de *injection* sunt *SQL Injections*, *LDAP Injections, OS Command Injection.*

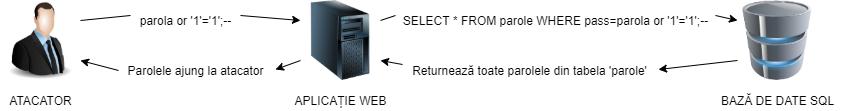
**

Figura 2.1. Exemplu SQL Injection

### SQL Injections

*Structured Query Language* (SQL) este un limbaj de programare specific bazelor de date. Astfel un *SQL Injection* este o vulnerabilitate care încearcă să manipuleze înregistrările unei baze de date cu scopul de a accesa înregistrările (*query-urile)* din componența acesteia. O astfel de practică presupune introducerea instrucțiunilor de tip SQL în *inputurile* aplicației care sunt legate la o baza de date SQL, și accesarea înregistrărilor, șirul introdus fiind astfel interpretat ca parte din limbajul SQL, permițând accesul la înregistrări la care utilizatorul nu este autorizat.

Observăm in figura 2.1 un exemplu de un astfel de *injection*. Un atacator introduce șirul de caractere “parola or ‘1’=’1’;--" care, interpretat de limbajul SQL, este o verificare în care prima parte a șirului poate fi ignorată, deoarece valoarea de adevăr a instrucțiunii ‘1’=’1’ este adevărată. La finalul șirului atacatorul introduce ‘;--‘ pentru ca *query-ul* să ignore orice se afla dupa verificarea precedentă. În felul acesta, baza de date returnează toate parolele stocate în tabela accesată atacatorului.

Pentru a preveni această vulnerabilitate soluția este găsirea unei metode care păstrează datele introduse, separat de comenzile și *query-urile* din baza de date.

### NOSQL Injections

*NOSQL Injections* sunt baze de date de tipul SQL cu mai puține restricții și constrângeri. Această tehnologie este mai eficientă computațional față de SQL.

*Injection-ul* de tip NOSQL funcționează pe același principiu ca și în cazul *SQL Injection*.

### OS Command Injection

Această vulnerabiliate este abuzată prin introducerea de comenzi care pot fi interpretate de sistemul de operare pe *serverul* pe care rulează *aplicația web* prin intermediul interfeței acesteia. Orice *input* din aplicație care nu este sanitizat cum trebuie, poate executa comenzi pe sistemul de operare.

Pentru a preveni această vulnerabilitate este nevoie ca *aplicația web* să ruleze sub niște restricții stricte care să nu permita rularea comenzilor pe *serverul* aplicației.

## Broken Authentication

Acest tip definește vulnerabilitațile aparute în urma configurării greșite a funcțiilor de autentificare și gestionare a unei sesiuni. O sesiune este o perioadă de timp definită de dezvoltatorul aplicației în care anumite date și preferințe ale utilizatorului sunt rețiune pe parcursul navigării pe *aplicația web.* O funcționalitate este că permite navigarea între paginile unui *site* fără a fi nevoie ca utilizatorul să se autentifice de fiecare dată.

Acestă vulnerabilitate este foarte răspândită în lumea *aplicațiilor web* și foarte complexă. Este foarte ușor pentru atacatori să se folosească de liste de parole și nume de utlizatori, folosind unelte automate, pentru a ghici datele de autentificare ale altor utilizatori. Este nevoie doar de un singur cont cu privilegii administrative pentru a compromite o intreagă aplicație.

Așa cum am menționat mai sus, există două tipuri importante de astfel de atacuri. Atacuri care se folosesc de vulnerabilități în implementarea funcțiilor care gestionează sesiunile, *session management*, și atacuri care vizeză datele de autentificare, cunoscute sub numele de *credential stuffing*.

### Credential stuffing

Un atac de tipul *credential stuffing* constă în încercarea de a introduce date valide în câmpul de autentificare cu speranța că atacatorul nimerește, din întâmplare, un cont valid. Atacul se realizează cu ajutorul uneltelor automatizate care dispun de liste mari ce conțin date de autentificare obținute din scurgerile de date confidențiale din trecut. Aceste liste, numite *dicționare,* conțin și parole comune, de obicei implicite pe baza că dezvoltatorii si administratorii unei aplicații uită să modifice o astfel de parolă.

Această practică este des folosită sub forma unui atac provenit din mai multe zone geografice. Un atacator se află în controlul mai multor calculatoare aflate în diferite zone, acesta lansează un atac simulan de pe toate aceste calculatoare cu scopul de a păcăli sistemele de siguranță. Acest atac este cunoscut sub numele de *Botnet*.

Acest tip de atac poate fi prevenit în multe feluri. Câteva dintre ele presupun ca dezvoltatorul să se asigure că nu a lăsat nici o parola implicită în componența aplicației, că a implementat un sistem care să nu-i permită unui utilizator să încerce să forțeze o autentificare într-un interval scurt de timp și că a implementat o condiție la înregistrarea unui cont ca parola setată să aibă o complexitate ridicată.

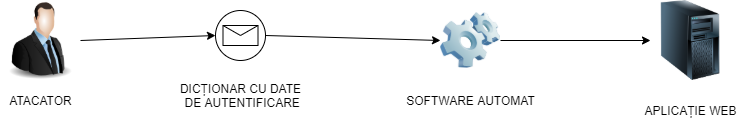


Figura 2.2. Exemplu credential stuffing

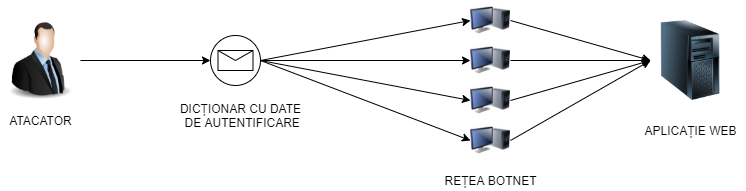


Figura 2.3. Exemplu atac BOTNET

Observăm în figurile 2.2 si 2.3 diferența uriașă pe care o are impactul unui

atac simplu, local, fată de un atac care folosește o rețea Botnet. Șansele ca atacul să aibă succes sunt exponențial mai mari în cazul figurii 2.3.

### Session attacks

Un alt tip de atac care intră în componența *Broken Authentication* este reprezentat de atacurile care vizează impersonarea unui alt utilizator. Acest lucru se întâmplă atunci când un atacator fură *ID-ul* sesiunii, prin diverse metode, unui utilizator autentificat. Acest lucru este realizabil din cauza unei configurari greșite a sistemului care gestionează sesiunile. Este posibil ca *ID-ul* să nu fie transportat sau stocat într-un text criptat, astfel un atacator poate să copieze pur și simplu *ID-ul*. Alte practici care trebuie evitate sunt autentificarea fără un *two factor login,* afișarea *ID-ului* în URL, păstrarea aceleași sesiuni pe toată durata procesului de autentificare, omiterea invalidării sesiunii atunci când un utilizator se deloghează sau este inactiv o perioadă mai lungă de timp.

Toate aceste obiceiuri duc la o aplicație nesigură și cu risc ridicat de compromitere. Pentru a evita astfel de evenimente, dezvoltatorul trebuie să se asigure că folosește un sistem de gestionare al sesiunii care rulează pe server și care este destul de bine configurat pentru a genera și a stoca *ID-ul* în siguranță.

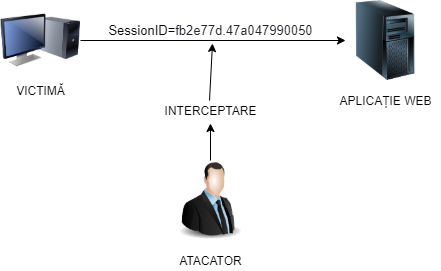


Figura 2.4. Un atacator interceptează o sesiune

## Sensitive Data Exposure

Așa cum reiese și din titlu, acest tip de vulnerabilitate reprezintă expunerea, într-o modalitate care să permită citirea, datelor sensibile, confidențiale, publicului. Atacurile practicate implică interceptarea datelor aflate în tranzit, între victimă și *aplicația web.* Datele personale cum ar fi parolele, secretele de serviciu, mesajele confidențiale, adresele, numerele de telefon, datele bancare, au nevoie de cea mai mare protecție. Metoda este cunoscută sub numele de *man in the middle*. Dezvoltatorul aplicației trebuie să se asigure că aplicația folosește protocoale criptografice actualizate și că este configurată în asa fel încât datele să fie transmise doar prin protocolul HTTPS. HTTPS este protocolul HTTP la care se adaugă stratul TLS/SSL cu rol de criptare, astfel toate datele aflate în tranzit între *browser* și server sunt transportate printr-un tunel criptat.

Alte vulnerabilități care intră în această categorie sunt date de interacțiunea dezvoltatorului cu *aplicația*. Acesta trebuie să se asigure că pe parcursul dezvoltării nu au fost lăsate, din greșeală mesaje sensibile la vedere, în comentarii sau undeva în pagina web. Mai mult, aplicația trebuie să conțină un certificat SSL valid, emis de un *Certificate Authority* (CA) de încredere și autorizat pentru a asigura utilizatorul că datele sunt criptate de o sursa de încredere.

Un atac frecvent întâlnit în astfel de cazuri este realizat de un atacator care se preface a fi un CA de încredere, care emite un certificat fals, care este apoi folosit de o *aplicație web* cu scopul de a păcăli utilizatorii pentru ca aceștia să-și introducă datele personale fără să suspecteze nici o tentativă de fraudă.

O astfel de vulnerabilitate poate fi evitată dacă dezvoltatorul evită să stocheze inutil date confidențiale, clasifică datele în funcție de confidențialiatea lor, respectând termenii de confidențialitate legali, se asigură că toate datele sensibile sunt criptate și foloseste parole puternice pentru securizarea punctelor de acces administrativ.

## XML External Entities (XXE)

Foarte asemănător cu tipul *Injections*, vulnerabilitățile de tip XEE au la bază exploatarea modului în care este interpretat un *input* XML. Dacă aplicația acceptă *input* XML în mod direct, în special de la surse care nu sunt de încredere sau dacă aplicația foloseste *document type definitions* (DTD) există riscul ca aplicația să fie vulnerabila. Vulnerabilitatea poate fi abuzată pentru a extrage date, executa diverse comenzi pe server sau pentru a-l supraîncărca, atac cunoscut sub numele de *denial-of-service* (DOS). Asemănător cu BOTNET, un astfel de atac realizat cu ajutorul mai multor calculatoare se numeșe *distributed denial-of-service* (DDOS)*.*

Fiind asemănătoare cu *Injections*, vulnerabilitatea poate fi evitată dacă *input-urile* sunt sanitizate, tehnologiile de interpretare a XML sunt actualizate și dacă se folosesc structuri de date mai puțin complexe de forma *JavaScript Object Notation* (JSON). JSON este un format de date ușor de interpretat de către aplicații și ușor de citit de către oameni.

## Broken Access Control

Funcția de *Access Control* gestionează privilegiile pe care utilizatorii unei aplicații le au. Cu alte cuvinte, funcția controlează ce date sunt accesibile și cui, la un moment dat. În cazul în care funcția nu este bine implementată, există riscul ca un simplu utilizator să aibă acces la resurse care, în mod normal, ar trebui să fie accesabile doar de un administrator. Atacatorii pot abuza de aceste scăpări și pot prelua controlul aplicației cu un minim efort.

Obținerea unui astfel de acces poate fi realizată în multe feluri și pentru scopuri diferite. Un atacator poate încerca să obțină acces de citire sau modificare a unor date de pe server, poate obține acces administrativ, sau poate să evite verificările privilegiilor în cazul în care dorește să acceseze o resursă restricționtă.

Acestă vulnerabiliate poate fi prevenită dacă dezvoltatorul implementeză metodele de control pe server. Acest lucru rezolvă situația în care un atacator poate să modifice diverse instrucțiuni din metode pentru a-și crea avantaje.

## Security Misconfiguration

Configurările greșite sunt unele dintre cele mai răspândite vulnerabilități de pe o *aplicație web.* Acestea pot apărea în orice strat al aplicației, fie că este vorba de rețeaua pe care rulează serverul, fie de *browserul* de pe care aceasta este accesată. Vulnerabilitatea apare atunci când există prea multe funcționalități inutile pe aplicație, setările implicite nu sunt modificate, când nu se actualizează sistemele de securitate ( Antivirus, Firewall), când există erori care furnizează mesaje sensibile pe care atacatorii le pot abuza pentru a obține informații sensibile sau când se folosesc funcționalități despre care se cunosc deja vulnerabilități.

Această vulnerabilitate crește riscul ca o aplicație să fie predispusă unui atac mai mult decât orice altă vulnerabilitate. Datoriă diversității de locuri în care această vulnerabilitate apare, este dificil pentru dezvoltatori și testeri să combată eficient orice greșeala. Deseori acesta este punctul de start în realizarea unui atac, deci este vital ca toate configurările de securitate să fie implementate corect pentru a descuraja orice tentativă de încurajare la un astfel de atac.

## Cross-Site Scripting (XSS)

Cea mai răspândită formă de vulnerabilitate este *Cross-Site Scripting*. Conform OWASP, două din trei aplicații au prezentat o astfel de vulnerabilitate. Această vulnerabilitate folosește *browserul* victimei pentru a executa cod malicios ca parte din HML sau JavaScript. JavaScript este limbajul de programare folosit de *browserul web*. Există trei tipuri de XSS.

### Reflected XSS

Acest atac presupune introducerea de cod extern în *browser* folosind doar un singur *request* HTTP. Un astfel de atac are loc atunci când un *browser* interpretează datele introduse de atacator prin *input-uri* nevalidate. Este o practică comuna ca un atacator să trimită cod JavaScript pentru a efectua diferite acțiuni asupra paginii web. Atacatorii pot instala *key loggers*, un timp de software care monitorizează tastele introduse de utilizator, pot modifica *link-uri* sau pot extrage date stocate în *browserul* victimei. Acest tip de atac este realizabil o singură dată, deoarece se bazează pe sistemul *request-response*, adică trimite o cerere serverului, iar acesta răspunde, în funcție de tipul *request-ului,* cu datele solicitate. Un *link* este o referință la o secțiune în cadrul documentului din care se accesează sau la alt document disponibil online.

### Stored XSS

Este același lucru cu tipul precedent, doar că, de data aceasta, aplicația reține codul introdus. Asta cauzează codul să fie executat permanent pe *browser*, astfel fiind posibil ca atacatorul să poată prelua controlul *browserului* victimei, să captureze informații sensibile și să scaneze rețeaua pe care aplicația rulează. Această vulnerabilitate este una dintre cele mai periculoase din cauza modului în care afectează utilizatorii. Un utilizator poate fi victima unui astfel de atac vizitând, pur și simplu o pagină web în care a fost introdus cod malicios. Acest atac este și mai periculos în zonele des frecventate de administratorii paginii. Datele conturilor acestora pot fi furate prin astfel de metode, atacatorii preluând astfel controlul aplicației.

### DOM XSS

Este foarte asemănător cu Stored XSS doar că este practicat îndeosebi pe aplicațiile de tip *single-page* *application* (SPA).

Toate aceste tipuri de vulnerabilități se ramifică în practici meticuloase pe care urmează să le prezint odată cu detalierea testelor implementate de *aplicația scanner.* Deci în capitolul următor voi prezenta arhitectura aplicației, împreună cu implementarea testelor de detecție pentru cele mai importante și răspândite vulnerabilițăți și voi detalia modul de utilizare și modul de raportare al *aplicației scanner.*

# Capitolul 3. Arhitectura aplicației și implementarea testelor

Aplicația are forma unei aplicații software standard. Aceasta este structurată într-un singur fișier Python cu mod de execuție diferit în funcție de sistemul de operare de pe care aceasta este rulată. Raportul generat este afișat în trei fișiere cu nume specific conținutului fiecăruia.



Codul aplicației este structurat în trei clase ajutătoare și una principală care implementează testele propriu-zise, fiecare clasă fiind responsabilă pentru o anumită colecție de metode și tehnici utilizate în procesul de scanare. Utilizatorul dispune de flexibilitate prin intermediul fisișierului de configurare *config.ini* pe care îl poate modifica cu orice editor text (ex. Notepad++).

## Parsarea variabilelor din fișierul de configurare

Acuratețea detecției testelor este cea mai importantă calitate a unei *aplicații scanner*. În acest scop am creat un fișier de configurare *config.ini* accesat prin intermediul modulului *ConfigParser* și am inițializat o variabila cu numele *config\_parser* cu rol de legatură între fisierul *.ini* și metodele de testare.

try:  
 config\_object = ConfigParser()  
 config\_object.read("config/config.ini")  
except Exception:  
 pass

Fișierul *config.ini* trebuie să existe în folderul *config* aflat la aceeași cale cu *scannerul.* Acesta conține text explicativ pentru o mai bună interacțiune cu utilizatorul și nume de variabile intuitive (vezi Figura 3.1).

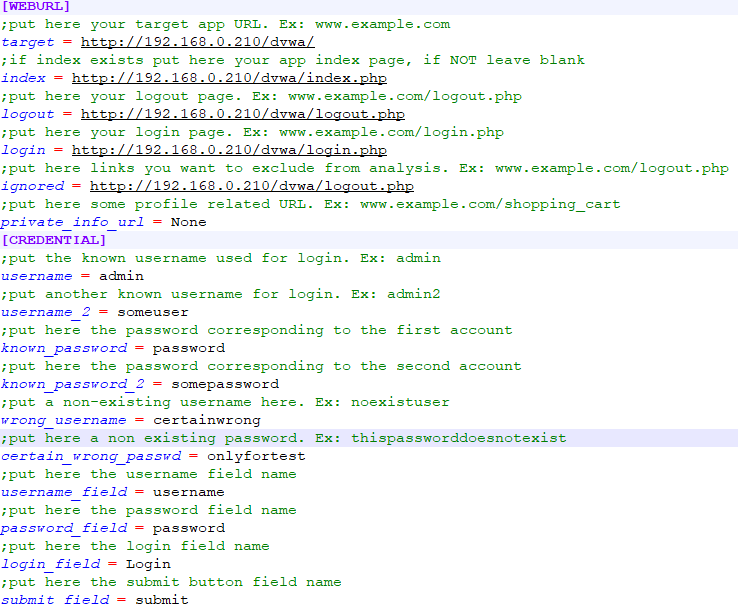


Figura 3.1. Formatul fișierului de configurare

## Clasa LoginTests

Această clasa este prima clasă apelată la rularea programului. În momentul apelării aplicația testează si încearcă autentificarea la aplicația de test folosind datele introduse în fișierul de configurare.

try\_brute\_force = LoginTests(  
 config\_object["CREDENTIAL"]["username"],  
 config\_object["WEBURL"]["login"],  
 config\_object["FILE"]["password\_dict"],  
 config\_object["CREDENTIAL"]["wrong\_username"],  
 config\_object["CREDENTIAL"]["known\_password"],  
 config\_object["CREDENTIAL"]["certain\_wrong\_passwd"],  
 config\_object["WEBURL"]["logout"],  
 report\_file,  
 error\_file  
)

Clasa accesează pagina de login aflată în fișierul de configurare și aplică pe aceasta o suită de teste din categoria *Broken Authentication.* Primul test pe care aplicația îl face este să detecteze daca *siteul web* este vulnerabil la *Brute Force Login.*

Brute Force este procedeul prin care un atacator ‘fortează’ autentificarea folosind un dicționar de date de autentificare. În cazul *aplicației* *scanner* dicționarul este *rockyou.txt* [19]. *Rockyou.txt* este un set de parole extras dintr-un *Data Leak* de acum câtiva ani. Setul conține un număr de 14,341,564 parole unice pe care atacatorii, dar și testerii le folosesc frecvent în practica de *Brute Force.*

with open(config\_object["FILE"]["password\_dict"], "rb") as f:  
 pass\_list = f.readlines()  
 f.close()  
pass\_q = queue.Queue()  
if len(pass\_list):  
 for passwd in pass\_list:  
 try:  
 passwd = passwd.decode("utf-8").rstrip()  
 pass\_q.put(passwd)  
 except Exception as e:  
 print(e)  
 passwd = passwd.decode("latin-1").rstrip()  
 pass\_q.put(passwd)  
  
for pass\_word in pass\_q.queue:  
 http = requests.post(  
 self.login\_url,  
 data={  
 config\_object["CREDENTIAL"]["username\_field"]: self.username,  
 config\_object["CREDENTIAL"]["password\_field"]: pass\_word,  
 config\_object["CREDENTIAL"]["login\_field"]: config\_object["CREDENTIAL"]["submit\_field"]  
 }  
 )  
 if http.url == config\_object["WEBURL"]["index"]:  
 self.password = pass\_word  
 self.password\_found = True  
 return 1

Metoda de test *Brute Force* deschide fișierul ales de utilizator (în cazul nostru un fișier mai care conține un fragment din *rockyou.txt*) și introduce parolele într-o coadă pentru a nu ține fișierul deschis în timpul testării. O dată ce parolele au fost încărcate și formatete penru a putea fi introduse în cămpul de *login*, testul trimite un *request* de tipul POST cu datele de autentificare la adresa la care se află pagina de *login* a aplicației. În acest test, numele de utilizator trebuie să fie unul existent pentru a avea rezultate mai rapid, astfel se evită procesul inuil în cazul de față de a testa și *usernameuri.* *Usernameul* poate fi setat din fișierul de configurare.

Următorul test pe care *scannerul* îl face este testul de verificare a mesajelor de autentificare. Acest test se realizează în același timp cu testul de *Brute Force* și constă în verificarea erorilor apărute în cazul unei autentificări nereușite. Este posibil ca aplicația să furnizeze date utile unui atacator prin mesajele furnizate în cazul în care fie un nume de utilizator este greșit, dar parola este corectă, fie numele de utilizator este corect și parola greșită. În acest caz, un atacator poate să-și formeze o listă de date valide. O astfel de vulnerabilitate este una din cauzele existenței dicționarelor cu date de autentificare.

print("Checking for Account Enumeration and Possible Guessable Users...", file=self.report\_file)  
wrong\_password\_res = requests.post(  
 self.login\_url,  
 data={  
 config\_object["CREDENTIAL"]["username\_field"]: self.username,  
 config\_object["CREDENTIAL"]["password\_field"]: self.wrong\_passwords,  
 config\_object["CREDENTIAL"]["login\_field"]: config\_object["CREDENTIAL"]["submit\_field"]  
 }  
)  
wrong\_password\_res\_content = str(wrong\_password\_res.content)  
wrong\_username\_res = requests.post(  
 self.login\_url,  
 data={  
 config\_object["CREDENTIAL"]["username\_field"]: self.wrong\_un,  
 config\_object["CREDENTIAL"]["password\_field"]: self.good\_password,  
 config\_object["CREDENTIAL"]["login\_field"]: config\_object["CREDENTIAL"]["submit\_field"]  
 }  
)  
wrong\_username\_req\_content = str(wrong\_username\_res.content)  
if wrong\_username\_req\_content != wrong\_password\_res\_content:  
 return 1  
return 0

Pentru a testa această vulnerabilitate am ales sa testez mesajele returnate în ambele situații. Prima oară metoda testează mesajele cu un nume de utilizator corect și o parolă despre care știm sigur că greșită (este introdusă în fișierul de configurare de către utilizator). Se testează apoi prin aceeași metodă procesul inversat, în care parola este corectă (din fișierul de configurare) și *usernameul* greșit. Capturăm *responseul* într-o variabilă în ambele cazuri și verificăm dacă există diferențe în acesta. Dacă răspunsul este afirmativ atunci sunt mari sanșe ca această vulnerabilitate să fie prezentă.

O altă vulnerabilitate cunoscută în procesul de autentificare este chiar cauza pentru care metoda *Brute Force* este posibilă. Pentru a evita un atac de tipul *Brute Force* este nevoie ca aplicația să blocheze încercările nereușite de autentificare, succesive și repetate într-un interval scurt de timp.

def check\_login\_attempts(self, n):  
 try:  
 my\_gui.update\_list\_gui("Checking Lock-Out Mechanism")  
 self.session = requests.session()  
 for i in range(n):  
 self.session.post(  
 self.login\_url,  
 data={  
 config\_object["CREDENTIAL"]["username\_field"]: self.username,  
 config\_object["CREDENTIAL"]["password\_field"]: self.wrong\_passwords[0],  
 config\_object["CREDENTIAL"]["login\_field"]: config\_object["CREDENTIAL"]["submit\_field"]  
 }  
 )  
 correct\_login = self.session.post(  
 self.login\_url,  
 data={  
 config\_object["CREDENTIAL"]["username\_field"]: self.username,  
 config\_object["CREDENTIAL"]["password\_field"]: self.good\_password,  
 config\_object["CREDENTIAL"]["login\_field"]: config\_object["CREDENTIAL"]["submit\_field"]  
 }  
 )  
 if correct\_login.url == config\_object["WEBURL"]["index"]:  
 self.session.post(self.logout\_url)  
 self.session.close()  
 print("[!!!-!!!] Wrong Password Lock Out Mechanism not triggered after ", n, " times", file=self.report\_file)  
 return 1  
 return 0

Metoda de test presupune încercarea de ‘n’ ori a unei autentificări nereușite urmate de o autentificare cu date valide. Dacă după ‘n’ ori *aplicația web* nu blochează încercările nereușite și permite autentificarea validă este posibil să existe această vulnerabilitate.

Pentru că orice aplicație de testare automată vrea să simuleze și să fie cel puțin la fel de eficientă, din punct de vedere al acurateței, ca o testare manuală, în unele situații pe care urmează să le detaliez mai târziu este nevoie de utilizarea a două sesiuni diferite, astfel am implementat o clasă care să creeze o sesiune diferită pentru a o folosi în anumite teste.

## Clasa OtherUser

Folosim sesiuni separate atunci când vrem să testăm interacțiuni cu alți utilizatori. Aplicația inițializează o sesiune noua cu ajutorul unor date de autentificare secundare, accesate din fișierul de configurare și modulului *requests.*

self.session = requests.Session()

Pentru a interacționa cu sesiunea am implementat două metode care returnează datele pe care o să le folosim pe parcursul testării.

def get\_sess\_id(self):  
 try:  
 global session\_id  
 self.session.get(self.url)  
 cookie\_dict = self.save\_cookies(self.url)  
 key\_list = list(cookie\_dict.keys())  
 for key in key\_list:  
 if key.lower() == "sid" or "sessionid" or "session" or "sessiontoken" or "sessid":  
 session\_id = cookie\_dict[key]  
 self.session.close()  
 return session\_id  
 return  
 except Exception as e:  
 print("\n[ERROR] Something went wrong when trying to get session id from another session. Error: ", e, file=self.error\_file)  
 pass

Pentru a accesa *ID-ul* sesiunii este nevoie să accesăm *cookie-urile* salvate atunci când o sesiune se crează. Un *cookie* este o colecție de fișiere de mici dimensiuni create pentru a reține date despre utilizatorul curent cu scopul de a îmbunătății experiența *web*. Deci din *cookie* putem extrage informații despre sesiunea curentă. Am salvat și stocat *cookie-urile* găsite, într-o variabilă pe care o parcurgem apoi pentru extrage și *ID-ul* sesiunii. În cazul în care este găsit un astfel de *ID* îl salvăm și îl returnăm.

Am salvat și întregul dicționar de *cookies* deoarece o să avem nevoie și de acesta la un moment dat.

def save\_cookies(self, url):  
 try:  
 self.session.get(url)  
 session\_cookies = self.session.cookies  
 cookies\_dictionary = session\_cookies.get\_dict()  
 return cookies\_dictionary  
 except Exception as e:  
 print("\n[ERROR] Something went wrong when trying to return cookies from another session. Error: ", e, file=self.error\_file)  
 pass

## Clasa GUI

Această clasă are ca scop înițializarea și modificarea modelului GUI pentru cazul când sistemul de operare folosit este Windows. Clasa inițializează o fereastră goala asupra căreia aduc modificări pentru a o customiza.

În componența acesteia am implementat metodele care modifcă interfața și interacționează cu alogritmul și cu clasa de scanare. Metodele folosite au rolul de a “lega” funcționalitatea anumitor butoane la anumite funcții. La rularea programului, interfața are forma portret o listă goală de teste efectuate, trei butoane și o bară de progres (vezi Figura 3.2).

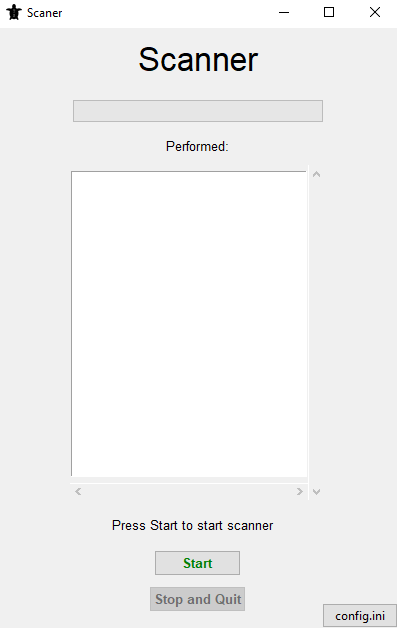


Figura 3.2. Interfața aplicației

Butoanele existente pe interfața sunt ‘legate’ la metodele din funcția GUI.

self.start\_button = Button(

self.gui\_app, text="Start",

command=self.start\_scan,

style='B1.TButton'

)  
self.start\_button.pack(pady=5)

Prin argumentul *command* specificăm butonului ce metodă să apeleze. În cazul butonului *start* acesta apeleaza metoda *start\_scan* care modifică interfața și incepe execuția algoritmului de scanare prin crearea unui *fir de execuție* aplicat asupra funcției *start\_program*. Acest lucru împiedică aplicația să devină *not responding* în procesul de scanare, fiind complet interacționabilă pe parcursul execuției.

def start\_scan(self):  
 try:  
 global t1  
 try:  
 if self.open\_report:  
 self.open\_report.pack\_forget()  
 self.close\_button.pack\_forget()  
 self.stop\_button = Button(self.gui\_app, text="Stop and Quit", command=self.stop\_scan, style='B2.TButton')  
 self.stop\_button.pack(pady=5)  
 except Exception:  
 pass  
 try:  
 if self.list.index("end") != 0:  
 self.list.delete(0, 'end')  
 except Exception:  
 pass  
 self.gui\_app.geometry('400x600')  
 self.label.config(text='Wait..')  
 self.state = 'started'  
 self.start\_button['state'] = DISABLED  
 self.start\_button.config(text='Scan')  
 self.stop\_button['state'] = NORMAL  
 self.progress\_bar['value'] = 0  
 t1 = threading.Thread(target=start\_program)  
 t1.start()  
 except Exception:  
 pass

Mai multe detalii despre aspectul interfeței va fi prezentat în subcapitolul *Utilizarea aplicației.*

Fiecare buton este legat la o astfel de funcție. Pentru butonul *Stop and Quit* este apelată funcția *stop\_scan* care modifică aspectul și oprește algoritmul forțat.

def stop\_scan(self):  
 try:  
 self.stop\_button['state'] = DISABLED  
 self.start\_button['state'] = NORMAL  
 self.label.config(text="Scan stopped!")  
 self.kill\_thread(t1)  
 self.gui\_app.quit()  
 quit()  
 except Exception:  
 pass

La finalul scanării interfața este iarăși modificată pentru a oferi accesibilitate și informații utilizatorului (vezi Figura 3.3).

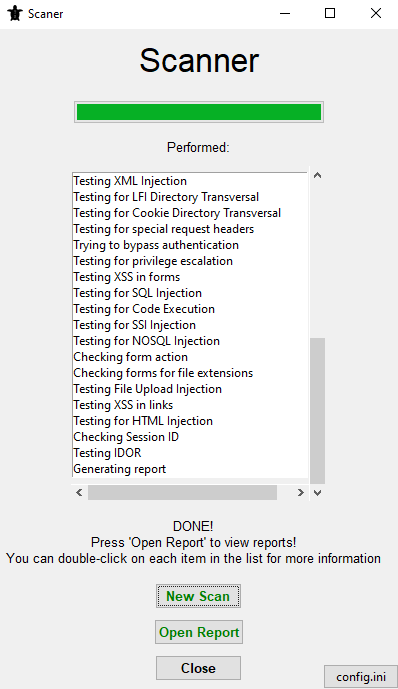


Figura 3.3. Interfața la finalul execuției

Metoda care aduce toate aceste modificări vizuale este apelată la finalul execuției algoritmului și foloseșe metode din modului *Tkinter* pentru a manipula interfața.

def done\_label(self):  
 try:  
 self.state = 'stopped'  
 self.stop\_button.pack\_forget()  
 try:  
 if self.open\_report:  
 self.open\_report.pack\_forget()  
 self.close\_button.pack\_forget()  
 except Exception:  
 pass  
 self.gui\_app.geometry('400x660')  
 self.open\_report = Button(self.gui\_app, text="Open Report", command=self.open\_output, style='B1.TButton')  
 self.open\_report.pack(pady=5)  
 self.close\_button = Button(self.gui\_app, text="Close", command=self.stop\_scan, style='B3.TButton')  
 self.close\_button.pack(pady=5)  
 self.start\_button['state'] = NORMAL  
 self.start\_button.config(text="New Scan")  
 self.label.config(text="DONE!\nPress 'Open Report' to view reports!\nYou can double-click on each item in the list for more information")  
 self.gui\_app.update()  
 try:  
 shutil.rmtree(temp\_dir)  
 except Exception:  
 pass  
 except Exception:  
 pass

În această clasă se mai găsesc și alte metode utilitare cu rol de actualizare a datelor și aspectului. Spre exemplu metodele *update\_list\_gui* și *update\_progress\_bar* sunt apelate la fiecare pas de testare pentru a ține utilizatorul la curent cu progresul aplicației.

def update\_list\_gui(self, text):  
 try:  
 if not self.contain(text):  
 self.list.insert(END, text)  
 except Exception:  
 pass  
  
def update\_progress\_bar(self, amount):  
 try:  
 self.progress\_bar['value'] += amount  
 self.gui\_app.update\_idletasks()  
 except Exception:  
 pass

## Clasa Scanner

Această clasă este responsabilă cu scanarea propriu-zisă. În această clasă se află atât metodele care gestionează diverse teste cât și metode care au rol utilitar.

Clasa este apelată în funcția *main* din cadrul funcției *start\_program*. Funcția *start\_program* are rolul de a deschide fișierele de *output*, în care urmează să fie generat raportul, și de a apela funcția *main* în care se apelează inițial clasa *LoginTests,* pentru stabilirea conexiunii și testarea vulnerabilitățiilor pentru autentificare, urmată de clasa *Scanner*

report\_path = os.path.join(report\_dir\_path, "Report.txt")  
open(report\_path, 'w').close()  
architecture\_path = os.path.join(report\_dir\_path, 'Web Application Map.txt')  
open(architecture\_path, 'w').close()  
error\_path = os.path.join(report\_dir\_path, 'Error Log.txt')  
open(error\_path, 'w').close()  
  
# Appends to emptied file  
rep\_file = open(report\_path, 'a')  
arch\_file = open(architecture\_path, 'a')  
err\_file = open(error\_path, 'a')  
  
# Runs program  
main(rep\_file, arch\_file, err\_file)

Funcția *main* este, de fapt, funcția care are ca rol inițializarea algoritmului de testare.

După realizarea testelor pentru autentificare, am apelat clasa *Scanner* cu datele returnate în procesul de testare menționat anterior și am inițializat o sesiune, urmând să apelez funcția care gestionează toate metodele de testare (functia de rulare a algoritmului).

vuln\_scanner.session.post(config\_object["WEBURL"]["login"], data=data\_dict)  
vuln\_scanner.run\_scanner()

Variabila *data\_dict* este un dicționar în care se află datele de conectare preluate din fișierul de configurare.

data\_dict = {  
 config\_object["CREDENTIAL"]["username\_field"]: config\_object["CREDENTIAL"]["username"],  
 config\_object["CREDENTIAL"]["password\_field"]: found\_password,  
 config\_object["CREDENTIAL"]["login\_field"]: config\_object["CREDENTIAL"]["submit\_field"]  
}

Sesiunea este inițializată cu ajutorul modulului *requests* cu metoda POST la care adăugăm URL-ul de autentificare și *payload-ul* cu datele necesare autentificării cu succes.

Un *payload* este un set de date, din componența unui mesaj, ce contine mesajul propriu-zis, fără să aiba alte informații utile pentru transport sau pentru alte scopuri, în componența lui.

Odata apelată metoda *run\_scanner* aceasta apelează metode implementate în clasă, succesiv, în funcție de opțiunile pe care utilizatorul le-a ales în fișierul de configurare. În această metodă se află metode de culegere a informațiilor, de testare, de generare a raportului și de actualizare a interfeței, asdar am să incep cu apelul singular al metodelor de culegere a informațiilor.

### Extragerea informațiilor

Înainte ca orice test să fie pus în practică, atât manual cât și automat, este nevoie să culegem informații despre aplicația testată.

def run\_scanner(self):  
 try:  
 global final\_list  
 my\_gui.update\_progress\_bar(10)  
 # print('\rPlease wait..', end='', flush=True)  
 self.gather\_info()  
 self.test\_broken\_auth(test=(True if config\_object['TEST']['test\_broken\_auth'].lower() == "true" else False))  
 self.test\_security\_misconfiguration(test=(True if config\_object['TEST']['test\_security\_misconfiguration'].lower() == "true" else False))  
 self.test\_sensitive\_data\_exposure(test=(True if config\_object['TEST']['test\_sensitive\_data\_exposure'].lower() == "true" else False))  
 visible\_links, final\_list = self.create\_return\_merge\_links()

Metodele de mai sus urmează să fie apelate o singură dată. O să vedem mai târziu ca în componența acestei metode se află funcționalități care vor fi aplelate de mai multe ori pe mai multe *linkuri*.

Metoda *gather\_info* este metoda care începe procesul de extragere a *linkurilor* din aplicație. Acest pas este unul foarte important deoarece pentru fiecare *link* extras, in funcție de forma lui, se vor aplica teste de detecție. Această metodă apelează o alta metodă utilitară din clasa *Scanner*, pe care am numit-o *spider*. Procesul de *spidering* este procesul prin care sunt extrase, înr-un mod recursiv, toate *linkurile* prezente în pagina sursă a unei *aplicații web*. În această metodă de spider se verifică numărul maxim de *linkuri* care pot fi extrase. Acest număr este configurabil în fișierul *config.ini*. *Link-urile* extrase sunt introduse apoi pe rând într-o listă.

my\_gui.update\_list\_gui("Extracting links from application")  
if url is None:  
 url = self.target\_url  
extracted\_links = self.extract\_links(str(url))  
for extracted\_link in extracted\_links:  
 extracted\_link = urllib.parse.urljoin(url, extracted\_link)  
 if "#" in extracted\_link:  
 extracted\_link = extracted\_link.split("#")[0]  
 if self.target\_url in extracted\_link and extracted\_link not in self.target\_links and extracted\_link not in self.ignored\_links and len(self.target\_links) <= int(config\_object['TEST']['max\_number\_of\_not\_hidden\_links']):  
 print(extracted\_link, file=self.map\_file)  
 self.target\_links.append(extracted\_link)  
 self.spider(extracted\_link)

După acest pas *scannerul* folosește un dicționar pentru a căuta *linkuri* ascunse sau care nu sunt prezente în codul paginii aplicației și care pot să ne ofere acces la diverse informații sensibile. Pentru a modifca URL-ul și pentru a găsi astfel de *linkuri* în aplicație, am folosit unelte din modulul *urlparse* și am modificat calea URL cu căi din dicționar [20].



Figura 3.4 Structura unui URL

În procesul de căutare vom adauga URL-ului standard, de forma *www.exemplu.ro* o cale către alte fișiere. Verificăm dacă calea există trimițând un *request* de tip GET la adresa compusă la pasul anterior și verificăm dacă serverul ne răspunde cu codul 200, specific pentru mesajul de conexiune realizată cu succes (OK). După ce am găsit astfel de căi la care am primit mesajul OK, adăugăm într-o listă atât *linkurile* vizibile cât și pe cele ascunse. Aceste *linkuri* urmează să fie iterate și parcurse unul câte unul pentru a testa tot ce se poate pentru fiecare, astfel restrângem aria de căutare a vulnerabilităților în funcție de tipul de URL găsit.

Tot în pasul de extragere al informațiilor încercăm să analizăm rețeaua pe care serverul rulează. În cazul în care în componența URL-ului există un IP putem afla informații despre acesta cu ajutorul modulului *nmap*. Folosim o expresie *re* pentru a căuta un IP în adresa web a aplicației (ex. www.80.5.12.32.com). Apelăm modulul *nmap* cu argumentele *-Pn -sT -sV* pentru a obține informații despre porturi, servicii și versiuni disponibile pe aplicație. În cazul în care acest test este realizat cu succes, aceste informații urmează să fie introduse în raportul final.

web\_app\_ip\_address = re.findall('http://(.\*?)/', config\_object['WEBURL']['target'])  
if web\_app\_ip\_address:  
 web\_app\_ip\_address = [ip\_address for ip\_address in web\_app\_ip\_address if ip\_address][0]  
 nmap\_scanner.scan(web\_app\_ip\_address, '0-65535', arguments='–Pn –sT –sV')  
 print('\nHost : ', nmap\_scanner[web\_app\_ip\_address].hostname(), file=self.report\_file)  
 print('State : ', nmap\_scanner[web\_app\_ip\_address].state(), file=self.report\_file)  
 for protocol in nmap\_scanner[web\_app\_ip\_address].all\_protocols():  
 print('----------', file=self.report\_file)  
 print('Protocol : ', protocol, file=self.report\_file)  
 port\_list\_inner = nmap\_scanner[web\_app\_ip\_address][protocol].keys()  
 port\_list\_inner.sort()  
 for port in port\_list\_inner:  
 print('Port : ', port, '\tState : ', nmap\_scanner[web\_app\_ip\_address][protocol][port]['state'], file=self.report\_file)

Alți pași care sunt realizați imediat finalizarea funcției *gather\_info* sunt testarea anumitor vulnerabilități din categoriile *Broken Authentication, Security Misconfiguration, Sensitive Data Exposure.* Înainte ca aceste funcții să fie apelate, se testează mai întâi dacă utilizatorul a optat pentru un astfel de test. Condiția urmatoare verifică daca, în fișierul de configurare utilizatorul a selectat opțiunea pe care urmează să o testăm. Această verificare are loc la fiecare apel al acestor suite de funcții categoriale.

test=(True if config\_object['TEST']['test\_sensitive\_data\_exposure'].lower() == "true" else False)

În cazul în care utilizatorul a optat pentru astfel de teste, următorul pas al algoritmului este să caute *linkuri* administrative prin exact aceeași modalitate ca în cazul *linkurilor* ascunse, doar că de data asta, se folosește un dicționar care conține numeroase de astfel de variante de *linkuri* administrative [21].

După ce aplicația a terminat de căutat *linkurile* administrative, urmază să apeleze metoda care verifică tipul *security misconfigurations*. Aici se analizează lista robots.txt. Această listă este legătura dintre motoarele de căutare și pagina *web.* Aici se introduc căile pe care dezvoltatorul le setează vizibile sau invizibile motoarelor de căutare. În acest pas *scannerul* caută *linkuri* cu informații sensibile pe care dezvoltatorul nu ar trebui să le lase acolo. Apoi cu ajutorul unui alt dicționar ce cuprinde *linkuri* populare din *robots.txt*, *scannerul* încearcă să găsescă alte *linkuri* ascunse prin aceeași metodă ca în cazurile anterioare.

Se testează apoi metodele HTTP de transport și securitatea acestora. În mod normal o *aplicație web* nu trebuie să permită utilizatorilor accesul la metode de tip PUT, DELETE. Astfel de metode reprezintă vulnerabilitați în proiectarea aplicației. Pentru testarea metodei PUT sau DELETE, *scannerul* trimite un *request* de tip PUT aplicației web și analizează răspunsul primit. Pentru testarea securitații metodei HTTP *scannerul* verifică dacă existența *headerului Strict Strict Transport Security* este găsită în *responsul* *aplicației web.* Un header este o porțiune dintr-un *request* care specifică informații despre acesta*.*

headers = self.get\_headers(config\_object['WEBURL']['target'])  
if 'strict' not in str(headers).lower():  
 return True  
return False

Un ultim test de tipul *Security Misconfiguration* nonrecursiv este testul pentru *Rich Internet Applications* (RIA). Acestea sunt fișiere care specifică tipul de permisiune pe care *clientii web* (Java, Adobe Flash, Adobe Reader) le au asupra resurselor de pe aplicație. Este vital ca aceste permisiuni sa fie restrictive pentru a proteja fișierele sensibile. *Scannerul* verifică dacă în componența codului sursă al paginii există astfel de fișiere în care permisiunile au fost setate ca *All* (\*), în caz afirmativ aplicația este vulnerabilă.

if 'clientaccesspolicy.xml' in link.lower() or 'crossdomain.xml' in link.lower():  
 content = self.session.get(link)  
try:  
 if '\*' in content:  
 return True  
except TypeError:  
 pass

Ultima categorie testată nonrecursiv este *Sensitive Data Exposure* unde se testează doar dacă aplicația web are un certificat SSL, și, în caz afirmativ, testează valabilitatea și autenticitatea acestuia.

context = ssl.create\_default\_context()  
with socket.create\_connection((self.target\_url, self.port)) as sockk:  
 with context.wrap\_socket(sockk, server\_hostname=self.target\_url) as tlssock:  
 y = getattr(tlssock, to\_check)  
 return y()

Aplicația folosește un socket pentru a se lega direct la acesta apoi culege informațiile de care are nevoie pentru a face verificările.

stripped = self.check\_tls("getpeercert")["notAfter"].split(sep, -1)[:-1]

În cazul acesta *scannerul* extrage data de expirare a certificatului și o compară cu data actuala, utilizatorului îi este precizată în raport un mesaj informativ.

În același context *scannerul* verifică dacă entitatea emițătoare a certificatului este cunoscută și o returnează utilizatorului.

### Aplicarea testelor asupra informațiilor

La finalul execuției verificărilor realizate o singură dată per scanare, aplicația aplică teste asupra *linkurilor* găsite în procesul de *spidering* plus *linkurilor* ascunse. Lista finală este compusă din toate aceste linkuri găsite în procesul de *information gathering*. Proces care presupune culegerea a cât mai multă informație despre *aplicația web.* Acest proces este comun atât atacatorilor, atunci când vor să infecteze o astfel de aplicație, cât și *penetration testeriilor* care vor să testeze aplicația din punctul de vedere al securității.

În acest pas, prima etapa a *scannerului* este să caute *taguri* *form* în codul HTML, adică să extragă formularele și *inputurile* în care utilizatorul poate să introducă date. Asa cum am observat în capitolul 2, există o mulțime de vulnerabilități cauzate de lipsa sanitizării *inputurilor,* deci este foarte important ca *scannerului* să aplice teste asupra acestor zone. Formularele sunt extrase cu ajutorul unei funcții utilitare *extract\_forms* în care este folosit modului *BeautifulSoup* pentru a selecta și parsa formularele pentru ca ulterior, acestea să fie introduse înr-o listă. Modul prin care extragem formularele constă în capturarea răspunsului pe care aplicația ni-l returnează și parsarea lui, modulului *BeautifulSoup* care decodează și formatează conținutul pentru a găsi si returna taguri de tip *form.*

response = self.session.get(url)  
parsed\_html = BeautifulSoup(response.content, "html.parser", from\_encoding="iso-8859-1")  
return parsed\_html.findAll("form")

Apoi pentru fiecare formular se aplica teste din suitele *Injections, Senstive Data Exposure, Security Misconfiguration*.

Primul tip de vulnerabilitate testată este din tipul *Injections,* anume, Stored XSS. Aplicația pregătește un *payload* XSS de forma *‘<sCriPt>alert('test')</sCRiPt>*’ și trimite un request cu acesta ca *submit* la formular. Metoda apelează funcția *submit\_form* care are ca rol indentificarea câmpului de trimitere a formularului, tipului *request* și adăugarea *payload-ului* în corpul mesajului pe care urmează să îl transmită *aplicației web*.

xss\_test\_script = "<sCriPt>alert('test')</sCRiPt>"  
response = self.submit\_form(form, xss\_test\_script, url)  
return xss\_test\_script.lower() in str(response.text) or xss\_test\_script in str(response.text)

După trimiterea mesajului, verificăm dacă în răspuns se află *payload-ul* XSS. Dacă *aplicația web* nu ar fi vulnerabilă ar trebui să nu fie procesat tagul ‘<script>’. Așadar, daca acest tag este încă existent în *response,* este clar că aplicația este vulnerabilă.

După testul XSS aplicația testează *injection* de tipul SQL. Acest test este asemănător cu mici excepții. Există două tipuri de SQL *Injections*, tipul în care ni se prezintă erori atunci cand încercăm caractere care pot fi interpretate de limbajul SQL, și tipul în care aceste erori sunt absente. Cel de-al doilea tip se numește Blind SQL *Injection*.Prin testul pe care *scannerul* îl face, ambele tipuri de SQL *Injections* sunt verificate cu succes.

global sql\_injection\_dict\_injected, sql\_injection\_dict\_normal  
sql\_no\_payload = ""  
response\_wh\_payload = self.submit\_form(form, sql\_no\_payload, url)  
normal\_response\_time = response\_wh\_payload.elapsed.total\_seconds()  
sql\_detect\_payload = "IF(SUBSTR(@@version,1,1)<5,BENCHMARK(2000000,SHA1(0xDE7EC71F1))," \  
 "SLEEP(0.5))/\*'XOR(IF(SUBSTR(@@version,1,1)<5," \  
 "BENCHMARK(2000000,SHA1(0xDE7EC71F1)),SLEEP(0.5)))OR'|'XOR(IF(SUBSTR(@@version,1,1)<5," \  
 "BENCHMARK(2000000,SHA1(0xDE7EC71F1)),SLEEP(0.5)))OR'\*/"  
response\_w\_payload = self.submit\_form(form, sql\_detect\_payload, url)  
sql\_response\_time = response\_w\_payload.elapsed.total\_seconds()  
  
if sql\_response\_time > normal\_response\_time and sql\_response\_time > 1.5:  
 sql\_injection\_dict\_normal[url] = normal\_response\_time  
 sql\_injection\_dict\_injected[url] = sql\_response\_time  
 return True  
return False

Testarea constă în injectarea unui *payload* special destinat detecției ambelor tipuri de vulnerabilități. Acesta cauzează pagina web să ‘doarmă’, aproximativ 5 secunde. Deci aplicația injectează *payload-ul* și compară apoi timpul normal de răspuns (fara *payload*) cu timpul după ce *payload-ul* a fost încarcat. Dacă diferența este mai mare de 1.5 secunde, *scannerul* consideră aplicația vulnerabilă [22]. *Scannerul* testează si tipul *NOSQL* în aceeași modalitate, doar că folosește un payload specific limbajului *NOSQL.*

Următoarele două tipuri de *injection* testat sunt *Code Execution* și *Server-Side Includes*. Acestea presupun introducerea unui *payload* care poate fi interpretat de sistemul de operare. *Scannerul* introduce comanda de afișare a orei curente, compatibilă cu sistemele Linux, apoi folosind o expresie *re*, caută în *response* un format de tipul *hh:mm:ss* pentru a detecta ambele forme de *injection*.

code\_exec\_script = "| uptime"  
response = self.submit\_form(form, code\_exec\_script, url)  
return re.findall('\d\d:\d\d:\d\d', str(response.content))

Pentru suita *Sensitive Data Exposure* aplicată pe formulare, am implementat o verficare asupra acțiunii din formular.

action = form.get("action")  
if not action:  
 return False  
elif "http" in action and "https" not in action:  
 return True  
return False

Rolul acestei implementări este de a verifica dacă există un formluar pe care *aplicația web* îl transmite printr-un protocol HTTP nesecurizat. Am folosit metoda *.get()* din *BeautifulSoup* pentru a captura acțiunea formularului.

Pentru testarea suitei *Security Misconfigurations* asupra formularelor, am implementat două teste. Primul test constă în verificarea extensiilor din acțiunea formularului. *Scannerul* verificădacă în componența unui formular există extensii cu atributul *hidden*. Acestea pot fi de folos pentru a extrage informații sensibile din aplicație. De exemplu tehnologiile pe care aceasta le utilizează sau fișierele uitate de dezvoltator pot ajuta atacatorul în pregătirea unui *payload* malicios customizat pentru tipul de tehnologie care rulează pe *site*, astfel crescându-și șansele de reușită în cazul unui atac.

Al doilea test efectuat în această etapă este verificarea punctelor în care *aplicația web* primeste fișiere de la utilizatorii ei. Așa cum am exemplificat înainte, există riscul ca un atacator să creeze un fișier cu conținut malicios și sa-i facă *upload*. Astfel acesta poate executa cod de la distanță reușind să preia controlul asupra serverului. *Scannerul* caută în formular cuvinte cheie specifice încarcării datelor. Dacă sunt găsite tipuri de *inputs* de forma *files* sau dacă șirul *‘multipart/form-data’*, specific încarcării de fișiere, este prezent în componența formularului, *scannerul* încearcă să facă *upload* la fișierele generate și apoi verifică statusul *request-ului*. În cazul în care statusul este OK, *scannerul* consideră că *aplicația web* este vulnerabilă. Fișierele generate sunt trimise la server prin intermediul funcției *sumit\_form* cu un argument în plus ce reprezintă fișierul de *upload.* Este generat un *request* în care fișierul este introdus în corpul mesajului.

if self.submit\_form(form, "value", url, files).status\_code == 200:

Acestea sunt toate testele pe care *scannerul* le aplică asupra formularelor. După acest pas *scannerul* testează toate *linkurile* găsite anterior pentru vulnerabilități asemănătoare sau specifice.

După ce testele asupra formularelor au luat sfârșit, *scannerul* testează, din nou, suitele *Injections, Broken Authentication, Sensitive Data Exposure, Broken Acces Control* și *XML External Entities* asupra linkurilor*.* În aceste suite se află teste realizate în funcție de parametrii pe care i-am introdus în apelarea funcției. Spre exemplu diferența dintre apelul simplu al suitei *Sensitive Data Exposure*, apelul pe formulare și apelul pe linkuri este dată de argumentele prezente în apel.

self.test\_sensitive\_data\_exposure(test=(True if config\_object['TEST']['test\_sensitive\_data\_exposure'].lower() == "true" else False))

Acesta este un exemplu de apel singular al suitei *Sensitive Data Exposure.* Se observă absența oricărui parametru, înafară de parametrul specific verificării dacă utilizatorul a optat pentru test sau nu.

self.test\_sensitive\_data\_exposure(link, form, test=(True if config\_object['TEST']['test\_sensitive\_data\_exposure'].lower() == "true" else False))

În cazul apelului pe formular se observă prezența parametrilor ‘form’ și ‘link’în apel.

self.test\_sensitive\_data\_exposure(link, test=(True if config\_object['TEST']['test\_sensitive\_data\_exposure'].lower() == "true" else False))

Iar în cazul apelului doar pe *linkuri* se observă absența parametrului ’form’.

# References

|  |  |
| --- | --- |
| [1] | T. B. Azad, Introduction to Security, 2008. |
| [2] | J. D. GROOT, What is Cyber Security? Definition, Best Practices & More, Data Insider, 2020. |
| [3] | G. S. M. E. Zachary Cohen, What we know about the pipeline ransomware attack: How it happened, who is responsible and more, CNN, 2021. |
| [4] | R. Gibb, What is a Web Application?, 2016. |
| [5] | OWASP, „Web Application Security Testing,” [Interactiv]. Available: https://owasp.org/www-project-web-security-testing-guide/v41/4-Web\_Application\_Security\_Testing/. [Accesat 01 Iunie 2021]. |
| [6] | „Requests: HTTP for Humans,” [Interactiv]. Available: https://docs.python-requests.org/en/master/. [Accesat 02 Iunie 2021]. |
| [7] | „urllib.parse — Parse URLs into components,” [Interactiv]. Available: https://docs.python.org/3/library/urllib.parse.html#module-urllib.parse. [Accesat 02 Iunie 2021]. |
| [8] | „urllib.request — Extensible library for opening URLs,” [Interactiv]. Available: https://docs.python.org/3/library/urllib.request.html#module-urllib.request. [Accesat 02 Iunie 2021]. |
| [9] | [Interactiv]. Available: https://www.crummy.com/software/BeautifulSoup/bs4/doc/. [Accesat 02 Iunie 2021]. |
| [10] | [Interactiv]. Available: https://docs.python.org/3/library/ssl.html. [Accesat 02 Iunie 2021]. |
| [11] | [Interactiv]. Available: https://docs.python.org/3/library/socket.html. [Accesat 02 Iunie 2021]. |
| [12] | [Interactiv]. Available: https://docs.python.org/3/library/subprocess.html. [Accesat 02 Iunie 2021]. |
| [13] | Randy. [Interactiv]. Available: https://whatsabyte.com/blog/processor-threads/. [Accesat 02 Iunie 2021]. |
| [14] | [Interactiv]. Available: https://docs.python.org/3/library/tkinter.html. [Accesat 02 Iunie 2021]. |
| [15] | [Interactiv]. Available: https://docs.python.org/3/library/os.html. [Accesat 02 Iunie 2021]. |
| [16] | [Interactiv]. Available: https://docs.python.org/3/library/re.html. [Accesat 02 Iunie 2021]. |
| [17] | „Metasploitable 2,” [Interactiv]. Available: https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/. [Accesat 02 Iunie 2021]. |
| [18] | [Interactiv]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\_Application\_Security\_Testing/. [Accesat 02 Iunie 2021]. |
| [19] | [Interactiv]. Available: https://github.com/praetorian-inc/Hob0Rules/blob/master/wordlists/rockyou.txt.gz. [Accesat 04 Iunie 2021]. |
| [20] | R. Janicki. [Interactiv]. Available: https://github.com/bl4de/dictionaries. [Accesat 04 Iunie 2021]. |
| [21] | spaddex. [Interactiv]. Available: https://github.com/spaddex/Admin-Finder/blob/master/admin\_locations.txt. [Accesat 04 Iunie 2021]. |
| [22] | F. N. A. Mathias Karlsson, „Detectify,” [Interactiv]. Available: https://labs.detectify.com/2013/05/29/the-ultimate-sql-injection-payload/. [Accesat 04 Iunie 2021]. |