

EXERCISE: VULNERABILITY ANALYSIS - CGI

Scanning with Niko

Aim: To perform vulnerability Analysis using CGI Scanning with Nikto

```
karthik@kali: ~  
- Nikto v2.1.6  
+ No web server found on 192.168.1.108:80  
+ 0 host(s) tested  
  
(karthik@kali)-[~]  
$ nikto -h 136.143.190.155 -tuning x  
- Nikto v2.1.6  
-----  
+ Target IP: 136.143.190.155  
+ Target Hostname: 136.143.190.155  
+ Target Port: 80  
+ Start Time: 2023-01-29 10:57:04 (GMT-5)  
-----  
+ Server: ZGS  
+ 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 'zproxy' found, with contents: domain_not_configured  
+ 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
```

```
karthik@kali: ~  
  
(karthik@kali)-[~]  
$ nikto -h 136.143.190.155 -cgidirs all  
- Nikto v2.1.6  
-----  
+ Target IP: 136.143.190.155  
+ Target Hostname: 136.143.190.155  
+ Target Port: 80  
+ Start Time: 2023-01-29 21:39:09 (GMT-5)  
-----  
+ Server: ZGS  
+ 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 'zproxy' found, with contents: domain_not_configured  
+ 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
```