

Command Injection Exploitation Using Commix

What is command injection: -

In terms of cyber security, command injection is also referred as shell injection and operating system injection.

Command injection lies in the OWASP top 10 every year.

Command injection is a hacking technique in which hackers execute commands in the host operating system through vulnerable web applications after scanning. This attack can be possible if a web application is sending user data to its system shell through some connectivity. This user data can be of any type which can be HTTP headers or cookies or forms etc. The history of command injection is very interesting because command injection was accidentally discovered by a programmer in Norway in mid-1997. The command injection vulnerability gave rise to another new type of command injection which is SQL command injection.

What is Commix: -

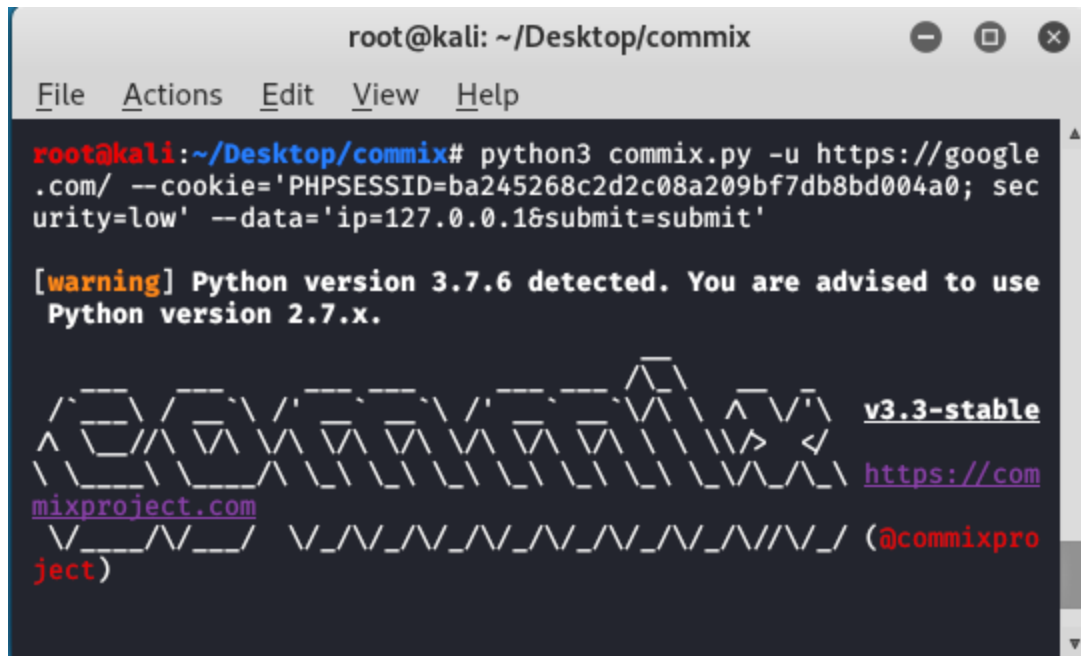
Commix is a free and open-source tool available on GitHub. This tool is a powerful tool used for exploiting command injection vulnerabilities in websites and web applications.

Command injection is a vulnerability that usually occurred in web applications. In terms of cyber security, command injection is also called shell injection. Commix is written in python language. You must have python installed on your kali Linux operating system. The interactive console is very similar to metasploitable 1 and metasploitable which makes it easy to use. This tool works as a tester of a command injection vulnerability in websites and web applications.

Commix tool comes with different modules installed within it which lets its user find out vulnerability in the target application. Commix attack on target URL using data strings or HTTP header or cookies also on authentication parameters. In commix, users can find different enumeration options. By using commix user can perform two types of command injection. The first is the result-based command injection technique and the second is the blind command injection technique.

Example: -

1. To find out if the domain has command injection vulnerability or not.



```
root@kali: ~/Desktop/commix
File Actions Edit View Help
root@kali:~/Desktop/commix# python3 commix.py -u https://google.com/ --cookie='PHPSESSID=ba245268c2d2c08a209bf7db8bd004a0; security=low' --data='ip=127.0.0.1&submit=submit'

[warning] Python version 3.7.6 detected. You are advised to use Python version 2.7.x.

  ^__^
  (oo)\_______
  (__)\       )\/\
     ||----w )
     ||     ||

  v3.3-stable
  https://commixproject.com
  (@commixproject)
```

2. To find out if the domain has command injection vulnerability or not using batch flag.

```
root@kali: ~/Desktop/commix
File Actions Edit View Help
+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2021 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[info] Resolving hostname 'dvwa.co.uk'.
[info] Testing connection to the target URL.
[info] Performing identification checks to the target URL.
[info] Setting the unix-based payloads.
```

3. To find out if the domain has command injection vulnerability or not using `-all` flag.

```
root@kali: ~/Desktop/commix
File Actions Edit View Help
+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2021 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[info] Resolving hostname 'testphp.vulnweb.com'.
[info] Testing connection to the target URL.
[info] Performing identification checks to the target URL.
```