# Grupo 4

|  |  |  |  |
| --- | --- | --- | --- |
| ITEM | CATEGORÍA | CHECKLIST (¿Qué se verifica?) | ¿Cómo se verifica? |
| A01 | Control de acceso inseguro | ¿Los roles de usuario están bien configurados? | wpscan --enumerate u |
|  |  | ¿Hay acceso administrativo restringido (wp-admin)? | .htaccess y wp-config.php |
|  |  | ¿Protección contra fuerza bruta en login? | Intentos múltiples de login |
| A02 | Fallos criptográficos | ¿Se usa HTTPS en todo el sitio? | curl -I https://[sitio] |
|  |  | ¿Las contraseñas están con hash seguro? | Verificar en la tabla wp\_users |
|  |  | ¿Claves de API están protegidas? | wp-config.php |
| A03 | Inyección | ¿Hay protección contra SQL Injection? | sqlmap -u "http://[sitio]/?s=test" |
|  |  | ¿Los inputs están sanitizados? | Pruebas en formularios |
|  |  | ¿Protección contra PHP injection? | Revisar uploads y ejecución de archivos |
| A04 | Diseño inseguro | ¿Existe límite de intentos de login? | Múltiples intentos de login |
|  |  | ¿Validación de datos en formularios? | Pruebas en campos de contacto |
|  |  | ¿Protección contra spam en comentarios? | Revisar configuración de comentarios |
| A05 | Configuración de seguridad | ¿La versión de WordPress está oculta? | Ver código fuente |
|  |  | ¿Mensajes de error controlados? | Provocar errores intencionales |
|  |  | ¿Archivos sensibles accesibles? | dirb http://[sitio] |
| A06 | Componentes vulnerables | ¿WordPress core actualizado? | wpscan --url http://[sitio] |
|  |  | ¿Plugins actualizados? | wpscan --enumerate vp |
|  |  | ¿Plugins/temas con CVEs conocidos? | wpscan --api-token [token] |
| A07 | Fallos en autenticación | ¿Hay autenticación de dos factores (2FA)? | Configuración de plugins de seguridad |
|  |  | ¿Las sesiones expiran correctamente? | Ver expiración de cookies |
|  |  | ¿Contraseñas con requisitos fuertes? | Política de contraseñas |
| A08 | Integridad de software y datos | ¿Backups protegidos? | Ubicación y cifrado de backups |
|  |  | ¿Verificación de integridad de archivos? | Plugins de monitoreo |
|  |  | ¿Actualizaciones seguras? | Proceso de actualización |
| A09 | Fallas de registro y monitoreo | ¿Logs de actividad de usuarios? | Plugins de logging |
|  |  | ¿Se registran intentos de ataque? | Logs de seguridad |
|  |  | ¿Monitoreo de cambios críticos? | Registro de cambios en archivos |
| A10 | Server-Side Request Forgery (SSRF) | ¿Validación de URLs en peticiones? | Pruebas en campos de URL |
|  |  | ¿Protección contra SSRF? | Pruebas de request forgery |
|  |  | ¿APIs internas protegidas? | Verificar acceso a endpoints internos |