Exercise No 9:VULNERABILITY ANALYSIS - CGI Scanning with Nikto

Aim: To perform vulnerability Analysis using CGI Scanning with Nikto

Procedure:

Step 1: open a terminal window and type nikto –H and press enter

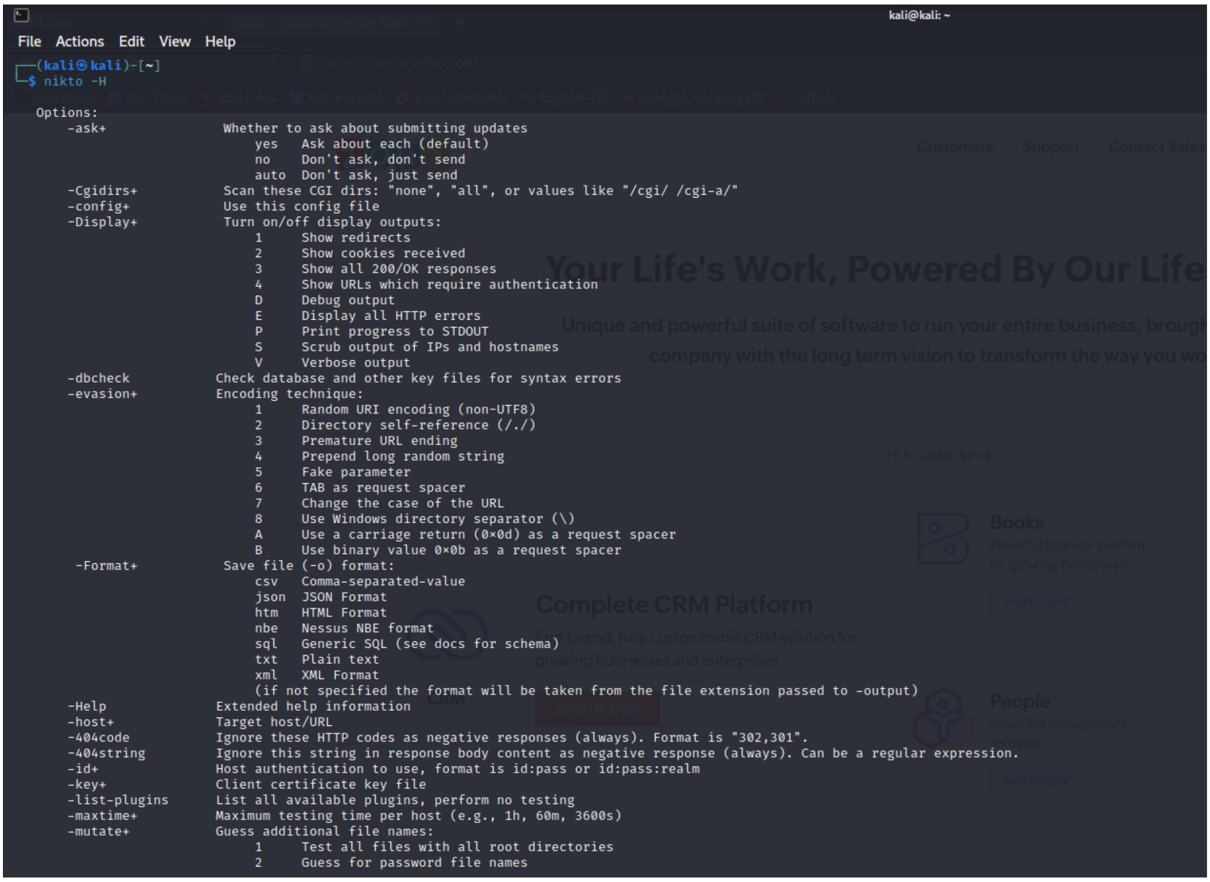
Step 2: Type nikto –h <website> Tuning x and press enter

Step 3: Nikto starts web server scanning with all tuning options enabled.

Step4:In the terminal window type “nikto –h <website>-Cgidirs all”and hit enter

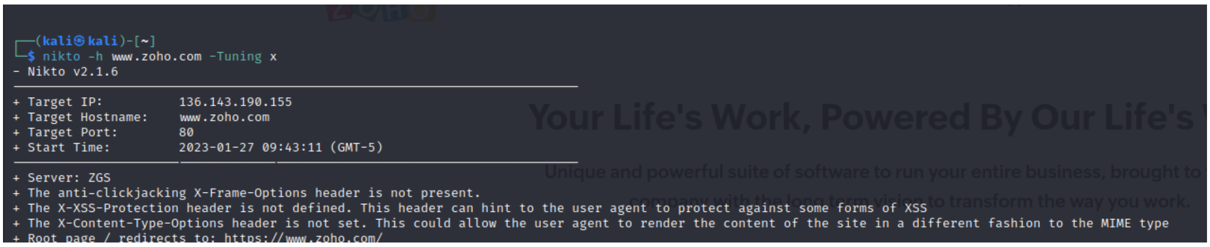
Step 5. Nikto will scan the webserver as it looks vulnerable CGI directories. It scans the webserverand list out the directories

OUTPUT:

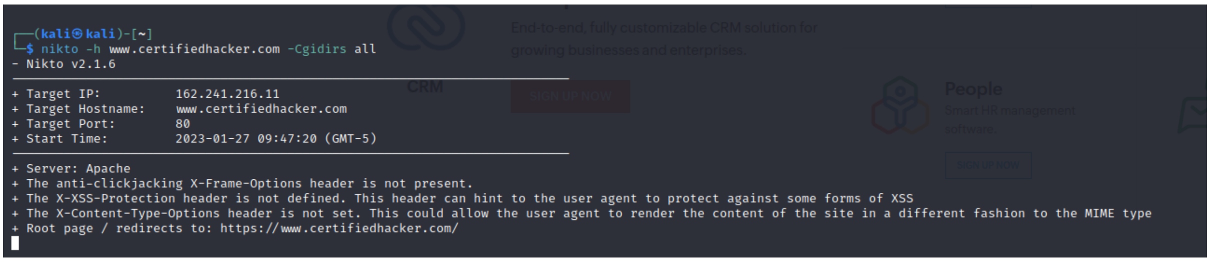


```
┌──(kali㉿kali)-[~]
└─$ nikto -H

   Options:
       -ask+               Whether to ask about submitting updates
                                yes   Ask about each (default)
                                no    Don't ask, don't send
                                auto  Don't ask, just send
       -Cgidirs+           Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
       -config+            Use this config file
       -Display+           Turn on/off display outputs:
                                1     Show redirects
                                2     Show cookies received
                                3     Show all 200/OK responses
                                4     Show URLs which require authentication
                                D     Debug output
                                E     Display all HTTP errors
                                P     Print progress to STDOUT
                                S     Scrub output of IPs and hostnames
                                V     Verbose output
       -dbcheck           Check database and other key files for syntax errors
       -evasion+          Encoding technique:
                                1     Random URI encoding (non-UTF8)
                                2     Directory self-reference (/./)
                                3     Premature URL ending
                                4     Prepend long random string
                                5     Fake parameter
                                6     TAB as request spacer
                                7     Change the case of the URL
                                8     Use Windows directory separator (\)
                                A     Use a carriage return (0×0d) as a request spacer
                                B     Use binary value 0×0b as a request spacer
        -Format+           Save file (-o) format:
                                csv   Comma-separated-value
                                json  JSON Format
                                htm   HTML Format
                                nbe   Nessus NBE format
                                sql   Generic SQL (see docs for schema)
                                txt   Plain text
                                xml   XML Format
                                (if not specified the format will be taken from the file extension passed to -output)
       -Help              Extended help information
       -host+             Target host/URL
       -404code           Ignore these HTTP codes as negative responses (always). Format is "302,301".
       -404string         Ignore this string in response body content as negative response (always). Can be a regular expression.
       -id+               Host authentication to use, format is id:pass or id:pass:realm
       -key+              Client certificate key file
       -list-plugins      List all available plugins, perform no testing
       -maxtime+          Maximum testing time per host (e.g., 1h, 60m, 3600s)
       -mutate+           Guess additional file names:
                                1     Test all files with all root directories
                                2     Guess for password file names
```



```
┌──(kali㉿kali)-[~]
└─$ nikto -h www.zoho.com -Tuning x
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          136.143.190.155
+ Target Hostname:    www.zoho.com
+ Target Port:        80
+ Start Time:         2023-01-27 09:43:11 (GMT-5)
---------------------------------------------------------------------------
+ Server: ZGS
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.zoho.com/
```



```
┌──(kali㉿kali)-[~]
└─$ nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2023-01-27 09:47:20 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.certifiedhacker.com/
```

RESULT: Hence we have performed vulnerability analysis using CGSI scanning with Nikto has executed successfully