

## EXPERIMENT 11:

## OUTPUT:

```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali-Linux-2021.4
Windows 7 x64
kali@kali:~$ nikto -h www.amazon.com -i 100.159.13.128 -p 80 -u https://www.amazon.com/ -e /etc/nikto/ -o /root/.nikto/ -f /root/.nikto/ -s /root/.nikto/ -t /root/.nikto/ -v 2.1.6
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-bin/"
  -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
              5 Debug output
              6 Display all HTTP errors
              7 Print progress to STDOUT
              8 Scrub output of IPs and hostnames
              9 Verbose output
  -dbschema+ Check database and other key files for syntax errors
  -encoding+ Encoding techniques:
              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 (\)
              9 Use a carriage return (0x0d) as a request spacer
              0 Use binary value 0x00 as a request spacer
  -format+   Save file (-o) format:
              csv Comma-separated-value
              json JSON Format
              htm HTML Format
              nbs Nessus NIS 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
  -ignore+   Ignore these HTTP codes as negative responses (always). Format is "302,301".
  -instring+ 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, 3000s)
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

```
Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali-Linux-2021.4
Windows 7 x64
kali@kali:~$ nikto -h www.amazon.com -i 100.159.13.128 -p 80 -u https://www.amazon.com/ -e /etc/nikto/ -o /root/.nikto/ -f /root/.nikto/ -s /root/.nikto/ -t /root/.nikto/ -v 2.1.6
+ Target IP: 100.159.13.128
+ Target Hostname: www.amazon.com
+ Target Port: 80
+ Start Time: 2022-09-29 01:06:39 (GMT-4)

+ Server: CloudFront
+ Retrieved via header: 1.1 dd93e58995887f8fc14ed6ebae575e.cloudfront.net (CloudFront), HTTP/1.1 forward.http.proxy:3128
+ 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
+ Uncommon header 'x-amz-cf-pop' found, with contents: MAA51-P3
+ Uncommon header 'x-cache' found, with contents: Redirect from cloudfront
+ Uncommon header 'x-amz-cf-id' found, with contents: w6x510w6029d9g0v58y8yhg8N72cU8RG0D76PTIWg-Q5Bp0v0vQ=
+ 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.amazon.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 19 error(s) and 7 item(s) reported on remote host
+ End Time: 2022-09-29 01:12:29 (GMT-4) (350 seconds)

+ 1 host(s) tested
kali@kali:~$ nikto -h www.certifiedhacker.com -cgidirs all -i 162.241.216.11 -p 80 -u https://www.certifiedhacker.com/ -e /etc/nikto/ -o /root/.nikto/ -f /root/.nikto/ -s /root/.nikto/ -t /root/.nikto/ -v 2.1.6
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2022-09-29 01:13:42 (GMT-4)

+ Server: nginx/1.19.10
+ Retrieved via header: HTTP/1.1 forward.http.proxy:3128
+ 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
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'host-header' found, with contents: c2h0wVxLm5dW0b3N0LmNvQ=
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ 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
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 16 error(s) and 9 item(s) reported on remote host
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

