Immunefi

HACKER ECOSYSTEM SURVEY 2024

PREPARED BY IMMUNEFI

Hacker Ecosystem Survey 2024

PREPARED BY IMMUNEFI

The team at Immunefi, the leading onchain crowdsourced security platform which protects over $190 billion in user funds, publishes the results of the Hacker Ecosystem Survey 2024.

Home to the largest community of security talent in the blockchain space, Immunefi maps the web3 security landscape and shares the survey results received.

SURVEY RESULTS

- Most whitehats (46%) are 20-29 years old. Although male hackers (88%) still comprise the largest share within the industry, more women are joining the community.
- On average, whitehats have been working in cybersecurity for over 3 years, and have been interested in web3 security for over 2 years.
- Money is a crucial factor driving hackers' interest – 77% of respondents are primarily motivated by financial opportunities.
- 63% of whitehats consider hacking their primary job, while 37% do it in their free time, spending most of their day working in IT, Information Security, or Web3.
- When asked about plans to switch to Web3 security full-time, most whitehats (41%) are not sure yet, 38% are interested in switching, and 21% are currently not planning to.
- Most respondents follow industry resources across social media (74%) and dedicated web pages (62%) to stay updated on the security industry and foster their learning.

1. THE SURVEY AT A GLANCE

KEY TAKEAWAYS AND INSIGHTS

Hacker Ecosystem Survey 2024

KEY TAKEAWAYS

The results of the Hacker Ecosystem Survey 2024 reveal insights into the preferences of whitehats within the cybersecurity landscape.

BLOCKCHAIN

- When it comes to preferred blockchains, whitehats are primarily interested in Ethereum (**87%**) with Polygon (**59%**) in second place.

SECURITY

- When it comes to the growth of attack surfaces as compared to increased security measures in the industry, whitehats see a balance. While most of the whitehats (**74%**) see attack surfaces growing, the majority (**88%**) also see increased security measures from projects across the industry.
- According to the survey, improper input validation (**47%**) is the most common vulnerability whitehats encounter when reviewing code, followed by incorrect calculation (**35%**).

AI

- Most whitehats (**58%**) do not incorporate AI tools into their security practices, while **42%** already use them for practices such as smart contract auditing and other security assessments.
- Only **4%** of hackers are extremely confident that AI tools can easily identify vulnerabilities. The majority of whitehats (**55%**) believe that AI tools are most suitable for educational purposes.

BOUNTY PROGRAM

- Whitehats consider the size of bounty as the main factor (**61%**), followed by the scope of the project (58%). In contrast, the lack of trust in a project or program (**64%**) is the main factor in why whitehats dismiss a particular bounty program, followed by inefficient communication (**49%**).

Hacker Ecosystem Survey 2024

KEY INSIGHTS

When compared to the previous period, the ecosystem remains fairly stable, with slight adjustments across specific areas.

GENDER

While **male** whitehats still hold the largest share of the industry, at **88%**, the number of **female** whitehats **continues to increase**, reaching **7%**, compared to 4% in the previous period, representing a **75% increase.**

INTEREST

When it comes to factors driving hackers' interest, there has been a **10% increase** in the interest in **money opportunities** to 77%, compared to the previous period at 70%. Interest in **solving technical challenges** dropped from 77% in the previous period to 71%, representing a **6% decrease**. Overall, whitehats interests have slightly shifted towards financial incentives. Respondents usually look for bigger bounty payments while still being motivated by technical challenges that will allow them to sustainably and professionally grow within the sector.

OCCUPATION

Hacking as a primary job has increased **by 12%** from 56% in the previous period to 63% in the current one. Overall, more whitehats are joining the field and working in web3 cybersecurity full-time, as there has been a slight decrease in whitehats hacking in their free time to 37%, compared to 44% in the previous period, representing a 16% decrease.

BLOCKCHAIN

When it comes to **preferred blockchains**, interest in **Ethereum** dropped from 94% in the previous period to 87% in the current one, representing a **7.45% decrease**. Interest in **Solana** increased from 32% in the previous period to 42% in the current one, representing a **31.3% increase**. Overall, the whitehats show bigger interest in **Polygon** (59%), **Arbitrum** (47%), **Optimism** (45%), and **BNB Chain** (29%).

Hacker Ecosystem Survey 2024

KEY INSIGHTS

When compared to the previous period, the ecosystem remains fairly stable, with slight adjustments across specific areas

COMMON VULNERABILITIES

- When it comes to the most common vulnerabilities, the majority of whitehats mention **improper input validation**. This vulnerability increased from 9.1% in the previous period to **47%**, representing a significant rise. **Reentrancy**, being the most common one in the previous period, dropped significantly from 43.2% to **16%** in the current one. **Weak access control** remains in the top three common vulnerabilities, nearly doubling from 18.2% in the previous period to **32%** in the current one.

TIME WORKING IN THE FIELD

- Most whites have been working in crypto for over **3 years.**
- On average, they have been interested in web3 security for over **2 years.**

BOUNTY PROGRAMS

- When it comes to **choosing a bounty program** to hunt on, whitehats consider different factors. **Bounty size** remains the main factor, with **61%** in the current period and 66.37% in the previous one. **Trust in the project** has become less important, dropping from 54.87% in the previous period to 44% in the current one. Instead, whitehats pay more attention to the **scope of the program**, which increased by 11%, from 52.21% in the previous period to 58% in the current one.
- In contrast, **lack of trust** in a project remains the main reason why whitehats **dismiss a particular bounty program**, with 62.8% in the previous period and **64% i**n the current one. **Inefficient communication** also remains the second main factor, with **49%** in both periods.

Hacker Ecosystem Survey 2024

CHALLENGES

When asked about the biggest challenges whitehats have experienced in Web3 security, most respondents highlighted:

- **Learning curve:** it remains challenging for whitehats to navigate the complexities of the Web3 security ecosystem, regardless of their previous background.
- **Crafting vulnerability reports:** whitehats experienced difficulty in preparing and submitting vulnerability reports that effectively communicate identified bugs to project teams.
- **Lack of educational materials:** a common challenge is the limited educational resources specifically tailored to Web3 security and native languages.
- **Difficult interactions with projects:** engaging with project teams can be challenging for some of the whitehats, particularly when projects avoid paying bounties or offer payouts in their own tokens.
- **Code reviewing:** whitehats still find code reviewing difficult due to varying levels of code quality across projects.

POSSIBILITIES

When asked about what makes Web3 exciting for whitehats, most respondents highlighted:

- **Monetary incentives:** various projects and large bounty payouts provide a chance to achieve a high and steady income.
- **Technical challenges:** solving technical challenges remains one of the main drivers of interest.
- **New career possibilities:** whitehats consider Web3 security a high-paying industry with greater career opportunities.
- **The early stage of industry development**: most whitehats are excited about the concept of decentralization and rapid development of the ecosystem.

77% of security researchers

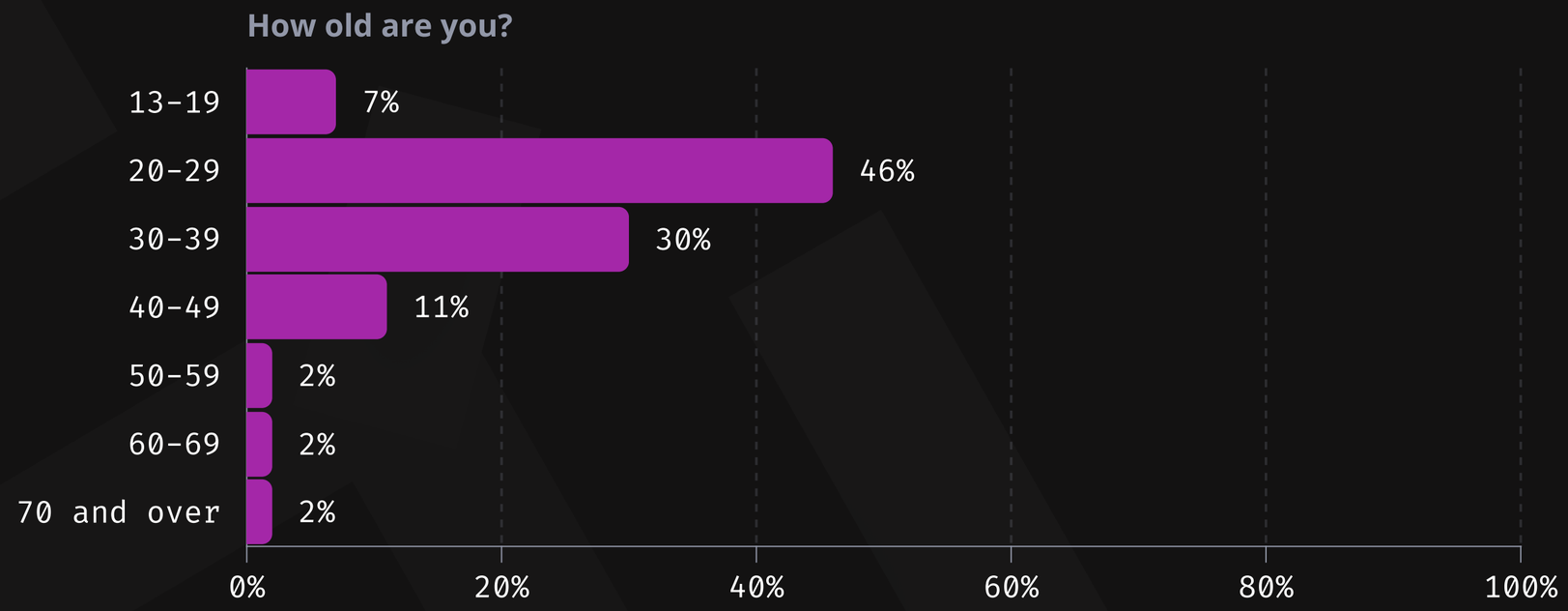
started in blocksec bounty hunting because of the **large bug bounties**

2. DEMOGRAPHICS AND LIFESTYLE

Demographics and Lifestyle

DEMOGRAPHICS

- Most whitehats (46%) are 20-29 years old. 30% of the respondents are between 30 and 39 years old, 11% are between 40 and 49 years old, 7% are between 13 and 19 years old, and 2% are between 50 and 59 years old.
- Although more women are joining the hacker community, male whitehats (88%) still comprise the largest share within the industry.



Demographics and Lifestyle

The Hacker Ecosystem Survey also observes the average time spent in the cybersecurity field and the specific interest in web3 security. This reveals the depth of experience and passion driving the whitehats. Most whites have been working in crypto for over **3 years.**
On average, they have been interested in web3 security for over **2 years.**

YEARS IN THE FIELD

- The majority (61%) of whitehats have been engaged in the industry for 1-3 years, reflecting the trend of more individuals entering the cybersecurity sector in recent years. This reflects the surge in interest and demand for cybersecurity professionals.
- 11.3% of whitehats have accumulated more than 10 years of experience in the field.
- Only 9.4% have entered the industry within the past year.

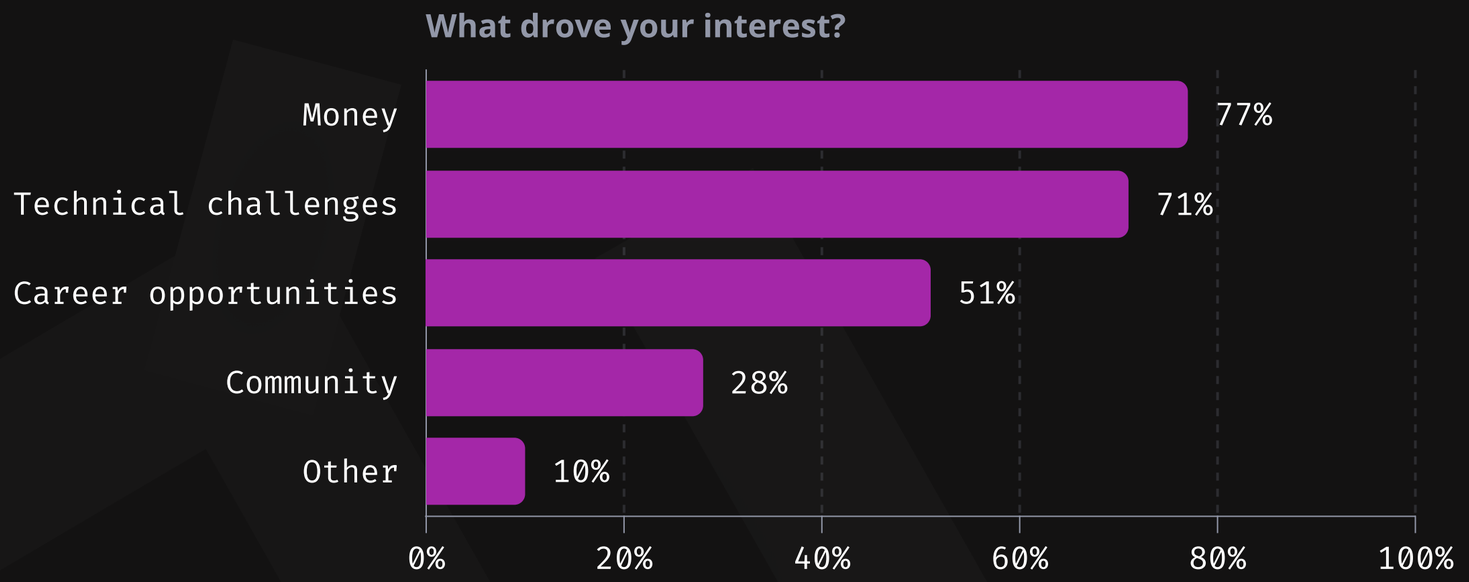
INTEREST IN WEB3

- The majority of whitehats (68%) have been interested for 1-2 years, which again confirms the trend of more people joining in recent years.
- 15% of whitehats have been interested for 3-5 years.
- 10% of whitehats have been interested in the field for more than 5 years.
- 5% have been interested for less than a year.

Demographics and Lifestyle

INTERESTS

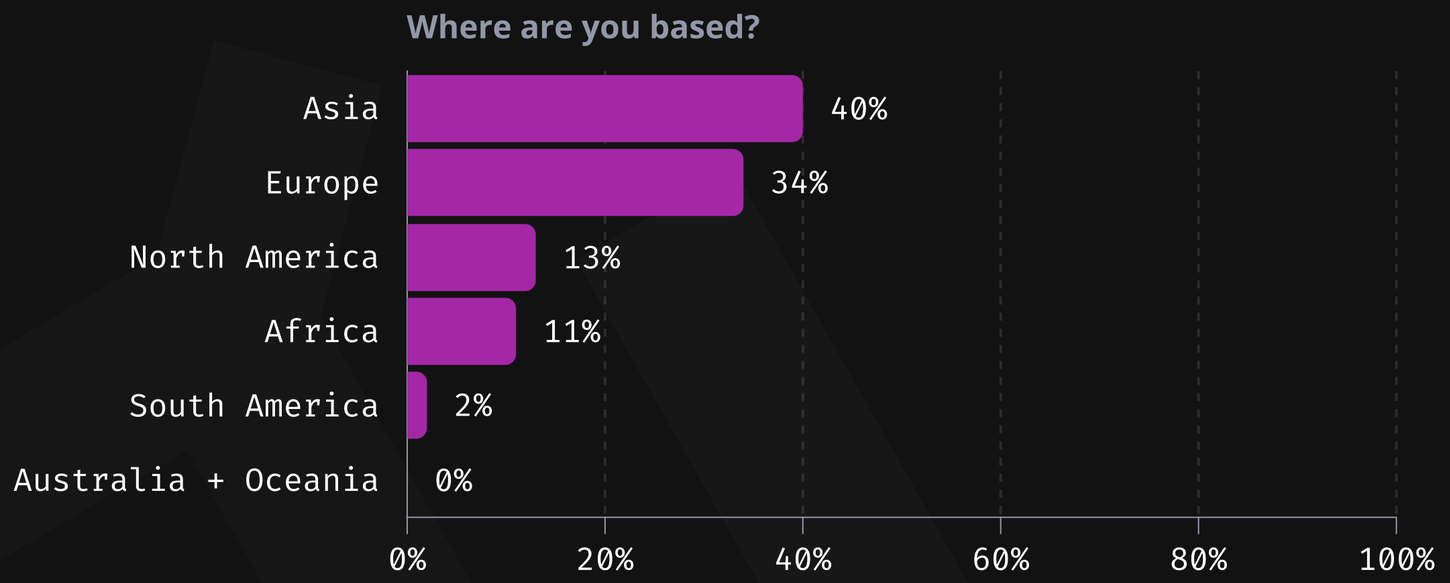
- Money is a crucial factor driving hacker interest—most respondents (77%) are primarily motivated by financial opportunities in Web3 security.
- The second significant driver of interest for whitehats is technical challenges (71%), followed by career opportunities (51%) and community (28%). Other motivating factors include decentralization and the recent increase in crimes and fraud. Furthermore, whitehats highlight the possibility of reporting bugs and receiving bounties anonymously without any kind of KYC.



Demographics and Lifestyle

GEOGRAPHY

- When considering geography, the majority of whitehats who participated in the survey (40%) are based in Asia, followed by Europe (34%), North America (13%), Africa (11%), and South America (2%).



63% of security researchers

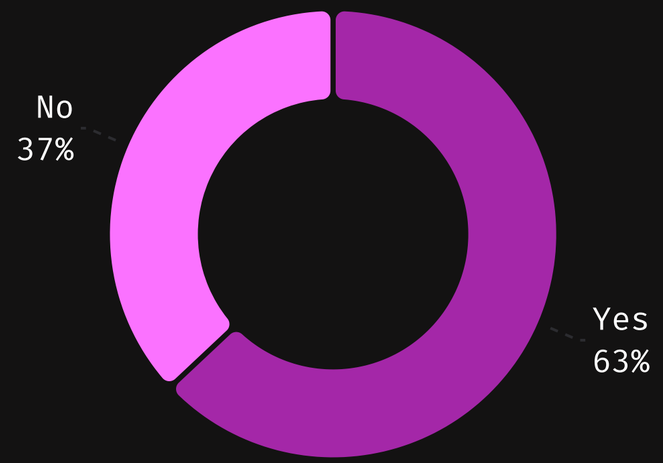
consider **hacking their main job**

Demographics and Lifestyle

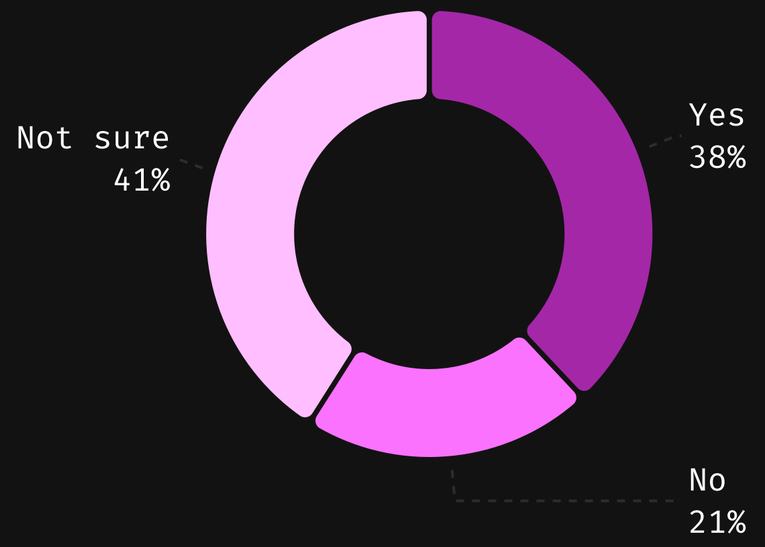
HACKING AS A JOB

- Most whitehats (63%) consider hacking their primary job, while 37% do it in their free time, spending most of their day working in the fields of IT, Security, and Web3.
- When asked about plans to switch to Web3 security full-time, most whitehats (41%) are not sure yet, 38% are interested in switching, and 21% are not planning to.

Do you consider hacking as your main job?



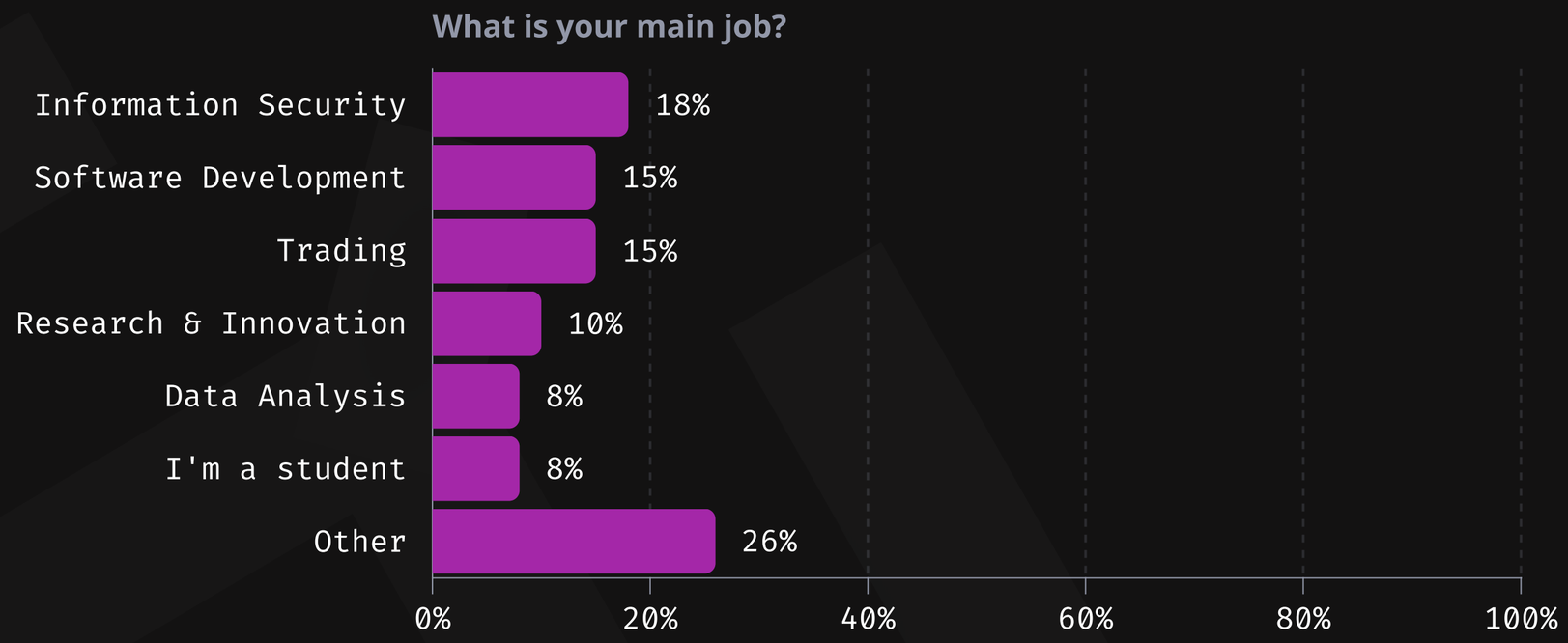
If hacking is not your main job yet, are you planning to switch to Web3 security full-time?



Demographics and Lifestyle

HACKING AS A JOB

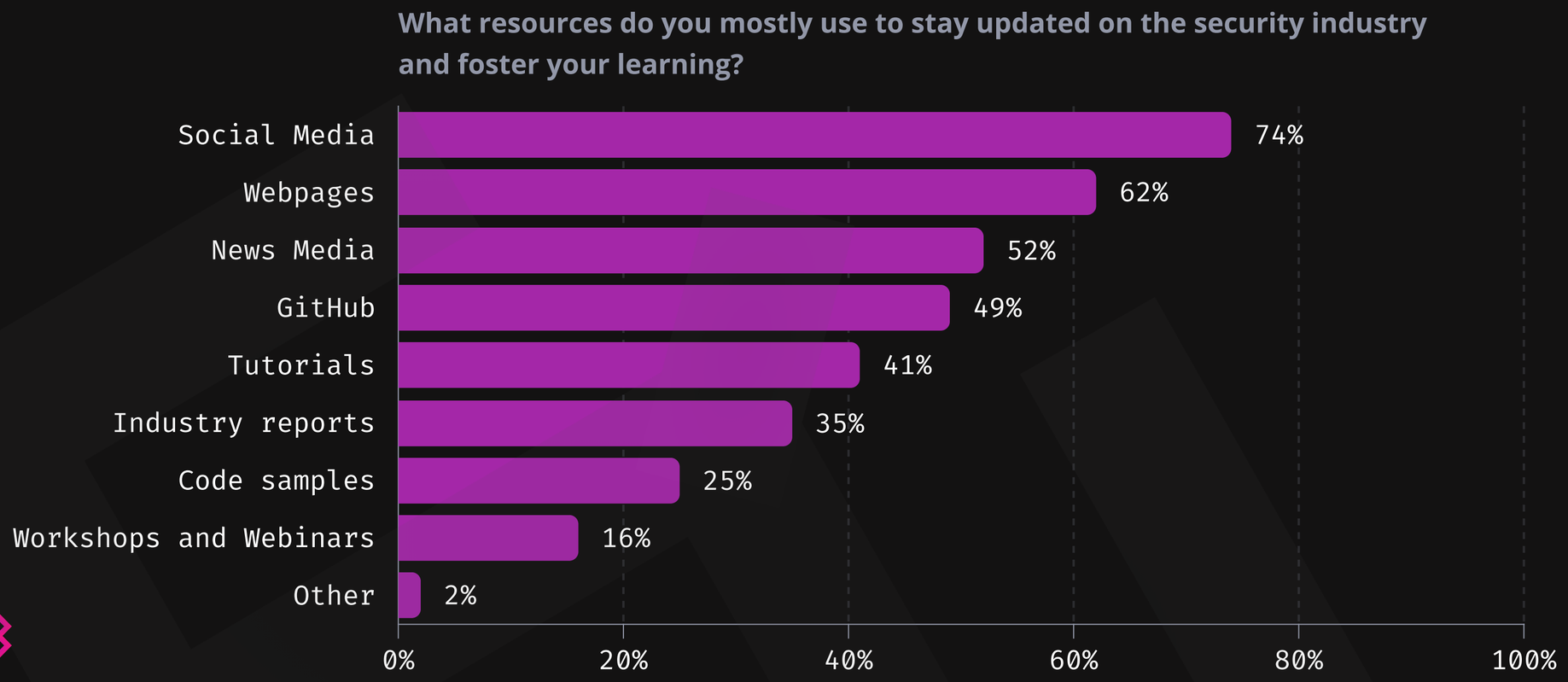
- When it comes to the main occupation for whitehats who don't consider hacking as their main job, most of them (18%) work in Information Security, followed by Software Development (15%), Trading (15%), Research and Innovation (10%), and Data Analysis (8%).
- 8% of hackers are still studying full-time.
- Other occupations mentioned by respondents include Helpdesk Support, Engineering, Testing, and Marketing.



Demographics and Lifestyle

RESOURCES

- Most whitehats follow industry resources across social media (74%) and dedicated webpages (62%), followed by news media (52%), GitHub (49%), tutorials (41%), and industry reports (35%), including bugfix reviews and write-ups.
- Respondents also highlighted code samples, workshops, and webinars as sources to stay updated on the security industry.

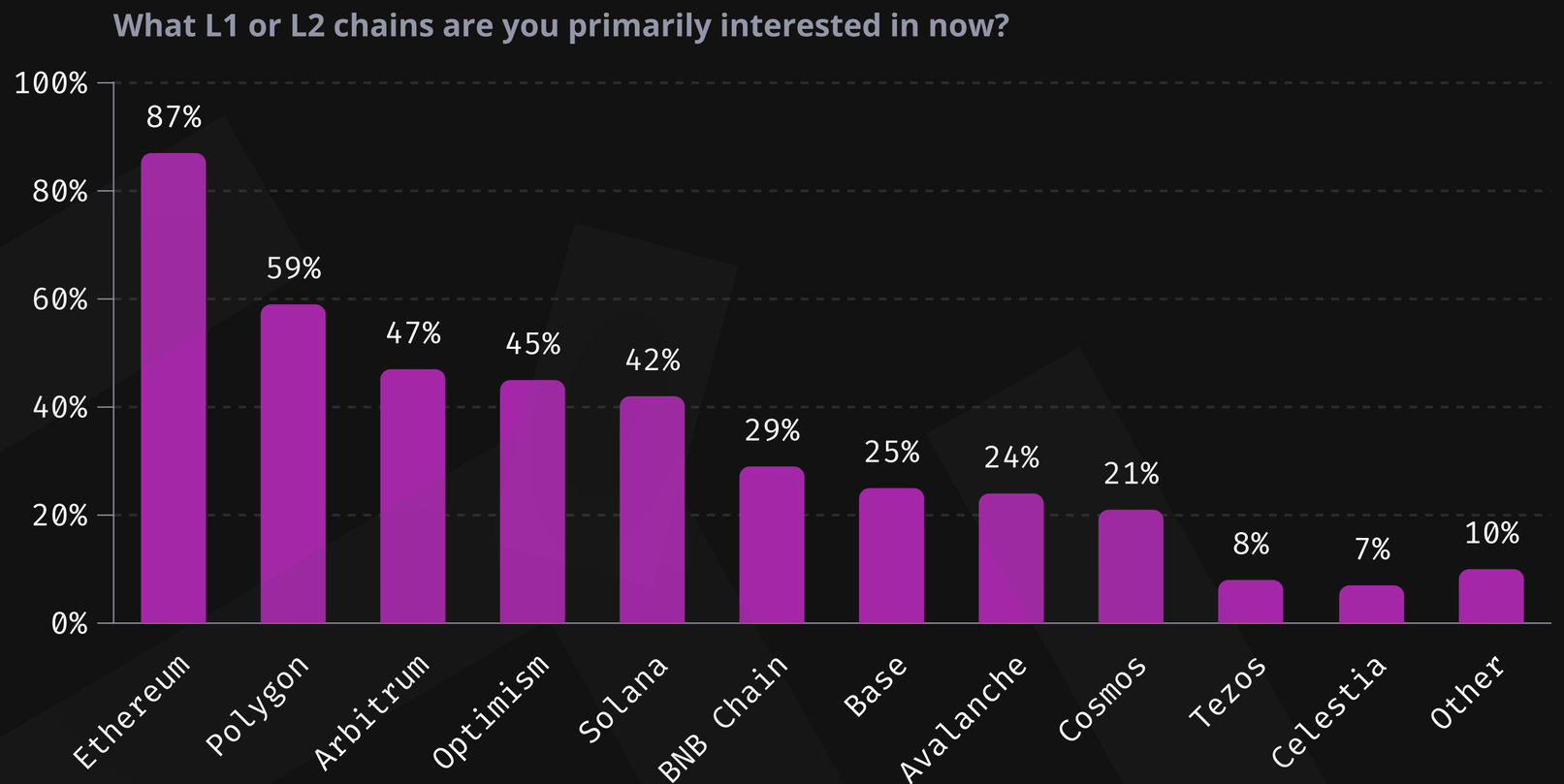


3. TECHNOLOGY

Technology

BLOCKCHAINS

- When it comes to preferred blockchains, whitehats are primarily interested in Ethereum (87%) with Polygon (59%) in second place.
- Next comes Arbitrum (47%), Optimism (45%), Solana (42%), and BNB Chain (29%).
- Among others, respondents also named Polkadot, NEAR, Polkadot, Starknet, and ZK chains.

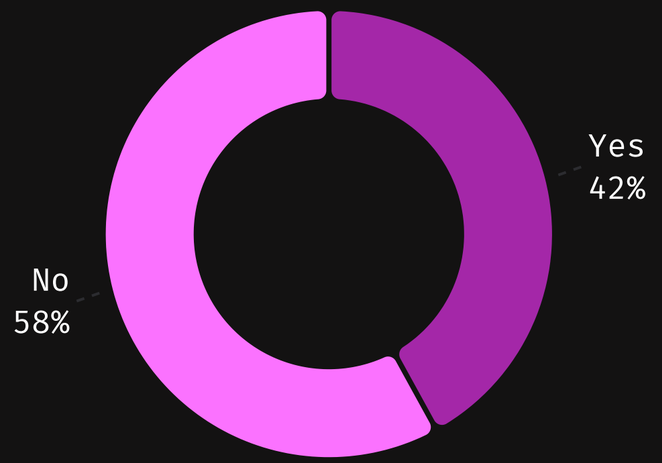


Technology

ARTIFICIAL INTELLIGENCE

- Most whitehats (58%) do not incorporate AI tools into their security practices, while 42% report that they already use them for security practices such as smart contract auditing, and other security assessments.
- Among the other AI tools used for security research, respondents mentioned ChatGPT, Gemini, Olympia Chat, CensysGPT, Codeium, Blackbox AI, and Claude.

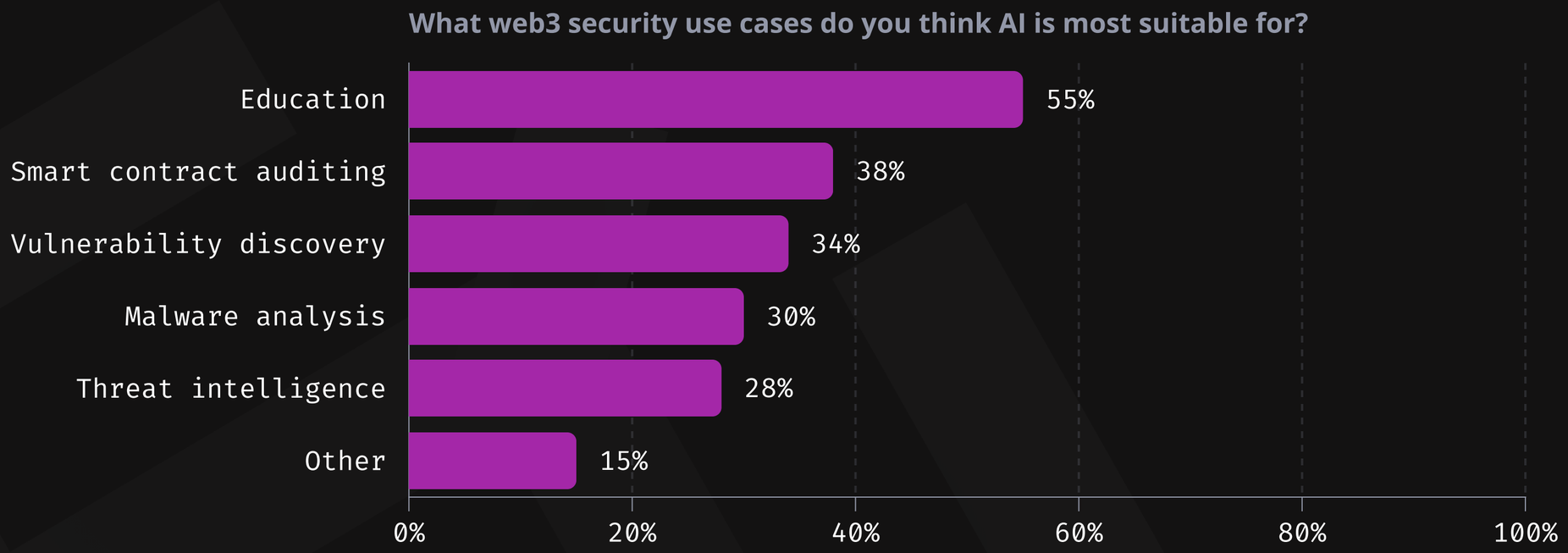
Do you use Artificial Intelligence (e.g. Github Copilot, etc.) for Web3 security practices such as smart contract auditing and other security assessments?



Technology

AI AND WEB3 SECURITY

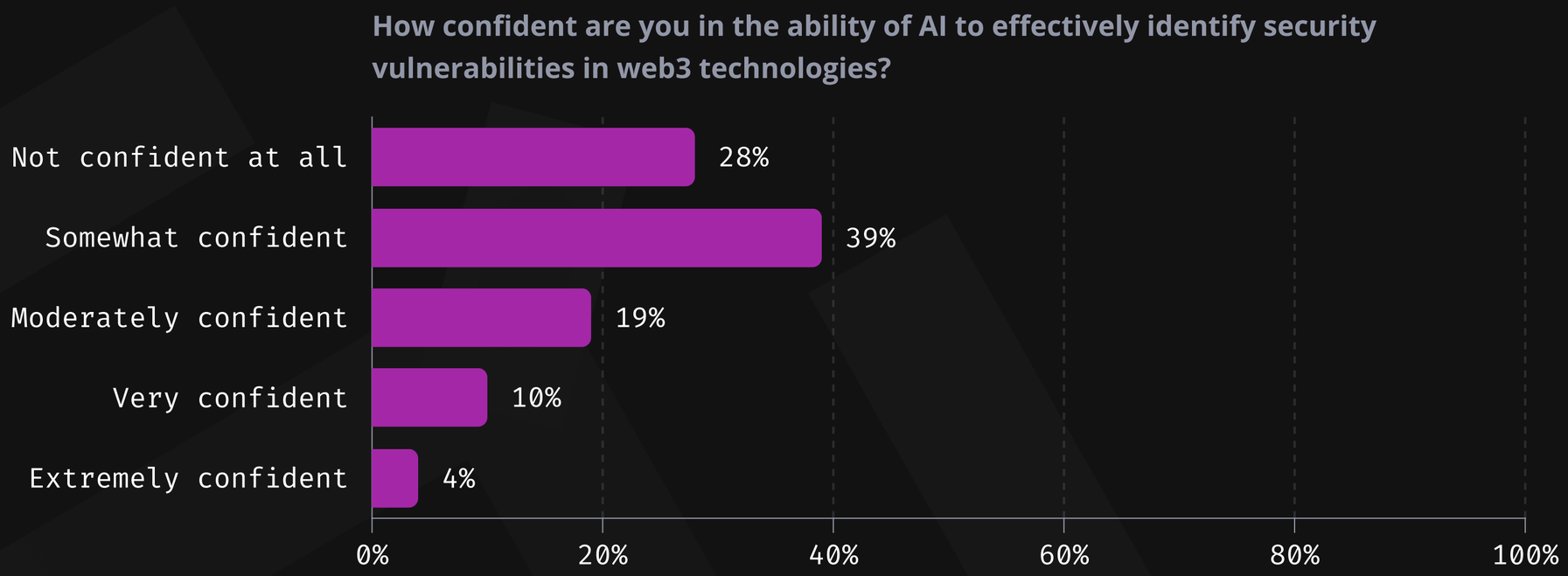
- The majority of whitehats (55%) believe that AI tools are most suitable for educational purposes, followed by smart contract auditing (38%), vulnerability discovery (34%), and malware analysis (30%).
- Among other use cases, hackers mention writing a Proof of Concept, pattern recognition, assisting in development, code summaries, and code evaluation.



Technology

LEVELS OF CONFIDENCE

- When it comes to whitehat confidence in the ability of AI to effectively identify security vulnerabilities, most respondents (39%) are somewhat confident, while 28% are not confident at all.
- Only 4% of whitehats who participated in the survey are extremely confident that AI tools can easily identify vulnerabilities.

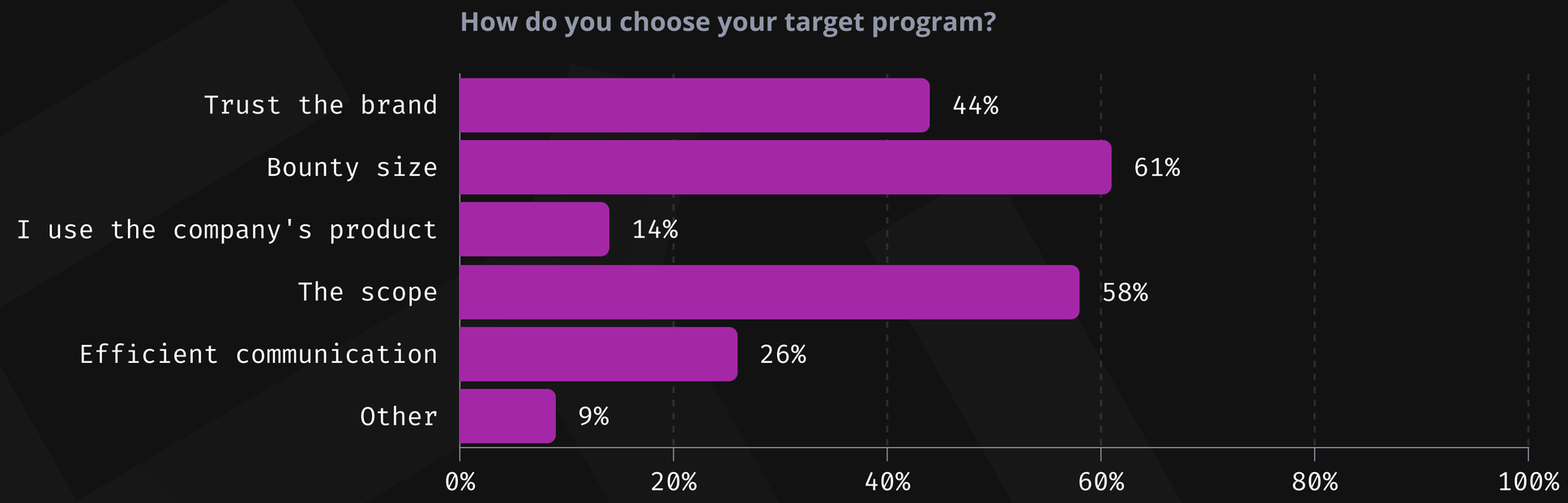


3. SECURITY

Security

BOUNTY PROGRAMS

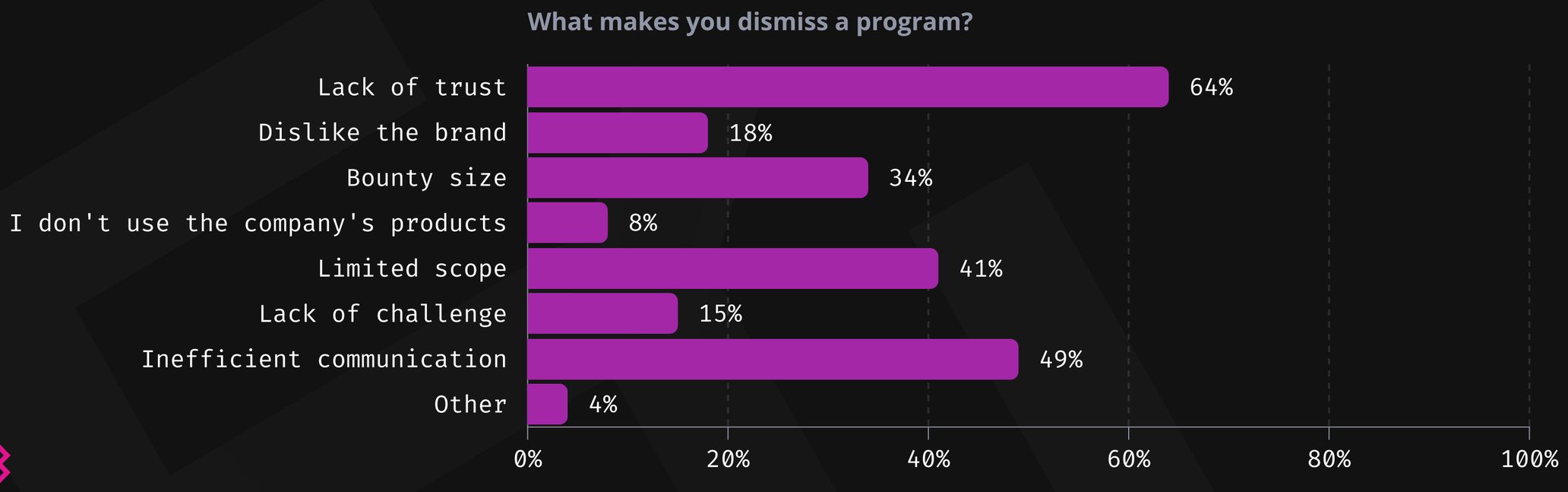
- When it comes to choosing a bounty program to hunt on, whitehats consider various factors. The bounty size is the main factor of choice (61%), followed by the scope of the project (58%). Other factors include trust in the brand (44%), efficient communication from the project side (26%), and, lastly, using the company's products (14%).
- Additional factors that respondents mentioned sparingly include the blockchain platform and programming language, code quality, technical interest, likelihood of bugs, and how long ago the project was listed.



Security

BOUNTY PROGRAMS

- In contrast, lack of trust in a project or program (64%) is the main factor in why whitehats dismiss a particular bounty program, followed by inefficient communication (49%). The remaining factors include limited scope (41%), bounty size (34%), dislike for the brand (18%), and lastly, the lack of challenge (15%).
- Other factors sparsely mentioned by respondents include the type of chain and payout in the company's own tokens.



88% of security researchers

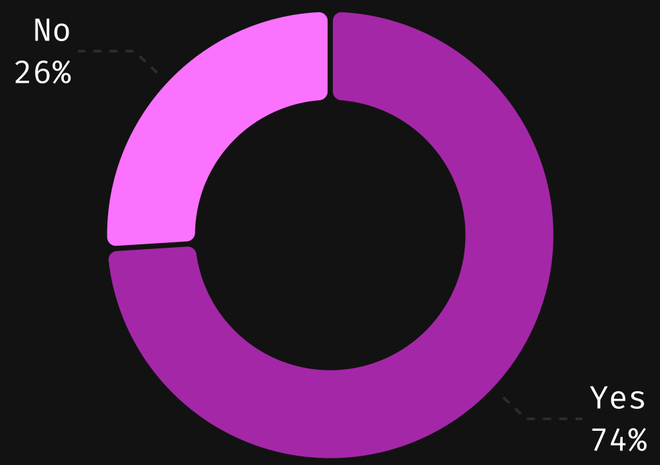
see **increased security measures** by projects across the industry

Security

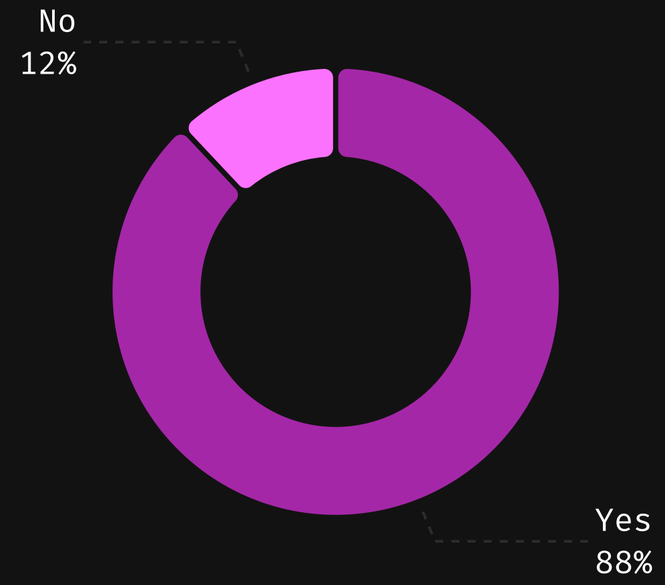
ATTACK SURFACES AND SECURITY MEASURES

- When it comes to the growth of attack surfaces in comparison to increased security measures in the industry, whitehats seem to see a balance. While most of the whitehats (74%) see attack surfaces growing, the majority (88%) also see increased security measures from projects across the industry — compared to 26% of respondents who don’t see attack surfaces growing, and 12% who don’t see particular increased security measures among projects.

Do you see attack surfaces growing?



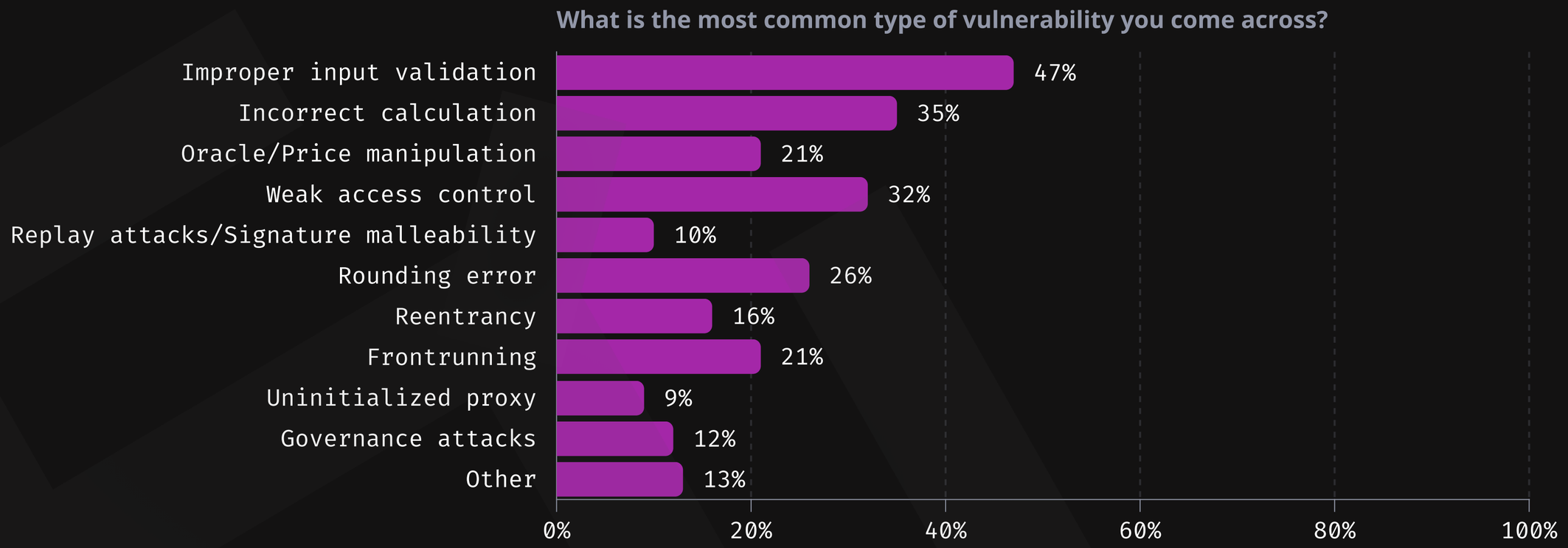
Do you see increased security measures by projects across the industry?



Security

VULNERABILITIES AND ATTACK VECTORS

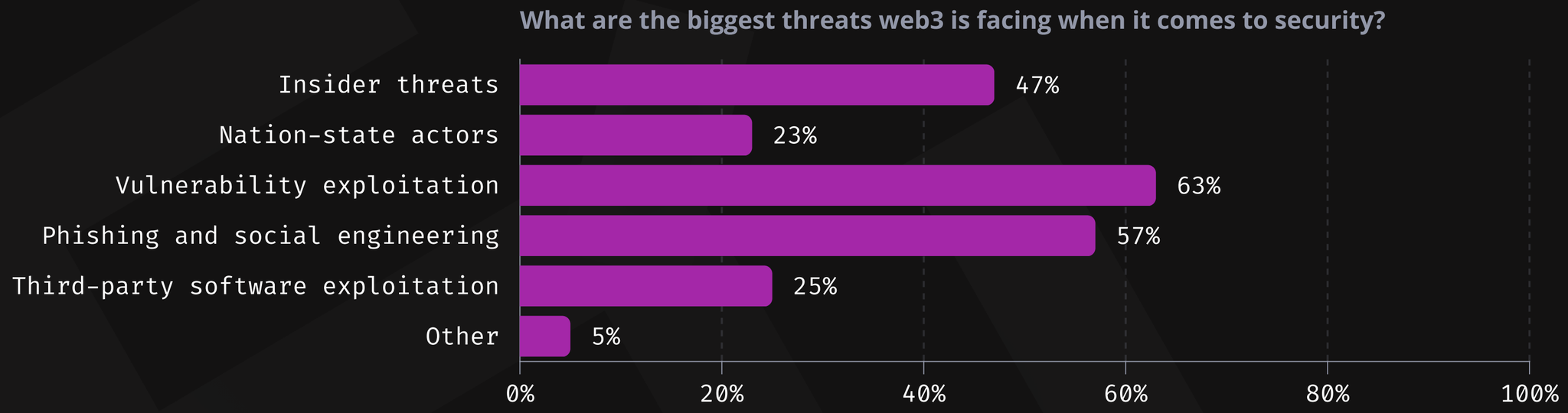
- Most whitehats mention improper input validation (47%) as the most common vulnerability they encounter when reviewing code, followed by incorrect calculation (35%).
- Other vulnerabilities listed include weak access control (32%), rounding errors (26%), Oracle/Price manipulation (21%), and frontrunning (21%).
- The least common vulnerabilities are reentrancy (16%), governance attacks (12%), replay attacks (10%), and uninitialized proxy (9%).
- Respondents also mentioned web application vulnerabilities among other common types.



Security

KEY THREATS

- The biggest threats that whitehats see across Web3 are vulnerability exploitation (63%), phishing and social engineering (57%), and insider threats (47%). They are followed by third-party software exploitation (25%) and nation-state actors (23%).
- Rug pulls and organized crime were mentioned among other threats across the ecosystem's security.

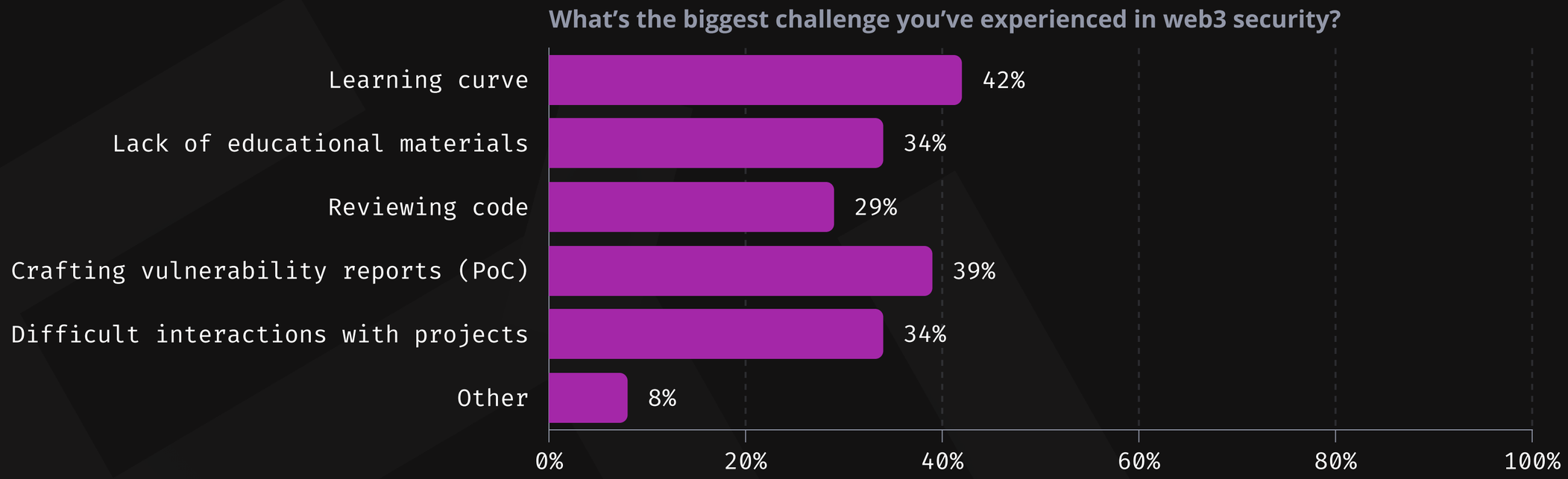


4. CHALLENGES AND POSSIBILITIES

Web3: Challenges and Possibilities

CHALLENGES

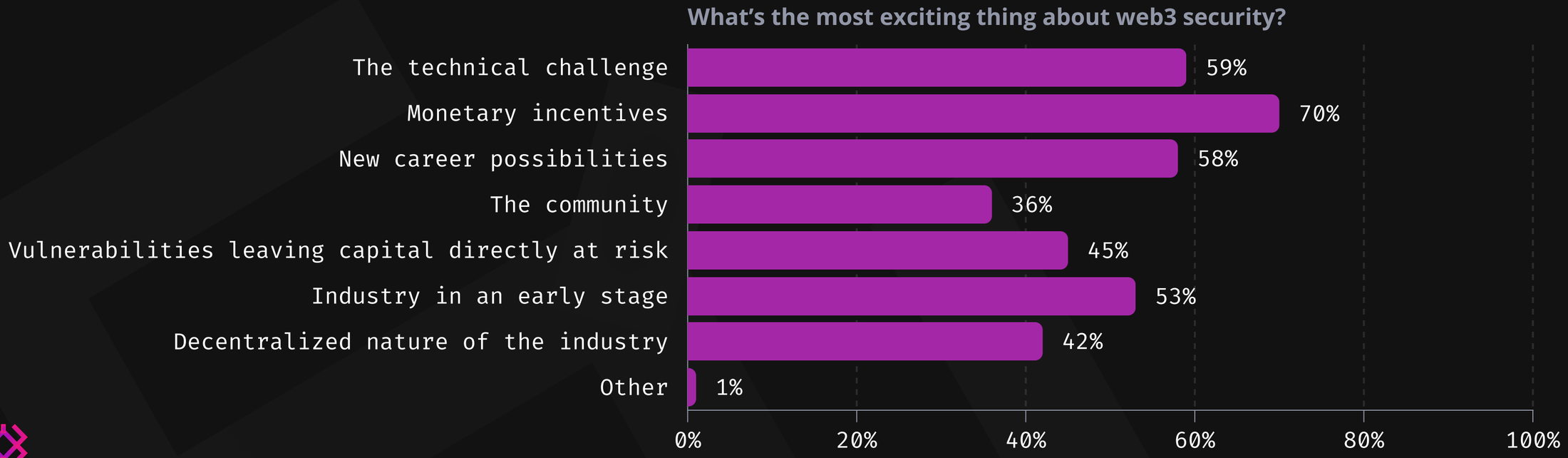
- When asked about the biggest challenges whitehats have experienced in Web3 security, most respondents highlighted the learning curve (42%), followed by crafting vulnerability reports (39%), lack of educational materials (34%), difficult interactions with projects (34%), and code reviewing (29%).



Web3: Challenges and Possibilities

POSSIBILITIES

- When asked about what makes Web3 exciting for whitehats, most respondents highlighted monetary incentives (70%), technical challenges (59%), new career possibilities (58%), and the early stage of industry development (53%).
- These possibilities are followed by vulnerabilities leaving capital directly at risk (45%), the decentralized nature of the industry (42%), and the community (36%).



“

We're observing that security researchers are increasingly drawn to financial and career opportunities while seeking technical challenges. With over half of security researchers already hacking as their main job, we must provide them with the right environment to thrive and also welcome the next generation. They will continue to be the backbone of the ecosystem, as they protect crypto from threats and vulnerabilities.

Mitchell Amador
Founder and CEO at Immunefi

Immunefi

Immunefi is the leading onchain crowdsourced security platform which protects over $190 billion in user funds. Immunefi features a massive community of whitehat hackers who review projects' blockchain and smart contract code, find and responsibly disclose vulnerabilities, and get paid for making crypto safer. With Immunefi, whitehat hackers are rewarded based on the severity of the vulnerability that they discover, creating incentives for as many experts as possible to examine project code for vulnerabilities.

Immunefi has pioneered the scaling web3 bug bounties standard, meaning that rewards should be priced accordingly with the severity of an exploit and the volume of funds at risk, which resulted in the company building the largest community of security talent in the web3 space.

TOTAL BOUNTIES PAID

Immunefi has paid out over **$100 million** in total bounties, while saving over **$25 billion** in user funds.

TOTAL BOUNTIES AVAILABLE

Immunefi offers over **$183 million** in available bounty rewards.

SUPPORTED PROJECTS

Trusted by established, multi-billion dollar projects like Chainlink, Wormhole, MakerDAO, TheGraph, Synthetix, and more, Immunefi now supports more than 300 projects across multiple crypto sectors.

LARGEST BUG BOUNTY PAYMENTS IN THE HISTORY OF SOFTWARE

Immunefi has facilitated the largest bug bounty payments in the history of software:

- **$10 million** for a vulnerability discovered in Wormhole, a generic cross-chain messaging protocol.
- **$6 million** for a vulnerability discovered in Aurora, a bridge, and a scaling solution for Ethereum.
- **$2.2 million** for a vulnerability discovered in Polygon, a decentralized Ethereum scaling platform that enables developers to build scalable, user-friendly dApps.

More:

- If you're a developer thinking about a bug-hunting career in web3, we got you. Check out our **Web3 Security Library**, and start taking home some of the over $183M in rewards available on Immunefi — leading onchain crowdsourced security platform.

For more information, please visit **https://immunefi.com/**