

ETHICAL HACKING

EXPERIMENT 9 – VULNERABILITY ANALYSIS USING NIKTO

1.OPEN TERMINAL AND TYPE `nikto -h www.zoho.com -Tuning x` COMMAND



```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
(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`



```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
(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 different fashion to the MIME type  
+ 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.