Nikto

Introduction

In Kali Linux, Nikto is a free and open-source web server and web application scanner. Nikto is a pluggable web server and CGI scanner written in Perl, using rfp's LibWhisker to perform fast security or informational checks. With the help of this popular Nikto Web Scanner tool, we can Scan your website and server immediately. This testing service can be used to test a Web Site, Virtual Host, and Web Server for known security vulnerabilities and misconfigurations. Nikto performs over 6000 tests against a website. A large number of tests for both security vulnerabilities and misconfigured web servers makes it a go-to tool for many security professionals and systems administrators. It can find forgotten scripts and other hard-to-detect problems from an external perspective. The Nikto web server scanner is a security tool that will test a website for thousands of possible security issues. Including dangerous files, misconfigured services, vulnerable scripts, and other issues. It is open source and structured with plugins that extend the capabilities. These plugins are frequently updated with new security checks. Nikto is by no means a stealthy tool. It will make over 2000 HTTP GET requests to the web server, creating a large number of entries in the web server's log files. This noise is actually an excellent way to test an in-place Intrusion Detection System (IDS) that is in place. Any web server log monitoring, host-based intrusion detection (HIDS), or network-based intrusion detection (NIDS) should detect a Nikto scan. Custom scans can be initiated using IDS bypass methods from libwhisker, however, the current version of our online scan is a default (no evasion) scan.

Features

The following are the features of the Nikto:

- Easily updatable CSV-format checks database,
- Output reports in plain text or HTML,
- Available HTTP versions automatic switching,
- Generic as well as specific server software checks,
- SSL support (through libnet-ssLeay-perl),
- Proxy support (with authentication),
- Cookies support.

Installation

If you're using Kali Linux, Nikto comes preinstalled and will be present in the "Vulnerability Analysis" category. If you don't have Nikto on Kali (for some reason), you can get Nikto from GitHub or just use the following command which is given below:

Open your Kali Linux and then Open your Terminal. Use the following command to install the tool:

```
sudo apt-get update
```

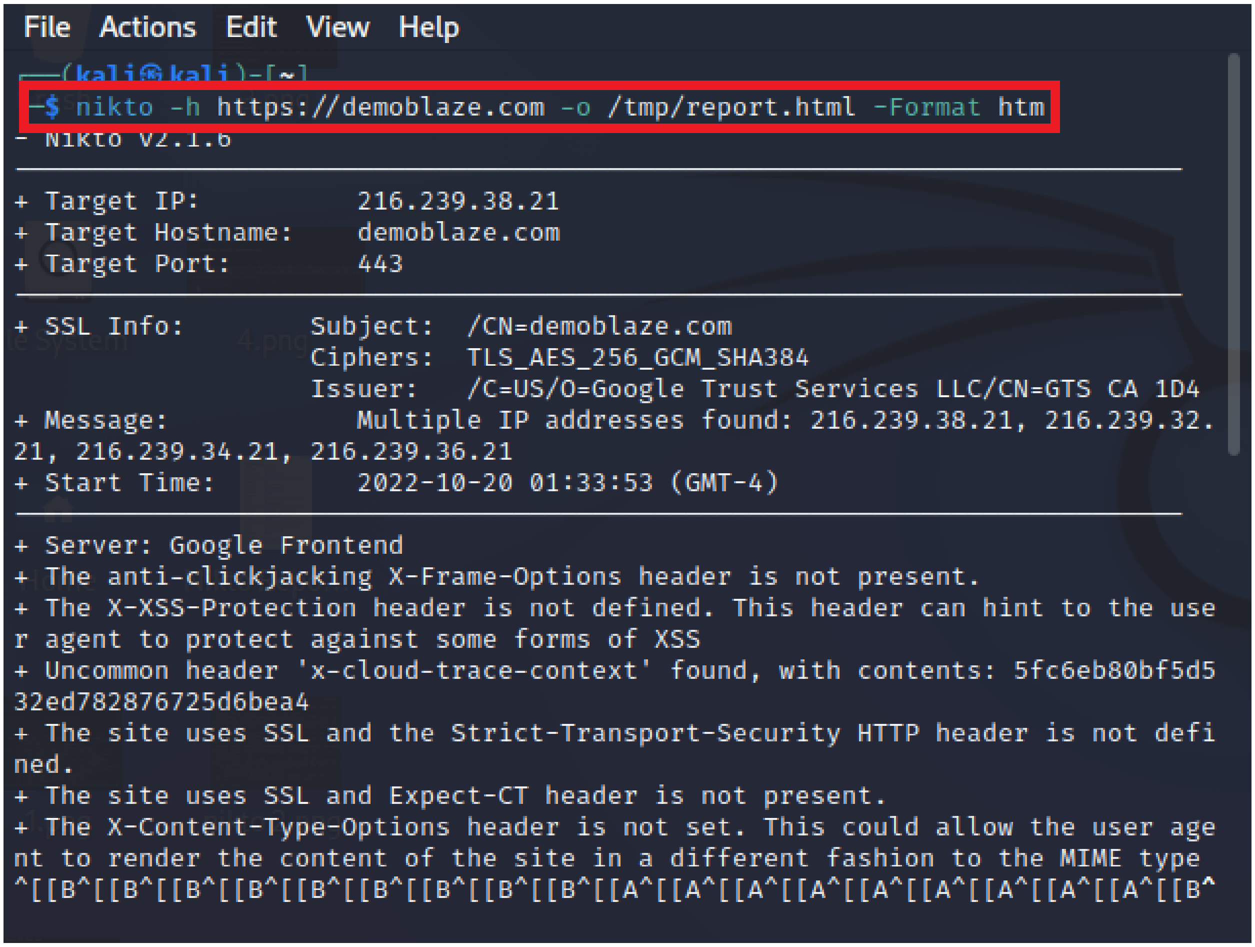
After updating apt database, We can install goldeneye using apt-get by running the following command:

```
sudo apt install nikto
```

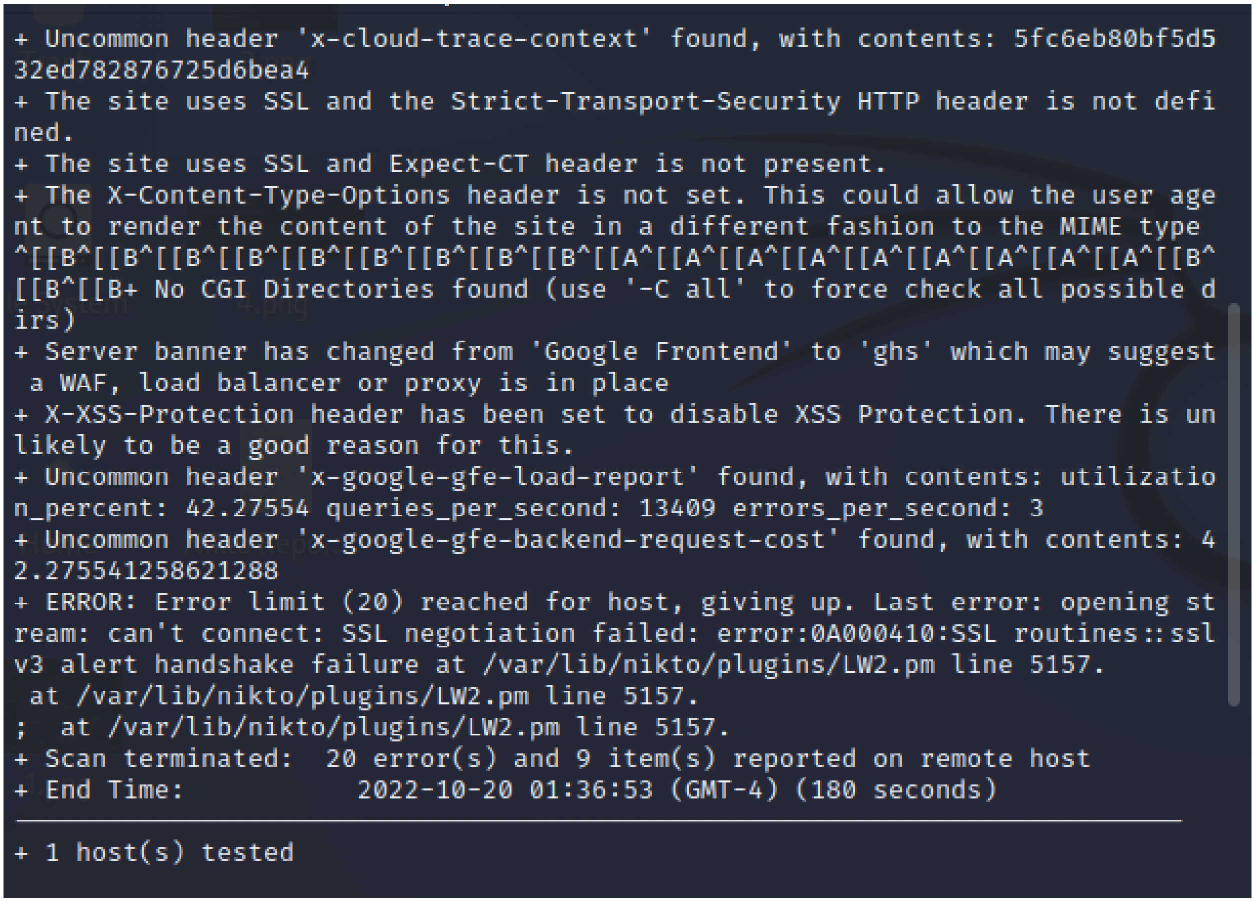
Usage

To check or scan the "demolaze.com" website and create an HTML report using the Nikto tool we can execute the following command:

```
Nikro –h https://demolaze.com –o /tmp/report.html –Format htm
```



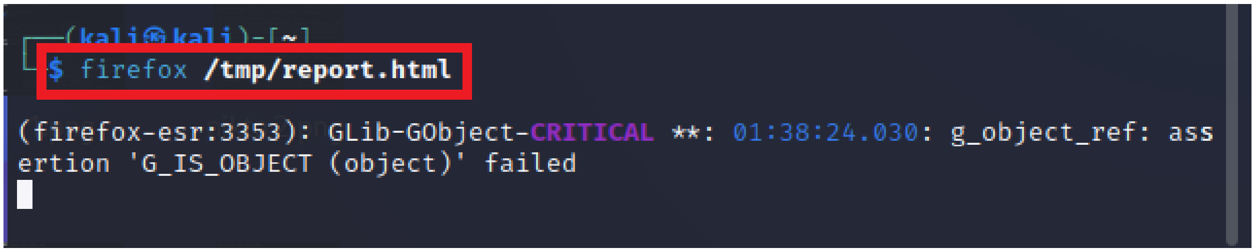
```
┌──(kali㉿kali)-[~]
└─$ nikto -h https://demoblaze.com -o /tmp/report.html -Format htm
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          216.239.38.21
+ Target Hostname:    demoblaze.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=demoblaze.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services LLC/CN=GTS CA 1D4
+ Message:            Multiple IP addresses found: 216.239.38.21, 216.239.32.
21, 216.239.34.21, 216.239.36.21
+ Start Time:         2022-10-20 01:33:53 (GMT-4)
---------------------------------------------------------------------------
+ Server: Google Frontend
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
r agent to protect against some forms of XSS
+ Uncommon header 'x-cloud-trace-context' found, with contents: 5fc6eb80bf5d5
32ed782876725d6bea4
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defi
ned.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[B^
```



```
+ Uncommon header 'x-cloud-trace-context' found, with contents: 5fc6eb80bf5d5
32ed782876725d6bea4
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defi
ned.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[B^
[[B^[[B+ No CGI Directories found (use '-C all' to force check all possible d
irs)
+ Server banner has changed from 'Google Frontend' to 'ghs' which may suggest
 a WAF, load balancer or proxy is in place
+ X-XSS-Protection header has been set to disable XSS Protection. There is un
likely to be a good reason for this.
+ Uncommon header 'x-google-gfe-load-report' found, with contents: utilizatio
n_percent: 42.27554 queries_per_second: 13409 errors_per_second: 3
+ Uncommon header 'x-google-gfe-backend-request-cost' found, with contents: 4
2.275541258621288
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening st
ream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::ssl
v3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5157.
 at /var/lib/nikto/plugins/LW2.pm line 5157.
;  at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated:  20 error(s) and 9 item(s) reported on remote host
+ End Time:           2022-10-20 01:36:53 (GMT-4) (180 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

To generate HTML report in Firefox browser using the Nikto tool we can execute the following command:

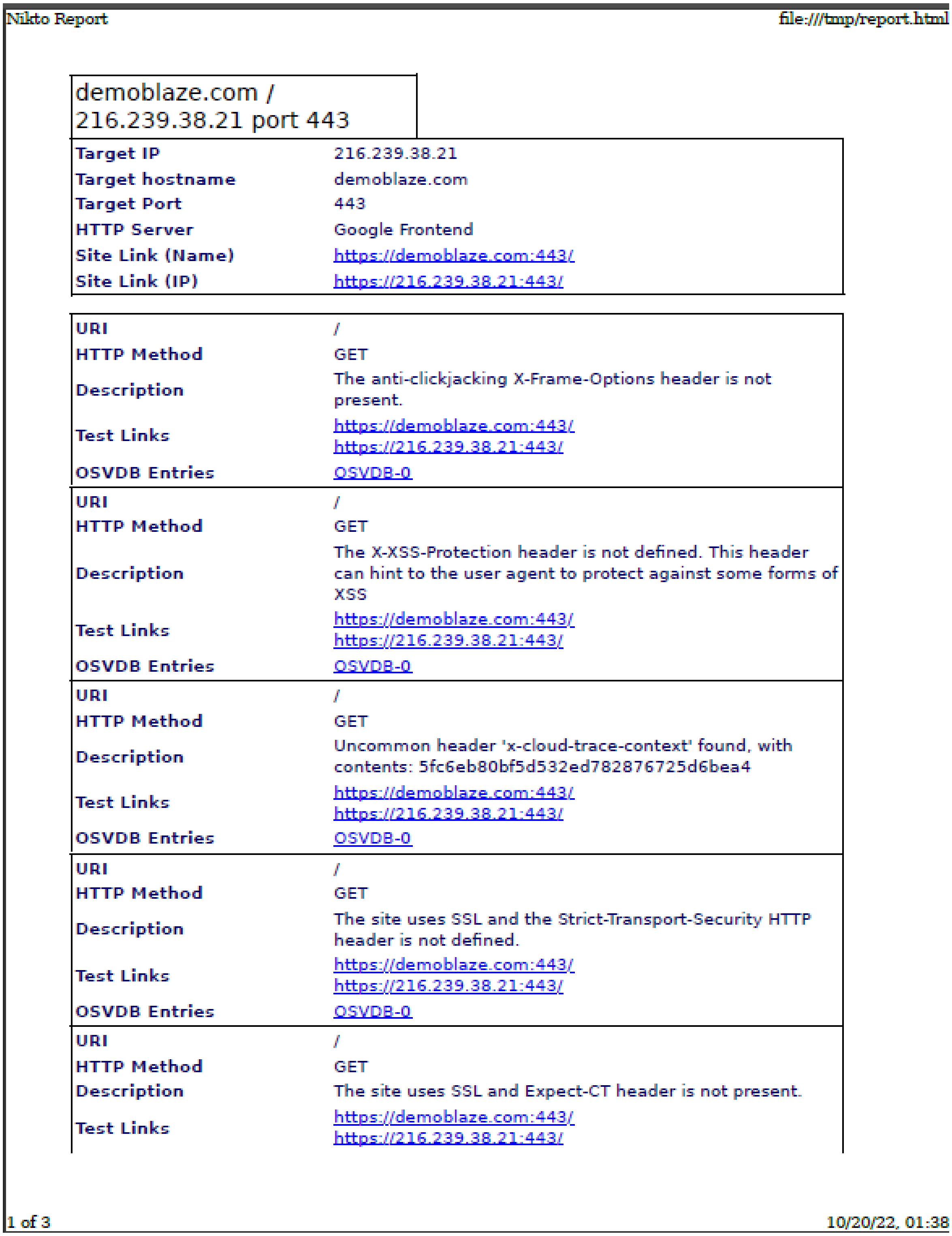
Firefox /tmp/report.html



```
┌──(kali㉿kali)-[~]
└─$ firefox /tmp/report.html

(firefox-esr:3353): GLib-GObject-CRITICAL **: 01:38:24.030: g_object_ref: ass
ertion 'G_IS_OBJECT (object)' failed
```

Generate report on above website given below:



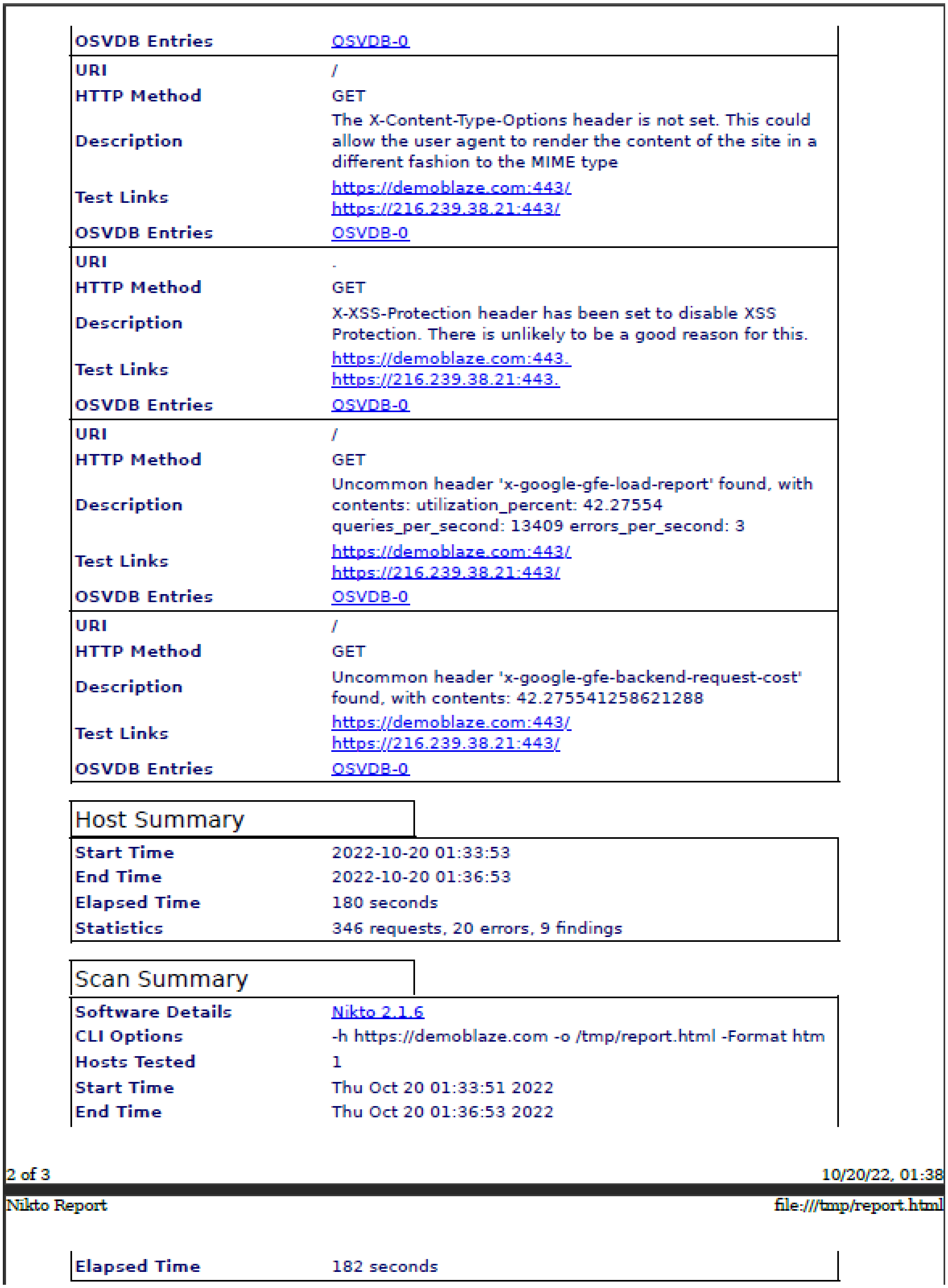
Nikto Report file:///tmp/report.html

demoblaze.com /
216.239.38.21 port 443

Target IP	216.239.38.21
Target hostname	demoblaze.com
Target Port	443
HTTP Server	Google Frontend
Site Link (Name)	https://demoblaze.com:443/
Site Link (IP)	https://216.239.38.21:443/

URI	/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	https://demoblaze.com:443/ https://216.239.38.21:443/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links	https://demoblaze.com:443/ https://216.239.38.21:443/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	Uncommon header 'x-cloud-trace-context' found, with contents: 5fc6eb80bf5d532ed782876725d6bea4
Test Links	https://demoblaze.com:443/ https://216.239.38.21:443/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
Test Links	https://demoblaze.com:443/ https://216.239.38.21:443/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The site uses SSL and Expect-CT header is not present.
Test Links	https://demoblaze.com:443/ https://216.239.38.21:443/

1 of 3 10/20/22, 01:38



OSVDB Entries	OSVDB-0

URI	/
HTTP Method	GET
Description	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
Test Links	https://demoblaze.com:443/ https://216.239.38.21:443/
OSVDB Entries	OSVDB-0

URI	.
HTTP Method	GET
Description	X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
Test Links	https://demoblaze.com:443. https://216.239.38.21:443.
OSVDB Entries	OSVDB-0

URI	/
HTTP Method	GET
Description	Uncommon header 'x-google-gfe-load-report' found, with contents: utilization_percent: 42.27554 queries_per_second: 13409 errors_per_second: 3
Test Links	https://demoblaze.com:443/ https://216.239.38.21:443/
OSVDB Entries	OSVDB-0

URI	/
HTTP Method	GET
Description	Uncommon header 'x-google-gfe-backend-request-cost' found, with contents: 42.275541258621288
Test Links	https://demoblaze.com:443/ https://216.239.38.21:443/
OSVDB Entries	OSVDB-0

Host Summary

Start Time	2022-10-20 01:33:53
End Time	2022-10-20 01:36:53
Elapsed Time	180 seconds
Statistics	346 requests, 20 errors, 9 findings

Scan Summary

Software Details	Nikto 2.1.6
CLI Options	-h https://demoblaze.com -o /tmp/report.html -Format htm
Hosts Tested	1
Start Time	Thu Oct 20 01:33:51 2022
End Time	Thu Oct 20 01:36:53 2022

Elapsed Time	182 seconds

References

1. https://hackertarget.com/nikto-website-scanner/
2. https://www.kali.org/tools/nikto/