



The OWASP Foundation

<http://www.owasp.org>

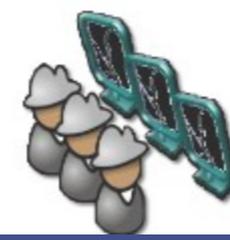
Técnicas de Intrusión de Aplicaciones Web con WebScarab framework (OWASP)

Mauricio Urizar

murizar@open-sec.com



@MauricioUrizar



Open-Sec

Ethical Hacking/Forensics/InfoSec



- | Trabajando los últimos 07 años como parte del equipo de hacker eticos de Open-Sec.
- ▣ Instructor de cursos de Ethical Hacking en Perú y Ecuador.

C|EH (Certified | Ethical Hacker)

CEI (Certified EC-Council Instructor)

CPTe (Certified Penetration Tester)

CPTe Mile2 - Authorized Instructor

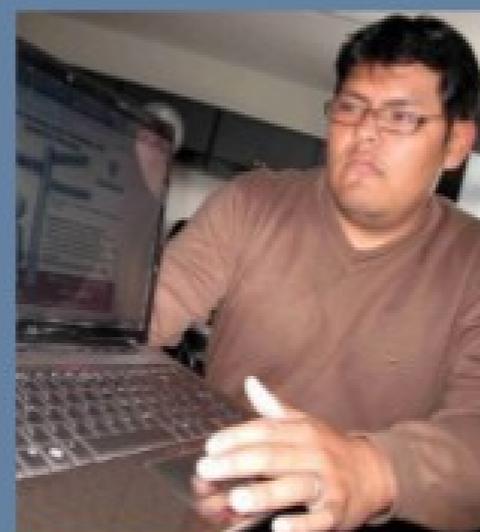
OSEH (Open-Sec Ethical Hacker)



Open-Sec

Ethical Hacking/Forensics/InfoSec

Los consultores...



www.Open-Sec.com





DESCARGO DE RESPONSABILIDADES

- Esta presentación tiene como propósito proveer únicamente información. No aplicar este material ni conocimientos sin el consentimiento explícito que autorice a hacerlo. Los lectores (participantes, oyentes, videntes) asumen la responsabilidad completa por la aplicación o experimentación de este material y/o conocimientos presentados. El(los) autor(es) quedan exceptuados de cualquier reclamo directo o indirecto respecto a daños que puedan haber sido causados por la aplicación de este material y/o conocimientos expuestos.
- La información aquí expuesta representa las opiniones y perspectivas propias del autor respecto a la materia y no representan ninguna posición oficial de alguna organización asociada.



Quienes deben estar aquí?

- **Desarrolladores que deseen conocer más respecto a seguridad informática y como proteger sus aplicaciones web.**
- **Profesionales de la seguridad informática que necesiten realizar evaluaciones a aplicación que se comuniquen sobre HTTP / HTTPS.**



Que es WebScarab ?

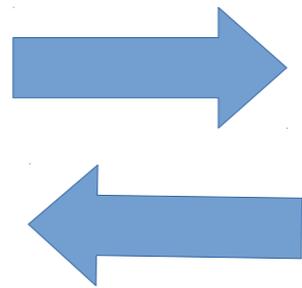
- **OWASP WebScarab es una herramienta para análisis de aplicaciones web y actúa como proxy entre un cliente (navegador web) y una aplicación web, es capaz de interceptar los protocolos HTTP y HTTPS.**
- **Permite al operador revisar y modificar pedidos creados por el navegador antes de ser enviados al servidor, de igual forma las respuestas devueltas desde el servidor pueden ser manipuladas antes de que sean recibidos por el navegador.**



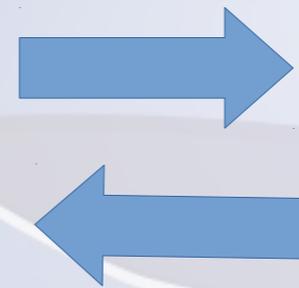
Que es Webscarab ?



Navegador Web



**Webscarab
(proxy)**



Aplicación Web



Como corro Webscarab?

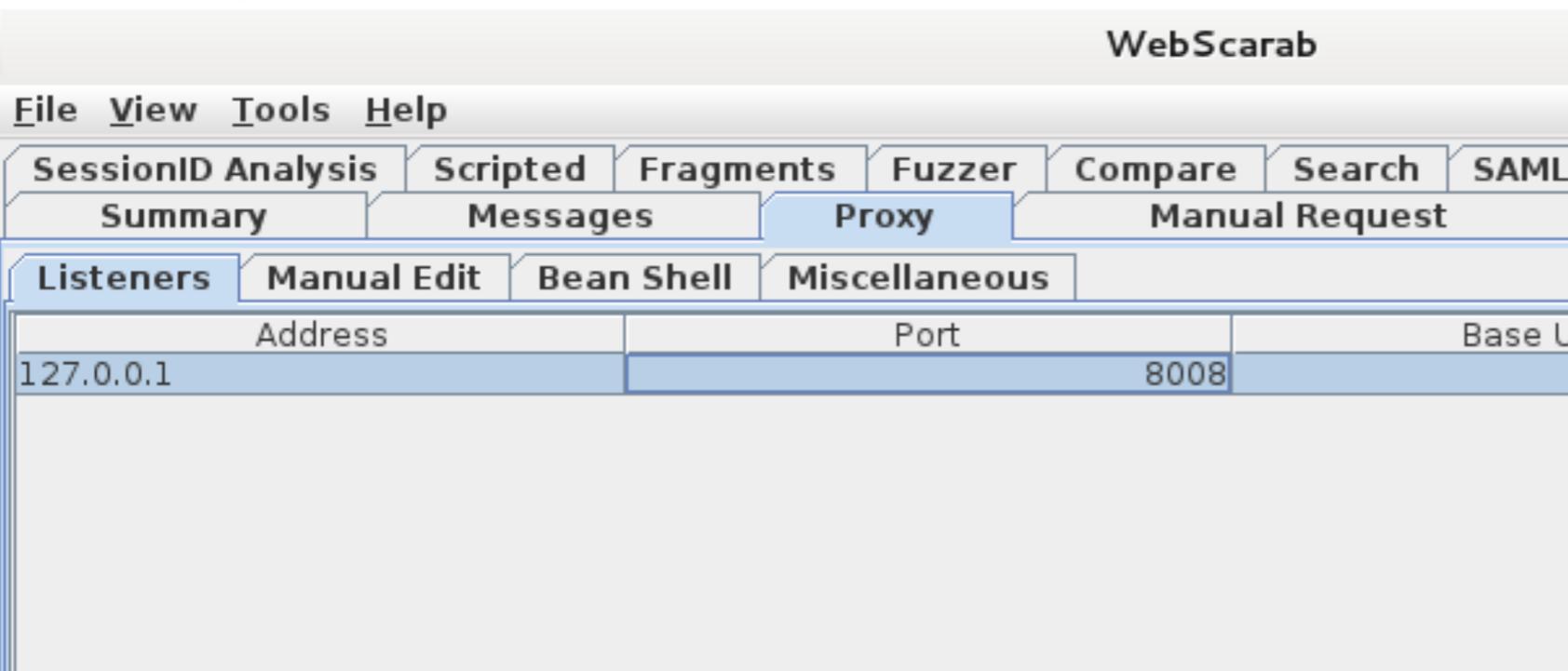
Ejecutemos el archivo **“.jar”** de la siguiente forma.

```
hackstation:~/Download#  
hackstation:~/Download#  
hackstation:~/Download# java -jar webscarab-one-20120422-001828.jar
```

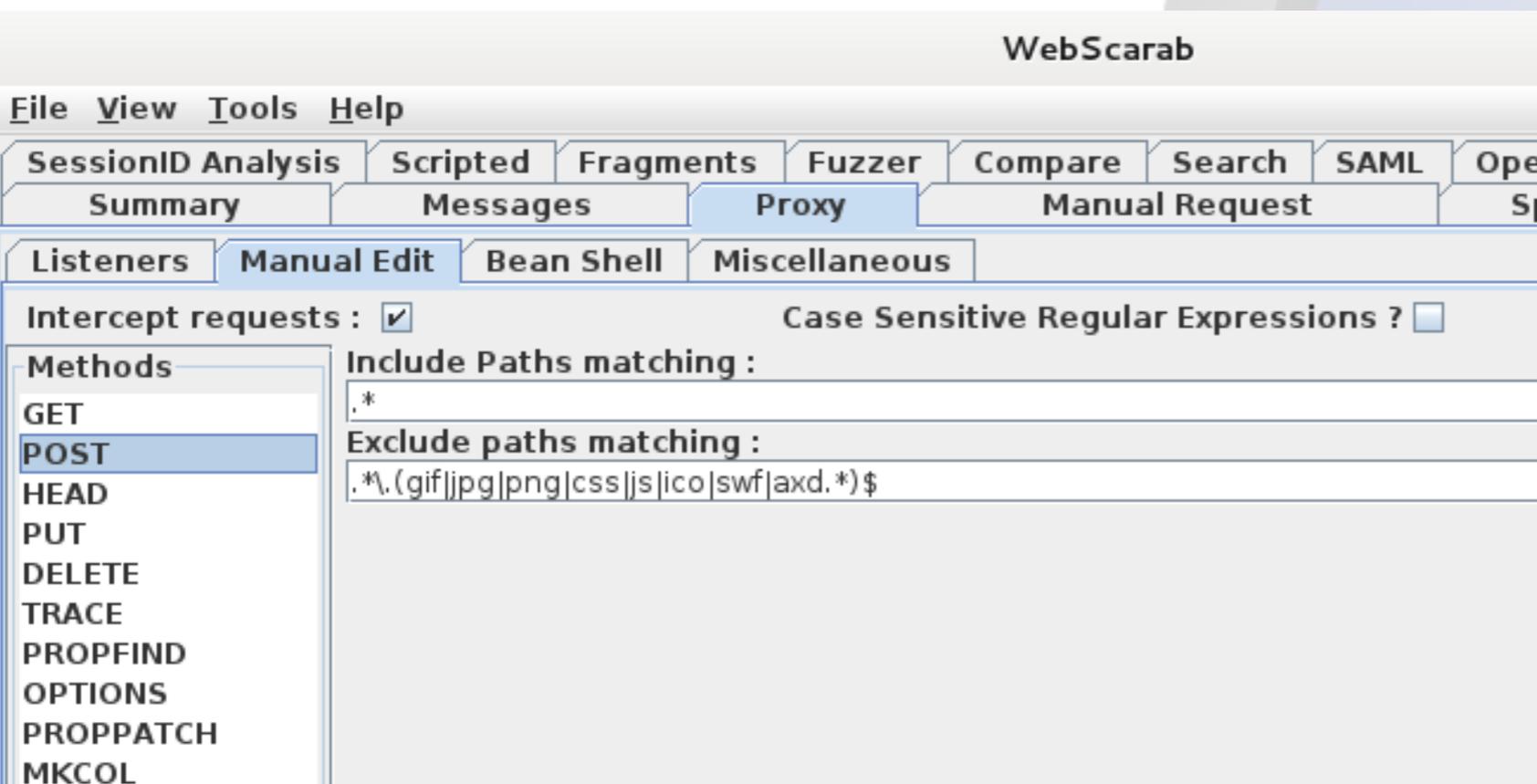




Configurando WebScarab



Puerto en escucha, el mismo que se configura en el navegador..



Interceptar solo peticiones POST (formularios web)



Configurando Navegador

The screenshot shows a web browser window with the title "Welcome to OWASP Mantra - Free and Open Source Browser based Security Framework - OWASP Mantra". The address bar shows "www.getmantra.com/welcome/". The page content is a grid of logos: YouTube, twitter, last.fm, YAHOO!, mantra, OWASP, Hackery, Galley, WIKIPEDIA, and SHODAN. The browser's "Tools" menu is open, showing options like "Preferences", "Managers", "Privacy and Security", "Debug Tools", "Utilities", "Information Gathering", "Editors", "Network Utilities", "Misc", "Application Auditing", "Proxy", and "Uncategorised". The "Application Auditing" option is highlighted, and a sub-menu is visible with items: "Tamper Data", "Live HTTP headers", "HttpFox", "HttpRequester Ctrl+Alt+P", "RefControl Options...", "Default User Agent", "Web Developer", "Show/hide hackbar F9", "Ra.2 Scanner", "NoRedirect", "Web Developer Extension", "Cookie", and "Cookies Manager+".

<http://www.getmantra.com/>



Configurando Navegador

Connection Settings

Configure Proxies to Access the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration:

HTTP Proxy: localhost Port: 8008
 Use this proxy server for all protocols

SSL Proxy: localhost Port: 8008

FTP Proxy: localhost Port: 8008

SOCKS Host: localhost Port: 8008
 SOCKS v4 SOCKS v5

No Proxy for:
localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Automatic proxy configuration URL:
[Empty field] [Reload]

[Help] [Cancel] [OK]



Eso es todo.. listo para analizar



Registra todo el trafico

WebScarab

File View Tools Help

Extensions XSS/CRLF SessionID Analysis Scripted Fragments Fuzzer Compare Search

Summary Messages Proxy Manual Request WebServices

Tree Selection filters conversation list

Url	Methods	Status	Possible l...	Injection	Set-Cookie	Comments	Scripts
⊖ http://www.acme.com:80/			<input type="checkbox"/>				
⊖ admin/			<input type="checkbox"/>				
index.html	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✓	<input type="checkbox"/>
⊖ page.php			<input type="checkbox"/>				
?seccion=Contactenos	GET	200 OK	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
?seccion=Inicio	GET	200 OK	✓	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
⊖ web-intranet/			<input type="checkbox"/>				
login.php	POST	200 OK	<input type="checkbox"/>				

ID	Date	Met...	Host	Path	Parameters
9	2014/03/14 07:52:49	POST	http://www.acme.com:80	/web-intranet/login.php	
8	2014/03/14 07:52:38	GET	http://www.acme.com:80	/admin/images/bg_submenu.gif	
7	2014/03/14 07:52:38	GET	http://www.acme.com:80	/admin/images/bg_menu.gif	
6	2014/03/14 07:52:38	GET	http://www.acme.com:80	/admin/images/tie_logo.gif	
5	2014/03/14 07:52:37	GET	http://www.acme.com:80	/admin/images/style.css	
4	2014/03/14 07:52:37	GET	http://www.acme.com:80	/web-intranet/	
3	2014/03/14 07:52:32	GET	http://www.acme.com:80	/page.php	?seccion=Contactenos
2	2014/03/14 07:52:26	GET	http://www.acme.com:80	/index.html	
1	2014/03/14 07:51:49	GET	http://www.acme.com:80	/page.php	?seccion=Inicio



Spider plug-in

WebScarab

File View Tools Help

Extensions XSS/CRLF SessionID Analysis Scripted Fragments Fuzzer Compare Search

Summary Messages Proxy Manual Request WebServices Spider

Tree Selection filters conversation list

Url	Methods	Status	Possible I...	Injection	Set-Cookie	Comments	Scripts
http://www.acme.com	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
demo/	GET	404 Not F...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
file.php	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
images/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
index.html	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
news.php	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
page.php	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
?seccion=Contactenos	GET	200 OK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
?seccion=Inicio	GET	200 OK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
?seccion=Nosotros	GET	200 OK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
?seccion=Productos	GET	200 OK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
?seccion=Servicios	GET	200 OK	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
web-intranet/	GET	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
login.php	POST	200 OK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Spider tree
Show scripts
Show comments

ID	Date	Met...	Host	Path	Parameters	Status	Origin
29	2014/03/14 08:12:45	GET	http://www.acme.com:80	/page.php	?seccion=Servicios	200 OK	Spider
28	2014/03/14 08:12:45	GET	http://www.acme.com:80	/page.php	?seccion=Productos	200 OK	Spider
27	2014/03/14 08:12:45	GET	http://www.acme.com:80	/page.php	?seccion=Nosotros	200 OK	Spider
26	2014/03/14 08:12:45	GET	http://www.acme.com:80	/page.php		200 OK	Spider
25	2014/03/14 08:12:45	GET	http://www.acme.com:80	/news.php	?id=5	200 OK	Spider
24	2014/03/14 08:12:45	GET	http://www.acme.com:80	/news.php	?id=2	200 OK	Spider
23	2014/03/14 08:12:45	GET	http://www.acme.com:80	/news.php	?id=1	200 OK	Spider
22	2014/03/14 08:12:45	GET	http://www.acme.com:80	/news.php		200 OK	Spider
21	2014/03/14 08:12:45	GET	http://www.acme.com:80	/images/style.css		200 OK	Spider
20	2014/03/14 08:12:45	GET	http://www.acme.com:80	/images/		200 OK	Spider
19	2014/03/14 08:12:45	GET	http://www.acme.com:80	/file.php	?file=file5.zip	200 OK	Spider
18	2014/03/14 08:12:45	GET	http://www.acme.com:80	/file.php	?file=file4.zip	200 OK	Spider
17	2014/03/14 08:12:45	GET	http://www.acme.com:80	/file.php	?file=file3.zip	200 OK	Spider
16	2014/03/14 08:12:45	GET	http://www.acme.com:80	/file.php	?file=file2.zip	200 OK	Spider
15	2014/03/14 08:12:44	GET	http://www.acme.com:80	/file.php	?file=file1.zip	200 OK	Spider
14	2014/03/14 08:12:44	GET	http://www.acme.com:80	/admin/		200 OK	Spider

Analiza las respuestas para identificar nuevos enlaces dentro del cuerpo de la respuesta HTML o cabecera HTTP.



Extension plug-in

The screenshot shows the WebScarab application window with the 'Extensions' plug-in open. The main window displays a list of URLs and a table of request logs. The 'Extensions' window has a 'File' tab selected, showing a list of file extensions and a 'Load' button.

ID	Date	Met...	Host	Path	Parameters	Status	Origin
30	2014/03/14 08:24:27	GET	http://www.acme.com:80	/file.php.1		200 OK	Extensions
31	2014/03/14 08:24:57	GET	http://www.acme.com:80	/index.html.1		200 OK	Extensions
32	2014/03/14 08:25:04	GET	http://www.acme.com:80	/page.php.bak		200 OK	Extensions
33	2014/03/14 08:25:04	GET	http://www.acme.com:80	/page.php.copia		200 OK	Extensions
34	2014/03/14 08:25:08	GET	http://www.acme.com:80	/web-intranet.tar.gz		200 OK	Extensions
35	2014/03/14 08:25:08	GET	http://www.acme.com:80	/web-intranet.zip		200 OK	Extensions

Extensions List:

- .1
- .2
- .3
- .4
- .5
- .6
- .7
- .8
- .9
- .0
- .a
- .b
- .c
- .d
- .e
- .f
- .g
- .aa
- .aaa
- .aaaa
- .aaaaa
- .demo
- .demo1
- .demo2
- .demo3
- .demo.txt
- .txt

Buttons: Edit Extensions, Check, Load

El plug-in “extensions” utiliza los archivos y directorios conocidos en el paso anterior para realizar una búsqueda usando un conjunto de extensiones comunes..



Manual Request plug-in

Your Shopping Cart | The Ghostly Store - OWASP Mantra

Your Shopping Cart | The G... x

www.acme.com/store_demo/

Special Offer: Take 25% o

 **THE GHOSTLY STORE**

GOODS MUSIC ART CLOTHING ACTION

 **TMA-1 Headphones - 1**
The TMA-1 headphone has been

Get shipping estimates here

Country State

Complete my purchase

All transactions are secure and encrypted, and we never store your credit card in



First Name
demo@demo.com

Credit Card Number

Expiration Date
1 - January

Card Security Cod

Subtotal \$199.00

CHECKOUT 

Continue Shopping



Manual Request plug-in

RedTie - OWASP Mantra

RedTie

www.acme.com/web-intranet/

Google

Your Company Name
Evergreen Terrace 742
Kansas Missouri
Phone: 432-653-3121
sales@thetiecompany.com

Inicio | Login | Intranet

RedTie

Inicio | Nosotros | Productos | Servicios | Contactenos

Submenu 1 | Submenu 2 | Submenu 3 | Submenu 4 | Submenu 5

Login Usuarios

Usuario : Usuario01 || contraseña : clave1234 || Acceso : Legal
Usuario : Usuario02 || contraseña : clave1234 || Acceso : Finanzas
Usuario : Usuario03 || contraseña : ***** || Acceso : Logistica



Fuzzer plug-in

WebScarab

SessionID Analysis | Scripted | Fragments | Fuzzer | Compare | Search | SAML | OpenID | WS-Federation | Identity

Summary | Messages | Proxy | Manual Request | Spider | Extensions

Tree Selection filters conversation list

Url	Methods	Status	Possible I...	Injection
http://www.acme.com:80/	GET			
file.php	GET			
file.php.1	GET			
images/	GET			
login-user.php	GET			
news.php	GET			
page.php	GET			
page.php.bak	GET			
page.php.copia	GET			
reset_pass_exec.php	GET			
web-intranet.tar	GET			
web-intranet.tar.gz	GET			

Method URL

GET http://www.acme.com:80/reset_pass_exec.php

Header	Value
Host	www.acme.com
User-Agent	Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate

ID	Date	Met...	Host	Accept-Encoding
29	2014/03/14	GET	w.acme.c	Accept-Encoding
28	2014/03/14	GET	w.acme.c	Accept-Encoding
27	2014/03/14	GET	w.acme.c	Accept-Encoding
26	2014/03/14	GET	w.acme.c	Accept-Encoding
25	2014/03/14	GET	w.acme.c	Accept-Encoding
24	2014/03/14	GET	w.acme.c	Accept-Encoding
23	2014/03/14	GET	w.acme.c	Accept-Encoding
22	2014/03/14	GET	w.acme.c	Accept-Encoding
21	2014/03/14 09:57:07	GET	http://www.acme.c	Accept-Encoding
20	2014/03/14 09:57:07	GET	http://www.acme.c	Accept-Encoding
19	2014/03/14 09:57:07	GET	http://www.acme.c	Accept-Encoding

Parameters

Location	Name	Type	Value	Priority	Fuzz Source
Query	user_nick	STRING	jperez	0	
Query	user_code	STRING	123456	0	code_list

Total Requests : 4

Current Request : 4

Sources Start Stop

ID	Date	Met...	Host	Path	Parameters	Size	9
32	2014/03/14 10:00:43	GET	http://www.acme.com:80	/reset_pass_exec.php	?user_nick=jperez&user_code=12345678	2523	20
33	2014/03/14 10:00:43	GET	http://www.acme.com:80	/reset_pass_exec.php	?user_nick=jperez&user_code=123456	2861	20
35	2014/03/14 10:00:43	GET	http://www.acme.com:80	/reset_pass_exec.php	?user_nick=jperez&user_code=654321	2523	20
34	2014/03/14 10:00:43	GET	http://www.acme.com:80	/reset_pass_exec.php	?user_nick=jperez&user_code=1234567	2523	20



Fuzzer plug-in

RedTie

www.redtie.com/reset_pass.php

Your Company Name
Evergreen Terrace 742
Kansas Missouri
Phone: 432-653-3121
sales@thetiecompany.com

Inicio | Login |

Inicio | Nosotros | Productos | Servicios | Con

Submenu 1 | Submenu 2 | Submenu 3 | Submenu 4 | Su



Recuperación de Contraseña

Usuario o Correo :

COMPOSE

- Inbox (842)**
Important
Chats
Sent Mail
- Drafts (1,132)**
- Spam (157)**
[Imap]/Drafts
[Imap]/Sent
[Imap]/Trash (275)

71ef22

Bridge Java and .NET - www.codemesh.com - Extreme performance, trivial deployment, drop

ACME.COM > Password Recovery Inbox x

 **Mauricio Urizar** <mauricio.urizar@gmail.com> 4:02 AM (0 minu

to Mauricio ▾

Haga click en el siguiente enlace para completar el proceso de cambio de contraseña .

[CAMBIAR CONTRASEÑA](#)



WEBSCARAB + SQLMAP !!

```
root@hackstation: ~/Download x root@hackstation: ~/OWASP-We... x root@hackstation: ~/Download/sq... x
root@hackstation:~/Download/sqlmap-dev# python sqlmap.py -l /root/OWASP-WebScarab_Press/report_to_sqlmap/reporte2012/conversations/ --batch --dbms=mysql --dbs

sqlmap/1.0-dev-97f603a - automatic SQL injection and database takeover tool
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 10:22:52

[10:22:52] [INFO] sqlmap parsed 13 (parameter unique) requests from the targets list ready to be tested
[10:22:52] [INFO] sqlmap got a total of 13 targets
URL 1:
GET http://www.acme.com:80/page.php?seccion=Inicio
do you want to test this URL? [Y/n/q]
> Y
[10:22:52] [INFO] testing URL 'http://www.acme.com:80/page.php?seccion=Inicio'
[10:22:52] [INFO] using '/root/Download/sqlmap-dev/output/results-03142014_1022am.csv' as the CSV results file in multiple targets mode
[10:22:52] [INFO] testing connection to the target URL
[10:22:52] [INFO] testing if the target URL is stable. This can take a couple of seconds
[10:22:53] [WARNING] user aborted in multiple target mode
do you want to skip to the next target in list? [Y/n/q] Y
URL 2:
GET http://www.acme.com:80/news.php?id=1
```



OWASP

The Open Web Application Security Project

<http://www.owasp.org>

info@owasp.org

**PREGUNTAS Y/O
COMENTARIOS**

Mauricio Urizar
murizar@open-sec.com