



WebPloit

INVINCIBILITY LIES IN THE DEFENSE

MATCHING SEQUENCE

Lorem ipsum dolor sit amet
adipiscing elit. Proin sed

**An Automated Vulnerability
Assessment Tool**



Project Members:

SHAFQAT ABBAS	(190774)
MUHAMMAD OZAIR MALIK	(190798)
MUHAMMAD ASIF MASOOD	(190794)

Supervised By:

DR. MOHAMMAD IMRAN
Department of Cyber Security
Air University, Islamabad

WHAT IS WEBPLOIT?

WebPloit is an ***automated vulnerability assessment tool***, capable of in depth evaluation of web applications. It is planned to be a ***complete web-based tool***, allowing the user to ***enter the URL of the target and get a complete assessment report*** in return.

WebPloit will have its own ***complete database of known payloads*** for the assessment of the following vulnerabilities:

- Reflected Open Redirect Vulnerability
- Reflected XSS
- Stored XSS
- Union based SQL Injection
- Blind SQL Injection
- XXE (XML External Entity)

All the payloads will be automatically launched on to the target, and on the basis of the success rate, the vulnerability will be categorized according to the ***CVSS (Common Vulnerabilities Scoring System)***. Upon the scan termination, user will be able to see a complete report for the targeted URL.



SIGNIFICANCE OF THE PROJECT

WebPloit aims at becoming an indigenous solution for the web application industry of Pakistan. It will always remain a closed-source tool built specifically for the IT industry and high profile departments, such as Government of Pakistan, and relevant organizations.

Following the broad level analysis of the standard assessment tools being currently used in the industry:

- **Nessus**
 - \$3390 / Year (Approx PKR 606000 / Year) for single user
- **Burp Suite Professional**
 - \$400 / Year (Approx PKR 71500 / Year) for single user

The above figures prove that there is a dire need of a self-made and fully capable tool for our local industry. WebPloit, in this regard, aims at filling this gap as a complete indigenous solution for the evaluation of web applications.



UTILITY OF THE PROJECT

This project aims to be utilized by the IT industry of Pakistan, so that our local departments can have a fully featured local built tool, meeting the industrial standards, and all this in a comparatively low price.

WebPloit will prove to be a significant milestone in the field of penetration testing for the local industry of Pakistan.



PROJECT SCOPE & DELIVERABLES



SCOPE

This project includes research and understanding of the relevant tools being used in today's world. Secondly, this project is aimed at creating a complete and fully capable of vulnerability assessment tool according to the description given in slide 03 (What is WebPloit).

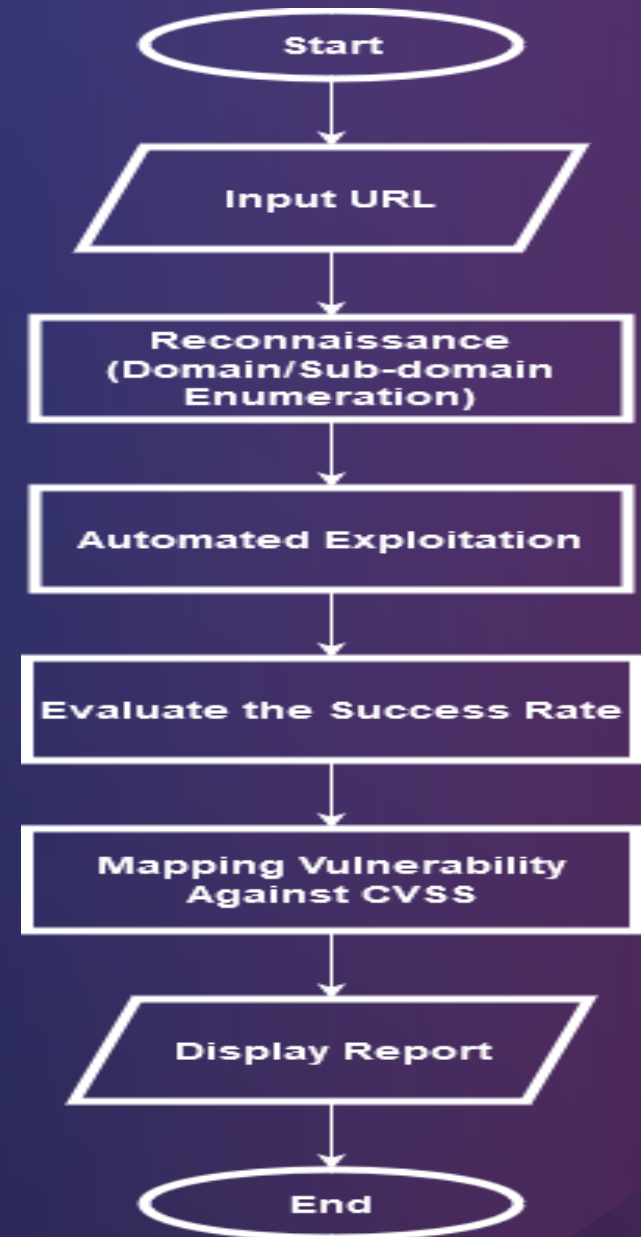


DELIVERABLES

A complete web application, along with complete documentation of the project.

HIGH LEVEL FLOW CHART

The beside mentioned is the high-level flowchart of the entire project, depicting the overall scenario of how this project is going to work.



TOOLS AND TECHNOLOGIES

FRONT-END

HTML



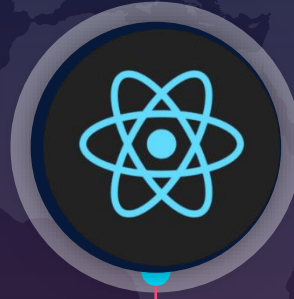
JAVASCRIPT



CSS



React JS



BACK-END

Django Framework
for APIs



Python



MongoDB



TIMELINE



FYP-I

INFORMATION GATHERING

- Research
- Study & understanding the related technologies
- Static front-end
- Developing initial APIs
- Reconnaissance (Enumeration)

FYP-II

VULNERABILITY ASSESSMENT

- Creation of payloads database
- Automating the exploitation
- Evaluation of vulnerabilities

FYP-III

FINALIZING

- Enhancing the whole project
- Report generation
- Adding user sign up / sign in features



***THANK
YOU***
