

1001 ataques a WordPress



WordPress



FAKEINET



WordCamp
Bilbao 2019



SH3LLCON
Security Hell Conference





- Maestro de Ed. Primaria, formador y desarrollador web.
- Especializado en ciberseguridad y WordPress
- CEO en **fakeinet.com**
- CEO en **miplanhoy.com**
- Organizador el **Congreso de Seguridad Sh3llcon**
- Organizador de la **WordCamp Santander** y miembro de la comunidad WordPress de España.

Ataques web



Distintos Ataques

Fuerza bruta

Diccionario

XSS

XSS almacenado

SQL Injection

Defacement

File Inclusion / Remote file Inclusion

Command injection

File Upload

Cross Site Request Forgery (CSRF)

Ingeniería social

Phishing

...

Fuerza bruta (Brute force)



Fuerza bruta (Brute force)

Ensayo/error con clave de cifrado

Muy costosos en tiempo computacional.

Suele combinarse con un ataque de diccionario.

```
GNU nano 2.2.2
aaaaa
aaaad
aaaam
aaaai
aaaan
aaada
aaadd
aaadm
aaadi
aaadn
aaama
aaamd
aaamm
aaami
aaamn
aaaia
aaaid
aaaim
aaaii
aaain
```


Fuerza bruta (Brute force)

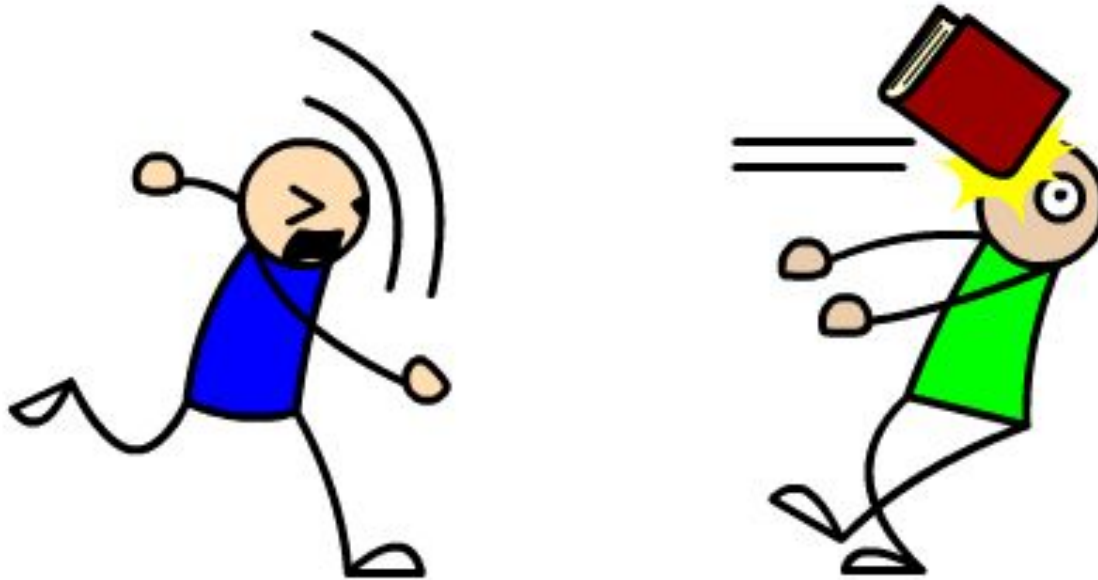
¿Cómo protegerse?

- Contraseñas fuertes y fáciles de recordar
- Letras (mayúsculas y minúsculas)
- Números
- Símbolos
- **Gran longitud**



Ataques de Diccionario

DICTIONARY ATTACK!



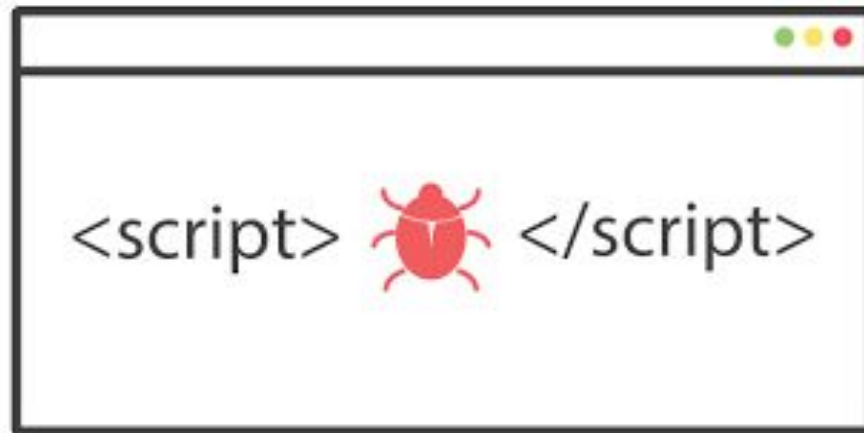
Ataques de Diccionario

¿Cómo protegerse?

- Contraseñas fuertes y fáciles de recordar
- Letras (mayúsculas y minúsculas)
- Números
- Símbolos
- Gran longitud
- Frases que no estén en ningún diccionario



XSS (inyección de código)



XSS (inyección de código)

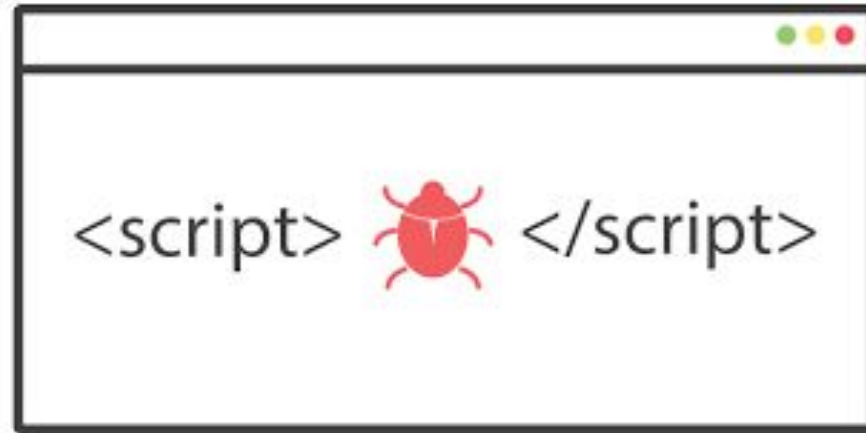
¿Cómo protegerse?

- Medidas a nivel de programación de la aplicación
- Filtros de HTML...



Stored XSS (inyección de código almacenado)

Persistent o Type-I XSS.



Stored XSS (inyección de código almacenado)

¿Cómo protegerse?

- Medidas a nivel de programación de la aplicación
- Filtros de HTML...



Stored XSS (inyección de código almacenado)

¿Cómo protegerse?

`htmlspecialchars($str);`

```
<?php
$str = "tiempo es <b>oro</b>";

echo htmlspecialchars($str);

// resultado: tiempo es
<lt;b>oro</b>;

?>
```



Stored XSS (inyección de código almacenado)

¿Cómo protegerse?

htmlspecialchars()

```
<?php
```

```
$nuevo = htmlspecialchars("<a  
href='link'>prueba</a>", ENT_QUOTES);
```

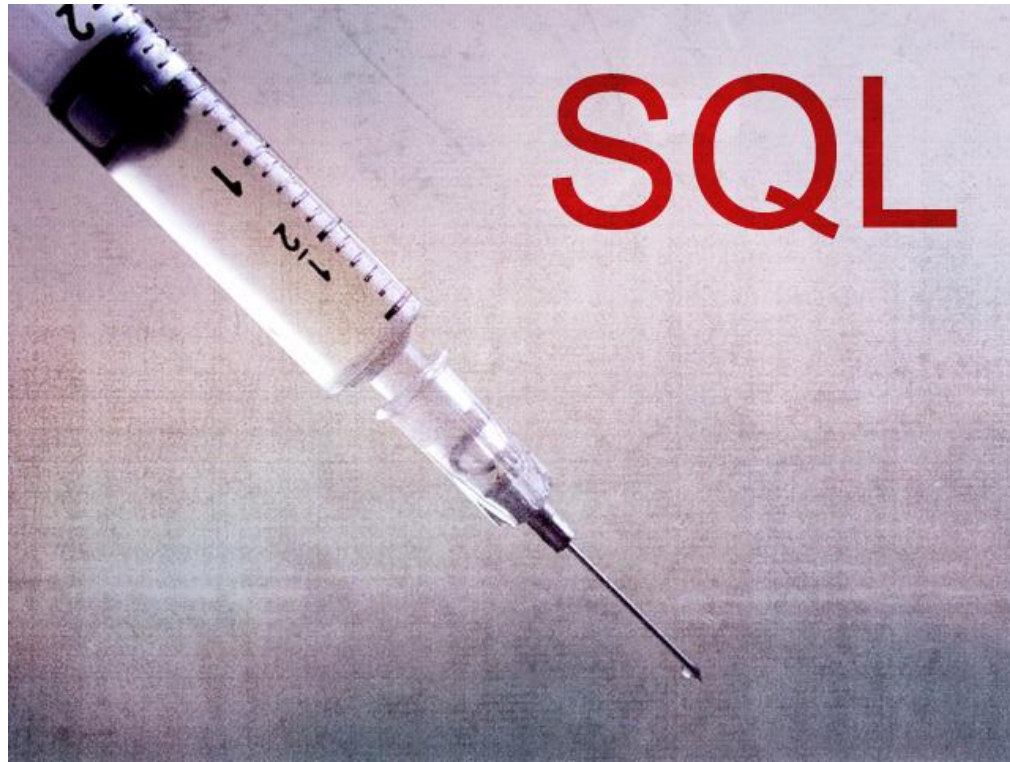
```
echo $nuevo;
```

```
// &lt;a  
href=&#039;link&#039;&gt;prueba&lt;/a&gt;
```

```
?>
```



SQL Injection



SQL Injection

or 1=1

or 1=0

%' or '0'='0

SELECT * FROM users WHERE id="0,1,2..."

%' or 0=0 union select null, database() #

SQL Injection

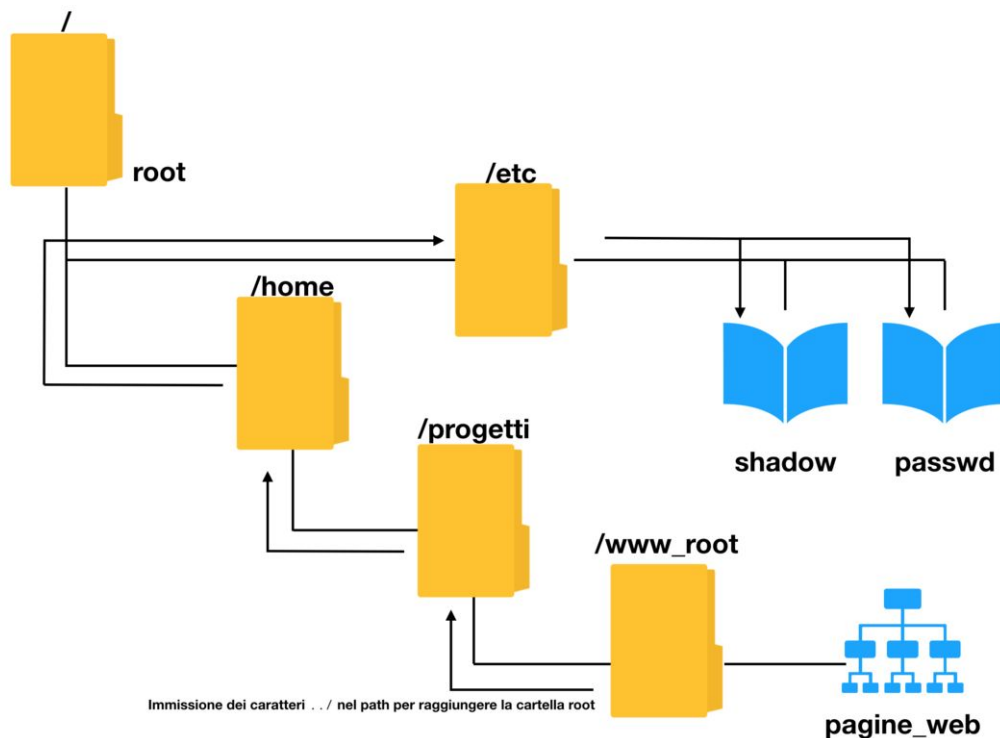
¿Cómo protegerse?

- No permitir caracteres especiales en formularios.
- Establecer permisos de cada usuario para acceder a la información.
- Controlar los mensajes de Error



File inclusion

Relacionado con Path Traversal, **Directory Traversal**,
escalado de directorios, backtracking...



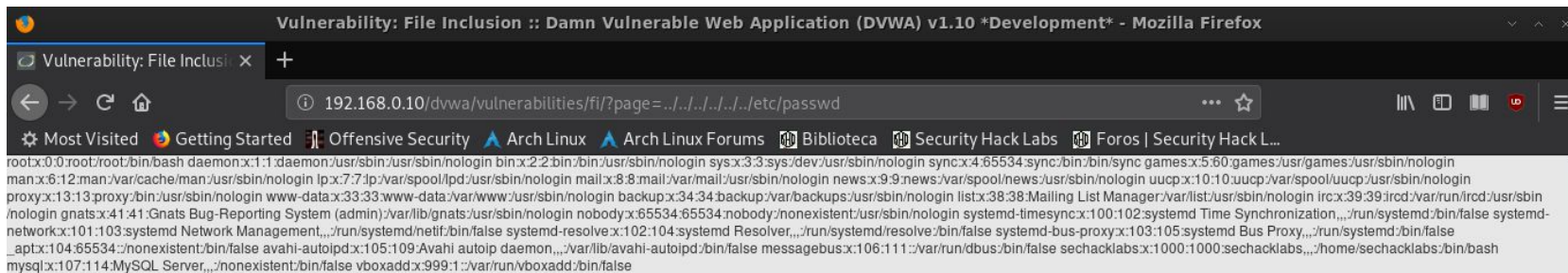
File inclusion

Causado por una seguridad insuficiente en:

- validación de un usuario
- en el código.

Permite acceder a cualquier tipo de directorio superior (padre)

`../../../../../../../../wp-config.php`



File inclusion

¿Cómo protegerse?

- Impedir el acceso a directorios superiores a los usuarios.
- Políticas de acceso a nivel de servidor.



Defacement

Cambio de “cara”.



Defacement



Defacement

¿Cómo protegerse?

- Políticas de acceso fuertes.
- Complementos actualizados (plugins, temas...:)

...



DoS (Denial of Service)



DoS (Denial of Service)

Consumo de recursos: ancho de banda, espacio de disco, o tiempo de procesador.

Interrupción de sesiones TCP (TCP reset).

Interrupción de aparatos físicos de red.

Interrupción la comunicación servicio - víctima

DoS (Denial of Service)

¿Cómo protegerse?

- Utilizar un buen server con muchos recursos.
- Mejor VPS o dedicado que compartido.



Otros Ataques

Fuerza bruta

Diccionario

XSS

XSS almacenado

SQL Injection

Defacement

File Inclusion / Remote file Inclusion

Command injection

File Upload

Cross Site Request Forgery (CSRF)

Ingeniería social

Phishing

...

Plugins





www.tomassierra.com



@Tomycant



tomycant

MUCHAS GRACIAS



WORDPRESS



FAKEINET



WordCamp
Bilbao 2019



SH3LLCON
Security Hell Conference

