



XSS

**Consecuencias
de sitios
comprometidos**



Xenotix



Diego Subero

Carlos Suarez

Hacked by LatinHackTeam!

Your Security.. Get Down

Are youuu hacked

LatinHackTeam, we are :

d4nlux + eCORE + Chip d3 b10s + J3H35 + Rayok3nt

TE AMO N.....

uid=0(root) gid=0(root) groups=48(apache),2522(psaserv)

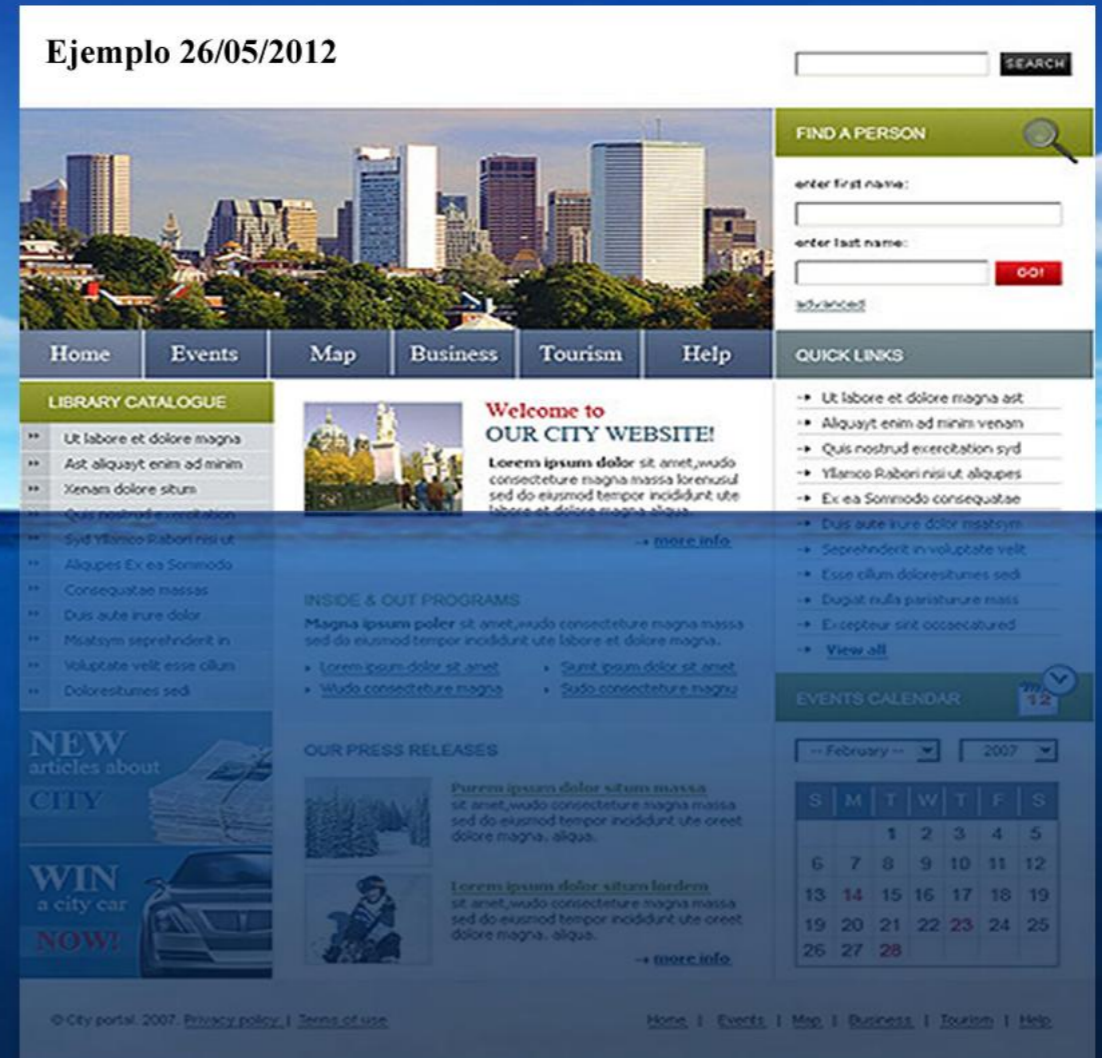
Fr0m: Ecuador ' Spain ' Chile ' Venezuela ' Colombia

Es todo lo que un intruso hace?

A simple vista



Lo que verdaderamente hay..



Nominas

Contraseñas

Correos

Mapa de Operaciones militares

Historiales médicos

Historial Bancario

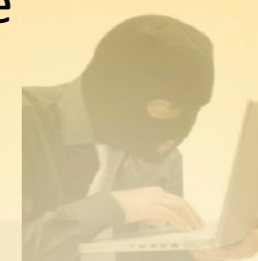
Mapas de infraestructuras criticas

Problemas en la Web

Ataques

DDOS

Espionaje



Sql injection

Manipulación de datos

Suplantación de identidad

Expuestas a:

Inadecuadas configuraciones

Inadecuados filtros de entrada

Contraseñas débiles

Expone a:

Estafas Bancarias

Indisponibilidad y desestabilización

Afectación de la reputación

Distribución de virus



Sitios y aplicaciones WEB



Ataques en el cliente

XSS...
Ingeniería Social

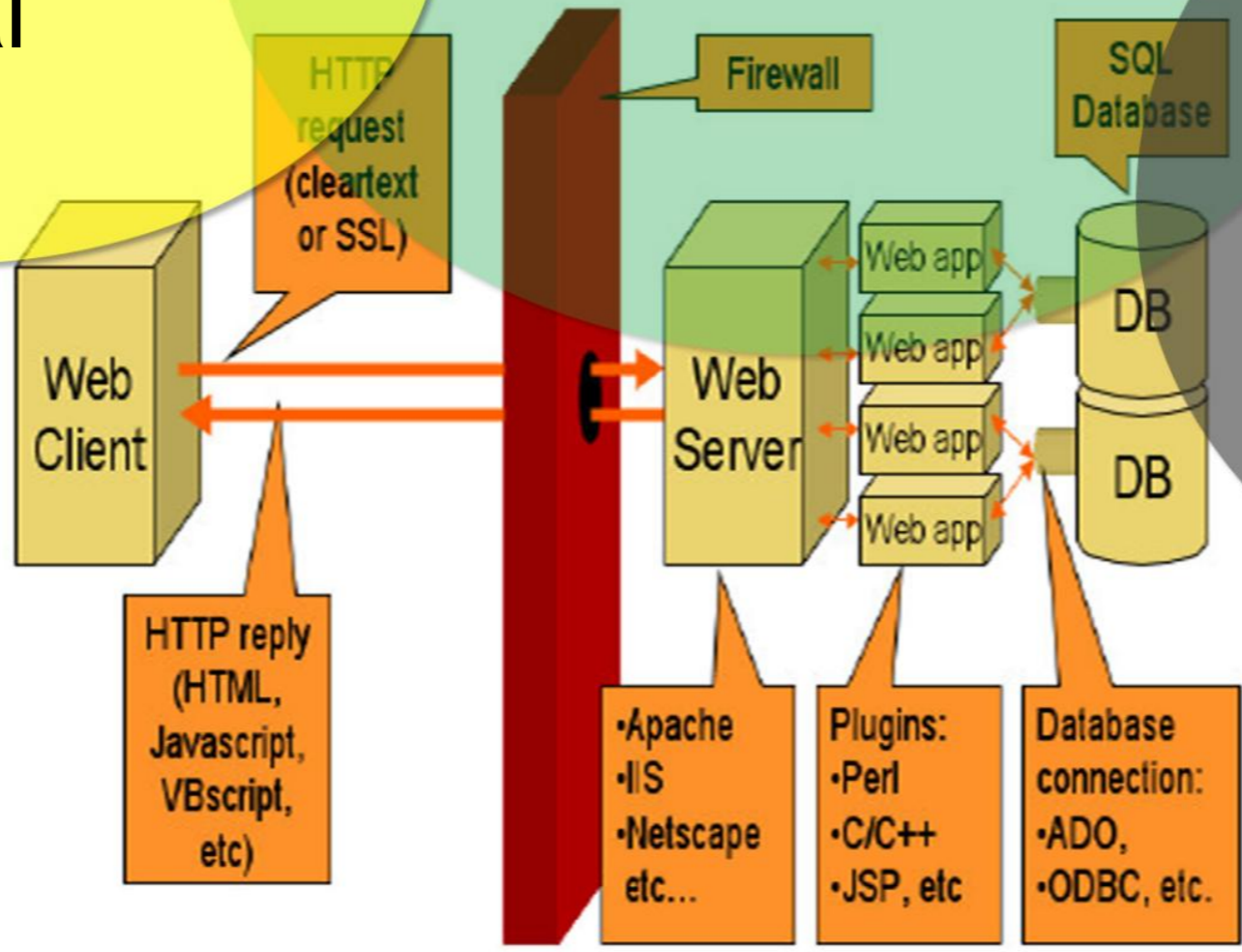


Ataques a las aplicaciones

RFI, LFI,
XSS, bug



Ataques a la base de datos
SQL Injection



¿Que atacamos?

The screenshot shows the homepage of the Soledad website. At the top, there is a navigation menu with links for 'INICIO', 'QUIENES SOMOS', 'EMPRESAS', 'AREAS', and 'CONTÁCTANOS'. Below the menu is a large banner image of a mountain landscape with the text 'COMPROMETIDOS CON EL MEDIO AMBIENTE'. To the right of the banner is a 'Nuestro Compromiso' section. Below the banner are several columns of text and images, including a 'Reciclado de Neumáticos' section with a list of bullet points, a 'Tratamiento del Neumático' section, and a 'Distribución de Neumáticos' section. There is also a 'Contactanos' form on the left side.

The screenshot shows a Toyota advertisement. At the top, there is contact information for Chacabuco 1299, Ramos Mejía, Buenos Aires, Argentina, with a phone number (5411)4460-1500 and an email address. Below this is a navigation bar with 'UBICACION' and 'CONTACTO' tabs. The main content features a large image of a red Toyota truck and several silver cars. The text 'con lo nuevo de Toyota' is prominently displayed. Below the image, there are three promotional boxes: 'Conocé el nuevo EGROGLAXRS', 'Toyota v130 Active \$101.250' with 'Anticipo \$ 48.000' and 'Cuotas \$ 2.700', and 'Ahorra tranquilidad' with a piggy bank icon. At the bottom, there is a 'TOYOTA DEMO | CHACABUCO 1299 OF. 4' contact block.

The screenshot shows a WordPress blog post titled 'Feria de Carros Margarita 2012' with the subtitle 'Septiembre del 6 al 7 de Septiembre, Asiste!'. The post is dated August 24th, 2012, and is authored by 'admin'. The main content of the post is 'Feria de carros tuning, Arenita playita y chicas sexys 2012 (6 y 7 de Septiembre)'. The post is categorized under 'Uncategorized (1)'. The sidebar contains a search bar, a 'Recent Posts' section with a link to the current post, and a 'Recent Comments' section. The right sidebar also includes 'Categories', 'Links', and 'WordPress Blog' sections.

Descubriendo vulnerabilidades



XSS

Cross Site Scripting

El gran desconocido..

¿Por que XSS?

Los 10 riesgos más críticos en aplicaciones web

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

XSS

¿Que es?

Es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado y validación adecuados en campos de entrada

```
<?php
```

```
$bug = $_GET["var"];  
echo "Has escrito: ".$bug;
```

```
?>
```

¿Cómo lo hace?

Permite el envío de scripts completos con secuencias de comandos maliciosos

¿Consecuencias?

Impacto directo en el sitio web o en el equipo de un usuario.



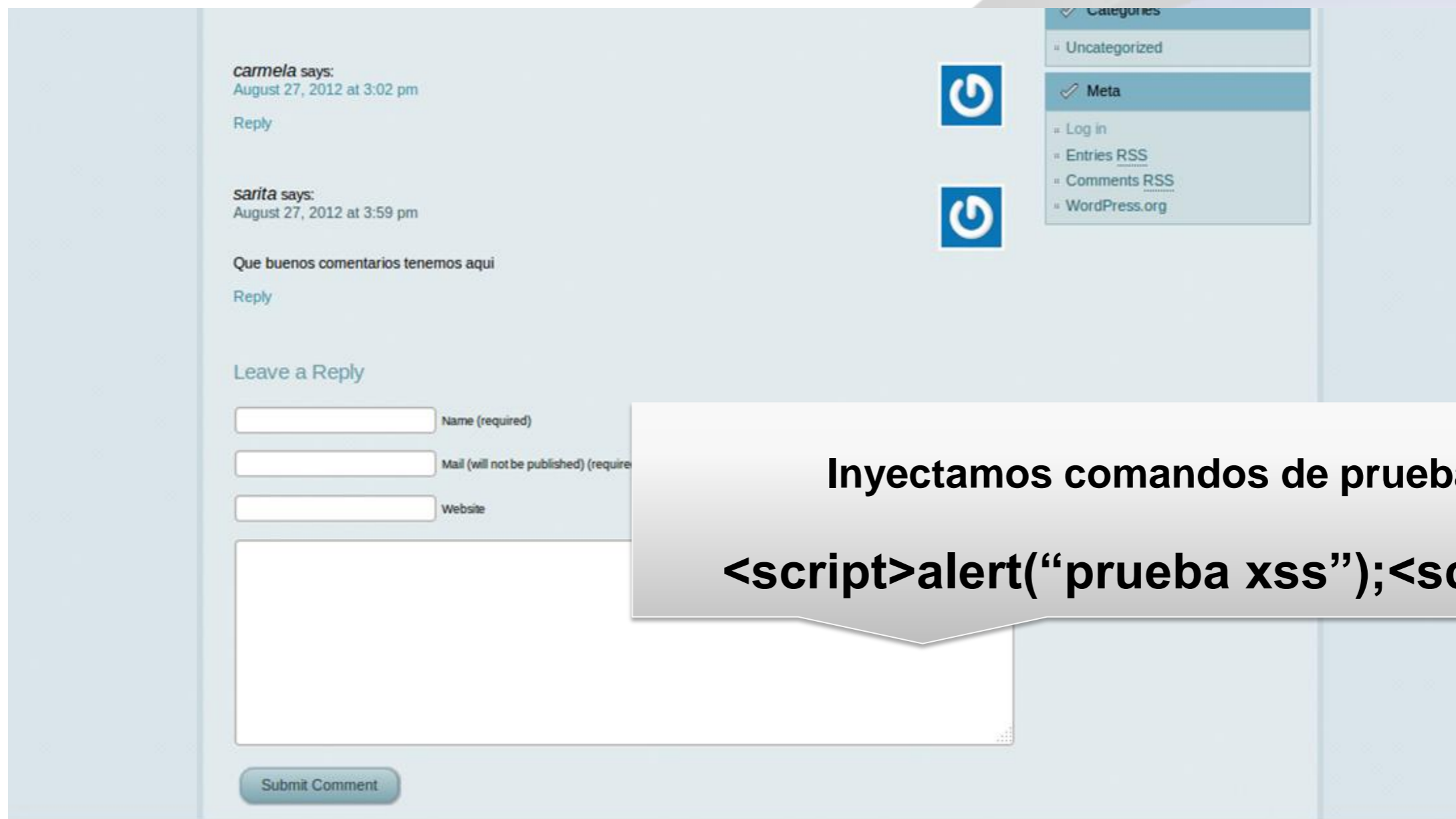


¿Donde encontramos vulnerabilidades de XSS?



¿Es vulnerable a XSS?

Detectar la vulnerabilidad a través del formulario del foro:



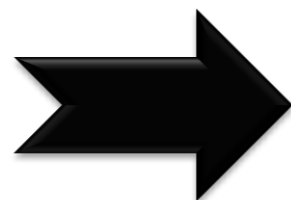
The screenshot shows a forum interface. On the left, there are two comments: one from 'carmela' dated August 27, 2012 at 3:02 pm, and another from 'sarita' dated August 27, 2012 at 3:59 pm. Below the comments is a 'Leave a Reply' section with three input fields: 'Name (required)', 'Mail (will not be published) (required)', and 'Website'. A large text area for the comment is below these fields, and a 'Submit Comment' button is at the bottom. On the right side, there is a navigation menu with a 'Categories' section containing 'Uncategorized' and a 'Meta' section containing 'Log in', 'Entries RSS', 'Comments RSS', and 'WordPress.org'. Two blue circular icons with a white power symbol are positioned between the comments and the navigation menu.

Inyectamos comandos de prueba
`<script>alert("prueba xss");</script>`

Explotamos...

Vulnerabilidad
de
XSS

¿Qué
hacemos?



Browser Exploitation Framework

Navegación dirigida

Spyware

Ejecución de acciones
automáticas

Robo de
credenciales

¿Soy vulnerable a XSS?

XENOTIX

OWASP Xenotix XSS Exploit Framework 2013 v3

URL: Parameter:

Inbuilt XSS Payloads Custom XSS Payloads

Select Test Mode:

Log in / create account

OWASP The Open Web Application Security Project

Page Discussion Read View source View history

OWASP Xenotix XSS Exploit Framework

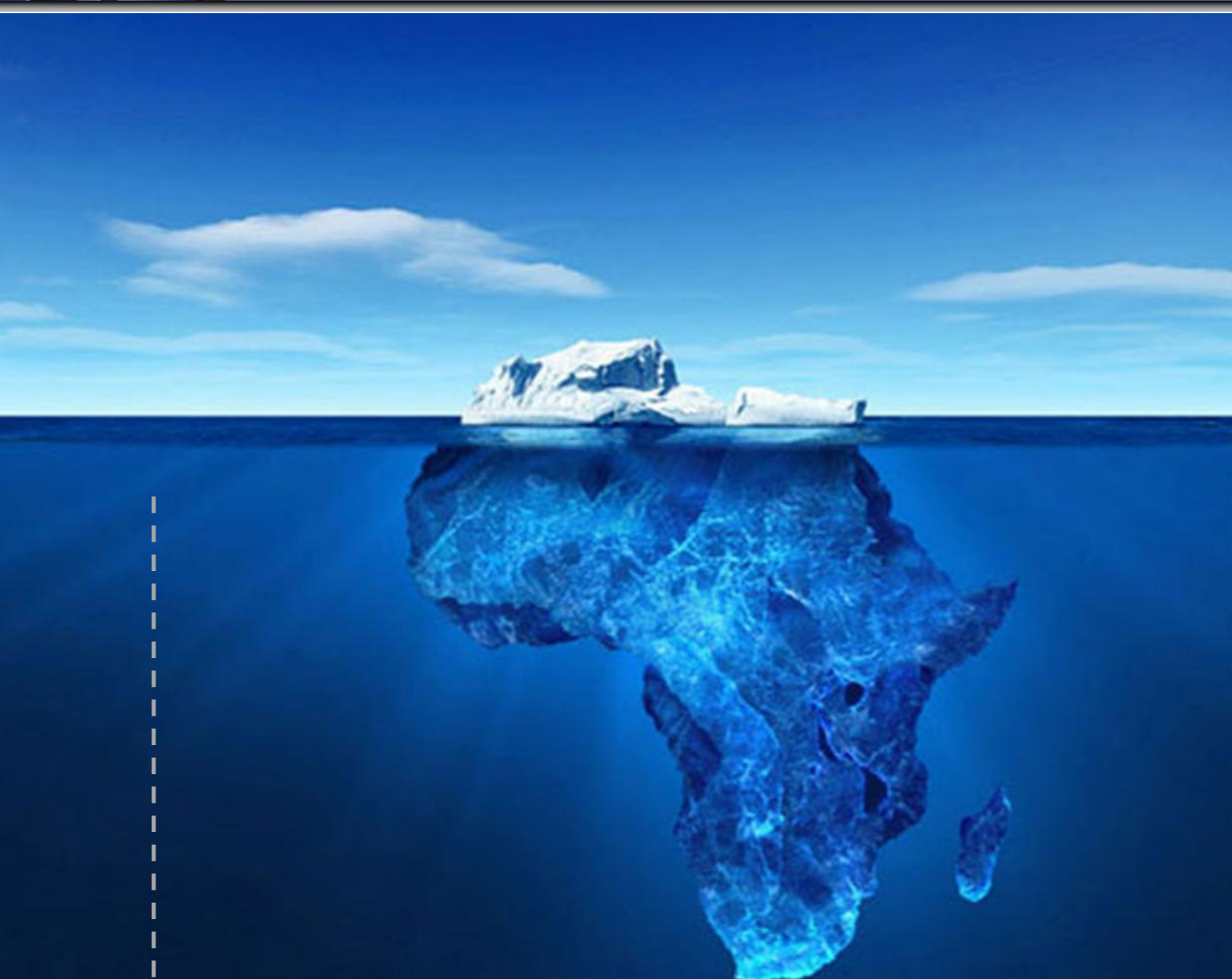
Contents [hide]
1 Xenotix XSS Exploit Framework
2 Features of Xenotix XSS Exploit Framework
3 Support us on Facebook
4 White Paper
5 Videos
6 Download
7 IMPORTANT

```
<!DOCTYPE html><html lang="en" dir="ltr" class="client-nojs"><head><title>OWASP Xenotix XSS Exploit Framework - OWASP</title><meta charset="UTF-8" /><meta name="generator" content="MediaWiki 1.18.0" /><link rel="shortcut icon" href="/favicon.ico" /><link rel="search" type="application/opensearchdescription+xml" href="/opensearch_desc.php" title="OWASP (en)" /><link rel="EditURI" type="application/rsd+xml" href="https://www.owasp.org/api.php?action=rsd" /><link rel="copyright" href="http://creativecommons.org/licenses/by-sa/3.0/" /><link rel="alternate" type="application/atom+xml" title="OWASP Atom feed" href="/index.php?title=Special:RecentChanges&feed=atom" /><link rel="stylesheet" href="/load.php?debug=false&lang=en&modules=mediawiki.legacy.commonPrint%2Cshared%2Cskins.vector&only=styles&skin=vector&*" /><meta name="ResourceLoaderDynamicStyles" content="*" /><link rel="stylesheet" href="/load.php?debug=false&lang=en&modules=site&only=styles&skin=vector&*" /><style>a lang(ar).a lang(ckb).a lang(fa).a lang(kk-arab).a lang(mzn).a lang(ps).a lang(ur){text-decoration:none}a new.#quickbar a new{color:#ba0000}.edtsection{display:none}/" cache key: wiki:resourceloader:filter:minify-css:4:40436297bd93906a010108e46094c495 "/></style><script src="/load.php?debug=false&lang=en&modules=startup&only=scripts&skin=vector&*" /></script><script>f(window.mw){ mw.config.set({"wgCanonicalNamespace":"","wgCanonicalSpecialPageName":false,"wgNamespaceNumber":0,"wgPageName":"OWASP_Xenotix_XSS_Exploit_Framework","wgTitle":"OWASP Xenotix XSS Exploit Framework","wgCurRevisionId":141077,"wgArticleId":26171,"wgIsArticle":true,"wgAction":"view","wgUserName":null,"wgUserGroups":[""],"wgCategories":["OWASP Project"],"wgBreakFrames":false,"wgRestrictionEdit":[""],"wgRestrictionMove":[""]});</script><script>f(window.mw){ mw.loader.load(["mediawiki.page.startup"]);</script><!--[if lt IE 7]><style type="text/css">body{behavior:url("/skins/vector/csshover.min.htc")}</style></endif--></head><body class="mediawiki ltr sitedir-ltr ns-0 ns-subject page-OWASP_Xenotix_XSS_Exploit_Framework action-view skin-vector">
```



Summary & Conclusion





Ejemplo 26/05/2012

SEARCH

FIND A PERSON

enter first name:

enter last name:

GO!

advanced

Home | Events | Map | Business | Tourism | Help

LIBRARY CATALOGUE

- Ut labore et dolore magna
- Ast aliquyt enim ad minim
- Xenam dolore solum
- Quis nostrud exercitation
- Syd Yllamco Rabori nisi ut
- Aliques Ex ea Sommodo
- Consequatue massas
- Duis aute iure dolor
- Msatsym seprehenderit in
- Voluptate velit esse cilum
- Doloresitumes sed

NEW articles about CITY

WIN a city car NOW!

WELCOME TO OUR CITY WEBSITE!

LOREM IPSUM DOLOR SIT AMET, WUDO CONSECTETURE MAGNA MASSA SED DO EUJMOD TEMPOR INCIDidunt UTE LABORE ET DOLORE MAGNA, ALIQUA.

INSIDE & OUT PROGRAMS

Magna ipsum polor sit amet, wudo consecteture magna massa sed do eiusmod tempor incididunt ute labore et dolore magna.

- lorem ipsum dolor sit amet
- Wudo consecteture magna
- Sunt ipsum dolor sit amet
- Sudo consecteture magnu

OUR PRESS RELEASES

Purem ipsum dolor situm massa sit amet, wudo consecteture magna massa sed do eiusmod tempor incididunt ute oreet dolore magna, aliqua.

lorem ipsum dolor situm lorderm sit amet, wudo consecteture magna massa sed do eiusmod tempor incididunt ute oreet dolore magna, aliqua.

QUICK LINKS

- Ut labore et dolore magna ast
- Aliquyt enim ad minim venam
- Quis nostrud exercitacion syd
- Yllamco Rabori nisi ut, aliques
- Ex ea Sommodo consequatue
- Duis aute iure dolor msatsym
- Seprehenderit in voluptate velit
- Esse cilum doloresitumes sed
- Dugiat nulla pariaturure mass
- Excepteur sint occaecabured
- View all

EVENTS CALENDAR

February 2007

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
19	20	21	22	23	24	25
26	27	28				

© City portal. 2007. Privacy policy | Terms of use

Home | Events | Map | Business | Tourism | Help

Validar

Indagar en lo que no esta a simple vista

Actualizar

SGSI

Revisiones de código

Monitoreo...

¿Como prevenir XSS?

- ✓ **No confiar nunca en datos que obtengas de los usuarios o de cualquier fuente de datos externa**
- ✓ **Saneando los datos**
- ✓ **Escapando los datos**
- ✓ **No caer en la famosa ingeniería social**
- ✓ **Seguir las mejores practicas OWASP(Prevention Cheat Sheet, testing guide and tools)**

Hacked by LatinHackTeam!

Your Security.. Get Down

Are youuu hacked

LatinHackTeam, we are :

d4n1ux + eCORE + Chip d3 b10s + J3H35 + Rayok3nt

TE AMO N.....

uid=0(root) gid=0(root) groups=48(apache),2522(psaserv)

Fr0m: Ecuador ' Spain ' Chile ' Venezuela ' Colombia

¿¿Esto es lo único que podemos hacer con un sitio vulnerable?????



Contactos

Diego Subero

Carlos Suarez

@cracksub

@kaarluus

diego.subero@owasp.org

carlosss764@gmail.com

Muchas Gracias...