Remote Code Execution By Dédalo

El Remote Code Execution es una vulnerabilidad de muy alto peligro ya que con este se ejecutan comandos del servidor de una manera remota...
Este bug es por un error del mal uso de la función System() o exec() en PHP.

Ahora les maestro un ejemplo con la función System()

```
<?php
$varerror = system('cat '.$_GET['pageid'], $valoretorno);
echo $varerror;
?>
```

En un Servidor linux el bug se podría explotar fácilmente de la siguiente manera...

Usando el Method GET que podríamos usar con el live http headers:

```
GET /vulnerable.php?pageid=loquesea;ls HTTP/1.1

Host: Localhost
```

Como resultado se ejecutaría el comando ls lo que quiere decir que mostraría los directorios quitándole discreción a su host y servidor sin mencionar que no solo se puede usar ls sino otros comandos linux.

¿A qué se debe este Bug?

Al igual que cuando algunos programan en php y por vagancia usan el * en ves
De una columna pues así pasa aquí en vez de usar archivos concretos usan ciertos comandos del servidor para facilitarse la tarea.

¿Corregirlo?

Existen múltiples formas de evadir esta Vulnerabilidad, una de ellas puede ser a través de la función escapeshellcmd() usándola de una manera correcta:

```
escapeshellcmd  (String $comando)
```

Lo que haría sería filtrar lo siguientes caracteres para que no afecten ningún tipo
De petición:

& ; ` | * ? ~ < > ^ ( ) [ ] { } $ \ , \x0A y \xFF.

Así como usamos la función escapeshellcmd() podemos hace nuestro propio
Filtrado de caracteres puede ser con str_replace y un arreglo o ya según su
Imaginación pueden hacer algunos otros.

Espero que les haya Gustado este paper...

[Milw0rm 2009]
[http://milw0rm.com]

[By Dédalo]
[http://seguridadblanca.blogspot.com]

Greets: Jbyte, Perverths0, D4rkD3m0n, Dr.N30x, Str0ke, Vit0y4 Y BackTracker