

XSSer

The Cross Site Scripting
Framework
(ES)



/ Cross Site “Scripter” /

- Última versión: [XSSer v1.6 “Grey Swarm”](#)

- Web del proyecto: <http://xsser.sf.net>

-¿Qué es XSSer?

-¿De dónde viene?

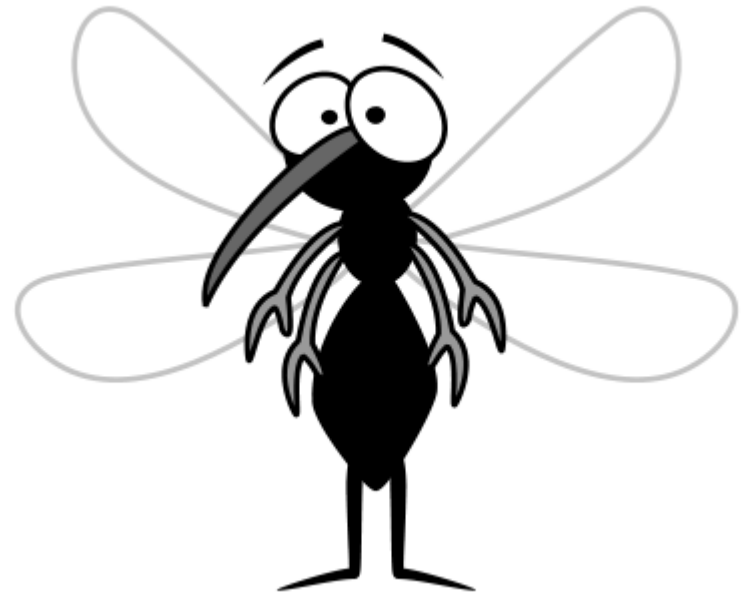
-¿Quién puede usarlo?

-¿Cómo funciona?

-¿Dónde encontrarlo?

-¿Cuál es su futuro?

-¿Cómo puedo colaborar?





/¿Qué es XSSer?/

- Definición de Wikipedia: [Cross Site Scripting \(XSS\)](#)

- "Top 10" riesgos en aplicaciones: [OWASP 2010](#)

Cross Site "Scripter" (aka XSSer) es un framework que permite:

- Detectar fallos de tipo XSS en aplicaciones web.
- Explotar código de forma local/remota "on the wild".
- Reportar las vulnerabilidades encontradas en *tiempo real*.



- Los fallos de tipo XSS ocurren cuando una aplicación utiliza datos que no son de confianza y los envía al navegador web sin una verificación o escapado previos.
- Los ataques XSS permiten a los atacantes ejecutar código script en los navegadores de las víctimas con el objetivos de; robar la sesión de usuario, realizar un deface, llevar a cabo un ddos, redireccionar los flujos de navegación a lugares maliciosos bajo su control, etc...

OWASP: *Open Web Application Security Project*: [Top 10 2010-A2-Cross-Site Scripting \(XSS\)](#)



/¿Qué es XSSer?/

- Licencia de XSSer: [GPLv3](#)

- Fecha de comienzo: [15 Marzo de 2010](#)

Opciones destacadas:

- Interfaz GTK
- Imágenes y películas flash con XSS
- Dorking
- Soporte: GET/POST
- Crawling
- Proxy

- Heurística
 - Chequeo inverso
 - 98 vectores (+HTML5)
 - Exploits pre-configurados
 - Exportar a-XML
 - Tweets (“Grey Swarm”
[...])
 - [Ver todas las opciones](#)
-

Tipos de inyecciones permitidas:

- Normal XSS (Persistente-Reflejado)
- Cookie Injections
- Cross Site “Agent” Scripting
- Cross Site “Referer” Scripting
- Inyecciones en el “Data Control Protocol”
- Inyecciones en el “Document Object Model”
- HTTP Response Splitting Induced

Tipos de “bypassers”:

- Método: String.fromCharCode()
- Función: Unescape()
- Encodeo: Decimal
- Encodeo: Hexadecimal
- Encodeo: Hexadecimal, con punto y coma
- Encodeo de Ips: DWORD, Octal
- “Character Encoding Mutations” (Combinaciones)



/¿De dónde viene?/

- PDF “XSS for fun and profit”: [EN](#) / [SP](#)

- Primer patrocinador: [Fundación NLNet](#)

Tutorial – SCG'09 : “XSS for fun and profit”



PDF Completo (174 páginas) sobre XSS con ejemplos detallados:

- Tipos de ataques
- Formas de evasión de filtros
- Ejemplos en escenarios reales
- Técnicas de ataque
- Trucos para XSS y vectores Fuzzing
- Herramientas / Enlaces / Bibliografía
- [...]

Fundación NLNet:



Premios NLNet: “[XSSer Ganador en Abril de 2010](#)”

- Comienzo: 01/07/2010 – Final: 01/02/2011
- 5 milestones (pasos)
- El proyecto XSSer recibe: 3.000 €



/¿Quién puede usarlo?/

- Security Tools Benchmarking: [XSSer “Best HTTP GET XSS”](#)

- XSSer es una de las: [Herramientas de Anonymous](#)

Profesionales de la seguridad / Pentesters:

- Contiene las técnicas necesarias para realizar un test de “hacking ético” completo
- Permite obtener estadísticas avanzadas en los resultados
- Automatiza buena parte de los procesos de inyección
- Permite exportar los resultados para la realización de informes
- Es sencillo proponer/implementar nuevas funcionalidades
- [...]

Comparación de 43 escáneres de vulnerabilidades web (25-01-2011):

“The best HTTP GET XSS detection ratio (while considering the low amount of false positives) of open source tools belongs to XSSer.”

Amateurs / Hacktivistas:

- Contiene un “Wizard Helper”, que permite generar ataques respondiendo a preguntas
- Tiene muchos ejemplos y documentación adjunta
- Permite conocer los resultados de otros “pentesters” *en tiempo real*
- La versión GUI, tiene un mapa para georeferenciar los ataques y hacer esquemas
- [...]

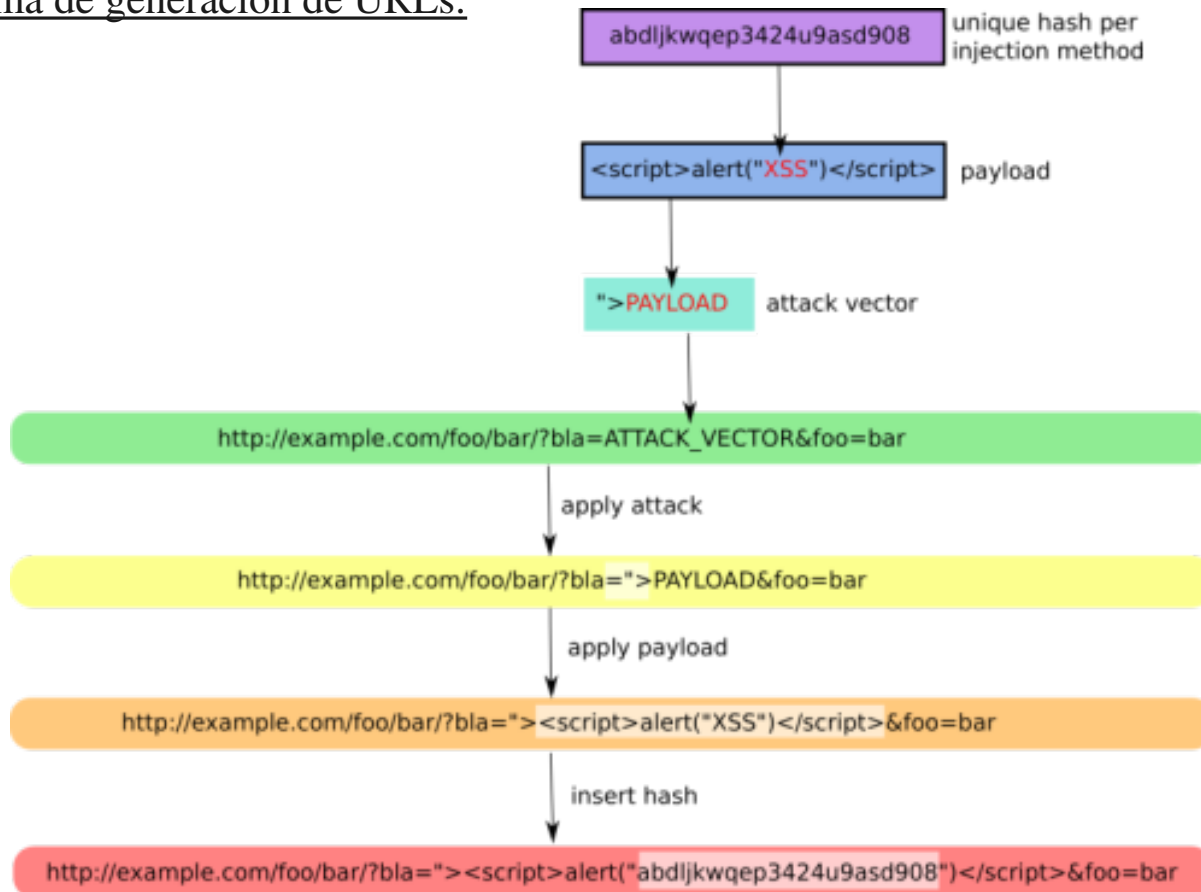


/¿Cómo funciona?/

- Videos de versiones antiguas de XSSer:

Simple automatic payloading vectors
Server side Apache logging
Dorking injections

Esquema de generación de URLs:





/¿Cómo funciona? /

\$ man xsser

Desde Shell:

```
$ python xsser [OPTIONS] [-u l-i l-d ] [-g l-p l-c ] [Request(s)] [Vector(s)]  
[Bypasser(s)] [Technique(s)] [Final Injection(s)]
```

- Listado de comandos disponibles: \$ python xsser -h / --help ()

** Inyección simple desde URL:*

```
$ python xsser.py -u "http://host.com"
```

** Múltiples inyecciones desde URL, utilizando “payloads” automáticos,
con un proxy TOR, aplicando un “encodeo” de tipo Hexadecimal,
en modo “verbose” y salvando los resultados en un fichero (XSSlist.dat):*

```
$ python xsser.py -u "http://host.com" --proxy "http://127.0.0.1:8118" --auto --Hex --verbose -w
```

- Más ejemplos: <http://xsser.sourceforge.net/#examples>



/¿Cómo funciona?/

- Video de versión 1.5b de XSSer:

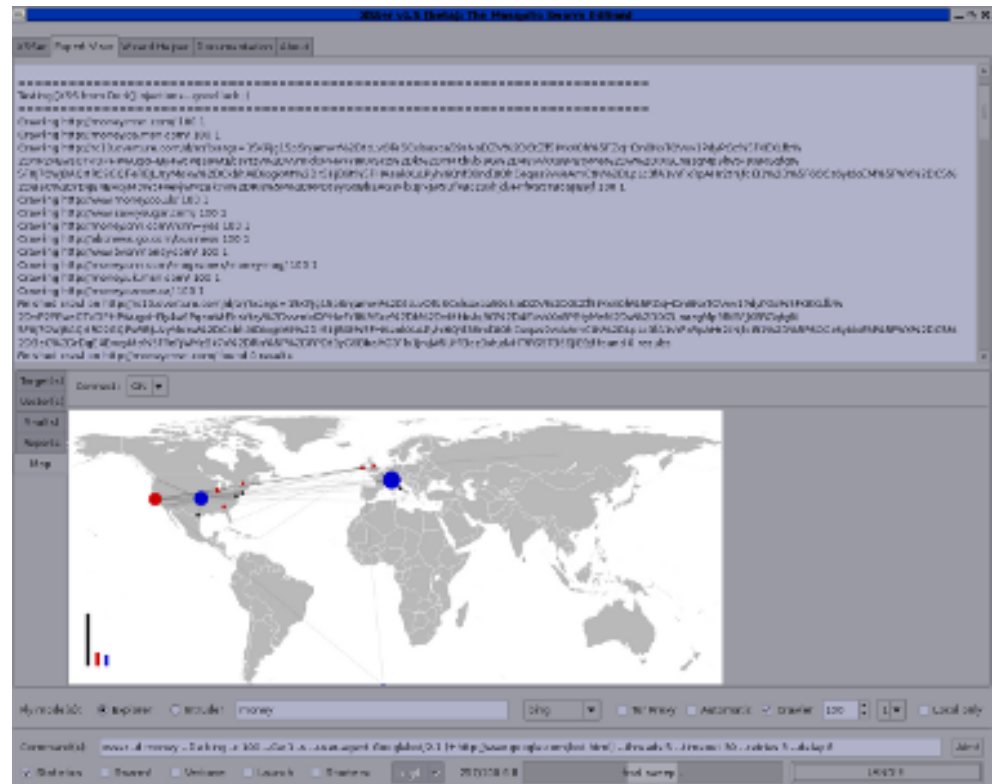
Swarm Edition!: <http://xsser.blip.tv>

Desde Interfaz:

`$ python xsser --gtk (--silent)`

- Navegación intuitiva
- Autocompletador de comandos
- Ayudante
- Visor Experto
- Geolocalización de víctimas
- Documentación
- [...]

“Vuela tus mosquitos rápido...”





/¿Cómo funciona?/

Todos los comandos de XSSer: `$ xsser -h / --help`

Detectar Vulnerabilidades:

- Inyección de XSS “clásico”: `$ python xsser -u/-i/-d "host.com" → "<><script>XSS</script>"`
- Inyección de XSS automático: `$ python xsser -u/-i/-d --auto "host.com" → 98 vectores`
- Inyección de XSS personalizado: `$ python xsser -u/-i/-d "host.com" --payload ">alert('XSS')..."`
- Explotación de XSS remoto: `$ python xsser -u/-i/-d "host.com" --Fr = "<script>alert('XSS')..."`
`(<script src="" + Fr parameters + ""></script>)"`
- Explotación masiva mediante dorking:

`$ python xsser -d "'inurl:fcgi-bin/echo'" --De "google" --Fp = "<script>alert('XSS')..."`



/¿Dónde encontrarlo?/

- Descargar XSSer: [v1.6b "Grey Swarm"](#)

- Última versión: [Estadísticas en SF](#)

Sources:

- Todas las versiones: <http://sourceforge.net/projects/xsser/files/>

Subversión:

- Repositorio: `$ svn co https://xsser.svn.sourceforge.net/svnroot/xsser xsser`

Paquetes pre-compilados:

- Ubuntu / Debian: [XSSer-1.6_all.deb](#)

Instalación (GNU/Linux):

```
tar xzvf xsser-1.6_all.deb.tar.gz
```

```
sudo dpkg -i xsser-1.6_all.deb
```

- ArchLinux: [AUR link \(v1.6b\)](#)
- Gentoo: [XSSer Gentoo ebuild \(v1.6b\)](#)
- RPM: [XSSer-1.6-1.noarch.rpm](#)





/¿Cuál es su futuro? /

- Todo tipo de ayuda es bienvenida :-)

Tareas activas:

- Testing
- Documentación
- Cerrar bugs (falsos positivos, arreglar el “swarm”, auto-update, multithreading, glibc corruption...)
- Refactorizar el código
- Comunidad
- XSSer: White Swarm (versión empresarial)+ Black Swarm (versión comunidad)
- [...]

Bajo Investigación (28-02-2012):

- Explotación AJAX
- Nuevos vectores de ataque
- XSS shell + Tunneling
- XSS “Nest” (código automático de lanzamiento de gusanos)
- XSSer social network visor
- [...]



/EXTRA !!!!!/

- BbZZZzZzZzzzZzzzzZzzzZZZZZ



 Accesibilidad

 Ayuda

 Mapa web

Matáu...
Oficina de A...
Ciudadano. Área...
Residencial Barrios de...
y Cortes



Vivienda

Madrid
que
vivienda

municip...

Semana santa 2008
Día Internacional de la Mujer
Día del 2 de Mayo

INICIO

AYUNTAMIENTO

CONTACTAR

SEDE

buscar

Está en: Inicio > Buscador Simple

Buscador Simple





/ EXTRA !!!!! /

- BbZZZzZzZzzzZzzzzZzzzzZZZZZ

Intereconomía

La Gaceta

Negocios

Punto Pelota

Blogs

Radio Intereconomía

Radio Inter

Business TV

Intereconomía TV

Club

Viajes

Acceder | ¿Olvidaste tu contraseña? | Registrarse | 28 de febrero de 2012

intereconomía



Buscar en intereconomía

BUSCAR

PORTADA BLOGS AMÉRICA DESTACADOS ARCHIVO PROGRAMAS

Servicios Suscripciones Tienda Ideario Apps



Sobre Rooted CON

Noticias

Congreso

Tienda

Colaborador

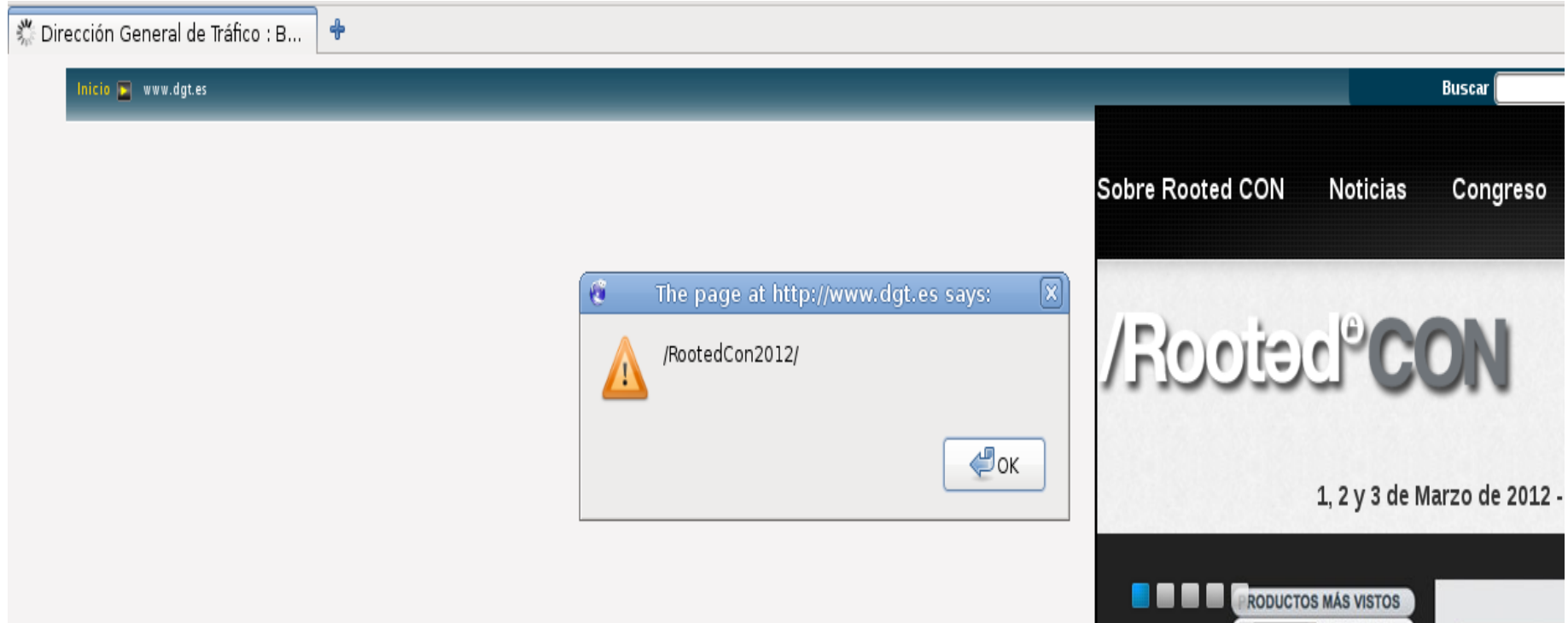
/Rooted° CON

1, 2 y 3 de Marzo de 2012 - Auditorio de la Fundación M



/ EXTRA !!!!! /

- BbZZZzZzZzzzZzzzzZzzzzZZZZZ





/EXTRA !!!!!/

- BbZZZzZzZzzzZzzzzZzzzZZZZZ



RootedCon2012

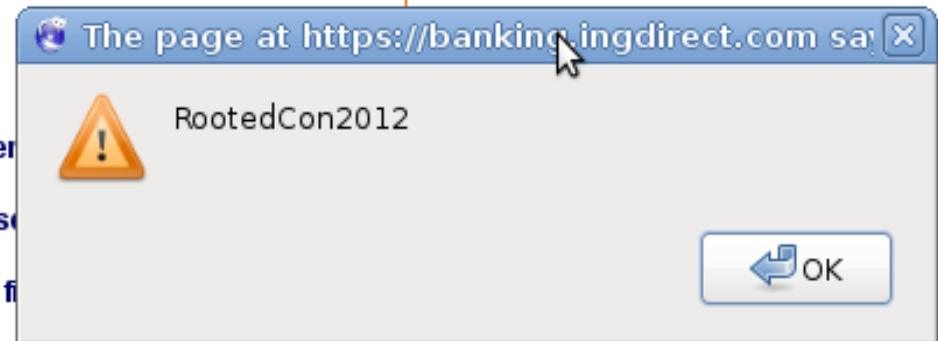


/ EXTRA !!!!! /

- BbZZZzZzZzzzZzzzzZzzzzZZZZZ



- ☒ I'm new to ING DIRECT
- ☐ I'm an existing ING DIRECT Customer
- ☐ I'm an Orange for Business Customer and want to open a per
- ☐ I'm an Orange Home Loan Applicant and want to open a pers
- ☐ I already started the account opening process and I want to f





/ EXTRA !!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

can  BANCA CÍVICA

Euskara | Català | English

Oficinas y cajeros

EMPRESAS

BANCA ELECTRÓNICA

BROKER ONLINE

TV CAN

Introduce palabra/s

Buscar

TUS DERECHOS

NUESTROS DEBERES

QUÉ NECESITAS

PARTICIPA

CONECTA EN DIRECTO

CONÓCENOS

Inicio > Asesor virtual

Bienvenido a la ayuda de Caja Navarra

Te facilitamos una serie de consejos para

Introduce aquí tu pregunta

   IMPRIMIR





/EXTRA !!!!!/

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

- **Cuenta Valores:** Para realizar sus inversiones en bolsa y en derivados
- **Tarjeta 4B Mastercard:** Para disponer de su cuenta en cajeros y comercios.
- **Servicio de Banca a Distancia:** Para operar por Internet y/o por teléfono.
- **Contrato marco de imposiciones a plazo:** Para gestionar cómodamente sus ahorros.

Continuar





/EXTRA !!!!!/

- BbZZZzZzZzzzZzzzzZzzzzZZZZZ

Forbes.com
U.S. EUROPE ASIA

Home Page for the World's Business Leaders

Free Trial Issue

Search Stock Quote

Home Business Investing Lifestyle Lists

Video ForbesWoman CEO Network Mobile

Advanced Search
Browse By Year:
All
Search Keywords:
Go

Subscribe to this RSS feed.

The page at http://search.forbes.com says:
/RootedCon2012/

No stories v

Sobre Rooted CON Noticias Congreso Tienda Colaborador

/Rooted°CON

1, 2 y 3 de Marzo de 2012 - Auditorio de la Fundación M



/EXTRA !!!!!/

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

USPTO PATENT FULL-TEXT AND IMAGE DATABASE

[Help](#)[Home](#)[Quick](#)[Advanced](#)[Pat Num](#)[Order Copy](#)[PTDLs](#)



/EXTRA !!!!!/

- BbZZZzZzZzzzZzzzzZzzzzZZZZZ



Si tienes contratados **Servicios de conectividad avanzada** (Empresas) u **Otros servicios de Fijo** (particulares) accede a nuestra **Zona** caso de que no recuerdes tu usuario y/o contraseña, puedes solicitar claves nuevas rellenando alguno de los formularios que a continuación. Una vez conozcas el nuevo usuario y/o contraseña, podrás acceder a la zona privada de clientes. En la zona privada de clientes podrás consultar factura, así como todos los servicios asociados a tus productos contratados.

¿HAS OLVIDADO TU CONTRASEÑA?

1. Rellena los campos del formulario. En caso que tengas:

* USUARIO:

* CIF/MIF/ME/PASAPORTE:

Introduce los datos sobre la última factura o los cuatro últimos

* NÚMERO DE CONTRATO:

* NÚMERO DE LA ÚLTIMA FACTURA:

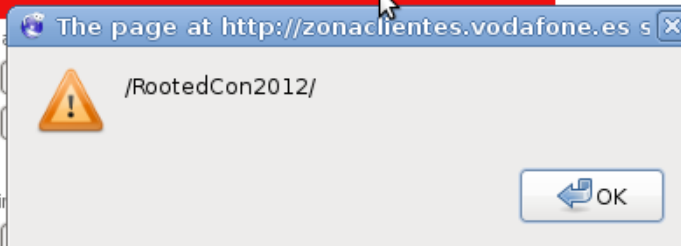
Introduzca el importe de la última factura o los últimos 4 dígitos de su cuenta corriente

IMPORTE DE LA ÚLTIMA FACTURA (CON IVA):

Céntimos separados por coma

ÚLTIMOS 4 DÍGITOS DE LA CUENTA CORRIENTE:

Continuar





/ EXTRA !!!!! /

- BbZZZzZzZzzzZzzzzZzzzzZZZZZ



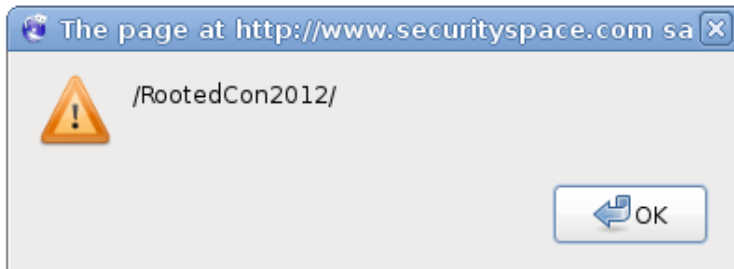
[English](#) | [Deutsch](#) | [Español](#) | [Português](#)

Home

Security
Audit

[Programas de Asociados](#) | [Testimonios](#) | [En la Prensa](#) | [Listas de Correos](#) | [Acerca Nuestro](#) | [Contáctenos](#) | [Privacidad](#) | [Abuso](#)

Contáctenos



Rooted CON

Noticias

Congreso

Tienda

Colaborador

/Rooted° CON

1, 2 y 3 de Marzo de 2012 - Auditorio de la Fundación M



/EXTRA !!!!!/

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

The screenshot shows the evidalia website interface. At the top, there is a header with a woman giving a thumbs up, the word "evidalia", a search bar with the text "Buscar", and a blue button. Below the header is a banner for "Alojamiento Web solo 2€ Registro de Dominios" featuring a child with a laptop. The main content area displays a search error: "ERROR EN LA BUSQUEDA" with a magnifying glass icon. Below the error message is a red-bordered box containing the text: "Lo sentimos, pero no se han encontrado registros que coincidan con la consulta: ">". At the bottom, there is a navigation bar with links: "Sobre Rooted CON", "Noticias", "Congreso", "Tienda", and "Colaborador". The footer features the "/Rooted[®]CON" logo and a small icon with three colored dots (blue, red, green).

evidalia Buscar

**Alojamiento Web solo 2€
Registro de Dominios**

España, Martes 28 - Febrero - 2012 Actualmente hay 181 usuarios online

ERROR EN LA BUSQUEDA

Lo sentimos, pero no se han encontrado registros que coincidan con la consulta: ">

Sobre Rooted CON Noticias Congreso Tienda Colaborador

/Rooted[®]CON



/EXTRA !!!!!/

- BbZZZzZzZzzzZzzzzZzzzzZZZZZ

The screenshot shows the NASA Space Place website interface. At the top left is the NASA logo. At the top right is the Space Place logo and a "View in English" link. Below these is a navigation bar with links: EL ESPACIO, EL SOL, LA TIERRA, SISTEMA SOLAR, PERSONAS Y TECNOLOGIA, and PADRES Y EDUCADORES. A search bar with the text "Search: "; is on the left. A central browser warning box is overlaid, stating "The page at http://spaceplace.nasa.gov says:" and "RootedCon2012" with a warning icon and an "OK" button. On the right, there are three main activity buttons: "JUGAR" (Juegos, Rompecabezas), "HACER" (Activades, Proyectos), and "EXPLORAR" (Ideas, Videos, Imágenes). At the bottom right, there is a "Download SpacePlace iPhone" button with an image of an iPhone. The background features a large moon and stars, with a "CLUBHOUSE" sign visible at the bottom.



/¿Cómo colaborar?/

IRC: [irc.freenode.net](irc://irc.freenode.net) / canal #xssec

Patrocinador:

- Donaciones (dinero, material, datos..)
- Invitaciones a eventos
- Trabajo
- Promoción de la herramienta
- Cerveza y amor :)
- [...]

Desarrollador:

- Testing
- Documentación
- Corregir bugs
- Hacking :)
- Sugerencias y nuevas funcionalidades
- [...]



Lista de correo: xsser-users@lists.sourceforge.net



- GPG Public ID Key: 0x3CAA25B3
- Email: epsylon@riseup.net

- Identi.ca: <https://identi.ca/psy>
- Twitter: https://twitter.com/lord_epsylon

The screenshot shows the homepage of the Spanish Presidency website (presidencia.es). The header features the site's logo and navigation links in Spanish, English, and Catalan. A red navigation bar contains links to Home, The Spanish Presidency, Agenda, Documents & News, The European Union, Spain in Focus, and Press. A search bar is located in the top right. On the left, a sidebar lists categories like 'The Spanish presidency', 'Agenda', and 'Documents & News', along with a 'TOP SEARCHES' section. The main content area displays a search result for 'query' with the message 'No se han encontrado Resultados !!' (No results found!!) and an error message: 'org.openmsearch.CmsSearchException: Búsqueda de "query:"'. Below the error message is a large image of Mr. Bean. To the right, there is a calendar for January 2010. At the bottom of the main content area, a small text string reads: 'fields:[meta, content] sort:[default]" fallida.'

“swarm means ... #lulz”