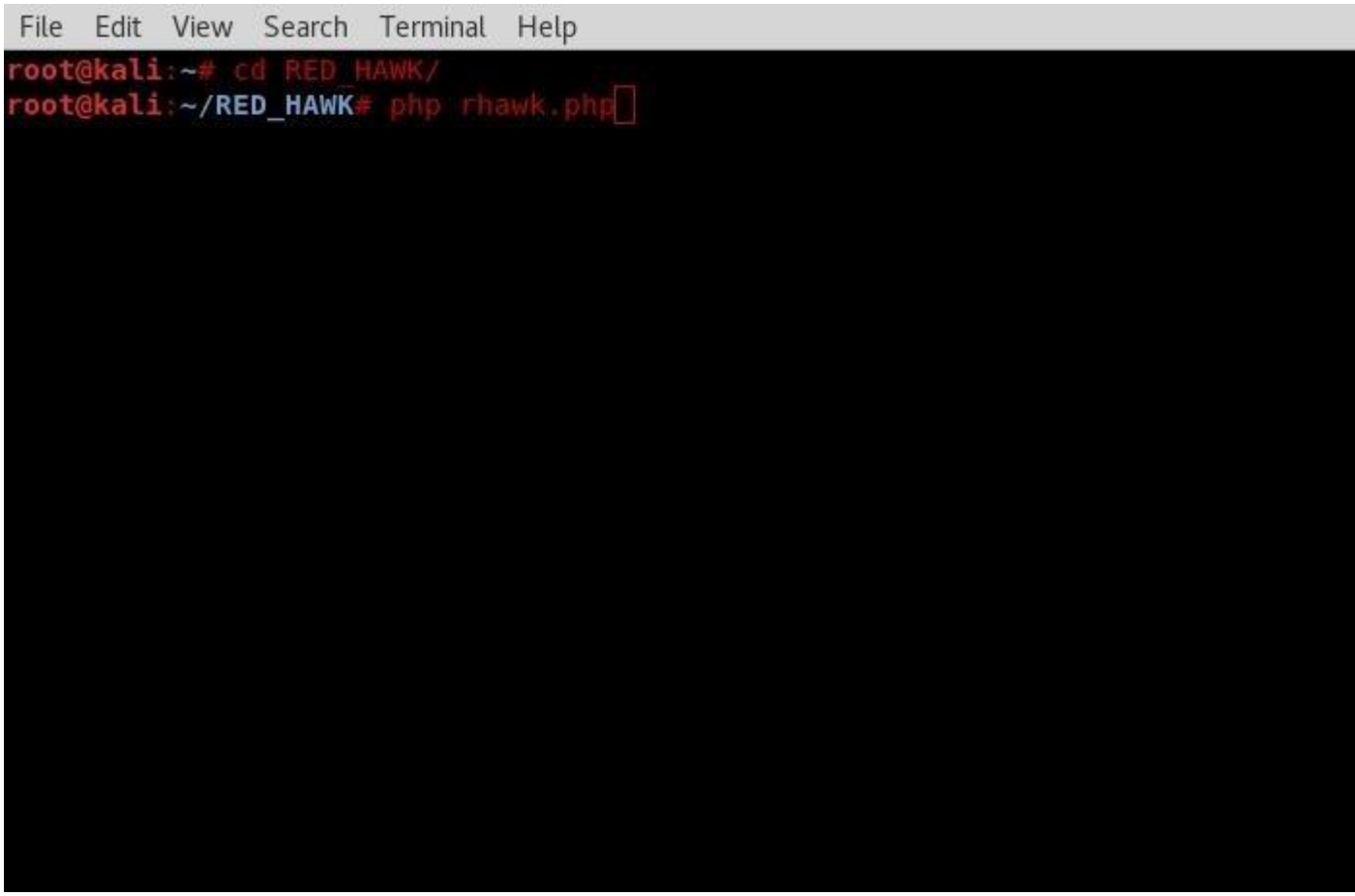
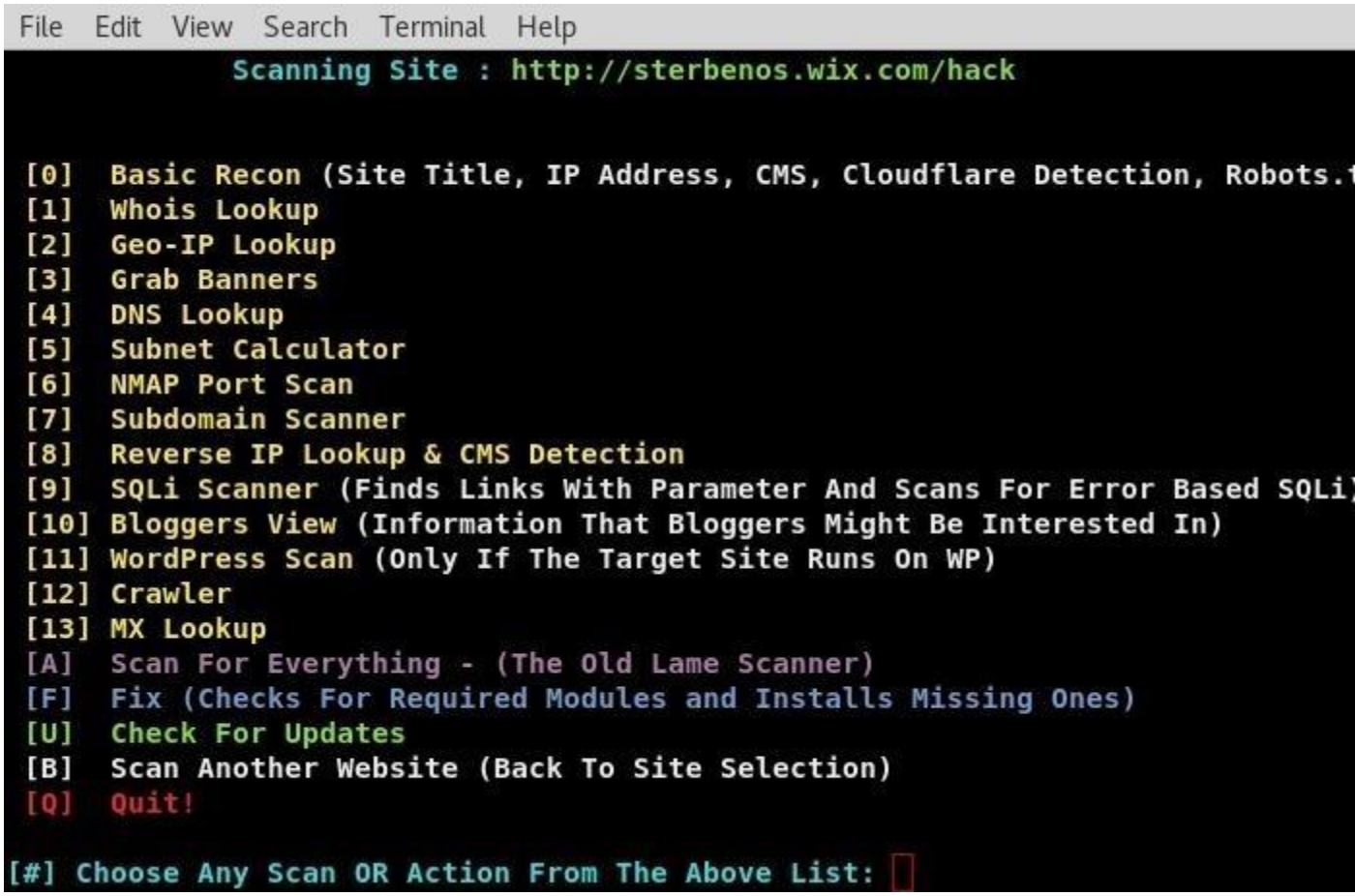
RED_HAWK:

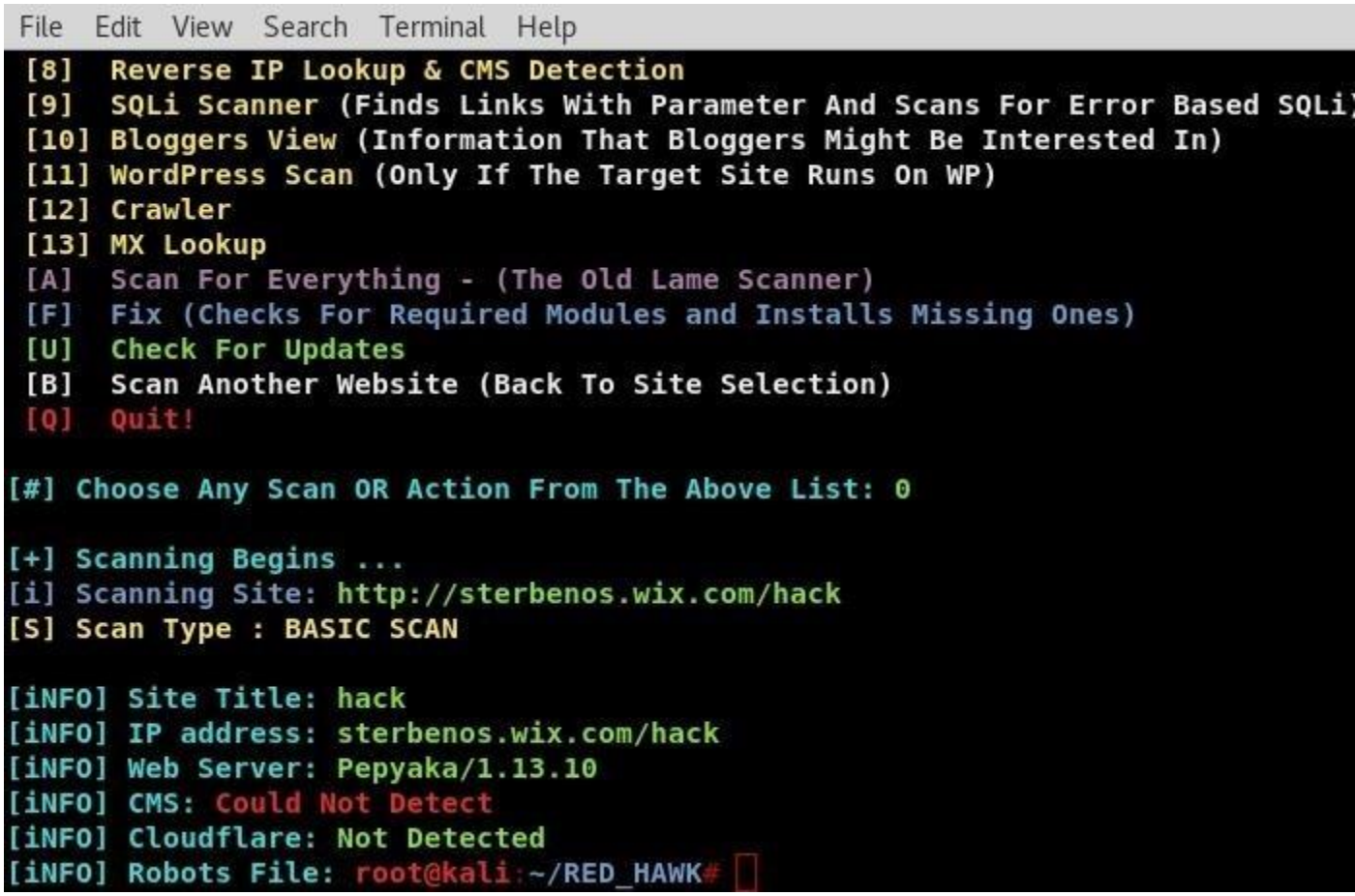
git clone github.com/Tuhinshubhra/RED_HAWK
Then change to red hawk directory:
cd RED_HAWK
Now lets run it:
php rhawk.php



Now enter your website and hit enter. Then specify between whether it uses http or https. We now have options of what we would like red hawk to search for. we are going to go with option one. As mapping out our target site is one of the first steps in pentesting, using red hawk can easily help speed up this process by having these tools in one place.



As you can see red hawk has scanned our target site. From these we learned the target site does not use cloudflare ddos protection, runs Pepyaka version 1.13.10 ect. This is all useful information for mapping out target and from there trying to find ways we can attack. To use it agin just enter php rhawk.php from the same terminal. **if you closed it change directories to RED_HAWK/ agin.** Thats all for today folks, get to scanning !


File Edit View Search Terminal Help
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner (Finds Links With Parameter And Scans For Error Based SQLi)
[10] Bloggers View (Information That Bloggers Might Be Interested In)
[11] WordPress Scan (Only If The Target Site Runs On WP)
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates
[B] Scan Another Website (Back To Site Selection)
[Q] Quit!
[#] Choose Any Scan OR Action From The Above List: 0
[+] Scanning Begins ...
[i] Scanning Site: http://sterbenos.wix.com/hack
[S] Scan Type : BASIC SCAN
[iNFO] Site Title: hack
[iNFO] IP address: sterbenos.wix.com/hack
[iNFO] Web Server: Pepyaka/1.13.10
[iNFO] CMS: Could Not Detect
[iNFO] Cloudflare: Not Detected
[iNFO] Robots File: root@kali:~/RED_HAWK#