HACK THE GOVERNMENT

2026 · FINAL EVENT

PRESS FILE

Wednesday 25 November 2026 | Centre for Cybersecurity Belgium (CCB)

1. Practical information for the press

Event: Hack the Government 2026 | Final Event
Date: Wednesday, 25 November 2026
Venue: Quartier Papier | Fabrieksstraat 55/59, 1930 Zaventem
Press info: comm@ccb.belgium.be
Press is welcome in person for the full day programme (including the award ceremony).

Interview window: 12:00 – 13:00

The following representatives are available to the press between 12:00 and 13:00:

Miguel De Brucyker : Director-General, Centre for Cybersecurity Belgium (CCB)

Requests for one-on-one interviews outside this slot should be directed to the CCB press office in advance.

2. Why Coordinated Vulnerability Disclosure (CVD) matters

Cybersecurity vulnerabilities are a fact of digital life. What matters is not whether they exist, but how quickly and responsibly they are handled once found. Coordinated Vulnerability Disclosure (CVD) is the structured process by which researchers report vulnerabilities to the affected organisation and to a trusted authority, giving developers time to fix the issue **before** it can be exploited.

Belgium has one of Europe's most forward-looking CVD frameworks. The **Belgian Law of 26 April 2024** explicitly protects ethical hackers who discover and responsibly disclose vulnerabilities in good faith, even where no formal bug bounty programme exists. The CCB serves as the national coordination point: it receives reports and mediates the fix process between researcher and organisation (see more in **Annex 1** and on the CCB dedicated web page).

Recent case: the PHP2Shell incident (October 2026)

The importance of a robust CVD process was thrown into sharp relief in October 2026 by the **PHP2Shell** case: a critical remote code execution vulnerability in PHP, one of the most widely deployed server-side languages on the web. On 21 October 2026, patched versions were released, but the coordinated disclosure process **broke down** before the fix could be applied at scale: leaked CVE identifiers, an accidental video release, and early patch distributions by some vendors collapsed the embargo, triggering a wave of emergency maintenance across banks, public services, gaming platforms and web hosting providers.

> **The lesson:** when the coordinated disclosure process works, defenders get a head start. When it breaks down (through a leak, an early release, or a failure to notify), attackers move before the patch does. PHP2Shell is a textbook illustration of why the CVD process must be rigorous, trusted and legally anchored.

The PHP2Shell incident also illustrates a wider trend: unpatched or newly disclosed vulnerabilities in widely used technologies attract rapid attention. Hack the Government directly serves the national CVD ecosystem by training the next generation of researchers in responsible disclosure practice, and by stress-testing government systems under legally controlled conditions before adversaries can find the same weaknesses.

3. AI and the vulnerability race: what the evidence shows

Artificial intelligence is changing the speed at which attackers can develop and deploy exploits. The evidence is now sufficiently strong to say that **AI is making exploit development and attack automation faster,** but the picture is more nuanced than headlines sometimes suggest.

What independent data shows

AI is shortening all timelines in the race to exploit vulnerabilities, but there is **no single, universal "time to exploit"**. Publication of exploit code, first observed exploitation by an attacker, and official confirmation in a Known Exploited Vulnerabilities (KEV) catalogue are distinct milestones, and each follows its own clock.

Current data shows that certain high-value vulnerabilities, particularly those affecting internet-facing and edge technologies, can be weaponised or exploited **within hours of disclosure, or even before it**. AI systems can now automate key stages of vulnerability research and exploit development, and threat intelligence providers have begun to observe these capabilities in real-world attacks.

Even so, **most disclosed vulnerabilities are never actively exploited in the wild**, and the available research does not establish the extent to which AI has shortened time from disclosure to real-world exploitation across all Common Vulnerabilities and Exposures (CVEs) (**Annex 2** provides an in-depth explanation and data).

Why this makes HTG more important, not less

If AI is compressing the time between vulnerability disclosure and exploitation for high-value targets, the case for proactive, **ethical vulnerability discovery by trusted human researchers becomes stronger not weaker**. Finding and fixing vulnerabilities before they reach the public domain is now a race where defenders can no longer assume they have weeks or months. Hack the Government puts the right people, with the right legal protections, on the right side of that race.

4. The CCB's role: building the national community

As Belgium's national cybersecurity authority, the Centre for Cybersecurity Belgium plays a dual role in Hack the Government: it is both the **organising authority** and an **active partner**, helping government organisations engage constructively with the ethical hacking community, often for the first time.

HTG 2026 brings 11 government systems into scope (almost triple the number of the first edition in 2024) with several organisations (including FPS Justice, the Federal Police, FAGG-AFMPS, Defense, etc.) among the participants this year. This growth reflects a maturing relationship between public institutions and the ethical hacker community, underpinned by Belgium's progressive CVD legal framework (**cf. Annex 1**)

Three editions: results at a glance

Metric	Edition 1 (2024)	Edition 2 (2025)	Edition 3 (2026)
Participants	-	71	77
of which senior / professional	-	39	45
of which students	-	32	32
Vulnerability reports submitted	154	352	TBC (live)
Vulnerabilities validated	85	98	TBC (live)
of which Critical / Exceptional	7	20	-
of which High	15	12	-
Government systems in scope	4	8	11

See the full fact sheet **in Annex 3**.

5. What participants say

Hack the Government is more than a competition. For many participants, it represents a career-defining moment: a first real encounter with professional offensive security, a chance to build a network, and proof of skills that no certificate can fully substitute. Three voices from past editions:

> **"Hack the Government was much more than a hacking competition. It was an important step in my professional journey."**
>
> **Pedro (alias: drop)** | Freelance offensive security consultant; Senior Penetration Tester; co-captain, Belgian HackerOne national team
>
> *Pedro joined HTG in its first edition (2024), finishing third place. A career-changer from marketing and data science, he used bug bounty and HTG to prove his skills in practice eventually landing a long-term assignment at an international organisation and an invitation to represent Belgium in the HackerOne World Cup.*

> **"The fact that we in Belgium can follow guidelines and basically hack anything and be recognised for it is amazing and unique in the world."**
>
> **Logan** | Final-year master's student; active bug bounty hunter; contributor to the CCB's national CVD programme
>
> *Already contributing to CVD two years before finishing his degree, he used HTG to build connections that led directly to finding vulnerabilities he would not have discovered on his own.*

> **"Events like HTG show that hackers and the government can work together instead of against each other, and that's how you build better security."**
>
> **Timothy** | Bug bounty hunter; founded his own cybersecurity company in June 2026; first participated in HTG at age 16
>
> *Timothy's first HTG edition was a reality check with almost no findings. He came back, finished 7th in 2025, and credits the mindset he built through HTG for his decision to launch his company.*

Full testimonials are available in **Annex 4**.

6. Frequently Asked Questions

What is an ethical hacker?

Originally, the term 'hacker' referred to people passionate about tinkering: experts at discovery and pushing systems to their limits. In the cybersecurity context, an **ethical hacker** is a vulnerability hunter who operates legally and constructively: identifying security flaws and reporting them responsibly rather than exploiting them for personal gain. They are, in essence, the defenders who think like attackers.

What is Hack the Government?

Hack the Government (HTG) is an initiative of the CCB that invites vetted ethical hackers to test the IT systems of Belgian public institutions under legally controlled conditions. Its sole aim is to detect and report vulnerabilities responsibly before malicious actors can find them. It is a genuine call for collaboration between the hacking community, government and academia.

Are participants legally protected?

Yes. Under the Belgian Law of 26 April 2024 and the CCB's national CVD framework, participants who act in good faith; limiting their actions to what is strictly necessary, without malicious intent, and reporting findings to the responsible organisation and the CCB are legally protected.

Who can participate?

HTG 2026 brought together **77 participants**: 45 senior/professional ethical hackers and 32 students. Participants are selected through an application process and must agree to strict rules of engagement. The programme is explicitly designed to mix experience levels and bridge the talent gap connecting students with senior practitioners in a live, hands-on setting.

What systems are tested?

12 government systems are in scope for HTG 2026, including systems from FPS Justice and the Federal Police. Organisations participate voluntarily, and the scope of each system under test is defined in advance. Findings are shared exclusively with the responsible organisations and the CCB, not disclosed publicly during the event.

What happens after the event?

All validated vulnerabilities are shared with the affected organisations, which are then responsible for patching them. The CCB tracks remediation through its coordinated disclosure process. Final results for HTG 2026 will be published following the event.

Annexes

- **Annex 1: CCB CVD framework (overview)**: Belgium's coordinated vulnerability disclosure policy, legal protections, and reporting process.
- **Annex 2: AI and the vulnerability race:** What the evidence actually shows.
- **Annex 3: HTG2026 Fact Sheet** (updated): 3 editions of impact, by the numbers.
- **Annex 4: Participant testimonials**: Pedro (drop), Logan, Timothy.

Contact: CCB Press Office
Michele Rignanese | michele.rignanese@ccb.belgium.be | +32 477 38 87 50
Katrien Eggers | katrien.eggers@ccb.belgium.be | +32 485 76 53 36
All editorial and statistical content is accurate as of 19 November 2026 and subject to revision pending final HTG 2026 event results.

CVD IN BELGIUM

Found a security flaw?

Report it. Help fix it.

Coordinated vulnerability disclosure means reporting a weakness privately so the people responsible can work on a fix.

CENTRE FOR CYBERSECURITY BELGIUM

THE DISCLOSURE PROCESS [1, 3]

1. **Read the rules**
   Check the organisation's disclosure policy, if it has one. Follow its scope and reporting instructions.
2. **Confirm with care**
   Do only what is needed to verify the weakness. Avoid disruption and unnecessary access to data.
3. **Report privately**
   Tell the organisation what is affected and how to reproduce the problem. Use a secure channel.
4. **Work on a fix**
   The organisation investigates and works on a fix. Stay in touch; the CCB can help coordinate.
5. **Coordinate any publication**
   Public sharing is optional. Under the legal route, obtain CCB authorisation before publishing.**

OPTIONAL LEGAL PROCEDURE [2]

Belgium's legal protection route

Use it with or without an organisation's CVD policy.

Send as soon as possible, within:

24 hours

Initial report

Identify the system and briefly describe the weakness.

72 hours

Full report

Explain how to reproduce it; include key technical details.

BOTH REPORTS GO TO

Organisation + CCB

Both deadlines run from discovery.*

STAY WITHIN THE CONDITIONS [1, 2]

Act in good faith
Do not threaten, extort or misuse data.

Check before testing
Some sensitive organisations require prior written permission.

Know the limits
Protection is conditional and applies under Belgian law only.

Use the CCB forms and secure submission instructions [2]

vulnerabilityreport@ccb.belgium.be

* Discovery: when you should reasonably recognise a potential vulnerability, after reasonable investigation and validation.

** The 90-day period starts with a formal publication request to the CCB. If no refusal is notified by its end, publication may be considered authorised.

CCB = Centre for Cybersecurity Belgium

[1] ccb.belgium.be/regulation/cvdp [2] ccb.belgium.be/cert/vulnerability-reporting-ccb [3] CCB Guide, Part I: process

Plain-language summary | 19 November 2026

AI and the vulnerability race:

What the evidence actually shows

Press Annex | Hack the Government 2026 | Centre for Cybersecurity Belgium 19 November 2026

1. 'Time-to-Exploit' is not a single metric

Coverage of AI-accelerated cyber threats often treats 'time-to-exploit' as a single, comparable number. It is not. At least four different clocks are routinely conflated in public reporting and mixing them produces numbers that cannot be directly compared.

Metric	What it actually measures	Why it matters	Key caveat
CVE disclosure → public exploit / PoC	Time until exploit code or a PoC becomes publicly available	Measures weaponization / public availability, not attacker use	Exploit availability ≠ exploitation in the wild
CVE disclosure → first observed exploitation	Time until credible evidence shows attackers using the vulnerability in the wild	Measures real-world exploitation	Observation may lag the actual first attack
Pre-disclosure exploitation	Exploitation occurs before public CVE disclosure or patch availability	Classic zero-day case, lag can be negative	Disclosure date is not the start of the race
CVE publication → KEV listing	Time until an intelligence provider has sufficient evidence to classify a CVE as exploited	Measures confirmation / reporting latency as well as attacker activity	KEV listing lags actual exploitation

CISA explicitly distinguishes a **public proof-of-concept (PoC)** from **active exploitation**: 'active' requires shared, observable, and reliable evidence that threat actors have used the vulnerability in the wild. VulnCheck similarly bases its analysis on the *earliest evidence of exploitation*, not simply the date exploit code appeared. This distinction explains apparent contradictions between different vendors' headline figures.

2. What independent data show

VulnCheck : H1 2026 exploitation analysis

VulnCheck examined **495 vulnerabilities** newly identified as exploited during H1 2026:

- **23.43%** showed evidence of exploitation **on or before the CVE publication date** (attackers moved before the patch even existed. The comparable 2025 figure was 28.93%.
- Median time from CVE publication to KEV confirmation: **80 days,** down from 120 days in 2025.
- Roughly **200 CVEs** reached KEV status within 31 days in H1 2026, broadly unchanged from 196 (2024) and 194 (2025), even as overall CVE volume rose sharply. This is an important counterweight to claims that all vulnerabilities are moving toward exploitation within hours.

- VulnCheck explicitly warns about the **maturation problem**: recent CVE cohorts continue accumulating exploitation evidence over time (early figures systematically undercount exploitation for recent CVEs).

Google Threat Intelligence Group (GTIG): 2026 analysis

GTIG recorded **141 vulnerabilities** both disclosed and exploited between January and August 2026, against 127 for all of 2025. The monthly average rose from 10.5 to 18.

- However, only about **0.23%** of disclosed vulnerabilities in the 2026 dataset were observed in active exploitation.
- Much of the growth involved rapid weaponisation of **n-days** (recently patched vulnerabilities), not an explosion in zero-days.
- Zero-days increased more modestly (from an average of 8 to 11 per month) before an August spike.

Mandiant M-Trends 2026 and Verizon DBIR 2026

Mandiant's incident-response data reports an estimated mean TTE of **–7 days**, meaning exploitation in its sample often preceded patch release. This is a *patch-relative* metric, not a CVE-disclosure-to-exploit metric.

Verizon's 2026 DBIR shows that vulnerabilities are an increasingly important breach entry point (**31% of breaches**) and reports AI augmentation across multiple attack techniques. It does not, however, establish that AI alone caused a specific universal time-to-exploit reduction.

---

3. What we now know about AI capability

The evidence for AI-assisted exploit development has strengthened materially in 2026:

- **October 2026 | Anthropic**: An internal research model discovered and built multi-stage exploit chains against Chrome, Safari, Android, Windows and Linux, including remotely exploitable vulnerabilities and sandbox escapes.
- **May 2026 | Google**: Reported its first observed threat actor using a zero-day exploit believed to have been developed with AI assistance.
- **16 November 2026 | GTIG/Mandiant**: Reported observing threat actors using LLM frameworks to **fully automate** vulnerability discovery, patch-diff analysis, exploit drafting and execution (without a human in the loop) including during live intrusion activity. This represents a qualitative threshold.

> **The state of the art as of November 2026:** *"AI demonstrably improves vulnerability discovery and exploit-development capability and is beginning to compress some real-world attack workflows. There is not yet evidence for a universal AI-driven exploitation window measured in hours for all CVEs. For the high-value targets, attackers prioritize (particularly internet-facing and edge technologies) defenders may have hours rather than days."*

---

4. What this means for defenders

The trend is clear and actionable, even if no single headline number tells the full story. AI is lowering the bar for exploit development. The relevant policy question is not *'exactly how many hours do defenders have?'* : the answer varies enormously by vulnerability type, exposure, and attacker profile. The relevant question is: **'are we finding our vulnerabilities before an AI-assisted adversary does?'**

That is precisely what Hack the Government is designed to answer. By putting vetted ethical hackers (including researchers actively working with AI-assisted tools) against government systems under legally controlled conditions, HTG provides defenders with the most realistic possible test of their exposure.

> **Coordinated vulnerability disclosure is the structural answer.**
> Whether the time window is hours or months, the organisations best placed to respond are those that have already established a trusted process for receiving, triaging and patching vulnerability reports. Belgium's national CVD framework (anchored in law since December 2022) provides exactly that infrastructure.

5. Primary sources

The following sources were used in preparing this annex.

- Cogent Security — Detection Gap Report Q2 2026 (blog post)
- Cogent Security — Detection Gap Report Q2 2026 (newsroom / methodology)
- VulnCheck — State of Exploitation 1H-2026
- Google Threat Intelligence Group — Vulnerability Discovery and Exploitation Trends in the AI Era (30 Sep. 2026)
- GTIG/Mandiant — Agentic Threat Activity Crosses a Significant Threshold (16 Nov. 2026)
- Mandiant — M-Trends 2026
- Anthropic — Discovering and exploiting vulnerabilities in critical, real-world software with Claude (27 Oct. 2026)
- Google — Adversaries Leverage AI for Vulnerability Exploitation, Augmented Operations, and Initial Access
- Verizon — 2026 Data Breach Investigations Report (DBIR)
- CISA — SSVC Guide (distinguishing PoC from active exploitation)

This annex was prepared by the Centre for Cybersecurity Belgium (CCB) for media use in connection with the Hack the Government 2026 final event (25 November 2026). Content is accurate as of 19 November 2026.

HACK THE GOVERNMENT 2026

Fact sheet: 3 editions of impact and why the need keeps growing

Hack the Government by the numbers

Metric	Edition 1 — [2024]	Edition 2 — [2025]	Edition 3 — [2026]
Final event date	*27 Nov. 2024*	*26 Nov. 2025*	*25 Nov.2026*
Total participants	*n.a*	*71*	*77*
Senior / professional participants	*n.a*	*39*	*45*
Junior participants (students)	*n.a*	*32*	*32*
Vulnerability reports submitted	*154*	*352*	*TBC*
Vulnerabilities validated	*85*	*98*	*TBC*
of which Critical / Exceptional	*7*	*20*	
of which High	*15*	*12*	
of which Medium / Low	*55*	*66*	
of which out-of-scope but validated	*8*	*9*	
Government systems / scopes tested	*4*	*8*	*12*

Source: Hack the Government internal reporting.

Why it matters: Belgium's cybersecurity talent gap

Hack the Government doesn't only make government systems safer today: it helps grow the talent pool Belgium needs.

A **2025 KPMG study*** of the Belgian cybersecurity sector puts numbers on a challenge every participant recognises first-hand:

~4,000
open cybersecurity vacancies in Belgium

44%
of organisations need 4–6 months to recruit a cybersecurity expert

19%
need 7–12 months to fill the role

43%
say recruiting cyber experts got harder vs. the previous year

1–5
dedicated security specialists is the norm for half of Belgian organisations

1 in 3
organisations employ no women at all in cybersecurity roles

** Source: KPMG, Cyber Security Study Belgium (2025), pp. 48–51.*

CENTRE FOR CYBERSECURITY BELGIUM

Hack the Government 2026

Participant testimonials

Ethical hackers, in their own words

THREE PERSPECTIVES

Career paths, community and lessons from Hack the Government.

01 **Pedro** — PAGE 2
Freelance offensive security consultant · known as drop
"I wouldn't be where I am today without the community."

02 **A student's perspective** — PAGE 6
Final-year master's student
"Also connect with people."

03 **Timothy** — PAGE 7
Bug bounty hunter and cybersecurity entrepreneur
"You can learn a lot if you pay attention to what people say."

TESTIMONIAL 01

Pedro

Freelance offensive security consultant · known as drop

> *"I wouldn't be where I am today without the community."*

1 Could you introduce yourself and give us a quick overview of your career path? Why were you attracted to penetration testing?

My name is Pedro, but I'm also known as drop in the bug bounty community.

I'm a freelance offensive security consultant, working with different private companies and government institutions. I'm currently on a long-term assignment in the governmental sector as a senior penetration tester.

What's interesting about my journey is that I don't come from a traditional cybersecurity background. My background was originally in marketing and data science. But during COVID, I decided to invest a huge amount of time in cybersecurity, and eventually managed to make a complete career switch.

I actually started on the blue team side, working in digital forensics and security operations. But deep down, I knew from the beginning that offensive security was where I wanted to be.

The challenge was proving that I had the skills, especially without a traditional background in the field.

And that's where bug bounty came in.

For me, bug bounty was the perfect way to demonstrate what I could do in practice, rather than just relying on certifications or a CV.

And honestly, that's really where everything started for me. It opened so many doors and played a huge role in building the career I have today.

2 How important is it for you to be recognized as an ethical hacker? What does the ethical hacking community represent to you and to Belgium?

For me, being an ethical hacker is first and foremost a mindset. And I think that mindset goes far beyond the technical side of cybersecurity.

It's about being curious, questioning how things work, and finding ways to solve problems that nobody has thought of before.

It might sound a bit cliché, but it's literally about thinking outside the box.

It's about making systems, applications, or even processes behave in ways they were never intended to, pushing boundaries, and ultimately demonstrating impact or finding creative solutions to complex problems.

And I think that's something incredibly valuable, not just in cybersecurity, but also for the organizations we work with.

Interview continues on the next page.

QUESTION 02 / CONTINUED

Now, when it comes to the community, for me, the community is everything.

I've worked in different industries before cybersecurity, and I can genuinely say that the hacking community is something special.

People are incredibly welcoming. They love sharing their research, their bugs, their successes, but also their failures and limitations.

And that's something I really appreciate.

I wouldn't be where I am today without the community. The knowledge sharing, the collaboration, the conferences, and all the people I've met along the way have played a massive role in my journey.

And I think Belgium has a really strong and talented ethical hacking community, even if we don't always realize it.

Actually, I'm currently one of the co-captains of the Belgian team that will be competing in the new HackerOne World Cup.

And hopefully, we'll make it onto the podium! That would be a fantastic achievement for the Belgian hacking community.

3 What brought you to Hack the Government?

I first heard about Hack the Government during BruCON in 2024.

And I remember thinking, "Wait, hacking the government? Legally? That's an opportunity I can't miss!"

So, of course, I immediately decided to participate.

It was the very first edition, which made it even more exciting.

For me, it was the perfect opportunity to challenge myself, test my skills against other talented hackers, and see where I stood compared to my peers.

I was also curious to see how other hackers would approach the same targets and what kind of vulnerabilities they would discover.

And in that first edition, I actually managed to finish in third place, which I was really happy about!

It was a great experience, especially because I was still building my reputation in the community at the time.

> *It was the very first edition, which made it even more exciting.*
>
> Pedro

4 Could you share a memorable moment or anecdote about Hack the Government?

Oh, definitely!

I think my most memorable moment was receiving the event coin directly from the Belgian Prime Minister.

That was something pretty special!

I remember being really proud of that moment, and I kept showing the picture to my colleagues, friends, and family.

I mean, how often do you get to say that you hacked government systems legally and then received a coin from the Prime Minister?

It's definitely a great conversation starter!

And beyond the recognition, it was also a really nice moment because it showed that ethical hacking was being taken seriously and recognized at such a high level.

For me, that was something really meaningful.

5 What did you take away from Hack the Government, and did it influence anything you did afterwards?

I would say that one of the biggest things Hack the Government gave me was visibility and credibility.

At that stage of my career, I was still trying to establish myself in offensive security.

And participating in an event like that, especially finishing on the podium, was a great way to demonstrate my skills and show that I knew what I was doing.

It also allowed me to meet a lot of interesting people, build connections, and become more visible within the Belgian cybersecurity community.

And I genuinely believe that this exposure helped me get invited to speak at conferences, participate in live hacking events, and access other opportunities later on.

Of course, it wasn't the only reason those opportunities came along, but it definitely helped open some doors.

So, looking back, Hack the Government was much more than just a hacking competition for me. It was also an important step in my professional journey.

> *"It was also an important step in my professional journey.*
>
> Pedro

6 What is still valuable to you about Hack the Government today?

Today, I would say the value is a little different for me.

Of course, I still enjoy the technical challenge and the competition. That's always going to be part of who I am.

But what I appreciate most now is the community aspect.

It's an opportunity to reconnect with familiar faces, meet new people, exchange ideas, and just enjoy being surrounded by people who share the same passion.

I also really enjoy discovering new talent.

There are some incredibly talented hackers out there who are just starting their journeys, and events like Hack the Government give them a chance to demonstrate what they can do.

And who knows? Maybe some of them will eventually join the Belgian HackerOne team, or perhaps we'll even end up working together someday.

You never know where those connections might lead, right?

That's one of the things I love about this community.

7 What advice would you give to someone participating in Hack the Government 2026?

First of all, enjoy the experience as much as you can!

Hack the Government is a fantastic opportunity, not just to find vulnerabilities, but also to learn, meet people, and become part of the community.

So, get involved in the Discord discussions, talk to other participants, and make the most of the event itself.

My second piece of advice would be to collaborate and really focus.

If you're aiming for a good ranking, those two weeks can get pretty intense. So you'll need to find the right balance between going deep into your research and taking enough breaks to stay sharp.

And here's something I would particularly recommend to less experienced participants: don't jump from target to target every few minutes.

Instead, pick one application that has a lot of functionality, take the time to really understand how it works, and go deep.

Understand its business logic, explore its features, and look for things that don't behave the way they should.

That's often where you'll find the really interesting bugs.

And who knows? Maybe you'll discover something significant enough to present during your first show-and-tell session!

But above all, don't put too much pressure on yourself.

Whether you finish first, last, or somewhere in between, you're going to learn a lot.

Stay curious, collaborate, push yourself, and most importantly, have fun. That's what hacking is all about.

TESTIMONIAL 02

Logan (A student's perspective)

Final-year master's student

> *"Also connect with people."*

1 Could you introduce yourself and give a quick overview of your career path ? (why were you attracted by pen testing in the first place ?)

I am still a student currently in last year of my masters but contributed almost 2 years ago to the CVDP , now doing masters and bug bounty gaining experience on for example working with ai in security testing. Among other things. Hacking/pen testing was always something i just did even when i was way younger, ways to "outsmart" or "cheat" a system is the default on which i go by. Trying to test the boundaries.

2 How important is it for you to be recognized as an "ethical hacker" ? What does the EH community represent to you and for Belgium ?

Very important, the fact that we in Belgium can follow guidelines and (basicly) hack anything and be recognized for it is amazing and unique in the world. And an amazing way to test your skills and contribute to the security of Belgium while even directly protecting your own sensitive data.

3 What brought you to Hack the Government?

Finding critical vulnerabilities in federal goverment systems and submitting them to the CVDP.

4 Could you give a memory or an anecdote about HTG ? What did you take away from it, and did it influence anything you did afterwards? What is still valuable to you today?

I met someone that i knew from a long time ago playing on dutch speaking minecraft servers, i recognized his name and was shocked to find out that he was also there. We reconnected and talked about the minecraft days and what we are doing now and how we both ended up here.

It also definitely influenced what i did after, i participated in events organized by the Belgium Hackerone Ambassadors that was also at HtG (dr0p). Which ultimately helped connect with people and find bugs i wouldnt have otherwise.

5 What would recommend younger participants to fully enjoy HTG 2026 ?

Enjoy it , do your best , find some vulnerabilities doesnt matter if they are duplicate. Lose sleep hours, share ideas/information in the discord because people will recognize/come up to you eventually at the in person event and know who you are.

Also connect with people. The belgian hacker scene is not *that* big its a bit of everyone knows everyone so this is a nice chance to get to know some people.

TESTIMONIAL 03

Timothy

Bug bounty hunter and cybersecurity entrepreneur

> *"Be patient. In bug bounty, patience is key."*

1 Could you introduce yourself and give a quick overview of your career path?

My name is Timothy. I got into cybersecurity at a young age and was already pretty familiar with it when I joined my first Hack the Government at 16. Since then I've been doing bug bounty hunting and responsible disclosure, helping companies of all sizes improve their security posture, and I've reported vulnerabilities twice through CVDP. In June this year I started my own cybersecurity company. What attracted me to pen testing in the first place is simple: I think it's fun to figure out how systems work and how they break.

2 How important is it for you to be recognised as an "ethical hacker"?

For me, ethical hacking is the legal way of doing what I enjoy most, and the fact that it helps other people makes it even better. Every vulnerability I report is of course one that can't be abused by someone with bad intentions. For Belgium, I think events like HTG show that hackers and the government can work together instead of against each other, and that's how you build better security.

3 What brought you to Hack the Government?

A friend recommended it to me. In the first edition there were more open spots than there are now, so I got the chance to join even though I was still young.

4 Could you give a memory or an anecdote about HTG?

Honestly, my first year didn't go great. I had hardly any findings, and it was a bit of a reality check. But instead of giving up, I kept learning and came back. Last year went a lot better (7th in total I believe), and I'm hoping this year will be better still. What I took away is that results don't come immediately; you grow by showing up, learning from what didn't work and trying again. That mindset is a big part of why I got into bug bounty seriously and eventually started my own company.

5 What would you recommend to younger participants to fully enjoy HTG 2026?

Be patient. In bug bounty, patience is key. Don't get discouraged if you don't find anything on day one, or even in your whole first edition; that happened to me too. Also, don't only chase fancy exploitation techniques (or get discouraged if they don't work). Some of the best bugs are simple logic flaws: understand how the application is supposed to work, then think about how it could be misused. And most of all, enjoy it and talk to the people around you. You can learn a lot if you pay attention to what people say.