Hacker insights: @Itsirkov on the business of ethical hacking

BY ANNA HAMMOND · AUGUST 15, 2024 · LAST UPDATED ON MARCH 6, 2025

Once viewed with caution, ethical hackers are now regarded as an essential asset for many cybersecurity teams around the globe. Their proactive approach to finding and surfacing security weaknesses enables security teams to stay several steps ahead of potential cyber attacks. As cyber threats grow in sophistication, the role of ethical hackers becomes increasingly critical, making them indispensable in our ongoing battle against cybercriminals.

Today, we're spotlighting Lyubomir Tsirkov, known in the bug bounty world as @Itsirkov. Lyubomir is one of a kind and an expert at pinpointing vulnerabilities organizations haven't spotted, a talent that recently saw him take the top spot on Intigriti's monthly leaderboard in just 30 days. He secured €57,250 in bounties and earned almost 1,000 reputation points from this feat—but we'll let him tell you more about that. Join us as we explore the impactful world of ethical hacking through Lyubomir's experiences.

Intigriti: Hi, Lyubomir! Tell us about yourself

@Itsirkov: Hi there! My name is Lyubomir, and I am from Bulgaria. I've been working in cybersecurity for about seven years now, with web application security being my greatest interest.

I currently have a full-time job as a Red Teamer, and in my spare time, I participate in bug bounty programs and CTFs (Capture the Flags.) When I am not hunting for bugs, I like working out and writing blog posts.

How did you get started in bug bounty hunting?

I remember the first bounty that I received for discovering a critical vulnerability in a widely used VoIP and messaging app back in 2017. At that point, the company didn't have an official bug bounty program, but it did have an incentive for reporting exceptional vulnerabilities. It was exciting to receive my first reward.

In the following years, I didn't take part in bug bounty programs. However, my involvement has increased over the past two years, and it's been amazing to see how much this industry has grown!

Congratulations on your recent achievement on our platform! Can you tell our readers about it?

Of course! I was invited to a private bug bounty program, and during my participation, I discovered 18 critical vulnerabilities within 30 days of hacking. Initially, I used automation for catching the low-hanging fruits. Later, I continued with manual testing which resulted in finding most of the vulnerabilities.

Lyubomir Tsirkov
OSCP | Penetration Tester | Bug Hunter
1y

I'm excited to share my greatest achievement in bug bounty! In 30 days of hacking on **Intigriti** platform, I accomplished:
Ranked #1 on the monthly leaderboard.
Ranked #1 on the monthly leaderboard - Category: high to exceptional
Total bounties awarded: €57,250
Crossed 1,000 reputation points

A few tips:
Learn everything about the applications you are testing -> Less duplicates.
Fuzzing and JS analysis is important to find interesting endpoints and bugs.
Chain vulnerabilities when possible for showing higher impact.

Thanks to **Intigriti** for the best triage process!

https://t.co/l8OZqAhpDZ
https://lnkd.in/dyAet2eC

90 13 Comments

Like **Comment** **Share**

I was able to demonstrate impact through exploiting vulnerabilities of different categories, such as broken access control issues, server-side injections, and common misconfigurations. As a result of my findings, I was awarded $57,250 and achieved the top ranking on the private program and monthly leaderboard.

And what were your big learnings from this experience?

I learned that despite the massive competition in bug bounty programs nowadays, if you spend enough time to thoroughly understand how the application works, it will eventually pay off.

I'd also like to highlight that I had the opportunity to collaborate with an amazing security team on this program. They take the security of their organization very seriously, and during the process, they fully

engaged with my reports. The takeaway here is that there are security teams out there that truly value and appreciate the significant contributions ethical hackers make toward strengthening cybersecurity.

What motivates you to participate in bug bounty programs?

I'm motivated by competitive rewards and constant competition with other hackers on these programs. On the other hand, there is a great sense of achievement when you find a critical vulnerability in a challenging target.

Another motivator is the recognition you receive and the possibility of sharing your experience with other hackers in the community.

How do you prioritize which vulnerabilities to pursue in a bug bounty program?

When I am working on a new target, I typically prioritize finding low-hanging fruits. As I progress, I dive deeper into the application to gain a comprehensive understanding of it. It's important to review the rules carefully and understand the weakest areas of the company's business model, too.

What strategies do you think companies should use to enhance their bug bounty programs for ethical hackers?

Setting a clear scope and expectation of what is considered critical for the organization along with offering competitive bounty ranges and efficient average response time will make the program significantly more attractive.

What types of vulnerabilities do you encounter most often? Are there common weak spots that slip past security teams?

In my experience, I mostly come across vulnerabilities like privilege escalation, IDOR (Insecure Direct Object References), cache issues, injections, and misconfigurations.

As for common weak spots, depending on the size of the organization, I noticed that companies mistakenly expose applications or leave forgotten old or misconfigured assets externally accessible.

Can you walk us through how you would document and report a discovered vulnerability?

I strive to keep the vulnerability reporting process simple. In my reports, I provide a clear description of the finding, a detailed proof of concept (if necessary, even a video), and the most important part is

demonstrating clearly the impact of the vulnerability. My goal is to ensure that both the triage team and the program manager can easily understand the report.

How important is collaboration between ethical hackers and internal security teams?

I can give an example with an interesting Cross Site Scripting (XSS) vulnerability that I discovered in a popular streaming service company which resulted in good collaboration with the internal security team.

A prerequisite was set; to exploit the vulnerability, the Smart TV needed to have its User-Agent set up with a malicious JavaScript payload. In a later stage, that payload could have been shared with other users by simply sending a specially crafted, malicious URL.

The internal security team was fully engaged with the report, and after collaborating and providing more specific details, the team successfully mitigated it.

How valuable do you find the feedback from companies after submitting vulnerabilities?

I've always appreciated it when companies shared positive feedback for my hard work. It further motivates me and certainly, it might influence my decision whether to hunt on their program or not in the future.

Where do you see the future of ethical hacking as part of standard cybersecurity practices heading?

Personally, I am confident that there will be an increase in the number of programs launched in the future due to the effectiveness of the model as well as the availability of skilled white hat hackers on the platform. The community has already grown a lot in recent years.

Do you find having triage available useful? And if so, why?

The short answer is yes, I find it useful to have a skilled triage team available. It's the party to engage with reported vulnerabilities and subsequently validate and prioritize them for companies.

However, the triage team must be well-structured to ensure the workload is effectively managed, preventing the team from being overwhelmed with reports as it might result in neglecting details in reports.

Thank you for your interview, Lyubomir. We've enjoyed learning from you!

Lyubomir is one of 100,000+ security researchers on Intigriti's platform—and we're still growing! Continue learning about our community of security specialists in the Ethical Hacker Insights Report 2024. [Download the report](#) now!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com