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

Mauricio Urizar

murizar@open-sec.com

@MauricioUrizar

- 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)

Los consultores...

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 comunique 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)

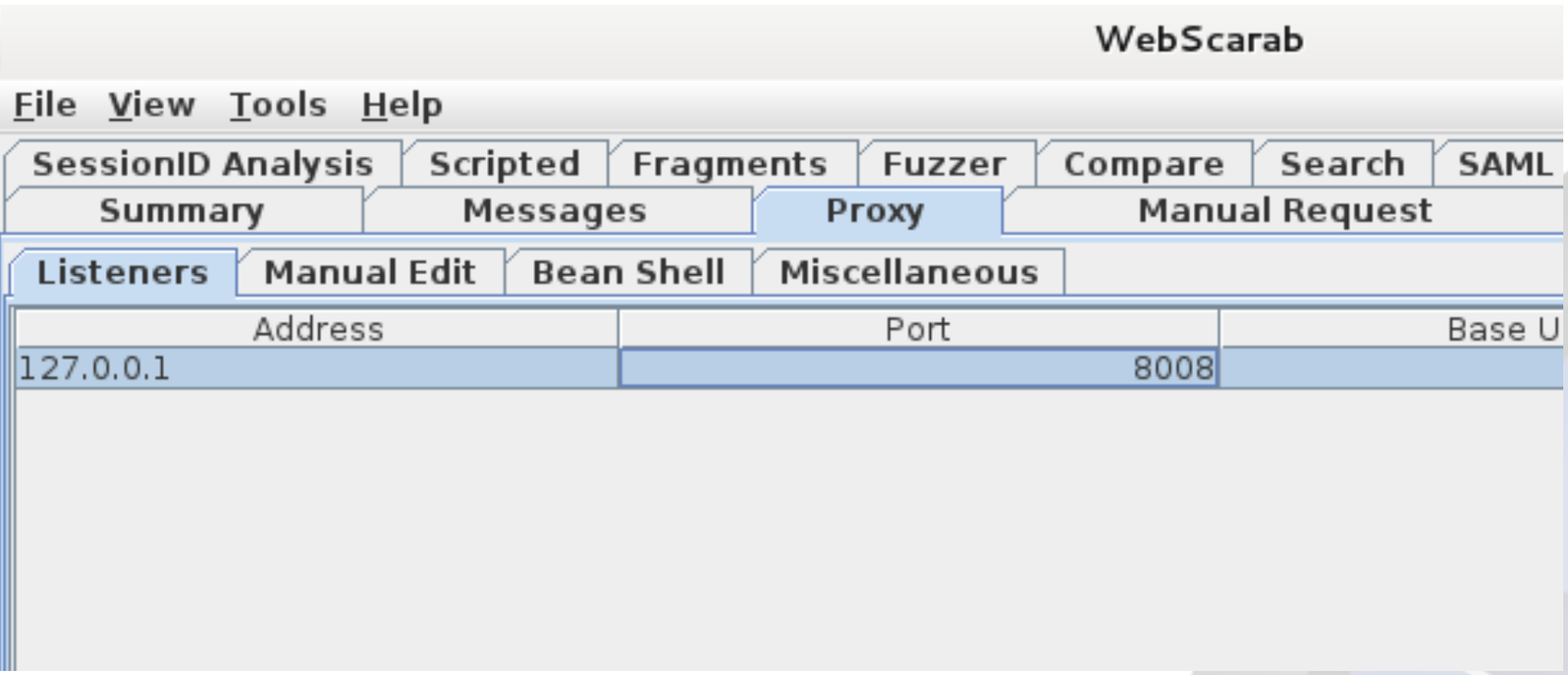
Aplicación Web

Como corro Webscarab?

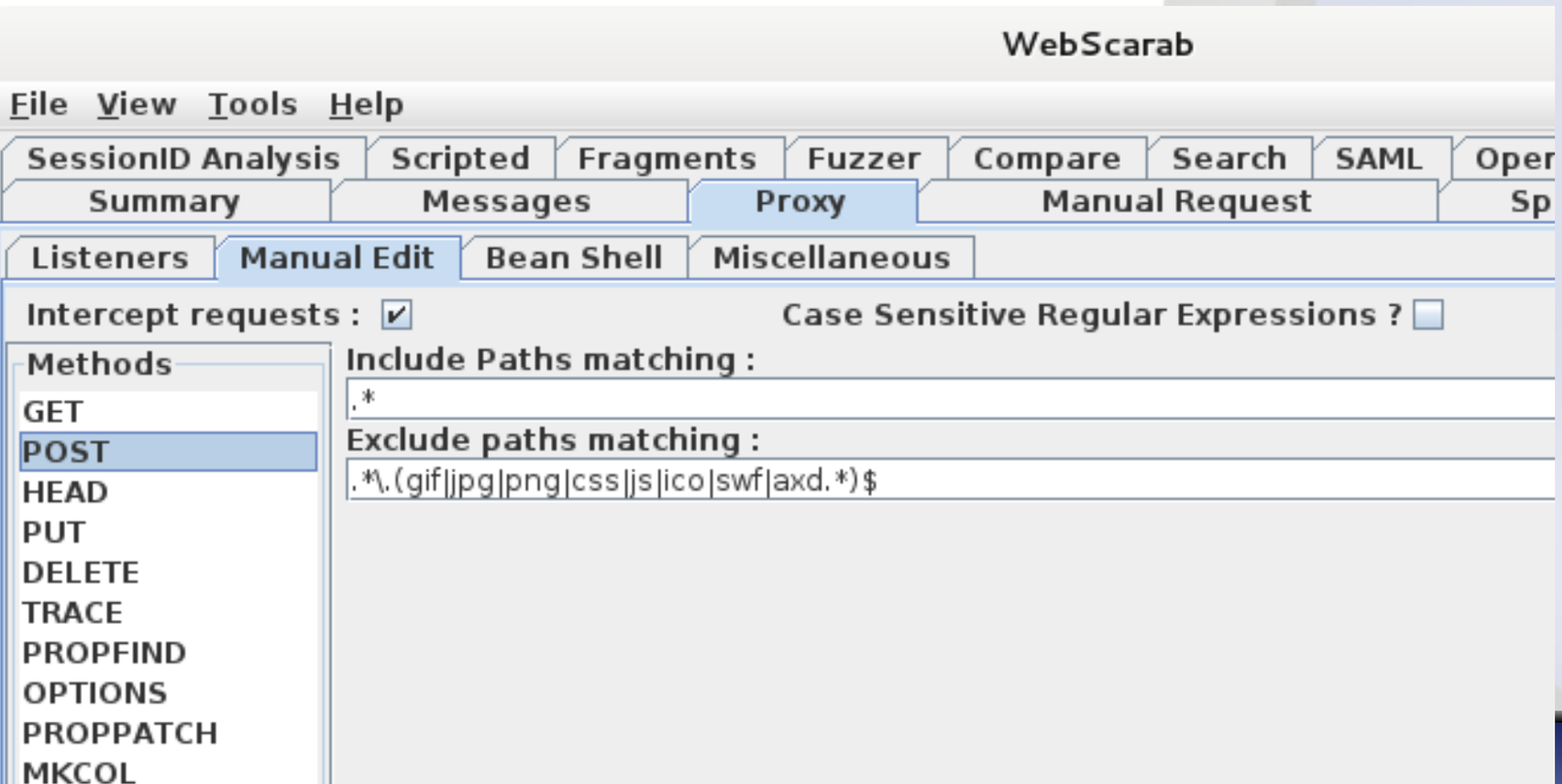
Ejecutemos el archivo**“.jar”**de la siguiente forma.

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

Configurando Webscarab

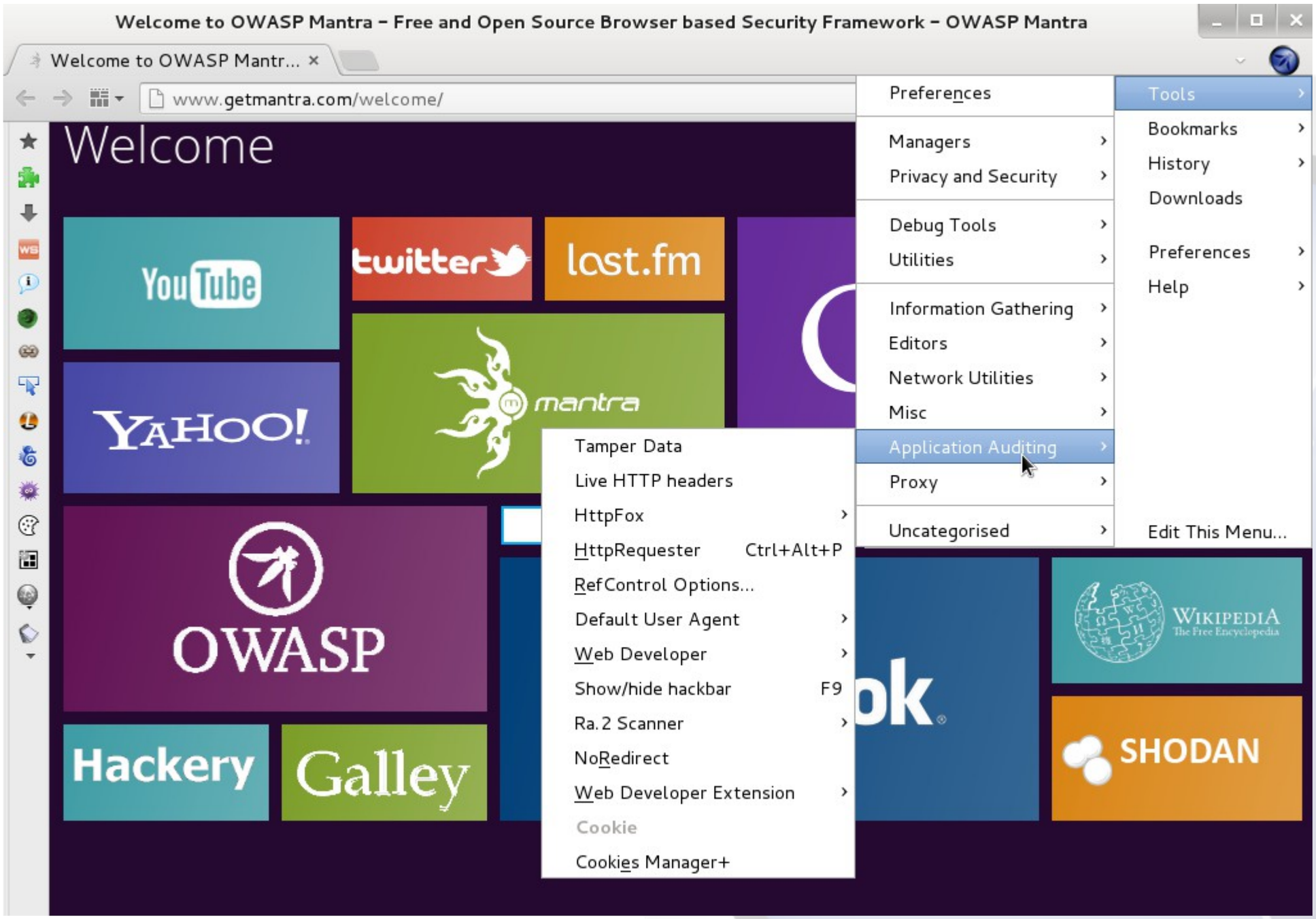


Puerto en escucha, el mismo que se configura en el navegador..



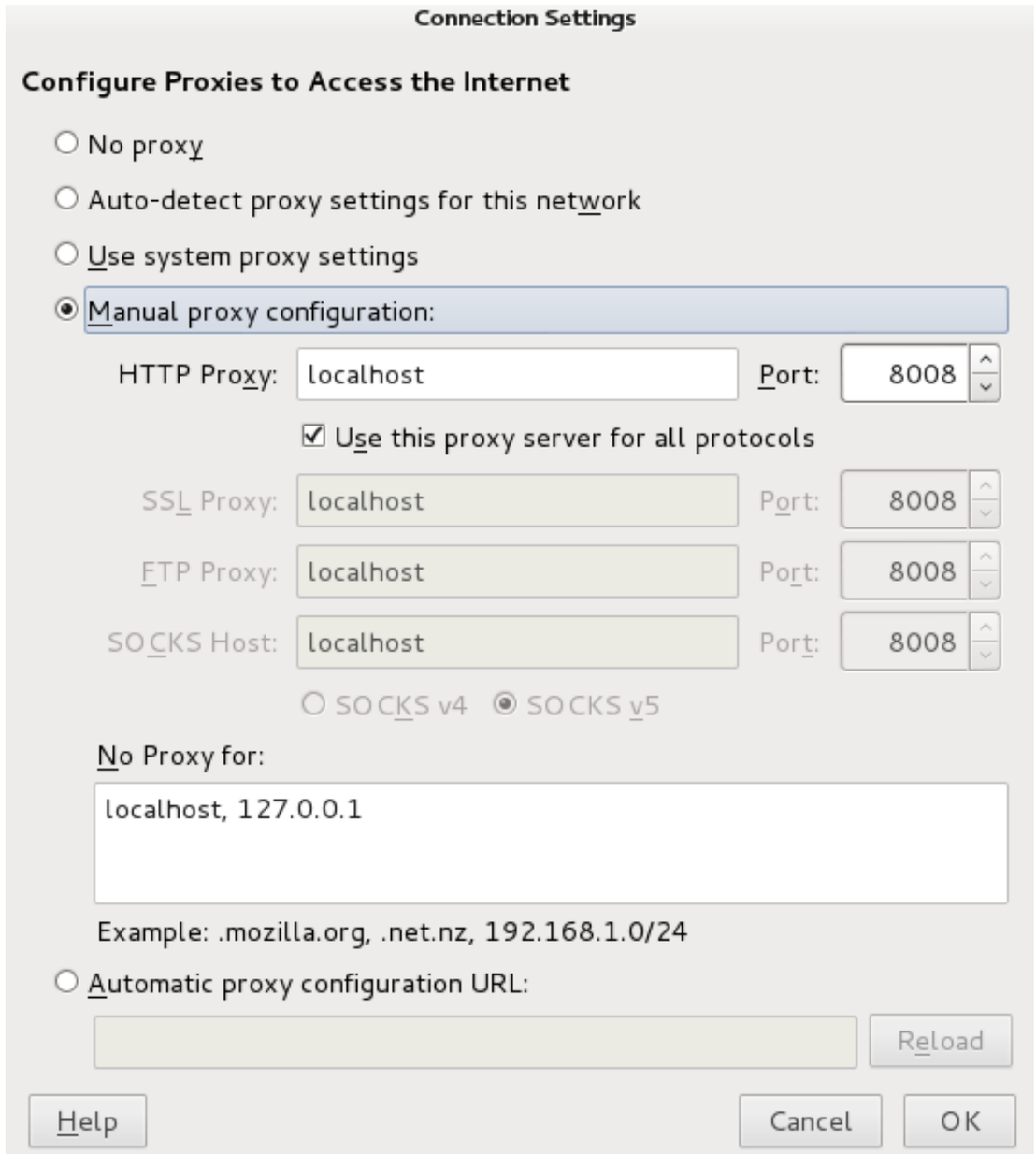
Interceptar solo peticiones POST (formularios web)

Configurando Navegador



http://www.getmantra.com/

Configurando Navegador



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

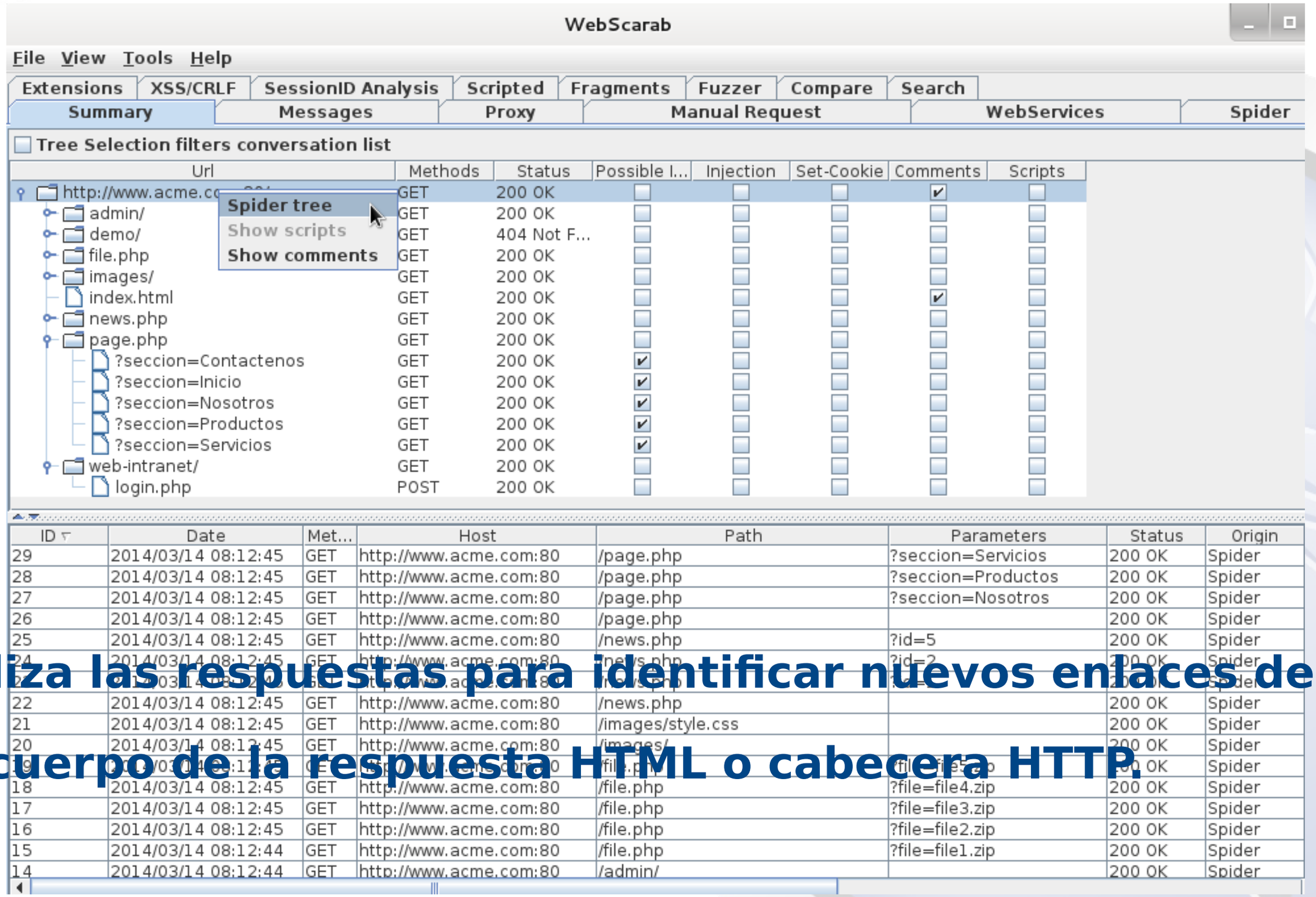
Summary | Messages | Proxy | Manual Request | WebServices

☐ Tree Selection filters conversation list

Url	Methods	Status	Possible I...	Injection	Set-Cookie	Comments	Scripts
http://www.acme.com:80/			☐	☐	☐	☐	☐
admin/			☐	☐	☐	☐	☐
index.html	GET	200 OK	☐	☐	☐	☑	☐
page.php			☐	☐	☐	☐	☐
?seccion=Contactenos	GET	200 OK	☑	☐	☐	☐	☐
?seccion=Inicio	GET	200 OK	☑	☐	☐	☐	☐
web-intranet/	GET	200 OK	☐	☐	☐	☐	☐
login.php	POST	200 OK	☐	☐	☐	☐	☐

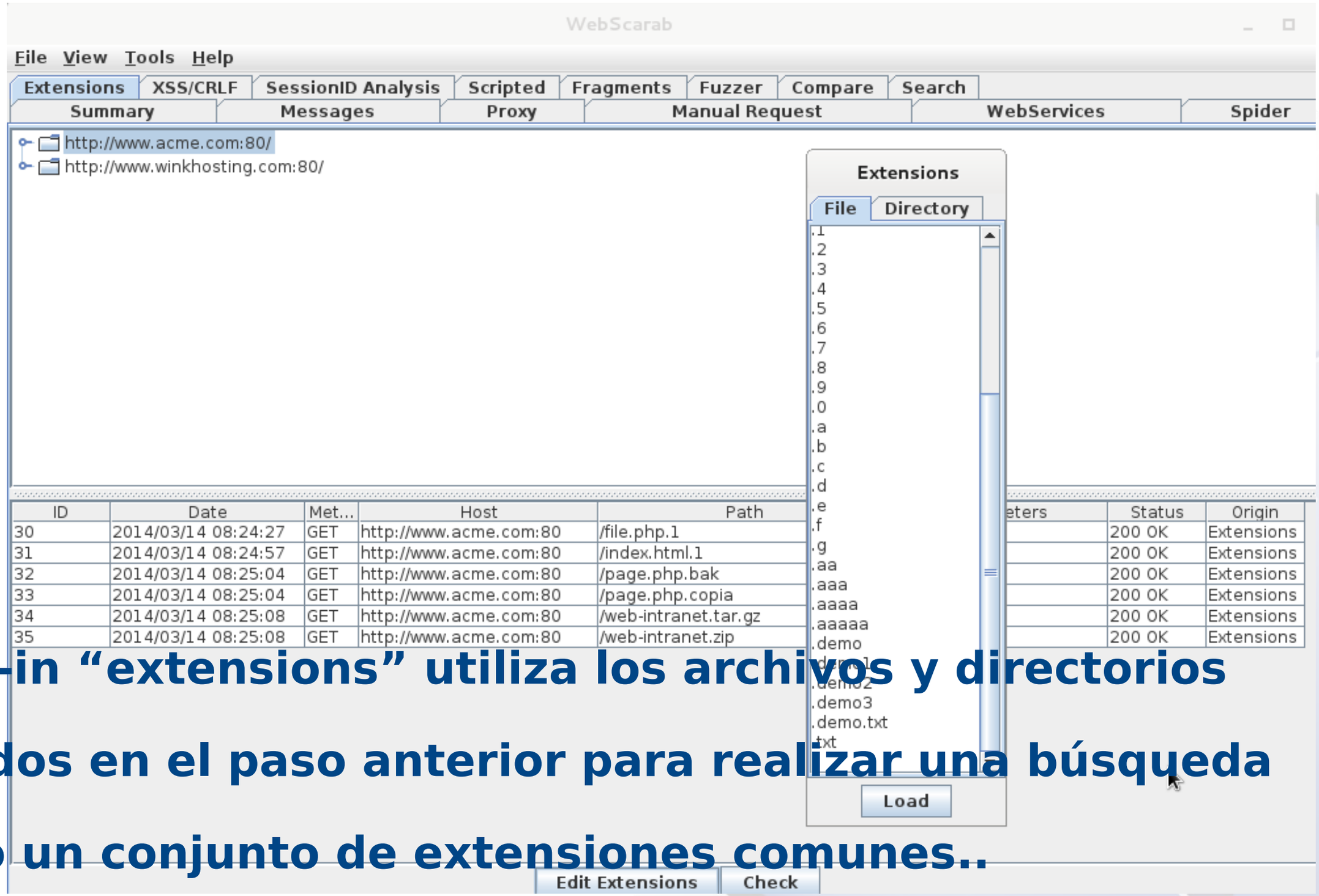
ID	Date	Met...	Host	Path	Parameters
9	2014/03/14 07:52:49	POST	http://www.acme.com:80	/web-intranet/login.php	
8	2014/03/14 07:52:38	GET	http://www.acme.com:80	/admin/images/bg_submenu.gif	
7	2014/03/14 07:52:38	GET	http://www.acme.com:80	/admin/images/bg_menu.gif	
6	2014/03/14 07:52:38	GET	http://www.acme.com:80	/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



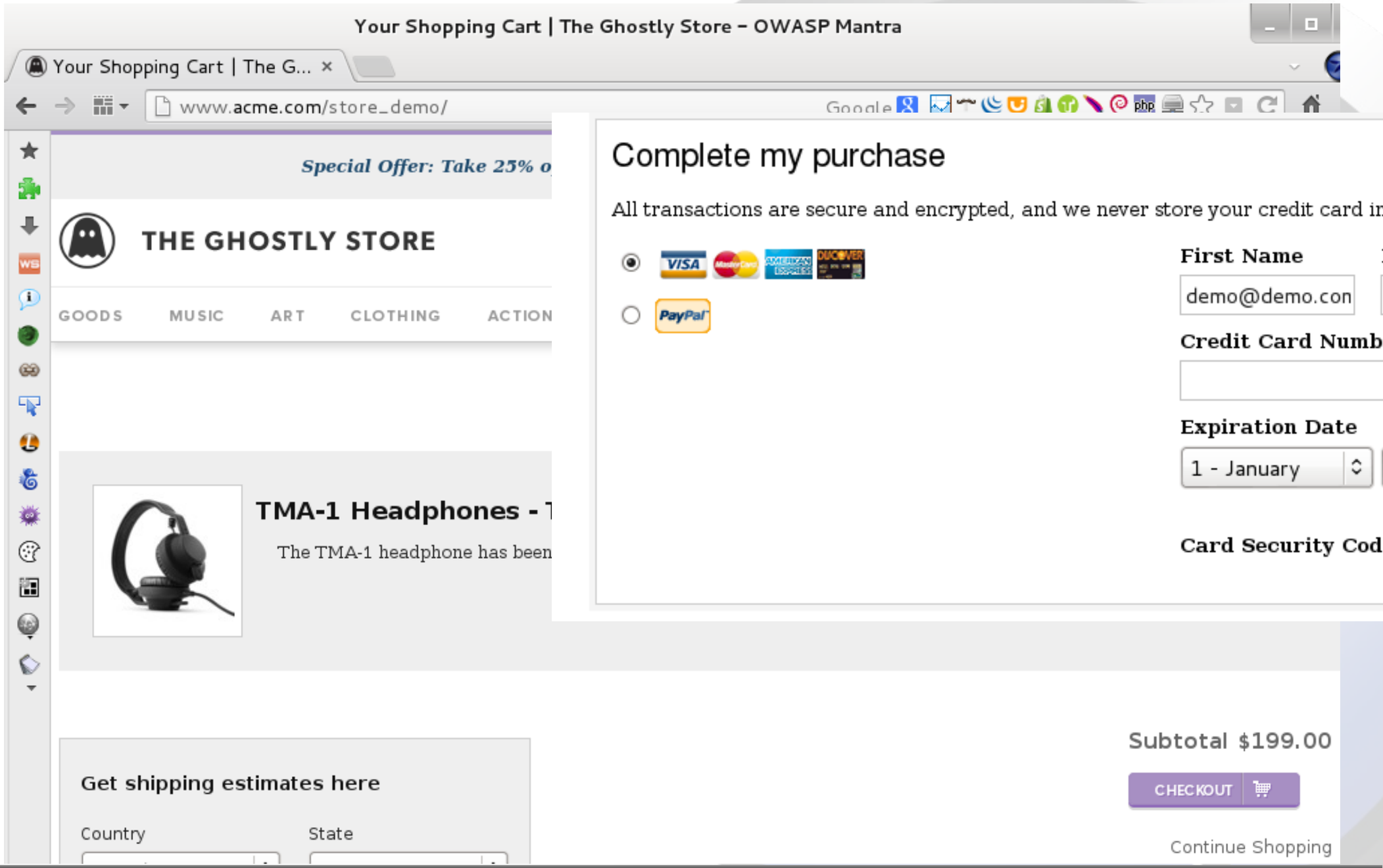
Analiza las respuestas para identificar nuevos enlaces dentro del cuerpo de la respuesta HTML o cabecera HTTP.

Extension plug-in

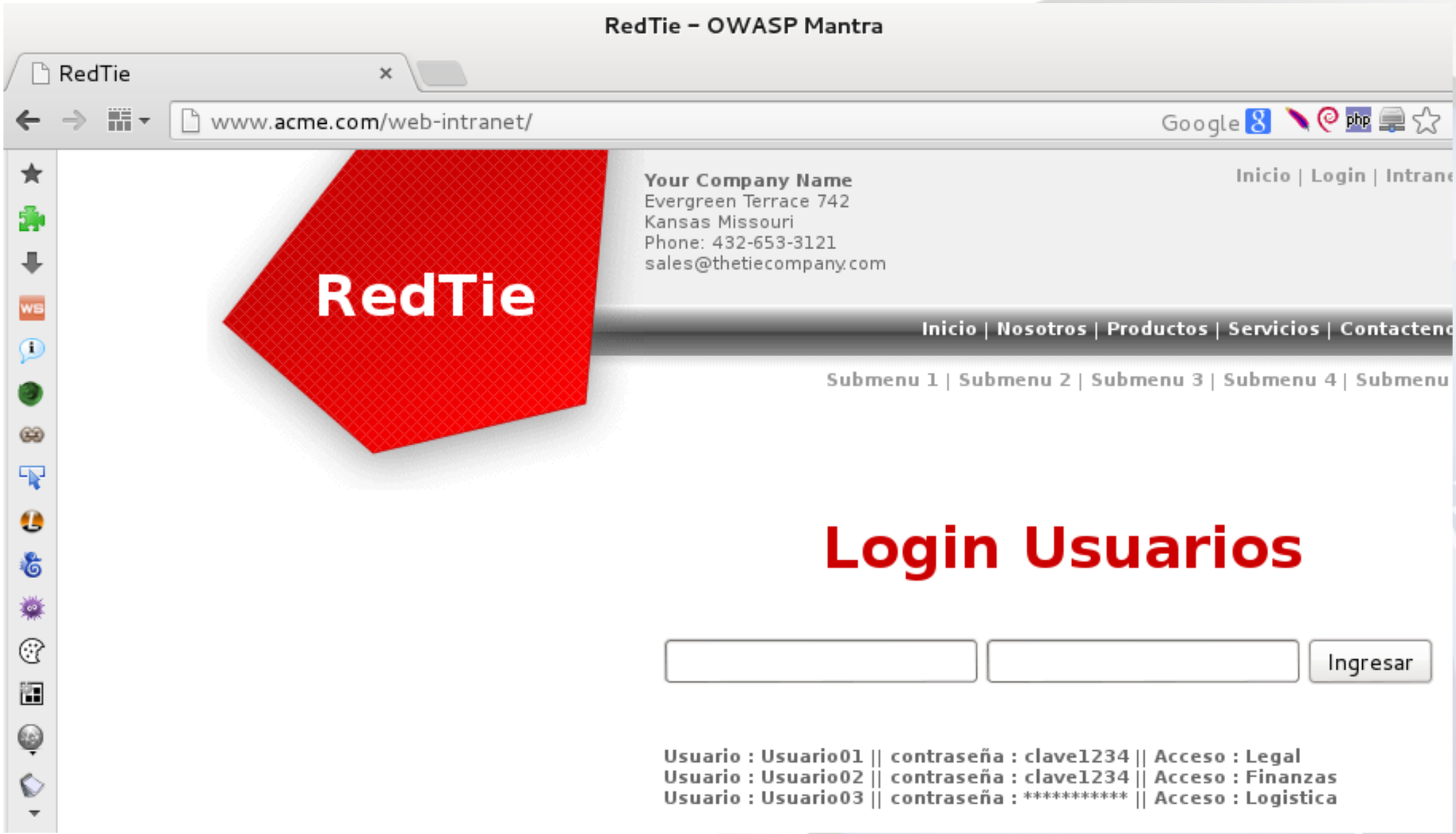


El plug-in “extensions” utiliza los archivos y directorios conocidos en el paso anterior para realizar una búsqueda usando un conjunto de extensiones comunes..

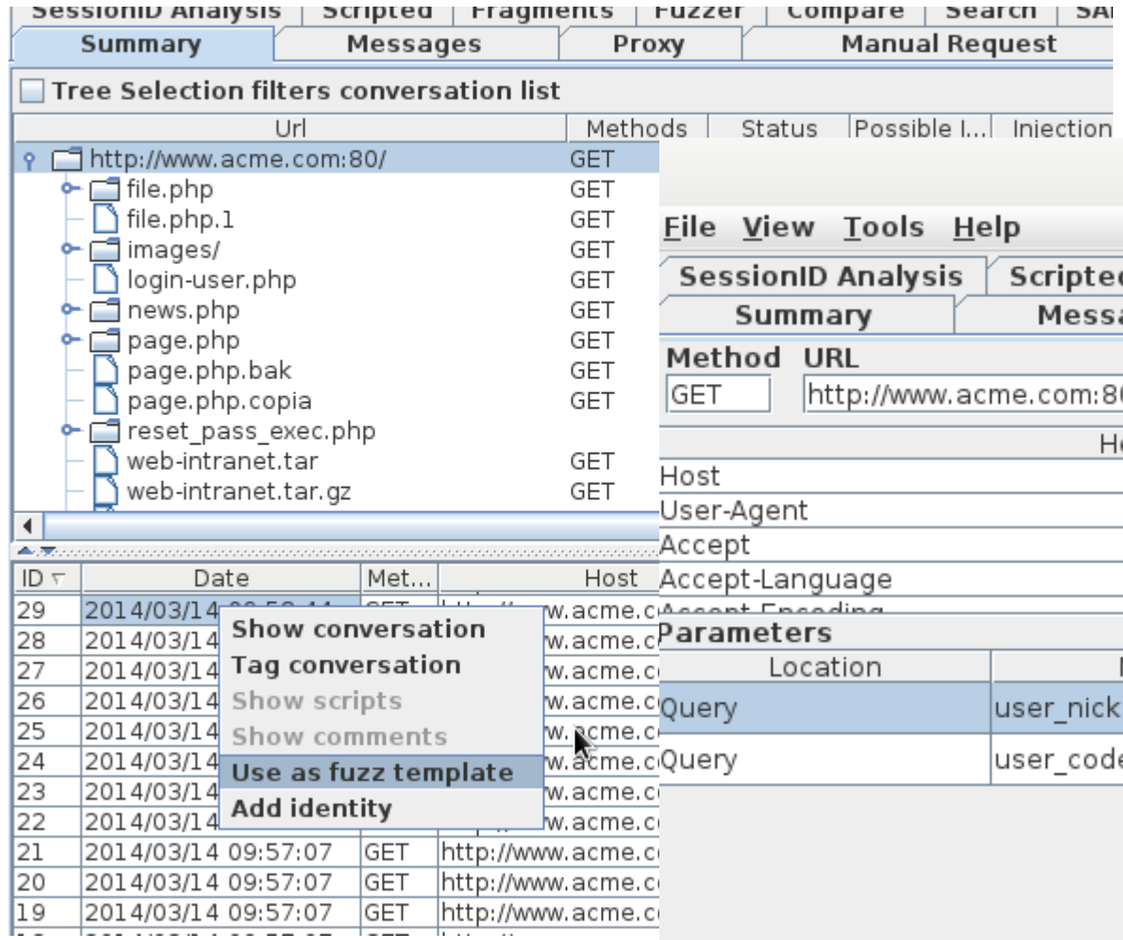
Manual Request plug-in

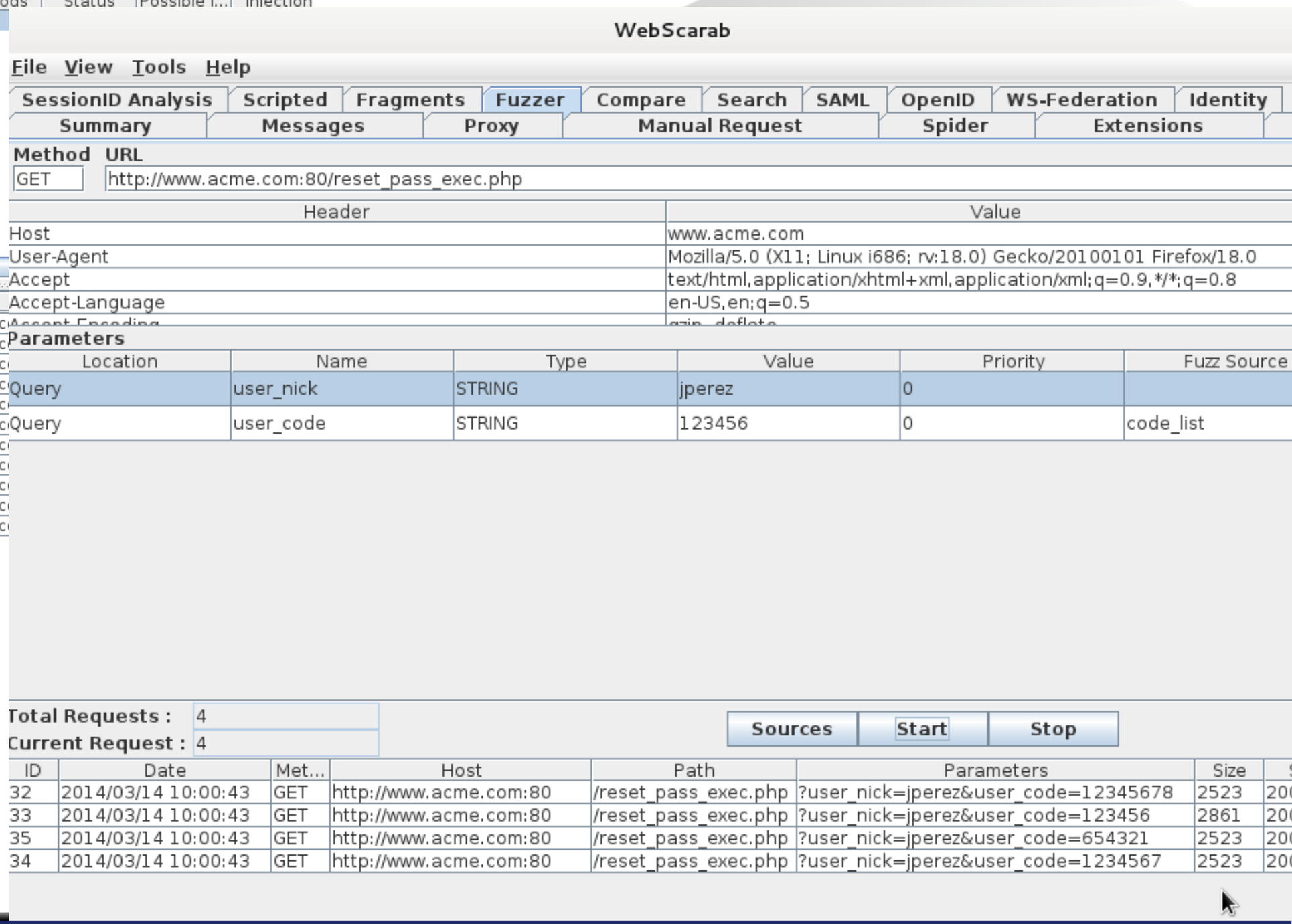


Manual Request plug-in

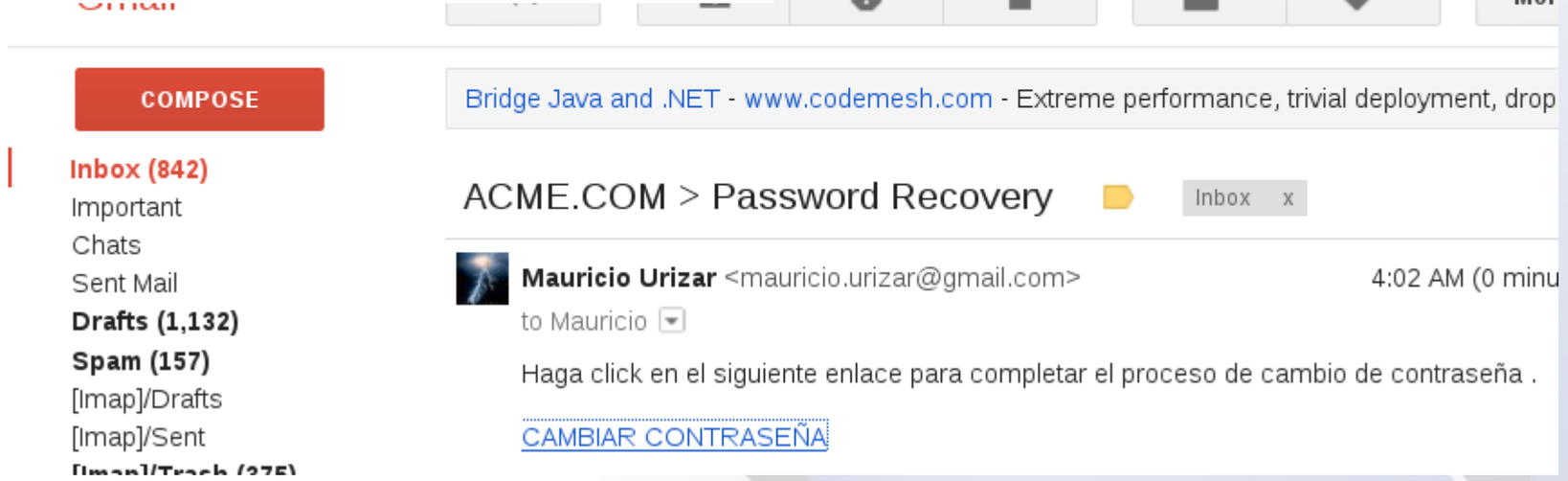


Fuzzer plug-in





Fuzzer plug-in



WEBSCARAB + SQLMAP !!

root@hackstation: ~/Download | root@hackstation: ~/OWASP-We... | root@hackstation: ~/Download/sq...

```
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 rea
dy 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' a
s 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

PREGUNTAS Y/O COMENTARIOS

Mauricio Urizar

murizar@open-sec.com