

**Discovering Knowledge**

**FYP Proposal Defense Proforma**

**2022**

**Black Pearl**

**Group Members**

|  |  |  |  |
| --- | --- | --- | --- |
| **Enrollment #** | **Name** | **Email** | **Contact No** |
| 02-131192-044 | Muhammad Umer Adeem | adeemumer800@gmail.com | 03470707178 |
| 02-131192-052 | Sajjad Ahmed |  |  |
| 02-131192-017 | Muhammad Hasnain |  |  |

**Supervised by**

<<Faculty Member Name>>

**Department of Software Engineering**

Bahria University Karachi Campus

# Introduction

# The project is related to the field of Cyber security.

# Specialized in automatic Web Application Penetration Testing.

# The application will conduct:

# Reconnaissance.

# Enumeration & Scanning.

# Vulnerability Scanning.

# Cross checking of any identified vulnerability.

# Background

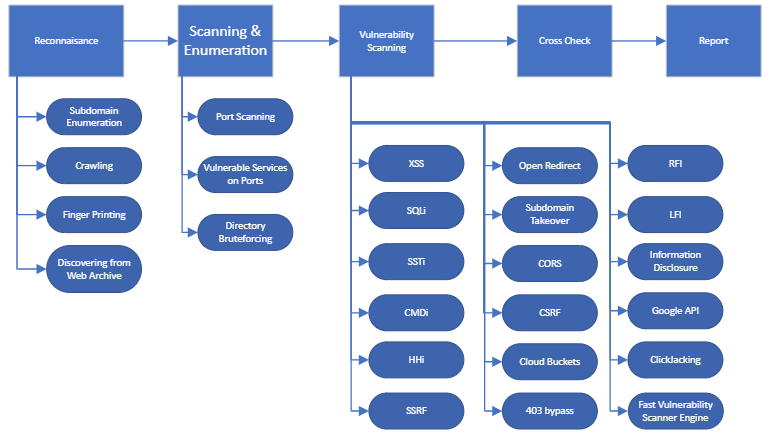
* **Previous FYPs:**
  + **OWAPT (2021)**
    1. Reconnaisance: Crawling
    2. Identify Vulnerabilities:
       - SQLi
       - Login Sequences
       - Buffer Overflow
       - HTTP parameter pollution
       - Content Spoofing
       - URL Manipulation
       - XSS
       - Clickjacking
    3. Reporting
  + **SWAPTT**
    1. **Reconnaissance:** Crawling, Hakrawler
    2. **Scanning:** Scanning for Open Ports
    3. **Identify Vulnerabilities:**
       - SSH brute force
       - Subdomain Takeover
       - CVE-41773
       - CORS
       - XSS
       - Proxyshell
       - Verb Tampering
       - SQLi
    4. **Reporting**
* **Some Vulnerability Scanners**
  + **Burp Suite's Active Scanner:**
    - Scans for a wide variety of vulnerabilities.
    - Large number of False positives.
    - Pro: 449$ per year.
    - Enterprise: 8000$ per year.
  + **Nessus:**
    - Scans limited web application vulnerabilities, more focused on network vulnerabilities.
    - 2000$ - 3000$ per year.

# Problem Statement

* + Web Applications are one of the main targets of adversaries. Many events have been reported, which led to complete compromise of confidentiality, integrity, availability of the Organizations because of Web vulnerabilities.
  + Organizations need to conduct vulnerability scanning and Penetration tests on their own.
  + Existing Solutions are scanning for limited vulnerabilities, generate many false positives and are quite expensive.

# Proposed Solution

* **Features of the project**
  + Reconnaissance:
    - Subdomain Enumeration
    - Crawling
    - Fingerprinting
    - Discover from web archive
  + Enumeration & Scanning:
    - Scan for Open Ports, discover services running on them and if they are vulnerable to an attack.
    - Finding hidden files and Directories and crawling again on discovered files if needed.
  + Vulnerability Scanning & exploitation:
    - XSS
    - SQLi
    - SSTi
    - Command Injections
    - Host Header Injections
    - Open Redirect
    - SSRF
    - Subdomain Takeover.
    - CORS
    - Cloud Bucket Misconfigurations
    - 403 bypass
    - Clickjacking
    - RFI
    - LFI
    - Information Disclosure
    - Google API Misconfiguration
    - CSRF
  + Cross Checking for any identified Vulnerability to minimize false positives.
  + Fast Vulnerability Scanner Engine:
    - Scanning for famous vulnerabilities not covered in previous section.
    - Scanning for vulnerabilities in outdated 3rd party components integrated with websites.
    - Zero False Positives.
    - E.g.
      * Get: <base url>/locale/?memory=/etc/passwd
      * Match: “:root:”
  + Reporting
* **Methodology**



* **Technologies to be used**
  + HTML, CSS, JS for front end.
  + Django for backend.
* **Sustainable Development Goals Mappings**
  + Goal 8: Decent Work and Economic Growth.
  + Goal 9: Industry, Innovation and Infrastructure.

# Project Scope

* The goal is to provide:
  + An automated Web Application Penetration Testing Software.
  + Recon a web domain to find many of the information related to it, which only an experienced hacker can harvest.
  + Testing each port of a website.
  + Testing many different types of vulnerabilities as discussed.
  + Fast Vulnerability Scanner Engine.
  + Having minimum false positives.
  + Reports.

# Gantt Chart

# Chart Description automatically generated

# References

* [1] OWASP TOP 10 SECURITY VULNERABILITIES - 2020

[OWASP Top Ten Web Application Security Risks | OWASP](https://owasp.org/www-project-top-ten/)

* [2] TENABLE’S NESSUS

[Nessus](https://www.tenable.com/buy)

* [3] PORTSWIGGER’S BURP SUITE

[Burp Suite](https://portswigger.net/burp)

**FYP Supervisor: FYP Coordinator:**

Signatures: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signatures: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Note: Supervisor! please write your email address against signatures if emailed)