

Exercise No:9

Dhanush S
192021037

VULNERABILITY ANALYSIS - CGI Scanning with Nikto

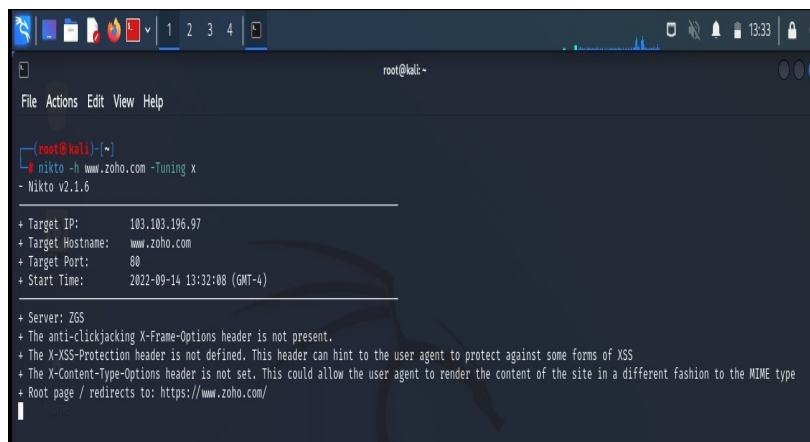
Aim:

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



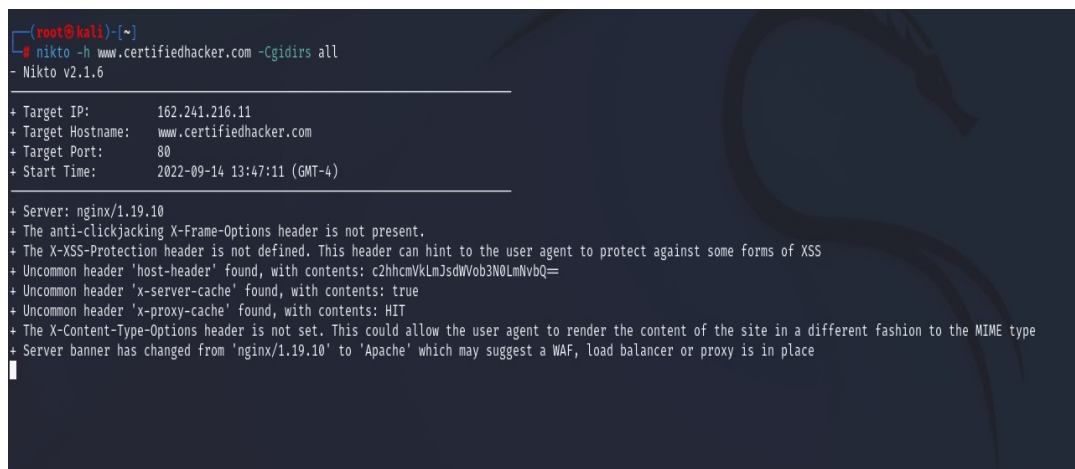
```
(root@kali)-[~]
└─$ nikto -h www.zoho.com -Tuning x
- Nikto v2.1.6

+ Target IP:      103.103.196.97
+ Target Hostname: www.zoho.com
+ Target Port:    80
+ Start Time:     2022-09-14 13:32:08 (GMT-4)

+ Server: 26S
+ 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/
```

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



```
(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:     2022-09-14 13:47:11 (GMT-4)

+ Server: nginx/1.19.10
+ 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 'host-header' found, with contents: c2hhcmVklmJsdWVob3N0LnNvbQ==
+ Uncommon header 'x-server-cache' found, with contents: true
+ 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
```

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

Output

1. nikto -h www.zoho.com -tuning x

```
(root@kali)~# nikto -h www.zoho.com -tuning x
- Nikto v2.1.6

+ Target IP: 169.148.146.97
+ Target Hostname: www.zoho.com
+ Target Port: 80
+ Start Time: 2023-01-27 03:18:07 (GMT-5)

+ Server: ZOS
+ 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
+ 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/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'zproxy' found, with contents: domain_not_configured
+ 510 requests: 6 error(s) and 5 item(s) reported on remote host
+ End Time: 2023-01-27 03:22:33 (GMT-5) (266 seconds)

+ 1 host(s) tested

(root@kali)~#
```

2. nikto -h www.certifiedhacker.com -Cgidirs all

```
(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: 2023-01-27 08:56:46 (GMT-5)

+ Server: Apache
+ 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
+ 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

vulnerability Analysis using CGI Scanning with Nikto is performed successfully.