



TALLER

Penetrando la web

Security High School

#SHS2k23



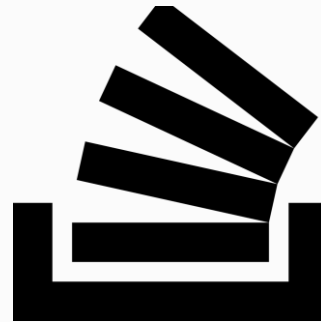
Recursos del taller



GITPAGE



PortSwigger



StackOverflow



Damn
Vulnerable Web
Application

INDCE

Quienes somos?



Tipos de ataque



XSS



SQLi



File Upload



Path traversal



ADVERTENCIA
INDICE
/ WARNING

Las escenas que estas a punto de ver
están realizadas por profesionales por
favor no lo intenten en sus casas y en
entornos controlados si lo intentan al
menos usa protección.

PONSELO PONTELO



Quienes somos



Pablo Crespo Cervantes

RRSS: @Doggymux



[Pablo Crespo Cervantes](#)

Quienes somos



Jose Antonio Montero Rodriguez

RRSS: @JAMon0702



[Jose Antonio Montero Rodriguez](#)

Quienes somos



Emilio José Iglesias Valera

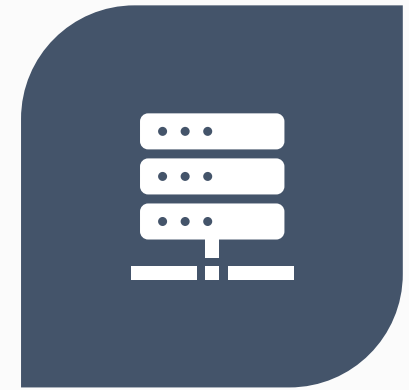


[@emilio.i.v emilux](#)

Tipos de ataque

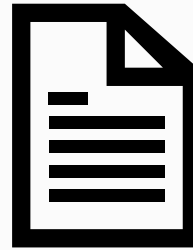


CLIENT SIDE
(XSS, FUERZA BRUTA)

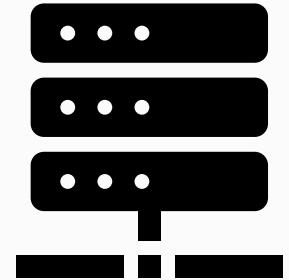


SERVER SIDE
(SQLI, XSS, FILE UPLOAD)

File Upload



EXPLOIT.PHP



COMO SE HACE LASUBIDA?

```
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        // No
        echo '<pre>Your image was not uploaded.</pre>';
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}

?>
```

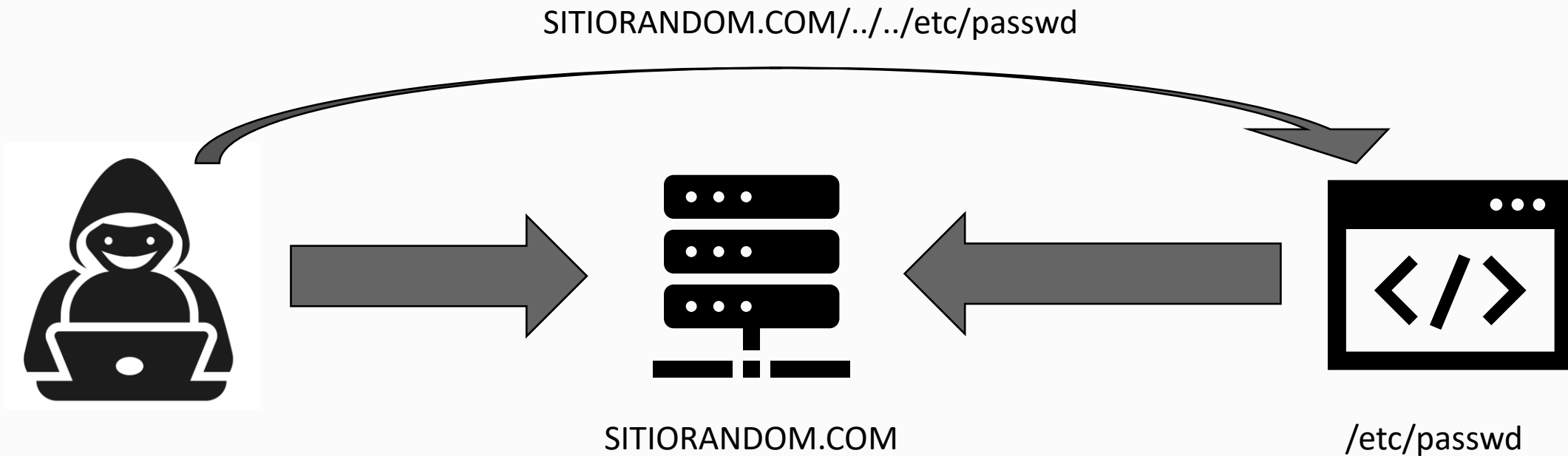
Usamos la información de la subida para comprobar

```
$uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];  
$uploaded_ext = substr( $uploaded_name, strrpos( $uploaded_name, '.' ) + 1 );  
$uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];  
$uploaded_tmp = $_FILES[ 'uploaded' ][ 'tmp_name' ];
```

```
if( ( strtolower( $uploaded_ext ) == "jpg" || strtolower( $uploaded_ext ) == "jpeg" || strtolower( $uploaded_ext )  
== "png" ) &&  
    ( $uploaded_size < 100000 ) &&  
    getimagesize( $uploaded_tmp ) ) {
```

¿Como me protejo?

File Inclusion / Path traversal



POR QUÉ SUCEDER?

```
<?php
```

```
// La pagina a mostrar
```

```
$file = $_GET[ 'page' ];
```

```
// Validaciones
```

```
$file = str_replace( array( "http://", "https://" ), "", $file );
```

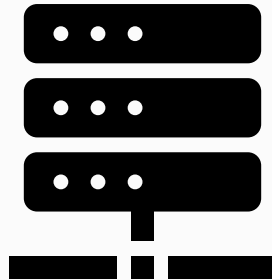
```
$file = str_replace( array( "../", "..\\" ), "", $file );
```

```
?>
```

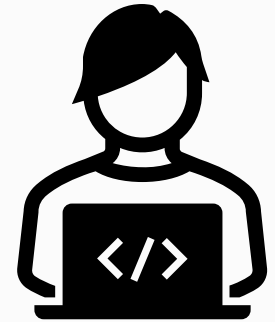
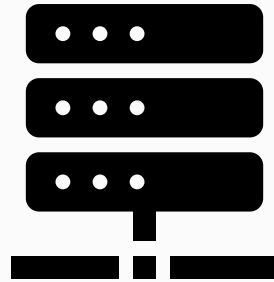
XSS

XSS o (Cross-Site Scripting) es una vulnerabilidad de seguridad que se produce cuando se inserta código malicioso (generalmente JavaScript) en una aplicación web

XSS REFLECTED



XSS STORED



MUY BIEN PERO
QUE PINTA TIENE?

```
<script>  
    alert(document.cookie);  
</script>
```

```
<?php
```

```
// Is there any input?
```

```
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
```

```
    // Check Anti-CSRF token
```

```
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );
```

```
    // Get input
```

```
    $name = htmlspecialchars( $_GET[ 'name' ] );
```

```
    // Feedback for end user
```

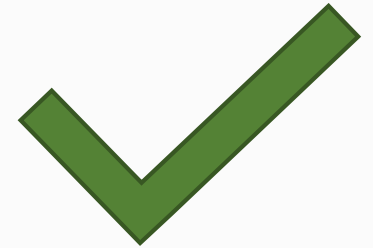
```
    echo "<pre>Hello ${name}</pre>";
```

```
}
```

```
// Generate Anti-CSRF
```

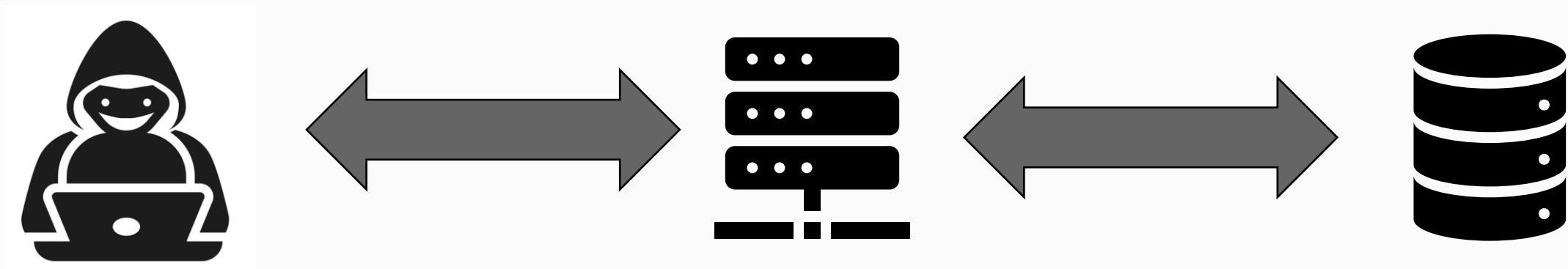
```
tokengenerateSessionToken();
```

```
?>
```

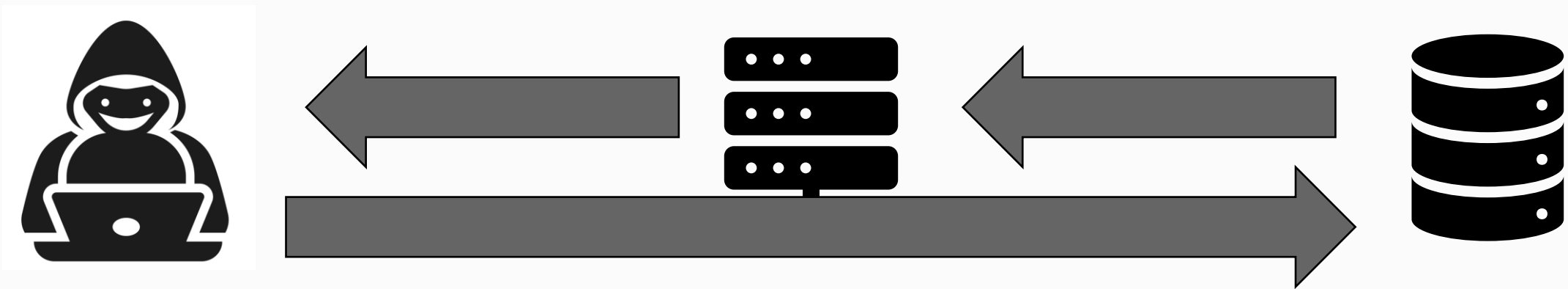


¿Como me protejo?

SQLi



SQLi



MUY BIEN PERO **SQLi** procedimientos
QUE TIPOS EXISTEN?

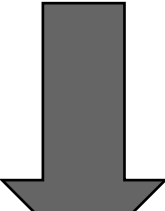
SQLi almacenados
SQLi de recuperación
SQLi de error
datos ocultos
SQLi de union
SQLi autenticación
SQLi Inyección código
SQLi basada en tiempo

SQLi campo oculto
SQLi de segundo orden
SQLi error de logica

QUE FORMA TIENE UNA SQLi?

Login

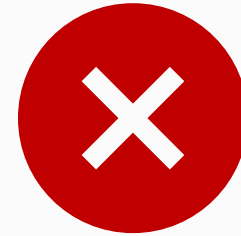
Welcome !! You are a Admin User



```
SELECT USERID FROM USERS WHERE USERNAME = 'PEØR'`1`='1'-- -
```

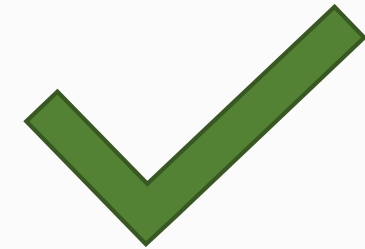


```
// Obtención del nombre de la película desde el formulario  
$nombre = $_POST["nombre"];
```



```
$nombre = htmlspecialchars($_POST["nombre"], ENT_QUOTES, 'UTF-8');
```

```
// Consulta a la base de datos usando sentencias preparadas  
$stmt = mysqli_prepare($conn, "SELECT * FROM usuarios WHERE nombre = ?");  
mysqli_stmt_bind_param($stmt, "s", $nombre);  
mysqli_stmt_execute($stmt);  
$result = mysqli_stmt_get_result($stmt);
```



¿Como me protejo?

RETOS QUE OS LANZAMOS

- Intenta subir la imagen en difícil
- Intenta sacar la versión de Ubuntu en DVWA con SQLi
- Dinos el usuario que corre DVWA
- Ejecuta un comando del sistema desde SQL
- Añade un botón con xss que te redirija a youtube.com

