**Experiment-1**

**Name: Dhrish S Kumar**

**Unique ID:** E0320008

**Problem Statement:**

Program to check vulnerabilities in web applications

**Tools Used:**

**Red-Hawk:**

Red Hawk is an open source tool that is used for information gathering and certain

vulnerability scanning. Red Hawk detects Content Management Systems (CMS) in use of a

target web application, IP address, web server record, Cloudflare information, and robots.txt

data. Red Hawk can detect WordPress, Drupal, Joomla, and Magento CMS. Other scanning

features of Red Hawk include WHOIS data collection, Geo-IP lookup, Banner grabbing, DNS

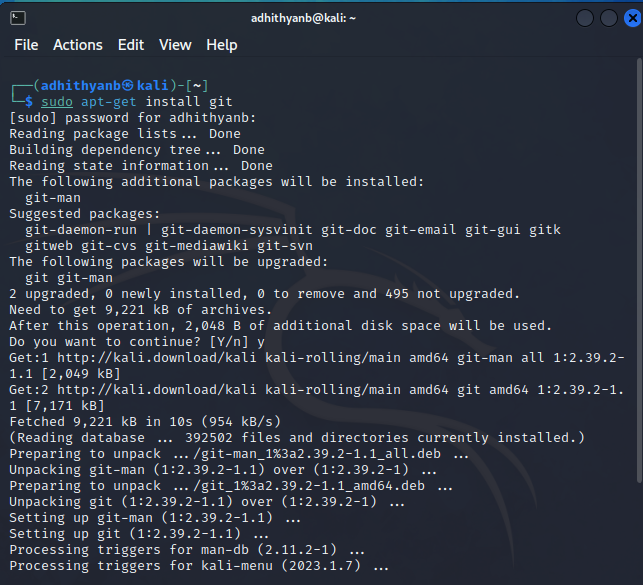
lookup, port scanning, sub-domain information, reverse IP, and MX records lookup. As a

vulnerability scanner, Red Hawk looks for error based SQL injections, WordPress sensitive

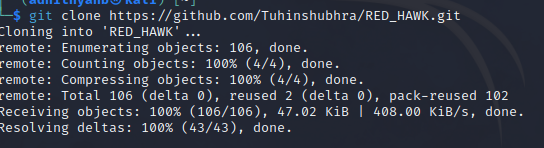
files, and WordPress version related vulnerabilities.

**Procedure:**

1. Installation of ‘git’ in linux:

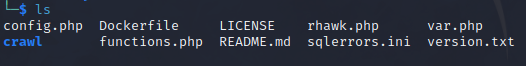


2. Red hawk installation:

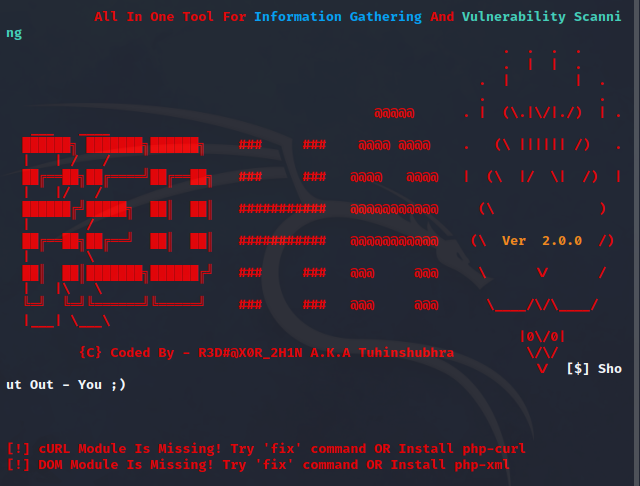


3. Using red hawk:

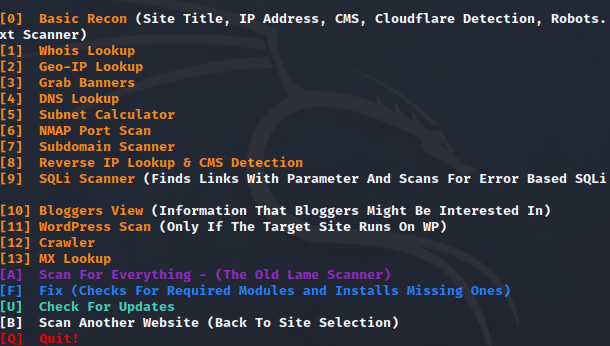




Php rhawk.php:-



4.Launching the tool:



5.Choosing Vulnerability assessment

