Safe Shell function Programming

Shell function Programming adalah sebuah fungsi atau API yang telah dibuat oleh berbagai macam bahasa pemrogramman. Tujuannya adalah agar dapat berinteraksi dengan Mesin (OS) secara lancar untuk berbagai kebutuhan. Namun penggunaan yang tidak aman dapat membahayahkan Mesin (OS) itu sendiri, karena bahasa pemrogramman dapat mengkontrol penuh Mesin meskipun dengan privileges yang sedang berjalan dari programming itu sendiri.

Escaping shell input

Dalam mengamankan sebuah shell function programming adalah dengan tidak memasukan RAW input user ke dalam sebuah shell function. Cara sederhananya adalah dapat melakukan replacing ataupun escaping terhadap RAW input. seperti berikut.

Replacing

```
<?php
    $input = "";
    system($input);
?>
```

Dalam fungsi di atas, `system` langsung menerima input dari user, kita dapat melakukan replacing ke shell next operationpada mesin seperti berikut ini contoh dari shell next operation.

1. `;`
2. `|`
3. `&&`
4. `\n`
5. `&`
6. `
7. `$()`
8. `--`

Dari 8 operator di atas, kita harus memastikan hal tersebut tidak ada dalam input shell function. Kita dapat melakukan pencarian atau membatalkan hal tersebut dengan cara.

```
<?php
    $input = "ls -la; id";
    $re = '/(;|\|\||\&\&|\&|\\\\n|\$(.*)|\`.*\`)/m';
    $sanitized = preg_replace($re, '',  $input);
?>
```

Kode di atas akan menggantikan `next operation shell` dengan string kosong, untuk membuat lebih tricky lagi, dapat mengantinya dengan string random seperti berikut ini.

```php
<?php
    $input = "ls -la; id";
    $re = '/(;|\|\||\&\&|\&|\\\\n|\$(.*)|\`.*\`)/m';
    $sanitized = preg_replace($re, str_repeat("A", rand(2,10)),  $input);
?>
```

Escaping

Ada cara lain untuk mengamankan Shell Function input dengan cara berikut ini, yaitu dengan mengescape string2 yang diluar range [aA-zZ].

```php
<?php
$input = "/tmp/";
system('ls '.escapeshellarg($input));
?>
```

Atau seperti berikut ini.

```php
<?php
$input = './binary'.$_GET[0];
$escaped_command = escapeshellcmd($command);
system($escaped_command);
?>
```