

VULNERABILITY ANALYSIS USING NIKTO

Ex No :6

Date :08-05-2023

Aim :

To do Vulnerability analysis using Nikto.

Procedure :

- Open the Kali Linux.
- Open the Root Terminal
- TYPE nikto -h www.zoho.com -Tuning x COMMAMD
- Nikto starts web scanning with all turning options enabled.
- TYPE nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto will scan web server as it looks vulnerable CGI directories. It scans webserver and list of directories.

Output :

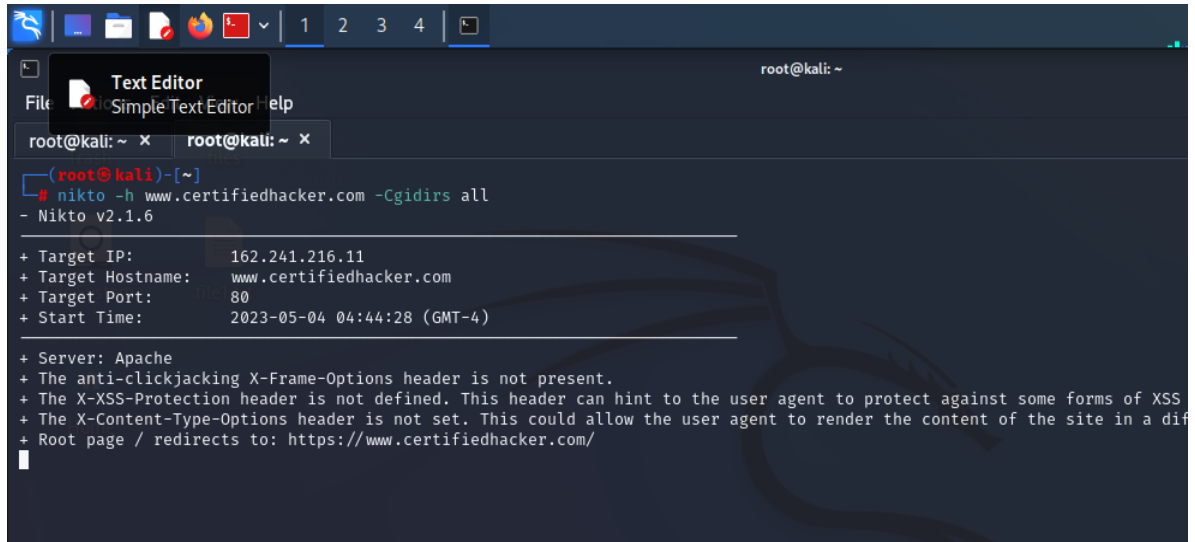
1.open terminal and type nikto -h www.zoho.com -tuning x commamd



```
root@kali: ~  
# nikto -h www.zoho.com -Tuning x  
- Nikto v2.1.6  
+ Target IP: 103.89.74.77  
+ Target Hostname: www.zoho.com  
+ Target Port: 80  
+ Start Time: 2023-05-04 04:43:14 (GMT-4)  
+ 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/
```

2.nikto starts web scanning with all tuning options enabled

3.type nikto -h www.certifiedhacker.com -cgidirs all



The screenshot shows a terminal window on a Kali Linux system. The user has executed the command `nikto -h www.certifiedhacker.com -cgidirs all`. The output displays the Nikto v2.1.6 version and scan details for the target IP 162.241.216.11. The scan identifies several security issues: the anti-clickjacking X-Frame-Options header is missing, the X-XSS-Protection header is not defined, and the X-Content-Type-Options header is not set. Additionally, it notes that the root page redirects to <https://www.certifiedhacker.com/>.

```
root@kali: ~  
root@kali: ~  
(root@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: 2023-05-04 04:44:28 (GMT-4)  
  
+ 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 dif  
+ Root page / redirects to: https://www.certifiedhacker.com/  
|
```

4.Nikto will scan web server as it looks vulnerable CGI directories. It scans webserver and list of directories.

Result :

Hence the Vulnerability Analysis using Nikto is Executed.