

Modèle de programme de Bug Bounty – Exemple PME

1. Présentation de l'entreprise

Notre entreprise, **[Nom de la société]**, est une PME belge active dans le secteur **[secteur d'activité]**.

Nous mettons un point d'honneur à assurer la sécurité de nos systèmes et des données de nos clients.

Ce programme de Bug Bounty s'inscrit dans une démarche proactive de cybersécurité et de collaboration responsable.

2. Objectif du programme

L'objectif est de permettre à des chercheurs en sécurité de **signaler de manière responsable** les vulnérabilités potentielles dans nos services numériques, avant qu'elles ne soient exploitées par des acteurs malveillants.

Nous encourageons les rapports **clairs, reproductibles et documentés** afin de nous aider à renforcer la sécurité de nos applications et infrastructures.

3. Portée du programme (Scope)

Systèmes inclus :

- <https://www.exemple-entreprise.be>
- <https://app.exemple-entreprise.be>
- API publique : <https://api.exemple-entreprise.be>

Systèmes exclus :

- Sous-domaines tiers (ex. analytics, support, marketing)
- Services internes non accessibles publiquement
- Tests physiques, d'ingénierie sociale ou de déni de service (DoS)

Toute activité sur des systèmes non mentionnés comme “inclus” sera considérée hors périmètre.

4. Règles de bonne conduite

Les chercheurs doivent :

- Respecter la confidentialité et ne **pas divulguer publiquement** les vulnérabilités.
- Ne pas altérer ou exfiltrer de données.
- Ne pas perturber la disponibilité du service.
- Signaler les failles via la plateforme, en fournissant les **étapes de reproduction**, le **contexte technique** et, si possible, une **preuve de concept**.

En contrepartie, nous nous engageons à :

- Accuser réception du rapport sous **72h ouvrées**.
- Fournir un suivi transparent du statut.
- Créditez le chercheur (s'il le souhaite) dans notre page "Hall of Fame".

5. Vulnérabilités recherchées

Exemples de failles acceptées :

- Injection SQL, XSS, CSRF
- Mauvaise configuration de sécurité (CORS, headers, etc.)
- Escalade de privilèges
- Fuite de données sensibles

Failles **hors scope** :

- Attaques de phishing, spam, DoS
- Problèmes d'UX/UI
- Versions obsolètes non exploitées
- Vulnérabilités déjà connues publiquement

6. Récompenses (Bounty)

Les récompenses varient selon la **gravité**, l'**impact** et la **qualité du rapport** :

Sévérité	Exemple d'impact	Récompense indicative
Critique	Accès admin / fuite massive de données	300 – 500 €

Sévérité	Exemple d'impact	Récompense indicative
Haute	Compromission d'un compte utilisateur	150 – 300 €
Moyenne	Failles XSS ou injections limitées	50 – 150 €
Faible	Mauvaise configuration sans impact direct	Mention / points

7. Soumission de rapports

Tous les rapports doivent être envoyés via la plateforme :

[Nom de ta plateforme Bug Bounty] – Espace Entreprise

Le chercheur recevra une confirmation automatique et un suivi en temps réel.

Les échanges se font exclusivement via la messagerie intégrée pour garantir la traçabilité.

8. Mentions légales

En participant à ce programme, le chercheur :

- Reconnaît agir **de bonne foi** dans le cadre d'un test responsable.
 - Accepte que les décisions finales de validation et de récompense reviennent à **[Nom de la société]**.
 - S'engage à respecter les lois belges et européennes en vigueur (RGPD, cybersécurité, confidentialité des données).
-

9. Remerciements

Nous remercions l'ensemble des chercheurs et membres de la communauté pour leur contribution à un internet plus sûr.

Votre expertise et votre collaboration sont essentielles à la protection de nos utilisateurs.

Annexe (optionnelle)

- Formulaire de soumission type (titre, gravité, étapes de reproduction, preuve, suggestion de correction)
- Contact d'urgence sécurité : security@[nom-entreprise].be

