Sri Lanka Institute of Information Technology

BUG BOUNTY REPORT - 6

Web Security – IE2062

IT22362780

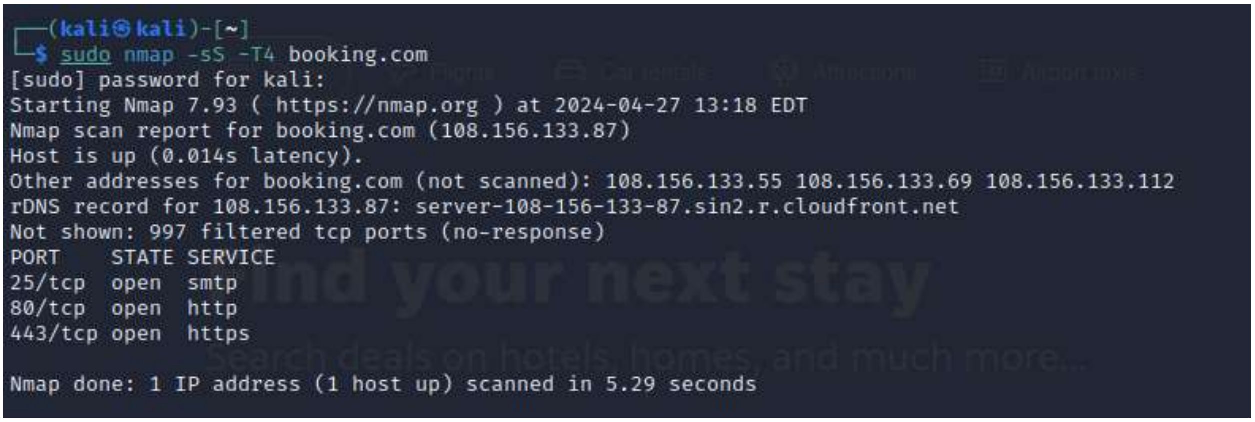
Jayaweera N.S

Report Details

Report #	- 06
Domain	- https://booking.com
Platform	-bugcrowd.com
Scans performed -	Recon-ng scan Nmap scan Wafw00f scan Dotdotpwn scan Nikto scan Sqlmap scan Manual scanning using Wapplyzer nslookup metasploit

Nmap scan

Using nmap scan all the open ports in the target can be identified.



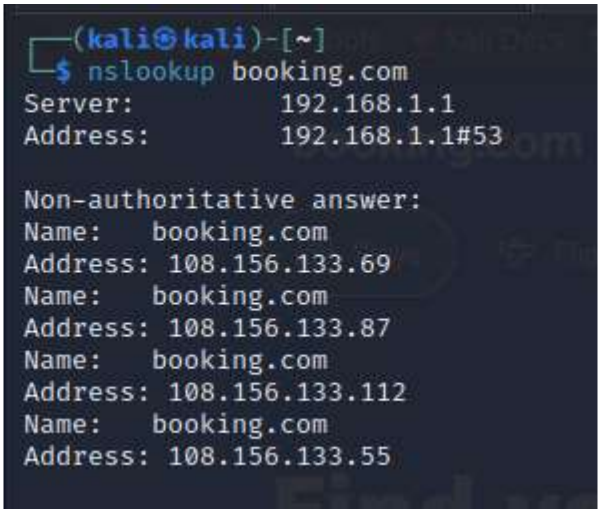
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -T4 booking.com
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-27 13:18 EDT
Nmap scan report for booking.com (108.156.133.87)
Host is up (0.014s latency).
Other addresses for booking.com (not scanned): 108.156.133.55 108.156.133.69 108.156.133.112
rDNS record for 108.156.133.87: server-108-156-133-87.sin2.r.cloudfront.net
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.29 seconds
```

No unusual ports are open.

But Smtp port 25 is vulnerable when it’s opened, because it lacks authentication and encryption.

Let’s see if we can establish a connection on port 25.

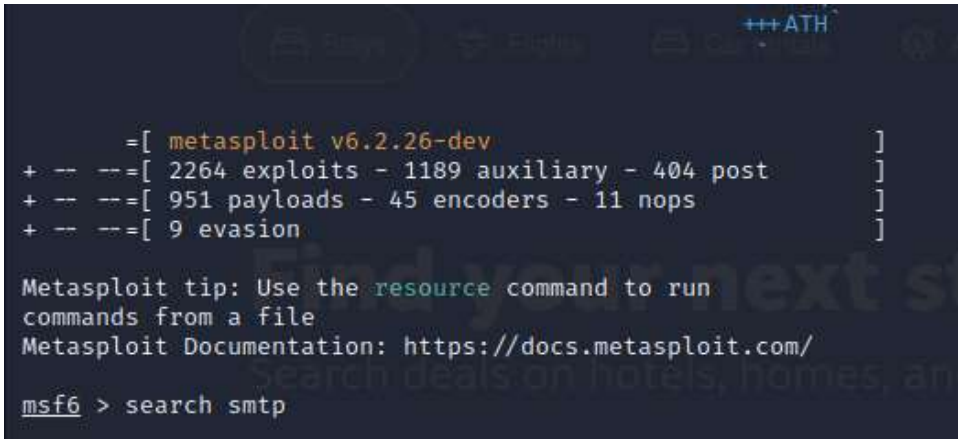
Nslookup



```
┌──(kali㉿kali)-[~]
└─$ nslookup booking.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   booking.com
Address: 108.156.133.69
Name:   booking.com
Address: 108.156.133.87
Name:   booking.com
Address: 108.156.133.112
Name:   booking.com
Address: 108.156.133.55
```

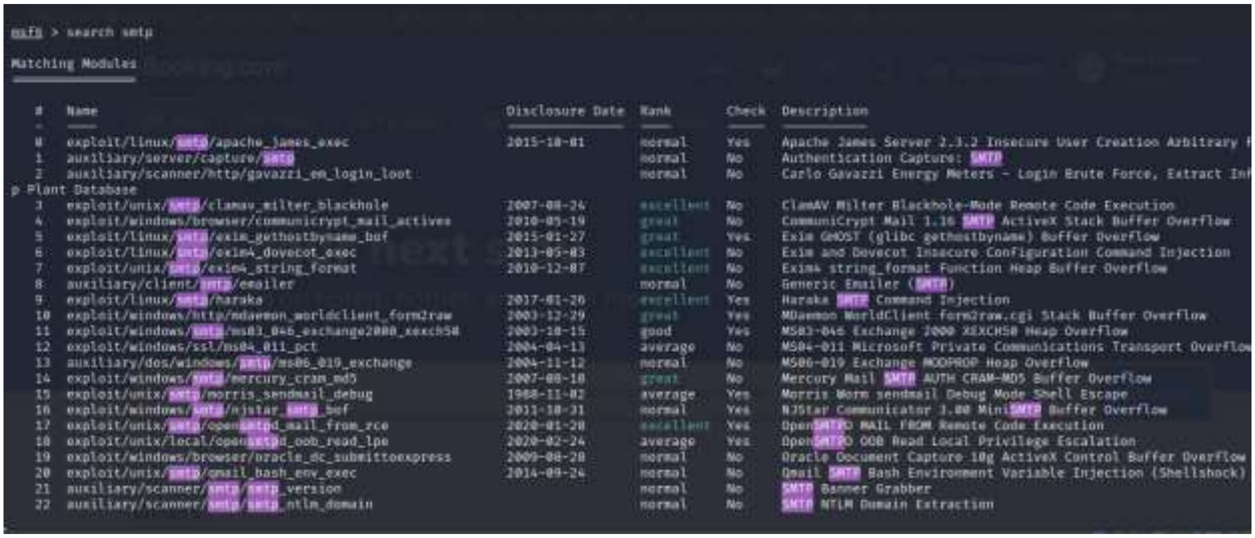
The ip address of bokking.com is found.

Metasploit



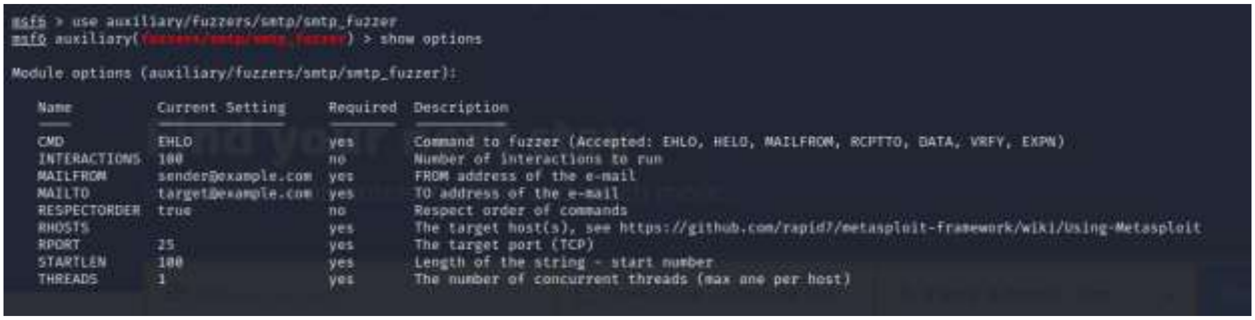
```
       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search smtp
```

Search for smtp.



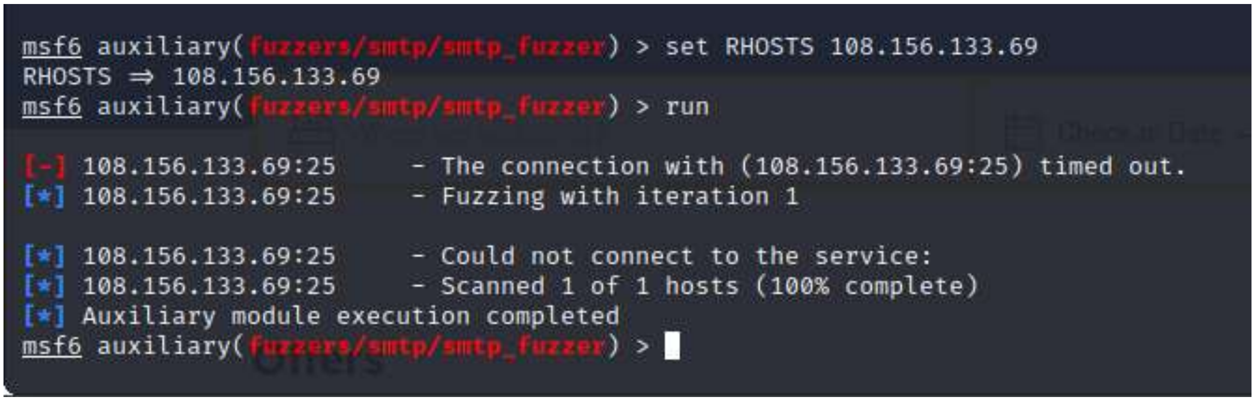
```
msf6 > search smtp

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                  2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary F
   1   auxiliary/server/capture/smtp                                          normal     No     Authentication Capture: SMTP
   2   auxiliary/scanner/http/gavazzi_em_login_loot                           normal     No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Inf
p Plant Database
   3   exploit/unix/smtp/clamav_milter_blackhole             2007-08-24       excellent  No     ClamAV Milter Blackhole-Mode Remote Code Execution
   4   exploit/windows/browser/communicrypt_mail_activex     2010-05-19       great      No     CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
   5   exploit/linux/smtp/exim_gethostbyname_bof             2015-01-27       great      Yes    Exim GHOST (glibc gethostbyname) Buffer Overflow
   6   exploit/linux/smtp/exim4_dovecot_exec                 2013-05-03       excellent  No     Exim and Dovecot Insecure Configuration Command Injection
   7   exploit/unix/smtp/exim4_string_format                 2010-12-07       excellent  No     Exim4 string_format Function Heap Buffer Overflow
   8   auxiliary/client/smtp/emailer                                          normal     No     Generic Emailer (SMTP)
   9   exploit/linux/smtp/haraka                             2017-01-26       excellent  Yes    Haraka SMTP Command Injection
   10  exploit/windows/http/mdaemon_worldclient_form2raw     2003-12-29       great      Yes    MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
   11  exploit/windows/smtp/ms03_046_exchange2000_xexch50    2003-10-15       good       Yes    MS03-046 Exchange 2000 XEXCH50 Heap Overflow
   12  exploit/windows/ssl/ms04_011_pct                      2004-04-13       average    No     MS04-011 Microsoft Private Communications Transport Overflow
   13  auxiliary/dos/windows/smtp/ms06_019_exchange          2004-11-12       normal     No     MS06-019 Exchange MODPROP Heap Overflow
   14  exploit/windows/smtp/mercury_cram_md5                 2007-08-18       great      No     Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
   15  exploit/unix/smtp/morris_sendmail_debug               1988-11-02       average    Yes    Morris Worm sendmail Debug Mode Shell Escape
   16  exploit/windows/smtp/njstar_smtp_bof                  2011-10-31       normal     Yes    NJStar Communicator 3.00 MiniSMTP Buffer Overflow
   17  exploit/unix/smtp/opensmtpd_mail_from_rce             2020-01-28       excellent  Yes    OpenSMTPD MAIL FROM Remote Code Execution
   18  exploit/unix/local/opensmtpd_oob_read_lpe             2020-02-24       average    Yes    OpenSMTPD OOB Read Local Privilege Escalation
   19  exploit/windows/browser/oracle_dc_submittoexpress     2009-08-28       normal     No     Oracle Document Capture 10g ActiveX Control Buffer Overflow
   20  exploit/unix/smtp/qmail_bash_env_exec                 2014-09-24       normal     No     Qmail SMTP Bash Environment Variable Injection (Shellshock)
   21  auxiliary/scanner/smtp/smtp_version                                    normal     No     SMTP Banner Grabber
   22  auxiliary/scanner/smtp/smtp_ntlm_domain                                normal     No     SMTP NTLM Domain Extraction
```

Use the “fuzzer” module to fuzz the smtp service and the “smtp_enum” is used to username enumeration.



```
msf6 > use auxiliary/fuzzers/smtp/smtp_fuzzer
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > show options

Module options (auxiliary/fuzzers/smtp/smtp_fuzzer):

   Name          Current Setting     Required  Description
   ----          ---------------     --------  -----------
   CMD           EHLO                yes       Command to fuzzer (Accepted: EHLO, HELO, MAILFROM, RCPTTO, DATA, VRFY, EXPN)
   INTERACTIONS  100                 no        Number of interactions to run
   MAILFROM      sender@example.com  yes       FROM address of the e-mail
   MAILTO        target@example.com  yes       TO address of the e-mail
   RESPECTORDER  true                no        Respect order of commands
   RHOSTS                            yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT         25                  yes       The target port (TCP)
   STARTLEN      100                 yes       Length of the string - start number
   THREADS       1                   yes       The number of concurrent threads (max one per host)
```

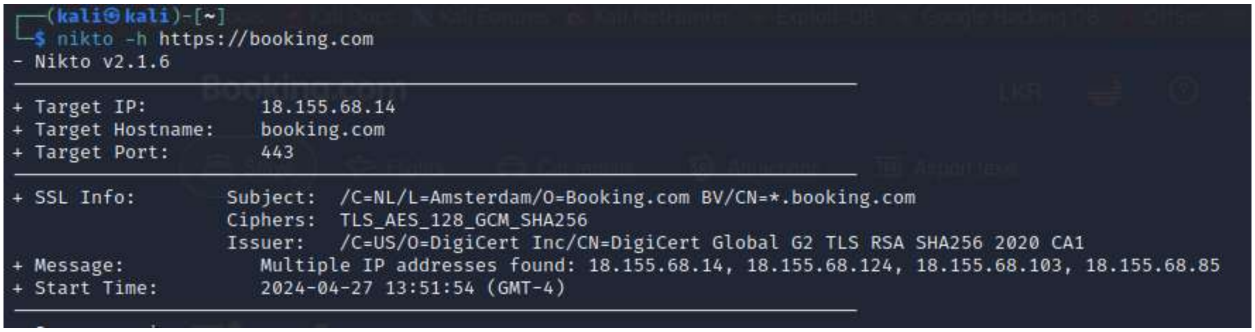
Set the RHOSTS to temu.com or the set the ip address of temu.com.



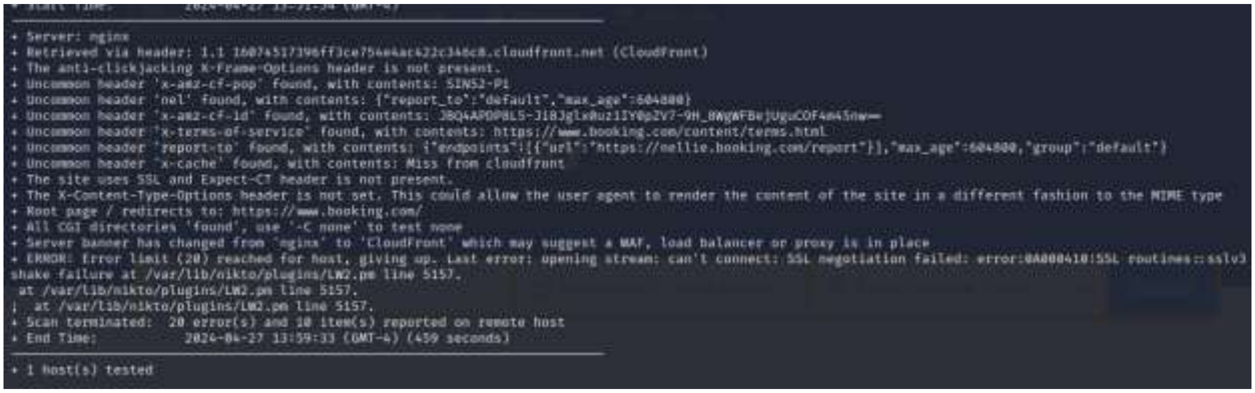
```
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > set RHOSTS 108.156.133.69
RHOSTS ⇒ 108.156.133.69
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > run

[-] 108.156.133.69:25     - The connection with (108.156.133.69:25) timed out.
[*] 108.156.133.69:25     - Fuzzing with iteration 1

[*] 108.156.133.69:25     - Could not connect to the service:
[*] 108.156.133.69:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > 
```

Fuzzing failed due to connection time out indicating inability to enumerate the service. fuzzing attempts blocked by server.

Nikto scan



```
┌──(kali㉿kali)-[~]
└─$ nikto -h https://booking.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          18.155.68.14
+ Target Hostname:    booking.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=NL/L=Amsterdam/O=Booking.com BV/CN=*.booking.com
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
+ Message:            Multiple IP addresses found: 18.155.68.14, 18.155.68.124, 18.155.68.103, 18.155.68.85
+ Start Time:         2024-04-27 13:51:54 (GMT-4)
---------------------------------------------------------------------------
```



```
+ Start Time:         2024-04-27 13:51:54 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ Retrieved via header: 1.1 16074517396ff3ce754e4ac422c346c8.cloudfront.net (CloudFront)
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-amz-cf-pop' found, with contents: SIN52-P1
+ Uncommon header 'nel' found, with contents: {"report_to":"default","max_age":604800}
+ Uncommon header 'x-amz-cf-id' found, with contents: JBQ4APDP8L5-J18JglxBuz1IY0pZV7-9H_8WgWFBejUguCOF4m45nw==
+ Uncommon header 'x-terms-of-service' found, with contents: https://www.booking.com/content/terms.html
+ Uncommon header 'report-to' found, with contents: {"endpoints":[{"url":"https://nellie.booking.com/report"}],"max_age":604800,"group":"default"}
+ Uncommon header 'x-cache' found, with contents: Miss from cloudfront
+ 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 agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.booking.com/
+ All CGI directories 'found', use '-C none' to test none
+ Server banner has changed from 'nginx' to 'CloudFront' which may suggest a WAF, load balancer or proxy is in place
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::sslv3
shake 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 10 item(s) reported on remote host
+ End Time:           2024-04-27 13:59:33 (GMT-4) (459 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Results obtained from the scan:

- The anti-clickjacking "X-Frame-Options" header, which helps prevent clickjacking attacks, is not present.
- The site uses SSL and Expect -CT header is not present.

The "expect-CT" header is a security feature that helps websites, and their users avoid the risks associated with incorrectly issued SSL certificates.

It supports transparency and accountability when issuing SSL certificates, which improves overall web security.

There are some issues/disadvantages occurred when the “expect-CT” header is absent:

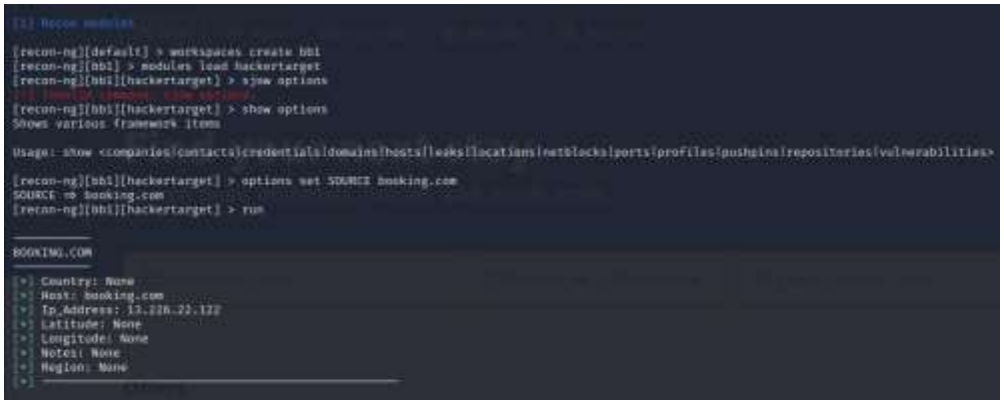
- The protection against the mis issuing of SSL certificates will be low.
- Mismanagement of SSL certificates.
- No trust and security

But the absence of “expected-CT” header is not a huge vulnerability or a security issue in a website.

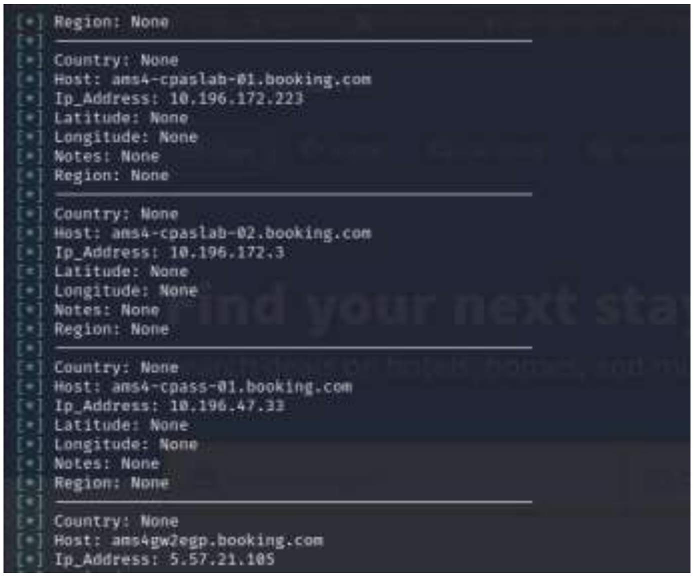
- The X-Content-Type-Options header is not set.

Recon-ng

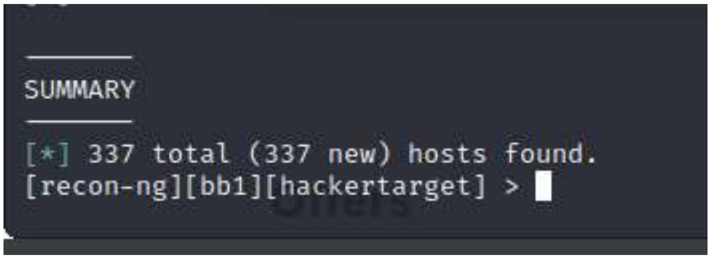
here the recon-ng will be used to find all the sub domains in the target.



```
[1] Recon modules

[recon-ng][default] > workspaces create bb1
[recon-ng][bb1] > modules load hackertarget
[recon-ng][bb1][hackertarget] > sjow options
[!] Invalid command: sjow options.
[recon-ng][bb1][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts||leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][bb1][hackertarget] > options set SOURCE booking.com
SOURCE => booking.com
[recon-ng][bb1][hackertarget] > run

-----------
BOOKING.COM
-----------
[*] Country: None
[*] Host: booking.com
[*] Ip_Address: 13.226.22.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
```



```
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: ams4-cpaslab-01.booking.com
[*] Ip_Address: 10.196.172.223
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: ams4-cpaslab-02.booking.com
[*] Ip_Address: 10.196.172.3
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: ams4-cpass-01.booking.com
[*] Ip_Address: 10.196.47.33
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: ams4gw2egp.booking.com
[*] Ip_Address: 5.57.21.105
```

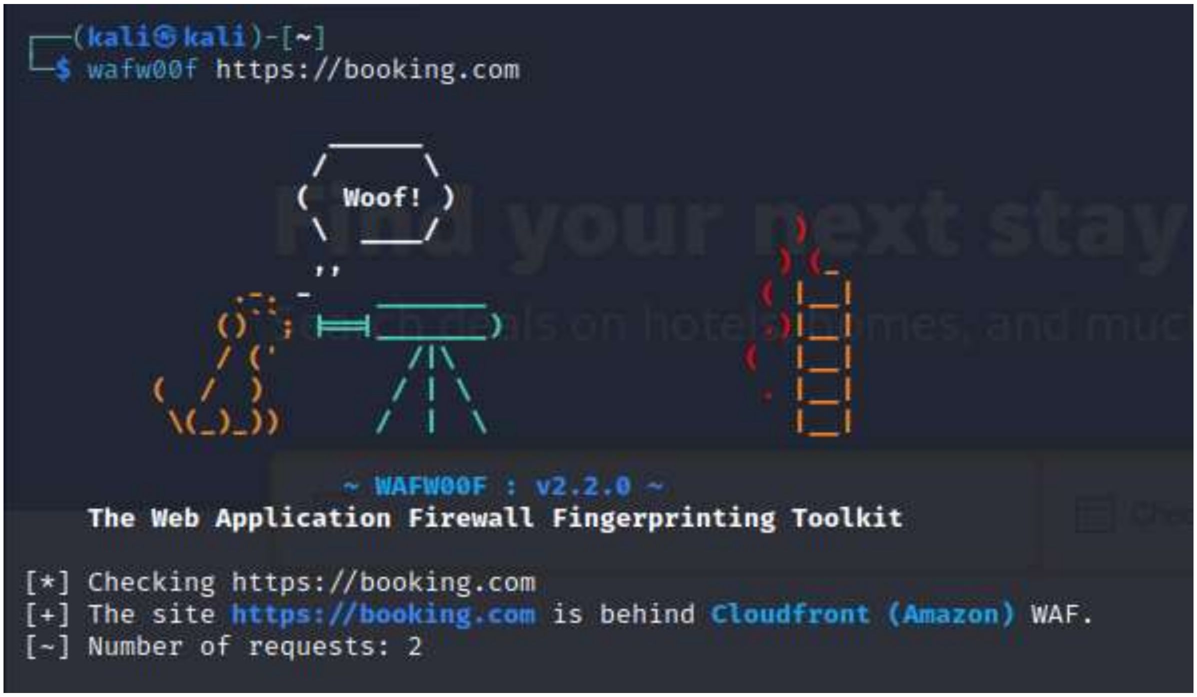


```
-------
SUMMARY
-------
[*] 337 total (337 new) hosts found.
[recon-ng][bb1][hackertarget] >
```

337 subdomains found.

Wafw00f scan

Used to identify the type of WAF that is used to protect the web application.

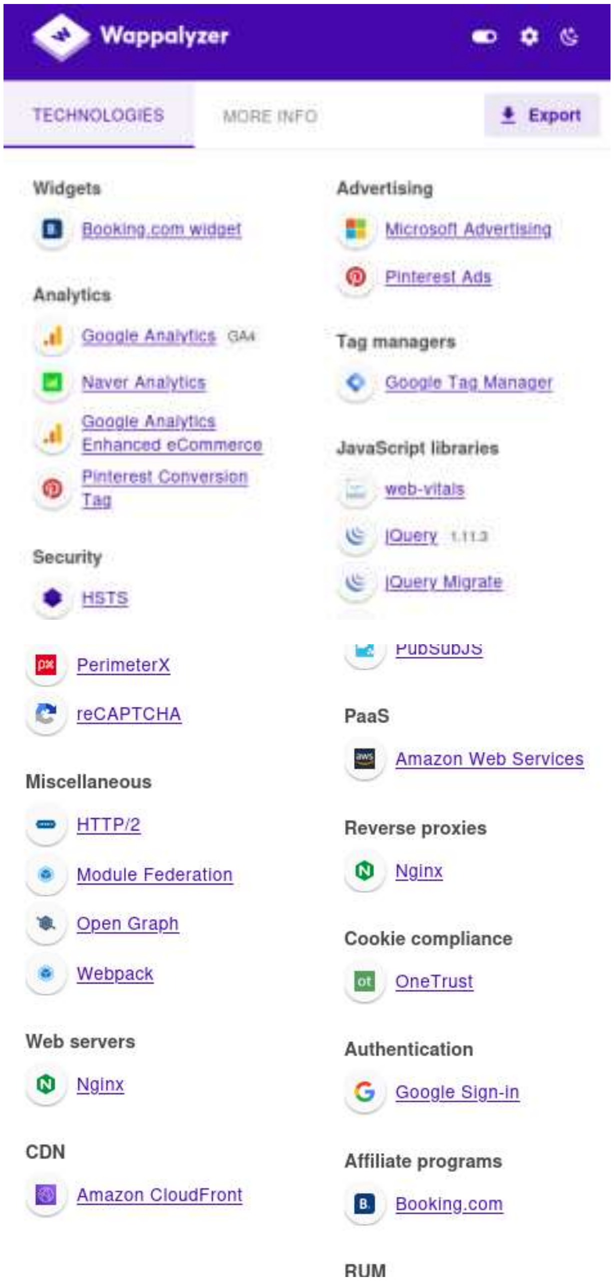


```
┌──(kali㉿kali)-[~]
└─$ wafw00f https://booking.com

                ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://booking.com
[+] The site https://booking.com is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

“CloudFront” is the firewall WAF used.

Wapplyzer

The Wapplyzer is used to identify the technologies used in the web application.



Widgets

- Booking.com widget

Analytics

- Google Analytics GA4
- Naver Analytics
- Google Analytics Enhanced eCommerce
- Pinterest Conversion Tag

Security

- HSTS
- PerimeterX
- reCAPTCHA

Miscellaneous

- HTTP/2
- Module Federation
- Open Graph
- Webpack

Web servers

- Nginx

CDN

- Amazon CloudFront

Advertising

- Microsoft Advertising
- Pinterest Ads

Tag managers

- Google Tag Manager

JavaScript libraries

- web-vitals
- jQuery 1.11.3
- jQuery Migrate
- PubSubJS

PaaS

- Amazon Web Services

Reverse proxies

- Nginx

Cookie compliance

- OneTrust

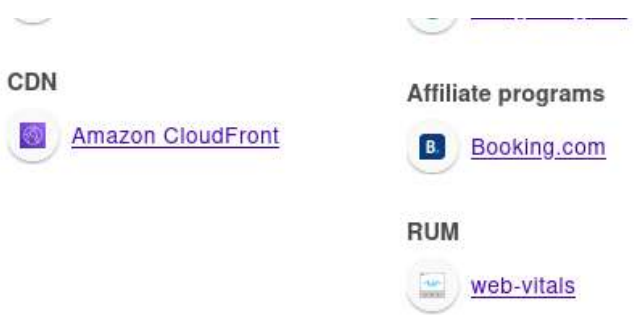
Authentication

- Google Sign-in

Affiliate programs

- Booking.com

RUM



CDN

Amazon CloudFront

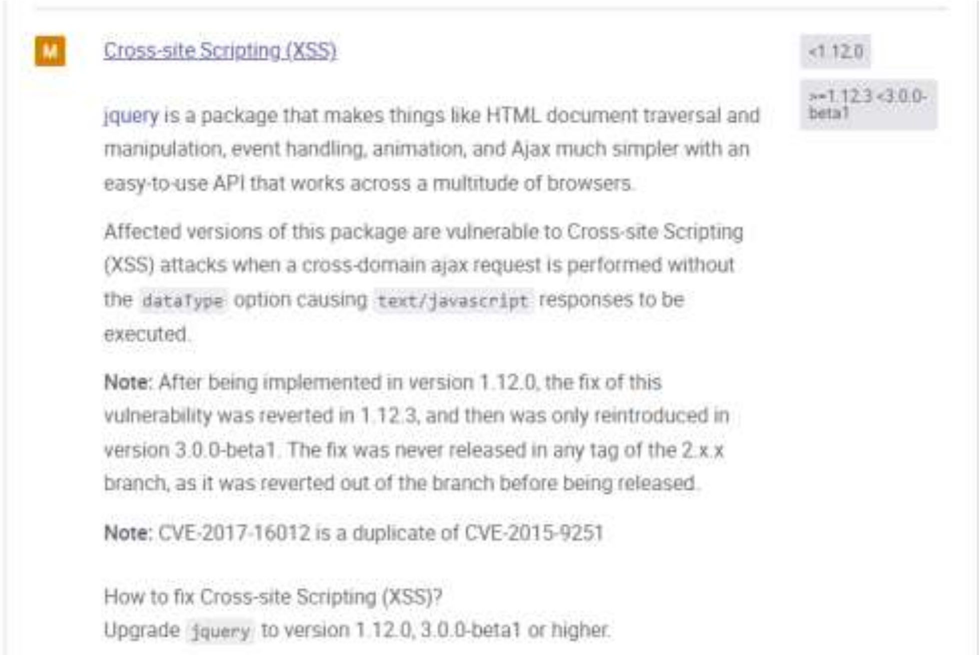
Affiliate programs

Booking.com

RUM

web-vitals

The version of jquery file is vulnerable.



M

Cross-site Scripting (XSS)

<1.12.0

>=1.12.3 <3.0.0-beta1

jquery is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.

Affected versions of this package are vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain ajax request is performed without the `dataType` option causing `text/javascript` responses to be executed.

Note: After being implemented in version 1.12.0, the fix of this vulnerability was reverted in 1.12.3, and then was only reintroduced in version 3.0.0-beta1. The fix was never released in any tag of the 2.x.x branch, as it was reverted out of the branch before being released.

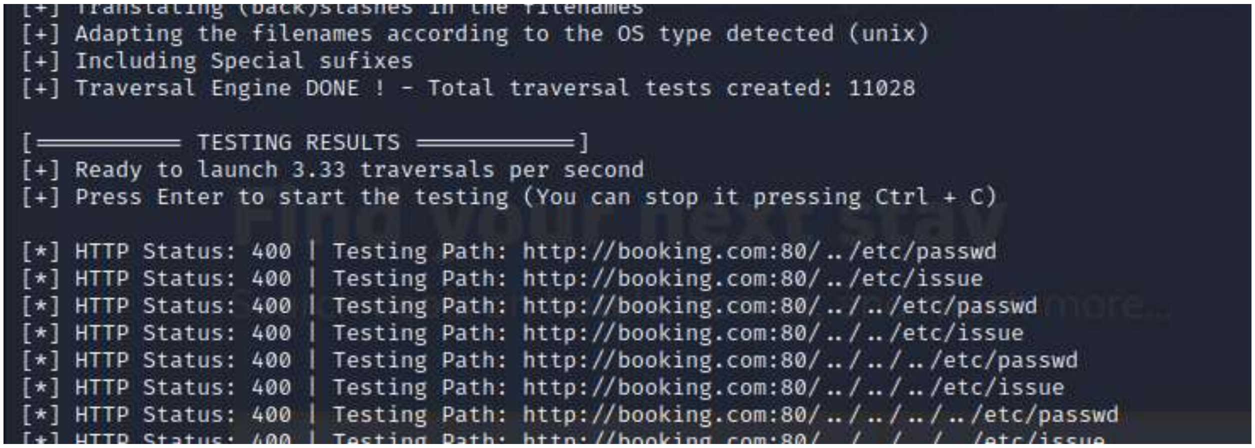
Note: CVE-2017-16012 is a duplicate of CVE-2015-9251

How to fix Cross-site Scripting (XSS)?
Upgrade `jquery` to version 1.12.0, 3.0.0-beta1 or higher.

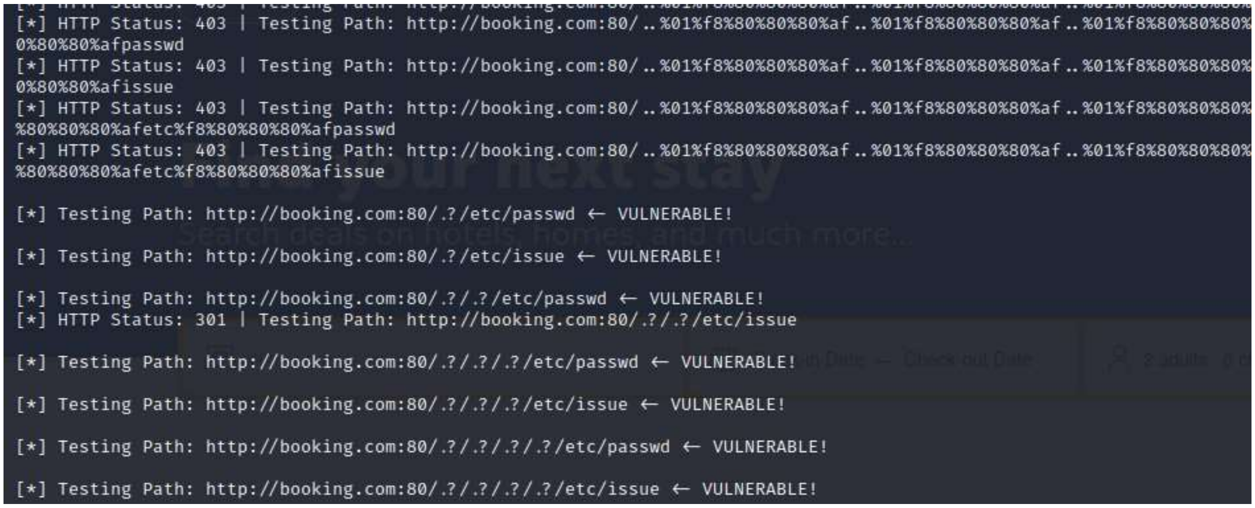
Update to jquery version 1.12.0, 3.0.0-beta1 or higher to mitigate the risk.

Dotdotpwn

Dotdotpwn is a directory traversal checker.



```
[+] Translating (back)slashes in the filenames
[+] Adapting the filenames according to the OS type detected (unix)
[+] Including Special sufixes
[+] Traversal Engine DONE ! - Total traversal tests created: 11028

[========== TESTING RESULTS ===========]
[+] Ready to launch 3.33 traversals per second
[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)

[*] HTTP Status: 400 | Testing Path: http://booking.com:80/../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://booking.com:80/../etc/issue
[*] HTTP Status: 400 | Testing Path: http://booking.com:80/../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://booking.com:80/../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://booking.com:80/../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://booking.com:80/../../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://booking.com:80/../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://booking.com:80/../../../../etc/issue
```



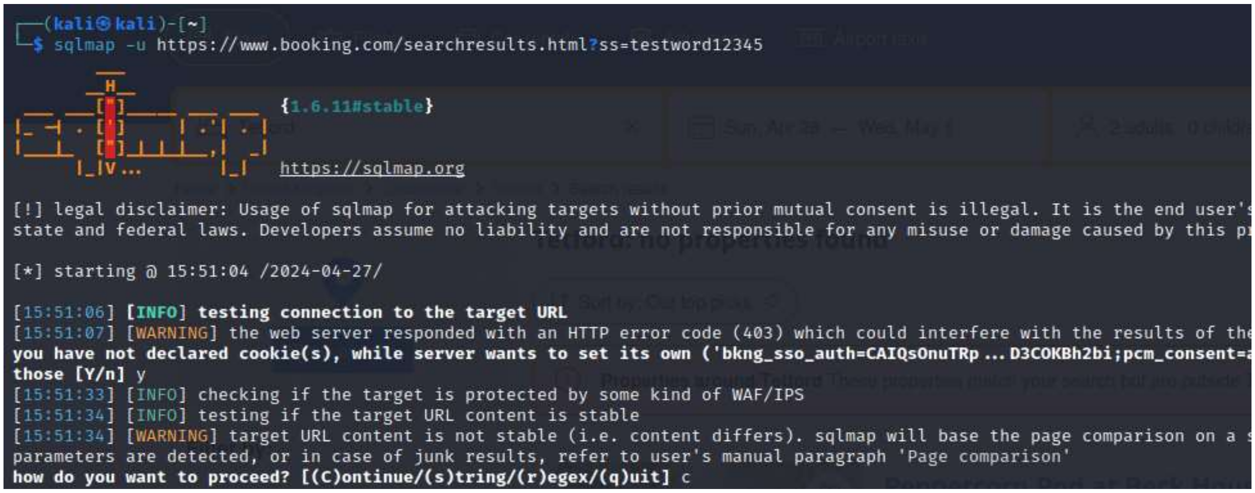
```
[*] HTTP Status: 403 | Testing Path: http://booking.com:80/..%01%f8%80%80%80%af..%01%f8%80%80%80%af..%01%f8%80%80%80%
0%80%80%afpasswd
[*] HTTP Status: 403 | Testing Path: http://booking.com:80/..%01%f8%80%80%80%af..%01%f8%80%80%80%af..%01%f8%80%80%80%
0%80%80%afissue
[*] HTTP Status: 403 | Testing Path: http://booking.com:80/..%01%f8%80%80%80%af..%01%f8%80%80%80%af..%01%f8%80%80%80%
%80%80%80%afetc%f8%80%80%80%afpasswd
[*] HTTP Status: 403 | Testing Path: http://booking.com:80/..%01%f8%80%80%80%af..%01%f8%80%80%80%af..%01%f8%80%80%80%
%80%80%80%afetc%f8%80%80%80%afissue

[*] Testing Path: http://booking.com:80/.?/etc/passwd ← VULNERABLE!

[*] Testing Path: http://booking.com:80/.?/etc/issue ← VULNERABLE!

[*] Testing Path: http://booking.com:80/.?/.?/etc/passwd ← VULNERABLE!
[*] HTTP Status: 301 | Testing Path: http://booking.com:80/.?/.?/etc/issue

[*] Testing Path: http://booking.com:80/.?/.?/.?/etc/passwd ← VULNERABLE!

[*] Testing Path: http://booking.com:80/.?/.?/.?/etc/issue ← VULNERABLE!

[*] Testing Path: http://booking.com:80/.?/.?/.?/.?/etc/passwd ← VULNERABLE!

[*] Testing Path: http://booking.com:80/.?/.?/.?/.?/etc/issue ← VULNERABLE!
```

The scan results returned status codes within the range 400 (400-499). It shows a client error.

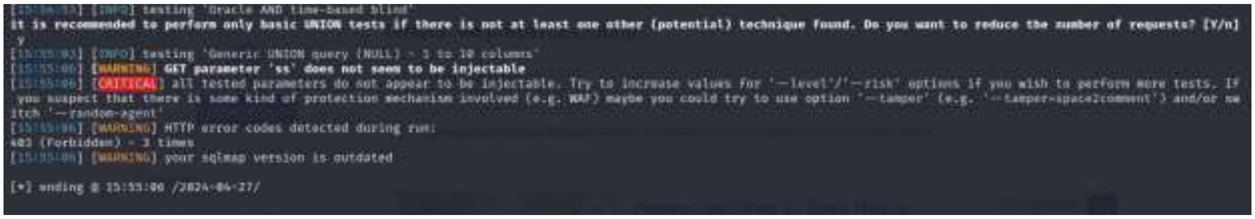
Some vulnerable paths were found.

Sqlmap

With the use of this scan, we can identify whether a sql injection can be done or not.



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u https://www.booking.com/searchresults.html?ss=testword12345
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.11#stable}
|_ -| . [']     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this pr

[*] starting @ 15:51:04 /2024-04-27/

[15:51:06] [INFO] testing connection to the target URL
[15:51:07] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the
you have not declared cookie(s), while server wants to set its own ('bkng_sso_auth=CAIQsOnuTRp...D3COKBh2bi;pcm_consent=a
those [Y/n] y
[15:51:33] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:51:34] [INFO] testing if the target URL content is stable
[15:51:34] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a s
parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
```



```
[15:54:53] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n]
 y
[15:55:03] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:55:06] [WARNING] GET parameter 'ss' does not seem to be injectable
[15:55:06] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If
 you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or sw
itch '--random-agent'
[15:55:06] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 3 times
[15:55:06] [WARNING] your sqlmap version is outdated

[*] ending @ 15:55:06 /2024-04-27/
```

There is no injection vulnerability in the above web application.