27 Nov 2024 -14:00

Belgian Federal Government invites Ethical Hackers for First-Ever 'Hack the Government' Event

The Centre for Cybersecurity Belgium (CCB) is hosting *Hack the Government 2024*, marking the first-ever ethical hacking event organised by the Belgian Federal Government. On Wednesday evening, 27 November, Alexander De Croo, Belgium's Prime Minister will present the winner of the event with the coveted "Ethical Government Hacker of 2024" award.

"In the spirit of innovation and security, we opened selected federal government digital assets to ethical hackers. We recognise the need for robust security measures, and we believe in the power of collective intelligence. This endeavour was not without risk, but we took a bold step towards strengthening Belgium's cyber defenses. The results are there and we are proud of the commitment, dedication, and determination of these exceptional ethical hackers."
– Alexander De Croo, Prime Minister of Belgium

Hack the Government 2024 is firmly rooted in the belief that ethical hackers can raise the level of cyber security in Belgium: a view that has led Belgium to authorise ethical hacking, subject to compliance with certain strict conditions defined by law.

This unprecedented initiative brings together the community of ethical hackers to identify vulnerabilities across government websites and systems, demonstrating Belgium's commitment to cybersecurity and proactive defense measures. Together we can make Belgium the least cyber vulnerable country in the EU.

Adding to the excitement, *Hack the Government 2024* features a diverse group of ethical hackers (professionals and students) eager to help make Belgian digital assets safer. They will join forces to put governmental systems to the test. This collaboration gives participants the rare opportunity to contribute directly to securing public infrastructure. Although it is a competition to become "Ethical Government Hacker of 2024", teamwork is developing with mentoring, collaborating, and sharing amongst the participants.

The government entities participating in this initiative are:

- FPS Policy and Support (FOD BOSA/SPF BOSA)
- L'Office national des vacances annuelles / Rijksdienst voor jaarlijkse vakantie (ONVA/RJV)
- The Federal Agency for Medicines and Health Products (FAMHP/FAMPS/FAGG)
- The Centre for Cybersecurity Belgium (CCB)

Hack The Government 2024 is organised in close collaboration with the renowned bug bounty platform, Intigriti, providing a unique opportunity to put governmental systems to the test through controlled, authorised penetration testing. Started on 13 November, the challenge will culminate in an in-person event on Wednesday, 27 November. The one crowned "Ethical Government Hacker of 2024" wins a training course from the renown SANS Institute, including the Global Information Assurance Certification exam

(GIAC) worth over € 10 000. A touch of IT humour cannot be missed, so we have also provided honourable mentions for a variety of fun awards including “The first to draw blood” and “The one submitting most duplicates”.

The Importance of Ethical Hacking and Bug Bounty Programs

Through exercises like penetration tests (pentests) and bug bounty programs, organisations proactively address cybersecurity risks, staying ahead of cyber threats and strengthening public trust in digital services.

“This is a landmark moment for Belgium. By inviting ethical hackers to test its digital defenses, the federal government is showing true leadership in cybersecurity. These collaborative efforts with the ethical hacking community provide an invaluable layer of protection, and I’m thrilled to see the Federal Government setting an example for others.” - *Inti De Ceukelaire, Chief Hacker Officer of Intigriti*

The event will conclude with an awards ceremony led by CCB’s General Director, *Miguel De Bruycker*, who emphasised the value of this collaboration:

“Hack The Government 2024 highlights the legal provisions (see below) in force since 15 February 2023 which authorise ethical hacking in Belgium. This doesn't mean it is easy! Ethical hackers have strict conditions to follow. CCB is working with selected ethical hackers to show what can be done while at the same time enhancing our defenses and this builds a culture of cybersecurity resilience within the government. It is quite exciting for us because we are also exposing our own CCB websites. These ambitious hackers are discovering vulnerabilities right now in our infrastructures. We see this as an opportunity to strengthen our cyber protection.”

Hack the Government meant federal agencies trusting CCB to guide and organise the process. This meant working closely together over several months to detail the scope of the event. But the work will not end on 27 November. Checking findings, validating processes and procedures, and making necessary adjustments to improve cybersecurity will be on-going for testing again in future.

"FAGG is excited to be part of Hack the Government 2024. As we continuously strive for excellence in ensuring public health safety, we see cybersecurity as a crucial part of our mission, especially in relation to NIS2 Law compliance. We believe in the power of ethical hacking as a tool to fortify our digital infrastructure. We are confident the collaboration and the lessons we learn from this initiative will further strengthen our systems and services." - *Pierre Colangelo*, ICT Infrastructure (FAGG)

"The RJV is extremely proud to be part of Hack The Government 2024. As an organisation that serves citizens, we recognise the importance of strong cybersecurity measures to protect their data. This initiative to invite ethical hackers to test our IT systems is therefore the ideal way to proactively strengthen our digital security." - Myriam DEMOL, Data protection officer-Information security officer

This initiative represents a major step forward in governmental cybersecurity, bringing together public entities, private expertise, and the ethical hacking community. *Hack The Government 2024* emphasizes the importance of cybersecurity collaboration, and we are eager to showcase the results of this pioneering effort.

National policy on reporting vulnerabilities

The event will be organised under the provisions of the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security (NIS2). This is the Belgian legal framework that allows individuals to report identified vulnerabilities in information systems to the Centre for Cybersecurity Belgium (CCB) and the organisation concerned without fear of criminal or civil prosecution, provided that certain rules are complied with. This legal framework makes it possible to strengthen Belgium's digital defences by encouraging public participation in cybersecurity efforts, and to provide an appropriate framework for such actions.

This type of event also encourages organisations in Belgium, such as federal public administrations, to develop a coordinated vulnerability disclosure policy (CVDP) enabling them to receive reports of vulnerabilities (with appropriate communication channels).

Each organisation may also offer a Bug Bounty programme (offering financial rewards for detected vulnerabilities), thus encouraging experts to contribute to the security of public services.

Centre for Cyber Security Belgium
Rue de la Loi 18
1000 Brussels
Belgium
http://www.ccb.belgium.be

Katrien Eggers
Spokesperson(NL/FR/E)
+32 485 76 53 36
katrien.eggers@ccb.belgium.be

Michele Rignanese
Spokesperson(NL/FR/E)
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be