Visma's "Mother of Hackers" speaks to Intigriti about running a successful virtual live hacking event

BY ANNA HAMMOND · DECEMBER 16, 2021 · LAST UPDATED ON MARCH 6, 2025

Intigriti live hacking events involve bringing together a select team of security researchers, also known as ethical hackers, for a group bug bounty engagement. The invited researchers participate from across the globe, focusing on a particular target and set of assets. Hackers are chosen to take part in the event based on the skills and creativity they've demonstrated on the platform over time.

In most cases, live hacking events are in-person but due to the pandemic and social distancing regulations, many companies are choosing to hold events virtually. A recent example of this was Visma's 1337UP1121 event in November 2021, which was run in partnership with Intigriti. Visma's Security Engineer, Ioana Piroska, tells us more about how they were able to make their live hacking event a success.

Intigriti: Welcome Ioana! Can you start the interview with an introduction of yourself?

Ioana: Of course! I'm currently part of Visma's Security Testing Team, based in Timisoara, Romania. Before that, I worked as a Security Engineer for the business for three years.

For my role within the security team, I mainly manage and coordinate Visma's bug bounty program. Some of my responsibilities include:

- Ensuring new service delivery teams have a smooth onboarding in the program.
- Offering guidance and counseling to the new teams that are in the process of starting the bug bounty program.
- Planning the new onboardings.
- Keeping our hacker's engagement.

This last part involves me doing my best to keep our hackers motivated, which in time has resulted in my nickname from colleagues: Mother of Hackers. We made this name official with a Twitter account (@HackersMothers), where I post updates about our bug bounty programs and special campaigns. So, if you are a hacker and want to stay up to date with Visma's Bug Bounty programs, make sure you follow me!

As well as all this, I am also part of the Visma triaging team. When time permits, I jump in and work on triaging the reports.

Intigriti: You must be busy! You recently ran Visma's virtual live hacking event. Can you tell us more about it?

Ioana: We started our bug bounty journey almost 3 years ago. We've carried out various hacker engagement campaigns but never a live hacking event. So, this was our first and exclusive live hacking event, which we organized with Intigriti — it was a great collaboration for making this a memorable event.

Because of the pandemic and social distancing regulations, we decided to run the event virtually, but we were continuously in touch with the hackers via different channels and hopefully managed to make this experience as close as possible to a physical one.

Visma 1337UP1121 Virtual Live Hacking Event

The event took place between 28th October 2021 to 11th November 2021. It was two weeks of live hacking, amazing reports, and great fun! But also, most importantly, Visma's assets became more secure

as a direct result of the virtual event.

Intigriti: Sounds like a success! Are you able to tell us more about the scope of the live hacking event?

Ioana: Absolutely. First, it is important to say a few words about Visma to completely understand the context of choosing the teams for this live hacking event.

Visma is one of Europe's leading software companies with a presence across the entire Nordic region along with Benelux, Central and Eastern Europe, and Latin America. We make software that simplifies and digitizes core business processes in the private and public sector, mainly ERP systems.

We are a conglomerate, composing of 200+ companies in 37+ countries, and we have around 40 new acquisitions per year. Our job in the security team is to assist and empower these 200+ companies to make good security decisions every day. For this, we have developed a security program called VSP (Visma Security Program) and bug bounty is an important part of it.

Regarding the live hacking event's scope, we decided to take the opportunity to retest some of our most valuable and mature assets, which were already part of our bug bounty programs. These were the so-called "hard targets" because usually in a Bug Bounty program, most of the attention is focused on the new targets. Since we continuously add new features for our applications, we decided to pick the most experienced teams and some of the most important assets for Visma and retest them.

However, we also wanted to have a fresh scope and make this event even more attractive for the hackers. A few days into the live hacking event, we launched a completely new application into the bug bounty scope. This was a successful approach because the hackers spent time on old assets in the beginning – we've had some great insights from this – and once we launched the fresh target, their focus was on the new scope.

Intigriti: What were the results of the event?

Ioana: In the two weeks of live hacking, Visma received 363 submissions and 251 were considered valid (including duplicates); we also had a dupe window where we also rewarded the duplicates. The vulnerabilities reported included two exceptional, two critical, and two 0-days.

We paid €93K+ bounties in total. We also gave out some nice bonuses for keeping our hackers motivated. One of these was a bonus for the best meme. It was extremely fun to see how creative the hackers were and it was difficult for us to choose the best meme because we got so many good ones!

Intigriti: Can you tell us about some of the vulnerabilities found?

Ioana: The live hacking event top submission types were improper access control issues, IDORs, improper authorization, horizontal and vertical privilege escalation, and cross-site scripting. As is the case with bug bounty programs in general, the findings during the event were bugs that can't be found with automated tools. You need to spend time understanding the application flow, of which only the human mind is

capable. Being in direct contact and communicating in real-time with the hackers was a real benefit for this aspect.

The most interesting findings were, of course, exceptional, and critical reports. There were two account takeovers, meaning there were two ways for potential attackers to gain access to any account they want. The first was found through an LFI, a local file inclusion. This was found in combination with an SSRF, a server-side request forgery, where an attacker can have the server browse to other websites, and so on.

The second account takeover was an XXE or an XML external entity attack, which occurs when a user input in XML is not thoroughly cleaned. This was used to get data from the server and interact with the internal network.

We also have two potential CVEs, which are not public yet. We are in the process of reporting them to upstream, so in a way, the benefits of our live hacking event will reach beyond Visma, and potentially help others as well.

Intigriti: How did it impact or change how you run your bug bounty program?

Ioana: We will continue adding fresh scope into our programs and we're keen to organize more live hacking events in the future. The event gave us a fantastic opportunity to engage with our community, and the result was a set of impactful reports in a short amount of time. Of course, now that we know about these vulnerabilities, we can fix them and remove the risk of a potential exploitation in the wild.

Intigriti: What advice would you give to other companies considering running a live hacking event?

Ioana: Organizing such an event needs time, planning, and preparation. In our case, the event ran smoothly due to:

- **Visma's internal team** committed in advance to validating and fixing the reported bugs quickly. They were available to answer questions and were happy to work extra hours to finish the reports in time to ensure the event kept the momentum.
- **Our partner, Intigriti,** helped us organize this event. They were there for Visma and the hackers throughout and kept motivation high. They also contributed to the event, not only with ideas but by implementing them too.
- **Visma's Security team**! It was intensive work and their contribution was priceless — but we all agreed that organizing such an event is worth all the effort.

I think it is very important to be in direct contact and communicate in real time with the hackers (even if the event is virtual); helping them to understand the applications flow and answering questions will engage them even more.

To summarize, we had some cool findings from the virtual live hacking event. Fixing all these vulnerabilities led to Visma being a more secure company — and we had a lot of fun doing it!

Interesting in running your own live hacking event? Speak to one of Intigriti's experts today. Contact us today.

About Ioana

Ioana Piroska is a Security Engineer at Visma Software, based in Timisoara, Romania.

Her goal is to keep up with everything new, which has helped her stay on top of her game since she first entered the IT field 15 years ago.

As a former Application Support Engineer, System Administrator, Network Engineer and for the last 3 years, a Security Engineer, she has gained a wide combination of technical and communication skills which have helped her succeed in the security field.

She is the Bug Bounty Program manager at Visma, helping the service delivery teams during the onboarding process and throughout their Bug Bounty journey. Her goal is the success of the program by making sure the hacker's engagement is maintained.

As a mother of two, she balances work life and family life very well, always finding some free time for her hobbies such as reading, sports, and baking. FUN FACT: Ioana's passion for Cyber Security and care for ethical hackers participating in Visma's Bug Bounty Programs earned her the nickname "The Mother of the Hackers".