VIEHGROUP

High Level Design (HLD)

Bug Bounty Automation

Aman Kumar

VIEHGROUP

Abstract

A **bug bounty program** is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to
security exploits and vulnerabilities.

These programs allow the developers to discover and resolve bugs before the general public is aware of them, preventing incidents of widespread abuse. Bug bounty programs have been implemented by a large number of organizations

Automation is the latest trend in bug bounty hunting, with new frameworks being released every day. This ranges from full-fledged solutions with user interfaces and back-end databases to collections of custom-built Bash scripts. All of which have their uses depending on the level of control and depth of testing preferred by the user.

Some obvious benefits to bug bounty automation include:

- Easily identify low-hanging vulnerabilities.
- Continuous recon to capture changing environments.
- Maximize time and profit by automating repetitive tasks.

VIEHGROUP

Introduction

1. Why this High-Level Design Document?

The purpose of this High-Level Design (HLD) Document is to add the necessary detail to the current project description to represent a suitable model for coding. This document is also intended to help detect contradictions prior to coding and can be used as a reference manual for how the modules interact at a high level.

The HLD will:

- Present all the design aspects and define them in detail
- Describe the user interface being implemented
- Describe the hardware and software interfaces
- Describe the performance requirements
- Include design features and the architecture of the project

2. Scope

The HLD documentation presents the structure of the system, such as the database architecture, application architecture (layers), application flow (Navigation), and technology architecture. The HLD uses non-technical to mildly technical terms which should be understandable to the administrators of the system.

General Description

Objectives

• It is the collection of pentesting tools. It's scan the target and generates the reports in text format.

Benefits

• Easily identify low-hanging vulnerabilities.

• Continuous recon to capture changing environments.

• Maximize time and profit by automating repetitive tasks.

Data Sharing Agreement (Domain URL)

• Data Folder Name: Domain Name

• Number of File s: 8+ (Depends on number of Subdomains)

• Number of Folder: <User Defined>

• Files Name: NmapScan_$url.txt, Subdomains.txt, SubdomainsSorted.txt, Whois_$url.com, aliveSubdomains.txt, JsAliveSubdomains.txt, DomainsTakeover.txt

• File type: .TXT format

Tools used :

- vm ware
- kali linux

Flow Chart