ViPER
Penetration Testing Tool

Second Code Review

Guide: Binu Sir

Name: PS Narayanan
Roll No: U314BCA043

Overview

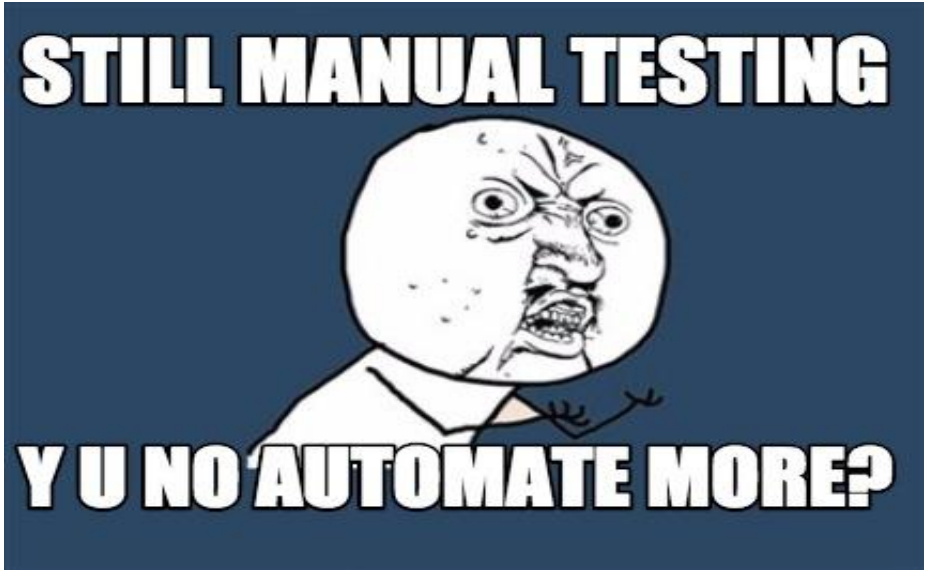
- **Introduction**
- **Information Disclosure**
  - Robots.txt Analysis
  - .git publicly exposed check
  - .svn/entries public access check
  - .htaccess public access check
- **Reconnaissance**
  - Extract Cookie
  - Decodes Base64 cookie automatically
- **Web Vulnerability Check**
  - SQli
    - URL based SQLi
    - Cookie Based
    - User-Agent Based

Introduction

- ViPER is a Web App Pentesting Tool / CTF Automator
- Automates manual reconnaissance technique
- Checks for Web based attacks

Introduction

Why ViPER ?



Information Gathering

Robots.txt Analysis

```
# username: admin
# password :@dm!n

User-Agent: *

Disallow: /admin/
```

Information Gathering

.git publicly exposed check

- It is a Version Control System
- It will keep a copy of source code
- We can see what changes are made and who has changed the file

Information Gathering

.git publicly exposed check

How it can be vulnerable?

- Git clone command [git clone www.example.com/.git] will give us the entire source code

Information Gathering

.svn entries publicly exposed check

- **It’s a Version Control System**
- **Is a collection of files and directories and keeps tracks of all changes that have made to this files**

Information Gathering

.svn entries publicly exposed check

How it can be vulnerable?

- Wget command [wget www.example.com/.svn/entries] will give us the entire source code

Information Gathering

.htaccess publicly exposed

- It’s a configuration file for use on web servers running the apache web server
- It gives information about server configuration

Reconnaissance

Cookie

- Extract Cookies
- Checks for encoded cookies and automatically decode it (Base64)

Web Attacks

SQLi

- Top one in OWASP top ten web attacks
- Injection of sql query
- Server side attack

Web Attacks

SQLi

- Types
  - URL Based
  - Cookie Based
  - User-Agent Based