Goal:

Web Fingerprinting & Vulnerability checks using whatweb & nikto

1. Command Used: **whatweb http://testfire.net**

Result:

http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][US], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.117], Java, Title[Altoro Mutual]

//////////////////////////

2. Command Used: **nikto -h http://testfire.net -o nikto1.txt**

Result:

+ Target IP: 65.61.137.117
+ Target Hostname: testfire.net
+ Target Port: 80
+ Start Time: 2025-09-12 07:32:56 (GMT-4)

+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ 7963 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2025-09-12 08:35:13 (GMT-4) (3737 seconds)

+ 1 host(s) tested