# Authentification

|  |  |  |
| --- | --- | --- |
| Utilisation de mots de passe forts | * Les mots de passe dépassent-ils dix caractères ? * Les mots de passe sont-ils suffisamment complexes ? | Oui / Non |
| La réinitialisation des mots de passe est-elle sécurisée ? | Un jeton unique est-il créé pour la réinitialisation ? | Oui / Non |
| Changement des données personnelles | Une réauthentification est-elle demandée lors des changements de données personnelles (Anti CSRF) ? | Oui / Non |
| Le stockage des mots de passes | Mots de passe hachés ?  Mots de passe salés en BDD ? | Oui / Non |
| Messages d’erreur | * Les messages d’erreurs sont ils réalisés de manière à n’afficher aucune information sensible ? * Le statut de retour des requêtes sont-ils bien gérés ? (Ex : Ne pas renvoyer de statut 200 si la requête a échoué) | Oui / Non |
| Brute force | L’application bloque-t-elle un utilisateur lors d’essais d’authentification excessifs ? | Oui / Non |

# Management des sessions

|  |  |  |
| --- | --- | --- |
| Les identifiants de session | Sont-ils chiffrés et au minimum de 128 bits de longueur ? | Oui / Non |
| Données personnelles | Les cookies contiennent-ils des données personnelles ? | Oui / Non |
| Secure flag | Est-elle mise en place ? | Oui / Non |
| HttpOnly | Est-elle mise en place ? | Oui / Non |
| Domaine et cookie | Le cookie est-il bien lié à un seul domaine (et non des sous domaines) ? | Oui / Non |
| Temps de vie du cookie | Le cookie a-t-il une limite de temps ? | Oui / Non |
| Bouton de déconnexion | La déconnexion est-elle disponible depuis n’importe quelle page du site ? | Oui / Non |
| Temps d’inactivité d’une  session | La session d’un utilisateur expire-t-elle après X minutes d’inactivité ? | Oui / Non |
| Date limite absolue | La session expire-t-elle à un moment donné ? | Oui / Non |

# Contrôle des accès

|  |  |  |
| --- | --- | --- |
| Liste des rôles | La liste des rôles et autorisations est-elle bien claire et documentée pour l’application ? | Oui / Non |
| Test de pénétration | Des tests de pénétrations ont-ils été effectués ? | Oui / Non |

# Validation des entrées

|  |  |  |
| --- | --- | --- |
| Périmètre des entrées | Toutes les entrées serveurs sont-elles nettoyées, comme les variables liées au réseau, cookie, session, entête http… ? | Oui / Non |
| Taille des entrées | La taille des entrées est-elle contrôlée ? | Oui / Non |
| Encodage | L’encodage possible des entrées est-il connu et pris en compte ? | Oui / Non |
| Contenu riche | Les contenus riches tels que les WYSIWYG sont ils contrôlés par des Framework spécifiques sécurisés ? | Oui / Non |

# Encodage des sorties

|  |  |  |
| --- | --- | --- |
| Se prémunir des vulnérabilités XSS | Les entrées utilisateurs sont-elles assainies de manière à ne pas pouvoir réaliser d’injection XPath ? | Oui / Non |
| Se prévenir des injections SQL | Les paramètres utilisés dans vos requêtes sont-ils assainis ? (Soit manuellement, soit via le framework utilisé) | Oui / Non |
| Se prévenir des injections XML | Les entrées utilisateurs sont-elles assainies ? | Oui / Non |
| Injection de code | Vérification des utilisations des fonctions eval() & include() | Oui / Non |

# Upload de fichiers

|  |  |  |
| --- | --- | --- |
| Upload de fichiers | * Les types et extensions sont-ils contrôlés ? * Les fichiers changent-ils de nom une fois stockés sur le serveur de production ? * Les fichiers spécifiques lié à l’admin (.htaccess, crossdomain.xml) sont-ils contrôlés et non appliqué sur le gestionnaire de code source ? | Oui / Non |

# XSS

|  |  |  |
| --- | --- | --- |
| Echappement des entrées | L’échappement des caractères spécifiques est-il bien réalisé ? | Oui / Non |
| Content Security Policy | La Content Security Policy est-elle en place avec une white list de fichiers de confiance ? | Oui / Non |

# CSRF

|  |  |  |
| --- | --- | --- |
| Jeton unique chiffré | Un système de jeton CRSF chiffré est-il mis en place et utilisé ? | Oui / Non |
| Captcha | Un système de Captcha est-il mis en place pour les formulaires avec des données sensibles ? | Oui / Non |

# Clickjacking

|  |  |  |
| --- | --- | --- |
| Content Security Policy | La CSP est-elle en place avec une whitelist de sources de confiance ? | Oui / Non |
| X-Frame-Options | Si la CSP n’est pas en place les X-Frame-Options le sont-ils ? | Oui / Non |

# Enregistrement des événements

|  |  |  |
| --- | --- | --- |
| Events liés au serveur | Les échecs d’authentification sont ils loggés afin de pouvoir identifier les tentatives de brute force ? | Oui / Non |
| Events liés au code | Les erreurs liées au code sont-elles loggés ? | Oui / Non |
| Events | Le journal des events est-il consulté régulièrement et accessible facilement ? | Oui / Non |
| Attaque | Si une attaque survient, sommes-nous capable de réagir rapidement grâce aux events ? | Oui / Non |

Cryptologie