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?

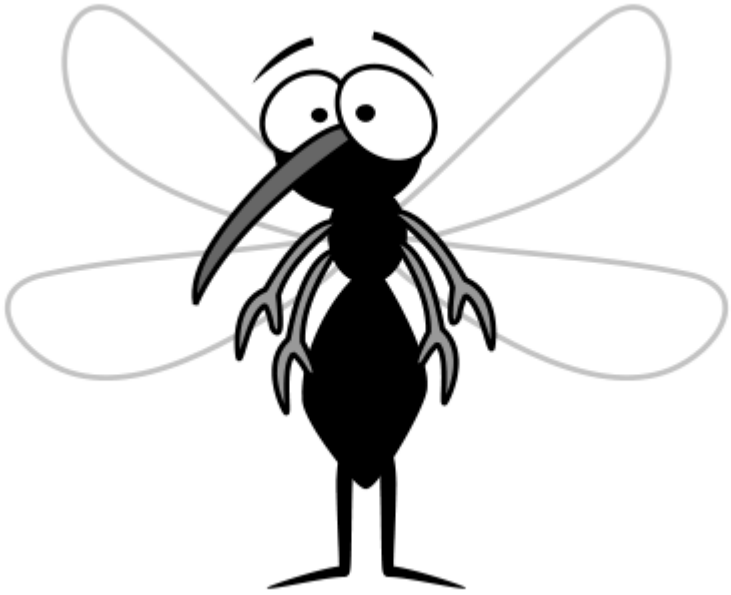
-¿Quién puede usarlo?

-¿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
- Heúristica
- 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:

nlnet FOUNDATION

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:

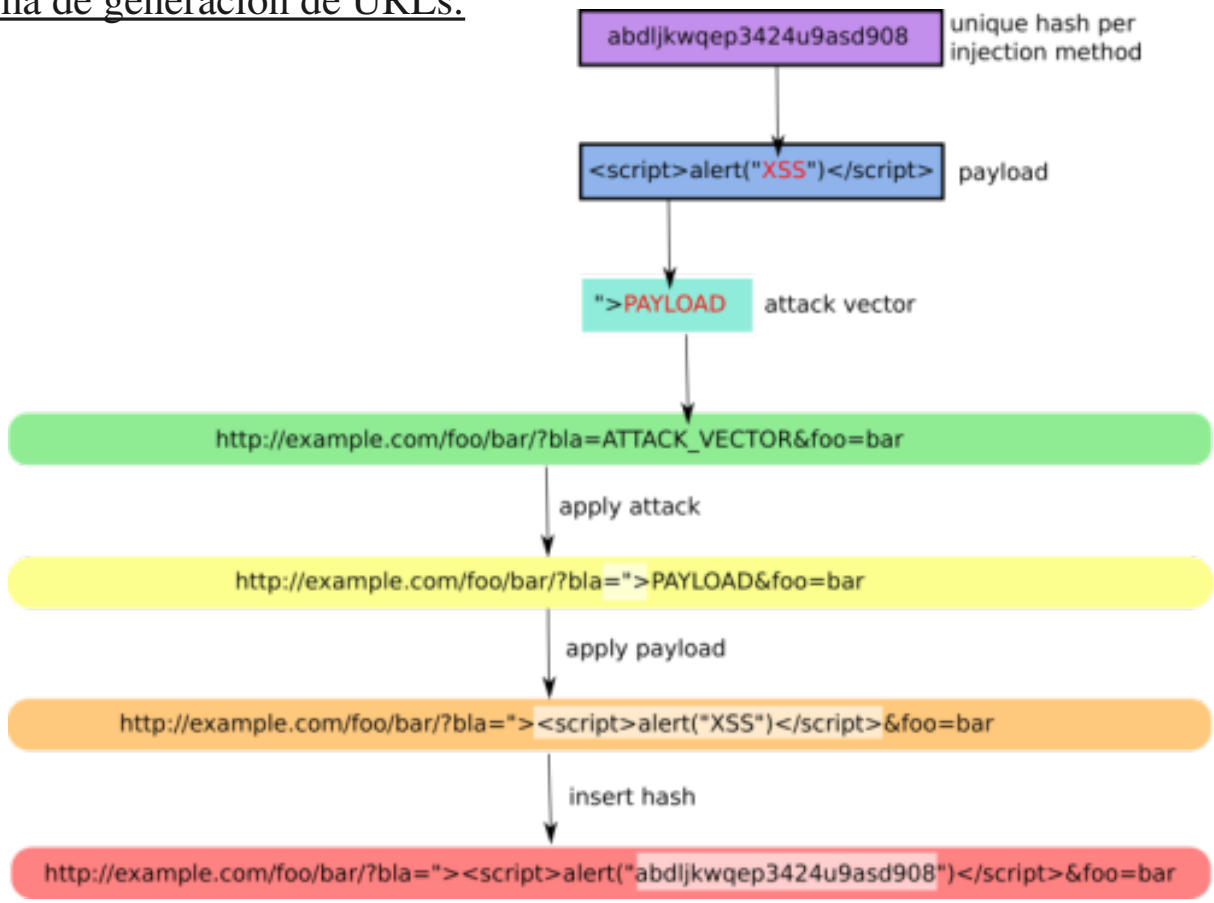
- Contiene un "Wizard Helper", que permite generar ataques respondiendo a preguntas
- Tiene muchos ejemplos y documentación adjunta
- Permite conocer los resultados de otros "pentesters" *en tiempo real*
- La versión GUI, tiene un mapa para georeferenciar los ataques y hacer esquemas
- [...]

/ ¿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 |-i |-d] [-g |-p |-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:

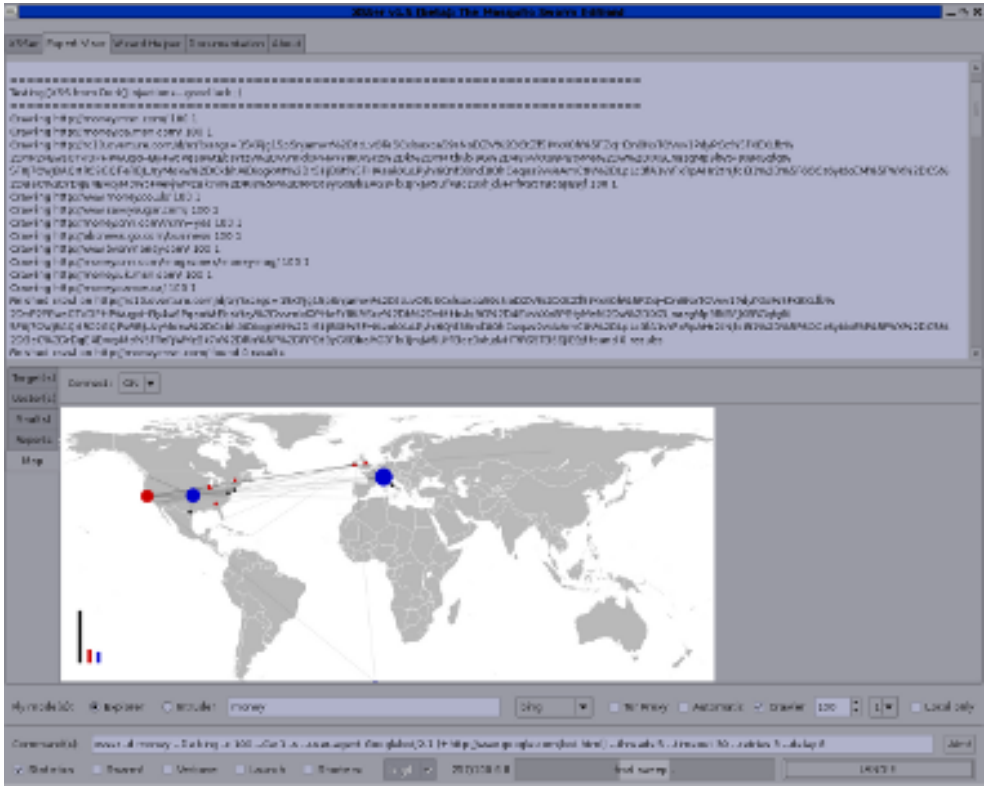
Swarm Edition!: http://xsser.blip.tv

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 comándos 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 =""><img src="x:x"...*

Explotación:

- Explotación de XSS local: *$ python xsser -u/-i/-d "host.com" --Fp = "<script>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:

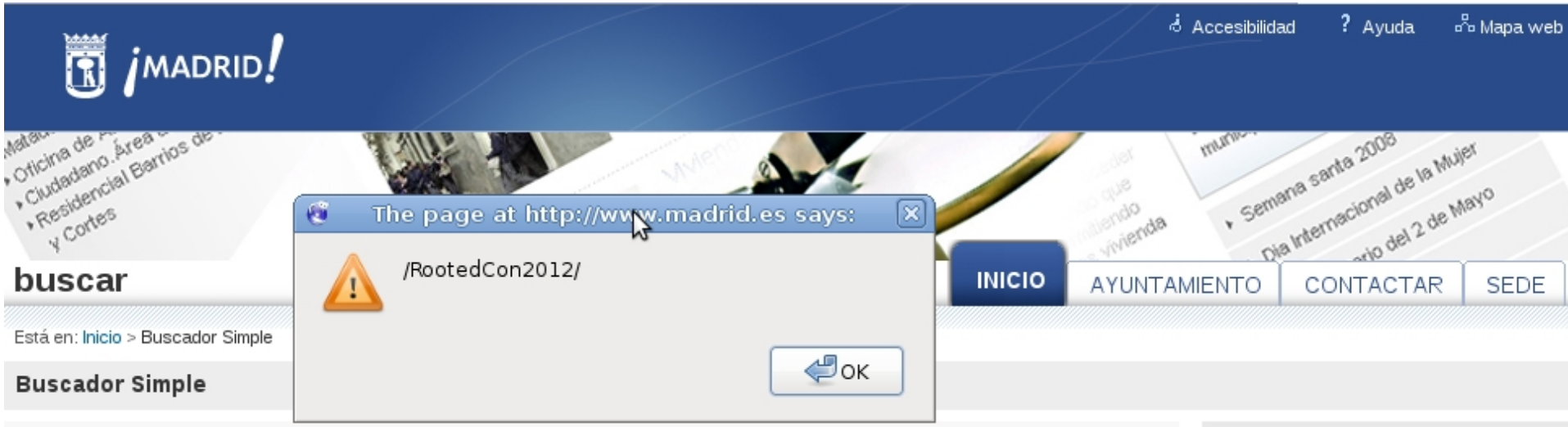
- Testing
- Documentación
- Cerrar bugs (falsos positivos, arreglar el “swarm”, auto-update, multithreading, glibc corruption...)
- Refactorizar el código
- Comunidad
- XSSer: White Swarm (versión empresarial)+ Black Swarm (versión comunidad)
- […]

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

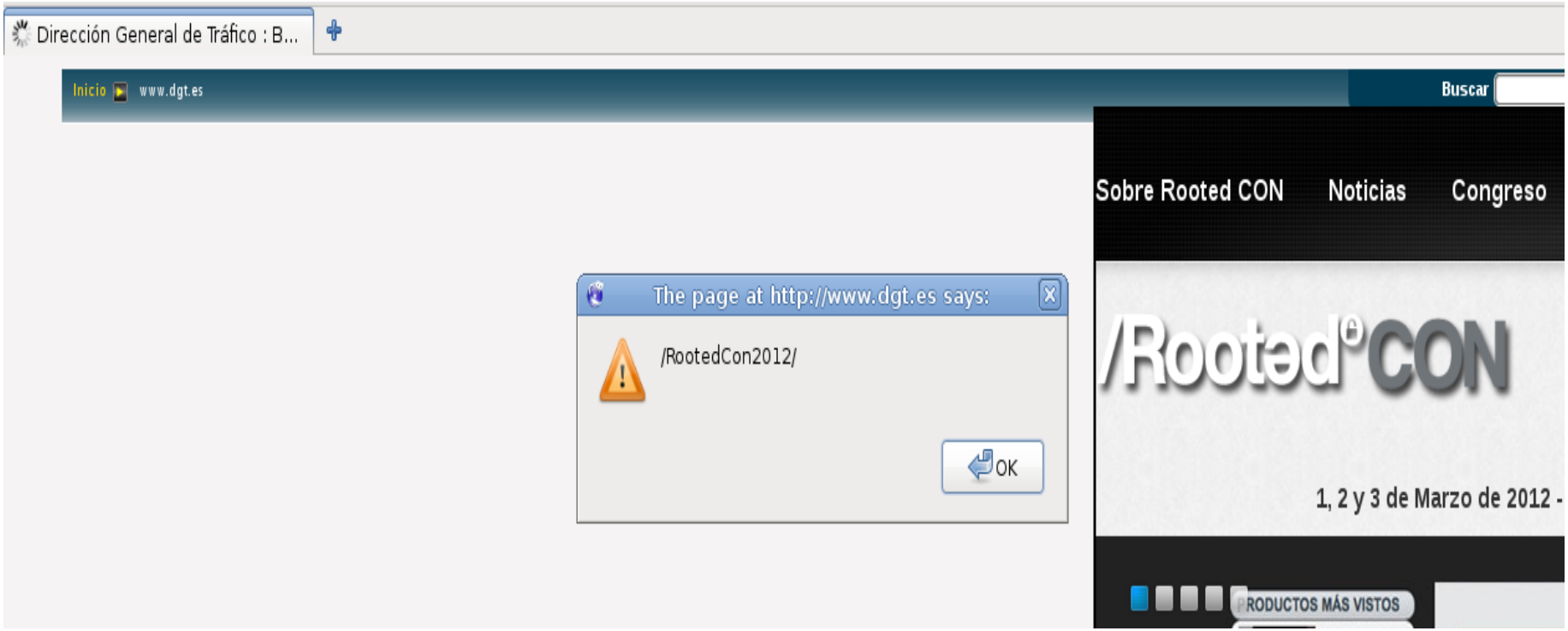


/ EXTRA !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

/ EXTRA !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ



/ EXTRA !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

RootedCon2012

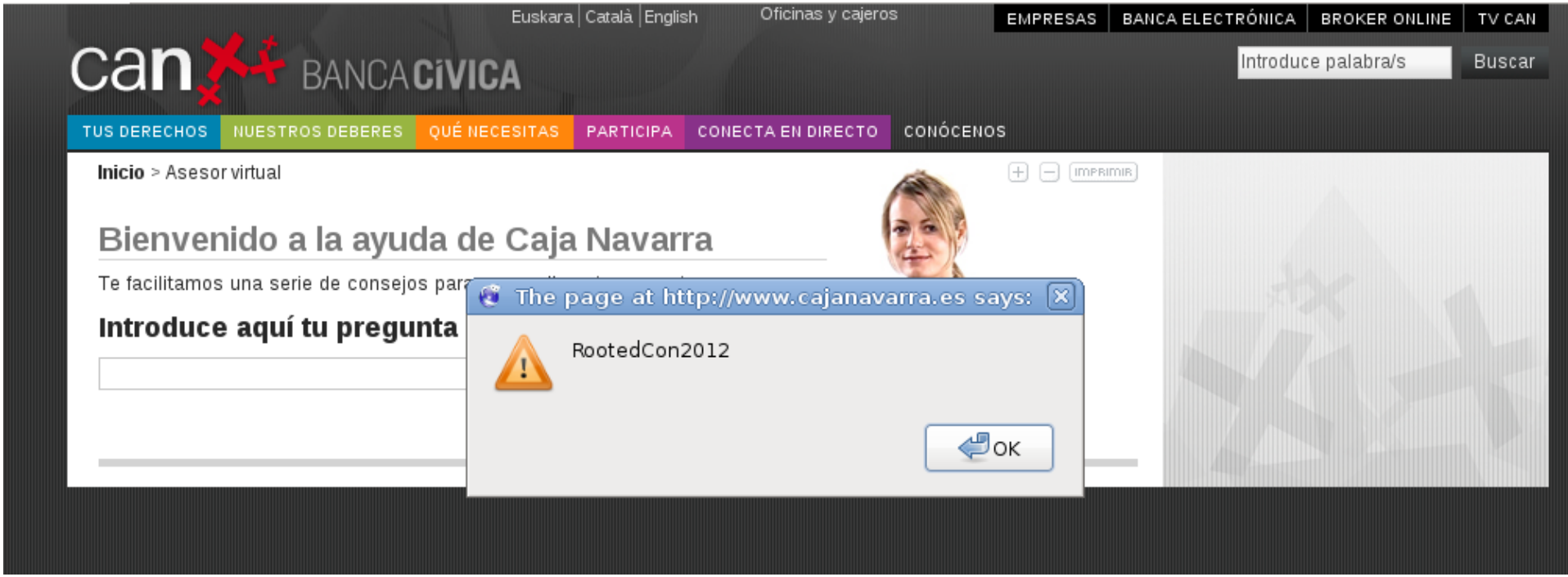
2:57

/ EXTRA !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

/ EXTRA !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ



/ 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 !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

/ EXTRA !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

USPTO Patent Full-Text and Image Database

Help | Home | Quick | Advanced | Pat Num | Order Copy | PTDLs

/ EXTRA !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

vodafone

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 cons
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/NIF/NIE/PASAPORTE:**

Introduce los datos sobre la última factura o los cuatro últi

* **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

Sobre Rooted CON Noticias Congreso Tienda Colaborador

/ EXTRA !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

English | Deutsch | Español | Português

Home | Security Audit

Programas de Asociados | Testimonios | En la Prensa | Listas de Correos | Acerca Nuestro | Contáctenos | Privacidad | Abuso

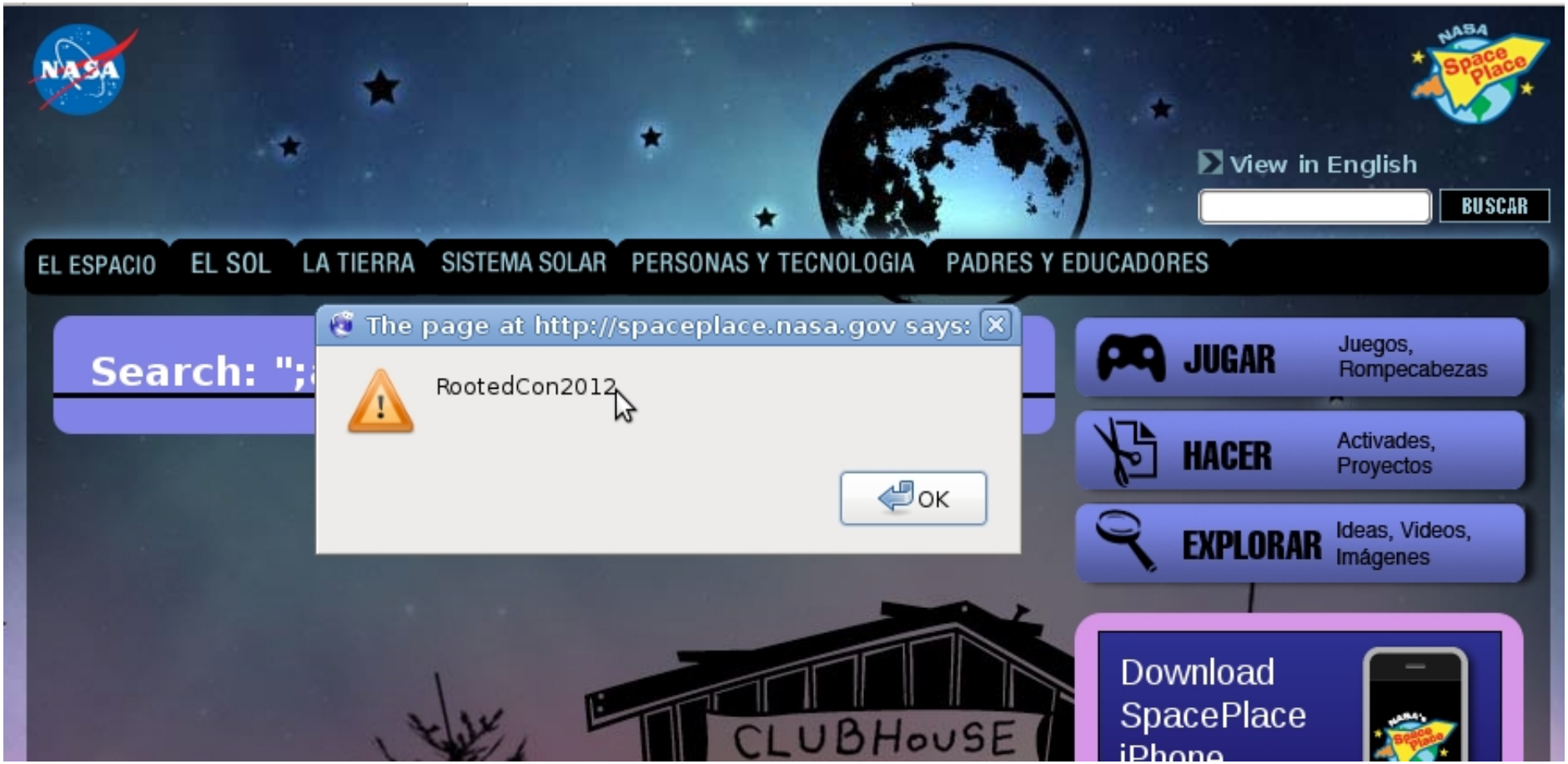
Contáctenos

/ EXTRA !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ

/ EXTRA !!!!!! /

- BbZZZzZzZzzzZzzzzZzzzZZZZZ



/ ¿Cómo colaborar? /

IRC: irc.freenode.net / canal #xsser

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

“swarm means … #lulz”