

Vulnerabilities Analysis Using CGI Scanning with Nikto

1) What is CGI Scanning?

CGI (Common Gateway Interface) scripts are used by web servers to generate dynamic content.

Misconfigured or outdated CGI scripts can lead to:

- Remote Code Execution (RCE)
- Command Injection
- Information Disclosure
- Directory Traversal

Nikto is very effective at detecting insecure CGI scripts.

Syntax or Command

```
nikto -h http://example.com -Plugins cgi
```

Example command

```
nikto -h https://saveetha.com/ cgi
```

```
(bobby@vbox)-[~]$ nikto -h https://saveetha.com/ cgi
- Nikto v2.5.0
+ Multiple IPs found: 198.185.159.144, 198.185.159.145, 64:ff9b::c6b9:9f90, 6
4:ff9b::c6b9:9f91
+ Target IP: 198.185.159.144
+ Target Hostname: https://www.saveetha.com/ cgi
+ Target Port: 443
+ SSL Info: Subject: /CN=saveetha.com
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=Let's Encrypt/CN=R13
+ Start Time: 2025-12-29 14:30:55 (GMT5.5)
+ Server: Squarespace
+ /: Cookie crumb created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-contextid' found, with contents: z2acr9hL/uBiDA74x.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is set with max-age=0. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.saveetha.com/ found, with contents: true.
+ /VuB7YHpc.cgi: Uncommon header 'x-sqsp-edge' found, with contents: true.
| MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/uncommon-headers/
```

