

# THE YESWEHACK BUG BOUNTY REPORT



9.1 Critical  
CVSS

+24 PTS

P5

8.5 High  
CVSS

P3

C-10.0

\$

<<SCRIPT>JAVASCRIPT:ALERT(1)</SCRIPT>



BUSINESS LOGIC ERRORS

34.57  
IMPACT



CWE-840



ACCEPTED

5 PTS AWARDED FOR REPORT QUALITY



+15 PTS

CWE-840

```
<img src=
src=file:
<?php
select
${class
'"><s
php://
```

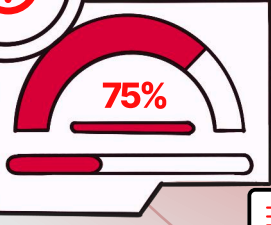
\$20,000

7.5 High  
CVSS

P4



M-6.8



CWE-840

SELECT @@VERSION

TRIAGE ASSESSMENT

NEED MORE INFORMATION

{CLASS.GETCLASSLOADER()}?

HACK ME  
I'M FAMOUS

P2



€26,000,000

\$20,000

2025 EDITION

7.5 High  
CVSS

P1

CWE-284

YesWeHack

ACCEPTED

€

# TABLE OF CONTENTS

<b>INTRODUCTION</b>	<b>01</b>
<b>HISTORY AND EVOLUTION OF YESWEHACK</b>	<b>02</b>
<b>THE BUG BOUNTY BOOM</b>	<b>03</b>
<b>PUTTING THE 'SUCCESS' INTO CUSTOMER SUCCESS MANAGEMENT: MEET OUR HEAD OF CSM</b>	<b>07</b>
<b>BUG BOUNTY VULNERABILITY TRENDS</b>	<b>11</b>
<b>'HAPPY CUSTOMERS EQUAL HAPPY HUNTERS AND VICE VERSA': MEET YESWEHACK'S TRIAGE CHIEF</b>	<b>14</b>
<b>HONOURING OUR HUNTERS: THE YESWEHACK HALL OF FAME</b>	<b>16</b>
<b>HOW TO SUCCEED AS A BUG BOUNTY HUNTER</b>	<b>23</b>
<b>DOJO: HELPING HUNTERS HONE THEIR HACKING SKILLS</b>	<b>25</b>
<b>LIVE HACKING EVENTS: A BANNER YEAR FOR IN-PERSON BUG HUNTS</b>	<b>26</b>
<b>BUG BOUNTY AND THE CHALLENGE OF SECURING OPEN SOURCE</b>	<b>30</b>
<b>TOP 7 TAKEAWAYS FROM OUR BUG BOUNTY REPORT</b>	<b>32</b>

# INTRODUCTION

**Happy New Year to our valued customers, hunters & any other InfoSec professionals reading this report!**

This is an opportune time to launch our first-ever annual review of Bug Bounty trends, based on the wealth of data generated on our platform. For a start, this year marks our 10th anniversary! It's incredible to reflect on the progress we've made since a trio of hackers hatched a business idea over a beer at 'La Nuit du Hack': a decade later and it's reasonable to say that we're now a truly global Bug Bounty and vulnerability management platform.

Our consistent expansion since our foundation in 2015 accelerated in 2024, driven by rising recognition of the Bug Bounty model's value in a complex threat landscape. We saw increasing adoption of crowdsourced security testing beyond the biggest market, North America (where YesWeHack recently established a strong presence), such as in Europe and southeast Asia (where we have local offices).

Growing interest in Bug Bounty has surely been fuelled by significant regulatory developments. A series of EU cyber acts that had progressed (to paraphrase Ernest Hemingway) *gradually* through the legislative process were then *suddenly* adopted or enacted in 2024.

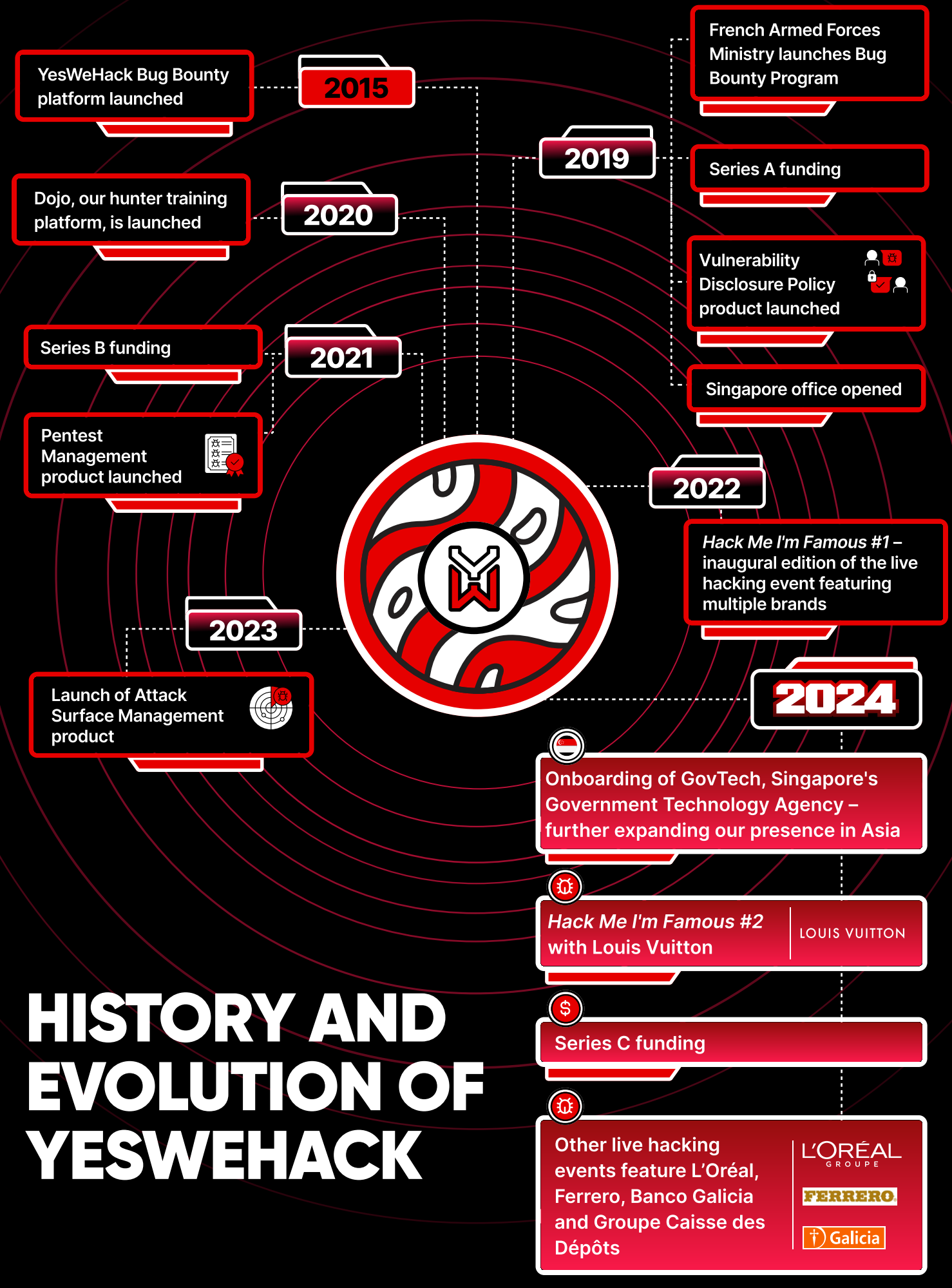
Central to these new laws – namely NIS 2, the Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA) – are requirements for the proactive discovery of vulnerabilities and a risk-based approach to their remediation. As with GDPR, we might expect Europe's regulatory moves in the cyber arena to be emulated by other jurisdictions in the years to come.

The cash injection we received last year from Series C funding was a bet by investors that YesWeHack's vulnerability management products are well placed to help organisations meet these new compliance obligations. But it's not just compliance requirements fuelling interest in Bug Bounty. It's surely no coincidence that investments in continuous, scalable and risk-based security testing are also growing in tandem with attack surfaces and the number of in-the-wild vulnerabilities. It's certainly easy to see why CISOs and regulators alike are prioritising vulnerability management when unaddressed vulnerabilities are, according to Mandiant, to blame for 38% of breaches.

This report distils and analyses activity on all our programs across the last 12 months. Among other insights, you'll find key vulnerability trends, exclusive advice and inspiration from hunters and customers, interviews with our heads of triage and customer success management, a recap of our 2024 live hacking events, and a hall of fame chapter honouring the achievements of our most prolific hunters.

## Happy New Year and Hack the Planet!





2015

YesWeHack Bug Bounty platform launched

French Armed Forces Ministry launches Bug Bounty Program

2020

Dojo, our hunter training platform, is launched

2019

Series A funding

Vulnerability Disclosure Policy product launched

2021

Series B funding

Singapore office opened

Pentest Management product launched

2022

Hack Me I'm Famous #1 – inaugural edition of the live hacking event featuring multiple brands

2023

Launch of Attack Surface Management product

2024

Onboarding of GovTech, Singapore's Government Technology Agency – further expanding our presence in Asia

Hack Me I'm Famous #2 with Louis Vuitton

LOUIS VUITTON

Series C funding

Other live hacking events feature L'Oréal, Ferrero, Banco Galicia and Groupe Caisse des Dépôts

L'ORÉAL GROUPE

FERRERO

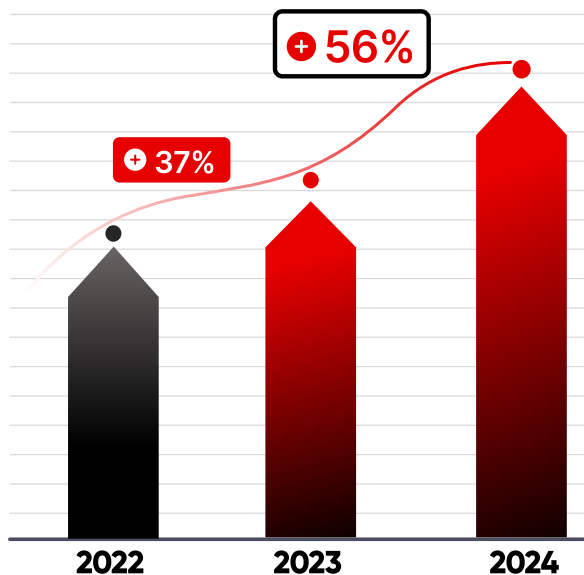
Galicia

# HISTORY AND EVOLUTION OF YESWEHACK



# THE BUG BOUNTY BOOM

## GROWTH IN THE NUMBER OF BUG BOUNTY PROGRAMS



The global Bug Bounty market is forecast to expand at a compound annual growth rate (CAGR) of nearly 16% between now and 2032 – up from \$1.52 billion to \$4.95 billion. Crudely measured by the increase in the number of programs (see above), our growth is perhaps outstripping even this brisk rate. As well as “growth and demand returning to pre-pandemic levels”, Business Research Insights attributes its prediction to organisations needing to “regularly test their IT infrastructure” given “constantly evolving” tech stacks and the fact “a hacker could potentially destroy a company's reputation in a matter of minutes”. It also reflects the fact that traditional testing methods are ill-equipped to meet multiple trends:

- » Growing **attack surfaces** and proliferating **vulnerabilities** due to digital transformation
- » Increasing numbers of **cyber-attacks** and fast-evolving **attack techniques**
- » Increasing **compliance demands** around IT risk assessment, vulnerability management and security testing
- » The persistence of a large global **cyber-skills gap**



A few things were revealed that were missed by a pentest before. A Bug Bounty Program is like a continuous, never-ending pentest with a large number of resources. It is a much larger scope and often more efficient than pentesting. It also generates less management overhead.”

👤 MICHAEL GILLIG

Senior Project Manager



In the face of these daunting challenges, some CISOs are now successfully convincing their boards of the necessity of increasing cybersecurity budgets. However, there’s also a recognition that simply throwing more resources at these problems – such as via the scattergun deployment of tools with overlapping functionalities – cannot tackle them alone. The solution also requires methodological, tool-agnostic improvements. After all, attackers are always innovating; defenders must too.



Bug Bounty Programs have become a security best practice nowadays. You have to embed it in your security program. Don't waste time and start soon!"

👤 VITTORIO ADDEO

Cyber Offence Manager

**FERRERO**



The volume and variety of vulnerabilities lurking in organisations' fast-expanding attack surfaces is only heightening the appeal of continuous, flexible and scalable security testing – especially when it's priced by results. Unlike a one-time pentest, a Bug Bounty Program provides an ongoing testing mechanism that leverages “the expertise of hundreds of researchers with diverse skill sets and unlimited time to thoroughly assess your applications' security,” according to Orange France Bug Bounty lead Yann Desevedavy. The value of crowdsourcing your offensive security skills from among tens of thousands of freelance hunters is obvious when you consider the stubbornly large cyber-skills gap. This appeal was illustrated starkly by a 2024 [UK government report](#) that found the average cybersecurity team had just two members, and that 57% were not confident in their ability to perform penetration tests.

**The world has moved on. People are investing more in resiliency because they know that attacks will happen.**

**GAURAV KUMAR SHARMA**  
Assistant Director, Security Architecture & Planning  
**ooredoo**

Cyber teams must also be able to efficiently find, fix and prevent vulnerabilities without disrupting accelerating release schedules. Fortunately, as well as accommodating traditional waterfall models (programs are configurable to run only during each testing phase, in a pre-production environment), Bug Bounty is ideal for CI/CD environments. “Bug Bounty is a great solution to address the new security challenges of agile methodologies and organisations that work in DevOps,” said Orange’s Yann Desevedavy.

**Because of the shift from project to product, the shift to CI/CD, it was really key to be able to be more agile and have continuous monitoring of the cybersecurity of all our websites.**

**JEAN-JACQUES MALLET**  
Group Cybersecurity Director  
**L'ORÉAL**

**A Bug Bounty Program enables assets to be added continuously and scopes to be extended as the environment evolves, enabling vulnerabilities to be discovered in real time.**

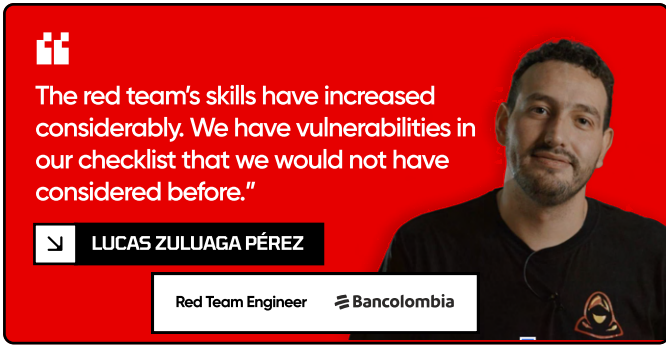
**SEBASTIÁN WILKE**  
Cybersecurity Manager  
**Galicia**

Another priority in an age of increasing vulnerabilities is prioritisation itself – namely of the most critical vulnerabilities, given there are usually too many to patch all at once. To this end, YesWeHack’s triage team helps customers validate impact and severity, and to prioritise the most critical bugs (although the customer has the final say). “The triage saved us an immense amount of time and enabled us to focus on what is essential,” said Fabrice Bru, CISO of the IT department at YesWeHack customer Les Mousquetaires Group, a major symbol group with 4,100 retail stores across multiple European countries.

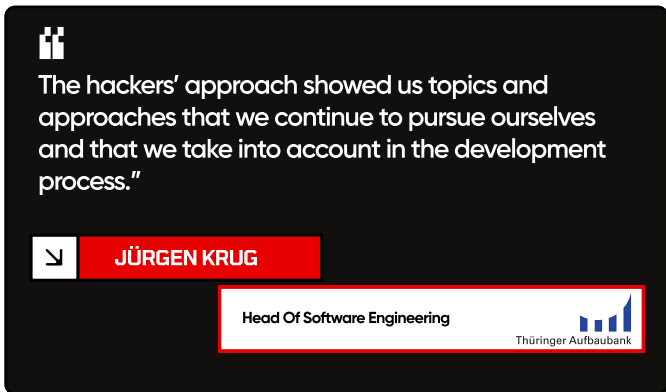
Crowdsourced security testing is also useful for increasing security awareness internally and instilling secure development practices. Orange France, for instance, intentionally leaves vulnerabilities reported by YesWeHack hunters on internally-accessible dummy websites. “Our employees then take on the role of ethical hackers to identify bugs that were previously discovered on our application,” said Yann. “It’s an engaging and effective awareness-raising activity.”

**Our work environment is very fast-paced. We launched our Bug Bounty Program to prevent problems from being introduced to our secure environment. We actively work with the security researcher community to use their feedback and findings to continuously improve our internal process.**

**YUEZHONG BAO**  
Group CISO  
**Lazada**

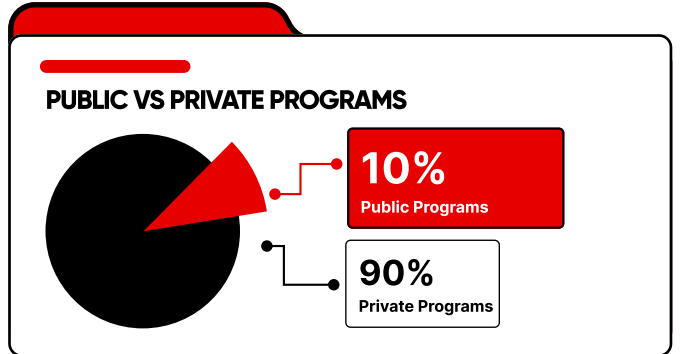


Early adopters of Bug Bounty Programs were predominantly Big Tech and software companies. However, more traditional sectors are increasingly recognising that, far from being a *risky* investment, Bug Bounty is an effective vehicle for *mitigating* risk. For instance, several financial institutions (such as Thüringer Aufbaubank and Banco Galicia) and public sector entities (such as the government of Quebec and Singapore's Government Technology Agency/ GovTech) have joined YesWeHack in recent years – and stayed with us having been impressed by the results.



These highly regulated industries have realised that fulfilling compliance obligations around security testing need not exclusively involve traditional pentests. Indeed, a raft of new EU regulations – specifically NIS 2, the Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA) – together prescribe a proactive, risk-based approach to vulnerability management that is arguably at odds with conventional time-boxed audits. “The requirements of the supervisory authorities for banks already include the performance of penetration tests,” said Jürgen Krug, head of software engineering at Thüringer Aufbaubank. “In this respect, Bug Bounty is a good addition, since it has the same objective as pentests, but utilises a different approach.”

Bug Bounty Programs can serve as a visible signal to users, customers and partners that an organisation is being proactive in strengthening its security posture with an incentive-based model.

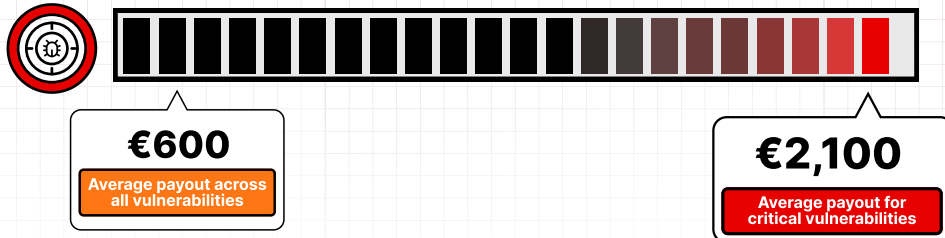


But this specifically relates to *public* programs, which are published for anyone to see on a Bug Bounty platform's website (or, in rare instances, self-managed by tech giants such as Meta or Google on their own domain). And public programs are actually only the tip of the iceberg, as the chart above demonstrates. On YesWeHack, public programs are often the culmination of a multiyear process that begins with private programs comprising a few scopes and a handful of hunters. Scopes, rules and bounty grids are continuously fine-tuned before the customer, once they feel internally ready, might consider launching a public program.

Private programs enable organisations, with the help of their CSM, to handpick hunters with the skill sets to suit their scopes, and set testing requirements in line with their security needs and budgetary constraints. Going public then provides maximum exposure to the diverse talents of tens of thousands of hunters (although some organisations decide that private programs better suit their needs in the long term). “The public program provides us with a broad access to talent,” said Michael Gillig, Bug Bounty lead at TeamViewer. “Customers really like that we run a Bug Bounty Program. It generates trust and shows strong commitment to security.” He added that “there is nothing to hide” when you run a public program. Previously averaging six vulnerabilities a month, the number of reports “exploded” once the first program went public – vindicating their extensive preparation, supported by YesWeHack.

# TOP BOUNTY PAYOUT 2024

# €50,000



The maximum reward paid out last year shows what a lucrative career ethical hacking can be – for hunters with the requisite patience, determination and skills. That a single vulnerability might earn a bounty comparable with a typical yearly salary in Western Europe is a huge incentive for ethical hackers to invest as much time as necessary to surface bugs that might take days, weeks or even months to find (although many are uncovered within an hour or two). By contrast, pentesters must conduct specific checks within pre-agreed time limits, meaning vulnerabilities that take longer to find can go undetected.

Nevertheless, financial rewards are just one variable among several influencing a Bug Bounty Program's performance. Other factors affecting the flow of vulnerabilities include the number of scopes and hunters invited, the skills required for the scopes, and how thoroughly the scopes have previously been tested (it makes sense to increase rewards when most 'low-hanging fruit' has been plucked).

At YesWeHack, we take great care in recommending hunters with skills that best fit the scopes and program objectives. Likewise, we help customers align the bounty range with the current maturity of each scope and the expectations of customers. Whatever the customer's budget, our community of hunters is large and diverse enough to produce results even at the low end of the reward scale. And being too generous, too soon, might generate more reports than a security team can handle anyway.



Bug Bounty gives you great insights into what's going on, because you use basically the same techniques for malicious hacking. And you get a fast return on investment. If we get serious vulnerabilities reported to us, it's worth it all day long to reward the hunter for those vulnerabilities."



ERIK TÄFVANDER

Head Of Cybersecurity



**"It's a very good way to uncover security vulnerabilities. And when you think about it, the high reward is still a good price for a critical bug."**



PAUL MARTY

Senior Product Security Engineer



# PUTTING THE 'SUCCESS' INTO CUSTOMER SUCCESS MANAGEMENT

Along with triage and the Bug Bounty platform itself, customer success management (CSM) is an indispensable pillar underpinning successful Bug Bounty Programs (BBPs). We quizzed the head of YesWeHack's CSM team about the CSM role, the keys to a flourishing BBP, and how his team ensures programs continually evolve to meet their security goals. Selim Jaafar joined YesWeHack in 2019 as our first customer success manager after roles in security consultancy, project management, communications and customer support.



## HOW DOES THE CSM TEAM TYPICALLY ENSURE A SUCCESSFUL BUG BOUNTY PROGRAM LAUNCH?

**Selim:** It's about finding an optimal balance in terms of scopes, rewards and rules. You want consistent results that build a use case for Bug Bounty as well as giving customers practical knowledge about running a program effectively, while being conservative enough to avoid a 'big bang' effect that overloads the customer with vulnerability reports or rapidly exhausts the budget. It's also important to help the customer adopt some basic good practices, notably with regards to collaboration with hunters. Pre-launch, we familiarise customers with:

- » Processing vulnerability reports and communicating with bug hunters to avoid miscommunications, mishandled reports or disputes
- » Using the platform to build strong processes and reduce time-to-fix and time-to-payout

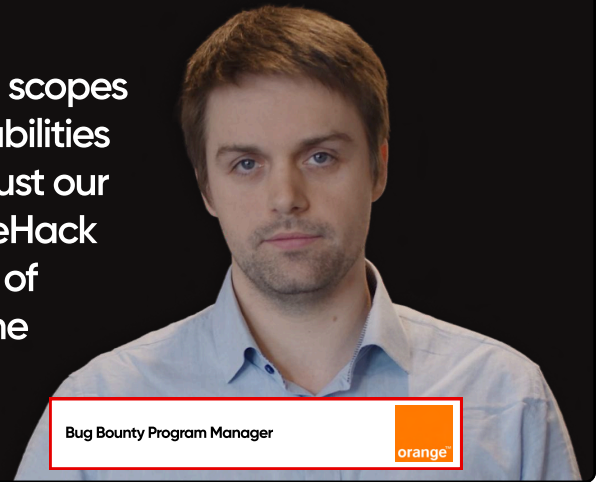
We also help the customer identify potential scopes; calibrate rules and rewards; finetune the program description for maximum clarity and fidelity to the customer's goals; set up roles and workflows; shortlist prospective hunters; and brief the triage team. To summarise: we ensure that the program reflects customer objectives, and is sufficiently detailed and attractive to hunters so as to promote their engagement and adherence to the rules.

- » How Bug Bounty works and the pitfalls to avoid
- » Program types and their requirements and pros/cons – such as public or private; grey-box or black-box; focused or wildcard (all assets in scope)





YesWeHack assisted us in determining which scopes to add, which hunters to invite, which vulnerabilities should be eligible, and how and when to adjust our reward structure and organise events. YesWeHack stands out due to their extensive knowledge of offensive security and their strong ties with the ethical hacker community."



YANN DESEVEDAVY

Bug Bounty Program Manager



## HOW DOES THE CSM SUPPORT THE CUSTOMER POST-LAUNCH?

**Selim:** The CSM guides the security team in handling the first tranche of reports, and setting high standards in terms of communication, qualifying reports, managing delays and so on. These early reports often generate many practical and theoretical questions about how best to handle communications with both triage and hunters, as well as considerations on platform functionality. So the training process, which identifies and tackles real-world problems and builds internal knowhow, continues beyond launch.

Initial reports can vary a lot in terms of quantity, quality and diversity. As CSMs, it's important to evaluate first impressions. Are the results consistent with expectations? And how were the results processed behind the scenes? This sets the tone for the security team's capacities and constraints.

We can then give better directions to the customer, whether it's to refine, slow down, extend or boost the program. We leverage our expertise to help the customer optimise their metrics in tune with their ambitions. We often propose tailored program development plans that enable the organisation to harness the community's talents in an achievable and productive way. We are then proactive in regularly reviewing and optimising the plan in collaboration with the customer to ensure it continues to align with their goals.



The relationship with YesWeHack is a true collaboration; the customer success team is always available and provides good advice. YesWeHack was able to adapt to our needs, which allowed us to quickly achieve our cybersecurity goals."



LOÏC DELEFORTERIE

Cybersecurity Engineer

WITHINGS

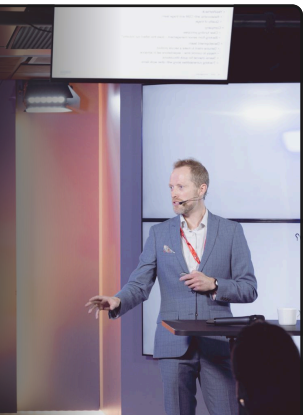


Excellent support and listening from the YesWeHack team, for both defining the most relevant vulnerability disclosure strategy and running operations."

CISO of a media company, from a Gartner Peer Insights review



YesWeHack provided a lot of handholding and guidance."



GEORGE MEDHURST

Head of Program Management and Testing, Digital Solutions



## HOW CAN **FRICTION IN CUSTOMER-HUNTER RELATIONSHIPS** ARISE AND HOW CAN YOU OR THE CUSTOMER AVOID OR MITIGATE THESE PROBLEMS?

**Selim:** Disputes typically arise due to miscommunications, response times, and divergent CVSS assessments or interpretations of scopes and program rules. There are also challenging edge cases that are invariably addressed by frank and friendly communication, and an empathic and constructive mindset (on both sides). We intervene at different junctures to varying degrees, depending on the situation, either to pre-empt a problem, resolve a dispute or draw lessons to prevent recurrences of the problem.

We continuously strive to prevent problems with effective training, by instilling best practices and by encouraging clear program specifications. Nevertheless, there are always unanticipated challenges – and it’s our duty to help both parties find common ground and sensible solutions. The success of Bug Bounty Programs ultimately hinges on mutual trust. As a man-in-the-middle, it’s up to us to set standards for improving the framework, rules and processes that can be leveraged to prevent and settle disputes.

## WHAT ARE THE **MOST COMMON MISTAKES** MADE BY CUSTOMERS?

**Selim:** Most misconceptions or mistakes come from transplanting traditional offensive security approaches to the Bug Bounty framework. Yes, Bug Bounty has similarities to pentests, but Bug Bounty success particularly hinges on engendering mutual trust and carefully incentivising and encouraging the engagement of hunters. While we strive to acculturate the customer to the crowdsourced testing model during the launch phase, we sometimes have to help them remedy issues such as:

### » **Scopes being unaligned with testing goals**

For example, testing a mobile app without considering web services/APIs; a complex scope fragmented into small pieces so the hunter cannot develop a consistent attack scenario; or insufficient detail about the scopes that allows for misinterpretation – all of which can lead to inconsistent results and problems with out-of-scope interpretations.

### » **Inappropriate reward grid**

For instance, applying low to average rewards to mature, complex and hardened scopes, or vice versa. Offering low or zero rewards to medium severity issues is also detrimental, especially when such vulnerabilities can be chained for higher impact and can help hunters familiarise themselves with the program and its scopes.

### » **Unsuitable testing conditions**

These typically arise from a mismatch between expectations and means. If your objective is to find complex vulnerabilities, for instance, then black-box testing a web application is usually unproductive.

### » **Misconceiving hunters as adversaries**

It’s legitimate to worry that the goals of hunters and customers might conflict. However, hunters are in reality incentivised to pursue the same primary objective as customers: unearthing vulnerabilities with real business impact. By understanding hunters’ motivations and pain points, customers will see clearly how an open, honest and collaborative relationship – within, of course, the framework of clearly defined rules of conduct – is necessary to produce the best results and avoid problems.

To prevent such issues surfacing, the CSM team must be detail-oriented in managing customer expectations and helping the customer continuously optimise rules, scopes and testing conditions in line with their goals.



## HOW HAS THE **CSM OPERATION** **IMPROVED DURING YOUR** **NEARLY SIX YEARS AT THE HELM?**

**Selim:** We've come a long way, not just as a company but as a team too. We have gained a lot of useful experience, as have many of our customers, some of which we've been working with for several years. We've developed all kinds of programs, with various setups, strategies and learning curves. Over time our team has grown, we've refined our processes, and we've built a set of best practices. However complex the customer's testing needs, and whatever their sector, development model or security maturity, we feel we can handle it.

Finally, our job is fundamentally about providing human, expert support. However, we continually seek ways to automate and streamline processes – which frees us up to focus on delivering best-in-class support.



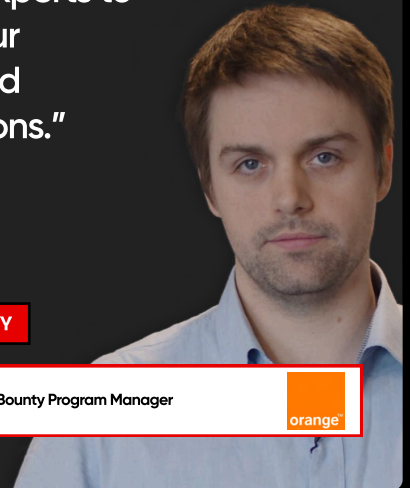
I think that, in the Bug Bounty world, service is more important than product. The platform itself works well, but what really matters is the ability of YesWeHack experts to understand our challenges and provide solutions.”



**YANN DESEVEDAVY**

Bug Bounty Program Manager

orange





# BUG BOUNTY VULNERABILITY TRENDS

The story of code vulnerabilities is one of rapid escalation – since 2016 we’ve seen a 521% rise in the annual volume of new CVEs – and innovation, with ethical and malicious hackers alike constantly pioneering new attack techniques for divergent ends. Last year we continued to see increasing numbers of relatively recent vulnerability types like OS binary, large language model (LLM) injection and HTTP request smuggling issues. And while development practices develop an immunological response over time and some bugs become less common (SQLi to some degree, for instance), XSS, which first emerged in the late 90s, continues to dominate, accounting for around one in five (21%) of all reports on our platform. It is also #1 on the [CWE top 25](#).

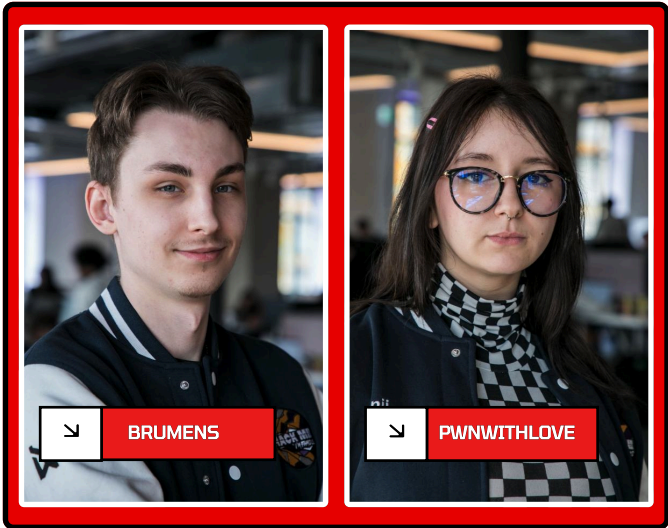
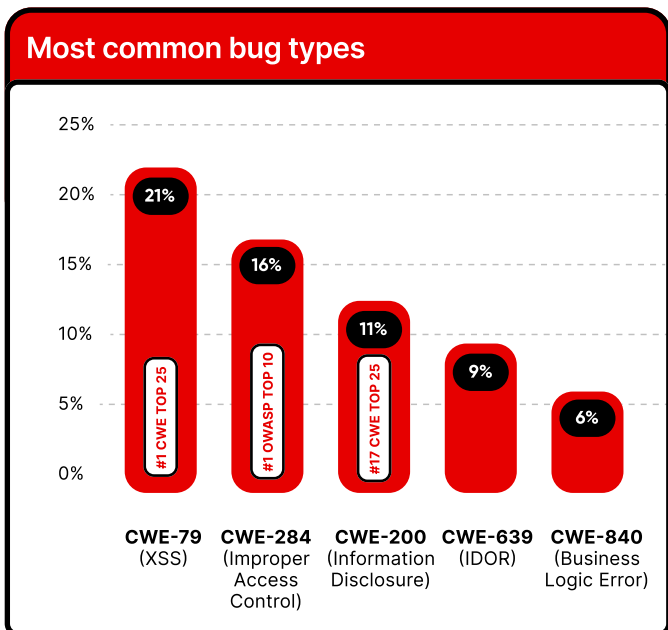
This shows that familiarity does not necessarily breed better detection by traditional testing methods, since pentests still often miss XSS bugs. We know this because a huge proportion of programs serve as a second line of defence after some initial hardening by conventional testing methods.

The other four categories in the list below concern design vulnerabilities whose identification and exploitation require a detailed understanding of the application. Their impacts are often high or critical.

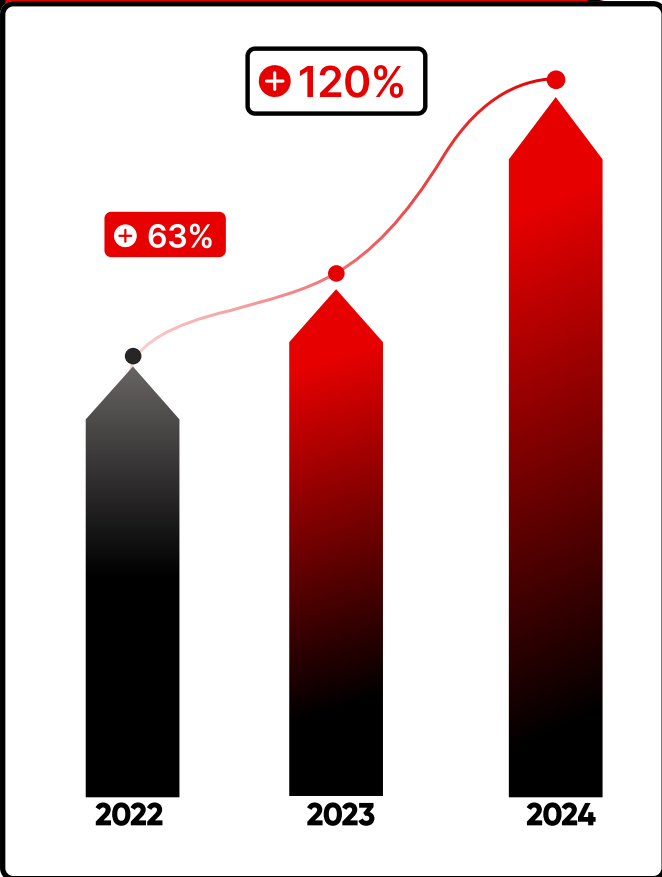
Top 5 biggest payouts		
€50,000	CWE-639 (IDOR)	July 24
€21,000	CWE-200 (Information Disclosure)	Feb 24
€20,000	CWE-284 (Improper Access Control)	Mar 24
€20,000	CWE-78 (OS Command Injection)	May 24
€20,000	CWE-78 (OS Command Injection)	July 24

But the most impactful vulnerabilities are not necessarily the most complex. Take IDOR (insecure direct object references) bugs, for instance: often simple to understand and explain, they nevertheless accounted for the most lucrative find of 2024. Swedish hunter Brumens and French hacker pwnwithlove collaborated to uncover an IDOR that earned a whopping €50,000 on a public program.

Finding and exploiting an IDOR, a type of access control vulnerability that occurs when applications use user-supplied input to access objects directly, doesn’t usually need especially advanced tools or complex exploit methodologies. That said, unearthing IDORs generally requires that hunters dig deep into applications in pursuit of anomalies. With IDORs, like many bug types, automated scans alone are rarely enough; humans, with capacity to invest whatever time is needed, are irreplaceable in the hunt.



Percentage increases of reports produced collaboratively



Hacking is not always the solo pursuit of popular perception. Hunters might have to share the spoils, but collaborating with their peers can open the door to vulnerabilities for which their own skill set is incomplete. This even applies to someone as multiskilled as ‘Nagli’, one of the world’s most successful hackers: “What helped me to become successful was a lot of collaboration,” he explained. “I got the insight that I can’t be the best hacker on every section, so I just find people who are experts” in the relevant areas. “Then, whenever you stumble on a lead, you can just pass it to them and you can explore it with them together.”

If the YesWeHack platform is a reliable barometer, ethical hackers seem to be collaborating more often than they used to – or at least collaborations are becoming more productive. In fact, as we’ve already explained, the vulnerability that earned the highest reward in 2024 emerged from a collaboration.

Nagli and Spanish hunters GoDiego, Djurado and Hipotermia collaborating during Louis Vuitton’s live hacking event

Collaboration is about sharing knowledge and combining different perspectives and experiences. It’s a great way to learn from others, build friendships and meet incredible people along the way! I’ll always remember the day Brumens and I got that reward – such a memorable experience to share with a friend after working together.”

↘ PWNWITHLOVE

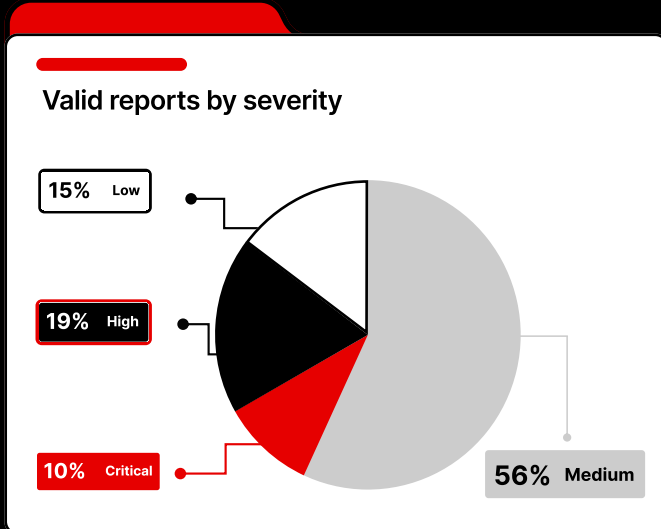
Co-collaborator on YesWeHack’s most lucrative bug of 2024

Allowing hackers to collaborate on a Bug Bounty Program enables hackers to work together with different skills and mindsets, which makes it easier to go down deeper when analysing applications.”

↘ BRUMENS

Co-collaborator on YesWeHack’s most lucrative bug of 2024





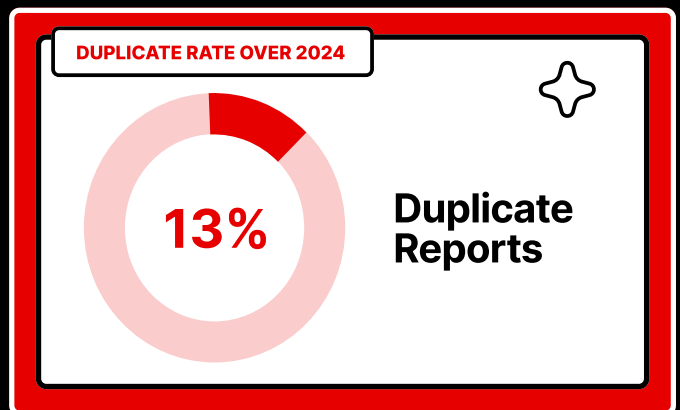
The frequency with which hunters find serious vulnerabilities is a testament to the value added by YesWeHack. Nearly one in three valid reports are designated as either critical or high severity.

**We've had, I would say, 20 really serious reports that we would never get from a traditional pentest. The collective knowledge we get from a Bug Bounty Program is huge, compared to a pentest where you hire a couple of researchers or consultants to help you."**

**ERIK TÄFVANDER**  
Head of Cybersecurity

During a Black Hat Europe 2024 panel, Vandana Verma, who sits on the OWASP Foundation's global board of directors, warned that malicious hackers were increasingly targeting low and medium severity vulnerabilities because organisations were so hyper-focused on addressing critical and high severity issues. Chained with other flaws, less severe vulnerabilities can still have serious adverse impacts.

YesWeHack still advises customers to address the most severe issues first – after all, organisations can typically only patch 10% of vulnerabilities in their environment each month, according to the Cyentia Institute. However, our model is geared towards facilitating the timely remediation of all vulnerabilities. The bug management process is streamlined through our platform's automations, dashboarding features and integrations with organisations' internal tools, together with our triagers' and hunters' prompt response to queries. YesWeHack is achieving an average first response to new reports of just 5-6 hours.



Duplicate reports – vulnerabilities the organisation already knows about, especially via previous reports from other hunters – are inevitable. Thankfully, however, most reports on YesWeHack (specifically 87%) notify vendors of vulnerabilities they were hitherto unaware of. Our low ratio of duplicate reports reflects the diligence with which our customer success team manages programs. Duplicate reports that *do* surface are then filtered out, along with other forms of invalid reports, by our triage team – saving customers considerable time. According to TeamViewer's Michael Gillig, YesWeHack's in-house triagers filter out around 30% of reports, whether as duplicates, out-of-scope reports or because they are missing a Proof of Concept (PoC) or other key information.

However, duplicates are understandably also frustrating for the hunters who uncover and report them in good faith. Organisations can maintain good relations with hunters who submit duplicates by acknowledging their efforts and being transparent in explaining why a report has been marked as a duplicate (for example, maybe another hunter found it recently, or a flaw was 'internally tracked' during a previous pentest). Equally, if not more, important is remediating vulnerabilities as fast as possible to reduce the potential time window for submitting duplicates. The customer should therefore continuously optimise their internal processes to reduce time-to-fix – something YesWeHack also facilitates by helping customers make remediation processes more efficient and outperforming our service-level agreements (SLAs) for responding to reports.

# "HAPPY CUSTOMERS EQUAL HAPPY HUNTERS AND VICE VERSA"

"Ensuring customers get clear, relevant and actionable vulnerability reports gives customers confidence in the process," says Adrien Jeanneau, who heads up YesWeHack's triage team. "This emboldens them to steadily expand the program and perhaps eventually launch a public program open to all registered and vetted hunters." In turn, this occasional addition of new hunting opportunities keeps hunters engaged, adds Adrien, himself a bug hunter since 2017. Founded and run by ethical hackers, YesWeHack recognises that "happy customers equal happy hunters and vice versa. It's a virtuous circle."

**MEET  
YESWEHACK'S  
TRIAGE CHIEF**



INTERVIEW WITH

**ADRIEN  
JEANNEAU**

## PROCESS AND PRIORITISATION

YesWeHack's full-time triagers aim to handle reports swiftly and objectively. The process involves analysing and validating/invalidating vulnerabilities, reproducing Proofs of Concept (PoCs), setting severity levels (CVSS), reviewing technical details, liaising with researchers to add missing technical information, and keeping customers up to date.

The triage team sometimes leverages knowledge accumulated from thousands of prior reports when setting severity scores. "A hunter might, for instance, send a PoC for an SSRF, and we know that in the past a similar report has been evaluated with a higher impact than initially estimated," explains Adrien. However, the final severity decision always lies with the customer. "If the customer has information about the technology that we don't, we need to trust their opinion," adds the triage chief.

Systematic prioritisation – based not just on submission date, but also severity and the triagers' initial impact evaluation – is a key plank of the YesWeHack model's success. "If a report is validated as truly critical, it gets triaged first," says Adrien.

Nevertheless, the process is speedy even for lower severity issues. "YesWeHack has a first-response SLA [service-level agreement] of two business days for all reports, but we're actually achieving an average of 5-6 hours," Adrien explains.

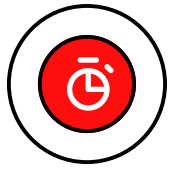
### YESWEHACK FIRST-RESPONSE SLA FOR REPORTS

**2 business days**

### YESWEHACK FIRST RESPONSE ACHIEVED

**5-6 hours average**





## THE ROLE OF A TRIAGER

The triage team keeps abreast of the risks, impact and possible mitigations of new vulnerabilities, such as large language model (LLM) injection, HTTP request smuggling or OS binary flaws. “That’s why we have an internal communication channel for sharing insights about the latest hacking techniques,” says Adrien.

Soft skills are as crucial as technical knowledge, however. “We’re intermediaries,” Adrien explains. “We collaborate with both hunters and customers to address problems or complaints, respond to comments and ensure reports are as clear and accurate as possible – including for customers who might lack technical knowledge.”



The reports come to us with valuable information added by the triage team during their assessment. These guys really know our products. We gave them subscriptions so they can look deep into the product without limits.”

MICHAEL GILLIG

Senior Project Manager 

The triage team also liaises closely with colleagues in the customer success management (CSM) team, which “shares information that helps us do our job – for instance, if scopes are accessible via accounts with four levels of privileges,” says Adrien. In return, “we are the eyes of the CSM team”.



The triage team are on the ball 24/7 almost, really rapidly giving us their insights on reports that we receive, and helping us during the process.”

ERIK TÄFVANDER

Head Of Cybersecurity 




For example, they might recommend new scopes, hunters or, if a program is underperforming, “making the program rules more restrictive to really focus on impactful vulnerabilities”.

Automation is streamlining the vulnerability management process, but not at the expense of human support. On the contrary, the team is only growing as its workload increases. “We cannot automate everything,” says Adrien. “It’s important to keep the human brain involved in triaging to ensure the impact reflects the context, our knowledge and the customer’s knowledge.”

So which of the triage team’s achievements is Adrien most proud of? “What started as a basic triage operation has evolved into a robust system with automation and seamless collaboration. I’m incredibly proud of how our team has built an efficient process and become trusted partners to our clients and security researchers alike.”



GEORGE MEDHURST

Head Of Program Management And Testing, Digital Solutions 



I think the triage team is world class. We’ve shown our technical support teams for software products how they deal with things. We’ve learned a lot – for free.”



# HONOURING OUR HUNTERS: THE YESWEHACK HALL OF FAME

Our hunters continue to impress with the depth and breadth of their skills. Determined by points awarded by our customers, their position on our leaderboards attests to the quality, clarity and frequency of their reports and their willingness to help customers understand exploits and remediate vulnerabilities.

Our fluctuating leaderboard reflects a closely-fought contest between hunters, all except one position: first place. Top position has been occupied non-stop – year on year, quarter on quarter – by the same hunter since 2019, and this did not change in 2024. And it's not even close, with the points gap to second place consistently enormous. 'Rabhi', who remarkably achieves this in concert with a full-time job, took time out from his mind-bogglingly prolific bug hunting to share the secrets behind his success (read his Q&A on the next page).

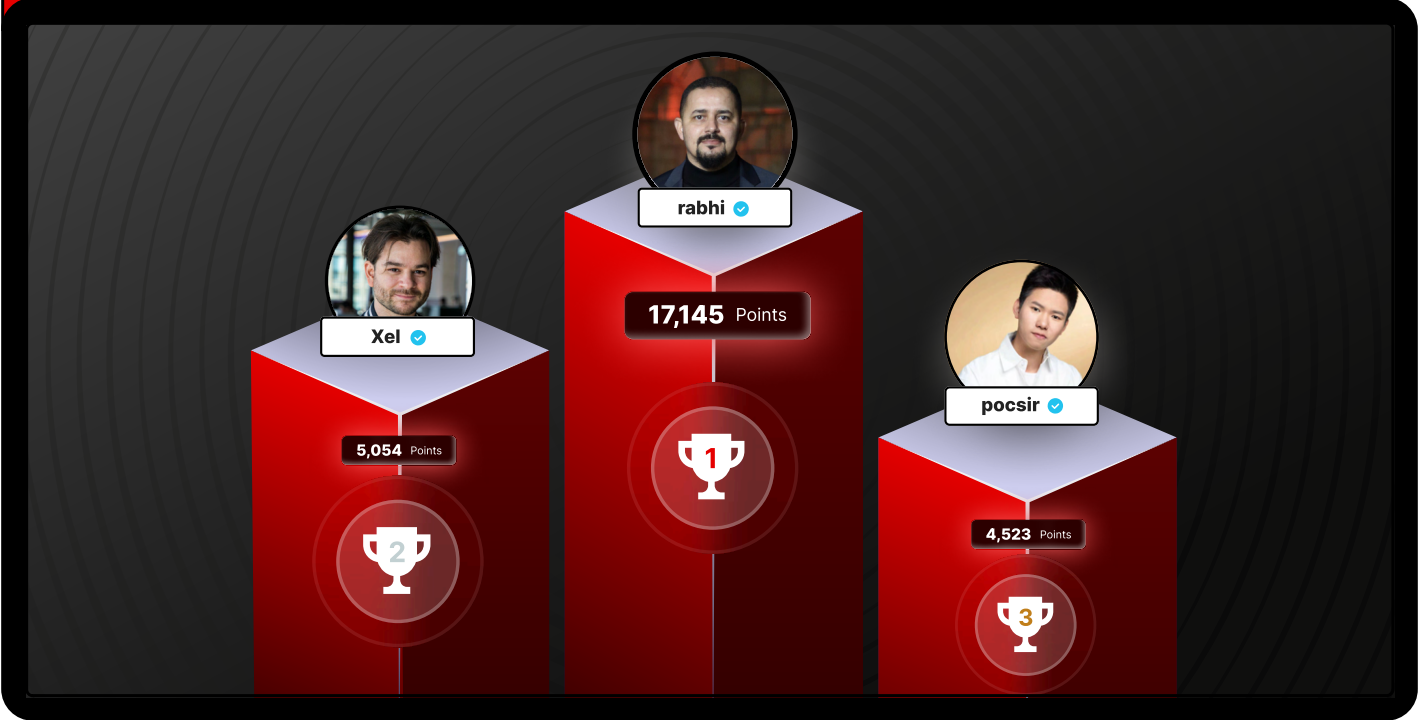


**Maintaining a strong relationship with hunters is critical to ensuring the longevity of your Bug Bounty Program. Being prompt in responding to hunters, maintaining transparency and ensuring fairness in the reward system will encourage hunters to continue working with you. Remember: without hunters there can be no successful Bug Bounty Program."**

YANN DESEVEDAVY

Bug Bounty Program Manager 

## YESWEHACK 2024 RANKING



# THE SECRETS OF MY SUCCESS: RABHI, RUNAWAY #1 ON OUR ALL-TIME LEADERBOARD



## HOW DID YOU BECOME A HACKER?

**Rabhi:** My involvement in hacking came from curiosity and a desire to experiment. I was fascinated by the idea of understanding systems and finding ways around them. My earliest success – reporting vulnerabilities to Zataz.com – reinforced my desire to specialise in hacking.

When I started out in Bug Bounty, I reported vulnerabilities to companies like Yahoo and PayPal. Over time, I developed a taste for more competitive programs, such as Google's, where making the top 10 was a defining experience. The first time I discovered a flaw in Google's program I spent a sleepless night wondering whether it would be accepted or not. That experience – a mixture of excitement and uncertainty – remains engraved in my memory as a key stage in my progress.



↙ **RABHI**

**YESWEHACK'S ALL-TIME  
#1 HUNTER**

## WHAT ARE THE SECRETS OF YOUR SUCCESS IN TERMS OF TECHNICAL SKILLS?

**Rabhi:** If there was one secret, it would be methodology. More than a set of skills, it's this ability to structure and perfect your research that will take you far.

Reconnaissance is the foundation of any successful test. Gather as much information as possible about your targets before you start testing. Because vulnerabilities and techniques are constantly evolving, you should also follow the latest trends and learn the most up-to-date workaround methods. Specialise in a specific area too, such as web, mobile or reverse engineering. In any vulnerability category, there is always something new to learn and master.

Finally, I recommend differentiating your approach. For example, on a search page, most bug hunters reflexively test the search field directly, because it's the most visible and intuitive element.

But I prefer to explore less obvious parameters, such as elements hidden in JavaScript. This 'off the beaten track' curiosity often leads to the discovery of unique flaws.

## WHAT ABOUT YOUR MINDSET AND SOFT SKILLS?



**Rabhi:** Soft skills are often underestimated, but they are essential in Bug Bounty. For example, you should trust your intuition and never give up. I've sometimes found vulnerabilities after days, even weeks, of painstaking research. And be disciplined. I devote at least two hours a day to Bug Bounty. This keeps me efficient and responsive, particularly when invitations are extended to new programs.

You should also respect the trust that companies place in researchers. The way you write reports and interact with program managers can make all the difference. Good communication can strengthen your relationships and increase your opportunities.

Finally, maintain a healthy work-life balance. Bug Bounty can be demanding, but it's important to know when to take a break to stay motivated.

## ANY ADVICE TAILORED TO HUNTERS WHO ARE JUST STARTING OUT?

**Rabhi:** The road to bug-hunting success may seem daunting, but with enough time and effort anyone can reach this destination. I recommend honing your technical skills on specialist training platforms such as TryHackMe, Root Me or Hack The Box. Also take part regularly in Capture-the-Flag (CTF) competitions, attend cybersecurity conferences to broaden your knowledge, and experiment with different approaches.

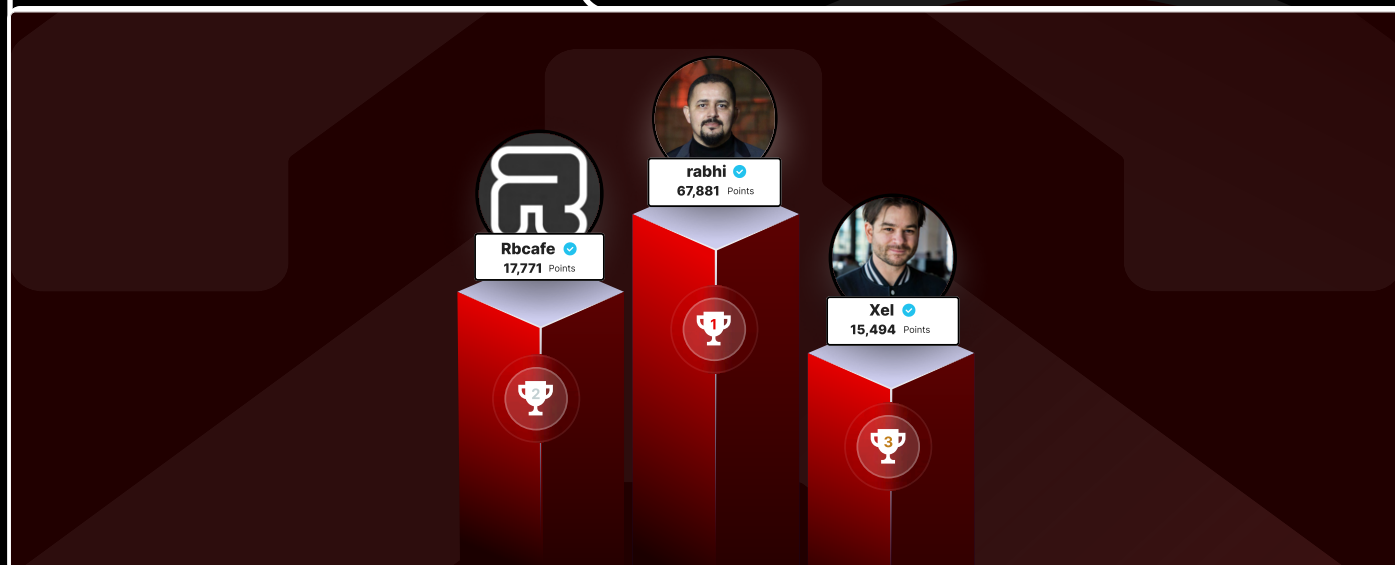
Finally, be patient and don't get discouraged: results don't come immediately. Duplicates or low scores are initially part of the process. Set yourself realistic goals and take things one step at a time. And remember: every discovery, however small, is a victory that brings you closer to your goals.

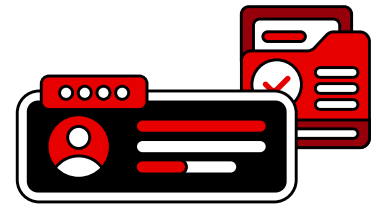
## ANYTHING ELSE TO ADD?

**Rabhi:** What sets YesWeHack apart for me is the community spirit and the quality of the programs on offer. It's a real source of inspiration. The team does a remarkable job of supporting researchers and improving programs.

For me, Bug Bounty isn't just a job: it's an intellectual and human adventure as much as a technical one. So to all those who are hesitating to take the plunge: dare to do it. It will be a long journey, but the rewards – in terms of learning, community and recognition – are well worth it.

### ALL-TIME LEADERBOARD



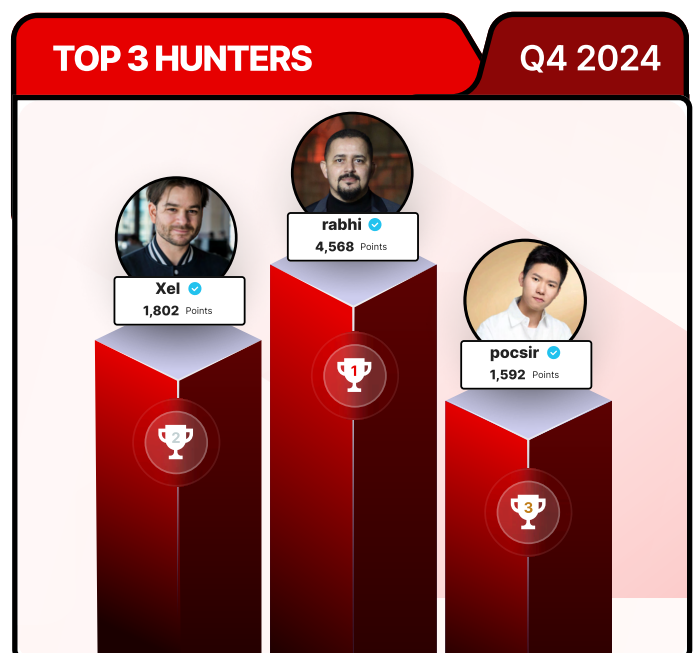
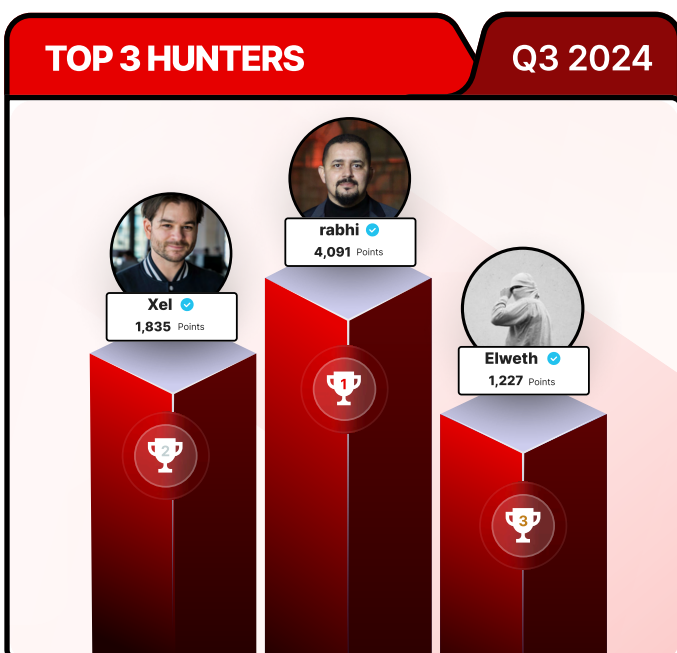
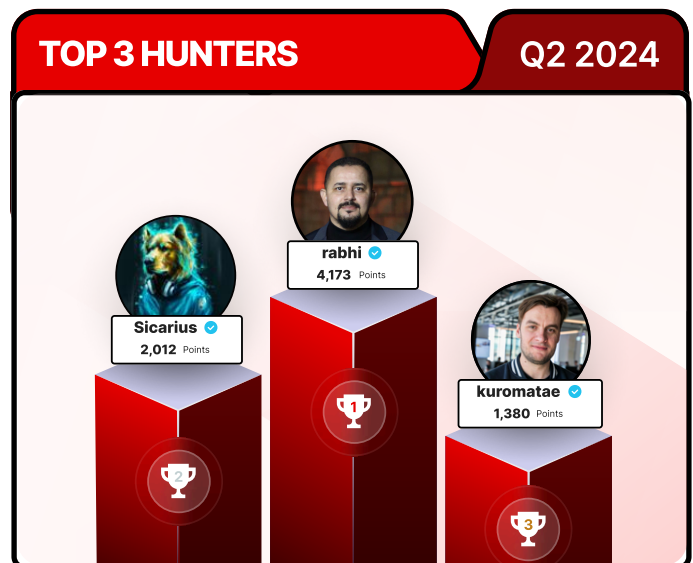
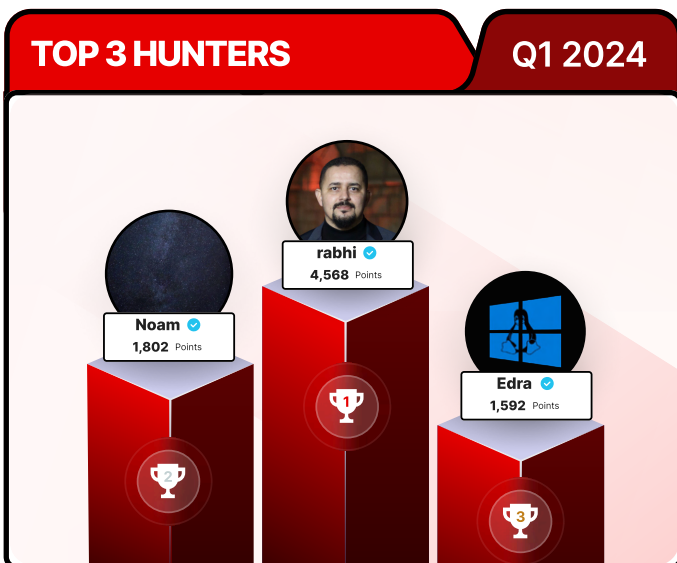


# QUARTERLY LEADERBOARDS


The overall leaderboards don't tell the whole story when it comes to honouring the patience, persistence and lateral thinking demonstrated by our hunters.

Our rundown of 2024's top performers for specific bug types also gives due recognition to hunters who made outsize contributions in certain niches. We can also see the vulnerability types that have particularly powered the success of overall #1 Rabhi (XSS) and #3 Xel (cryptographic issues).

As much as the continuous nature of testing and the size of our community – we're talking tens of thousands of hunters – it's the variety and depth of their skills that really distinguishes Bug Bounty from traditional pentesting. "They dig really deep into our products," said Michael Gillig, Bug Bounty lead at TeamViewer. The DNV team, meanwhile, "laughed" at the ingenuity of one particularly prolific hunter. "How clear he was with his reports, the intelligence behind it", and so many ways of escalating privileges, said program manager George Medhurst.



# TOP-PERFORMING HUNTERS BY CWE TYPES



**rabhi** ✓


#1 hunter for CWE-79 (XSS)



**Xel** ✓


**Solankip** ✓

#1 hunter for CWE-310 (Cryptographic Issues)



**bytehx** ✓

#1 hunter for CWE-312 (Cleartext Storage of Sensitive Information)




**Noam** ✓

#1 hunter for CWE-89 (SQL Injection)




**Oxsnpaii** ✓

#1 hunter for CWE-284 (Improper Access Control)




**Supr4s** ✓

#1 hunter for CWE-1336 (SSTI)




**Kto94** ✓

#1 hunter for CWE-840 (Business Logic Error)




**Icare** ✓

#1 hunter for CWE-78 (OS Command Injection)



**sagarbanwa1337** ✓

#1 hunter for CWE-611 (XXE)



**Codejump** ✓

#1 hunter for CWE-349 (Cache Poisoning Bugs)

KTO94

#1 HUNTER FOR CWE-840 (BUSINESS LOGIC ERROR BUGS)

## KTO94'S MAGIC METHODOLOGY

"I start by using the application as a regular user to understand how it works, exploring as many features as possible. I try to bypass limitations on features that I believe could have a business impact. If I succeed, I delve deeper to identify a business logic error that could have a real impact on the company.

"Most of the time, I focus on identifying a financial impact, whether direct or indirect. For example, take a booking company that adjusted its prices based on user demand. The more often users initiated a booking, the higher the prices would go. It was possible therefore for an attacker to manipulate the prices simply by initiating bookings without completing payment. Carried out on a large scale, this could lead to a loss of revenue for the company, as its prices would no longer be competitive.

"My main advice for business logic error bugs is to prioritise impactful issues rather than technically complex ones."

CODEJUMP

#1 HUNTER FOR CWE-349 (CACHE POISONING BUGS)

## CODEJUMP'S MAGIC METHODOLOGY

"First, do the [PortSwigger labs](#) for web cache poisoning, which are really very useful for getting a good understanding of the vulnerability. Then it's a lot of research to understand how the cache works on each technology, reading blog posts of research already done in this field etc...

"This vulnerability interested me, so I started looking at tools that existed to find/scan this vulnerability. But I noticed that most tools only checked a small part [of the process] or were out of date. From what I saw, only one checked for Cache-Poisoned Denial-of-Service (CPDoS) and was very verbose, so was therefore complicated to understand at a glance.

"So I built a tool that would be accessible and understandable for everyone: [HEXHTTP](#). Thanks to this, I've been able to research cache poisoning (and CPDoS in particular) in greater depth. I'm now putting pretty much all my research and findings into it, so I can re-scan Bug Bounty applications."

SUPR4S

#1 HUNTER FOR CWE-1336 (SSTI BUGS)

## SUPR4S'S MAGIC METHODOLOGY

"For the SSTI/CSTI hunt, it's important to analyse the technologies offered by the application (with Wappalyzer <3). Naturally, I like to go for big web applications with several technologies and different rendering depending on the part of the application you're accessing. This has enabled me to find CSTIs that are not visible at first glance, but can be triggered in another part of the application. Once you've got your injection point, you need to think IMPACT! A CSTI in your pocket? Try extracting session cookies, localStorage or any other way to get an ATO from your victim. An SSTI? Go for the RCE!

"One of my CSTIs was triggered by an exotic view of the application, via a VueJS that converted my `{{8*8}}` input into 64. Knowing this view was accessible for several other people, it was essential not to affect other users by using 'silent' payloads like `console.log({{ _openBlock.constructor('console.log('\"Stored XSS via CSTI by Supr4s\"')()}})`.

"My recommended resources for SSTIs/CSTIs: [SSTIMap](#), [TlnjA](#) and [tplmap](#) tools; the template injection chapter of Bug Bounty Bootcamp by Vicky Li (p261-274); [Template Injection Playground](#) on GitHub and other 'Hackmanit' resources; and '[Evading defences using VueJS script gadgets](#)' by PortSwigger researcher Gareth Heyes."

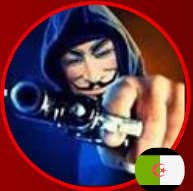
TOP 3 HUNTERS ON PUBLIC PROGRAMS BY NUMBER OF VALID REPORTS IN 2024

1



ralphspencer

2



djamel-ghorab

3



hktn0x

ALL-TIME TOP 3 HUNTERS ON OPEN SOURCE SCOPES



CALEHURI  
999 Points



MDISEC  
526 Points



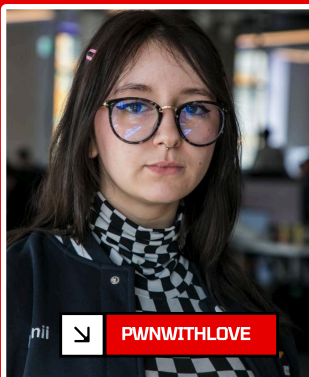
FOOBAR7  
326 Points



BIGGEST BUG BOUNTY PAYOUT OF 2024



BRUMENS

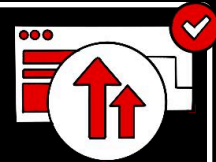


PWNWITHLOVE



**Brumens** and **pwnwithlove** netted **€50k** from an **IDOR (CWE-639)** collaboration on a public program





# HOW TO SUCCEED AS A BUG BOUNTY HUNTER

Not having a computer science degree or OSCP certification doesn't seem to be a major impediment to becoming a successful bug hunter.

It is true that many ethical hackers do indeed progress to Bug Bounty hunting after formal higher education in related disciplines, and often after (or concurrent with) careers as developers, pentesters or security engineers. This much was evident from our interviews with ethical hackers over the past two years (available on our blog and YouTube channel). However, these conversations also demonstrated that many of our most successful hunters (including pwnwithlove, Blaklis and GoDiego among our interviewees) got into hacking as teenagers, and their skills are often largely self-taught. In fact, a recurring theme of our hunter Q&As is that soft skills – such as patience, persistence and a talent for problem-solving – are as, if not more, important than teachable technical skills.

Bug Bounty is also the ultimate meritocracy. Hunters, who use pseudonyms (but are thoroughly vetted), earn rewards and points solely based on the quality of their work – namely the severity of their vulnerabilities, the clarity of their reports, and whether they respond promptly to queries around reproducing bugs, potential remediations and so on.

Below is some invaluable advice for how newbies and inexperienced hackers can excel in these areas, gathered from our conversations with some of YesWeHack's most successful hunters. Topics include developing the right mindset, sharpening your skills, methodological advice and tips for choosing targets and tools.



NAGLI

176

All-Time Ranking

"Follow everyone on X, ask them questions. It's good to be curious for insights. And look for products that you have extra authentication or privileges for, like if your bank has a Bug Bounty Program. If you have a privileged account that is not easy to create, you have an advantage over other hackers."



HAKUPIKU

45

All-Time Ranking

"Most people just look at API endpoints, making API calls from their mobile app, and since everyone does that, it's hard to find bugs of that kind. But I try to look more at native app bugs basically, like Android app bugs."



SERIZAO

33

All-Time Ranking

"Above all, be very patient. Get to know as much as possible about the applications you're going to target, and try and understand how the platform has designed its functions."



BLAKLIS

22

All-Time Ranking

"The most difficult aspect is the huge biases you can have at the beginning: 'I'm not skilled enough to take on big companies', 'there are already too many people who've tested before me' or 'I've spent three days hacking, I'm never going to find anything'. But we've all encountered these things."



GODIEGO

12

All-Time Ranking

"Experiment. Most times I find bugs while trying random theories, or saying: 'well, what would happen if I tried this or tried that?' Just don't rely on other people's tools; be creative and do your own thing. Because in the end that's what's gonna make you stand out and be different!"



CHACKAL

15

All-Time Ranking

"Surround yourself with people who want to teach you. And find a program with a huge number of features, so you can stay on it as long as possible and get to know the application well. Then you can spot potentially vulnerable features or unexpected behaviour – and dig even deeper."



PWNII

49

All-Time Ranking

"Sometimes you have to admit that you just can't find bugs. And it's pretty hard to deal with duplicates. But don't forget that a duplicate bug is still a valid bug. Be patient and motivated. Use Dojo. Don't be scared to go on public programs either. There are a lot of bugs."



ICARE

10

All-Time Ranking

"Newbies are often afraid of the programs. If it's a public program they think: 'Everyone's been there, I'm not going to find anything' – when in fact you can always find something. Be curious, be persistent, gather information, learn, understand the application and how to bypass it."

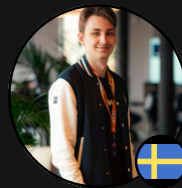


XEL

3

All-Time Ranking

"Stay creative, see what exists and come with your own approach. Familiarise yourself with all the basic security concepts. You need to invest time to be proficient – so don't give up! After some time, more and more vulnerabilities will come in and you will get better at hunting."



BRUMENS

77

All-Time Ranking

"Pick a target that you're comfortable with, that you feel motivated to hunt on. New hackers commonly spray a lot of features on the target with a default configuration, with no customisation. So make your own wordlist, understand the technology and adapt your payloads to the target."



# DOJO: HELPING HUNTERS HONE THEIR HACKING SKILLS

YesWeHack runs a Bug Bounty training and Capture-the-Flag (CTF) platform to increase the depth and breadth of skills available to customers. Launched in 2020, Dojo helps hunters sharpen their hacking skills in a fun environment before unleashing them on real Bug Bounty Programs.

Dojo, a free resource, accelerates the learning process by providing instant visual feedback to payloads. This 'under the hood' view helps hunters understand why their attacks succeeded or failed and to adapt their methods accordingly.

When hunters successfully complete monthly Dojo challenges they earn extra leaderboard points, which can unlock invitations to more lucrative private programs and, eventually, Live Bug Bounty events. In other words: the more they learn, the more they earn.

Dojo has three key features:

- » **Interactive training modules:** Ranging from beginner to expert level and covering various hacking techniques and vulnerabilities, from XSS to insecure deserialisation. New modules are added periodically to help hunters keep up to date with the latest vulnerability types.

- » **Monthly CTF challenges:** Crafted by renowned hackers to replicate in-the-wild security puzzles, these challenges are great preparation for tackling Bug Bounty Programs. The three best reports are rewarded with YesWeHack swag as well as points. The winners and the best overall writeup are published monthly on the YesWeHack blog.

- » **CTF playground:** Hunters can craft their own challenges without needing to set up a server, and enjoy the community's efforts to solve their web security puzzles.

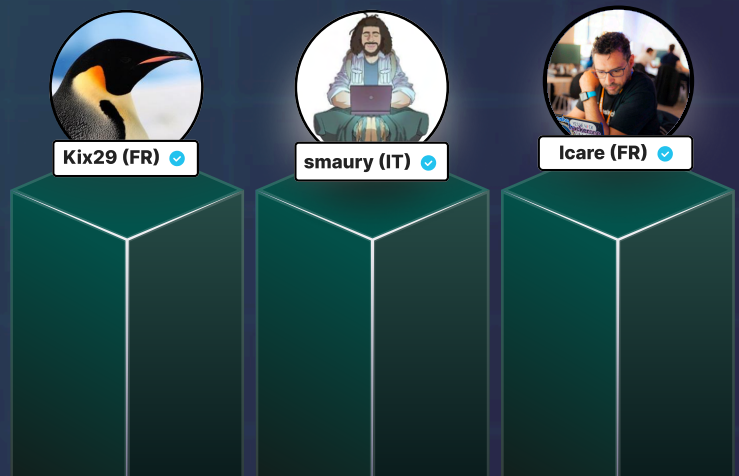
Hunters must sign up to the YesWeHack platform to participate in Dojo challenges. We recommend that they obtain KYC verification too, since this becomes mandatory for hunting on regular Bug Bounty Programs. Dojo is maintained by YesWeHack's in-house bug hunters and CTF players: [Bitk](#), [Hisxo](#), [Brumens](#) and [pwnii](#).

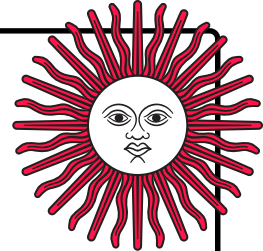
Visit [www.dojo-yeswehack.com](http://www.dojo-yeswehack.com) to find out more.

YesWeHack's in-house security researchers also develop and maintain a [variety of tools](#) to streamline and enhance the bug-hunting process.



## TOP HUNTERS ON DOJO CHALLENGES BY NUMBER OF SUCCESSFUL REPORTS





# LIVE HACKING EVENTS

## A BANNER YEAR FOR IN-PERSON BUG HUNTS

When organisations conduct live hacking events they reliably surface numerous vulnerabilities in a short space of time. The prompt remediation of these security flaws then serves as reassurance to customers and partners that the organisation takes security very seriously indeed.

Across two days, participants in these live bug bounties – sometimes handpicked based on their track record, sometimes drawn from a co-located hacker con – hack against the clock to unearth dozens of serious vulnerabilities and bug chains in websites, APIs and other internet-facing assets, in pursuit of financial rewards and points that propelled them up the leaderboard. The quality of their findings owes as much to in-person camaraderie and collaboration as it does to the race to make the podium.

For customers, these thrilling contests are a chance to meet and learn from the world’s most accomplished security researchers. “These events are interesting because we are not just behind a screen,” said Adrien Jeanneau, YesWeHack’s head of security analysts and researcher enablement. “Communication is always smoother when you can communicate and have a drink with customers and hunters face to face. It’s a good opportunity for customers to meet the triagers, to meet the bug hunters, and to introduce some specific new scopes.”

Taking part in this live event was an opportunity to meet the hunters who work all year round on our programs, which allow us to interact in real time. We discussed the bugs they reported, their understanding of our applications. An exceptional experience to be repeated. Thanks again to the hunters and to YesWeHack!

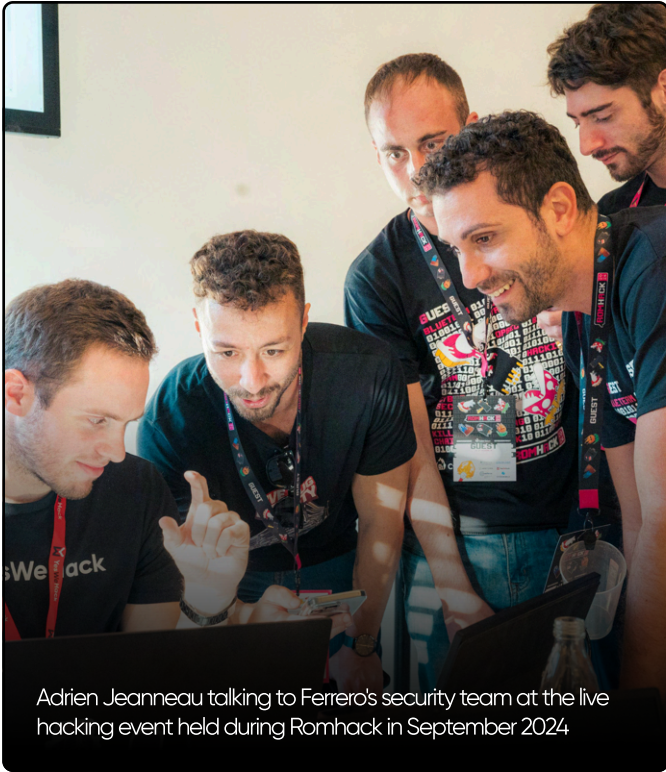
**HOCINE MAHTOUT**  
 Offensive Security Manager

This year again, the event was intense and full of twists and turns. It’s always great to interact with other hunters and introduce Bug Bounty to younger ones. A big shoutout to Caisse des Dépôts for the quality of triaging, transparency of their communication and the trust they placed in the ethical hacking community.

**ZAX**  
 Winner of the Live Bug Bounty featuring the Caisse des Dépôts

**FINAL PODIUM OF CAISSE DES DÉPÔTS EVENT** March 2024

Aituglo  
 ZaX  
 Gromak123



Adrien Jeanneau talking to Ferrero's security team at the live hacking event held during Romhack in September 2024



The key benefits were meeting the security researchers, meeting the triage team, and working together to find and fix some complex vulnerabilities. Thanks to this live event we could test some new scopes with very specific configurations that couldn't be added to our continuous program. We found some interesting vulnerabilities."



GUILLAUME KERMARREC

Threat And Vulnerability Manager

L'ORÉAL

Last year was our most spectacular yet for live hacking events – and not just because an iconic fashion house and the world's largest cosmetics brand provided some of the targets. It was also an unprecedented year in terms of the number of in-person competitions and the impressive results produced by participating hunters. Our second *Hack Me I'm Famous* edition took place at Louis Vuitton's Paris HQ, while the comparably glamorous L'Oréal also had its scopes hardened in the French capital, at leHACK.



DINDINDIN

Winner of the Live Bug Bounty featuring L'Oréal

FINAL PODIUM OF L'ORÉAL EVENT

July 2024





This was a tremendous opportunity to have the crème de la crème of hackers with us, to share with all LV employees tips and tricks for what they should do in their personal and professional life to mitigate cyber risk, and share what Louis Vuitton does to protect the company's assets and information systems."

CHRISTOPHE PLOUSEAU

Chief Information Officer

LOUIS VUITTON



The hunters, joined by the Louis Vuitton and YesWeHack teams, gather in front of Louis Vuitton HQ to celebrate the event's successful conclusion

Other events featured Ferrero (Italy's first-ever live Bug Bounty) at RomHack in Rome; Groupe Caisse des Dépôts (CDC), a French public financial institution, at InCyber Forum in Lille; and Banco Galicia at Ekoparty, Buenos Aires.

All live Bug Bounty clients declared themselves impressed by the results. With the help of the hunters and YesWeHack's triage team, they were generally able to rapidly assess and remediate the vulnerabilities discovered (133 bugs at the most prolific event).

FINAL PODIUM OF LOUIS VUITTON EVENT

April 2024



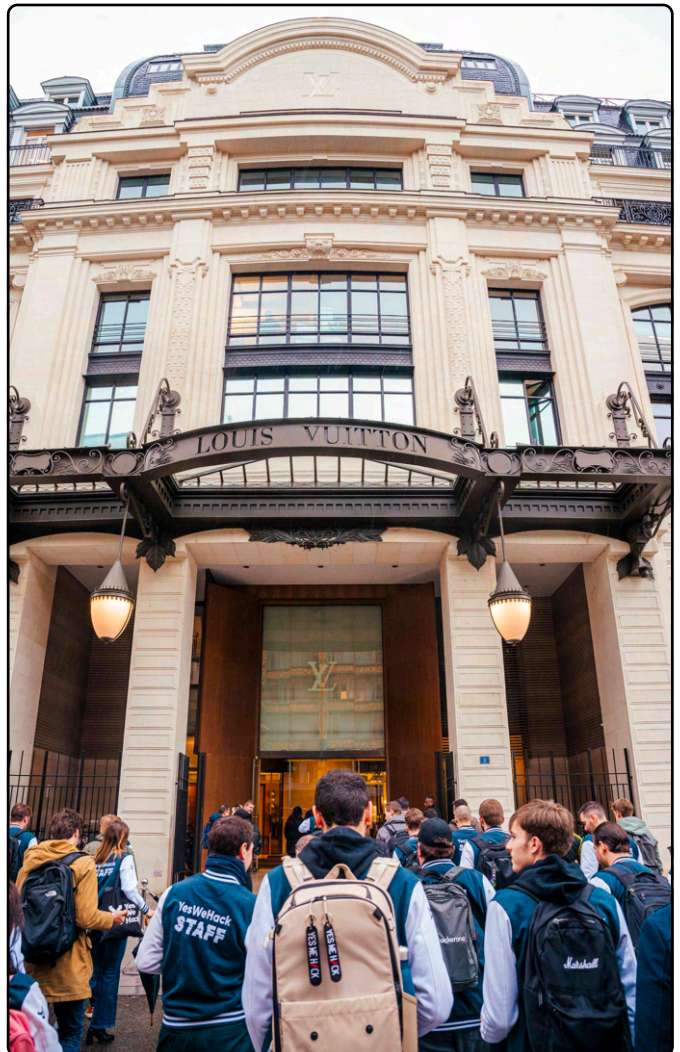
DJURADO



GODIEGO



HIPOTERMIA



**FINAL PODIUM OF FERRERO EVENT** September 2024

ELWETH  
COSADES  
ALI4S

**FINAL PODIUM OF BANCO GALICIA EVENT** November 2024

G4MB4  
SOYELMAGO  
LEMONOFTROY



"The atmosphere is really cool. it's nice to see other hunters, to discuss together, to exchange some hints... it's very cool."

ELWETH

#2 of the Live Bug Bounty featuring Ferrero

This opportunity was essential to explore new areas and methodologies for detecting vulnerabilities, push the limits of security testing, and strengthen our proactive approach to protecting digital assets and data. The goal is to learn, grow and continue to build a more secure digital environment."

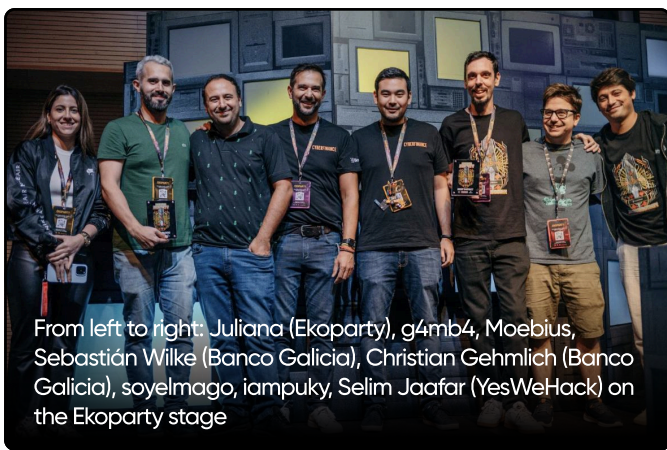
ANDREA LOMBARDINI

Group Cybersecurity Manager **FERRERO**

It's like an emotional rollercoaster: you're calm and then suddenly you have to triage vulnerabilities, understand them, discuss them with the hunters."

CHRISTIAN GEHMLICH

Offensive Cybersecurity Leader **Galicia**



"A live hacking event is always a good experience because we are able to meet the people behind their handle or nickname."

G4MB4

#2 of the Live Bug Bounty featuring Banco Galicia

# BUG BOUNTY AND THE CHALLENGE OF SECURING OPEN SOURCE

We can expect to see increasing adoption of crowdsourced security testing within the open source ecosystem given the proliferation of vulnerabilities across this ubiquitous, critically important software. In turn, we anticipate that growing numbers of hunters will acquire the specialist skills required for probing open source scopes.

The vast majority of applications (97%) contain open source components, according to GitHub, while legacy open source software continues to persist. The implications of inadequate vulnerability management were particularly laid bare by 'Log4Shell', which is widely considered to be one of, if not the, most damaging vulnerability of all time. The super-critical flaw in Log4j, an open-source Java logging tool built into applications with billions of users collectively, caused havoc when it surfaced in 2021 through an otherwise unremarkable software update.

A 2024 report from Sovereign Tech Fund (STF), which invests in open digital infrastructure to ensure a resilient, sustainable open source ecosystem, says bug bounties are effective at boosting the number and quality of vulnerability reports. In *'Bug Bounties and FOSS: Opportunities, Risks, and a Path Forward'*, Dr Ryan Ellis also writes that crowdsourcing security testing helps "projects retain expert talent and reduce community churn, and they can provide accountability mechanisms and tools that are otherwise lacking". Moreover, the report from STF, a YesWeHack customer, endorses how Bug Bounty platforms incentivise honest, professional conduct on the part of hunters through financial rewards, as well as a points-based system that rewards quality vulnerabilities, and clear, responsive communication with customers.

Bug Bounty is particularly useful as an extra layer of security for mature open-source projects, said the report.





Dr Ellis noted the mixed security performance of this huge, diverse ecosystem, with some libraries much better resourced and more attentively maintained than others. After all, the likes of Google, Microsoft and Red Hat help to fund some projects, while others are maintained unassisted by volunteers who juggle the task in conjunction with day jobs. The STF report therefore recommends that projects invest in remediation capabilities and, to prevent an overload of low quality reports, general maintenance before embarking on a Bug Bounty Program.

Whether they provide critical functions or are built into applications used by millions, open source targets on YesWeHack currently include some highly consequential libraries. As well as Log4j, STF has public programs for systemd, GNOME, ntpd-rs, OpenPGP.js, Sequoia PGP and CycloneDX Rust Cargo. (Given other STF active investments include the likes of Drupal, PHP and GNU libmicrohttpd, the organisation may well be a source of exciting new hunting opportunities in the not-too-distant future.)

Despite the resource constraints dogging some corners of the ecosystem, the open source rewards on offer on YesWeHack are among the most generous on our platform – reflecting the commitment to security of their custodians and the challenging nature of many of the targets. All seven STF programs are currently offering rewards up to €10,000 for critical vulnerabilities. We also have a trio of open source programs from Open-Xchange, with PowerDNS offering max rewards of €8,000 and Ox App Suite plus Dovecot offering up to €5,000.



**Our societies increasingly rely on open source software as critical infrastructure, and it takes a lot of effort to keep that infrastructure safe. Which is why STF is committed to fostering the community of security researchers looking to use their skills to secure the open source ecosystem in the public interest."**

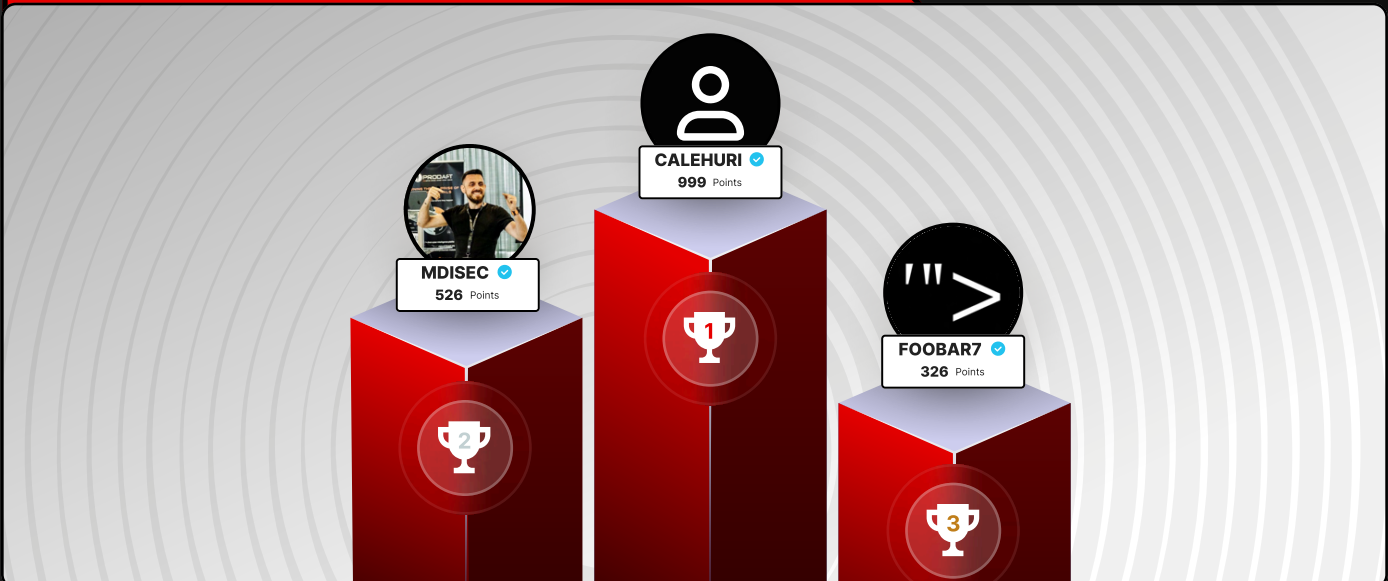


**TARA TARAKEYEE**

FOSS Technologist Sovereign Tech Fund

Not just motivated by money, we believe hunters also relish the chance to secure critical infrastructure that underpins a free and open internet – and to help others do the same. Consider for instance how 'Sigabrt', who stars on our open source leaderboard, contributed to community knowledge with a case study detailing a vulnerability he found on GNOME.

### ALL-TIME TOP 3 HUNTERS ON OPEN SOURCE SCOPES



# TOP 7 TAKEAWAYS FROM OUR BUG BOUNTY REPORT

As we enter our 10th year, YesWeHack is continuing to play our part in popularising Bug Bounty worldwide, including in territories with modest levels of crowdsourced security testing. Of course, in a world of accelerating change, we must also strive to more fully realise the intrinsic benefits of Bug Bounty by strengthening our people, processes and platform. In pursuit of this goal, it's impossible to ignore one technology in particular. It's also a transformational technology for ethical and malicious hackers alike. While AI is not explicitly mentioned elsewhere in this report, it doubtless played an increasing role in the emergence of new hacking techniques and the automation of vulnerability discovery, validation and remediation – and this trend will surely accelerate. We can expect LLM bugs to become more common, for instance.

YesWeHack's experiences during 2024 offer salutary lessons about not just the value of our own products but the nature of the Bug Bounty model in general too. In summarising the statistics amassed from our platform and anecdotal evidence provided by hunters and customers, the following seven trends stand out:

01

- » The rapid increase in the number of YesWeHack programs evidences **increasing Bug Bounty adoption worldwide** – and the visible segment (public programs) is just the tip of the iceberg (namely 10% of all our programs)

04

- » Bug Bounty is potentially lucrative given the size of top-end payouts and the prolific performance of many hunters – and an **excellent return on investment** for customers given results-based pricing and the size of more typical bounties

02

- » CISOs and other senior security professionals frequently cite the same **Bug Bounty benefits** as their release schedules accelerate: agility, scalability, continuous testing of unparalleled depth and breadth, an aid to compliance, and a facilitator of secure development practices

05

- » Yet **hunters are not just motivated by money** – their palpable enthusiasm is also born of a passion for hacking itself, the thrill of climbing the leaderboard, and the chance to collaborate and share advice with peers. It's not for nothing that we describe our hunters as a 'community'

03

- » As scopes are hardened, new products are launched and numbers of vulnerability reports of various severities fluctuate, it's clear how pivotal **customer success and triage teams** are to programs' alignment with customer goals and prompt remediation of bugs, especially the most critical (our low duplicate rate attests to our success in this latter area)

06

- » Customers and hunters alike extol the value of not just technical hacking expertise but **soft skills** too – in particular tenacity and a talent for communication and collaboration. Our points-based system rewards hunters who excel in both dimensions

07

- » **Live hacking events** are producing impressive results for some of the world's most illustrious brands – whose experiences may help persuade other organisations to follow suit

We're confident that these insights will continue to hold true as we progress through 2025 and beyond – alongside, no doubt, some trends that few of us had foreseen. Whether you're a hunter, CISO or other security professional, we hope to continue our exciting journey with your support. No doubt we'll see many of you at conferences and live hacking events throughout 2025.

**HAPPY NEW YEAR AND HACK THE PLANET!**