WS Assignment (weekly report – Week 3)

Student ID: IT19147192

Name: K.A.P.P. Wickramarathne

Group: Y2S2.14.2 CS WD

IT19147192

Y2S2.14.2 WD CS

K.A.P.P.Wickramarathne

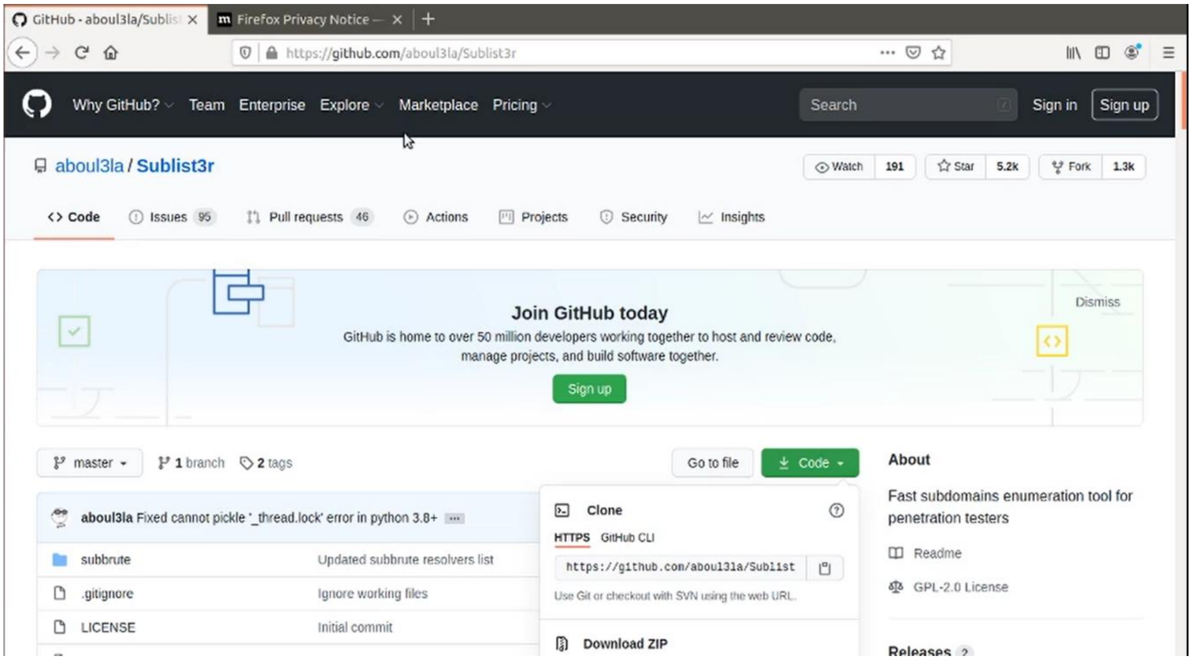
Week 1:

When we told to pick a domain scan and find vulnerabilities first I look for domains in Hacker One and Bug crowd but then I found out about Facebook white hat program. After picking a domain I search through the internet for a scanner

Then I found out some tools like SubBrute, Knock, DNSRecon and Sublist3r then I decided to use the Sublist3r because it is easy to install and easy to work with.

Installing Sublist3r:

1. First, I Had to get to the root access using “Sudo -i”
2. Then I install git using “apt install git”
3. After that I had to install python3 using “apt-get install python3.6”
4. Then “apt install python-pip”
5. Then went to git hub to clone sublist3r in my device



Join GitHub today

GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.

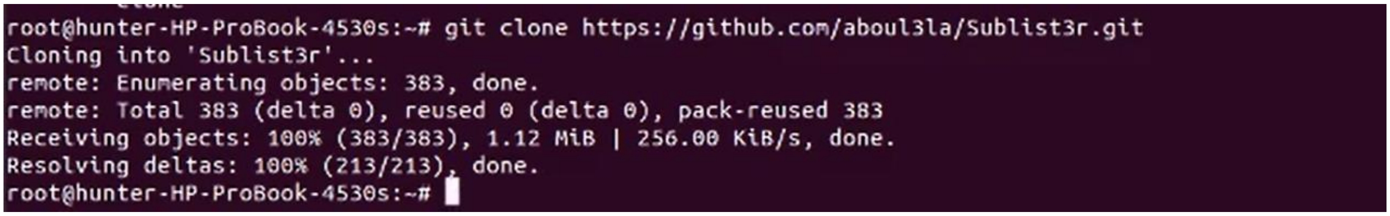
aboul3la Fixed cannot pickle '_thread.lock' error in python 3.8+

subbrute	Updated subbrute resolvers list
.gitignore	Ignore working files
LICENSE	Initial commit

```
https://github.com/aboul3la/Sublist
```

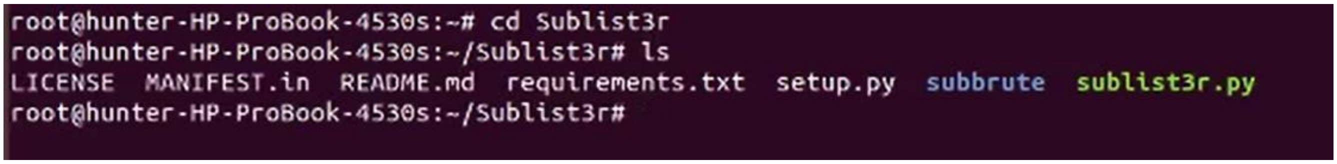
Use Git or checkout with SVN using the web URL.

Fast subdomains enumeration tool for penetration testers



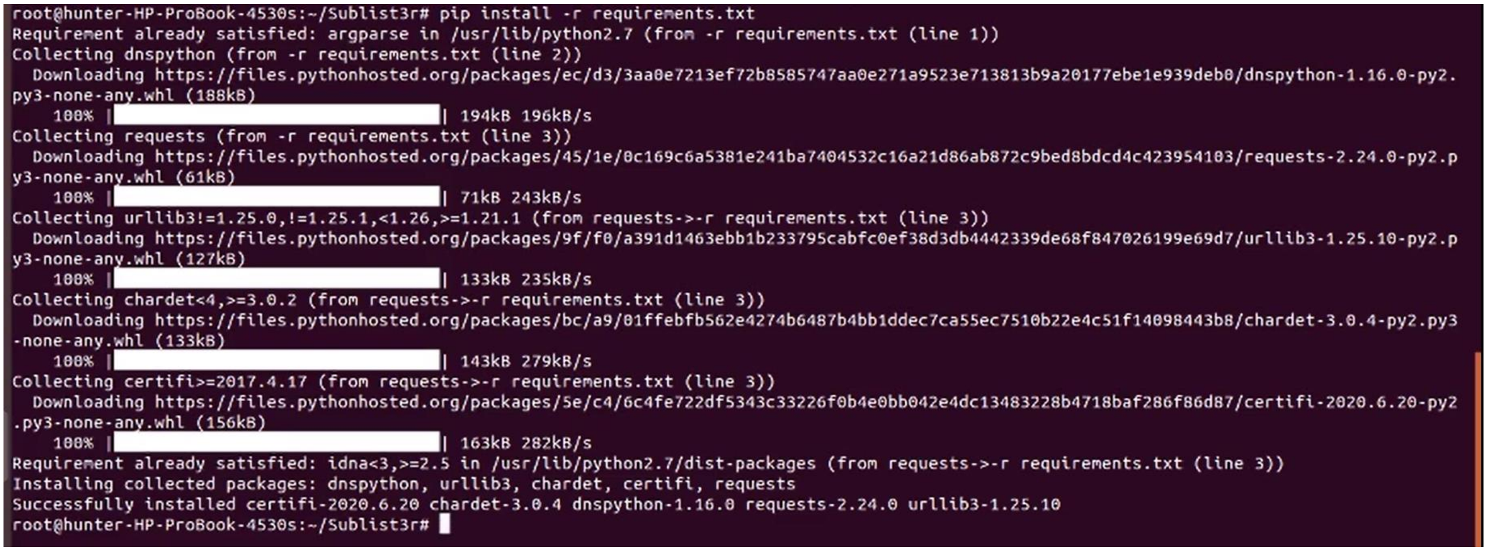
```
root@hunter-HP-ProBook-4530s:~# git clone https://github.com/aboul3la/Sublist3r.git
Cloning into 'Sublist3r'...
remote: Enumerating objects: 383, done.
remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383
Receiving objects: 100% (383/383), 1.12 MiB | 256.00 KiB/s, done.
Resolving deltas: 100% (213/213), done.
root@hunter-HP-ProBook-4530s:~#
```

6. Then get in the Sublist3r directory “cd Sublist3r” and check the files “ls”



```
root@hunter-HP-ProBook-4530s:~# cd Sublist3r
root@hunter-HP-ProBook-4530s:~/Sublist3r# ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py
root@hunter-HP-ProBook-4530s:~/Sublist3r#
```

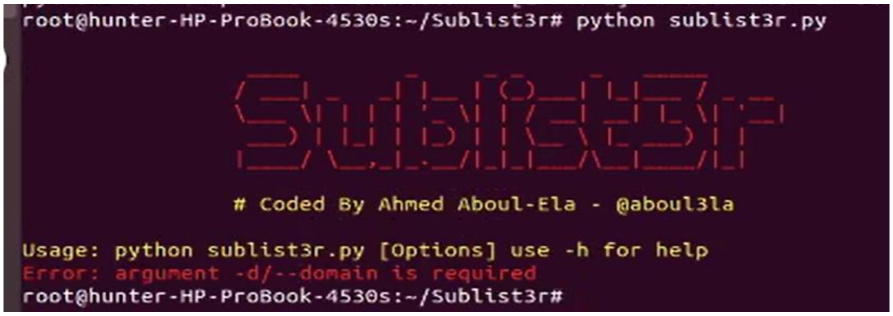
7. Then install requirements.txt file “pip install -r requirements.txt”



```
root@hunter-HP-ProBook-4530s:~/Sublist3r# pip install -r requirements.txt
Requirement already satisfied: argparse in /usr/lib/python2.7 (from -r requirements.txt (line 1))
Collecting dnspython (from -r requirements.txt (line 2))
  Downloading https://files.pythonhosted.org/packages/ec/d3/3aa0e7213ef72b8585747aa0e271a9523e713813b9a20177ebe1e939deb0/dnspython-1.16.0-py2.
py3-none-any.whl (188kB)
    100% |████████████████████████████████| 194kB 196kB/s
Collecting requests (from -r requirements.txt (line 3))
  Downloading https://files.pythonhosted.org/packages/45/1e/0c169c6a5381e241ba7404532c16a21d86ab872c9bed8bdcd4c423954103/requests-2.24.0-py2.p
y3-none-any.whl (61kB)
    100% |████████████████████████████████| 71kB 243kB/s
Collecting urllib3!=1.25.0,!=1.25.1,<1.26,>=1.21.1 (from requests->-r requirements.txt (line 3))
  Downloading https://files.pythonhosted.org/packages/9f/f0/a391d1463ebb1b233795cabfc0ef38d3db4442339de68f847026199e69d7/urllib3-1.25.10-py2.p
y3-none-any.whl (127kB)
    100% |████████████████████████████████| 133kB 235kB/s
Collecting chardet<4,>=3.0.2 (from requests->-r requirements.txt (line 3))
  Downloading https://files.pythonhosted.org/packages/bc/a9/01ffebfb562e4274b6487b4bb1ddec7ca55ec7510b22e4c51f14098443b8/chardet-3.0.4-py2.py3
-none-any.whl (133kB)
    100% |████████████████████████████████| 143kB 279kB/s
Collecting certifi>=2017.4.17 (from requests->-r requirements.txt (line 3))
  Downloading https://files.pythonhosted.org/packages/5e/c4/6c4fe722df5343c33226f0b4e0bb042e4dc13483228b4718baf286f86d87/certifi-2020.6.20-py2
.py3-none-any.whl (156kB)
    100% |████████████████████████████████| 163kB 282kB/s
Requirement already satisfied: idna<3,>=2.5 in /usr/lib/python2.7/dist-packages (from requests->-r requirements.txt (line 3))
Installing collected packages: dnspython, urllib3, chardet, certifi, requests
Successfully installed certifi-2020.6.20 chardet-3.0.4 dnspython-1.16.0 requests-2.24.0 urllib3-1.25.10
root@hunter-HP-ProBook-4530s:~/Sublist3r#
```

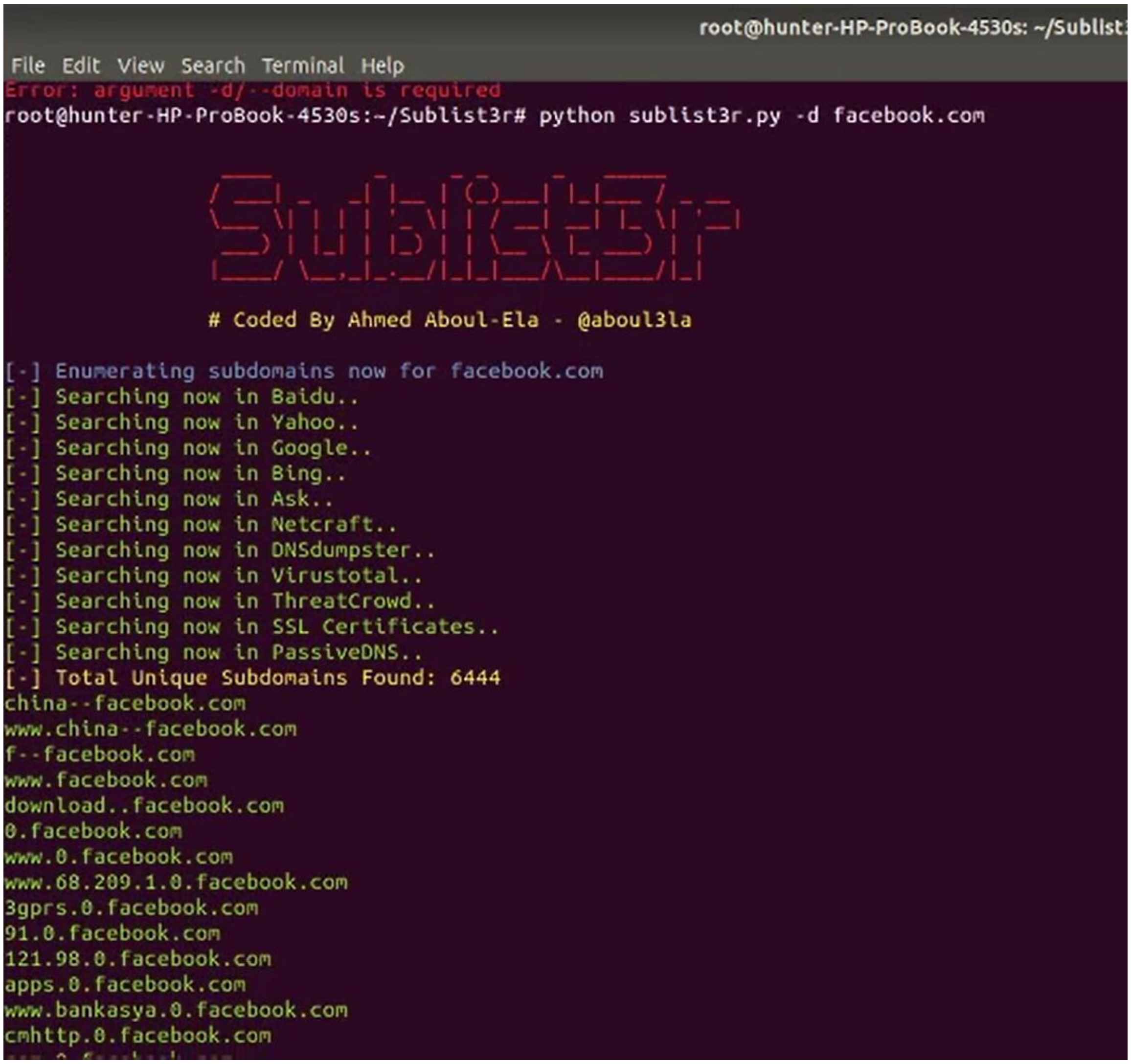
8. Then install setup.py “python setup.py install”

9. Then Run Sublist3r.py



```
root@hunter-HP-ProBook-4530s:~/Sublist3r# python sublist3r.py

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

Usage: python sublist3r.py [Options] use -h for help
Error: argument -d/--domain is required
root@hunter-HP-ProBook-4530s:~/Sublist3r#
```

10. Then I scan Facebook.com for subdomains “python sublist3r.py -d facebook.com”
11. Total of 6444 subdomains were found



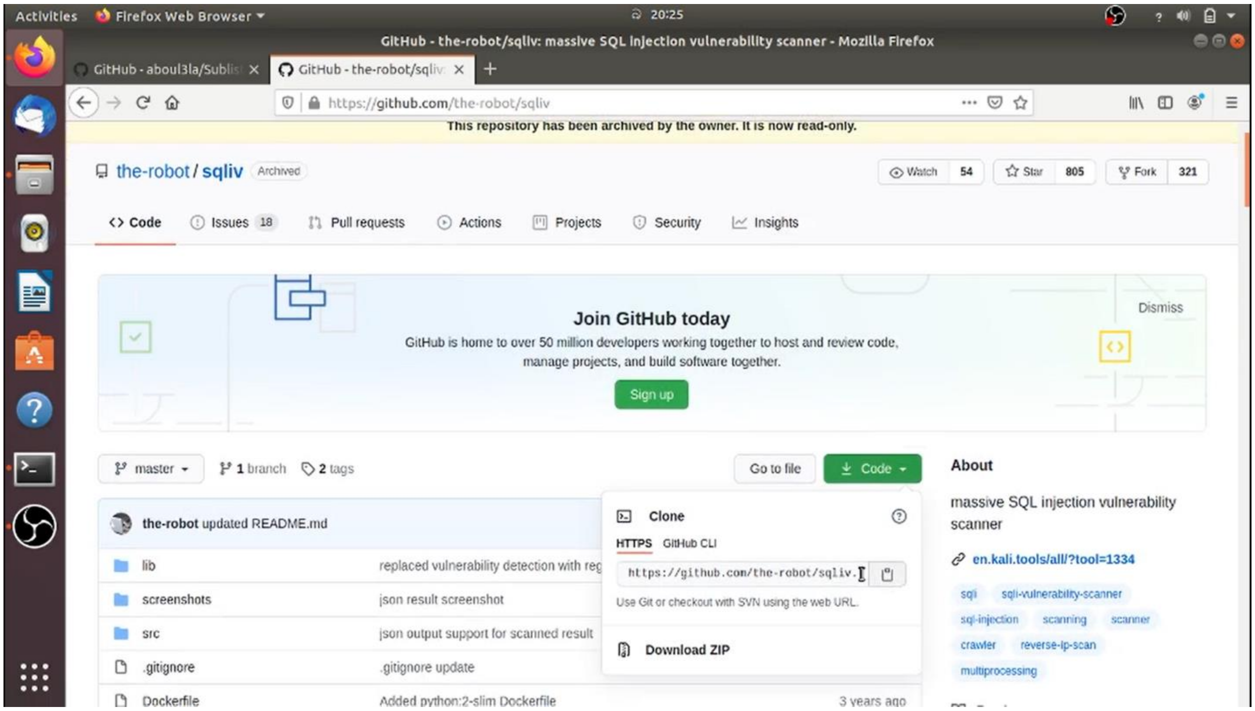
root@hunter-HP-ProBook-4530s: ~/Sublist
File Edit View Search Terminal Help

```
Error: argument -d/--domain is required
root@hunter-HP-ProBook-4530s:~/Sublist3r# python sublist3r.py -d facebook.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for facebook.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 6444
china--facebook.com
www.china--facebook.com
f--facebook.com
www.facebook.com
download..facebook.com
0.facebook.com
www.0.facebook.com
www.68.209.1.0.facebook.com
3gprs.0.facebook.com
91.0.facebook.com
121.98.0.facebook.com
apps.0.facebook.com
www.bankasya.0.facebook.com
cmhttp.0.facebook.com
```

Week 2:

In the second week I decided to search for scanners in internet and I found tool called sqliv and Nikto. Sqliv is a scanner to scan a web site a sql injection vulnerability and nikto scan for vulnerabilities like xss, week passwords, remote access and etc. but first I decided to scan facebook.com/login with Sqliv because to test if facebook login is vulnerable to sql injection attaks.

Cloning sqliv from git-hub



This repository has been archived by the owner. It is now read-only.

Join GitHub today

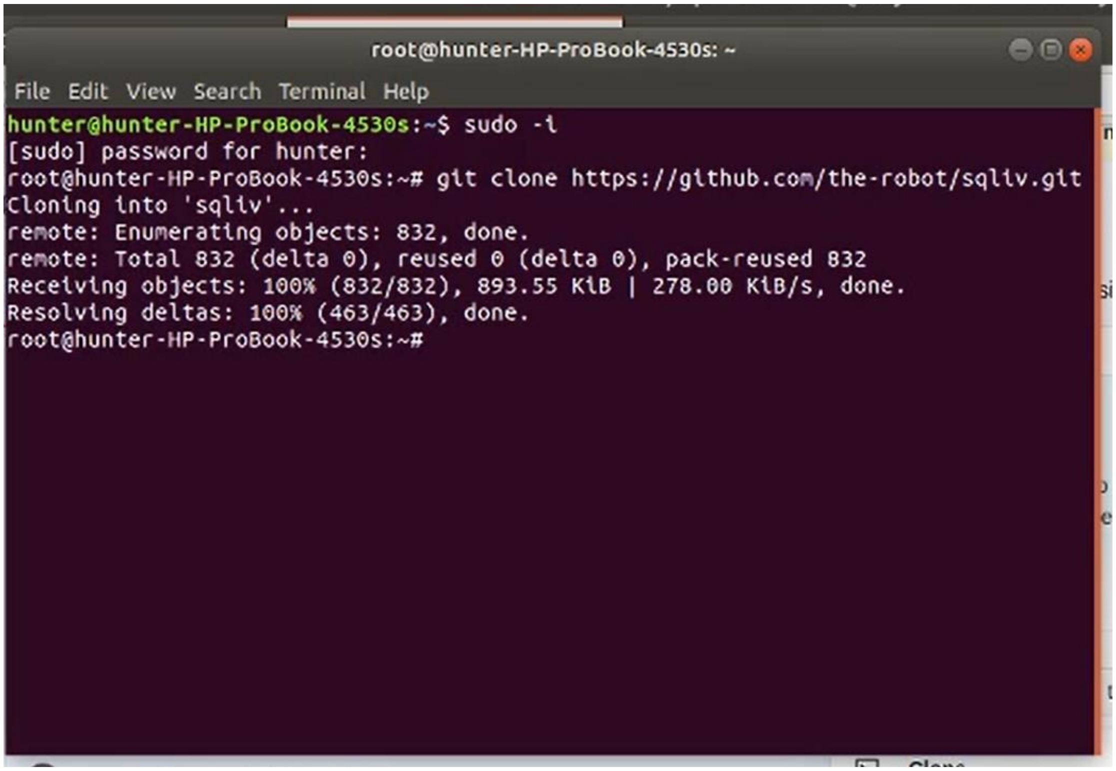
GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.

Use Git or checkout with SVN using the web URL.

massive SQL injection vulnerability scanner

the-robot updated README.md

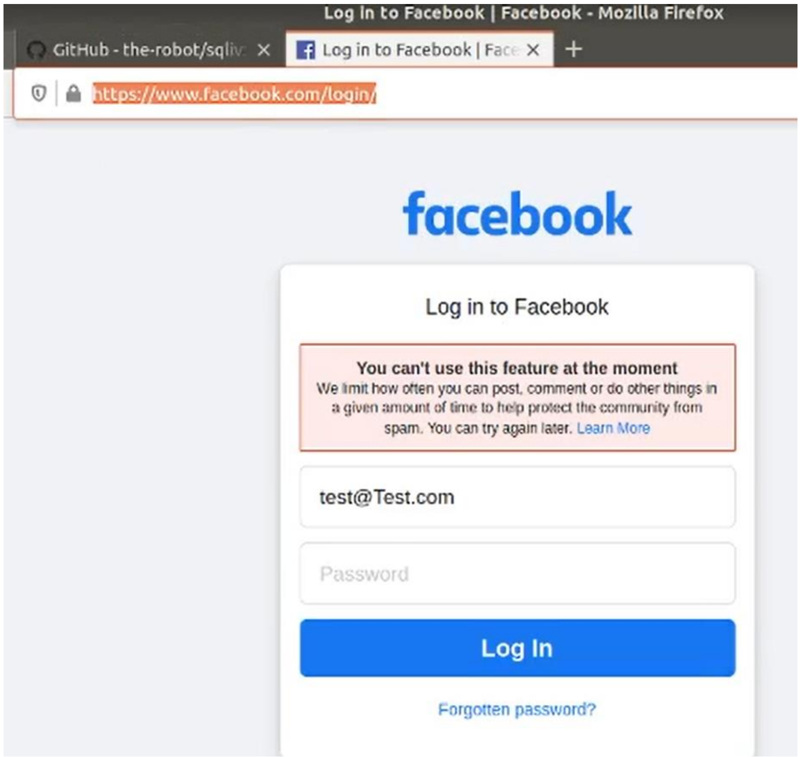
lib	replaced vulnerability detection with reg	
screenshots	json result screenshot	
src	json output support for scanned result	
.gitignore	.gitignore update	
Dockerfile	Added python:2-slim Dockerfile	3 years ago



root@hunter-HP-ProBook-4530s: ~
File Edit View Search Terminal Help

```
hunter@hunter-HP-ProBook-4530s:~$ sudo -i
[sudo] password for hunter:
root@hunter-HP-ProBook-4530s:~# git clone https://github.com/the-robot/sqliv.git
Cloning into 'sqliv'...
remote: Enumerating objects: 832, done.
remote: Total 832 (delta 0), reused 0 (delta 0), pack-reused 832
Receiving objects: 100% (832/832), 893.55 KiB | 278.00 KiB/s, done.
Resolving deltas: 100% (463/463), done.
root@hunter-HP-ProBook-4530s:~#
```

Target Location



Log in to Facebook | Facebook - Mozilla Firefox
GitHub - the-robot/sqliv
Log in to Facebook | Face
https://www.facebook.com/login/
facebook

Log in to Facebook

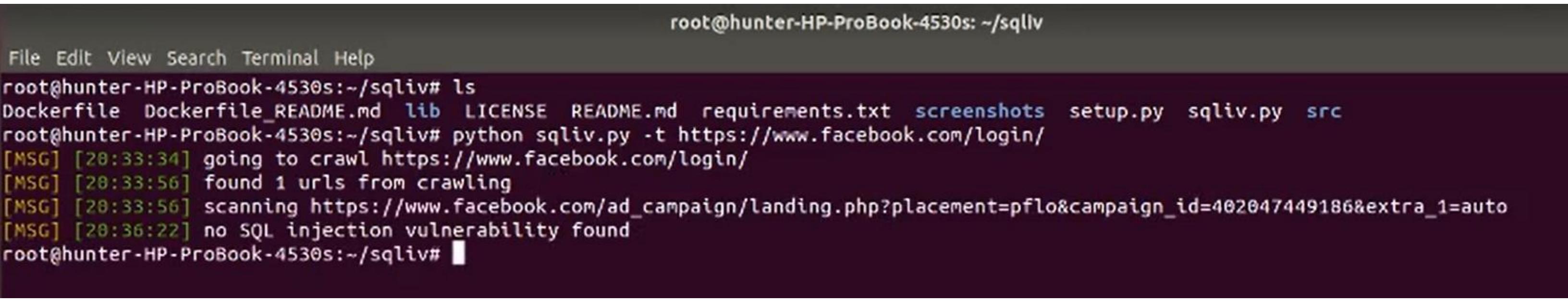
You can't use this feature at the moment
We limit how often you can post, comment or do other things in a given amount of time to help protect the community from spam. You can try again later. Learn More

test@Test.com

Password

Log In
Forgotten password?

Scanning With sqliv

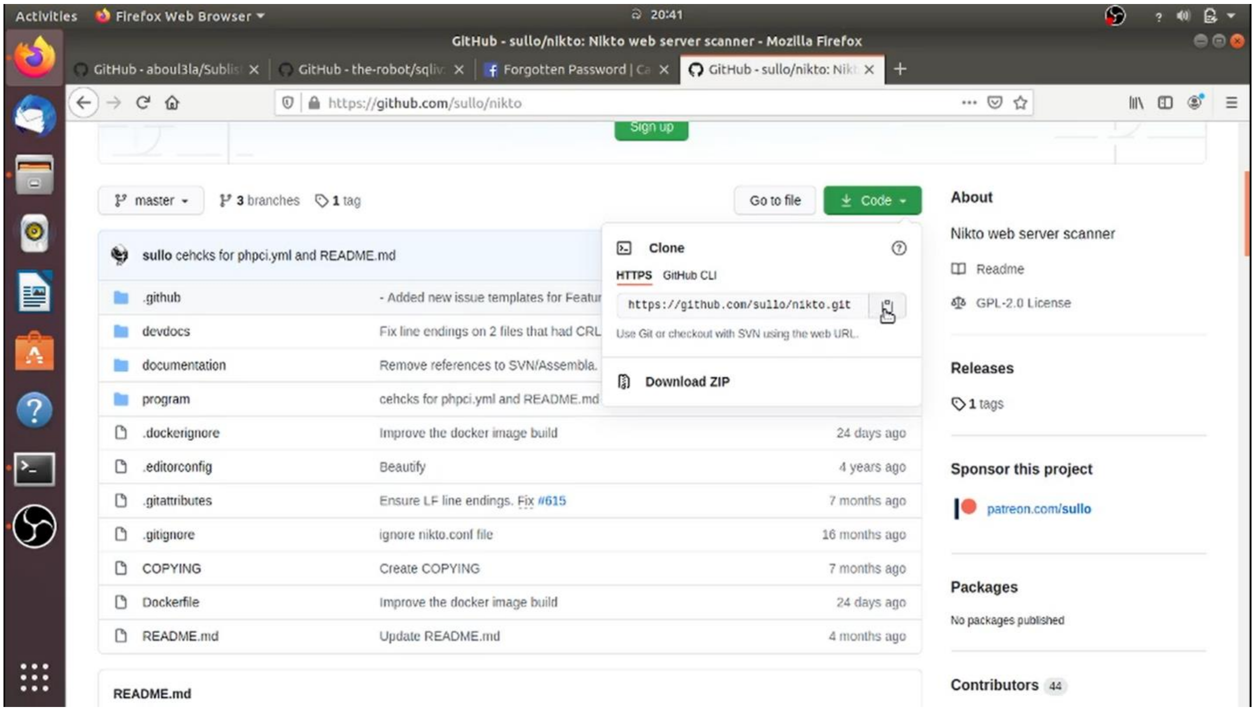


root@hunter-HP-ProBook-4530s: ~/sqliv

```
root@hunter-HP-ProBook-4530s:~/sqliv# ls
Dockerfile  Dockerfile_README.md  lib  LICENSE  README.md  requirements.txt  screenshots  setup.py  sqliv.py  src
root@hunter-HP-ProBook-4530s:~/sqliv# python sqliv.py -t https://www.facebook.com/login/
[MSG] [20:33:34] going to crawl https://www.facebook.com/login/
[MSG] [20:33:56] found 1 urls from crawling
[MSG] [20:33:56] scanning https://www.facebook.com/ad_campaign/landing.php?placement=pflo&campaign_id=402047449186&extra_1=auto
[MSG] [20:36:22] no SQL injection vulnerability found
root@hunter-HP-ProBook-4530s:~/sqliv# 
```

But using Sqliv I was unable to find any kind of sql injection vulnerability. Then I decided to install the nikto and scan facebook.com.

Cloning nikto



https://github.com/sullo/nikto

sullo cehcks for phpci.yml and README.md

```
.github          - Added new issue templates for Featur
devdocs          Fix line endings on 2 files that had CRL
documentation    Remove references to SVN/Assembla.
program          cehcks for phpci.yml and README.md
.dockerignore    Improve the docker image build      24 days ago
.editorconfig    Beautify                            4 years ago
.gitattributes   Ensure LF line endings. Fix #615    7 months ago
.gitignore       ignore nikto.conf file              16 months ago
COPYING          Create COPYING                      7 months ago
Dockerfile       Improve the docker image build      24 days ago
README.md        Update README.md                    4 months ago
```

README.md

Clone

HTTPS GitHub CLI

https://github.com/sullo/nikto.git

Use Git or checkout with SVN using the web URL.

Download ZIP

About

Nikto web server scanner

Readme

GPL-2.0 License

Releases

1 tags

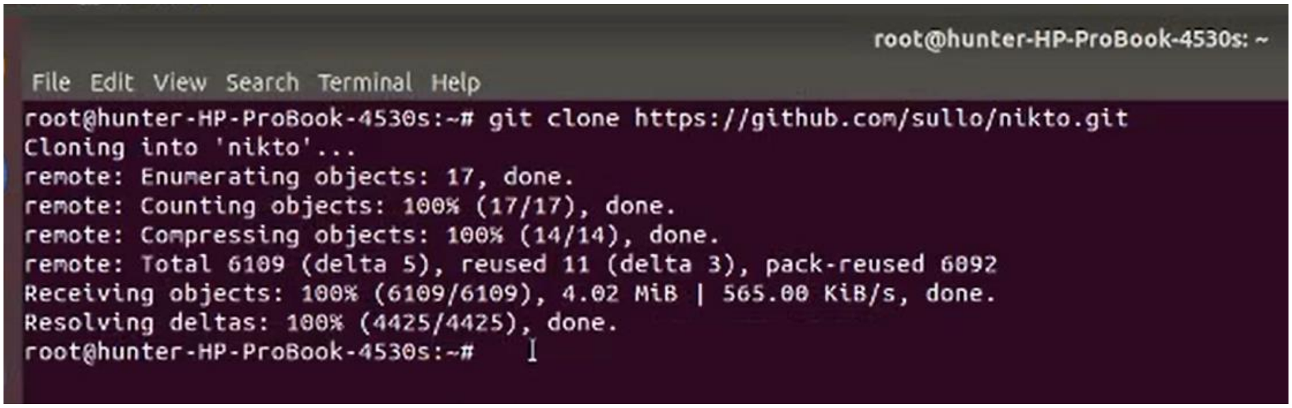
Sponsor this project

patreon.com/sullo

Packages

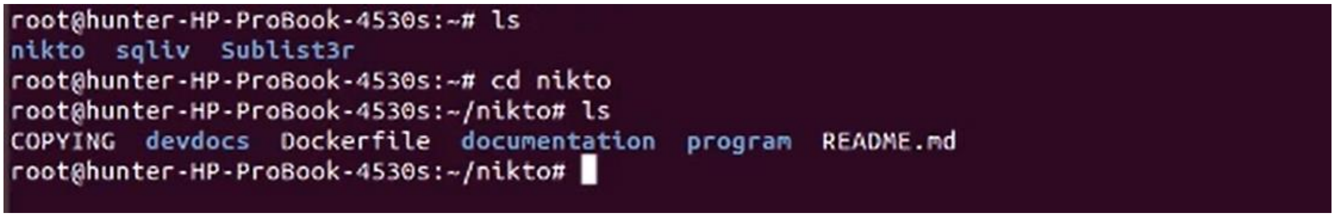
No packages published

Contributors 44



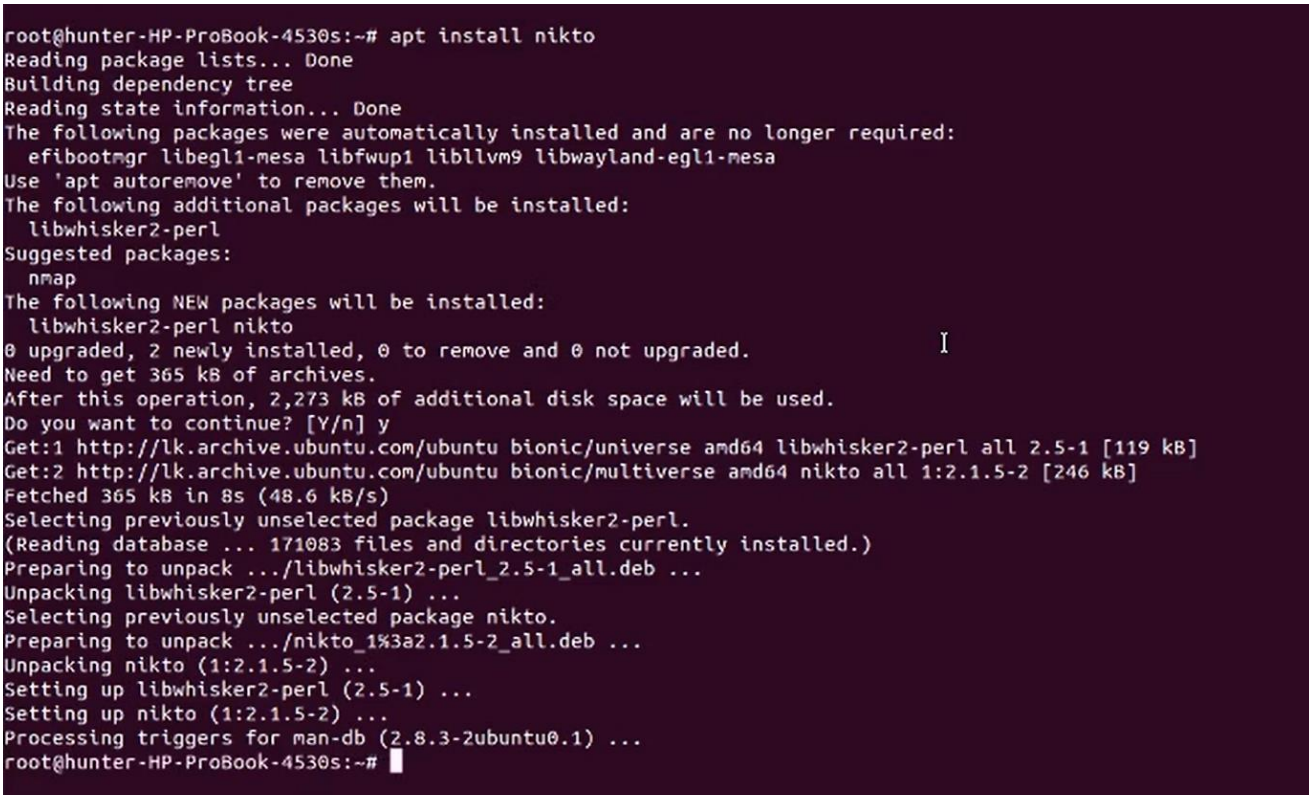
root@hunter-HP-ProBook-4530s: ~
File Edit View Search Terminal Help

```
root@hunter-HP-ProBook-4530s:~# git clone https://github.com/sullo/nikto.git
Cloning into 'nikto'...
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 6109 (delta 5), reused 11 (delta 3), pack-reused 6092
Receiving objects: 100% (6109/6109), 4.02 MiB | 565.00 KiB/s, done.
Resolving deltas: 100% (4425/4425), done.
root@hunter-HP-ProBook-4530s:~#
```



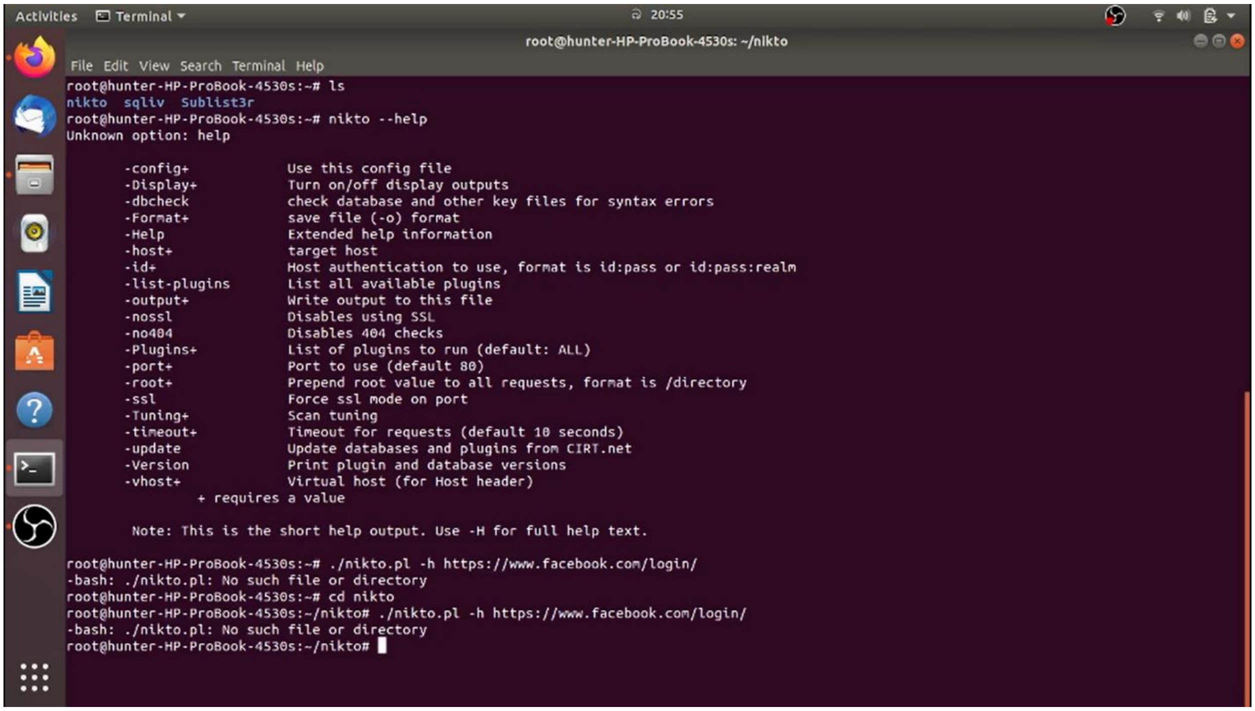
```
root@hunter-HP-ProBook-4530s:~# ls
nikto  sqliv  Sublist3r
root@hunter-HP-ProBook-4530s:~# cd nikto
root@hunter-HP-ProBook-4530s:~/nikto# ls
COPYING  devdocs  Dockerfile  documentation  program  README.md
root@hunter-HP-ProBook-4530s:~/nikto#
```

Installing using Apt command



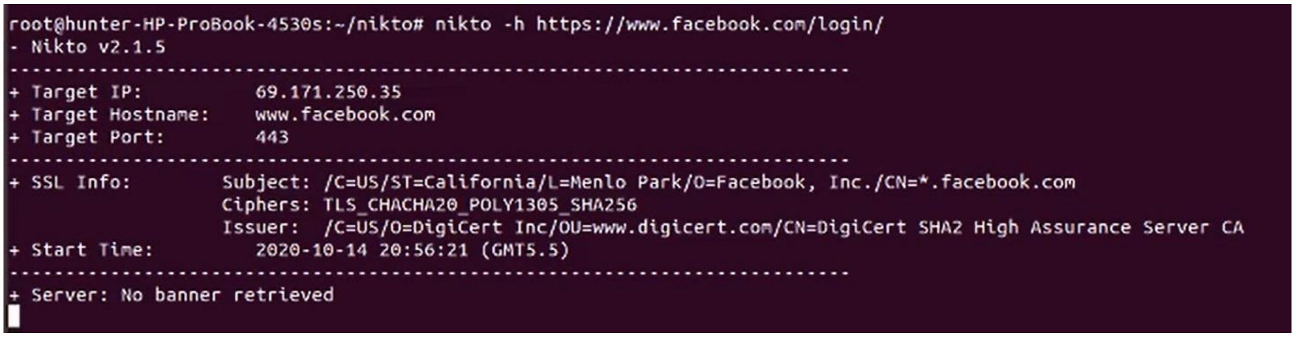
```
root@hunter-HP-ProBook-4530s:~# apt install nikto
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  efibootmgr libegl1-mesa libfwup1 libllvm9 libwayland-egl1-mesa
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libwhisker2-perl
Suggested packages:
  nmap
The following NEW packages will be installed:
  libwhisker2-perl nikto
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 365 kB of archives.
After this operation, 2,273 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu bionic/universe amd64 libwhisker2-perl all 2.5-1 [119 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu bionic/multiverse amd64 nikto all 1:2.1.5-2 [246 kB]
Fetched 365 kB in 8s (48.6 kB/s)
Selecting previously unselected package libwhisker2-perl.
(Reading database ... 171083 files and directories currently installed.)
Preparing to unpack .../libwhisker2-perl_2.5-1_all.deb ...
Unpacking libwhisker2-perl (2.5-1) ...
Selecting previously unselected package nikto.
Preparing to unpack .../nikto_1%3a2.1.5-2_all.deb ...
Unpacking nikto (1:2.1.5-2) ...
Setting up libwhisker2-perl (2.5-1) ...
Setting up nikto (1:2.1.5-2) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
root@hunter-HP-ProBook-4530s:~#
```

After that I had to use help command in nikto to have an idea how to use it and also I watched some YouTube videos and search on internet. (all the sources will be in last page)


Activities
Terminal
20:55
root@hunter-HP-ProBook-4530s: ~/nikto
File Edit View Search Terminal Help

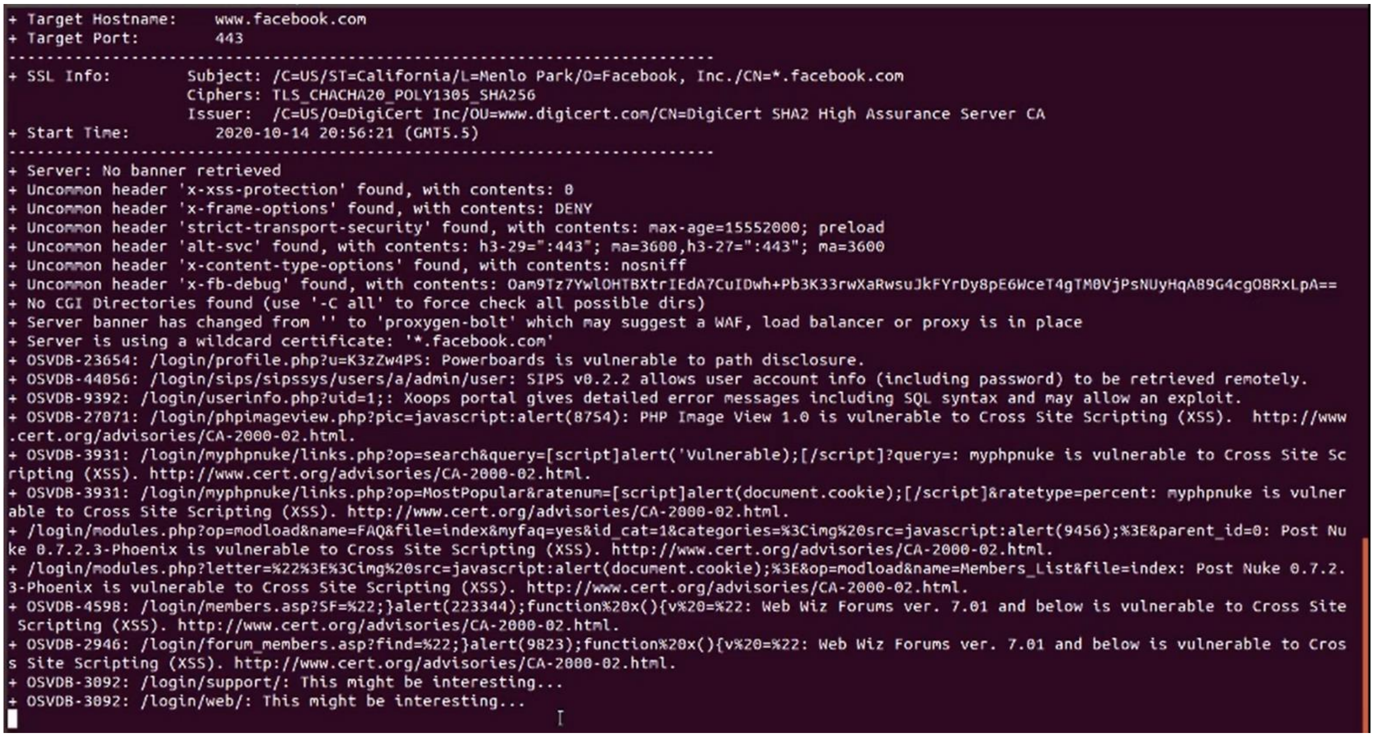
```
root@hunter-HP-ProBook-4530s:~# ls
nikto  sqliv  Sublist3r
root@hunter-HP-ProBook-4530s:~# nikto --help
Unknown option: help

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.

root@hunter-HP-ProBook-4530s:~# ./nikto.pl -h https://www.facebook.com/login/
-bash: ./nikto.pl: No such file or directory
root@hunter-HP-ProBook-4530s:~# cd nikto
root@hunter-HP-ProBook-4530s:~/nikto# ./nikto.pl -h https://www.facebook.com/login/
-bash: ./nikto.pl: No such file or directory
root@hunter-HP-ProBook-4530s:~/nikto#
```

Scanning Facebook.com using nikto



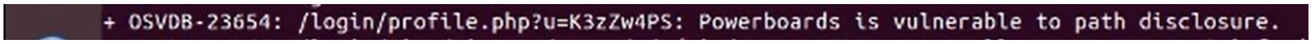
```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h https://www.facebook.com/login/
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.35
+ Target Hostname:    www.facebook.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=Menlo Park/O=Facebook, Inc./CN=*.facebook.com
                   Ciphers:  TLS_CHACHA20_POLY1305_SHA256
                   Issuer:   /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA
+ Start Time:         2020-10-14 20:56:21 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
```

Result Found after scanning



```
+ Target Hostname:    www.facebook.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject: /C=US/ST=California/L=Menlo Park/O=Facebook, Inc./CN=*.facebook.com
                   Ciphers: TLS_CHACHA20_POLY1305_SHA256
                   Issuer:  /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA
+ Start Time:         2020-10-14 20:56:21 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'strict-transport-security' found, with contents: max-age=15552000; preload
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-fb-debug' found, with contents: Oam9Tz7YwlOHTBXtrIEdA7CuIDwh+Pb3K33rwXaRwsuJkFYrDy8pE6WceT4gTM0VjPsNUyHqA89G4cgO8RxLpA==
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ Server is using a wildcard certificate: '*.facebook.com'
+ OSVDB-23654: /login/profile.php?u=K3zZw4PS: Powerboards is vulnerable to path disclosure.
+ OSVDB-44056: /login/sips/sipssys/users/a/admin/user: SIPS v0.2.2 allows user account info (including password) to be retrieved remotely.
+ OSVDB-9392: /login/userinfo.php?uid=1;: Xoops portal gives detailed error messages including SQL syntax and may allow an exploit.
+ OSVDB-27071: /login/phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS).  http://www
.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3931: /login/myphpnuke/links.php?op=search&query=[script]alert('Vulnerable);[/script]?query=: myphpnuke is vulnerable to Cross Site Sc
ripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3931: /login/myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent: myphpnuke is vulner
able to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /login/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nu
ke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /login/modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.
3-Phoenix is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-4598: /login/members.asp?SF=%22;}alert(223344);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site
 Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-2946: /login/forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cros
s Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3092: /login/support/: This might be interesting...
+ OSVDB-3092: /login/web/: This might be interesting...
```

When the Scanning started it shows the protection and some results and after 2 – 3 hours I was able to get this results but it's still scanning, because of that I decided to wait another 3 hours but nothing happed. I assumed its stuck due to lack of resources in my computer then I decided to abort the scanning process. But I was able to find something interesting in that I was able to find some vulnerabilities

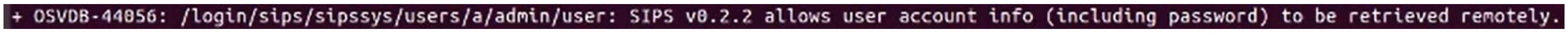


```
+ OSVDB-23654: /login/profile.php?u=K3zZw4PS: Powerboards is vulnerable to path disclosure.
```

Then I decided to search what is "**powerboards is vulnerable to path disclosure**"**.** When I search through the internet I was able to found CVE-2002-1723 vulnerability and it was also about the powerboards is vulnerable to path disclosure. According to the cvedetails.com this vulnerability "Powerboards 2.2b allows remote attackers to view the full path to the backend database by sending a cookie containing a non-existent username to profiles.php, which displays the full path in the error message."

And also, according to the cvedetails.com due to this vulnerability impact on confidentiality in partial and there is no impact on integrity and availability also no one was able to gain access due to this vulnerability.

Then I was able to find something in the scan results

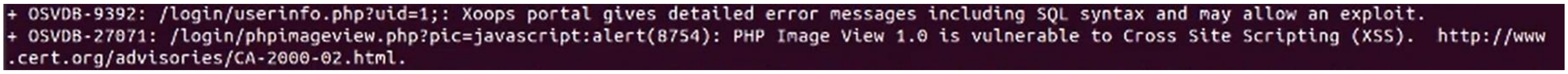


```
+ OSVDB-44056: /login/sips/sipssys/users/a/admin/user: SIPS v0.2.2 allows user account info (including password) to be retrieved remotely.
```

When I was searching through the internet about SIPS v0.2.2 I was able to find some information about that from exploit-db.com and cvedetails.com. this vulnerability is about user information disclosure. According to the exploit-db.com this vulnerability: " **It has been reported that authentication is not required to view user account information. As a result, an unauthorized remote attacker may be able to view potentially sensitive information. This may aid in launching further attacks against a target user or system**."

And according to the cvedetails.com due to this vulnerability (CVE-2003-1553) impact on confidentiality in partial and there is no impact on integrity and availability also no one was able to gain access due to this vulnerability. But there is medium impact on access.

And also I found some more vulnerabilities from this scan



```
+ OSVDB-9392: /login/userinfo.php?uid=1;: Xoops portal gives detailed error messages including SQL syntax and may allow an exploit.
+ OSVDB-27071: /login/phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS).  http://www
.cert.org/advisories/CA-2000-02.html.
```

I'm planning to do another scan using nikto and also with some new tools and also planning to do some search on these remaining vulnerabilities and add more details to next report.

Links to resources :

Sqliv: https://github.com/the-robot/sqliv

Nikto: https://github.com/sullo/nikto

Nikto: https://cirt.net/Nikto2

Using nikto tutorial: https://www.youtube.com/watch?v=GH9qn_DBzCk

: https://www.youtube.com/watch?v=K78YOmbuT48&t=23s

CVE-2002-1723: https://www.cvedetails.com/cve/CVE-2002-1723/

CVE-2003-1553: https://www.cvedetails.com/cve/CVE-2003-1553/

Expolid-db.com: https://www.exploit-db.com/exploits/22381

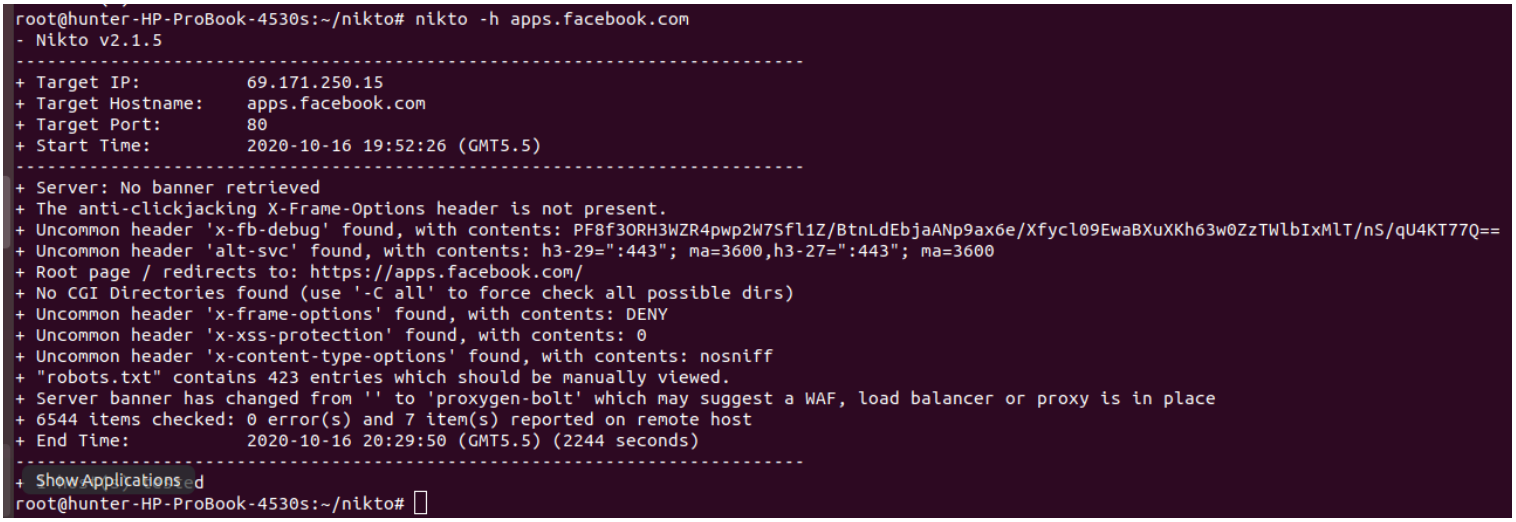
Facebook login that I scanned: https: //www.facebook.com/login/

Week 3:

In this week I decided to do some more search on the vulnerabilities that I found on last week scan and then I'm planning to do more scan on other subdomains in facebook.com using nikto and some more tools. Last week I was able to find a vulnerability message "xoops portal gives detailed error messages including SQL syntax and may allow an exploit" then I search about this vulnerability through the internet and I was able to find 45 CVE recorded vulnerabilities on xoops but I was unable find a vulnerability that happen due to sql syntax. Most of them were cross site scripting and sql injection.

Then I scanned for subdomains in facebook.com again then I scan these subdomains for vulnerability with nikto scanner.

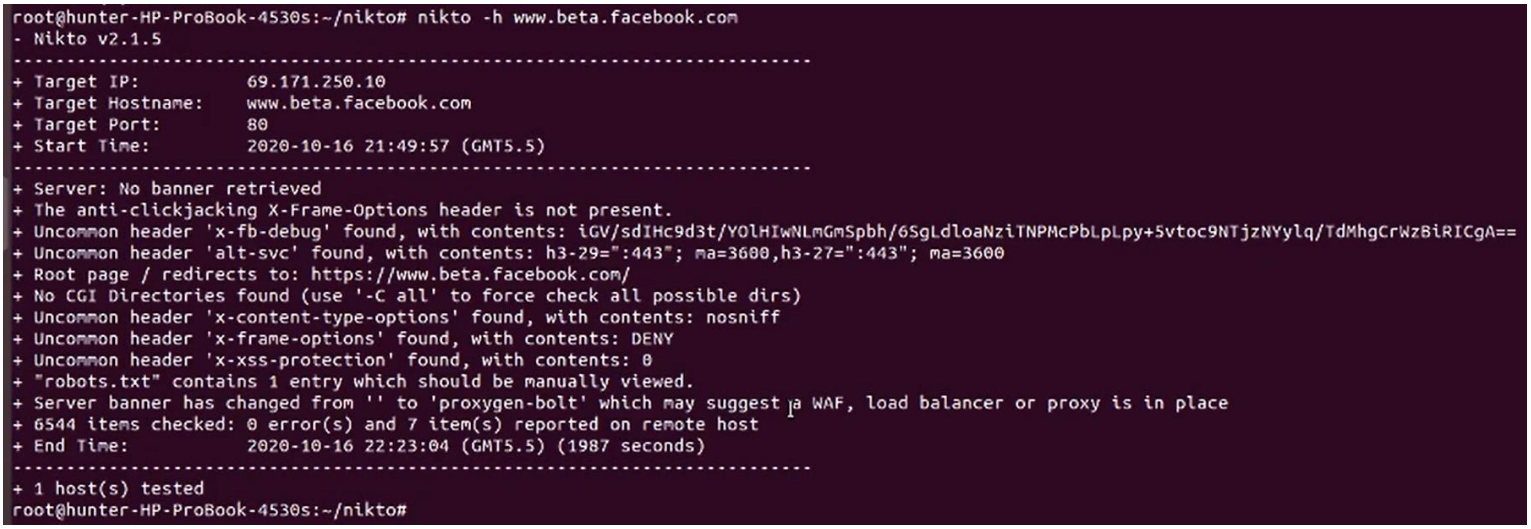
First, I scanned "apps.facebook.com"



```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h apps.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.15
+ Target Hostname:    apps.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-16 19:52:26 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-fb-debug' found, with contents: PF8f3ORH3WZR4pwp2W7Sfl1Z/BtnLdEbjaANp9ax6e/Xfycl09EwaBXuXKh63w0ZzTWlbIxMlT/nS/qU4KT77Q==
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Root page / redirects to: https://apps.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ "robots.txt" contains 423 entries which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-10-16 20:29:50 (GMT5.5) (2244 seconds)
---------------------------------------------------------------------------
+ Show Applications d
root@hunter-HP-ProBook-4530s:~/nikto# 
```

This scan took around 30 minutes 6544 items were scanned but 0 errors were found and only 7 items were reported for remote host. After that I decided to scan another sub-domain.

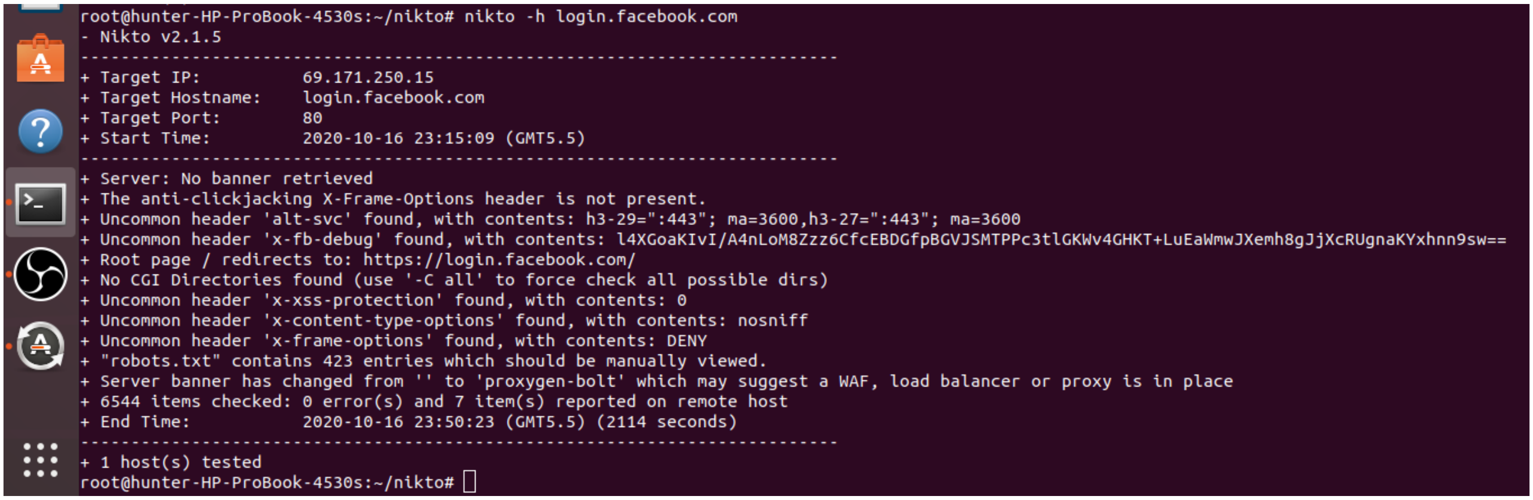
Second scan “www.beta.facebook.com”



```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h www.beta.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.10
+ Target Hostname:    www.beta.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-16 21:49:57 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-fb-debug' found, with contents: iGV/sdIHc9d3t/YOlHIwNLmGmSpbh/6SgLdloaNziTNPMcPbLpLpy+5vtoc9NTjzNYylq/TdMhgCrWzBiRICgA==
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Root page / redirects to: https://www.beta.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-10-16 22:23:04 (GMT5.5) (1987 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto#
```

This scan also took around 30 minutes also 6544 items were scanned but I was unable to find any error in this subdomain. The scan results was same as the apps.facebook.com subdomain results. Then I continue to scan other subdomains.

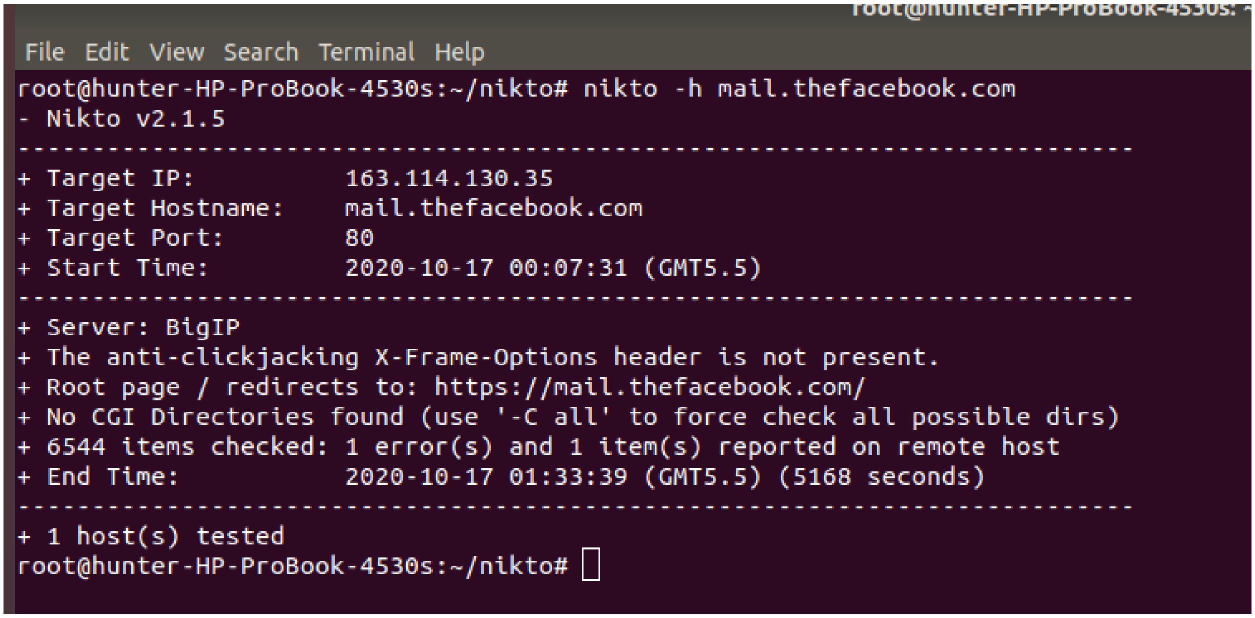
Third scan “login.facebook.com”



```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h login.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.15
+ Target Hostname:    login.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-16 23:15:09 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Uncommon header 'x-fb-debug' found, with contents: l4XGoaKIvI/A4nLoM8Zzz6CfcEBDGfpBGVJSMTPPc3tlGKWv4GHKT+LuEaWmwJXemh8gJjXcRUgnaKYxhnn9sw==
+ Root page / redirects to: https://login.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ "robots.txt" contains 423 entries which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-10-16 23:50:23 (GMT5.5) (2114 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto#
```

In this scan results were same as above, but the scan time took around 35 to 40 minutes. Then decided to scan another subdomain.

Fourth scan “mail.thefacebook.com”

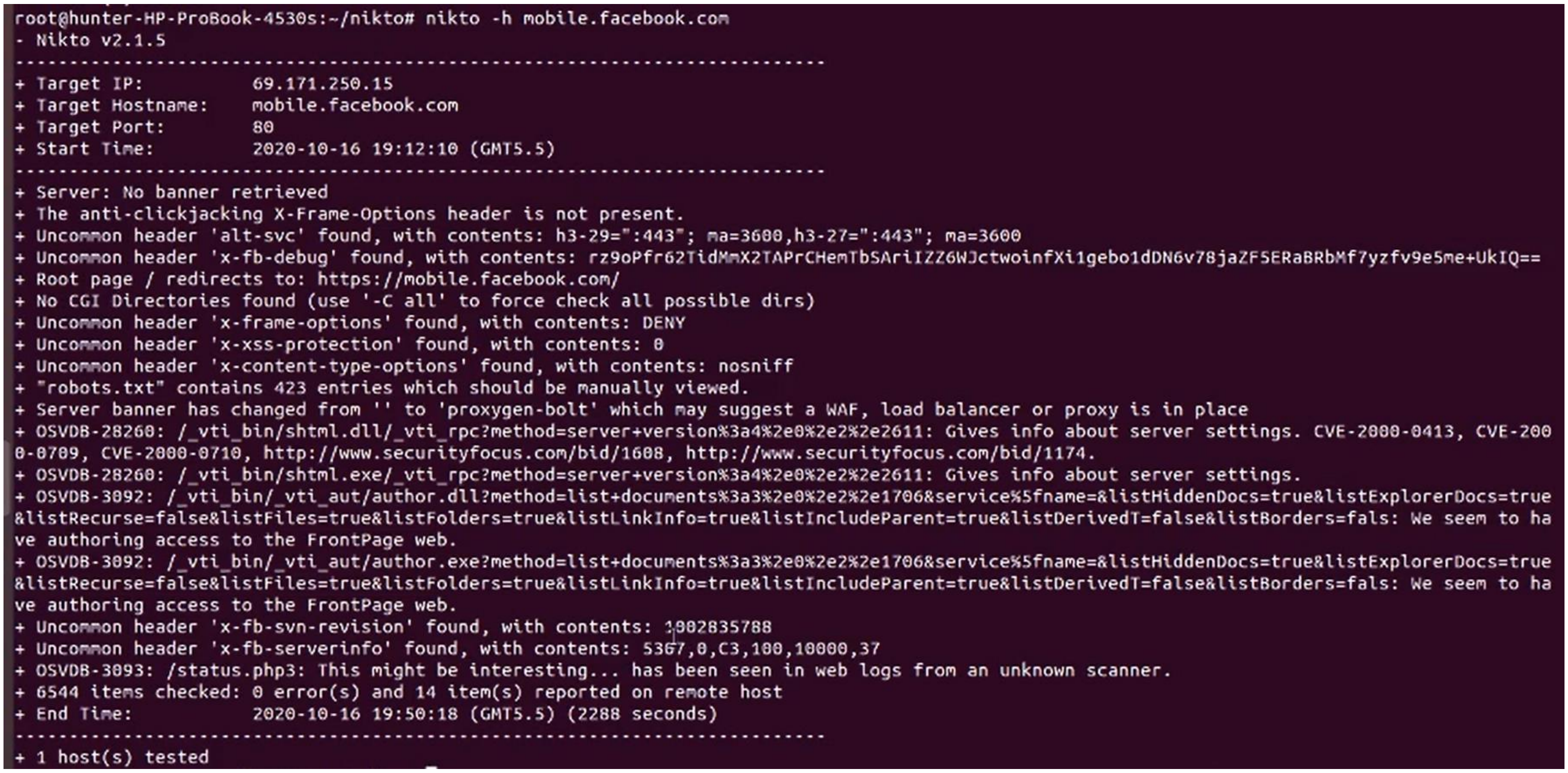

root@hunter-HP-ProBook-4530s:
File Edit View Search Terminal Help

```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h mail.thefacebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          163.114.130.35
+ Target Hostname:    mail.thefacebook.com
+ Target Port:        80
+ Start Time:         2020-10-17 00:07:31 (GMT5.5)
---------------------------------------------------------------------------
+ Server: BigIP
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://mail.thefacebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 6544 items checked: 1 error(s) and 1 item(s) reported on remote host
+ End Time:           2020-10-17 01:33:39 (GMT5.5) (5168 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto# 
```

This scan took around 1 hour and 40 minutes but in scan results it shows 1 error found and only 1 item is reported on remote host. Also 6544 items were scanned.

But I was unable to find the error in mail.thefacebook.com subdomain.

Fifth scan “mobile.facebook.com”



```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h mobile.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.15
+ Target Hostname:    mobile.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-16 19:12:10 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Uncommon header 'x-fb-debug' found, with contents: rz9oPfr62TidMmX2TAPrCHemTbSAriIZZ6WJctwoinfXi1gebo1dDN6v78jaZF5ERaBRbMf7yzfv9e5me+UkIQ==
+ Root page / redirects to: https://mobile.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ "robots.txt" contains 423 entries which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ OSVDB-28260: /_vti_bin/shtml.dll/_vti_rpc?method=server+version%3a4%2e0%2e2%2e2611: Gives info about server settings. CVE-2000-0413, CVE-200
0-0709, CVE-2000-0710, http://www.securityfocus.com/bid/1608, http://www.securityfocus.com/bid/1174.
+ OSVDB-28260: /_vti_bin/shtml.exe/_vti_rpc?method=server+version%3a4%2e0%2e2%2e2611: Gives info about server settings.
+ OSVDB-3092: /_vti_bin/_vti_aut/author.dll?method=list+documents%3a3%2e0%2e2%2e1706&service%5fname=&listHiddenDocs=true&listExplorerDocs=true
&listRecurse=false&listFiles=true&listFolders=true&listLinkInfo=true&listIncludeParent=true&listDerivedT=false&listBorders=fals: We seem to ha
ve authoring access to the FrontPage web.
+ OSVDB-3092: /_vti_bin/_vti_aut/author.exe?method=list+documents%3a3%2e0%2e2%2e1706&service%5fname=&listHiddenDocs=true&listExplorerDocs=true
&listRecurse=false&listFiles=true&listFolders=true&listLinkInfo=true&listIncludeParent=true&listDerivedT=false&listBorders=fals: We seem to ha
ve authoring access to the FrontPage web.
+ Uncommon header 'x-fb-svn-revision' found, with contents: 1002835788
+ Uncommon header 'x-fb-serverinfo' found, with contents: 5367,0,C3,100,10000,37
+ OSVDB-3093: /status.php3: This might be interesting... has been seen in web logs from an unknown scanner.
+ 6544 items checked: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2020-10-16 19:50:18 (GMT5.5) (2288 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

This scan also took around 35 minutes 6544 items were scanned, 0 errors found and 14 items reported on remote host. But I was able to find 3 CVE vulnerability codes in this scan. CVE-2000-0413, CVE-2000-0709, CVE-2000-0710 I search about these vulnerabilities and I was able to find some interesting details.

CVE-2000-0413 : according to the NVD and CVEdetails.com web sites “in this vulnerability, The shtml.exe program in the FrontPage extensions package of IIS 4.0 and 5.0 allows remote attackers to determine the physical path of HTML, HTM, ASP, and SHTML files by requesting a file that does not exist, which generates an error message that reveals the path.”

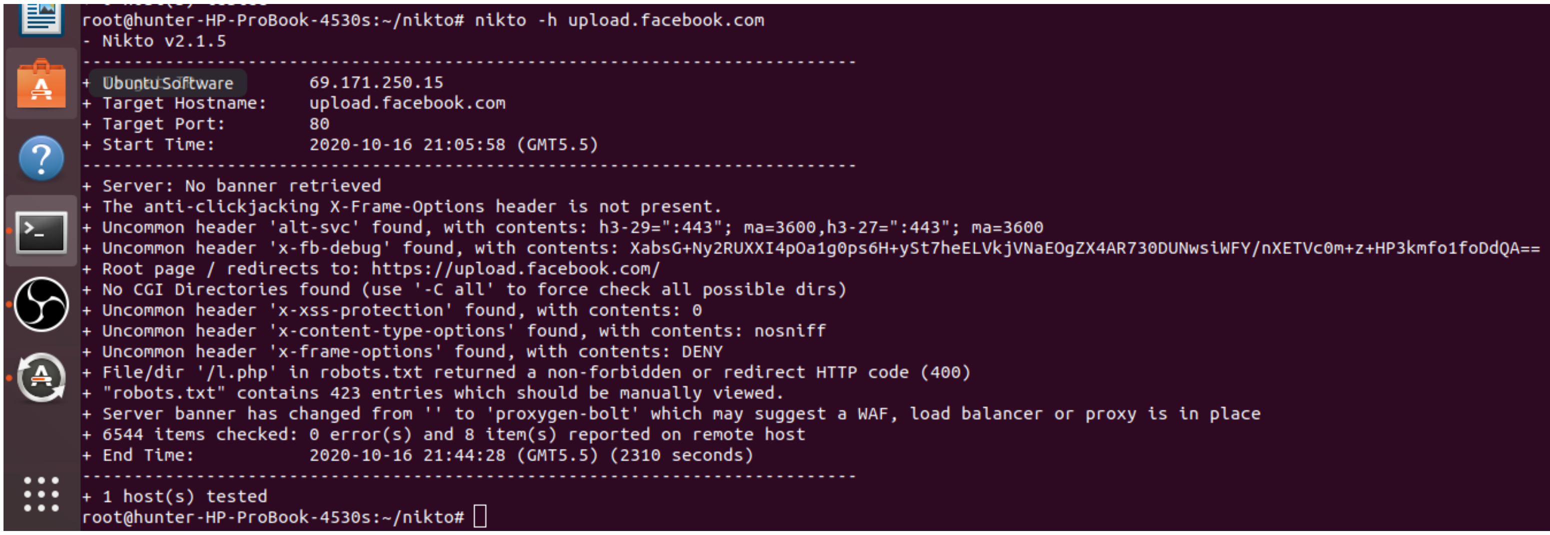
According to the CVEdetails.com site impact on Confidentiality is partial and no impact on Integrity and Availability due to this vulnerability.

CVE-2000-0709 : according to the NVD and CVEdetails.com web sites “The shtml.exe component of Microsoft FrontPage 2000 Server Extensions 1.1 allows remote attackers to cause a denial of service in some components by requesting a URL whose name includes a standard DOS device name.”

According to the CVEdetails.com site impact on Integrity is partial and no impact on Confidentiality and Availability due to this vulnerability.

CVE-2000-0710 : according to the NVD and CVEdetails.com web sites “The shtml.exe component of Microsoft FrontPage 2000 Server Extensions 1.1 allows remote attackers to determine the physical path of the server components by requesting an invalid URL whose name includes a standard DOS device name.”

According to the CVEdetails.com site impact on Confidentiality is partial and no impact on Integrity and Availability due to this vulnerability.

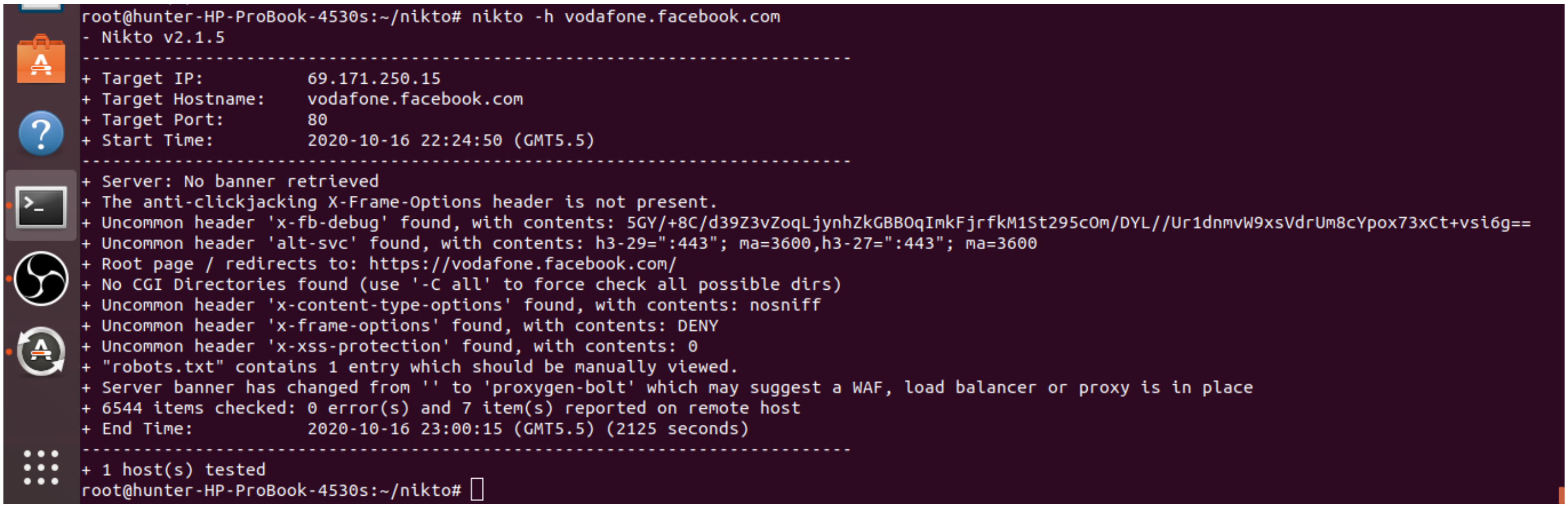


```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h upload.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Ubuntu Software        69.171.250.15
+ Target Hostname:    upload.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-16 21:05:58 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Uncommon header 'x-fb-debug' found, with contents: XabsG+Ny2RUXXI4pOa1g0ps6H+ySt7heELVkjVNaEOgZX4AR730DUNwsiWFY/nXETVc0m+z+HP3kmfo1foDdQA==
+ Root page / redirects to: https://upload.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ File/dir '/l.php' in robots.txt returned a non-forbidden or redirect HTTP code (400)
+ "robots.txt" contains 423 entries which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2020-10-16 21:44:28 (GMT5.5) (2310 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto# 
```

Sixth scan “Upload.facebook.com”

This scan took around 40 minutes, 0 errors were found, and 8 items were reported on remote host. As I couldn’t find any error or vulnerability on this subdomain, I decided to scan another sub domain.

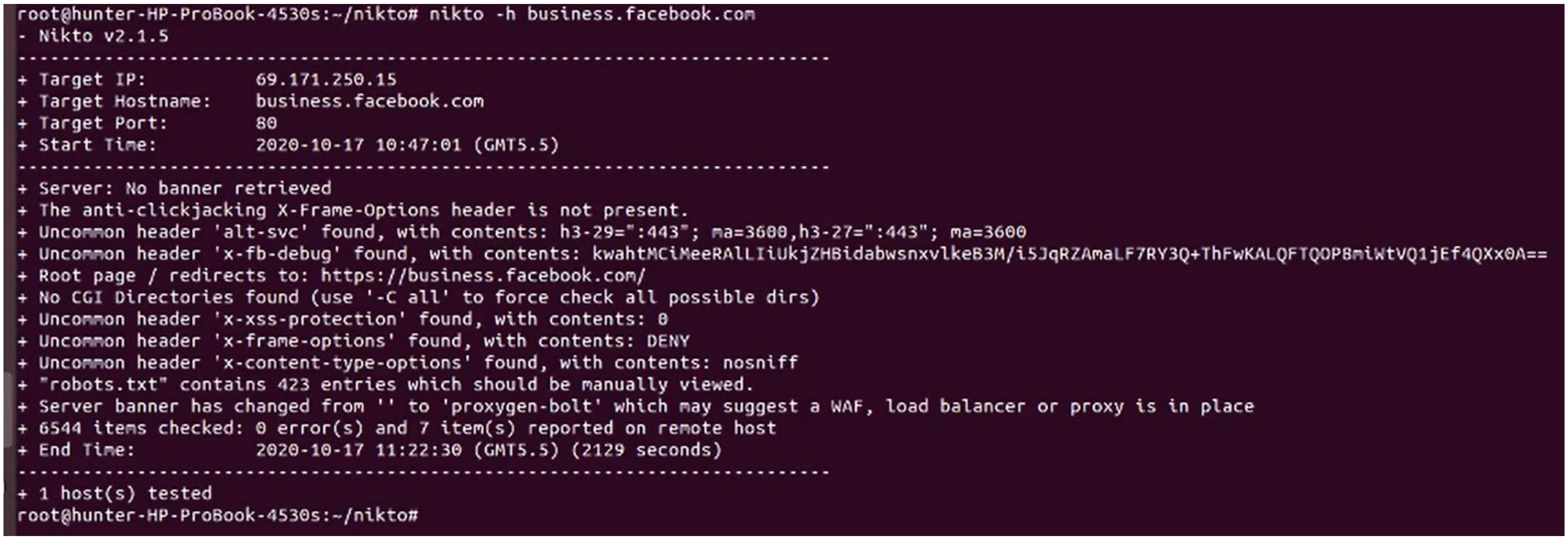
Seventh scan “vodafone.facebook.com”



```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h vodafone.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.15
+ Target Hostname:    vodafone.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-16 22:24:50 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-fb-debug' found, with contents: 5GY/+8C/d39Z3vZoqLjynhZkGBBOqImkFjrfkM1St295cOm/DYL//Ur1dnmvW9xsVdrUm8cYpox73xCt+vsi6g==
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Root page / redirects to: https://vodafone.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-10-16 23:00:15 (GMT5.5) (2125 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto# 
```

I choose this subdomain because Vodafone is a famous internet service provider in India. This scan took around 30 minutes and 0 errors were found this subdomain is protected against cross site attacks as all other subdomains.

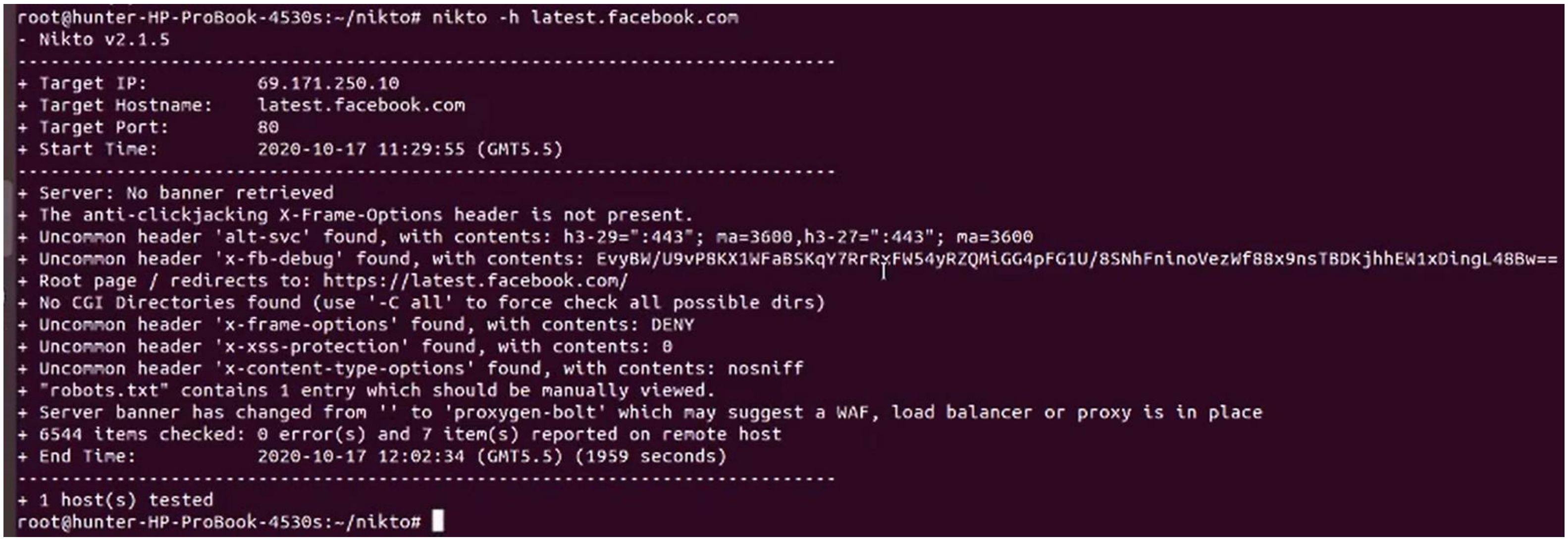
Eighth scan “business.facebook.com”



```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h business.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.15
+ Target Hostname:    business.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-17 10:47:01 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Uncommon header 'x-fb-debug' found, with contents: kwahtMCiMeeRAlLIiUkjZHBidabwsnxvlkeB3M/i5JqRZAmaLF7RY3Q+ThFwKALQFTQOP8miWtVQ1jEf4QXx0A==
+ Root page / redirects to: https://business.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ "robots.txt" contains 423 entries which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-10-17 11:22:30 (GMT5.5) (2129 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto#
```

This scan also took around 30 minutes. Results were same as the above. 0 errors were found 7 items reported on remote host, total scanned items 6544.

Ninth scan “latest.facebook.com”

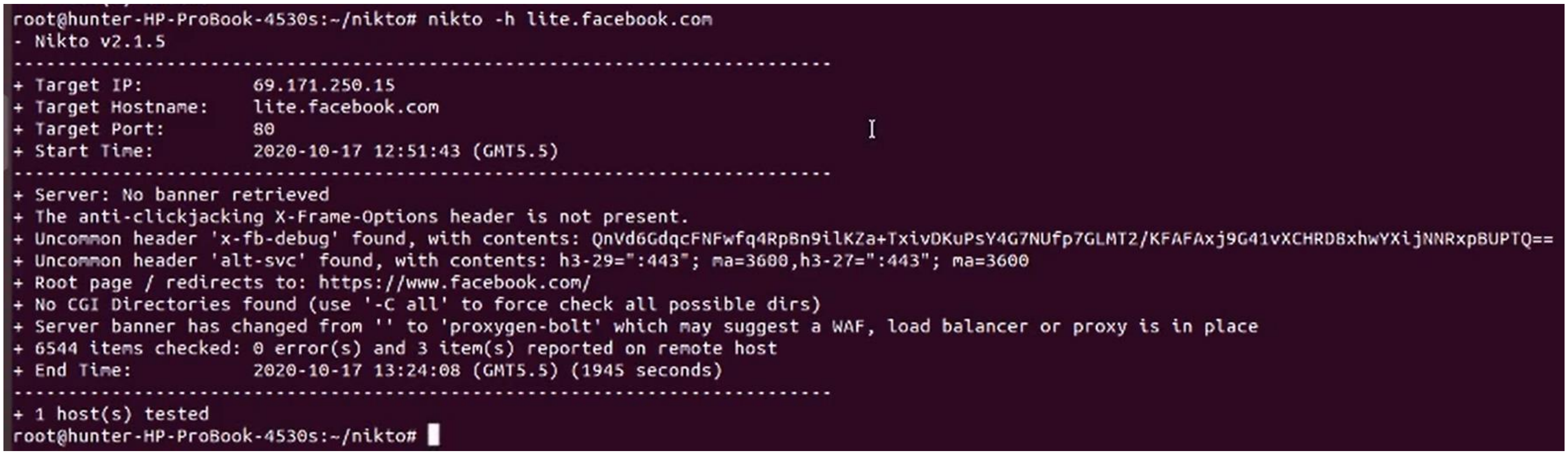


```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h latest.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.10
+ Target Hostname:    latest.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-17 11:29:55 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Uncommon header 'x-fb-debug' found, with contents: EvyBW/U9vP8KX1WFaBSKqY7RrRxFW54yRZQMiGG4pFG1U/8SNhFninoVezWf88x9nsTBDKjhhEW1xDingL48Bw==
+ Root page / redirects to: https://latest.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-10-17 12:02:34 (GMT5.5) (1959 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto# 
```

This scan took around 25 minutes. This subdomain also has nosniff protection as other subdomains. Nosniff prevents the browser from doing MIME-type sniffing.

0 errors were found. Target IP: 69.171.250.10

Tenth scan “lite.facebook.com”

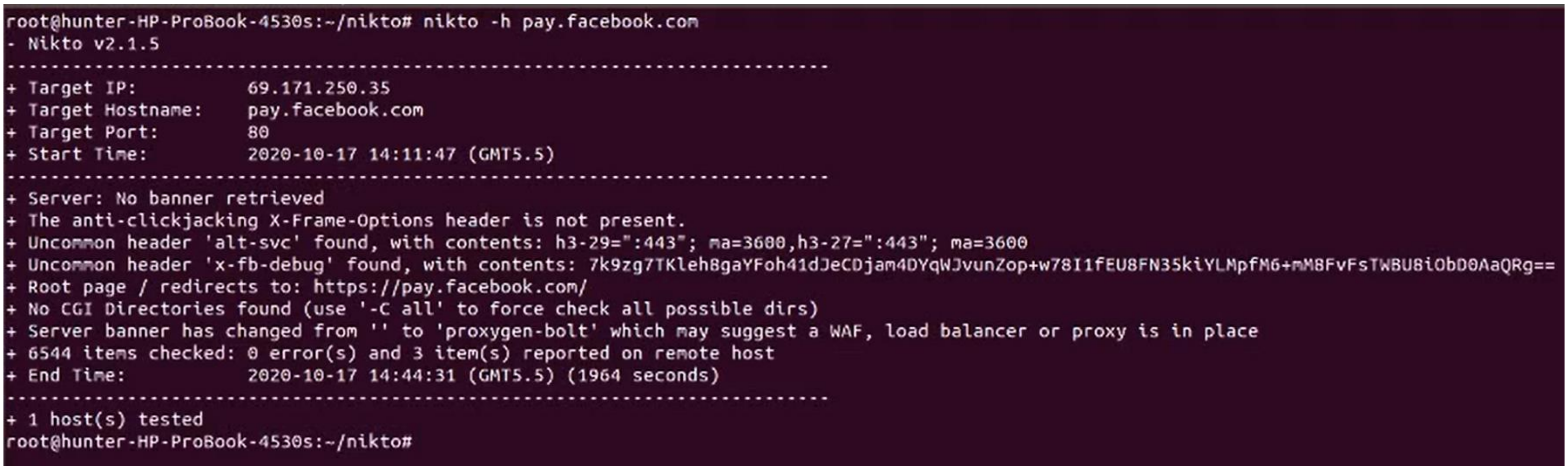


```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h lite.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.15
+ Target Hostname:    lite.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-17 12:51:43 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-fb-debug' found, with contents: QnVd6GdqcFNFwfq4RpBn9ilKZa+TxivDKuPsY4G7NUfp7GLMT2/KFAFAxj9G41vXCHRD8xhwYXijNNRxpBUPTQ==
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Root page / redirects to: https://www.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2020-10-17 13:24:08 (GMT5.5) (1945 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto# 
```

Scanning lite.facebook.com took around 30 minutes. This subdomain don’t have sniffing protection as the results shows. I choose this because there Is a Facebook lite app and it have a subdomain, and this is it.

0 errors were found and only 3 items were reported on remote host.

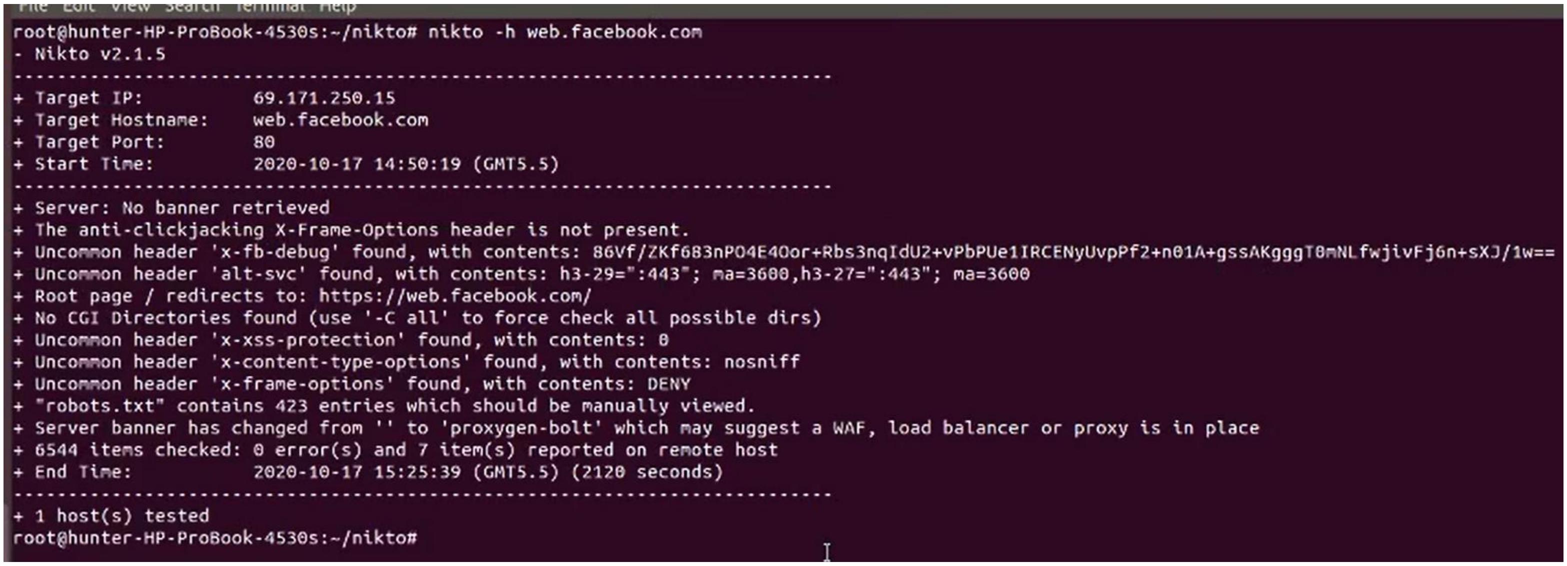
Eleventh scan “pay.facebook.com”



```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h pay.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.35
+ Target Hostname:    pay.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-17 14:11:47 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Uncommon header 'x-fb-debug' found, with contents: 7k9zg7TKleh8gaYFoh41dJeCDjam4DYqWJvunZop+w78I1fEU8FN35kiYLMpfM6+mM8FvFsTWBU8iObD0AaQRg==
+ Root page / redirects to: https://pay.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2020-10-17 14:44:31 (GMT5.5) (1964 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto#
```

This scan was also taking around 30 minutes and 0 errors found, 3 items were reported on remote host. Target IP: 69.171.250.35

Twelfth scan “web.facebook.com”

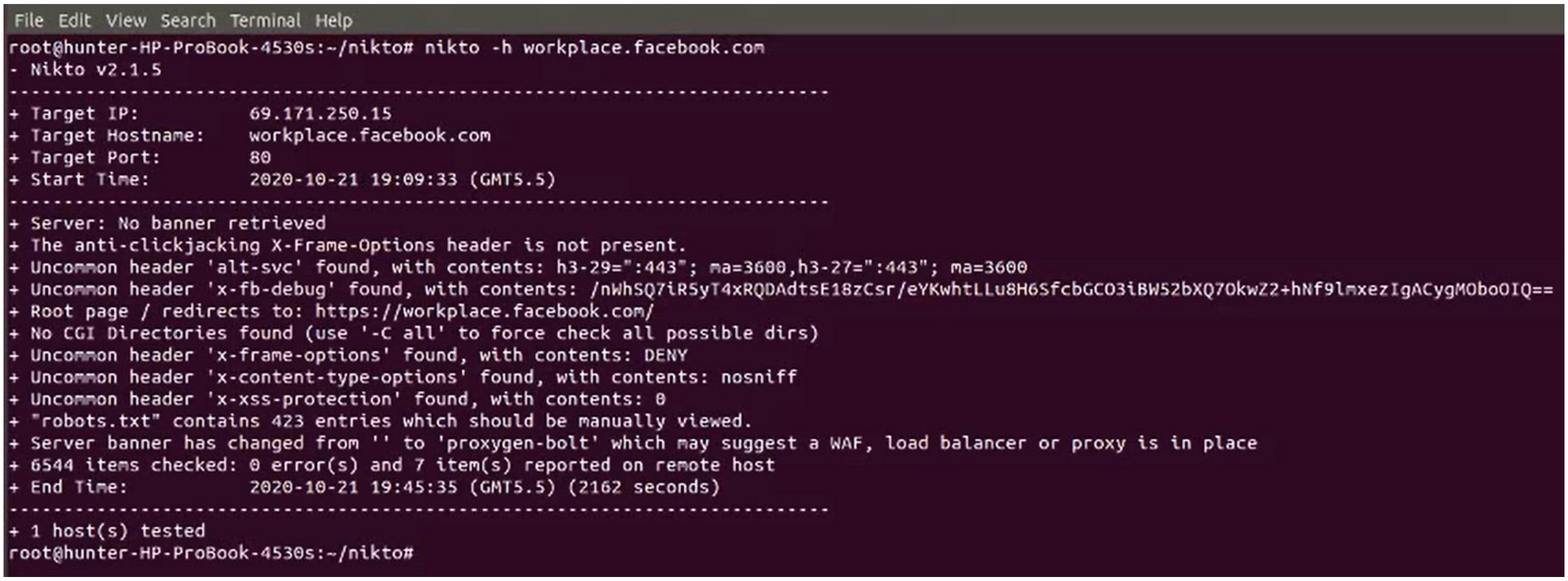


```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h web.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.15
+ Target Hostname:    web.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-17 14:50:19 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-fb-debug' found, with contents: 86Vf/ZKf683nPO4E4Oor+Rbs3nqIdU2+vPbPUe1IRCENyUvpPf2+n01A+gssAKgggT0mNLfwjivFj6n+sXJ/1w==
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Root page / redirects to: https://web.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ "robots.txt" contains 423 entries which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-10-17 15:25:39 (GMT5.5) (2120 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto#
```

I choose this because this is their main web application domain. Took around 40 minutes, 0 errors were found and 7 items reported on remote host.

Sniffing protection is add to this subdomain. Scanned items : 6544.

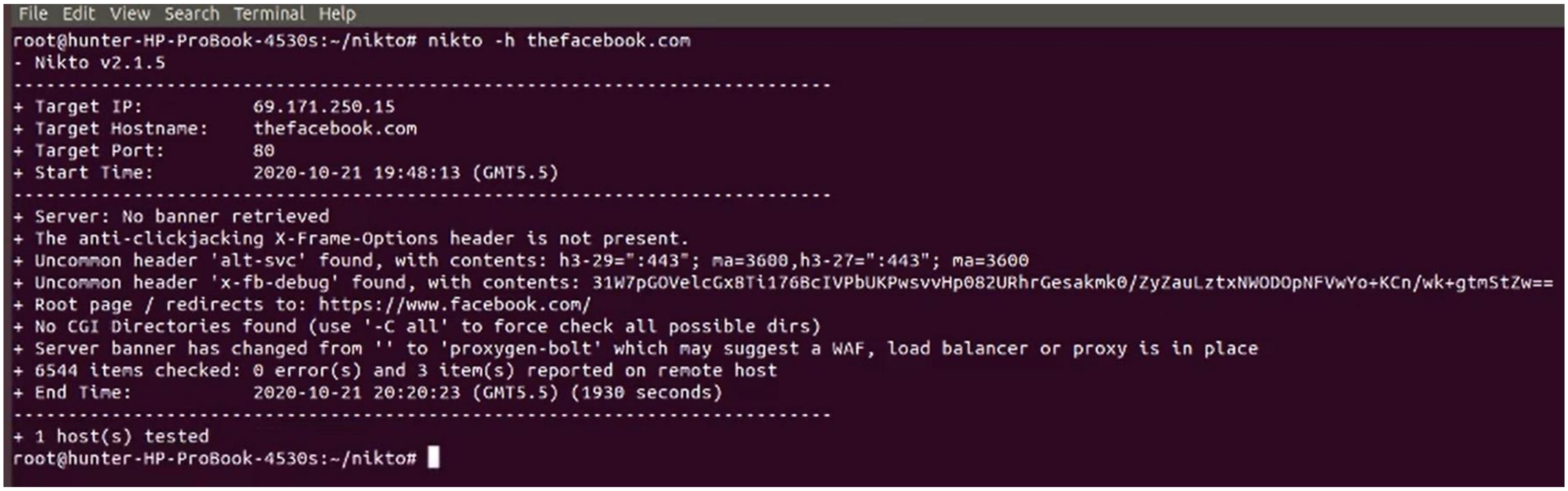
Thirteenth scan “workplace.facebook.com”



```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h workplace.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.15
+ Target Hostname:    workplace.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-21 19:09:33 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Uncommon header 'x-fb-debug' found, with contents: /nWhSQ7iR5yT4xRQDAdtsE18zCsr/eYKwhtLLu8H6SfcbGCO3iBW52bXQ7OkwZ2+hNf9lmxezIgACygMOboOIQ==
+ Root page / redirects to: https://workplace.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ "robots.txt" contains 423 entries which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-10-21 19:45:35 (GMT5.5) (2162 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto#
```

This scan took around 40 minutes. 0 errors were found, and 7 items reported on remote host. Sniffing protection is also added to this subdomain. Target IP: 69.171.250.15

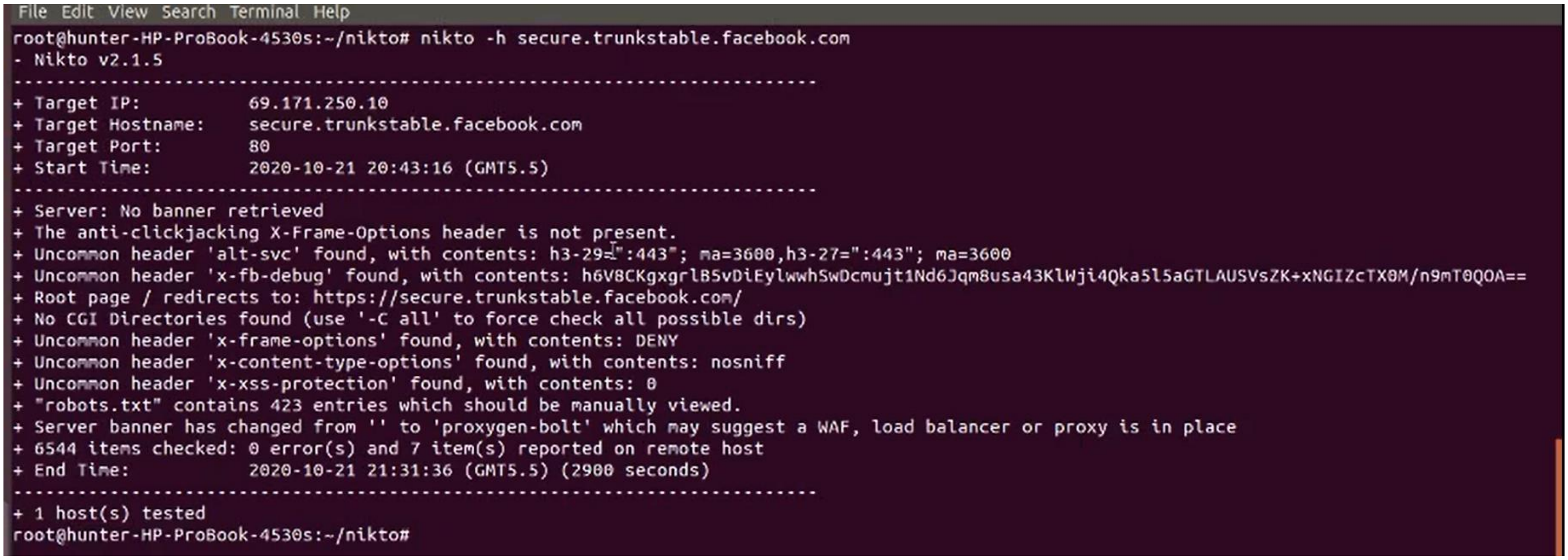
Fourteenth scan “thefacebook.com”



```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h thefacebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.15
+ Target Hostname:    thefacebook.com
+ Target Port:        80
+ Start Time:         2020-10-21 19:48:13 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Uncommon header 'x-fb-debug' found, with contents: 31W7pGOVelcGx8Ti176BcIVPbUKPwsvvHp082URhrGesakmk0/ZyZauLztxNWODOpNFVwYo+KCn/wk+gtmStZw==
+ Root page / redirects to: https://www.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2020-10-21 20:20:23 (GMT5.5) (1930 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto#
```

This scan only took around 20 minutes. Thefacebook.com subdomain was redirected to the www.facebook.com domain as the results shows. But last week I did a scan on www.facebook.com domain and it took around 3 hours to scan and I was able to find 3 vulnerabilities on that domain but I was unable to find out any vulnerability or a CVE code for a vulnerability in this scan results. It's only shows 0 errors and 3 items reported on remotes host just like the most of subdomains.

Fifteenth scan "secure.trunkstable.facebook.com"



```
root@hunter-HP-ProBook-4530s:~/nikto# nikto -h secure.trunkstable.facebook.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          69.171.250.10
+ Target Hostname:    secure.trunkstable.facebook.com
+ Target Port:        80
+ Start Time:         2020-10-21 20:43:16 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'alt-svc' found, with contents: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600
+ Uncommon header 'x-fb-debug' found, with contents: h6V8CKgxgrlB5vDiEylwwhSwDcmujt1Nd6Jqm8usa43KlWji4Qka5l5aGTLAUSVsZK+xNGIZcTX0M/n9mT0QOA==
+ Root page / redirects to: https://secure.trunkstable.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ "robots.txt" contains 423 entries which should be manually viewed.
+ Server banner has changed from '' to 'proxygen-bolt' which may suggest a WAF, load balancer or proxy is in place
+ 6544 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-10-21 21:31:36 (GMT5.5) (2900 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@hunter-HP-ProBook-4530s:~/nikto#
```

I choose this subdomain because it was in secure section subdomain list with other secure submains. To scan this subdomain, it took around 45 minutes. Sniffing protection is added to this subdomain like some other subdomains. But I was unable to find any vulnerability and scan results shows there was 0 errors.

Links to resources :

Xoop error details: https://www.cvedetails.com/vulnerability-list/vendor_id-1081/product_id-1876/Xoops-Xoops.html

Sniffing protection: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

CVE-2000-0413: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0413

https://www.idplr.com/136-free-articles/page-1.html?orderby=4

CVE-2000-0709: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0709

https://nvd.nist.gov/vuln/detail/CVE-2000-0709

CVE-2000-0710: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0710

https://nvd.nist.gov/vuln/detail/CVE-2000-0710