



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Objectifs et règles de sécurité numérique du ministère de l'Intérieur

PGSN – E02

**Préconisations à la mise en place d'un
programme de Bug Bounty**

Version 1.0

TABLE DES MATIERES

1	QUELS SONT LES AVANTAGES DU BUG BOUNTY ?	4
2	QUELS SONT LES INCONVENIENTS D'UN BUG BOUNTY ?	4
3	LA PLATEFORME DE L'EDITEUR PROTEGERA-T-ELLE SUFFISAMMENT MES DONNEES ?	5
4	QUAND RECOURIR AU BUG BOUNTY ?	5
5	J'AI DEJA FAIT DES AUDITS PASSI, LE BUG BOUNTY ME SERA-T-IL VRAIMENT UTILE ?	5
6	AVEC UN BUG BOUNTY, LES AUDITS EXIGES DANS LA DISSIP RESTENT-ILS NECESSAIRES ?	5
7	ET SI LE CHERCHEUR GARDE POUR LUI SES DECOUVERTES ?	6
8	QUELS SONT LES PIEGES A EVITER ?	6
9	COMMENT BIEN PREPARER SON PROGRAMME ?	7
10	UNE FOIS LANCEE, AI-JE ENCORE LE CONTROLE DU PROGRAMME ?	7
11	QUE FAIRE LORSQUE LE PLAFOND DE MA CAGNOTTE EST PRESQUE ATTEINT ?	7
12	UN DISPOSITIF RESERVE AUX PROJETS EN MODE AGILE ?	8
13	DOIT-ON LE LANCER UNIQUEMENT SUR LES PLATEFORMES DE PRODUCTION ?	8
14	QUELS MARCHES POUR COMMANDER MON PROGRAMME ?	8
15	ANNEXE : MODELE D'ACCORD DE NON-DIVULGATION D'UN PROGRAMME.....	9

Préambule

Le présent document a vocation à répondre aux interrogations des directions et services du ministère de l'Intérieur sur la mise en place d'un programme de Bug Bounty.

Un Bug Bounty est une démarche de cybersécurité participative initiée par n'importe quelle entité qui souhaite en bénéficier.

L'objectif d'un Bug Bounty est d'offrir une récompense financière à toute personne qui trouvent des failles de sécurité dans un périmètre préalablement défini, chaque organisateur énonce les limites à ne pas franchir afin d'éviter tout débordement. Très concrètement, le Bug Bounty consiste à mettre en relation des chercheurs (de failles) avec des entreprises. Ces dernières demandent aux premiers de détecter les bugs dans les systèmes. Et de leur faire un rapport détaillé.

L'objectif principal du Bug Bounty est d'optimiser la correction des failles de sécurité informatique de façon préventive et ciblée. Il permet à l'entreprise de se concentrer sur l'essentiel et d'entrer dans une logique de résultat.

1 Quels sont les avantages du Bug Bounty ?

Les avantages d'un programme de Bug Bounty peuvent être nombreux :

- Financier : Malgré un coût de lancement important, les paiements des primes se font uniquement en fonction des rapports publiés par les chercheurs. C'est le commanditaire qui fixe les montants des récompenses en fonction du niveau de criticité des vulnérabilités et seuls les rapports détaillés, mettant en avant des failles réellement exploitables, feront l'objet d'un paiement.
- Optimisation dans la gestion des vulnérabilités : Un programme de Bug Bounty permet d'avoir un retour direct sur les failles découvertes et ainsi éviter au commanditaire de perdre cette connaissance au profit d'attaquant peu scrupuleux. Ainsi, le Bug Bounty permet d'être proactif sur sa sécurité en amenant l'information cruciale de la découverte d'une faille jusqu'au commanditaire.
- Expertises variées des chercheurs : Le Bug Bounty permet de disposer d'un vivier conséquent de chercheurs là où d'autres prestations sont limitées en termes de ressources humaines. Le commanditaire pourra donc bénéficier d'un éventail très important de profils expérimentés, pouvant amener à un nombre plus important de failles découvertes. Cela est également un facteur de maintenabilité du programme dans le cas où certains hackers qui se démotiveraient, d'autres pourront prendre le relais.
- Surveillance continue : un avantage d'un programme de Bug Bounty consiste à permettre des tests en continu, par un grand nombre de personnes. Grâce au Bug Bounty les systèmes de sécurité du commanditaire sont testés en permanence par une équipe d'hackers éthiques qui délivrent des retours riches et variés. Et permettent par la même occasion aux développeurs du commanditaire de monter en compétences. Là où un audit intervient une fois par an dans le meilleur des cas, sur une durée de quelques jours, le Bug Bounty permet de profiter d'une veille agile et constante 7j/7j, 24h/24h, et cela même si le code évolue.
- Gain sur l'image : un programme de Bug Bounty est signe d'une volonté de transparence en s'adressant à une communauté qu'on ne maîtrise pas directement. Un Bug Bounty contribue donc à l'amélioration de l'image de l'entité ayant recours à ce type de programme.

Communiquer autour du programme de Bug Bounty permet de rassurer quant à la robustesse de ses systèmes et met en valeur son état d'esprit proactif sur le sujet de la sécurité.

2 Quels sont les inconvénients d'un Bug Bounty ?

En fonction de la méthode retenue pour gérer un programme, ce dernier peut être chronophage et impliquer beaucoup de ressources qui ne seront donc pas allouées à d'autres tâches.

L'éthique des chercheurs est également un point qui peut être problématique tout comme le facteur humain l'est généralement pour tout système. En effet, il reste possible pour des chercheurs peu scrupuleux de profiter du programme de manière légale pour découvrir des failles sur l'application. Si l'appât du gain est plus important en exploitant cette faille ou si le chercheur souhaite nuire à l'image de l'organisme, il pourra ne pas vouloir fournir sa découverte.

Néanmoins, deux points viennent considérablement atténuer ce risque :

- Le recours à des programmes privés de Bug Bounty afin de pouvoir sélectionner des chercheurs de confiance sur des critères spécifiques.

- Le principe même de concurrence entre les chercheurs dans un programme. Le premier qui trouve la faille et qui publie un rapport viable sera celui qui touchera la prime, ainsi un chercheur n'a pas la garantie qu'il a l'exclusivité de sa découverte et peut donc perdre la rémunération associée s'il ne publie rien.

3 La plateforme de l'éditeur protégera-t-elle suffisamment mes données ?

Bénéficiant d'un hébergement SecNumCloud, la plateforme de Bug Bounty mis à disposition du ministère offre toutes les garanties requises pour protéger les rapports d'audits produits.

Par ailleurs, la plateforme de l'éditeur fait elle-même l'objet d'un programme de Bug Bounty permettant ainsi de s'assurer de la confidentialité des rapports stockés.

4 Quand recourir au Bug Bounty ?

Un programme de Bug Bounty ne doit pas être lancé sans prérequis, sous peine de le voir se terminer prématurément. Il convient donc de s'assurer que le SI cible est suffisamment robuste en termes de sécurité.

C'est pourquoi il est recommandé qu'un programme ne soit lancé que sur les SI dont un audit PASSI a été réalisé dans les 12 derniers mois et que tous les écarts identifiés ont été corrigés. Ne pas respecter ces prérequis reviendrait à payer deux fois pour la découverte d'une même vulnérabilité et surtout de voir sa cagnotte diminuer rapidement, pouvant ainsi mettre fin au programme.

5 J'ai déjà fait des audits PASSI, le Bug Bounty me sera-t-il vraiment utile ?

Il est important de ne pas confondre ces prestations.

Un audit PASSI se déroule sur une période de temps limitée où l'auditeur tente de trouver avant tout un maximum de vulnérabilités. La limite de ces prestations est qu'elles ne peuvent en aucun cas être exhaustives et peuvent amener l'auditeur à passer à côté de certaines failles qui nécessiteraient un investissement plus important pour être découvertes et exploitées. Un audit PASSI permet de s'assurer de la compétence des auditeurs et de garantir la robustesse du socle de sécurité. Un audit PASSI participera à une défense en profondeur au fur et à mesure de leurs reconductions.

Le Bug Bounty vient compléter ces prestations en permettant à des chercheurs de s'affranchir des limites temporelles (exception faite de celle imposée par la durée du programme) dans leurs recherches de vulnérabilités, tout en permettant au commanditaire de ne payer qu'aux résultats. Les chercheurs peuvent ainsi se focaliser sur une unique vulnérabilité et en découvrir toutes les conséquences possibles sur le système cible.

6 Avec un Bug Bounty, les audits exigés dans la DISSIP restent-ils nécessaires ?

Un programme de Bug Bounty ne doit en aucun cas remplacer les audits (PASSI ou non) demandés dans le cadre de la DISSIP. En effet, comme indiqué précédemment, les audits PASSI sont des prestations qui apportent des garanties de résultats et dont la compétence des auditeurs est garantie par la qualification ANSSI, ce qui n'est pas le cas des programmes de Bug Bounty et de ses chercheurs.

Par ailleurs, le manque de maturité du ministère dans l'emploi du Bug Bounty ne permet pas de s'affranchir des audits demandés dans la DISSIP. Cela ne veut pas dire que la démarche n'évoluera pas à l'avenir dans ce sens mais à ce stade, une telle option ne doit pas être envisagée dans une démarche d'homologation.

7 Et si le chercheur garde pour lui ses découvertes ?

Cette interrogation est source d'une grande inquiétude de la part des instances décisionnaires mais le Bug Bounty n'offre pas moins de garanties que les audits PASSI :

- Un accord de non-divulgaration est signé par les chercheurs lors de leur enrôlement à la plateforme de l'éditeur. Aucun chercheur ne peut participer à un programme sans avoir préalablement signé cet accord
- Chaque programme peut imposer, en plus de celui précédemment cité, son propre accord de non-divulgaration associé à son programme. Un chercheur devra donc en plus de celui de l'éditeur de la plateforme de Bug Bounty, signer celui propre au programme avant de pouvoir y participer.
- Le lancement d'un programme privé permet de limiter les chercheurs et donc de mieux les encadrer, au même titre que les prestations réalisées par des PASSI ;
- Tous les chercheurs sont des concurrents potentiels, ainsi une faille découverte par un chercheur qui souhaite la garder peut tout à fait être découverte par un autre qui lui voudra être payé pour cette découverte.
- Les chercheurs sont par défaut dans les conditions réelles d'un attaquant lambda. A ce titre, si votre système ne vous permet pas par défaut (notamment pour les systèmes ouverts sur Internet) de vous assurer le contrôle des failles découvertes, alors pourquoi se poser la question pour le Bug Bounty ?

In fine, les bénéfices à tirer du Bug Bounty sont bien plus à l'avantage de l'entité qu'autre chose. Le risque de divulgation existant déjà

8 Quels sont les pièges à éviter ?

Le manque ou l'absence de préparation est bien évidemment le plus gros écueil à éviter. Eviter les plus gros écueils, c'est réaliser à minima les étapes suivantes :

- Ne pas lancer un programme sur des systèmes dont les audits PASSI ont plus de 12 mois ;
- Avoir terminé les actions de remédiations issus des audits demandés par la DISSIP ;
- Ne pas se lancer directement dans un programme public. Ce type de programme doit être réservé uniquement aux systèmes ayant grandement éprouvé leur programme et en capacité opérationnelle de gérer le Bug Bounty.
- Identifier les acteurs clés du programme :
 - o Pilote du programme ;
 - o Expert technique amené à qualifier les rapports des chercheurs ;
 - o Gestionnaire des primes (par défaut, ce rôle est assuré par le pilote du programme) ;
 - o Coordinateur des équipes de développement. Il doit assurer la liaison entre les chercheurs et les équipes de développement si ces derniers n'ont pas directement accès à la plateforme.

- Réserver ou dédier les ressources nécessaires durant toute la durée du programme ;
- Attribuer une échelle de prime suffisante pour garantir l'appétence des chercheurs. Cette échelle devra évoluer dans le temps pour maintenir la motivation des chercheurs dans la durée.

9 Comment bien préparer son programme ?

Tout d'abord, on ne peut que conseiller de lancer un programme managé pour éviter que la charge en ETP ne pèse trop sur l'entité au détriment d'autres chantiers de l'entité du ministère.

Pour tout lancement, il convient de s'assurer des points suivants :

- Le respect du SI dans les prérequis du Bug Bounty ;
- La capacité des équipes de l'entité à gérer le programme. Les prestations de programme dit « managé » permettent de grandement alléger la charge des équipes et reste donc le mode de fonctionnement à privilégier ;
- Le cadrage du programme en amont afin de l'adapter au mode de fonctionnement des équipes de l'entité (ex : fonctionnement en mode Agile ou non) ;
- Ne pas négliger la sélection des chercheurs et le choix des primes. Ce dernier point est crucial pour attiser l'appétence des chercheurs et donc obtenir des résultats probants.

Note : Pour chaque prime, aucune commission ne sera reversée à l'éditeur conformément au cadre contractuel en place avec le ministère de l'Intérieur.

10 Une fois lancée, ai-je encore le contrôle du programme ?

C'est le commanditaire qui définit la marche à suivre et le périmètre de l'audit. Ainsi, cela permet d'y aller progressivement en proposant aux chercheurs uniquement les sites, applications ou services qui ont été retenus dans le cadre du programme.

C'est le commanditaire qui choisit le montant et le type des récompenses, que le programme de Bug Bounty soit public ou privé.

Il est également possible de stopper à tout moment le programme afin de prendre le temps de corriger les failles découvertes. Le commanditaire pourra alors relancer le programme quand il souhaitera, s'assurant ainsi de son total contrôle sur celui-ci.

11 Que faire lorsque le plafond de ma cagnotte est presque atteint ?

Dans la mesure où le commanditaire a le contrôle intégral de son programme, il lui est possible :

- Soit d'arrêter le programme avant la date d'échéance initialement prévue ;
- Soit d'alimenter sa cagnotte pour poursuivre le programme.

12 Un dispositif réservé aux projets en mode agile ?

Contrairement à une idée reçue, et ce qu'on peut lire sur Internet, le Bug Bounty est parfaitement modulable à n'importe quelle organisation et méthode de gestion de projet. Que celle-ci soit classique (Cycle en V) ou en mode agile, cela ne doit pas constituer un frein au lancement d'un programme.

Tout dépendra de la gestion du programme qui sera mise en place. L'objectif principal à garder en mémoire est qu'un programme de Bug Bounty vous permet d'éviter qu'une faille exploitable vous échappe. La connaissance est au final la meilleure arme face à l'évolution constante des risques. Ainsi, quelle que soit la méthode de gestion en place sur votre projet, un programme de Bug Bounty pourra être mis en œuvre pour renforcer la maîtrise des risques sur le système d'information cible.

13 Doit-on le lancer uniquement sur les plateformes de production ?

Au même titre qu'un audit PASSI, le Bug Bounty peut se faire sur une plateforme de pré-production. L'important reste que la plateforme audité doit être au même niveau de sécurité que la plateforme de production.

La seule contrainte sera donc architecturale dans le cas où les plateformes ne sont pas ouvertes sur Internet et donc non accessibles aux différents chercheurs. Cela devra être géré lors de l'élaboration du programme :

- Intervention des chercheurs sur site (pour les programmes privés) : nécessité de prévoir les moyens logistiques et humains pour l'encadrement des chercheurs ;
- Filtrage des accès : Login/mot de passe pour l'accès à l'application depuis Internet, filtrage depuis leur box Internet, ...

14 Quels marchés pour commander mon programme ?

Au travers de l'UGAP, deux types de prestations permettent de lancer un programme de Bug Bounty :

1. Prestations liées à la plateforme de Bug Bounty :

Référence SCC/UGAP	Nom UO	Description UO
YOG07	Espace Bug Bounty	Acquisition d'un Workspace ¹ sur la plateforme de l'éditeur pour le lancement d'un programme avec une cagnotte de 15 000 € HT.
YOG06	Cagnotte supplémentaire	Création d'un Workspace supplémentaire ou alimentation d'un cagnotte d'un programme existant d'un montant 15 000 € HT.
YOG08	Service Managé	Accompagnement au tri des rapports de vulnérabilité. Cette prestation s'accompagne de 5 jours d'expertise technique.

¹ Un Workspace correspond à un espace dédié sur la plateforme de l'éditeur pour gérer ses programmes de bug Bounty. Il n'y a pas de cloisonnement des accès aux données des programmes présents au sein d'un même Workspace.

2. Prestations d'initialisation et d'accompagnement à un programme :

Marché UGAP	Libellé	Description UO
Marché P2I - SOGETI	Lot 2 – Accompagnement Espace Bug Bounty	Accompagnement complet pour un programme avec cagnotte de 15 000 €. Cette prestation intègre le tri des rapports de vulnérabilité par un expert technique.
Marché P2I - SOGETI	Option 1 – Accompagnement Cagnotte Supplémentaire	Accompagnement complet pour cagnotte supplémentaire de 15 000 € avec tri des rapports de vulnérabilité par un expert technique.
Marché P2I - SOGETI	Option 2 – Conseil et Assistance remédiation	Prestation de conseil et d'accompagnement sur la remédiation des vulnérabilités découvertes lors du programme.

15 Annexe : Modèle d'accord de non-divulgaration d'un programme

Dans le cadre d'un programme qui souhaite ajouter à celui de l'éditeur de la plateforme, son propre accord de non-divulgaration, la trame suivante peut être utilisée et amendée le cas échéant :

Dans le cadre du présent programme, en tant que chercheur, vous considèrerez comme strictement confidentiel et vous vous engagez à ne pas divulguer à des tiers, toute information liée à une vulnérabilité, potentielle ou avérée, dont vous pourriez avoir connaissance à l'occasion du présent programme de Bug Bounty.

En tant que chercheur, vous vous engagez à ne pas faire état des résultats de vos recherches dans le cadre du programme à d'autres parties que le Client titulaire du programme.

En tant que chercheur, vous vous engagez à ne pas conserver de données au-delà de la durée d'ouverture du programme de Bug Bounty.

En tant que chercheur, vous vous engagez à alerter sans délais le Client titulaire du programme dans le cas où vous parviendriez à accéder à un autre système de traitement ne faisant pas partie du périmètre défini pour le présent Bug Bounty. Vous vous engagez ainsi, dès la découverte d'un tel évènement, à stopper les investigations sur ce système et à ne commettre aucune action pouvant le mettre en péril.