Immunefi

THE HACKER ECOSYSTEM SURVEY 2023

THE HACKER ECOSYSTEM SURVEY 2023

Prepared by Immunefi

The team at Immunefi, the leading bug bounty and security services platform for web3 which protects over $60 billion in user funds, releases the results of the Hacker Ecosystem Survey 2023.

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

Survey Results

Key Takeways

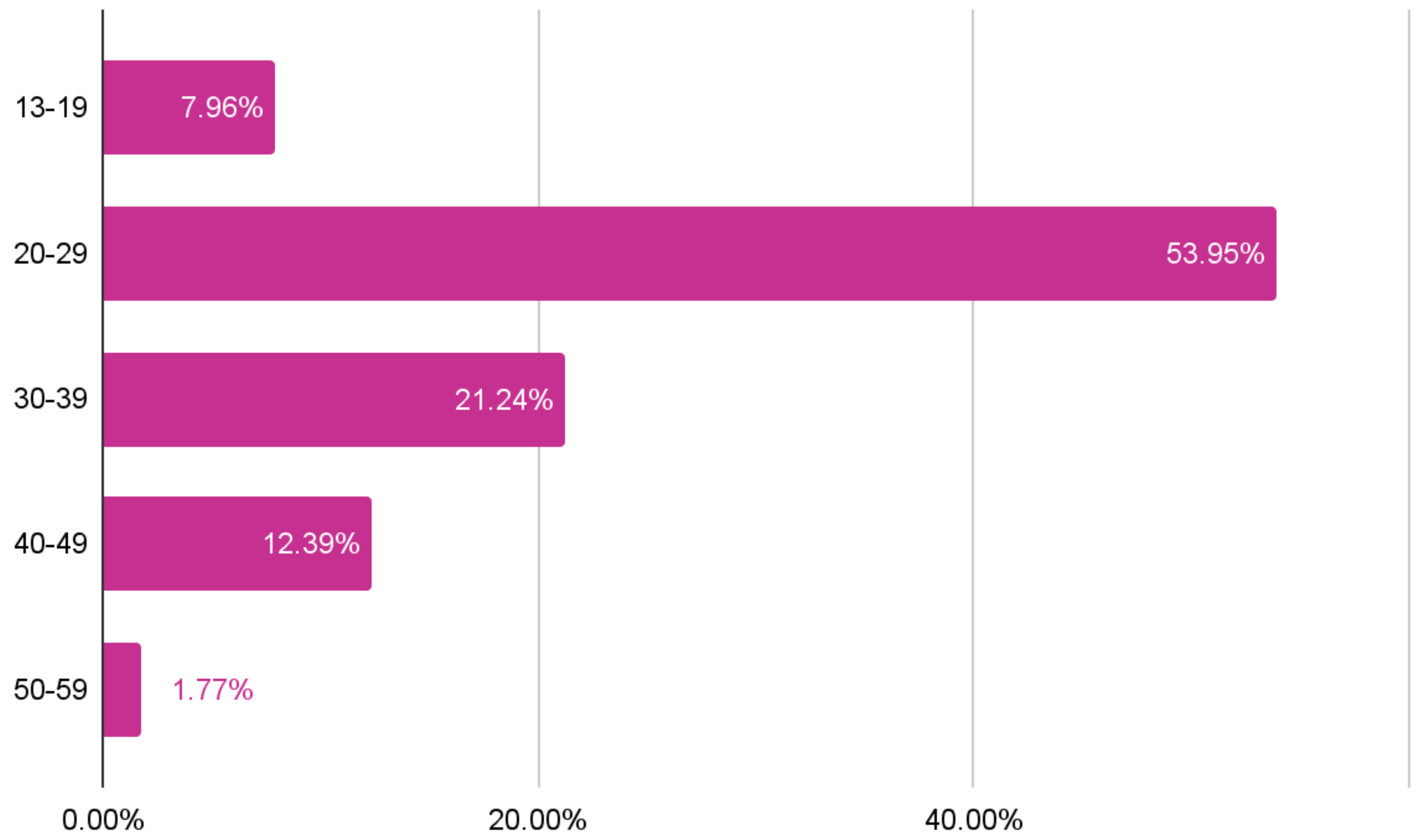
- Money does not act as a crucial factor in driving whitehat hackers' interest — most of the respondents (**77%**) are interested mainly in solving technical challenges, followed by money (**69%**), then career opportunities (**62%**), and community (**38%**). Other motivating factors cited are the opportunity to learn the future of the internet and decentralization technologies, and also to be ahead of the curve.
- Most whitehats (**55.8%**) consider hacking their primary job, while 44.2% do it in their free time, spending most of their day as software developers within the web3 or security industries.
- Most whitehats have been working in cybersecurity for almost **4 years**.
- On average, they have been interested in web3 security for almost **2 years**.
- The top three whitehats in the survey by number of bugs submitted have submitted **100+**, **86**, and **45** bug reports each.

Immunefi

Demographics and Lifestyle

Demographics

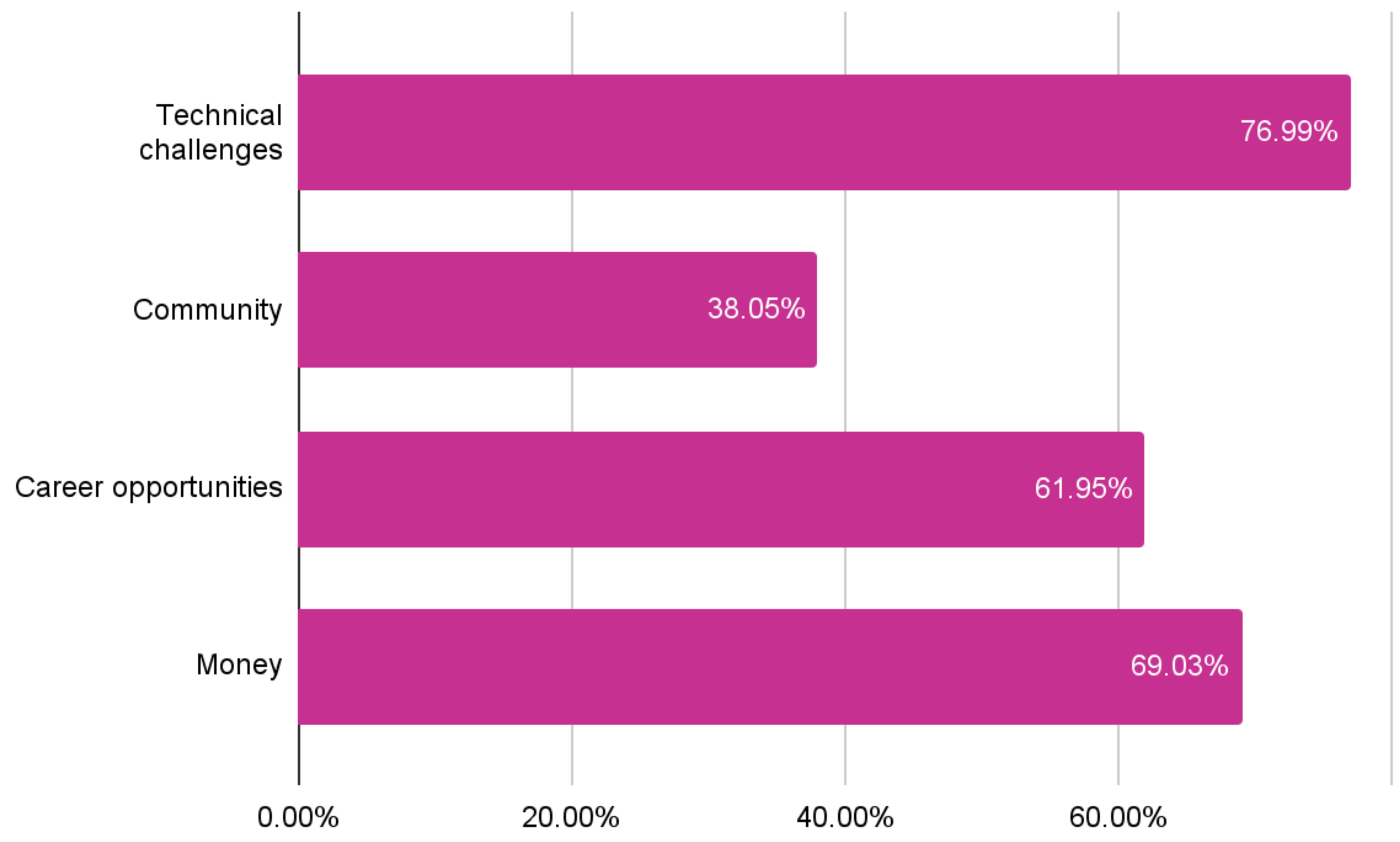
- Most whitehats (**54%**) are 20-29 years old. **21.2%** of the respondents are between 30 and 39 years old, **12.4%** are between 40 and 49 years old, **8%** are between 13 and 19 years old, and lastly, **1.8%** are between 50 and 59 years old.
- Although more women are joining the hacker community, male whitehats (**95.5%**) still comprise the largest share within the industry.



Demographics and Lifestyle

Years in the field and Interests

- Most whitehats have been working in crypto for almost 4 years. On average, they have been interested in web3 security for almost 2 years.
- Most whitehats (**55.8%**) consider hacking their primary job, while **44.2%** do it in their free time, spending most of their day as software developers within the web3 or security industries. When asked about plans to switch to web3 security full-time, most whitehats (**67.2%**) are interested in switching, **21.2%** are not sure yet, and **11.5%** are not planning to.
- Money does not act as a crucial factor in driving hackers' interest — most of the respondents (**77%**) are interested mainly in solving technical challenges, followed by money (**69%**), then career opportunities (**62%**), and community (**38%**). Among other motivating factors, they also name the opportunity to learn the future of the internet and decentralization technologies, and also to be ahead of the curve.

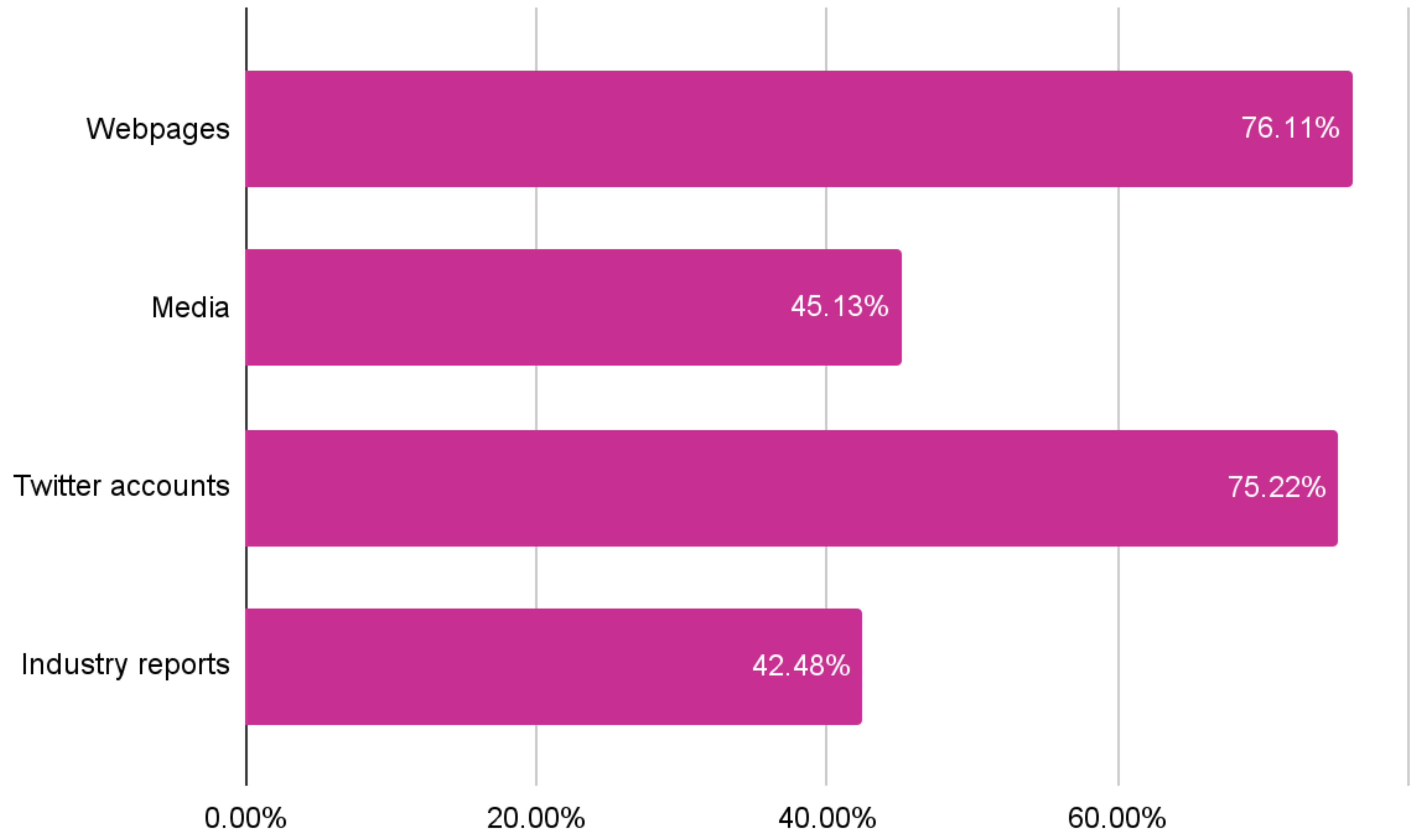


Immunefi

Demographics and Lifestyle

Resources

Most of the whitehats follow industry resources on dedicated webpages (**76.1%**) and Twitter accounts (**75.2%**), followed by media (**45.1%**) and industry (**42.5%**) reports, including bugfix reviews and write-ups. Respondents also highlighted YouTube, Discord, newsletters, and GitHub.

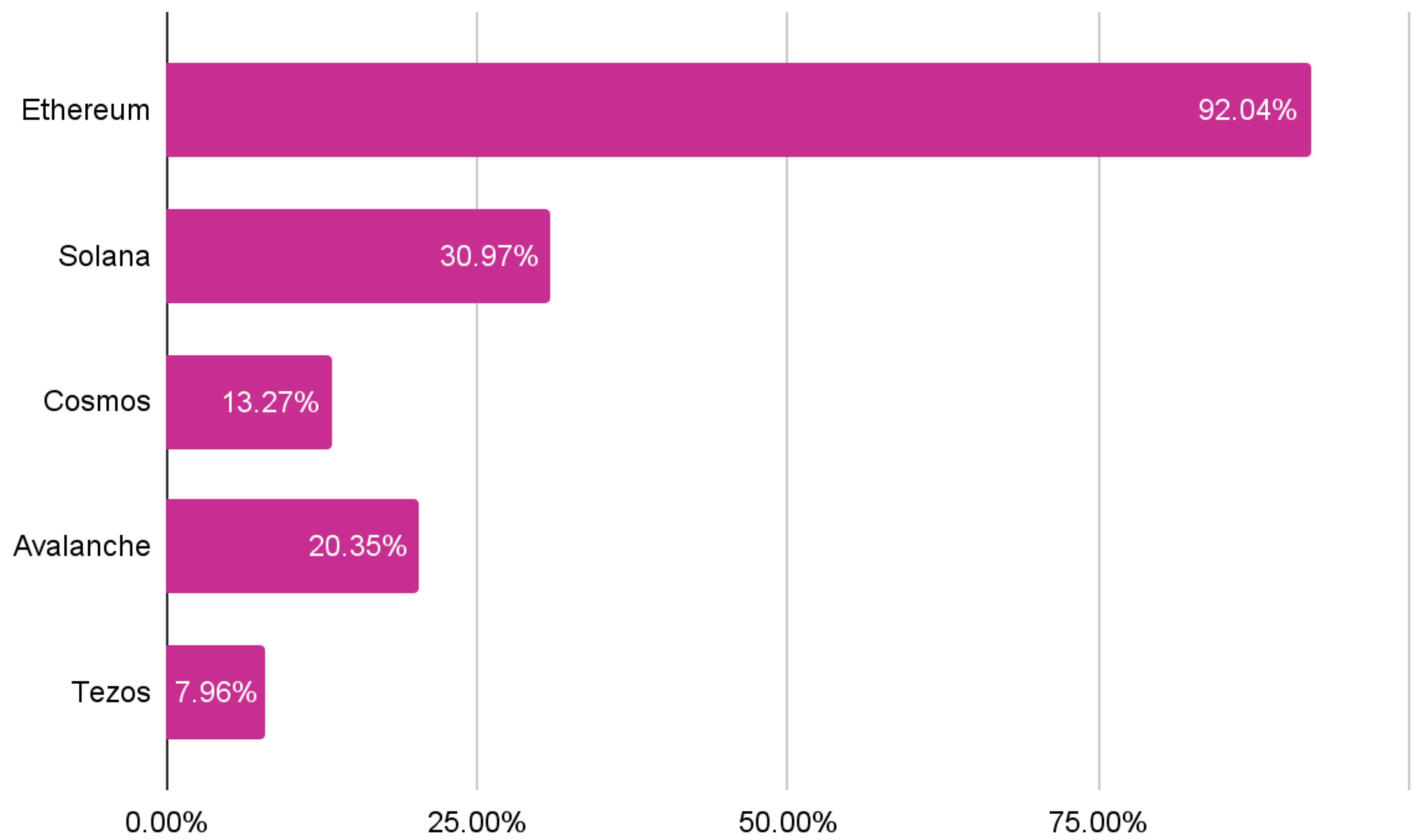


Tech

Blockchains

When it comes to preferred blockchains, whitehats are primarily interested in Ethereum (**92%**) with Solana (**31%**) in second place. Next comes Avalanche (**20.4%**), Cosmos (**13.3%**), and Tezos (**8%**).

Among others, respondents also name Polygon, Arbitrum, Optimism, NEAR, Polkadot, BSC, Fantom, and zkSync.



Immunefi

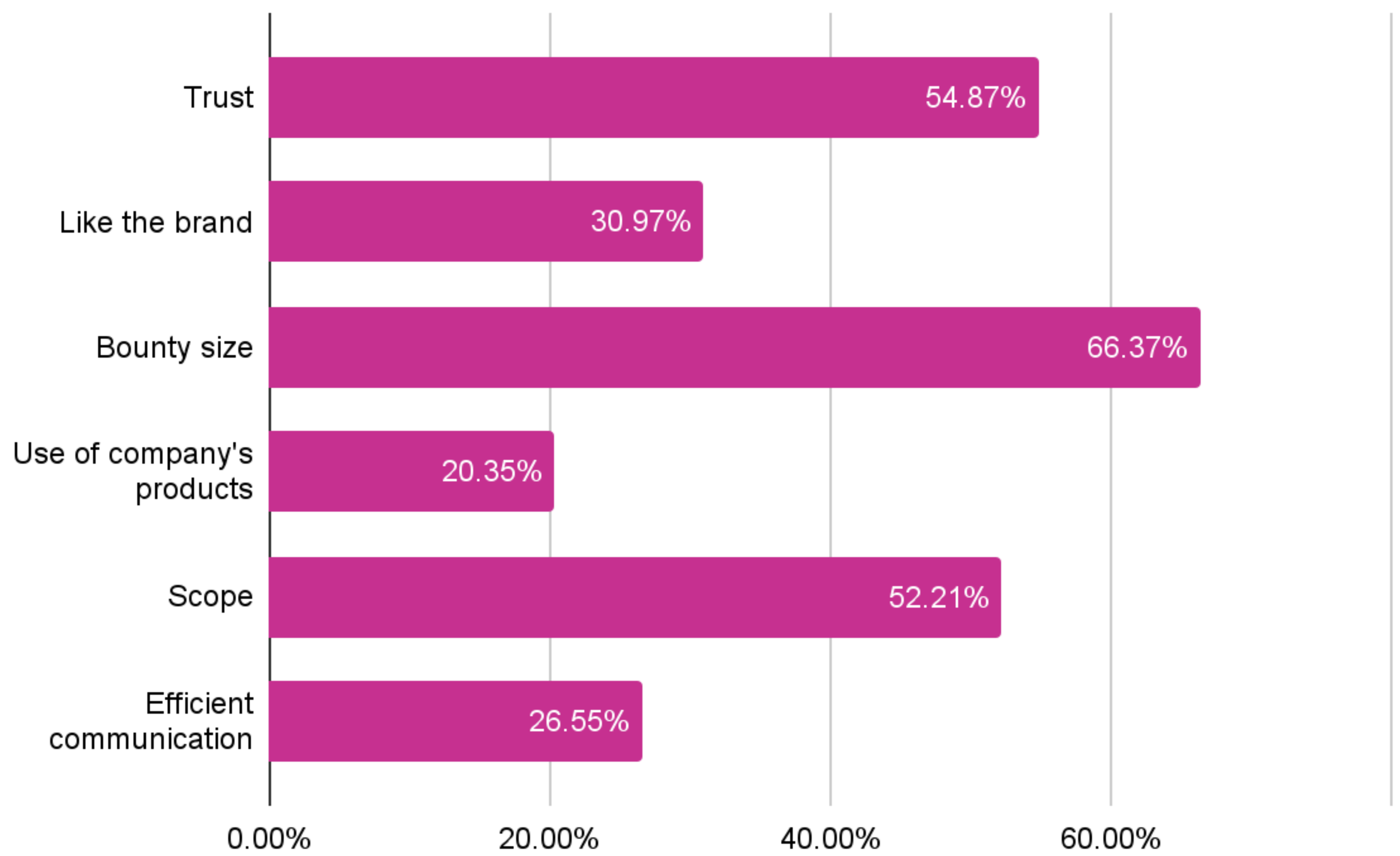
Security

Bounty Programs

When it comes to choosing a bounty program to hunt on, whitehats take into consideration different factors. The bounty size is the main factor of choice (**66.4%**), followed by trust in the project and program (**54.9%**). Remaining factors include the scope of the bug bounty program (**52.2%**), liking the brand (**31%**), efficient communication (**26.6%**), and lastly the use of the company's products (**20.4%**).

Other factors sparsely mentioned by respondents include the complexity, size, and initial interest in the smart contract, website, or applications' code.

.



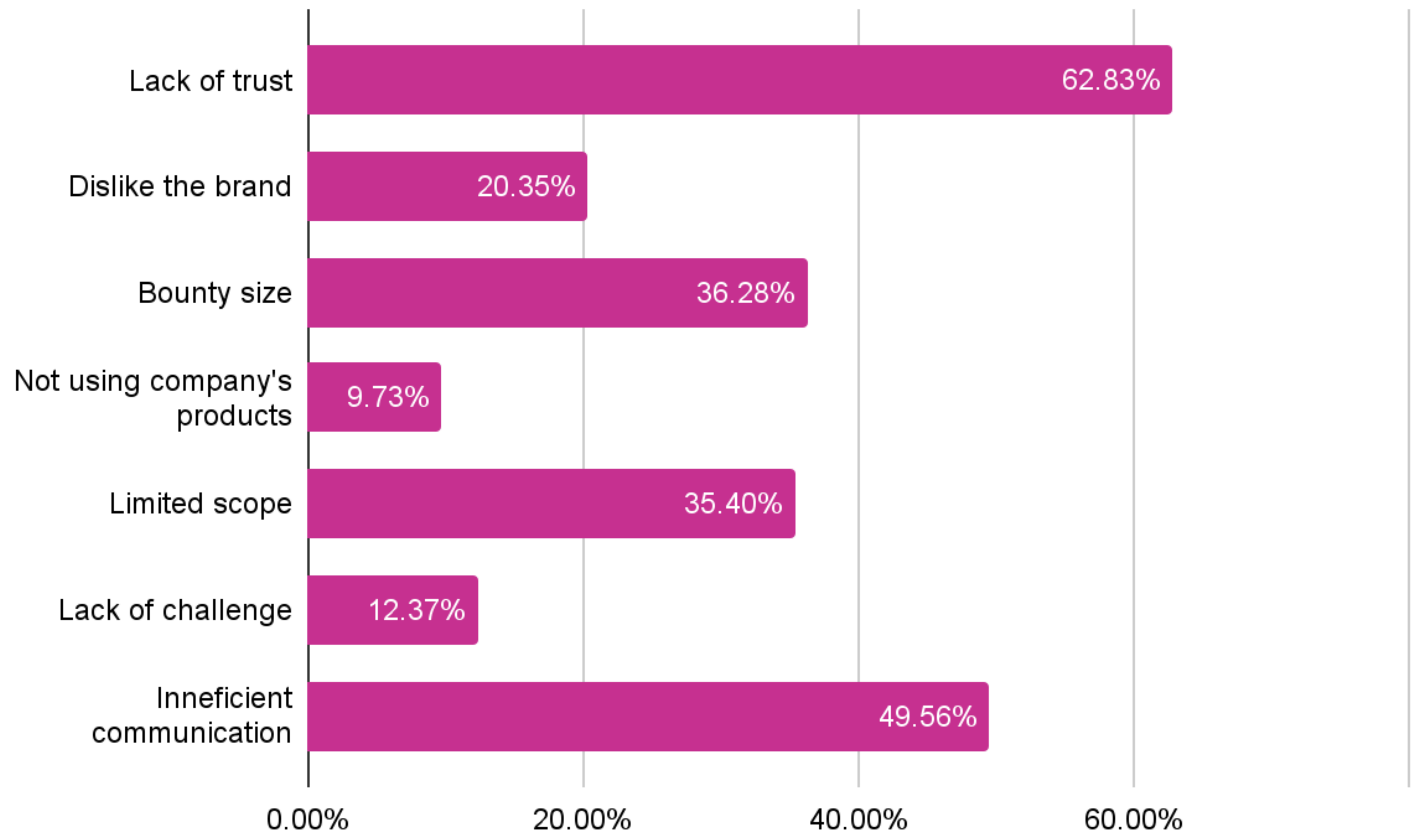
Immunefi

Security

Bounty Programs

In contrast, the lack of trust in a project or program (**62.8%**) is the main factor in why whitehats dismiss a particular bounty program, followed by inefficient communication (**49.6%**). The remaining factors include the bounty size (**36.2%**), the limited scope of the program (**35.4%**), disliking the brand (**20.4%**), the lack of a challenge (**12.4%**), and lastly not using the company's products (**9.7%**).

Other factors sparsely mentioned by respondents include the lack of significant funds locked in the smart contracts in scope and poor or sparse documentation.

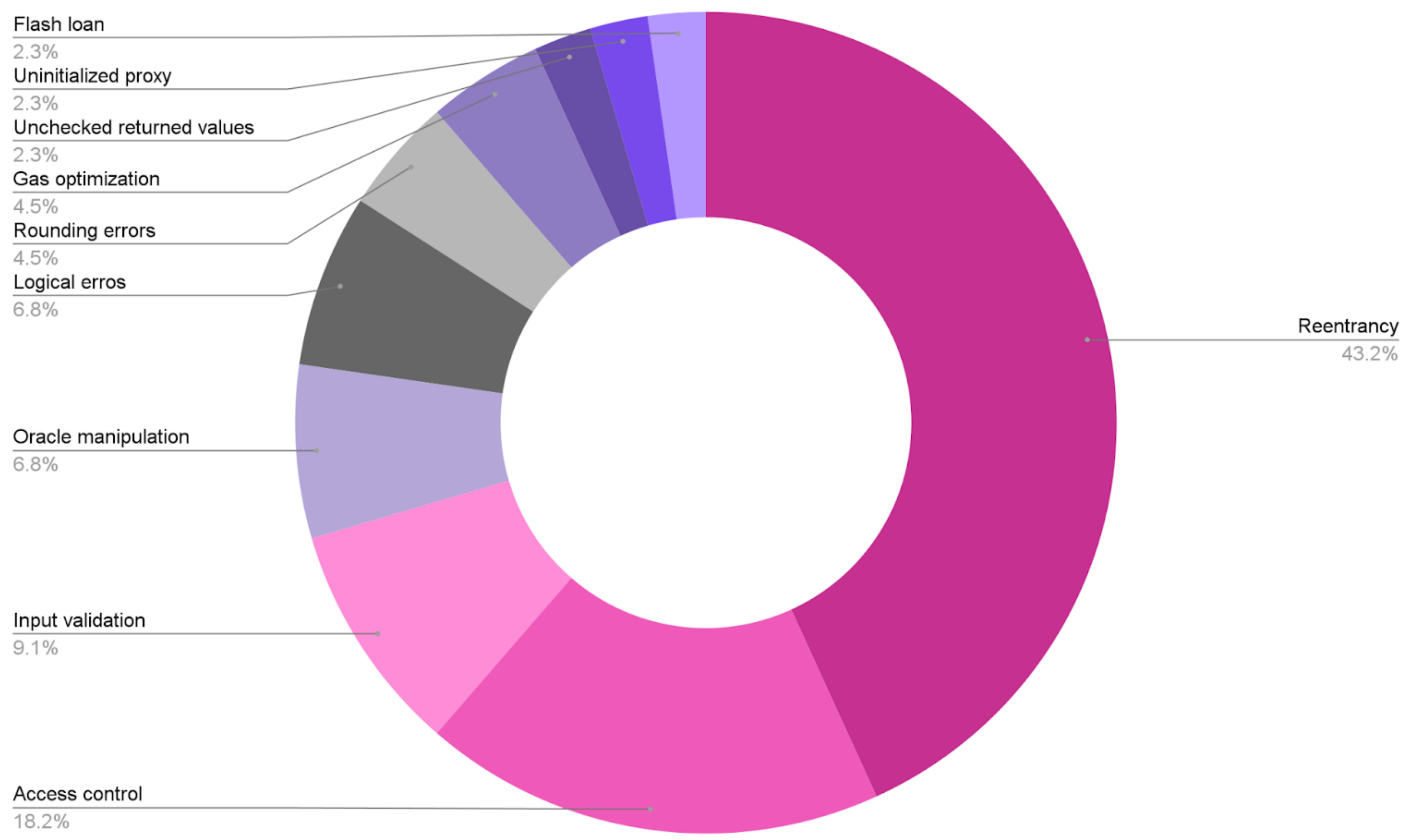


Immunefi

Security

Vulnerabilities and Attack Vectors

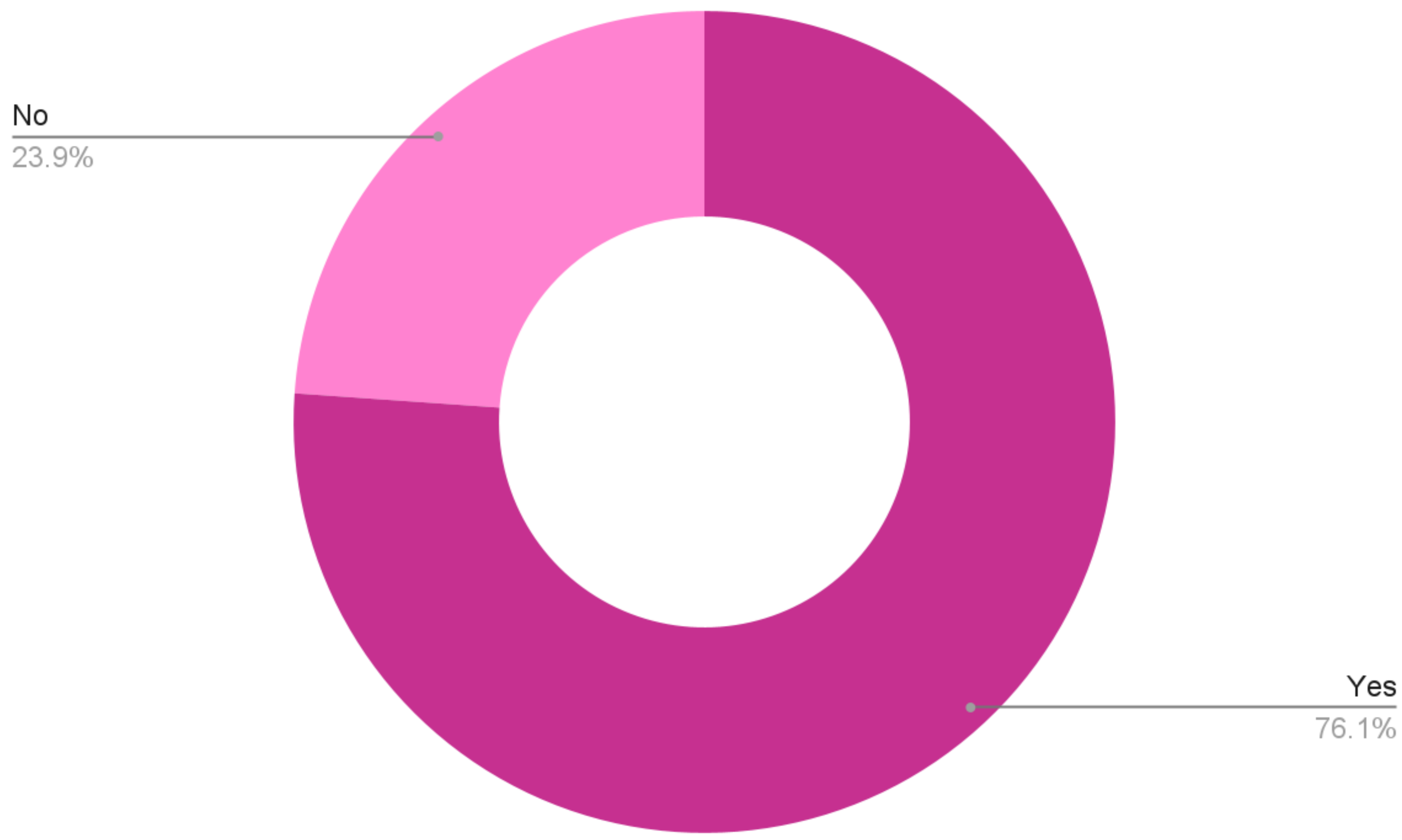
Most of the whitehats mention reentrancy (**43.2%**) as the most common vulnerability they come across when reviewing code, followed by access control (**18.2%**). Other vulnerabilities mentioned include input validation (**9.1%**), oracle manipulation (**6.8%**), and logical errors (**6.8%**). Rounding errors (**4.5%**), gas optimization (**4.5%**), unchecked returned values (**2.3%**), uninitialized proxy (**2.3%**), and flash loan (**2.3%**).



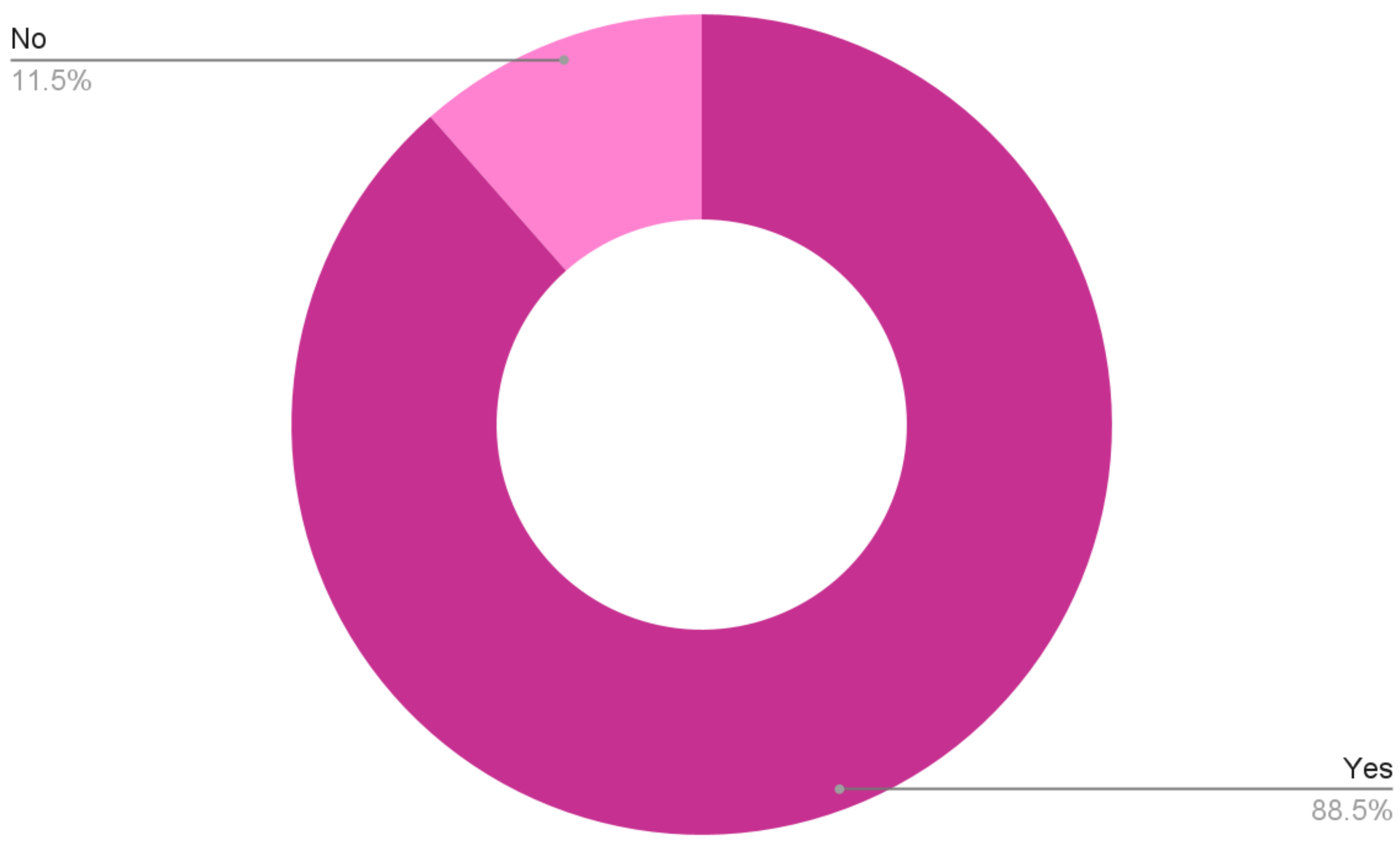
Security

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 (**76.1%**) see attack surfaces growing, the majority (**88.5%**) also see increased security measures by projects across the industry - compared to **23.9%** of respondents who don't see attack surfaces are growing, and **11.5%** who don't see particular increased security measures among projects.



Attack Surfaces Growth



Increased Security Measures

Immunefi

Web3: Challenges and Possibilities

Challenges

When asked about the biggest challenges whitehats have experienced in web3 security, most respondents highlighted*:

- **Learning and resources:** whitehats particularly highlight the steep learning curve, regardless of previous background in cybersecurity or web2 development. Regarding resources, most whitehats consider that these are hard to find, limited, and often too sparse or not well-structured. Resources available in the specific languages that whitehat hackers speak are also limited.
- **Technology:** most whitehats consider working with this new technology to be challenging because of its rapidly evolving and changing nature. Respondents also highlighted the complexity of Solidity coding, protocols, and the possible attack vectors in web3.
- **Security:** most whitehats have experienced increased security measures across the industry, which makes bug hunting more challenging. With more security measures in place, audits, and bug bounty programs, whitehats can go months without uncovering a vulnerability. With requirements continuously evolving, whitehats feel the challenge of keeping up with the industry.

* Overview based on an assessment of open-ended responses.

Immunefi

Web3: Challenges and Possibilities

Possibilities

When asked about the possibilities and what makes web3 exciting for whitehats, most respondents highlighted*:

- **Learning opportunity and challenge:** whitehats particularly highlight the excitement of becoming a part of a new and evolving industry. They feel web3 is giving everyone relatively the same chances of succeeding, as they believe hard work, learning, and acquiring the necessary skillset are the most key. Learning becomes both exciting and rewarding.
- **Technology:** respondents feel excited to be working on new technology. The concepts of decentralization and transparency are exciting.
- **Money and career opportunities:** respondents consider web3 a high-paying industry with greater career opportunities as the field keeps developing. The industry provides a chance to achieve a high and steady income, in addition to the extremely high payouts whitehats can receive through bug disclosures.
- **Impact and security:** whitehats mention that particular attack vectors, in a technology where monetary funds are directly at risk, contribute to making security a high-impact role in the industry.

* Overview based on an assessment of open-ended responses.

Relevant Insights

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

- When it comes to age, there has been a significant **increase in the percentage of whitehats between the ages of 20 and 29 years old to 54%**, as compared to **45.7%** in the previous period, becoming a clear majority in the ecosystem.
- While **male whitehats still take the largest share within the industry at 95.5%**, the number of **female whitehats continues to increase, reaching 3.5%**, as compared to **2.4%** in the previous period, representing a 45.8% increase.
- On average, **most whitehats have been working in cybersecurity for almost 4 years**, with a maximum case of **25 years** engaged in cybersecurity. They have been interested in web3 security for almost **2 years**, an increase of 1 year when compared with the previous period.
- There's been a significant **increase in whitehats hacking in their free time to 44.2%** when compared to **39.8%** in the previous period, representing a 11% increase. On the other hand, **hacking as a primary job has decreased 7.3%** from **60.2%** in the previous period to **55.8%** in the current one. Overall, more whitehats are joining the field and using their free time to work on transitioning to web3 cybersecurity full-time.
- When it comes to preferred blockchains, there has been a significant **increase in interest in Tezos to 8%**, when compared to the previous period at **3.6%**, representing a 122.2% increase. **Interest in Ethereum dropped from 96.4%** in the previous period to **92%** in the current one, representing a 4.6% decrease. **Interest in Solana dropped significantly from 47%** in the previous period to **31%** in the current one, representing a 51.6% decrease. **Interest in Avalanche dropped slightly from 21.7%** in the previous period to **20.4%** in the current one, representing a 6% decrease, as well as **Cosmos, with a 8.3% decrease from 14.5%** in the previous period to **13.3%** in the current one. Overall, the whitehats' interests have stayed the same by order of importance, with slight adjustments in the magnitude of interest for each.

Immunefi

Relevant Insights

- When it comes to factors driving hackers' interest, there has been a **7.3% increase in the interest in career opportunities to 62%**, when compared to the previous period at **57.8%**. On the other hand, **interest in money dropped from 79.5%** in the previous period to **69%**, representing a 13.2% decrease. **Interest in the community dropped significantly to 38%**, when compared to the previous period at **50.6%**, representing a 24.9% decrease. **Interest in solving technical challenges continues to be the main factor in driving hackers' interest**, although it witnessed a slight 4.6% decrease to **77%**, when compared to the previous period at **80.7%**. Overall, the whitehats' interests have stayed the same by order of importance, with slight adjustments in the magnitude of interest for each. Whitehats look for continuous technical challenges but are more eager to grab opportunities that will allow them to sustainably and professionally grow within the sector.

Immunefi

Immunefi is the leading bug bounty and security services platform for web3 protecting over $60 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 **$65 million** in total bounties, while saving over **$25 billion** in user funds.

Total bounties available

Immunefi offers over **$130 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 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 decentralised Ethereum scaling platform that enables developers to build scalable user-friendly dApps.