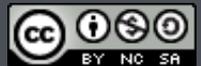


Jornadas “Espacios de Ciberseguridad”

Fundamentos del análisis de sitios Web

www.incibe.es

INSTITUTO NACIONAL DE
CIBERSEGURIDAD
NATIONAL CYBERSECURITY
INSTITUTE OF SPAIN



Esta presentación se publica bajo licencia Creative Commons del tipo:
Reconocimiento – No comercial – Compartir Igual
<http://creativecommons.org/licenses/by-nc-sa/4.0/>

Índice

1. INCIBE - ¿Qué es?

2. Introducción a la ciberseguridad

3. Objetivos del curso

4. Introducción

5. Fundamentos de comunicaciones

6. Análisis de vulnerabilidades

7. Explotación de vulnerabilidades

8. Seguridad en aplicaciones web

9. Actividades prácticas

10. Otros datos de interés

INCIBE - ¿Qué es?

El Instituto Nacional de Ciberseguridad de España (**INCIBE**) es una sociedad dependiente del Ministerio de Industria, Energía y Turismo (**MINETUR**) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (**SETSI**).

INCIBE es la entidad de referencia para el desarrollo de la **ciberseguridad** y de la **confianza digital** de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos (Agenda Digital para España, aprobada en Consejo de Ministros el 15 de Febrero de 2012).

Como **centro de excelencia**, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia , INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

www.incibe.es



INCIBE - ¿Qué es?

Pilares fundamentales sobre los que se apoya la actividad de INCIBE

- **Prestación de servicios** de protección de la privacidad, prevención y reacción a incidentes en ciberseguridad
- **Investigación** generación de inteligencia y mejora de los servicios
- **Coordinación** colaboración con entidades públicas y privadas, nacionales e internacionales

Área de Operaciones



I+D+i y Promoción del Talento en Ciberseguridad

Fomento del Ecosistema de I+D+i en Ciberseguridad

“...INCIBE como Centro de Excelencia impulsa el ecosistema nacional de I+D+i en Ciberseguridad...”

Enfoque **INTEGRADO** de la I+D+i

- Análisis y diagnóstico de la Investigación en Ciberseguridad (**Conocimiento** de las actividades que se llevan a cabo, contar con los **investigadores** como activo principal y tener **infraestructuras**)
- Red de Centros de Excelencia en I+D+i en Ciberseguridad (Plan Director e inteligencia colectiva) a través del lanzamiento de la **Agenda Estratégica Nacional I+D+i en Ciberseguridad**

Mejor **ENFOQUE** y coordinación

- Agenda Estratégica Nacional I+D+i en Ciberseguridad (programas nacionales I+D)
- Agenda Estratégica Internacional I+D+i Comisión Europea (**NIS WG3**) (programa internacional H2020)

Resultados **orientados a Negocio**

- SPIN-OFF / SPIN-UP.
- Lanzaderas / incubadoras / aceleradoras de START-UPs.
- Capital semilla / Capital riesgo (VC).
- Transferencia de conocimiento a la industria
(capital humano investigador y adquisición de patentes).

Enfoque basado en la **INTERNACIONALIZACIÓN** desde el inicio



I+D+i y Promoción del Talento en Ciberseguridad

Mejores prácticas en la Gestión del Talento en Ciberseguridad

“...INCIBE como Centro de Excelencia impulsa la alta capacitación de profesionales en el ámbito de la Ciberseguridad”

Enfoque **INTEGRADO**

- Itinerarios educativos en Ciberseguridad (alineado con la demanda del sector).
- Coherente a todos los niveles (FP, Grado y Máster y Pre-doctorales y Post-doctorados).
- Iniciativas para la gestión de talento: **atracción, detección, promoción y retención.**



Mejor **ENFOQUE**

- Análisis del GAP entre los itinerarios educativos vs. oferta formativa vs. Iniciativas para la gestión del talento.
- Acciones:
 - **Detección:** Retos tipo pruebas de habilidad.
 - **Atracción:** Formación avanzada y ponentes / premios / reconocimientos / ofertas de empleo.
 - **Promoción:** Reorientación / Nuevos Contenidos prácticos (aspectos técnicos en profundidad para todos los itinerarios educativos) / Formación para jóvenes en ciberseguridad (“Espacios” de Ciberseguridad).
 - **Atracción / Retención:** Financiación de apoyo una vez identificado el talento.

Enfoque basado en la **INTERNACIONALIZACIÓN** desde el inicio buscando su residencia en España

I+D+i y Promoción del Talento en Ciberseguridad

Oportunidad para una acción global que estimule la
Industria Española de Ciberseguridad

“...INCIBE como Centro de Excelencia impulsa la competitividad de la Industria nacional de Ciberseguridad en base a un modelo de colaboración público-privada (PPP): Polo de Ciberseguridad ...”

Enfoque **INTEGRADO**

- Potenciar el tejido empresarial español en ciberseguridad.
- Renovar la imagen del sector.
- Guiar la innovación y comercialización de nuevos productos/servicios a la demanda nacional/internacional.
- Mejorar el posicionamiento y la comercialización de la industria de la ciberseguridad española.
- Aumentar la actividad productiva competitiva de los participantes a nivel internacional.

Mejor **ENFOQUE**

- Facilitar un **pensamiento estratégico conjunto** para identificar ventajas competitivas y diferenciación.
- Definición de **acciones colectivas** para abordar los desafíos estratégicos.
- **Priorización e implementación rápida** de las acciones identificadas.
- Fomento de una **colaboración público-privada** con los principales actores de la industria.
- Definición de un **modelo de gobierno** que permite una **sostenibilidad** a largo plazo.

Resultados orientados a NEGOCIO

- Acceso a nuevos mercados.
- Innovación.
- Demanda sofisticada, certificación y la concienciación.
- Financiación.



Índice

1. INCIBE - ¿Qué es?
- 2. Introducción a la ciberseguridad**
3. Objetivos del curso
4. Introducción
5. Fundamentos de comunicaciones
6. Análisis de vulnerabilidades
7. Explotación de vulnerabilidades
8. Seguridad en aplicaciones web
9. Actividades prácticas
10. Otros datos de interés

Introducción a la ciberseguridad

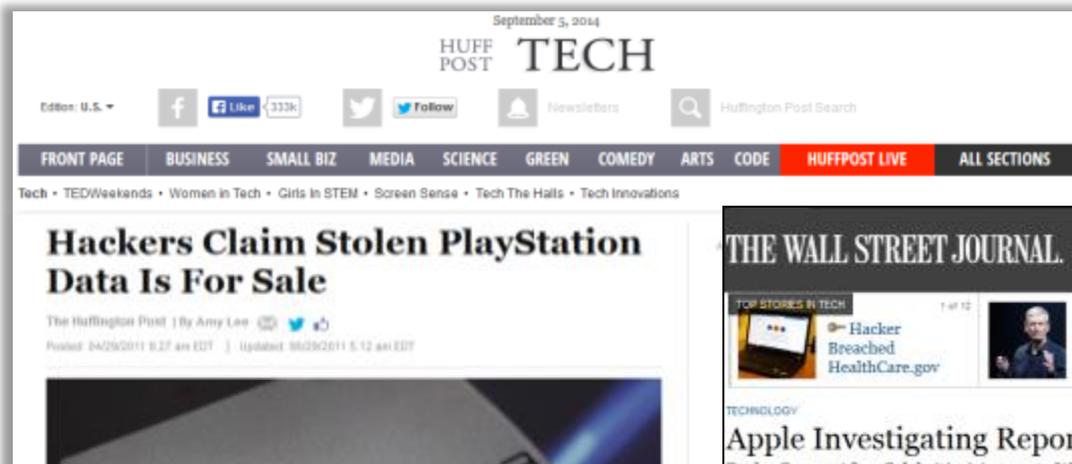
Evolución de las Tecnologías de la Información

- La **información** es uno de los principales activos de una empresa.
- Las empresas almacenan y gestionan la información en los **Sistemas de Información**.
- Para una empresa resulta fundamental proteger sus Sistemas de Información para que su información esté a salvo. Dificultades:
 - El entorno donde las empresas desarrollan sus actividades es cada vez más complejo debido al desarrollo de las tecnologías de información y otros factores del entorno empresarial
 - El perfil de un ciberdelincuente de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar) en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede llegar a ser.
- Es fundamental poner los medios técnicos y organizativos necesarios para garantizar la seguridad de la información. Para lograrlo hay que garantizar la **confidencialidad**, **disponibilidad** e **integridad** de la información.



Introducción a la ciberseguridad

Casos notorios



Bonopark denunciará los ataques al sistema informático de BiciMad



Introducción a la ciberseguridad

Seguridad de la Información

La seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información:

- La **confidencialidad** es la propiedad de prevenir la divulgación de información a personas no autorizadas.
- La **integridad** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- La **disponibilidad** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- La **autenticidad**: la información es lo que dice ser o el transmisor de la información es quien dice ser.
- El **no repudio**: Estrechamente relacionado con la Autenticidad. Permite, en caso de ser necesario, que sea posible probar la autoría u origen de una información.



Introducción a la ciberseguridad

Riesgos para los Sistemas de Información

¿Qué son los riesgos en los sistemas de información?

- Las amenazas sobre la información almacenada en un sistema informático.

Ejemplos de riesgos en los sistemas de información

- **Daño físico:** fuego, agua, vandalismo, pérdida de energía y desastres naturales.
- **Acciones humanas:** acción intencional o accidental que pueda atentar contra la productividad.
- **Fallos del equipamiento:** fallos del sistema o dispositivos periféricos.
- **Ataques internos o externos:** hacking, cracking y/o cualquier tipo de ataque.
- **Pérdida de datos:** divulgación de secretos comerciales, fraude, espionaje y robo.
- **Errores en las aplicaciones:** errores de computación, errores de entrada, etc.



Introducción a la ciberseguridad

La figura del HACKER

¿Qué es un hacker?

Experto en seguridad informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

¿Qué tipos de hackers existen en función de los objetivos que tienen?



Black Hat Hackers: Suelen quebrantar la seguridad de un sistema o una red con fines maliciosos.



White Hat Hackers: normalmente son los que penetran la seguridad de los sistemas bajo autorización para encontrar vulnerabilidades. Suelen ser contratados por empresas para mejorar la seguridad de sus propios sistemas.



Gray (Grey) Hat Hackers: Son una mezcla entre los dos anteriores puesto que tienen una ética ambigua. Normalmente su cometido es penetrar en sistemas de forma ilegal para luego informar a la empresa víctima y ofrecer sus servicios para solucionarlo.

Introducción a la ciberseguridad

Clases de ataques

- **Interrupción:** se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.
- **Intercepción:** se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.
- **Modificación:** se trata de modificar la información sin autorización alguna.
- **Fabricación:** se crean productos, tales como páginas web o tarjetas magnéticas falsas.



Introducción a la ciberseguridad

Técnicas de hacking

- **Spoofing:** se suplanta la identidad de un sistema total o parcialmente.
- **Sniffing:** se produce al escuchar una red para ver toda la información transmitida por ésta.
- **Man in the middle:** siendo una mezcla de varias técnicas, consiste en interceptar la comunicación entre dos interlocutores posicionándose en medio de la comunicación y monitorizando y/o alterando la comunicación.
- **Malware:** se introducen programas dañinos en un sistema, como por ejemplo un virus, un keylogger (herramientas que permiten monitorizar las pulsaciones sobre un teclado) o rootkits (herramientas que ocultan la existencia de un intruso en un sistema).
- **Denegación de servicio:** consiste en la interrupción de un servicio sin autorización.
- **Ingeniería social:** se obtiene la información confidencial de una persona u organismo con fines perjudiciales. El Phishing es un ejemplo de la utilización de ingeniería social, que consigue información de la víctima suplantando la identidad de una empresa u organismo por internet. Se trata de una práctica muy habitual en el sector bancario.
- Adicionalmente existen multitud de ataques como **XSS**, **CSRF**, **SQL injection**, etc.

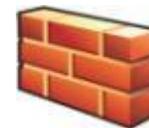
Introducción a la ciberseguridad

Mecanismos de defensa

Ante esta figura, ¿cómo pueden protegerse las compañías con las nuevas tecnologías?

Los principales sistemas y más conocidos son los siguientes:

- **Firewall:** sistemas de restricción de tráfico basado en reglas.
- **Sistemas IDS / IPS:** sistemas de monitorización, detección y/o prevención de accesos no permitidos en una red.
- **Honeypot:** equipos aparentemente vulnerables diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.
- **SIEM:** sistemas de correlación de eventos y generación de alertas de seguridad.
- **Antimalware:** sistemas de detección de malware informático.



Introducción a la ciberseguridad



Las prácticas del taller se realizan sobre un entorno controlado.

Utilizar las técnicas mostradas en el presente taller sobre un entorno real como Internet, puede ocasionar problemas legales.

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
- 3. Objetivos del curso**
4. Introducción
5. Fundamentos de comunicaciones
6. Análisis de vulnerabilidades
7. Explotación de vulnerabilidades
8. Seguridad en aplicaciones web
9. Actividades prácticas
10. Otros datos de interés

Objetivos del curso

¿Qué vamos a aprender hoy?

- Breve introducción a las aplicaciones web.
- Arquitectura: funcionamiento de las aplicaciones web en Internet.
- Fundamentos de la seguridad web.
- Seguridad web.



¿Cómo lo vamos a aprender?

1. Teoría.
2. Práctica:
 - a. Ejercicios prácticos a lo largo de la presentación.
 - b. Prácticas finales sobre una aplicación creada para el curso

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
- 4. Introducción**
5. Fundamentos de comunicaciones
6. Análisis de vulnerabilidades
7. Explotación de vulnerabilidades
8. Seguridad en aplicaciones web
9. Actividades prácticas
10. Otros datos de interés

Introducción

Introducción a las aplicaciones web

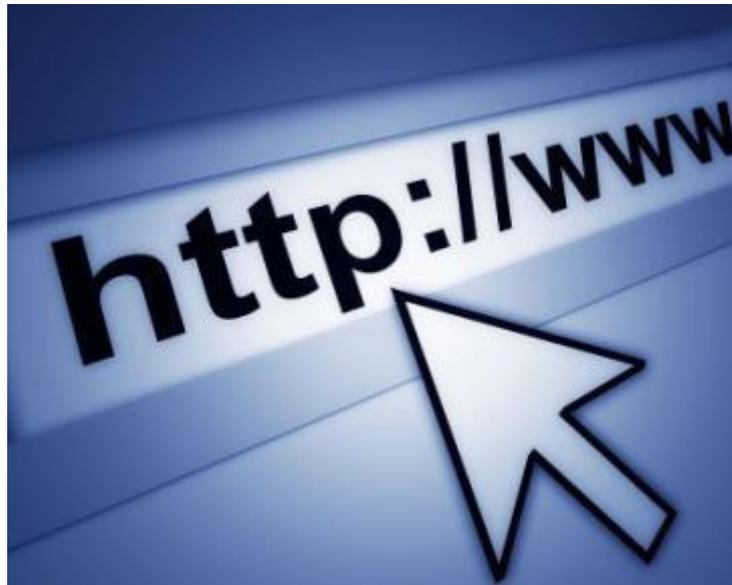
- Antes de ver los fundamentos de la seguridad web, es necesario conocer algunos de los fundamentos del funcionamiento de una aplicación web.
- Las aplicaciones web se basan en una **arquitectura cliente-servidor**, donde el cliente solicita la información y servidor es el encargado de proporcionar el contenido.
- Una **aplicación estática** sirve los recursos de forma idéntica para todas las peticiones sin procesarla, de forma que independientemente del usuario, contexto, etc., la respuesta será la misma.
- Una **aplicación dinámica** por el contrario, genera la respuesta en función de multitud de variables, consultando información de una base de datos, consultando un directorio y en general procesando la petición.

Introducción

Introducción a las aplicaciones web

- La solicitud de un recurso se realiza a través de una URL, que no es más que un localizador, una cadena de texto con un formato determinado:

<http://www.midominio.com:80/recurso.html>



Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Introducción
- 5. Fundamentos de comunicaciones**
6. Análisis de vulnerabilidades
7. Explotación de vulnerabilidades
8. Seguridad en aplicaciones web
9. Actividades prácticas
10. Otros datos de interés

Fundamentos de comunicaciones

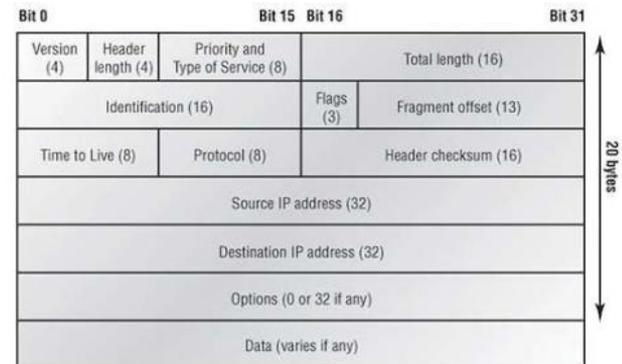
El protocolo HTTP

- El protocolo HTTP es el **conjunto de reglas** que gobierna la comunicación entre el cliente y el servidor en las distintas peticiones que se realizan en una aplicación web.
- Un protocolo es conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos para transmitir información. El protocolo especifica los aspectos como la sintaxis de los mensajes, la recuperación de errores, la sincronización, etc.
- El **protocolo HTTP** (Hypertext Transfer Protocol) es el protocolo principal de la World Wide Web y es un **protocolo sin estado** y **orientado a conexión**.
 - No mantiene estado (stateless) o, dicho de otro modo, cada transferencia de datos es una conexión diferente a la anterior, sin relación entre ellas.
 - Usa una conexión (establecida por el protocolo TCP) para garantizar el establecimiento de un canal de comunicación entre los interlocutores.

Fundamentos de comunicaciones

DNS

- El **protocolo DNS** es el conjunto de reglas que gobierna la **traducción entre direcciones IP y nombres de dominio**.
- **IP (Internet Protocol)** es uno de los protocolos fundamentales para el funcionamiento de Internet e identifica con una dirección ip a los elementos de su red.
 - El mensaje IP se forma por:
 - ✓ La cabecera → Indica todo lo necesario para que el paquete llegue a su destino
 - ✓ Los datos → Lugar donde va toda la información

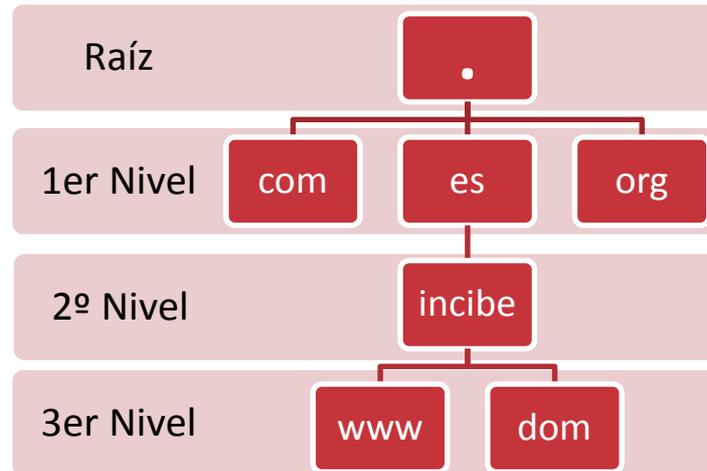


- Estas direcciones son difíciles de manejar para los humanos (especialmente en IPv6), de forma que en internet existe un sistema de traducción de nombres para identificar clientes y servidores con nombres amigables para los humanos.
 - Dirección IPv4 (32 bits): 192.168.1.10
 - Dirección IPv6 (128 bits): 2001:0db8:1234:0000:0000:0000:0000:0001

Fundamentos de comunicaciones

DNS

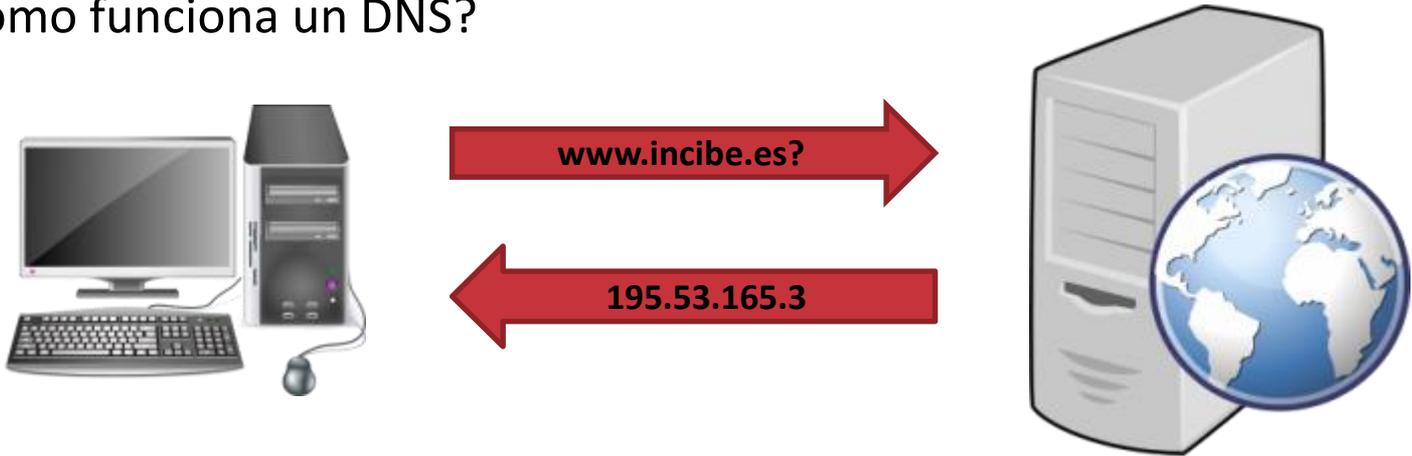
- El DNS (Domain Name System) es un conjunto de programas y protocolos para cumplir esta función de traducción.
- Originalmente se trataba de un fichero de texto (HOST.TXT) centralizado, que se distribuía periódicamente.
- Esta solución tenía infinitud de limitaciones (colisiones, escalabilidad, etc.)
- DNS surgió como una alternativa distribuida para gestionar la administración y la carga de la traducción de nombres.
- DNS utiliza una arquitectura cliente-servidor
- DNS es una base de datos: distribuida y jerárquica (estructura en árbol).



Fundamentos de comunicaciones

DNS. Funcionamiento

- ¿Cómo funciona un DNS?



```
root@EYLab: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
root@EYLab:~# host www.incibe.es  
www.incibe.es has address 195.53.165.153  
root@EYLab:~#
```

Fundamentos de comunicaciones

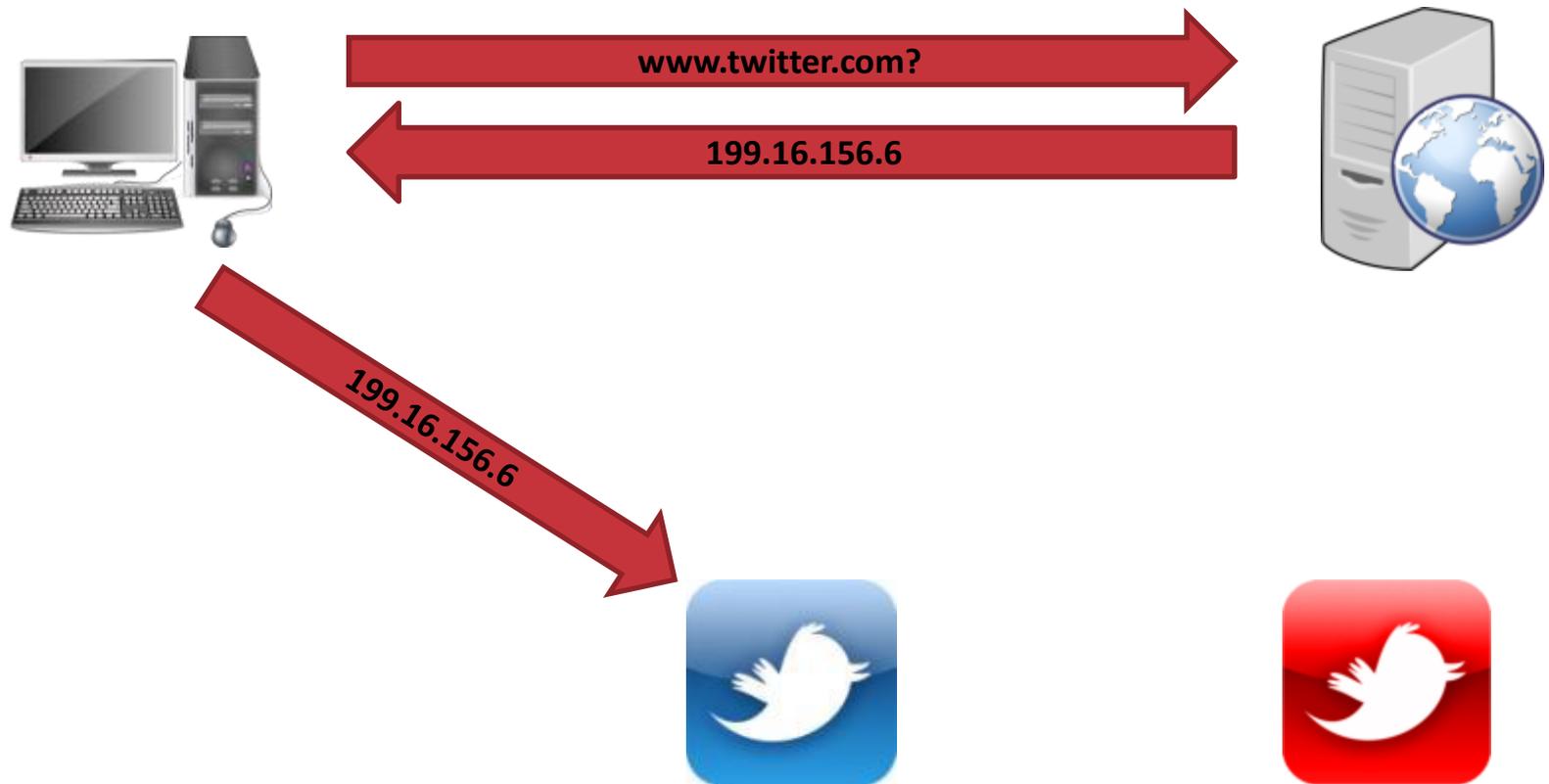
DNS. Funcionamiento

- Veamos cómo funciona este servicio con un ejemplo de navegación web:
 - Tecleamos la página web que queremos visitar en nuestro navegador favorito. En este ejemplo, visitaremos la web www.incibe.es
 - La primera acción que se realizará es comprobar si la petición www.incibe.es está almacenada en nuestro ordenador. Si la petición está almacenada se termina el proceso.
 - Si no tenemos esta información de manera local, entonces se realizará la petición a un servidor DNS. El servidor DNS, una vez recibida la petición, comprobará si la tiene almacenada en su memoria. Si la tiene almacenada, devuelve la información y el proceso termina.
 - En el caso que el servidor DNS no tuviera almacenada nuestra petición entonces lo que haría sería consultar otro servidor DNS y de manera sucesiva, un servidor final nos devolverá la dirección IP del dominio de www.incibe.es

Fundamentos de comunicaciones

DNS. Ataques

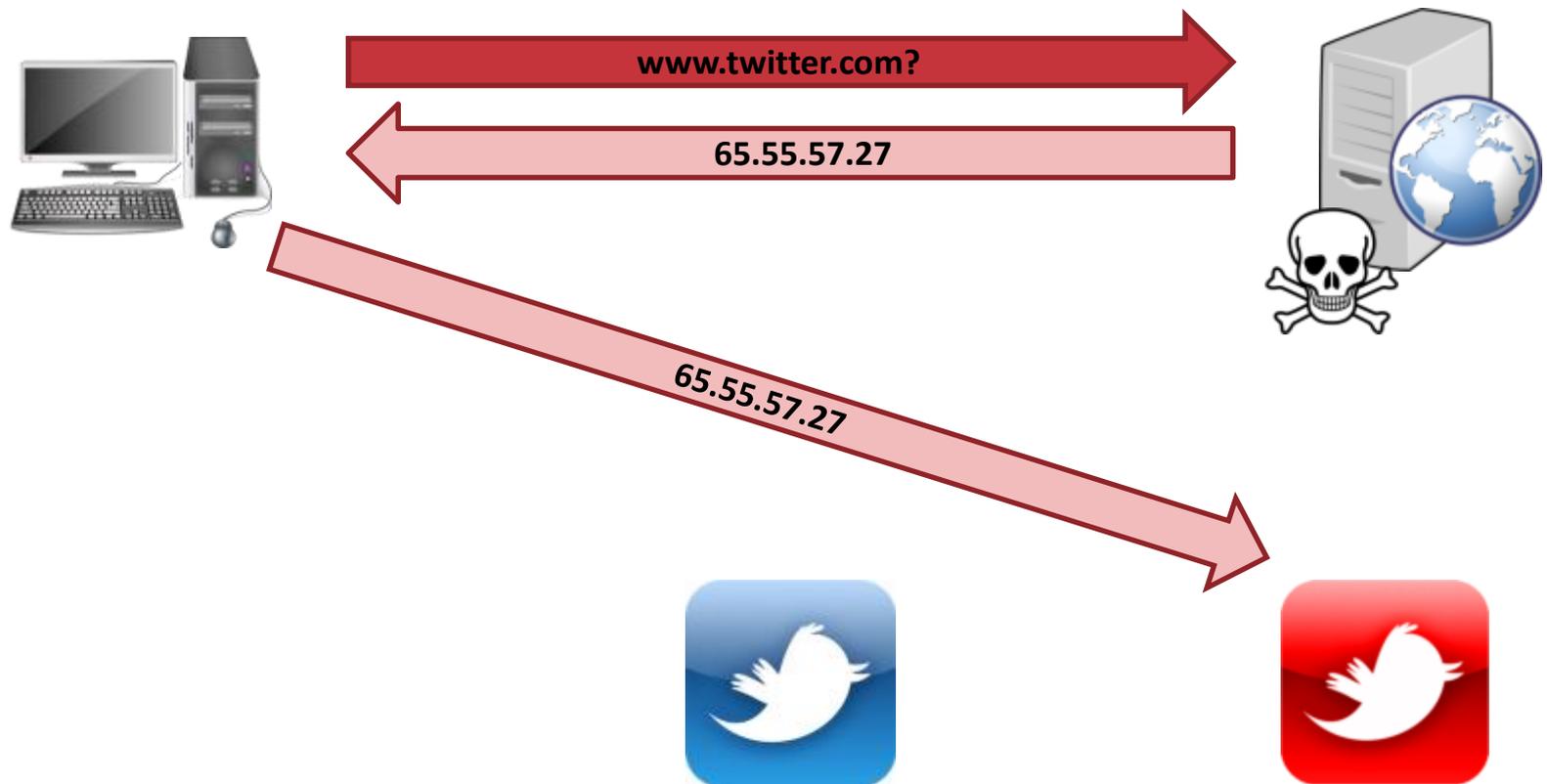
- Ataque **DNS Spoofing**. Petición y resolución lícita.



Fundamentos de comunicaciones

DNS. Ataques

- Ataque **DNS Spoofing**: Petición y resolución falsificada.



Fundamentos de comunicaciones

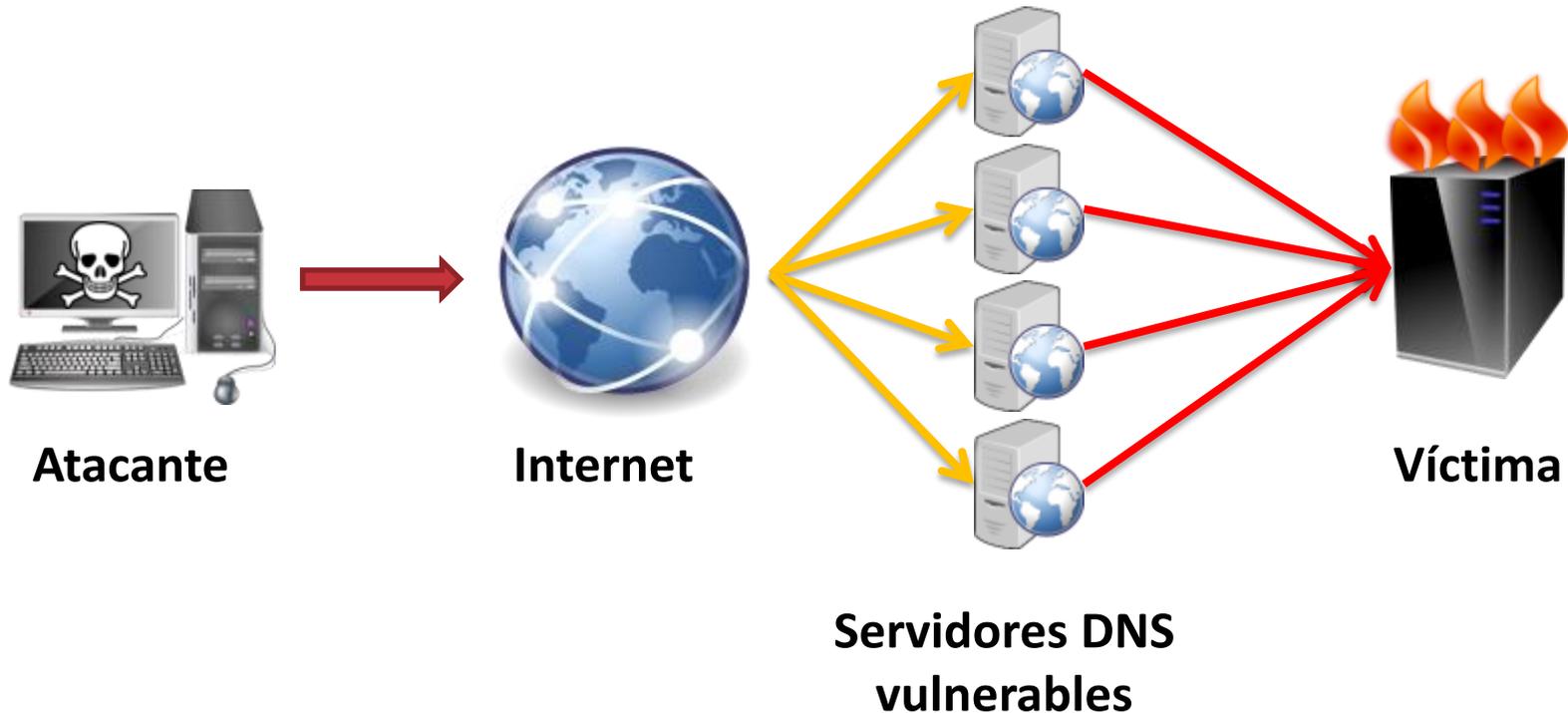
DNS. Ataques

- Un ataque de tipo DNS Spoofing puede ser tan simple como modificar un archivo y manipular la información de DNS, tener una dificultad media como comprometer un router o ser muy complejo e infectar servidores DNS mediante malware.
- Este ataque podría redirigirnos a páginas maliciosas para robar nuestras credenciales (usuarios y contraseñas) y suplantar nuestra identidad.

Fundamentos de comunicaciones

DNS. Ataques

- Ataques de amplificación **DNS (Smurf)**:



- Ataque a spamhaus:

<http://www.securitybydefault.com/2013/03/como-cyberbunker-ataco-spamhaus-y-casi.html>

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Introducción
5. Fundamentos de comunicaciones
- 6. Análisis de vulnerabilidades**
7. Explotación de vulnerabilidades
8. Seguridad en aplicaciones web
9. Actividades prácticas
10. Otros datos de interés

Análisis de vulnerabilidades

¿Qué es?

- La detección de servicios, protocolos o software vulnerables.

¿Qué quiere decir vulnerable?

- Que posee fallos de seguridad.
- El proceso de explotación puede estar publicado, documentado y accesible.
- Existen vulnerabilidades no conocidas previamente y cuando se publican pueden explotarse si no se han parcheado (Vulnerabilidades 0day).



Ejemplo:

- Una página web está soportada por un servidor web Apache.
- La versión de dicho servidor posee una vulnerabilidad conocida y documentada.
- Un atacante utiliza la documentación citada para obtener el control del servidor.

Análisis de vulnerabilidades

¿Cómo se realiza?

- El descubrimiento y análisis de vulnerabilidades esta basado en:
 - Análisis de puertos
 - Banner Grabbing
- Una vez obtenidos los puertos abiertos y los servicios en ejecución y sus versiones:
 - Se comparan las versiones y servicios con una base de datos de vulnerabilidades conocidas.
 - Si alguna coincide, se considera dicho servicio vulnerable.
 - Es posible que existan falsos positivos y que realmente no sea vulnerable.
- Este proceso se automatiza mediante programas que realizan las siguientes fases:
 - Análisis de puertos.
 - Banner Grabbing.
 - Comparación con base de datos de vulnerabilidades.



Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Introducción
5. Fundamentos de comunicaciones
6. Análisis de vulnerabilidades
- 7. Explotación de vulnerabilidades**
8. Seguridad en aplicaciones web
9. Actividades prácticas
10. Otros datos de interés

Explotación de vulnerabilidades

¿En qué consiste?

- Aprovechar las vulnerabilidades de un servicio o protocolo para realizar una acción no permitida en el sistema:
 - Obtener acceso al sistema o a la base de datos.
 - Obtener información confidencial.
 - Modificar, eliminar o añadir información.
 - Causar daños en el sistema.
 - Etc.

¿Cómo se realiza?

- Tanto de forma manual, como utilizando exploits públicos.



Explotación de vulnerabilidades

¿Qué es un exploit?

- Fragmento de código especialmente preparado para explotar una vulnerabilidad conocida.
- Normalmente, son pequeños programas en los que el atacante tiene que especificar :
 - IP destino.
 - Puerto destino.
 - Otros parámetros propios de la vulnerabilidad.
 - El payload.

```
#!/usr/bin/env perl
use LWP::UserAgent;
use HTTP::Cookies;

$ua = LWP::UserAgent->new();
$ua->agent("Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:31.0) Gecko/20100101 Firefox/31.0");
$ua->cookie_jar({});
$username = "username) from user where userid=$ARGV[4]#";
$email = "email) from user where userid=$ARGV[4]#";
$password = "password) from user where userid=$ARGV[4]#";
$salt = "salt) from user where userid=$ARGV[4]#";
@tofinds = ('database()#'); push(@tofinds,$username); push(@tofinds,$email); push(@tofinds,$password); push(@tofinds,$salt);

sub request
{
    my $token = dumping("vbloginout.txt","token");

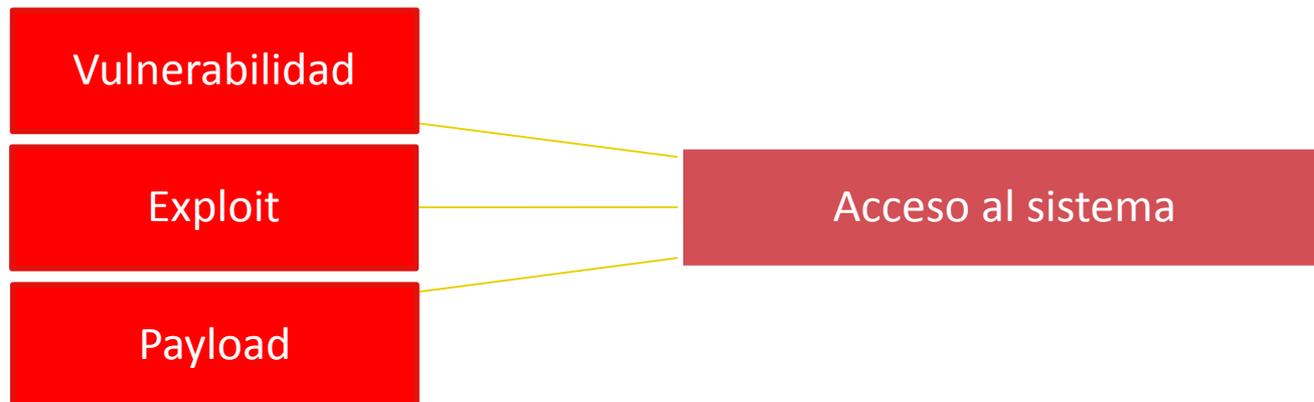
    if($token eq '')
    {
        print "SECURITYTOKEN not found (Make sure to log out from any other previous logged sessions before running the exploit).\n";
        #print "Attempting using 1409594055-f2133dfe1f26a36f6349eb3a946ac38c94a182e6 as token.\n";
        $token = "1409750140-51ac26286027a4bc2b2ac38a7483081c2a4b2a3e"; # HERE
        print "Attempting using $token as token.\n";
    }
    else
    {
        print "SECURITYTOKEN FOUND: $token\n";
    }
}
```

Lo complicado es encontrar la vulnerabilidad que hay dentro del exploit y crear el payload.

Explotación de vulnerabilidades

¿Qué es un payload?

- Es un fragmento de código que va siempre asociado al exploit.
- Mientras que con el exploit se evade la seguridad del sistema, con el payload se ejecuta una acción provechosa para el atacante.
- Ejemplo:
 - Ejecutamos un exploit en un sistema vulnerable.
 - A ese exploit le asociamos un payload que, por ejemplo, va a crear un usuario administrador en el sistema con credenciales conocidas.



Post-explotación de vulnerabilidades

¿Y ahora qué?

- Una vez se ha obtenido acceso al sistema, los atacantes tienen multitud de opciones:
 - Robo de información.
 - Modificación de datos.
 - Realización de daños al sistema.
 - Robo de identidad.
 - Espionaje.
 - Robo de datos personales.
 - Extorsión.
 - Fraude.
 - Uso del sistema comprometido para saltar a otro sistema (pivoting).
 - Etc.

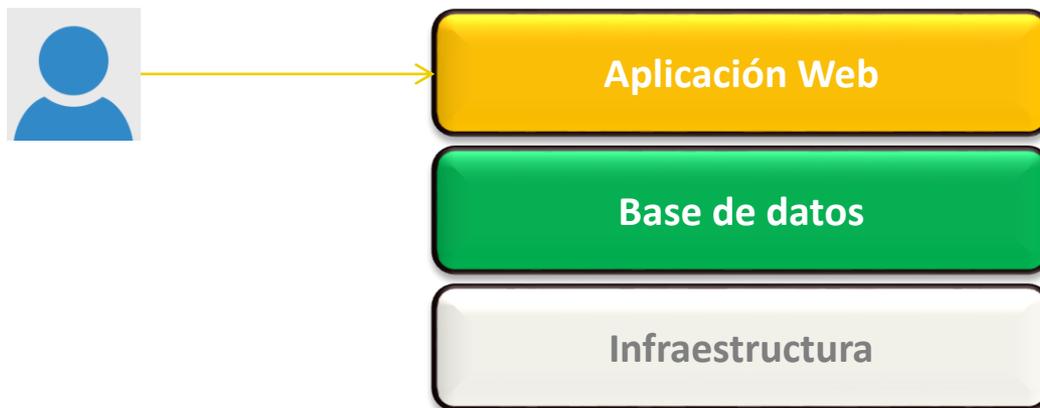
Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Introducción
5. Fundamentos de comunicaciones
6. Análisis de vulnerabilidades
7. Explotación de vulnerabilidades
- 8. Seguridad en aplicaciones web**
9. Actividades prácticas
10. Otros datos de interés

Seguridad en aplicaciones web

Seguridad en aplicaciones web

- Multitud de los problemas de seguridad web se pueden encontrar a nivel aplicación, éstos son el resultado de una programación errónea. El desarrollo de aplicaciones web seguras es una tarea compleja, ya que demanda una concepción general de los riesgos de la información contenida, solicitada y recibida por el sistema, más allá de cumplir con el objetivo funcional básico de la aplicación.



Seguridad en aplicaciones web

Bases de datos. SQL

- Una base de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
- Una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.



Seguridad en aplicaciones web

Bases de datos. SQL

- El **lenguaje de consulta estructurado** o **SQL** (por sus siglas en inglés Structured Query Language) es un lenguaje de acceso a bases de datos que permite especificar diversos tipos de operaciones en ellas, como lectura y escritura de registros, actualizaciones y borrados.

ID_Cliente	Nombre_Cliente	Teléfono	Contraseña	Importe
1	Pablo	913342134	@palabra65.net	100
2	David	934567923	123456	299
3	Javier	915557788	lampara	2500

- ¿Cuáles son los nombres de los clientes?



```
SELECT Nombre_Cliente FROM Customers;
```

Seguridad en aplicaciones web

Aplicaciones web. PHP

- Existen muchas tecnologías para desarrollar una aplicación web (PHP, ASP, Java Server Pages, etc.)
- Se trata de un lenguaje de programación que permite interactuar con la capa de datos (base de datos) y que presenta un resultado final a un navegador mediante código HTML.

A screenshot of a web application's login form. It has a title 'Login' and two input fields: 'Email' and 'Password'. Below the fields is a 'Log In Now' button and a 'forgot password?' link. Two yellow arrows point from the input fields to the corresponding parts of the SQL query below.

```
SELECT * FROM Users WHERE Username='$username' AND Password='$password'
```

Seguridad en aplicaciones web

OWASP

- Para ver los riesgos y fallos de seguridad más importantes en una aplicación web, existen organizaciones cuyo objetivo es facilitar el análisis de vulnerabilidades y dotar de herramientas para la auditoría, aprendizaje y prevención de los fallos de seguridad web.

*“OWASP (acrónimo de **Open Web Application Security Project**, en inglés ‘Proyecto abierto de seguridad de aplicaciones web’) es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo.”*



OWASP

The Open Web Application Security Project

Seguridad en aplicaciones web

OWASP

- OWASP publica y revisa periódicamente un documento de los diez riesgos de seguridad que considera más importantes en aplicaciones web de mayor a menor importancia.
- De estos tipos de vulnerabilidades, veremos los fundamentos de únicamente los 3 tipos más importantes y pondremos posteriormente en práctica los conocimientos adquiridos.

Seguridad en aplicaciones web

OWASP

OWASP Top 10-2013
A1- Inyección
A2-Pérdida de autenticación y gestión de sesiones
A3-Secuencia de comandos en sitios cruzados. [XSS]
A4-Referencia directa insegura a objetos
A5-Configuración de seguridad incorrecta
A6-Exposición de datos sensibles
A7-Ausencia de control de acceso a las funciones
A8-Falsificación de peticiones en sitios cruzados. [CSRF]
A9-Uso de componentes con vulnerabilidades conocidas
A10-Redirecciones y reenvíos no validados

Seguridad en aplicaciones web

A1. Inyección

- Distintas variedades de inyección: SQL (Bases de datos), LDAP (Directorios), etc.
- Se trata de hacer que la aplicación web interprete los datos proporcionados por el usuario como parte de una orden o consulta.
- Este hecho es empleado por un atacante para alterar el funcionamiento correcto de la aplicación web, pudiendo comprometer la integridad de la información o su privacidad, así como la seguridad de los sistemas subyacentes.



Seguridad en aplicaciones web

A1. Inyección

ID_Cliente	Nombre_Cliente	Teléfono	Contraseña	Importe
1	Pablo	913342134	@palabra65.net	100
2	David	934567923	123456	299
3	Javier	915557788	lampara	2500

Login

Email

Password

Log In Now

[forgot password?](#)

Pablo

@palabra65.net

```
SELECT * FROM Users WHERE Username='Pablo' AND Password='@palabra65.net'
```

Seguridad en aplicaciones web

A1. Inyección. ¿Cómo evitarlo?

- Para protegerse es necesario validar las entradas del usuario.
- Se deben adoptar medidas adicionales como acceder con los mínimos privilegios, no dar información en los mensajes de error, etc.



Seguridad en aplicaciones web

A2. Pérdida de autenticación y gestión de sesiones

- Se trata de aprovechar un defecto en el mecanismo de autenticación de la aplicación, teniendo como consecuencias el robo de credenciales o el acceso no autorizado a los recursos de la aplicación web.
- Para **protegerse** es necesario:
 - Emplear los mecanismos de sesión proporcionados por el lenguaje de programación
 - No aceptar identificadores de sesión inválidos
 - No permitir el proceso de autenticación desde una página sin cifrado.
 - Emplear políticas de caducidad de sesiones.
 - No exponer las sesiones o las credenciales en las URLs.
 - Disponer en cada página de un mecanismo de finalización de la sesión.

Seguridad en aplicaciones web

A3. Secuencia de comandos en sitios cruzados

- Se trata de hacer que datos de entrada sean interpretados como fragmentos de código.
- Ejecución de scripts en el navegador de la víctima.
- También conocido como **XSS [Cross Site Scripting]**.
- Dos tipos
 - **XSS persistente o directo**: Se introduce código HTML con etiquetas <script> o <iframe> en sitios donde se almacene dicho texto, como foros o sitios donde se puedan incluir comentarios. El código queda implantado en la web de manera interna y afecta a cualquier usuario que acceda a dicha página.
 - **XSS reflejado o indirecto**: Se introduce el código malicioso en la URL, formularios, cookies, etc., lugares donde el código malicioso no quede almacenado en la aplicación Web. Es necesario que un usuario acceda al enlace manipulado con el XSS para que se vea afectado.
- Para **protegerse** es necesario **validar las entradas del usuario**.

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Introducción
5. Fundamentos de comunicaciones
6. Análisis de vulnerabilidades
7. Explotación de vulnerabilidades
8. Seguridad en aplicaciones web
- 9. Actividades prácticas**
10. Otros datos de interés

Actividades prácticas

Práctica: Página web vulnerable



Username

Password

Login



Práctica realizada en un entorno controlado. Intentar hacer esto en entornos reales puede tener consecuencias legales

Actividades prácticas

Práctica: Página web vulnerable



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Bienvenidos a las jornadas de Ciberseguridad

Las jornadas de seguridad de ciberseguridad están organizadas por el Instituto Nacional de Ciberseguridad de España (INCIBE).

El Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad dependiente del Ministerio de Industria, Energía y Turismo (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

Este taller y el resto de Jornadas "Espacio de Ciberseguridad" están orientadas a la promoción del talento en ciberseguridad y forman parte del "Eje V: Programa de Excelencia en ciberseguridad" del Plan de Confianza Digital elaborado por el Ministerio de Industria, Energía y Turismo

Descarga de responsabilidad

Esta aplicación está basada en DVWA y posee numerosas vulnerabilidades conocidas y fácilmente explotables. Su uso debe realizarse en entornos de desarrollo y representa una amenaza para la seguridad de la infraestructura donde se instale.



Esta aplicación y la explotación de diferentes vulnerabilidades se realizarán de manera local en una red privada. Llevar a cabo la explotación de vulnerabilidades en aplicaciones en Internet puede tener consecuencias legales.

Actividades prácticas

Práctica: Inyección SQL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Vulnerability: SQL Injection

User ID:

More info

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://feruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout



' or 1=1#

Actividades prácticas

Práctica: Inyección SQL


INSTITUTO NACIONAL DE CIBERSEGURIDAD

Vulnerability: SQL Injection

User ID:

More info

- <http://www.securiteam.com/securityreviews/SDP0N1P746.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://f0r4h.mavibank.com/sql-injection-cheatsheet-0ku/>
- <http://perthesmonkey.net/cheat-sheets/sql-injection/mysql-sql-injection-cheat-sheet/>

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP info
About
Logout



1' UNION SELECT 1,2#

Actividades prácticas

Práctica: Inyección SQL


INSTITUTO NACIONAL DE CIBERSEGURIDAD

Vulnerability: SQL Injection

User ID:

More info

- <http://www.securiteam.com/securityreviews/SDP0N1P746.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://f0r4h.mavibank.com/sql-injection-cheatsheet-0ku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet/>

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP info
About
Logout



```
1' UNION SELECT 1,select database(); #
```

Actividades prácticas

Práctica: Inyección SQL


INSTITUTO NACIONAL DE CIBERSEGURIDAD

Vulnerability: SQL Injection

User ID:

More info

- <http://www.securiteam.com/securityreviews/SDP0N1P746.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://fr.mh.mavibank.com/sql-injection-cheatsheet-0ku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP info
About
Logout



```
1' UNION SELECT 1,group_concat(schema_name) FROM information_schema.schemata;#
```

Actividades prácticas

Práctica: XSS en una aplicación web



The screenshot displays the DVWA web application interface. At the top, the logo for 'incibe_' (INSTITUTO NACIONAL DE CIBERSEGURIDAD) is visible. The main content area is titled 'Vulnerability: Reflected Cross Site Scripting (XSS)'. Below the title is a form with the text 'What's your name?' and a 'Submit' button. To the left of the main content is a navigation menu with various options, including 'Home', 'Instructions', 'Setup', 'Brute Force', 'Command Execution', 'CSRF', 'Insecure CAPTCHA', 'File Inclusion', 'SQL Injection', 'SQL Injection (Blind)', 'Upload', 'XSS reflected' (highlighted in yellow), 'XSS stored', 'DVWA Security', 'PHP Info', 'About', and 'Logout'. Below the form, there is a 'More info' section with three links: <http://hackers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>.

Actividades prácticas

Cuestiones

1. ¿Qué tipos de ataques XSS existen y cuáles son sus diferencias?
2. ¿Podrías nombrar los 3 tipos de vulnerabilidades web más graves del top 10 de vulnerabilidades según OWASP?
3. ¿Qué es un exploit?
4. ¿Dónde reside la información obtenida mediante SQL injection?

Actividades prácticas

Respuestas

1. Existen dos tipos: XSS reflejado y almacenado, se diferencian en el lugar donde se incluye el código malicioso. Los ataques de XSS reflejado se suelen encontrar en motores de búsqueda, los ataques XSS almacenado suelen estar en foros o webs.
2. Inyección, Pérdida de autenticación y gestión de sesiones, Secuencia de comandos en sitios cruzados (XSS).
3. Es un fragmento de código especialmente preparado para explotar una vulnerabilidad conocida.
4. Reside en el servidor, en la base de datos de esa aplicación web.

Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Introducción
5. Fundamentos de comunicaciones
6. Análisis de vulnerabilidades
7. Explotación de vulnerabilidades
8. Seguridad en aplicaciones web
9. Actividades prácticas
- 10. Otros datos de interés**

Encuesta de satisfacción



incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Encuesta satisfacción

Estimado alumno, te agradecemos que hayas asistido a esta Jornada y esperamos que te haya resultado interesante. Nos gustaría conocer tu opinión de cara a poder mejorar en las próximas Jornadas, por este motivo te pedimos que, por favor, rellenes esta encuesta.

La encuesta es totalmente anónima y no se recabará ningún dato personal tuyo

¡Muchas gracias por tu colaboración!

*Obligatorio

Nombre de la jornada *

Fecha y hora de la jornada *

Día Mes 2015 h : min

Datos generales

Nombre de tu centro de estudios *

Actuaciones

I+D+i y Promoción de Talento en Ciberseguridad

Este taller y el resto de las Jornadas “Espacio de Ciberseguridad” forman parte del «Eje V: Programa de Excelencia en Ciberseguridad» dentro del Plan de Confianza Digital del Ministerio de Industria, Energía y Turismo (MINETUR) que se está llevando a cabo desde INCIBE para la promoción y captación de talento en Ciberseguridad.

Si te gusta la ciberseguridad y quieres profundizar en este tema, dentro del Plan de Confianza Digital se están desarrollando las siguientes actividades y eventos de ciberseguridad:

-  **Formación especializada en ciberseguridad:** MOOC que se desarrollan a través de la plataforma de formación de INCIBE (<http://formacion-online.incibe.es>) sobre conceptos avanzados en ciberseguridad tales como ciberseguridad industrial, seguridad en dispositivos móviles, programación segura, malware y sistemas TI.
-  **Programa de becas:** Programa de becas anual en el que se establecerán diferentes tipologías de becas: formación de cursos especializados y másteres en ciberseguridad, y becas de investigación. Todas las publicaciones de este tipo se realizará a través de la siguiente página <https://www.incibe.es/convocatorias/ayudas/>.
- Evento de ciberseguridad – CyberCamp** (<http://cybercamp.es>).





CyberCamp es el evento internacional de INCIBE para **identificar**, **atraer** y **promocionar el talento** en ciberseguridad.

- Identificar trayectorias profesionales de los jóvenes talentos.
- Detectar y promocionar el talento mediante talleres y retos técnicos.
- Atraer el talento ofreciendo conferencias y charlas de ciberseguridad por profesionales y expertos de primer nivel.

Y muchas cosas más....

- Evento para **familias**, contando con actividades de concienciación y difusión de la ciberseguridad para padres, educadores e hijos.
- Promoción de la **industria** e **investigación** en ciberseguridad.



<https://cybercamp.es/>



<https://twitter.com/CybercampEs>



<https://www.facebook.com/CyberCampEs>

Gracias
por tu atención

Contáctanos

Contacto (más información y dudas sobre las jornadas):



espaciosciberseguridad@incibe.es

En las redes sociales:



@incibe
@certsi
@osiseguridad
@CyberCampES



Oficina de Seguridad del internauta
(Pienso luego clico)



INCIBE
OSIseguridad



Oficina de Seguridad del internauta
CyberCamp



Pág. INCIBE
Grupo INCIBE



Oficina de Seguridad del internauta

En la sede:

Avenida José Aguado, 41 - Edificio INCIBE
24005 León
Tlf. 987 877 189

En los sitios web:

www.incibe.es
www.osi.es
www.cybercamp.es

www.incibe.es

INSTITUTO NACIONAL DE
CIBERSEGURIDAD
NATIONAL CYBERSECURITY
INSTITUTE OF SPAIN



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, ENERGIA
Y TURISMO