Sri Lanka Institute of Information Technology

BUG BOUNTY JOURNAL

Web Security – IE2062

IT22362780

Jayaweera N.S

Date - 17/03/2024

- Did a small research on OWASP top 10 vulnerabilities.

Vulnerability	Description
1. Broken access control	Improper authentication and access restrictions, which will allow the attackers to launch attacks, access sensitive information and access privileges.
2. Cryptographic failures	The use of outdates cryptographic algorithms, weak crypto keys and hardcoded passwords can result sensitive data breaches.
3. Injection	The web applications that accept untrusted data can get exploited by the attackers on their vulnerable points.
4. Insecure design	Implementing designs with flaws, improper controls, and development lifecycles.
5. Security misconfiguration	Misconfiguration or the improperly handling the error messages that leaks sensitive information, bad permissions, and leaving less secure default values unchanged.
6. Vulnerable and outdated components	Softwares that have previously known and reported vulnerabilities which can be exploited by an attacker.
7. Identification and authentication failures	Unavailability of mechanisms to identify and authorize between users and robots.
8. Software and data integrity failures	Malicious activities that happen during the building process such as creating insecure deployments, stealing secrets and using insecure tools.
9. Security logging and monitoring failures	the vulnerabilities that happen when the systems fails to monitor or log the security activities.
10. Server-side request forgery (SSRF)	Attacker attacking the server and accessing and modifying the resources unauthorizedly

- *Date - 18/03/2024*

- Created accounts on hacker one and bugcrowd.
- Started learning about tools that can be used to perform vulnerability scans.
- Found an automated scanning tool.

<u>Nmap scan</u>

- What is nmap scan?

  Nmap scan is used to identify all the open ports in a web application.

Type “nmap -sS -T4 <domain name>” to start the scan.

- -sS : known as SYN scan. It’s a default scan that can be used to scan thousands within a small amount of time.
- -T4 : defines the speed of the scan.

Therefore it performs a TCP SYN on the domain. The benefit of this scan is that it won’t send any ping probes when the hosts are shown.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap -sS -T4 truecaller.com
You requested a scan type which requires root privileges.
QUITTING!
```

Initially it requires administrator privileges to perform the scan. (Type : sudo <relevant command>)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -T4 truecaller.com
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-10 01:44 EDT
Nmap scan report for truecaller.com (65.2.43.23)
Host is up (0.014s latency).
Other addresses for truecaller.com (not scanned): 13.232.183.173
rDNS record for 65.2.43.23: ec2-65-2-43-23.ap-south-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https
```

And it shows all the open ports. Analyze the port using other tools well, if the vulnerability level is high.

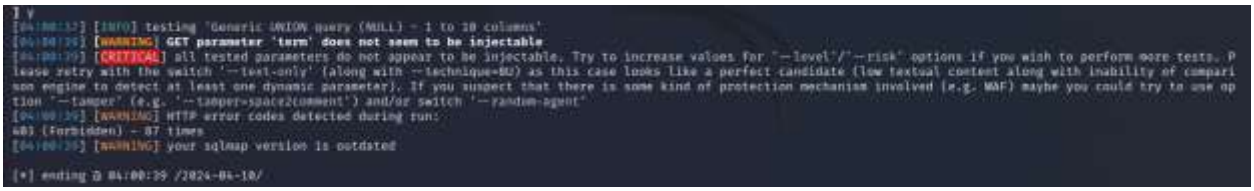
Date - 19/03/2024

- Continued learning about new scanning tools.

Sqlmap Scan

- What is sqlmap?

  Sqlmap is an exploitation tool that can be used to test whether it's vulnerable to sql injection. It automatically identifies and starts to exploit sql injection vulnerabilities.

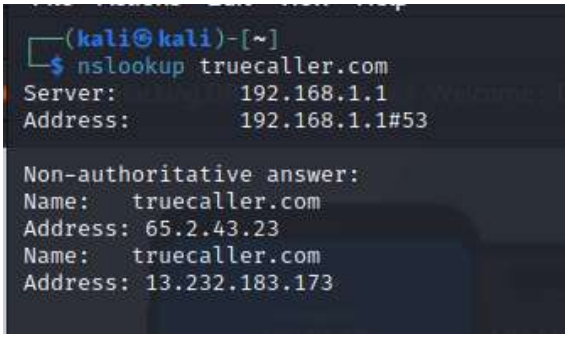


this tool is pre-installed in kali and it'll show the user whether it found injectable or not.

Nslookup

- What is nslookup?

  Nslookup also known as the DNS lookup is a scan that we can run in order to find ip addresses or DNS record.



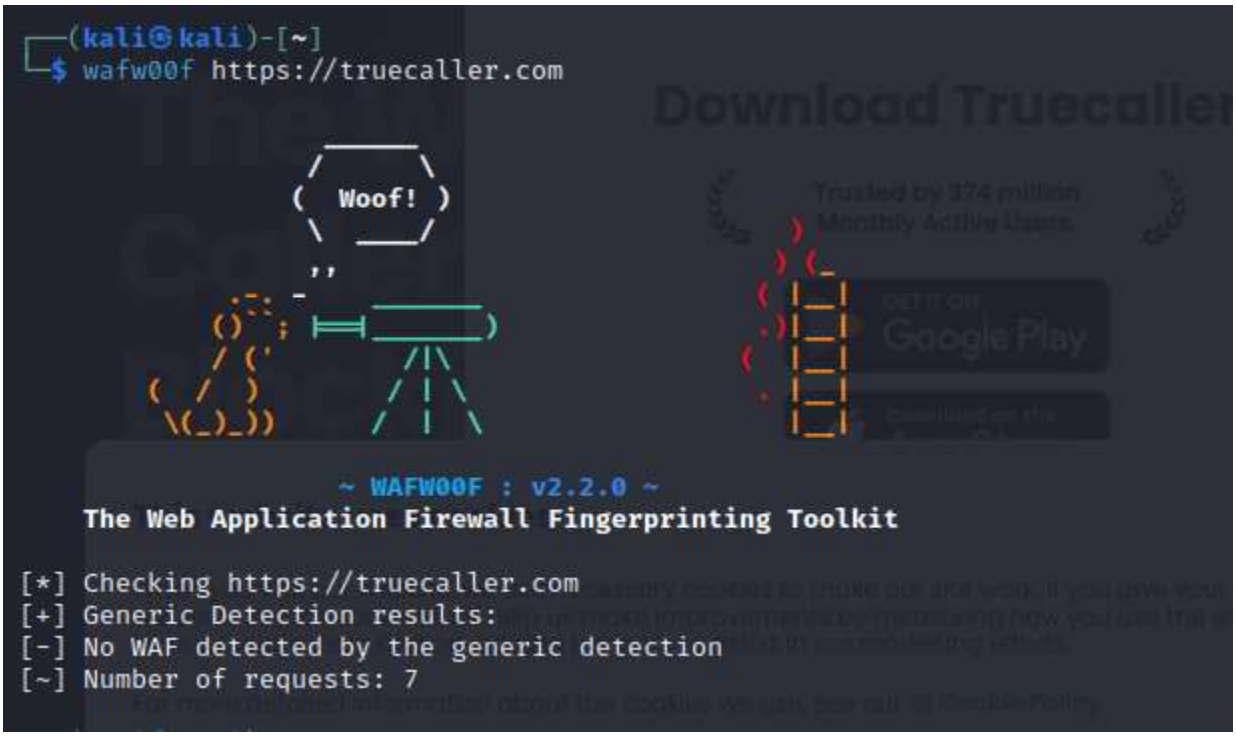
Date - 20/03/2024

- Continued learning about new tools.

Wafw00f scan

- What is Wafw00f?

  With the use of this tool the WAF that is used to protect the web application can be found. It is a python script. It can be easily done using the command “wafw00f <domain name>”



It displays the WAF used, if detected.

Date – 21/03/2024

- Continued learning about new tools.

Dotdotpwn scan

- What is dotdotpwn?

  It's used to identify directory traversal vulnerabilities in a web application. It is basically a fuzzer.

  With the use of the command "dotdotpwn -m http -h <domain name>"

```
[========== TARGET INFORMATION ==========]
[+] Hostname: truecaller.com
[+] Protocol: http
[+] Port: 80

[========== TRAVERSAL ENGINE ==========]
[+] Creating Traversal patterns (mix of dots and slashes)
[+] Multiplying 6 times the traversal patterns (-d switch)
[+] Creating the Special Traversal patterns
[+] 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://truecaller.com:80/../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../etc/issue
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../../../etc/issue
```

  It will directly show the vulnerability, if found.

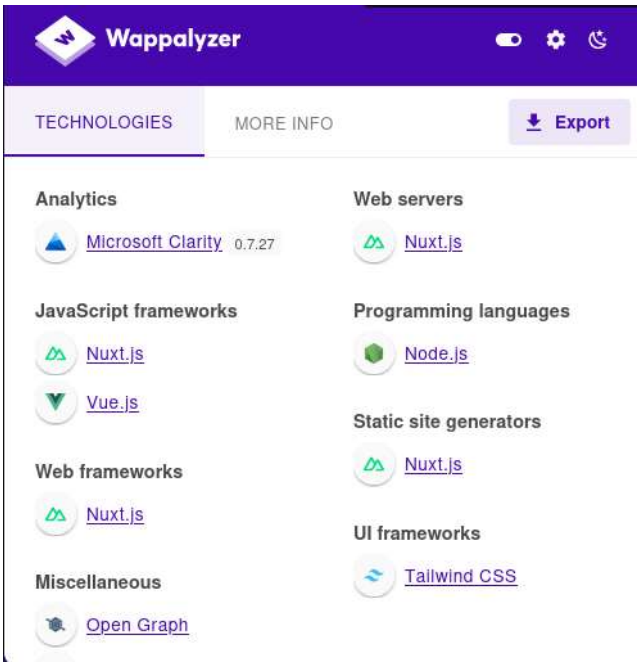
Date – 22/03/2024

- Continued searching for new scanning tools.

Manual scanning using Wapplyzer

- What is wapplyzer?

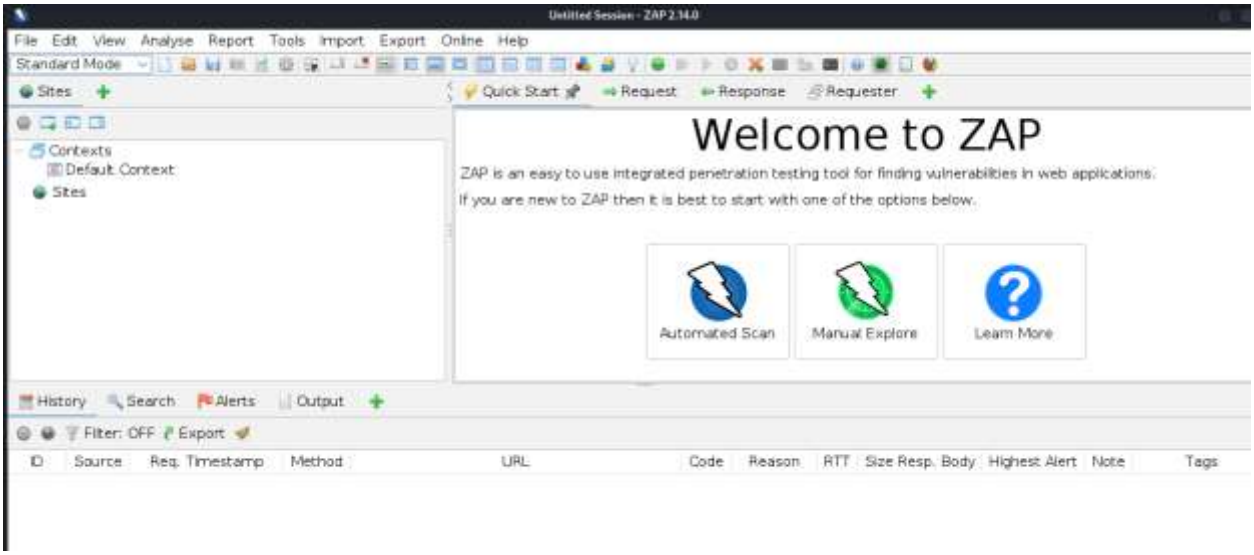
  Wapplyzer can be added to the browser as an extension and with the use of that tool we can view the technologies used inside the websites and the versions of the relevant scripts used.



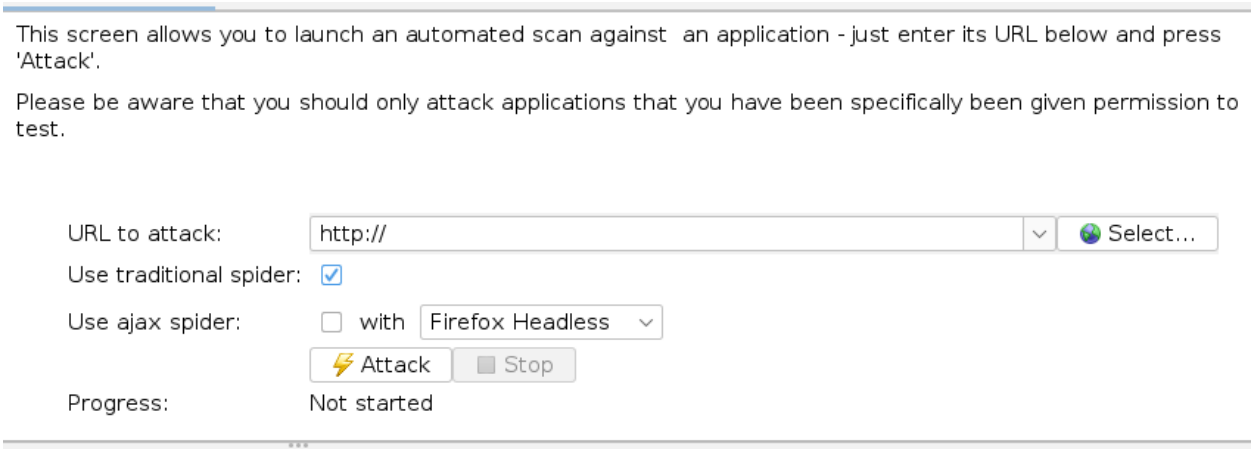
Zap scanner.

- What is zap scanner?

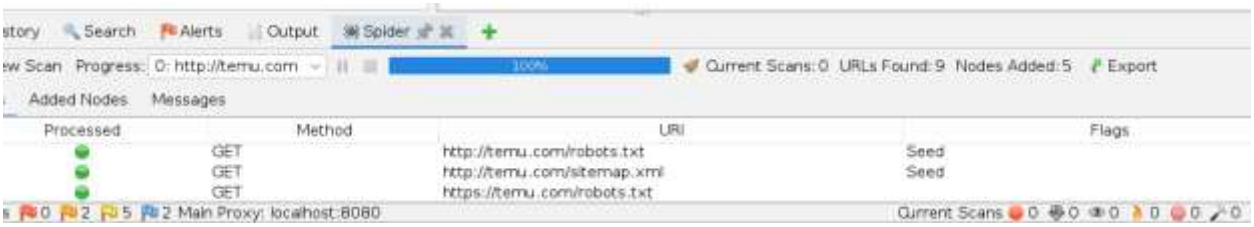
  Zap scan is a tool that can be used to identify the vulnerabilities inside a web application. It can be installed in kali and run to find vulnerabilities.



The type of the scan can be chosen based on the requirement of the user.



With the use of automated scan, we can scan the web application easily. Click it, give the domain name and launch the attack.



Once the attack is done, a comprehensive report will be generated, and we can get further information about the vulnerabilities.

Date – 23/03/2024

- Continued working on finding new scanners.

<u>Nikto scan</u>

- What is Nikto scan?

  Nikto is scanner that checks for dangerous files, programs and outdated versions of the web applications.

```
┌──(kali㉿kali)-[~]
└─$ nikto -h https://canva.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          104.16.102.112
+ Target Hostname:    canva.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=canva.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services LLC/CN=GTS CA 1P5
+ Message:           Multiple IP addresses found: 104.16.102.112, 104.16.103.112
+ Start Time:         2024-04-22 04:59:12 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
+ Uncommon header 'nel' found, with contents: {"success_fraction":0.01,"report_to":"cf-nel","max_age":60
+ Uncommon header 'report-to' found, with contents: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com
BuAzqx4%2F3Rot%2B61zbkAo43s68J1ANJK4UxTCUYLFIkGTsUZWAVCZRg%2BWztftKF%2F90I2YpsDYl%2Fw%3D%3D"}],"group":"
+ The site uses SSL and Expect-CT header is not present.
+ Root page / redirects to: https://www.canva.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
-C
-C all
- STATUS: Completed 5630 requests (~82% complete, 1.2 hours left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 135.40550 sec, 10 requests: 148.7700 sec.
+ 7786 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2024-04-22 10:40:37 (GMT-4) (20485 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

It will list down missing headers, other vulnerabilities and whether they have a WAF protecting their resources.

Nikto scans can usually take a lot of time to finish.

Gobuster

- What is gobuster?

  Gobuster is a brute force tool. It searches for DNS subdomains, hidden files and directories, virtual host names on web servers.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u https://www.truecaller.com -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://www.truecaller.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
```

Directory enumeration will be started automatically.

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/a                    (Status: 301) [Size: 123] [--> https://play.google.com/store/apps/details?id-
/about                (Status: 200) [Size: 171143]
/About                (Status: 200) [Size: 192417]
/Blog                 (Status: 200) [Size: 334387]
/blog                 (Status: 200) [Size: 334413]
/careers              (Status: 200) [Size: 156012]
/contact              (Status: 301) [Size: 70] [--> https://corporate.truecaller.com/newsroom/media
/cookies              (Status: 301) [Size: 29] [--> /cookie-policy]
/directory            (Status: 200) [Size: 137880]
/download             (Status: 200) [Size: 177165]
/Download             (Status: 200) [Size: 197989]
/es                   (Status: 301) [Size: 21] [--> /es-la]
/features             (Status: 200) [Size: 199879]
/id                   (Status: 301) [Size: 21] [--> /id-id]
/i                    (Status: 301) [Size: 94] [--> https://itunes.apple.com/app/apple-store/id4481
```

Date – 24/03/3024

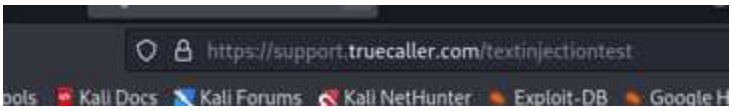
- Started researching on manual scanning methodologies.

<u>Text injection testing</u>

- What is text injection?

  An arbitrary string value is appended to the URL to see whether the web application is vulnerable towards a text injection.

Append a random string value to the latter part of the URL.



Hit enter.

If the entered text is reflected on the error response of the web page, there is a possibility to inject malicious content.

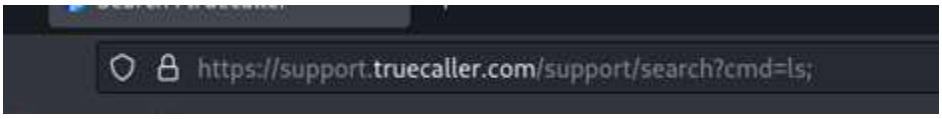
If not, the web application is safe.

Command injection testing

- What is command injection?

  It injects arbitrary commands on a host operating system with the use of an application.

Go to the search query and append a command (i/e ls - it will list down all the directories) and hit enter.



If the web application is vulnerable to command injection, the directories will be displayed (because we used “ls” command) on the screen.

If it displays “no results found”, then it can be concluded that there is no command injection vulnerability existing in the web application.

Date – 25/03/2024

Recon-ng

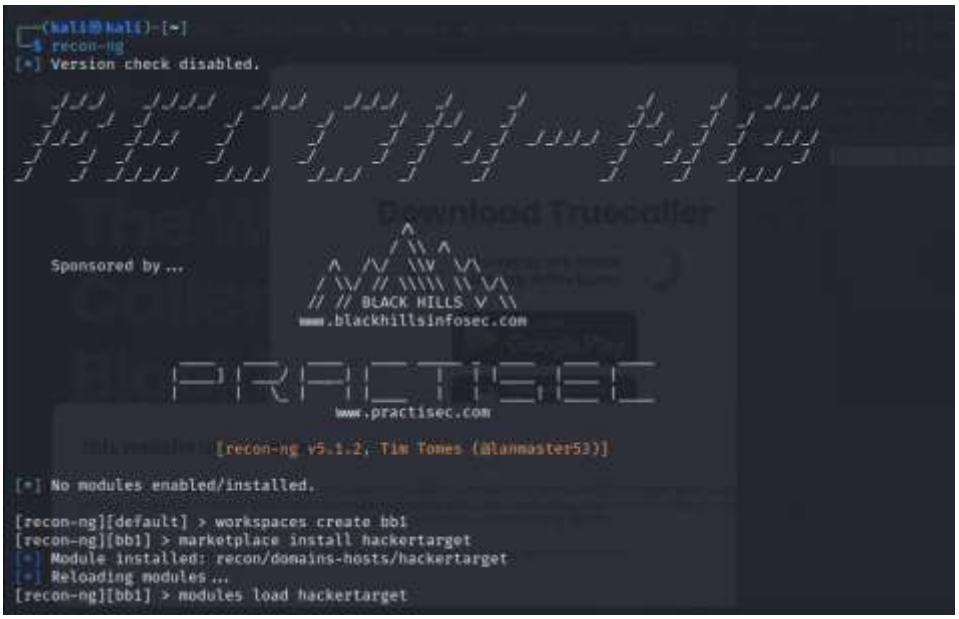
- What is Recon-ng?

  It's a tool used to gather information about and assess the vulnerabilities in the target and it finds information about the following:

- Geo-IP lookup
- Banner grabbing
- DNS lookup
- port scanning
- sub-domain information
- reverse IP using WHOIS lookup

In order to perform this type "Recon-ng" inside the terminal.

Once it initializes, it displays an interface like this.



If the required modules are missing, it will display a message asking to install the module.

```
[*] No modules enabled/installed.
```

Install the relevant modules using the command “marketplace install hackertarget”

```
[recon-ng][bb1] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
```

Once the installation is done, start creating a workspace(technically a folder) using the command “workspaces create <workspace name>”

```
[recon-ng][default] > workspaces create bb1
```

Now the modules should be loade in order to perform the scan. Here I used a module called “hackertarget”.

```
[recon-ng][bb1] > modules load hackertarget
[recon-ng][bb1][hackertarget] > show options
Shows various framework items
```

. .

To test the target the following command should be used, and the domain name should be added to the command.

```
[recon-ng][bb1][hackertarget] > options set SOURCE truecaller.com
SOURCE ⇒ truecaller.com
[recon-ng][bb1][hackertarget] > run
```

XSS injection testing

- What is Cross site scripting?

  Injecting malicious scripts into a code of a trusted application.

  Example: an attacker can host a XSS attack through trojan horse program with the intension of stealing sensitive information by changing the resources in the application.

Locate to the search function of the web application and append the following payload to the URL.

If a notification is shown there is a possibility to launch a XSS attack.

If not, the web application is not vulnerable.

Date – 26/03/2024

- Did another research on 2 other scanning tools.

<u>Metasploit</u>

- What is Metasploit?

  Metasploit is a penetration testing framework that enables security professionals to find and exploit computer system vulnerabilities.

Type “msfconsole” and start the scanner.

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

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search
Metasploit Documentation: https://docs.metasploit.com/
```

Once after it’s done search for the relevant service (i/e I have used smtp service)

```
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 File W
   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 Info and
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
```

From that use the module that requires for the scan. (I have used the module fuzzer)

Module fuzzer – it's used to fuzz the smtp service.

Smtp_enum – used for username enumeration.

After that use that scanner to continue the process.

```
Interact with a module by name or index. For example info 35, use 3

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
```

```
Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                  Required  Description
   ----       ---------------                                  --------  -----------
   RHOSTS                                                      yes       The target host(s), see https://github.com/
                                                                         it
   RPORT      25                                               yes       The target port (TCP)
   THREADS    1                                                yes       The number of concurrent threads (max one p
   UNIXONLY   true                                             yes       Skip Microsoft bannered servers when testin
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/un  yes       The file that contains a list of probable u
              ix_users.txt

View the full module info with the info, or info -d command.
```

Set the RHOSTS to the domain name. (or you can use the ip address too)

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 65.2.43.23
RHOSTS => 65.2.43.23
msf6 auxiliary(scanner/smtp/smtp_enum) > RUN
[-] Unknown command: RUN
msf6 auxiliary(scanner/smtp/smtp_enum) > run
```

The scan results will be there once after the "run" command is given.

CSRF scanning.

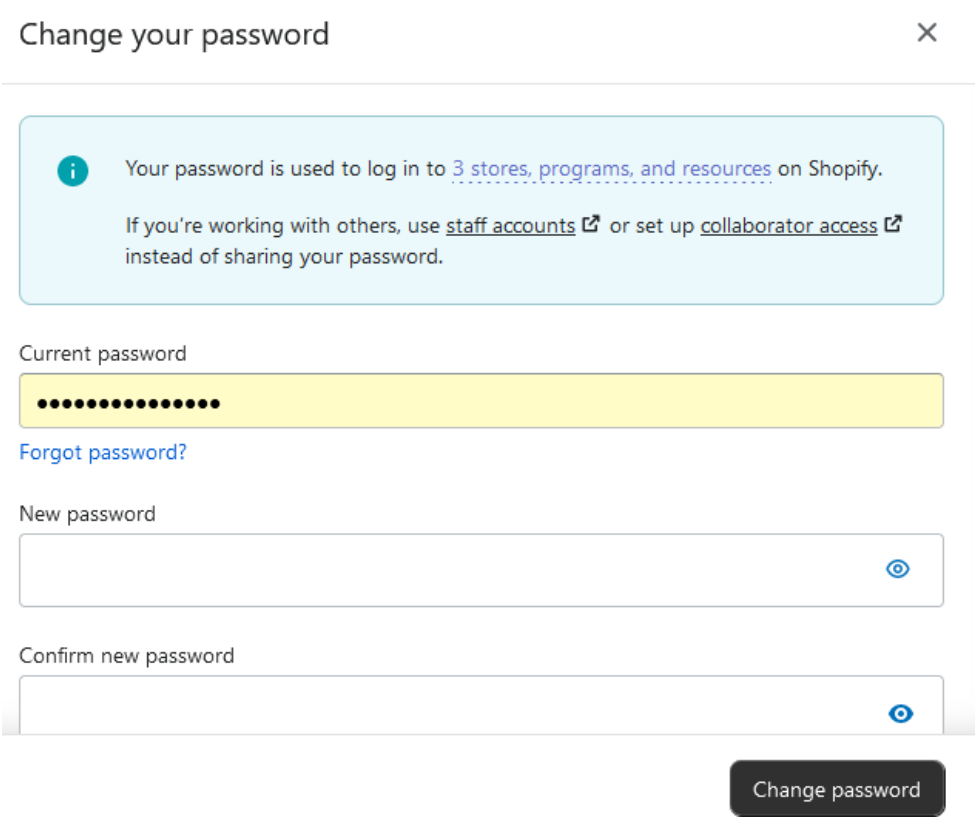
- What is CSRF?

  Attacker may cause the user to do an action on the page that the user doesn't intend.The attacker can forge a specially crafted request that would allow the attacker to make the user do a specific action such as change password to one that the attacker has set,once the user executes the attackers request on the users device(typically by sending a link to the attackers website which sends the request as soon as it is opened)

Therefore with the use of burpsuite, we are checking whether the web applications is vulnerable towards CSRF attacks.

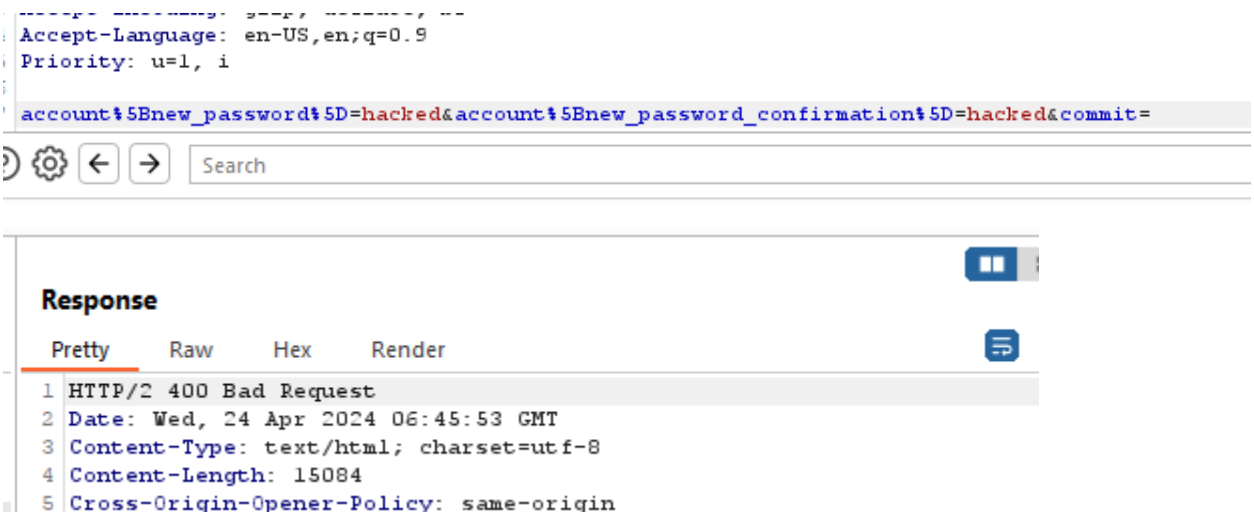
Here in this example Im testing the CSRF attack against the password change facility.

- locate to the password change page. Enter a random password to the current password and a value to the new one.



- with the help of burp capture that request which goes when the change button button is clicked. After that send it to the repeater.

- check whether the old password is being checked by the server by removing the old password.



- so here the old password is needed and being checked, so csrf on change password is not possible.
- If the old password is not checked, we can send this modified request and it would trigger a password change. The prescience of anti csrf tokens can be used to stop this even if the old password is not verified.

Date 27/03/2024

- developed a methodology for the reports.

Automated scans and reconnaissance scans	
Nikto scan	Scans web application vulnerabilities
Nmap scan	Shows all open ports
Wafw00f scan	Detects the WAF used
Zap scan	Scans for web application vulnerabilities
Gobuster scan	Sub domain enumeration
Recon-ng	Finding sub domains
Dotdotpwn	Scanning for all sub domains
Automated scans	
wapplyzer	Shows the technologies used in the web application
Text injection	
Command injection	Scanning for any command injection vulnerabilities
XSS injection	Scanning for any XSS injection vulnerabilities
File upload vulnerability	Tests whether the php files/scripts can be uploaded and executed on the server
CSRF testing	Testing to see if CSRF is possible

Date 28/03/2024

- started bug bounty hunting on the first domain.

PLATFORM	DOMAIN
HACKERONE.COM	Truecaller.com

Scans performed:

Recon-ng scan

Nmap scan

Metasploit testing

Nslookup

Wafw00f scan

Gobuster scan

Wapplyzer scan

Zap scan

Dotdotpwn scan

Sqlmap scan

Text injection testing

XSS injection testing

Command injection testing

Summary of the vulnerabilities found:

•The anti-CSRF tokens are absent.

•One hidden file found.

•Cloud meta data are potentially exposed.

•Content security policy (CSP) header not set.

Apart from them no major vulnerabilities found.

Day 29/03/2024

- started bug bounty hunting on the second domain.

PLATFORM	DOMAIN
BUGCROWD.COM	canva.com

Scans performed:

nmap scan

recon-ng

wafw00f scan

dotdotpwn scan

nikto scan

sqlmap scan

wapplyzer scan

text injection testing

file upload vulnerability scan

command and XSS injection testing.

Summary of the vulnerabilities found:

- The anti-clickjacking "X-Frame-Options" header, which helps prevent clickjacking attacks, is not present.
- The "X-XSS-Protection" header is not defined, which can protect against some forms of XSS.
- 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.
  - when the “expect-CT” header is absent:
  - The protection against the mis issuing of SSL certificates will be low.
  - Mismanagement of SSL certificates and no trust and security/

Date 30/03/2024

- started bug bounty hunting on the third domain.

PLATFORM	DOMAIN
HACKERONE.COM	grammarly.com

Scans performed:

Nmap scan

Nslookup

Wafw00f scan

Recon-ng

Dotdotpwn scan

Wapplyzer

Zap scan

File upload vulnerability testing

Text injection

Command injection

XSS Iinjection

Summary of the vulnerabilities found:

- Cloud metadata potentially exposed
- Hidden file found - .hg
- CSP allow wildcard sources in following directives: style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, form-action
- The web application is leaking information via the server" HTTP response header.
- There is no HttpOly flag - high possibility of xss attacks and session highjacking.
- There is an absence of "Samesite" attribute -might be vulnerable to XSS injection and CSRF attacks

Apart from that no major vulnerabilities found.

Date 31/03/2024

- started bug bounty hunting on the fourth domain.

PLATFORM	DOMAIN
HACKERONE.COM	shopify.com

Scans performed:

Nmap scan

Nslookup

Wafw00f scan

Recon-ng scan

Dotdotpwn scan

CSRF testing

Sqlmap scan

Wapplyzer

Nikto scan

Zap scan

File upload vulnerability testing

Text injection testing

Command injection

Xss injection testing

Summary of the vulnerabilities found:

•The anti-clickjacking X-Frame-Options header which is used for preventing clickjacking is not found.

•The X-XXS-Protection header that is useful in preventing some forms of XSS attacks is not found.

•This site uses SSL and Expect-CT header is not found.

- 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.

- Content security policy (CSP) header is not found. Due to the absence of this header, there can be XSS injections, data injections and clickjacking.

- There is an application error disclosure where the sensitive information could be exposed with a simple error/warning message.

- The Anti-clickjacking header which is used to prevent XSS attacks and enhance security posture is not present.

- There is an intentional disclosure of sensitive time stamp information where it could possibly lead to user tracking, session prediction, reconnaissance attacks, and temporal correlation attacks.

- Hidden file found.

- Informational disclosure-debug message error -inside the server response there is a message(error) that contains sensitive information about server.

Apart from that no major vulnerabilities found.

Date 01/04/2024

- started bug bounty hunting on the fifth domain.

PLATFORM	DOMAIN
BUGCROWD.COM	temu.com

Scans performed:

Nmap scan

Nslookup

metasploit

Wafw00f scan

Dotdotpwn scan

Nikto scan

Sqlmap scan

Manual scanning using Wapplyzer

Recon-ng scan

Summary of the vulnerabilities found:

- The anti-clickjacking "X-Frame-Options" header, which helps prevent clickjacking attacks, is not present.
- The "X-XSS-Protection" header is not defined, which can protect against some forms of XSS.
- 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 site uses SSL and the Strict-transport-security HTTP header is not defined.
- The X-content-Type-options header is not set.

Apart from that no major vulnerabilities found.

Date 02/04/2024

- started bug bounty hunting on the sixth domain.

PLATFORM	DOMAIN
BUGCROWD.COM	booking.com

Scans performed:

Nmap scan

Nslookup

Metasploit

Nikto scan

Recon-ng scan

Wafw00f scan

Wapplyzer

Dotdotpwn scan

Sqlmap

Summary of the vulnerabilities found:

- 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.
  - 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.

Apart from that no major vulnerabilities found.

Date 03/04/2024

- started bug bounty hunting on the seventh domain.

PLATFORM	DOMAIN
BUGCROWD.COM	pinterest.com

Scans performed:

Nmap scan

Recon-ng

Nslookup

Wafw00f scan

Wapplyzer

Text injection testing

File upload vulnerability testing

Dotdotpwn

Command injection testing

CSRF testing

Sqlmap

XSS injection testing

Summary of the vulnerabilities found:

Day 04/04/2024

- started bug bounty hunting on the eighth domain.

PLATFORM	DOMAIN
BUGCROWD.COM	tripadvisor.com

Scans performed:

Nmap scan

metasploit

Text injection testing

Wafw00f scan

Wapplyzer

Nslookup

File upload vulnerability testing

Dotdotpwn

Command injection testing

Sqlmap

XSS injection testing

Recon-ng

Summary of the vulnerabilities found:

- no major vulnerabilities found.

Date 05/04/2024

- started bug bounty hunting on the ninth domain.

PLATFORM	DOMAIN
BUGCROWD.COM	pixabay.com

Scans performed:

Nmap scan

Recon-ng

Text injection testing

Sqlmap scan

Nslookup

Wafw00f scan

Dotdotpwn

Wapplyzer

File upload vulnerability testing

Command injection

XSS injection testing

Summary of the vulnerabilities found:

- The jquery 1.12.4 used is vulnerable.
  - In order to mitigate the risk, update the jquery scripts to 1.12.0, 3.0.0-beta1 or higher.

No other major vulnerabilities found.

Date 06/04/2024

- started bug bounty hunting on the tenth domain.

PLATFORM	DOMAIN
BUGCROWD.COM	soundcloud.com

Scans performed:

Nmap scan

Nikto scan

Wafw00f scan

Nslookup

Dotdotpwn scan

Metasploit scan

Wapplyzer

File upload vulnerability testing

Sqlmap scan

Recon-ng scan

Text injection testing

Command injection testing

Zap scan

Summary of the vulnerabilities found:

•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.
- 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.

•PII disclosure: PII data can be used to identify an individual therefore maintaining the data securely can mitigate risks.

•Content security policy (CSP) header not set:it works an an extra layer of security which should be set and configured correctly.

•Strict-transport-security header not set.

•Server leaks version information via “server” HTTP response header field- with the use of leaked data the attackers can exploit the vulnerable parts of the server.

•Application error disclosure: the warning messages disclose sensitive information which can be used to launch attacks by the attackers. A mechanism can be introduced which reference the errors so it can solve this issue.

•Cross-domain javascript source file inclusion – it’s a warning. Happened when the external javascript is not validated.

•X-Content-Type-Option header is not set- allows to perform MIME-sniffing on the response body of old versions of chrome.

•Time stamp disclosure: the timestamp of a request will be revealed.