HACK THE GOVERNMENT

2026 | ÉVÉNEMENT DE CLÔTURE

DOSSIER DE PRESSE

Mercredi 25 novembre 2026 | Centre pour la Cybersécurité Belgique (CCB)

1. Informations pratiques pour la presse

Événement : Hack the Government 2026 | Événement de clôture
Date : mercredi 25 novembre 2026
Lieu : Quartier Papier | Fabrieksstraat 55/59, 1930 Zaventem
Contact presse : comm@ccb.belgium.be
La presse est la bienvenue sur place pendant tout le programme de la journée, jusqu'à la cérémonie de remise des prix.

Créneau réservé aux interviews : 12 h 00 – 13 h 00

Les représentants suivants se tiendront à la disposition de la presse entre 12 h 00 et 13 h 00 :

Miguel De Brucyker : Directeur général, Centre pour la Cybersécurité Belgique (le CCB)

Toute demande d'entretien individuel en dehors de ce créneau doit être adressée au préalable au service de presse du CCB.

2. Pourquoi la divulgation coordonnée de vulnérabilités (CVD) est-elle importante ?

Les vulnérabilités en matière de cybersécurité font partie intégrante de la vie numérique. Ce qui compte, ce n'est pas leur existence, mais la rapidité et le sens des responsabilités avec lesquels elles sont traitées une fois détectées. La divulgation coordonnée de vulnérabilités (CVD) est le processus structuré par lequel les chercheurs signalent les vulnérabilités à l'organisation concernée et à une autorité de confiance, laissant ainsi aux développeurs le temps de corriger le problème **avant** qu'il ne puisse être exploité.

La Belgique dispose de l'un des cadres de CVD les plus avancés d'Europe. La **loi NIS2 de 2024** protège explicitement les hackers éthiques qui découvrent et divulguent de manière responsable des vulnérabilités de bonne foi, même en l'absence de programme officiel de *bug bounty*. Le CCB joue le rôle de point de coordination national : il reçoit les signalements et assure la médiation entre le chercheur et l'organisation tout au long du processus de correction (pour en savoir plus, voir **l'annexe 1** et la page web dédiée du CCB).

Cas récent : l'incident PHP2Shell (octobre 2026)

L'importance d'un processus de CVD solide a été mise en lumière en octobre 2026 par l'affaire **PHP2Shell** : une vulnérabilité critique permettant l'exécution de code à distance dans PHP, l'un des langages côté serveur les plus largement déployés sur le Web. Le 21 octobre 2026, des versions corrigées ont été publiées, mais le processus de divulgation coordonnée **s'est effondré** avant que le correctif ne puisse être appliqué à grande échelle : la fuite d'identifiants CVE, la diffusion accidentelle d'une vidéo et la distribution prématurée de correctifs par certains éditeurs ont levé l'embargo de fait, déclenchant une vague d'opérations de maintenance d'urgence dans les banques, les services publics, les plateformes de jeux et chez les hébergeurs web.

> **La leçon:** lorsque le processus de divulgation coordonnée fonctionne, les défenseurs prennent une longueur d'avance. Lorsqu'il échoue (en cas de fuite, de publication prématurée ou de défaut de notification), les attaquants agissent avant même que le correctif ne soit déployé. PHP2Shell illustre parfaitement pourquoi le processus CVD doit être rigoureux, fiable et solidement ancré dans le droit.

L'incident PHP2Shell illustre également une tendance plus large : les vulnérabilités non corrigées ou récemment révélées dans des technologies largement utilisées attirent rapidement l'attention. Hack the Government contribue directement à l'écosystème national de CVD en formant la prochaine génération de chercheurs aux pratiques de divulgation responsable, et en soumettant les systèmes gouvernementaux à des tests de résistance dans des conditions légalement contrôlées avant que des adversaires ne puissent découvrir ces mêmes faiblesses.

3. L'IA et la course aux vulnérabilités : ce que révèlent les données

L'intelligence artificielle modifie la vitesse à laquelle les attaquants peuvent développer et déployer des exploits. Les données sont désormais suffisamment solides pour affirmer que **l'IA accélère le développement d'exploits et l'automatisation des attaques,** mais la réalité est plus nuancée que ne le suggèrent parfois les gros titres.

Ce que révèlent les données indépendantes

L'IA réduit les délais dans la course à l'exploitation des vulnérabilités, mais il n'existe **pas de « délai d'exploitation » unique et universel**. La publication du code d'exploitation, la première exploitation observée et la confirmation officielle dans un catalogue de vulnérabilités connues comme exploitées (KEV) constituent des étapes distinctes, chacune suivant son propre calendrier.

Les données actuelles montrent que certaines vulnérabilités à fort impact, en particulier celles affectant les technologies connectées à Internet et les technologies de périphérie, peuvent être transformées en armes ou exploitées **dans les heures qui suivent leur divulgation, voire avant celle-ci**. Les systèmes d'IA peuvent désormais automatiser des étapes clés de la recherche sur les vulnérabilités et du développement d'exploits, et les fournisseurs de renseignements sur les menaces ont commencé à observer ces capacités dans des attaques réelles.

Malgré tout, **la plupart des vulnérabilités divulguées ne sont jamais activement exploitées dans le monde réel**, et les recherches disponibles ne permettent pas d'établir dans quelle mesure l'IA a raccourci le délai entre la divulgation et l'exploitation dans le domaine public (*in the wild*) pour l'ensemble des vulnérabilités et expositions communes (CVE) (**l'annexe 2** fournit une explication détaillée et des données).

Pourquoi cela renforce, et non affaiblit, l'importance de HTG

Si l'IA réduit le délai entre la divulgation d'une vulnérabilité et son exploitation pour des cibles de grande valeur, **cela renforce, et non affaiblit,** l'argument en faveur **d'une découverte** proactive et **éthique des vulnérabilités par des chercheurs humains de confiance**. Détecter et corriger les vulnérabilités avant qu'elles ne tombent dans le domaine public est désormais une course où les défenseurs ne peuvent plus compter sur des semaines, ni sur des mois. Hack the Government place les bonnes personnes, bénéficiant des protections juridiques adéquates, du bon côté de cette course.

4. Le rôle du CCB : construire la communauté nationale

En tant qu'autorité nationale de cybersécurité, le Centre pour la Cybersécurité Belgique joue un double rôle dans Hack the Government : il est à la fois **l'autorité organisatrice** et un **partenaire actif**, aidant les organisations gouvernementales à dialoguer de façon constructive avec la communauté des hackers éthiques, souvent pour la première fois.

HTG 2026 porte sur 12 systèmes gouvernementaux (près du triple de la première édition, en 2024), avec la participation, cette année, de plusieurs organisations, dont le SPF Justice, la Police fédérale, l'Agence des médicaments (AFMPS) et la Défense. Cette croissance témoigne d'une relation de plus en plus mature entre les institutions publiques et la communauté des hackers éthiques, soutenue par le cadre juridique belge, résolument progressiste, en matière de CVD (**cf. annexe 1**).

Trois éditions : aperçu des résultats

Indicateur	Édition 1 (2024)	Édition 2 (2025)	Édition 3 (2026)
Participants	-	71	77
dont seniors / professionnels	-	39	45
dont étudiants	-	32	32
Rapports de vulnérabilité soumis	154	352	À confirmer (en direct)
Vulnérabilités validées	85	98	À confirmer (en direct)
dont critiques / exceptionnelles	7	20	-
dont élevées	15	12	-
Systèmes gouvernementaux concernés	4	8	12

Voir la fiche d'information complète **à l'annexe 3**.

5. Ce qu'en disent les participants

« Hack the Government » est bien plus qu'un simple concours. Pour de nombreux participants, cet événement marque un tournant dans leur carrière : une première véritable immersion dans la sécurité offensive professionnelle, l'occasion de se constituer un réseau et une preuve de compétences

qu'aucun diplôme ne saurait pleinement remplacer. Voici quelques témoignages de participants aux éditions précédentes:

> **« Hack the Government était bien plus qu'un simple concours de piratage. Ce fut une étape importante dans mon parcours professionnel. »**
>
> **Pedro (alias : drop)** | Consultant indépendant en sécurité offensive ; testeur d'intrusion senior dans le secteur gouvernemental ; co-capitaine de l'équipe nationale belge HackerOne
>
> *Pedro a participé à la première édition de HTG (2024), où il a terminé troisième. Après une reconversion depuis le marketing et la science des données, il s'est appuyé sur les programmes de bug bounty et sur HTG pour faire la preuve de ses compétences sur le terrain, ce qui lui a permis de décrocher une mission de longue durée dans une grande institution internationale ainsi qu'une invitation à représenter la Belgique à la Coupe du monde HackerOne.*

> **« Le fait qu'en Belgique, nous puissions suivre des lignes directrices, tester pratiquement n'importe quoi et en être reconnus est incroyable et unique au monde. »**
>
> **Logan** | Étudiant en dernière année de master ; chasseur de bugs actif ; contributeur au programme national de CVD du CCB
>
> *Déjà actif dans le CVD deux ans avant la fin de ses études, il s'est servi de HTG pour nouer des contacts qui lui ont directement permis de découvrir des vulnérabilités qu'il n'aurait pas repérées seul.*

> **« Des événements comme HTG montrent que les hackers et les pouvoirs publics peuvent travailler ensemble plutôt que les uns contre les autres, et c'est ainsi que l'on renforce la sécurité. »**
>
> **Timothy** | Chasseur de bug bounty ; a créé sa propre entreprise de cybersécurité en juin 2026 ; a participé à HTG pour la première fois à 16 ans
>
> *Sa première participation à HTG a été un véritable électrochoc : il n'avait pratiquement rien trouvé. Il est revenu, a terminé 7e en 2025 et attribue sa décision de lancer son entreprise à l'état d'esprit forgé grâce à HTG.*

Les témoignages complets sont disponibles à **l'annexe 4**.

6. Foire aux questions

Qu'est-ce qu'un hacker éthique ?

À l'origine, le terme « hacker » désignait des personnes passionnées par le bricolage : des experts dans l'art d'explorer les systèmes et de repousser leurs limites. Dans le contexte de la cybersécurité, un **hacker éthique** est un chasseur de vulnérabilités qui agit de manière légale et constructive : il identifie les failles de sécurité et les signale de manière responsable, plutôt que de les exploiter à des fins personnelles. Il s'agit, en substance, de défenseurs qui pensent comme des attaquants.

Qu'est-ce que « Hack the Government » ?

Hack the Government (HTG) est une initiative du CCB qui invite des hackers éthiques sélectionnés à tester les systèmes informatiques des institutions publiques belges dans des conditions légalement contrôlées. Son seul objectif est de détecter et de signaler les vulnérabilités de manière responsable avant que des acteurs malveillants ne puissent les trouver. Il s'agit d'un véritable appel à la collaboration entre la communauté des hackers, les pouvoirs publics et le monde académique.

Les participants bénéficient-ils d'une protection juridique ?

Oui. En vertu de la loi belge du 26 avril 2024 et du cadre national de CVD du CCB, les participants qui agissent de bonne foi, en limitant leurs actions au strict nécessaire, sans intention malveillante, et en signalant leurs découvertes à l'organisation responsable et au CCB, bénéficient d'une protection juridique.

Qui peut participer ?

HTG 2026 a réuni **77 participants** : 45 hackers éthiques expérimentés ou professionnels et 32 étudiants. Les participants sont sélectionnés à l'issue d'un processus de candidature et doivent accepter des règles d'engagement strictes. Le programme est explicitement conçu pour mélanger les niveaux d'expérience et contribuer à réduire la pénurie de talents en mettant en relation étudiants et professionnels chevronnés dans un cadre pratique et en conditions réelles.

Quels sont les systèmes testés ?

Douze systèmes gouvernementaux sont concernés par HTG 2026, notamment ceux du SPF Justice et de la Police fédérale. Les organisations participent sur la base du volontariat, et le périmètre de chaque système testé est défini à l'avance. Les résultats sont communiqués exclusivement aux organisations concernées et au CCB ; ils ne sont pas rendus publics pendant l'événement.

Que se passe-t-il après l'événement ?

Toutes les vulnérabilités validées sont communiquées aux organisations concernées, qui sont ensuite chargées de les corriger. Le CCB assure le suivi des mesures correctives dans le cadre de son processus de divulgation coordonnée. Les résultats finaux de HTG 2026 seront publiés à l'issue de l'événement.

Annexes

- **Annexe 1 : Cadre CVD du CCB (aperçu)** : politique belge de divulgation coordonnée de vulnérabilités, protections juridiques et processus de signalement.
- **Annexe 2 : L'IA et la course aux vulnérabilités :** ce que révèlent réellement les données.
- **Annexe 3 : Fiche d'information HTG 2026** (mise à jour) : l'impact des trois éditions en chiffres.
- **Annexe 4 : Témoignages de participants** : Pedro (alias drop), Logan, Timothy.

Contact : Service de presse du CCB
Michele Rignanese |michele.rignanese@ccb.belgium.be | +32 477 38 87 50

Katrien Eggers |katrien.eggers@ccb.belgium.be | +32 485 76 53 36

L'ensemble du contenu rédactionnel et statistique est arrêté au 19 novembre 2026 et pourra être actualisé dès la publication des résultats définitifs de HTG 2026.

CVD EN BELGIQUE

Une faille de sécurité ?

CENTRE FOR CYBERSECURITY BELGIUM

Signalez-la. Aidez à la corriger.

La divulgation coordonnée des vulnérabilités (CVD) consiste à signaler une faille en toute confidentialité pour permettre aux responsables de la corriger.

LE PROCESSUS DE DIVULGATION [1, 3]

1. **Consultez les règles**

   Consultez la politique de divulgation de l'organisation, si elle en a une. Respectez son périmètre et ses consignes de signalement.

2. **Vérifiez avec prudence**

   Limitez-vous au nécessaire pour confirmer la faille. Évitez toute perturbation et tout accès inutile aux données.

3. **Signalez en toute confidentialité**

   Indiquez à l'organisation les éléments touchés et comment reproduire le problème. Utilisez un canal sécurisé.

4. **Participez à la correction**

   L'organisation analyse la faille et prépare un correctif. Restez en contact ; le CCB peut faciliter la coordination.

5. **Coordonnez toute publication**

   La publication est facultative. Dans le cadre de la procédure légale, obtenez l'autorisation du CCB avant de publier.**

PROCÉDURE LÉGALE FACULTATIVE [2]

La protection légale en Belgique

Accessible avec ou sans politique CVD de l'organisation.

Signalez au plus vite, au plus tard sous :

24 heures

Rapport initial

Identifiez le système et décrivez brièvement la faille.

72 heures

Rapport complet

Expliquez comment la reproduire, avec les détails techniques clés.

DESTINATAIRES DES DEUX RAPPORTS

Organisation + CCB

Les deux délais débutent à la découverte.*

RESPECTEZ LES CONDITIONS [1, 2]

Agissez de bonne foi

Ni menaces, ni extorsion, ni usage abusif des données.

Vérifiez avant de tester

Certaines organisations sensibles exigent un accord écrit préalable.

Connaissez les limites

Protection soumise à conditions, valable uniquement en droit belge.

Utilisez les formulaires du CCB et ses consignes d'envoi sécurisé [2]

vulnerabilityreport@ccb.belgium.be

* Découverte : moment où vous devriez raisonnablement identifier une vulnérabilité potentielle, après investigation et validation raisonnables.

** Le délai de 90 jours court à compter d'une demande formelle de publication au CCB.
Si aucun refus n'est notifié avant son expiration, la publication peut être considérée comme autorisée.

CCB = Centre pour la Cybersécurité Belgique

[1] ccb.belgium.be/regulation/cvdp

[2] ccb.belgium.be/cert/vulnerability-reporting-ccb

[3] Guide du CCB, partie I : processus

L'IA et la course aux failles de sécurité :

Ce que révèlent réellement les données

Annexe presse | Hack the Government 2026 | Centre pour la Cybersécurité Belgique 25 novembre 2026

1. Le « délai d'exploitation[1] » n'est pas un indicateur unique

Les articles consacrés aux cybermenaces accélérées par l'IA traitent souvent le « délai d'exploitation » comme un chiffre unique et comparable. Ce n'est pas le cas. Au moins quatre repères temporels différents sont régulièrement confondus dans les rapports publics, et leur amalgame produit des chiffres qui ne sont pas directement comparables.

Indicateur	Ce qu'il mesure réellement	Pourquoi c'est important	Mise en garde essentielle
Divulgation du CVE[2] → exploit public / PoC[3]	Délai avant la publication d'un code d'exploitation ou d'une preuve de concept	Mesure la disponibilité publique d'un exploit, et non son utilisation par les attaquants	Disponibilité de l'exploit ≠ exploitation en milieu réel
Divulgation du CVE → première exploitation observée	Délai avant l'apparition de preuves crédibles montrant que des attaquants exploitent la vulnérabilité en conditions réelles	Mesure l'exploitation dans le monde réel	L'observation peut intervenir après la première attaque effective
Exploitation avant la divulgation	L'exploitation a lieu avant la divulgation publique du CVE ou la mise à disposition d'un correctif	Cas classique de « zero-day[4] » : le décalage peut être négatif	La date de divulgation ne marque pas le début de la course
Publication du CVE → inscription sur la liste KEV[5]	Délai nécessaire à un fournisseur de renseignements sur les menaces pour réunir des preuves suffisantes afin de classer un CVE comme exploité	Reflète à la fois le délai de confirmation et de signalement et l'activité des attaquants	L'inscription au KEV intervient après l'exploitation effective

L'agence américaine de cybersécurité (CISA) distingue explicitement une **preuve de concept (PoC) publique d'une exploitation active** : pour qu'une exploitation soit qualifiée d'« active », il faut des preuves partagées, observables et fiables indiquant que des acteurs malveillants ont utilisé la vulnérabilité en conditions réelles. De la même manière, VulnCheck fonde son analyse sur les *premières preuves*

[1] Dans la littérature anglophone désigné par « *time-to-exploit* » ou TTE.
[2] **CVE** (*Common Vulnerabilities and Exposures*, ou « vulnérabilités et expositions communes ») est un catalogue public et un système d'identifiants uniques qui répertorie les failles de sécurité informatique connues.
[3] En cybersécurité, une preuve de concept (souvent appelée **PoC**, pour *proof of concept*) est une démonstration concrète qui prouve l'existence d'une faille ou d'une vulnérabilité informatique, généralement à l'aide d'un programme ou d'une méthode de test.
[4] En cybersécurité, une vulnérabilité **zero-day** (ou faille zero-day / 0-day) est une faille de sécurité informatique inconnue du public et de l'éditeur, pour laquelle aucun correctif n'a encore été publié.
[5] En cybersécurité, la **liste KEV** (ou catalogue *Known Exploited Vulnerabilities*, traduit en français par « vulnérabilités exploitées connues ») est un référentiel public tenu par la CISA, l'agence américaine de cybersécurité.

d'exploitation, et non simplement sur la date d'apparition du code d'exploitation. Cette distinction explique les contradictions apparentes entre les chiffres avancés par différents fournisseurs.

2. Ce que révèlent les données indépendantes

VulnCheck — Analyse des exploitations du premier semestre 2026

VulnCheck a examiné 495 vulnérabilités nouvellement identifiées comme exploitées au cours du premier semestre 2026 :

- **23,43 %** présentaient des preuves d'exploitation **à la date de publication du CVE ou avant** (les attaquants ont agi avant même que le correctif n'existe). Le chiffre correspondant pour 2025 s'élevait à 28,93 %.
- Délai médian entre la publication du CVE et son inscription sur la liste KEV : 80 jours, contre 120 jours en 2025.
- Environ 200 CVE ont été inscrits sur la liste KEV en moins de 31 jours au premier semestre 2026, un chiffre globalement stable par rapport à 196 (2024) et 194 (2025), alors que le volume total de CVE a fortement augmenté. Ce constat contredit nettement l'idée selon laquelle toutes les vulnérabilités seraient exploitées en quelques heures.
- VulnCheck met expressément en garde contre le problème de maturation : les cohortes récentes de CVE continuent d'accumuler des preuves d'exploitation au fil du temps (les premiers chiffres sous-estiment systématiquement l'exploitation des CVE récentes).

Google Threat Intelligence Group (GTIG) : analyse de 2026

Le GTIG a recensé **141 vulnérabilités** à la fois divulguées et exploitées entre janvier et août 2026, contre 127 pour l'ensemble de l'année 2025. La moyenne mensuelle est passée de 10,5 à 18.

- Toutefois, seulement environ 0,23 % des vulnérabilités divulguées dans le jeu de données 2026 ont fait l'objet d'une exploitation active.
- Cette augmentation s'explique en grande partie par l'exploitation rapide des vulnérabilités de type « n-days » (vulnérabilités récemment corrigées) et non par une explosion du nombre de vulnérabilités de type « zero-day ».
- Les vulnérabilités « zero-day » ont augmenté plus modérément (d'une moyenne de 8 à 11 par mois) avant de connaître un pic en août.

Mandiant M-Trends 2026 et Verizon DBIR 2026

Les données de Mandiant relatives à la réponse aux incidents font état d'un délai d'exploitation (TTE, « time-to-exploit ») moyen estimé à -7 jours, ce qui signifie que, dans cet échantillon, l'exploitation a souvent précédé la publication du correctif. Il s'agit d'un indicateur *relatif aux correctifs*, et non d'un indicateur mesurant le délai entre la divulgation d'un CVE et son exploitation.

Le rapport DBIR 2026 de Verizon montre que les vulnérabilités constituent un vecteur d'intrusion de plus en plus fréquent dans les violations de données (31 % des violations) et fait état d'un recours croissant à l'IA dans de multiples techniques d'attaque. Il n'établit toutefois pas que l'IA, à elle seule, ait entraîné une réduction généralisée du délai d'exploitation.

3. Ce que nous savons aujourd'hui des capacités de l'IA

Les éléments attestant le développement d'exploits assisté par l'IA se sont considérablement multipliés en 2026 :

- **Mai 2026 | Google** : a signalé avoir observé, pour la première fois, un acteur malveillant utilisant un exploit « zero-day » qui aurait été développé avec l'aide de l'IA.
- **Octobre 2026 | Anthropic** : un modèle de recherche interne a découvert et élaboré des chaînes d'exploits en plusieurs étapes visant Chrome, Safari, Android, Windows et Linux, y compris des failles exploitables à distance et des évasions de bac à sable (*sandbox*).
- **16 novembre 2026 | GTIG/Mandiant** : a signalé avoir observé des acteurs malveillants utilisant des frameworks fondés sur des LLM pour automatiser entièrement la découverte de vulnérabilités, l'analyse différentielle des correctifs, la conception et l'exécution d'exploits (sans intervention humaine), y compris lors d'activités d'intrusion en temps réel. Un seuil qualitatif a ainsi été franchi.

> **État des lieux en novembre 2026 :** *« L'IA améliore nettement les capacités de découverte de vulnérabilités et de développement d'exploits, et commence à raccourcir certains scénarios d'attaque dans le monde réel. À ce jour, rien ne prouve l'existence d'une fenêtre d'exploitation universelle, pilotée par l'IA et mesurée en heures, pour l'ensemble des CVE. Pour les cibles de grande valeur, les attaquants fixent leurs priorités (en particulier sur les technologies exposées à Internet et les équipements de périphérie) ; les défenseurs peuvent n'avoir que quelques heures, et non plusieurs jours, pour réagir. »*

4. Ce que cela signifie pour les défenseurs

La tendance est claire et exploitable, même si aucun chiffre isolé ne rend compte de toute la réalité. L'IA abaisse la barrière d'entrée pour développer des exploits. La question stratégique n'est pas *« de combien d'heures exactement les défenseurs disposent-ils ? »* : la réponse varie fortement selon le type de vulnérabilité, l'exposition et le profil de l'attaquant. La vraie **question est :** « repérons-nous nos vulnérabilités avant qu'un adversaire assisté par l'IA ne le fasse ? »

C'est précisément à cette question que répond « Hack the Government » (HTG). En confrontant des hackers éthiques agréés (dont des chercheurs qui utilisent activement des outils assistés par l'IA) aux systèmes gouvernementaux, dans un cadre légal et contrôlé, HTG offre aux défenseurs le test le plus réaliste possible de leur exposition.

> **La divulgation coordonnée de vulnérabilités est la réponse structurelle.**
>
> Que le délai se compte en heures ou en mois, les organisations les mieux placées pour réagir sont celles qui ont déjà mis en place un processus fiable de réception, de tri et de correction des signalements de vulnérabilités. Le cadre belge de divulgation coordonnée des vulnérabilités (CVD), inscrit dans la loi depuis décembre 2022, offre précisément cette infrastructure.

5. Sources principales

Les sources suivantes ont été utilisées pour la préparation de cette annexe.

- Cogent Security — Rapport sur les lacunes de détection, 2e trimestre 2026 (article de blog)
- Cogent Security — Rapport sur les lacunes de détection, 2e trimestre 2026 (salle de presse / méthodologie)
- VulnCheck — État des lieux de l'exploitation au 1er semestre 2026
- Google Threat Intelligence Group — Tendances en matière de découverte et d'exploitation des vulnérabilités à l'ère de l'IA (30 septembre 2026)
- GTIG/Mandiant — L'activité des menaces agentiques franchit un seuil significatif (16 novembre 2026)
- Mandiant — M-Trends 2026
- Anthropic — Découverte et exploitation de vulnérabilités dans des logiciels critiques du monde réel avec Claude (27 oct. 2026)
- Google — Les attaquants exploitent l'IA pour exploiter les vulnérabilités, renforcer leurs opérations et obtenir un accès initial
- Verizon — Rapport 2026 sur les enquêtes relatives aux violations de données (DBIR)
- CISA — Guide SSVC (distinguer une preuve de concept (PoC) d'une exploitation active)

Cette annexe a été préparée par le Centre pour la Cybersécurité Belgique (CCB) à l'intention des médias à l'occasion de l'événement final « Hack the Government 2026 » (25 novembre 2026). Les informations qu'elle contient sont à jour au 19 novembre 2026.

HACK THE GOVERNMENT 2026

Fiche d'information : trois éditions, un impact tangible et un besoin qui ne cesse de croître

Hack the Government en chiffres

Indicateur	1re édition – 2024	2e édition – 2025	3e édition – 2026
Date de l'événement final	*27 novembre 2024*	*26 novembre 2025*	*25 novembre 2026*
Nombre total de participants	*n.d.*	*71*	*77*
Participants seniors / professionnels	*n.d.*	*39*	*45*
Participants juniors (étudiants)	*n.d.*	*32*	*32*
Rapports de vulnérabilité soumis	*154*	*352*	*À confirmer (en cours)*
Vulnérabilités validées	*85*	*98*	*À confirmer (en cours)*
dont critiques / exceptionnelles	*7*	*20*	
dont « élevées »	*15*	*12*	
dont moyennes / faibles	*55*	*66*	
dont hors périmètre, mais validées	*8*	*9*	
Systèmes gouvernementaux / périmètres testés	*4*	*8*	*12*

Source : rapport interne de Hack the Government.

Pourquoi est-ce important ? La pénurie de talents en cybersécurité en Belgique

Hack the Government ne se contente pas de renforcer aujourd'hui la sécurité des systèmes gouvernementaux : il contribue aussi à développer le vivier de talents dont la Belgique a besoin.

Une étude **KPMG* de 2025** consacrée au secteur belge de la cybersécurité quantifie un défi que chaque participant connaît de près :

environ 4 000
postes vacants en cybersécurité en Belgique

44 %
des organisations mettent 4 à 6 mois à recruter un expert en cybersécurité

19 %
mettent 7 à 12 mois à pourvoir le poste

43 %
des organisations estiment que le recrutement d'experts en cybersécurité est plus difficile qu'il y a un an

1 à 5
spécialistes dédiés à la cybersécurité : c'est la norme pour la moitié des organisations belges

1 sur 3
des organisations n'emploient aucune femme dans des postes liés à la cybersécurité

** Source : KPMG, Étude sur la cybersécurité en Belgique (2025), pp. 48–51.*

CENTRE FOR CYBERSECURITY BELGIUM

Hack the Government 2026

Témoignages de participants

Des hackers éthiques prennent la parole

TROIS REGARDS

Parcours, communauté et enseignements de Hack the Government.

01 **Pedro** — PAGE 2

Consultant indépendant en sécurité offensive · alias drop

« Je n'en serais pas là aujourd'hui sans la communauté. »

02 **Logan** — PAGE 6

Étudiant en dernière année de master

« Nouez aussi des contacts. »

03 **Timothy** — PAGE 7

Chercheur de vulnérabilités et entrepreneur en cybersécurité

« Vous pouvez apprendre beaucoup en prêtant attention à ce que disent les autres. »

TÉMOIGNAGE 01

Pedro

Consultant indépendant en sécurité offensive · alias drop

> *« Je n'en serais pas là aujourd'hui sans la communauté. »*

1 Pourriez-vous vous présenter et nous donner un bref aperçu de votre parcours professionnel ? Qu'est-ce qui vous a attiré vers les tests d'intrusion ?

Je m'appelle Pedro, mais je suis aussi connu sous le nom de drop au sein de la communauté du bug bounty.

Je suis consultant indépendant en sécurité offensive et je travaille avec différentes entreprises privées et institutions gouvernementales. Je suis actuellement en mission de longue durée dans le secteur gouvernemental en tant que spécialiste senior des tests d'intrusion.

Ce qui est intéressant dans mon parcours, c'est que je n'ai pas suivi une voie classique pour arriver dans la cybersécurité. À l'origine, je venais du marketing et de la science des données. Mais pendant la pandémie de Covid-19, j'ai décidé de consacrer énormément de temps à la cybersécurité, et j'ai finalement réussi à me reconvertir complètement.

J'ai en fait commencé du côté défensif, en travaillant dans l'investigation numérique et les opérations de sécurité. Mais au fond, je savais dès le départ que c'était dans la sécurité offensive que je voulais évoluer.

Le défi, c'était de prouver que j'avais les compétences, surtout sans avoir un parcours classique dans ce domaine.

Et c'est là que le bug bounty est entré en jeu.

Pour moi, le bug bounty était le moyen idéal de montrer ce que je savais faire concrètement, plutôt que de m'appuyer uniquement sur des certifications ou un CV.

Et honnêtement, c'est vraiment là que tout a commencé pour moi. Cela m'a ouvert tellement de portes et a joué un rôle énorme dans la construction de la carrière que j'ai aujourd'hui.

2 Quelle importance accordez-vous au fait d'être reconnu comme hacker éthique ? Que représente la communauté du hacking éthique pour vous et pour la Belgique ?

Pour moi, être hacker éthique, c'est avant tout un état d'esprit. Et je pense que cet état d'esprit va bien au-delà de l'aspect technique de la cybersécurité.

Il s'agit d'être curieux, de s'interroger sur le fonctionnement des choses et de trouver des façons de résoudre des problèmes auxquelles personne n'avait encore pensé.

Cela peut paraître un peu cliché, mais il s'agit littéralement de sortir des sentiers battus.

Il s'agit de faire fonctionner des systèmes, des applications, voire des processus, d'une manière qui n'avait jamais été prévue, de repousser les limites et, au bout du compte, de démontrer un impact ou de trouver des solutions créatives à des problèmes complexes.

Et je pense que c'est extrêmement précieux, pas seulement dans la cybersécurité, mais aussi pour les organisations avec lesquelles nous travaillons.

Quant à la communauté, pour moi, elle représente tout.

Pedro

TÉMOIGNAGE 01 / SUITE

CENTRE FOR CYBERSECURITY BELGIUM

QUESTION 02 / SUITE

J'ai travaillé dans différents secteurs avant la cybersécurité, et je peux sincèrement dire que la communauté du hacking a quelque chose de particulier.

Les gens sont incroyablement accueillants. Ils aiment partager leurs recherches, leurs bugs, leurs réussites, mais aussi leurs échecs et leurs limites.

Et c'est quelque chose que j'apprécie vraiment.

Je n'en serais pas là aujourd'hui sans la communauté. Le partage de connaissances, la collaboration, les conférences et toutes les personnes que j'ai rencontrées en chemin ont joué un rôle considérable dans mon parcours.

Et je pense que la Belgique possède une communauté de hackers éthiques vraiment solide et talentueuse, même si nous ne nous en rendons pas toujours compte.

D'ailleurs, je suis actuellement l'un des co-capitaines de l'équipe belge qui participera à la nouvelle HackerOne World Cup.

Et j'espère que nous monterons sur le podium ! Ce serait une formidable réussite pour la communauté belge du hacking.

3 Qu'est-ce qui vous a amené à participer à Hack the Government ?

J'ai entendu parler de Hack the Government pour la première fois à BruCON, en 2024.

Et je me souviens m'être dit : « Attendez, hacker le gouvernement ? Légalement ? C'est une occasion que je ne peux pas manquer ! »

Alors, bien sûr, j'ai immédiatement décidé de participer.

C'était la toute première édition, ce qui rendait l'expérience encore plus passionnante.

Pour moi, c'était l'occasion idéale de me lancer un défi, de confronter mes compétences à celles d'autres hackers talentueux et de voir où je me situais par rapport à mes pairs.

J'étais aussi curieux de voir comment les autres hackers aborderaient les mêmes cibles et quels types de vulnérabilités ils découvriraient.

Et lors de cette première édition, j'ai réussi à terminer à la troisième place, ce qui m'a vraiment fait plaisir !

C'était une très belle expérience, d'autant plus qu'à l'époque, je construisais encore ma réputation au sein de la communauté.

4 Pourriez-vous partager un souvenir marquant ou une anecdote à propos de Hack the Government ?

Oh, absolument !

Je pense que mon souvenir le plus marquant est d'avoir reçu la pièce commémorative de l'événement directement des mains du Premier ministre belge.

C'était vraiment un moment particulier !

Je me souviens avoir été très fier à ce moment-là, et je n'arrêtais pas de montrer la photo à mes collègues, à mes amis et à ma famille.

Franchement, combien de fois a-t-on l'occasion de dire qu'on a hacké des systèmes gouvernementaux en toute légalité, puis reçu une pièce du Premier ministre ?

Pedro

TÉMOIGNAGE 01 / SUITE

CENTRE FOR CYBERSECURITY BELGIUM

QUESTION 04 / SUITE

C'est assurément un excellent sujet pour engager la conversation !

Et au-delà de cette reconnaissance, c'était aussi un très beau moment, parce qu'il montrait que le hacking éthique était pris au sérieux et reconnu à un tel niveau.

Pour moi, cela comptait vraiment beaucoup.

5 Qu'avez-vous retiré de Hack the Government, et cela a-t-il influencé ce que vous avez fait par la suite ?

Je dirais que l'un des principaux apports de Hack the Government a été de me donner de la visibilité et de la crédibilité.

À ce stade de ma carrière, je cherchais encore à me faire une place dans la sécurité offensive.

Et participer à un événement comme celui-là, surtout en terminant sur le podium, était un excellent moyen de démontrer mes compétences et de montrer que je savais ce que je faisais.

Cela m'a aussi permis de rencontrer beaucoup de personnes intéressantes, de nouer des liens et de gagner en visibilité au sein de la communauté belge de la cybersécurité.

Et je pense sincèrement que cette visibilité m'a aidé à être invité à prendre la parole lors de conférences, à participer à des événements de hacking en direct et à accéder ensuite à d'autres opportunités.

Bien sûr, ce n'était pas la seule raison pour laquelle ces opportunités se sont présentées, mais cela a clairement contribué à m'ouvrir des portes.

Avec le recul, Hack the Government a donc été bien plus qu'une simple compétition de hacking pour moi. Cela a aussi été une étape importante dans mon parcours professionnel.

6 Qu'est-ce que Hack the Government vous apporte encore aujourd'hui ?

Aujourd'hui, je dirais que ce que l'événement m'apporte est un peu différent.

Bien sûr, j'aime toujours le défi technique et la compétition. Cela fera toujours partie de ma personnalité.

Mais ce que j'apprécie le plus maintenant, c'est l'aspect communautaire.

C'est l'occasion de retrouver des visages familiers, de faire de nouvelles rencontres, d'échanger des idées et de profiter tout simplement du fait d'être entouré de personnes qui partagent la même passion.

J'aime aussi beaucoup découvrir de nouveaux talents.

Il y a des hackers incroyablement talentueux qui débutent tout juste, et des événements comme Hack the Government leur donnent l'occasion de montrer ce dont ils sont capables.

Et qui sait ? Certains d'entre eux rejoindront peut-être un jour l'équipe belge HackerOne, ou peut-être que nous finirons même par travailler ensemble un jour.

On ne sait jamais où ces liens peuvent mener, n'est-ce pas ?

C'est l'une des choses que j'aime dans cette communauté.

7 Quels conseils donneriez-vous à quelqu'un qui participe à Hack the Government 2026 ?

Avant tout, profitez autant que possible de l'expérience !

Hack the Government est une occasion formidable, non seulement de trouver des vulnérabilités, mais aussi d'apprendre, de faire des rencontres et de rejoindre la communauté.

Alors, participez aux discussions sur Discord, échangez avec les autres participants et profitez au maximum de l'événement lui-même.

Mon deuxième conseil serait de collaborer et de vraiment vous concentrer.

Si vous visez un bon classement, ces deux semaines peuvent être assez intenses. Vous devrez donc trouver le bon équilibre entre approfondir vos recherches et prendre suffisamment de pauses pour garder les idées claires.

Et voici quelque chose que je recommande tout particulièrement aux participants moins expérimentés : ne passez pas d'une cible à l'autre toutes les quelques minutes.

Choisissez plutôt une application qui propose de nombreuses fonctionnalités, prenez le temps de vraiment comprendre comment elle fonctionne et explorez-la en profondeur.

Comprenez sa logique métier, explorez ses fonctionnalités et cherchez ce qui ne se comporte pas comme prévu.

C'est souvent là que vous trouverez les bugs vraiment intéressants.

Et qui sait ? Vous découvrirez peut-être quelque chose d'assez important pour le présenter lors de votre première session de présentation et de démonstration !

Mais surtout, ne vous mettez pas trop de pression.

Que vous terminiez premier, dernier ou quelque part entre les deux, vous allez apprendre énormément.

Restez curieux, collaborez, dépassez-vous et, surtout, amusez-vous. C'est tout l'esprit du hacking.

> *« Je n'en serais pas là aujourd'hui sans la communauté.*
>
> Pedro

TÉMOIGNAGE 02

Logan (Le point de vue d'un étudiant)

Étudiant en dernière année de master

1 Pourriez-vous vous présenter et retracer brièvement votre parcours ? Qu'est-ce qui vous a attiré au départ vers les tests d'intrusion ?

Je suis encore étudiant, actuellement en dernière année de master, mais j'ai contribué au CVDP il y a presque deux ans. Aujourd'hui, je poursuis mon master et je participe à des programmes de bug bounty pour acquérir de l'expérience, notamment dans l'utilisation de l'IA pour les tests de sécurité. J'ai toujours fait du hacking et des tests d'intrusion, même quand j'étais beaucoup plus jeune. Mon réflexe, c'est de chercher des moyens de « déjouer » ou de « tromper » un système, d'en tester les limites.

2 Quelle importance accordez-vous au fait d'être reconnu comme un « hacker éthique » ? Que représente la communauté des hackers éthiques pour vous et pour la Belgique ?

C'est très important. Le fait qu'en Belgique, nous puissions respecter des consignes et, en gros, hacker n'importe quoi tout en étant reconnus pour cela est formidable et unique au monde. C'est aussi un excellent moyen de tester ses compétences et de contribuer à la sécurité de la Belgique, tout en protégeant même directement ses propres données sensibles.

3 Qu'est-ce qui vous a amené à participer à Hack the Government ?

Avoir découvert des vulnérabilités critiques dans des systèmes du gouvernement fédéral et les avoir signalées via le CVDP.

4 Pourriez-vous partager un souvenir ou une anecdote à propos de HTG ? Qu'en avez-vous retiré, et cette expérience a-t-elle influencé ce que vous avez fait ensuite ? Qu'est-ce qui reste précieux pour vous aujourd'hui ?

J'ai rencontré quelqu'un que j'avais connu il y a longtemps en jouant sur des serveurs Minecraft néerlandophones. J'ai reconnu son nom et j'ai été stupéfait de découvrir qu'il était là, lui aussi. Nous avons renoué le contact et parlé de l'époque de Minecraft, de ce que nous faisons aujourd'hui et de la façon dont nous nous étions retrouvés là tous les deux.

Cela a aussi clairement influencé ce que j'ai fait ensuite : j'ai participé à des événements organisés par les ambassadeurs belges de HackerOne, dont dr0p, qui était également présent à HTG. Ces événements m'ont finalement aidé à nouer des contacts et à trouver des bugs que je n'aurais pas découverts autrement.

5 Que recommanderiez-vous aux plus jeunes participants pour profiter pleinement de HTG 2026 ?

Profitez-en, donnez le meilleur de vous-même, trouvez quelques vulnérabilités, peu importe s'il s'agit de doublons. Dormez moins, partagez des idées et des informations sur Discord : les gens finiront par vous reconnaître ou par venir vous parler lors de l'événement en présentiel, et ils sauront qui vous êtes.

Nouez aussi des contacts. Le milieu des hackers belges n'est pas *si* grand : c'est un peu un monde où tout le monde se connaît. C'est donc une belle occasion de rencontrer du monde.

TÉMOIGNAGE 03

Timothy

Chercheur de vulnérabilités et entrepreneur en cybersécurité

1 Pourriez-vous vous présenter et retracer brièvement votre parcours ?

Je m'appelle Timothy. Je me suis intéressé à la cybersécurité très jeune et je connaissais déjà assez bien ce domaine lorsque j'ai participé à mon premier Hack the Government, à 16 ans. Depuis, je pratique la recherche de vulnérabilités dans des programmes de bug bounty et la divulgation responsable, en aidant des entreprises de toutes tailles à renforcer leur sécurité, et j'ai signalé des vulnérabilités à deux reprises via le CVDP. En juin de cette année, j'ai créé ma propre entreprise de cybersécurité. Ce qui m'a attiré au départ vers les tests d'intrusion est simple : je trouve amusant de comprendre comment les systèmes fonctionnent et comment ils peuvent être mis en défaut.

2 Quelle importance accordez-vous au fait d'être reconnu comme un « hacker éthique » ?

Pour moi, le hacking éthique est une façon légale de faire ce qui me plaît le plus, et c'est encore mieux puisque cela aide d'autres personnes. Chaque vulnérabilité que je signale est bien sûr une vulnérabilité qui ne peut pas être exploitée par une personne malintentionnée. Pour la Belgique, je pense que des événements comme HTG montrent que les hackers et le gouvernement peuvent coopérer au lieu de s'opposer, et c'est ainsi que l'on améliore la sécurité.

3 Qu'est-ce qui vous a amené à participer à Hack the Government ?

Un ami me l'a recommandé. Lors de la première édition, il y avait davantage de places disponibles qu'aujourd'hui, et j'ai donc eu la possibilité de participer même si j'étais encore jeune.

4 Pourriez-vous partager un souvenir ou une anecdote à propos de HTG ?

Honnêtement, ma première année ne s'est pas très bien passée. Je n'avais presque rien trouvé, et cela m'a un peu ramené à la réalité. Mais au lieu d'abandonner, j'ai continué à apprendre et je suis revenu. L'année dernière s'est beaucoup mieux passée (7e au classement général, je crois), et j'espère que cette année sera encore meilleure. J'en ai retenu que les résultats ne viennent pas tout de suite : on progresse en participant, en tirant les leçons de ce qui n'a pas fonctionné et en réessayant. Cet état d'esprit a beaucoup compté dans ma décision de me lancer sérieusement dans le bug bounty et, finalement, de créer ma propre entreprise.

5 Que recommanderiez-vous aux plus jeunes participants pour profiter pleinement de HTG 2026 ?

Soyez patients. En bug bounty, la patience est essentielle. Ne vous découragez pas si vous ne trouvez rien le premier jour, ou même pendant toute votre première édition : cela m'est arrivé aussi. Ne cherchez pas non plus uniquement des techniques d'exploitation sophistiquées (et ne vous découragez pas si elles ne fonctionnent pas). Certains des bugs les plus intéressants sont de simples failles logiques : comprenez comment l'application est censée fonctionner, puis réfléchissez aux façons dont elle pourrait être détournée. Et surtout, profitez de l'expérience et parlez aux personnes qui vous entourent. Vous pouvez apprendre beaucoup en prêtant attention à ce que disent les autres.