Immunefi

TOP CRYPTO BOUNTY AND RANSOM PAYMENTS REPORT

Immunefi

Top Crypto Bounty and Ransom Payments Report

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, has created a comprehensive crypto bug bounty report detailing the most important industry bug bounty payments to date, as well as ransom payments made by projects to malicious hackers to receive back a portion of stolen funds throughout 2022.

Immunefi has also included a high-level analysis of its own paid bug report database as a relevant overview of what the crypto bug bounty ecosystem looks like, as Immunefi is the industry leader and features the largest database.

Quick Facts

- In total, **$65,918,994** crypto bounty payments have been made through Immunefi. Of that number, **$13,428,419** was paid in 2021, and **$52,490,575** was paid in 2022.
- The top five crypto bug bounty payments in the industry have brought a total of **$21,700,042** in rewards to whitehat hackers alone.

The Bug Bounty: Web2 vs. Web3

Bug Bounty Programs, also known as Vulnerability Rewards Programs (VRP), are essentially open invitations to security researchers to discover and disclose potential software bugs and vulnerabilities in projects' websites and code in exchange for a reward, and in some cases additional recognition.

While the web2 ecosystem mostly does not have to worry about the direct loss of financial assets, the reality in web3 couldn't be more different. Incentives to exploit projects in web3 are significantly larger, due to the amount of capital that exists in smart contracts. Web3 is also unique because vulnerabilities in code can result in a direct loss of this capital.

This difference has led to a dramatic repricing of bug bounties in the web3 world, where they have quickly become the largest in the entire software industry by orders of magnitude. The goal of this repricing is to incentivize whitehats to responsibly disclose, rather than exploit, the vulnerabilities.

A $5,000 bounty payout for a critical vulnerability may work in the web2 world, for example, but it does not work in the web3 world. If the direct loss of funds for a web3 vulnerability could be up to $50 million dollars, then it makes sense to offer a much larger bounty size to incentivize good behavior.

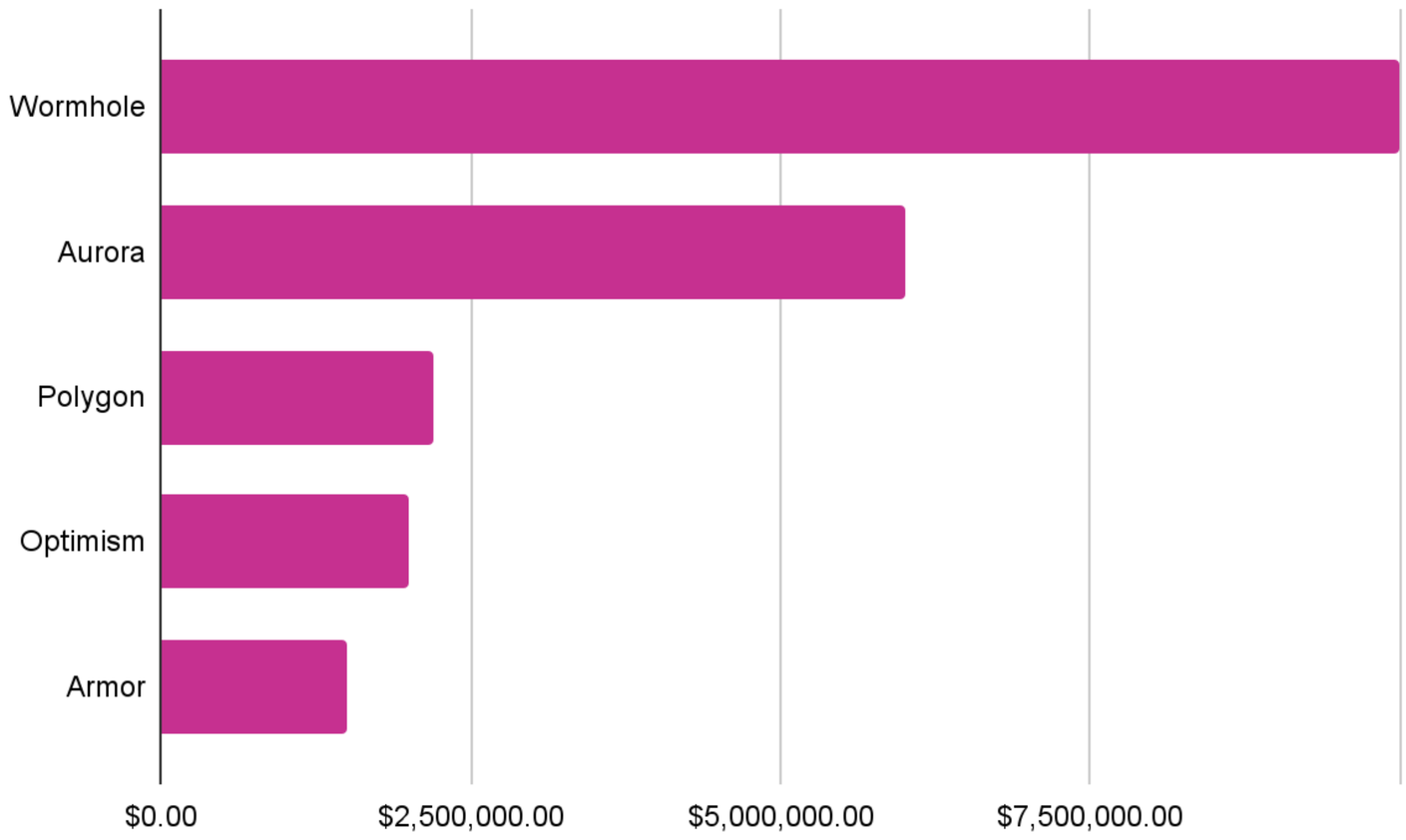
A reliable incentivize system is more necessary than ever, as malicious hackers are continuously targeting vulnerabilities in (decentralized finance) DeFi smart contracts, which is a subset of the web3 industry. In fact, a recent report by Immunefi revealed that over $2.3 billion was already lost in DeFi this year alone to hacks and scams.

Additionally, web3 is a far more adversarial environment, which means every step of the bug bounty process works differently, from the submission and processing of a report, to the validation of a report, to the negotiation for a payout. Where traditional web2 bug bounties are a convenient bug fixing tool, web3 bug bounties are a far more critical emergency response system for DeFi projects. As such, cybersecurity has become a crucial component of market recognition in web3.

But how do web3 bug bounty payments compare to some of the most prominent conventional bounty programs?

Top 5 Bug Bounty Payments

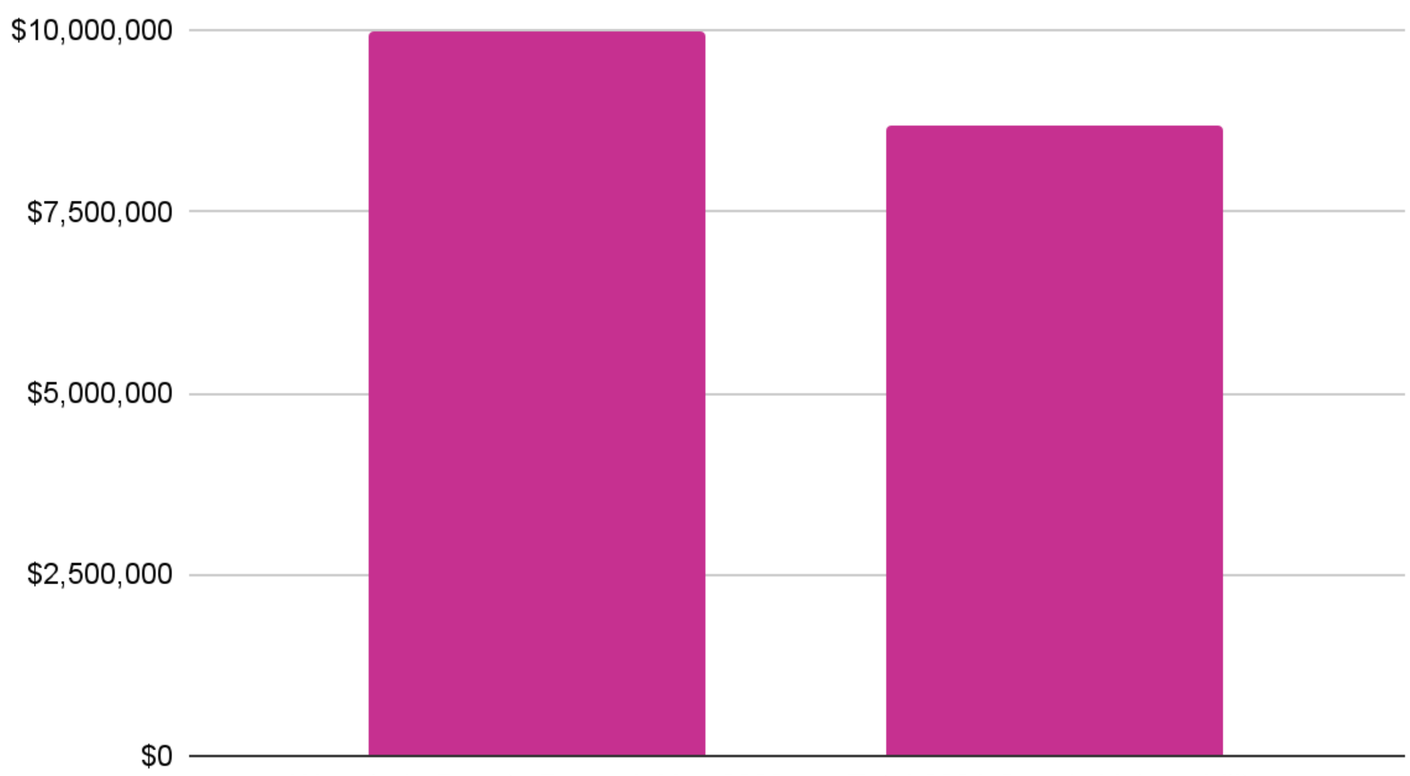
The top five public crypto bug bounty payments in the industry have brought a total of **$21,700,042** in rewards to whitehat hackers alone.



- **$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 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.
- **$2 million** for a vulnerability discovered in Optimism, an Ethereum Layer 2 blockchain.
- **$1.5 million** for a vulnerability discovered in Armor, a smart insurance-alternative for DeFi assets.

Top 5 Bug Bounty Payments

To put it into perspective, the Wormhole reward alone is larger than the total amount of bounties paid across all Google Vulnerability Reward Programs in 2021, at $8.7 million.



Immunefi Bounty Payments Analysis

Immunefi has released an overview of all paid bug reports processed through its platform to provide a comprehensive categorization of bug bounties in the crypto space. This report also separately includes a list of ransom payments that projects have paid to malicious hackers.

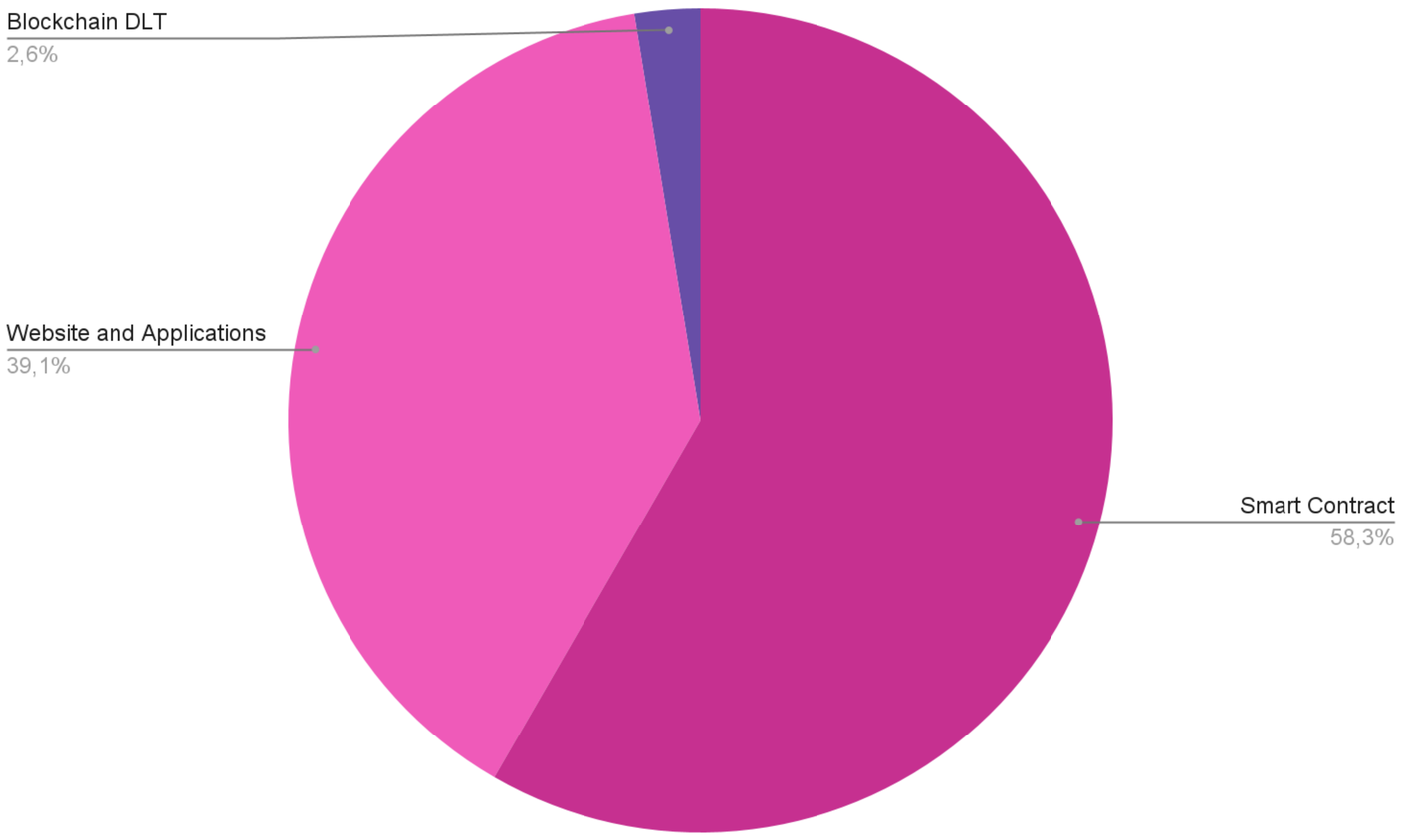
Immunefi classifies bugs on a simplified 5-level scale from Critical, High, Medium, Low, and Informational across Smart Contracts, Blockchain/DLT and Websites and Applications bug report submissions.

The development of the scale takes into consideration multiple factors that may affect a vulnerability and its likelihood of exploitation, but finalizes them largely by the impact that they cause. The classification table is mostly concerned with the consequences of a successful exploit.

Overview

Type

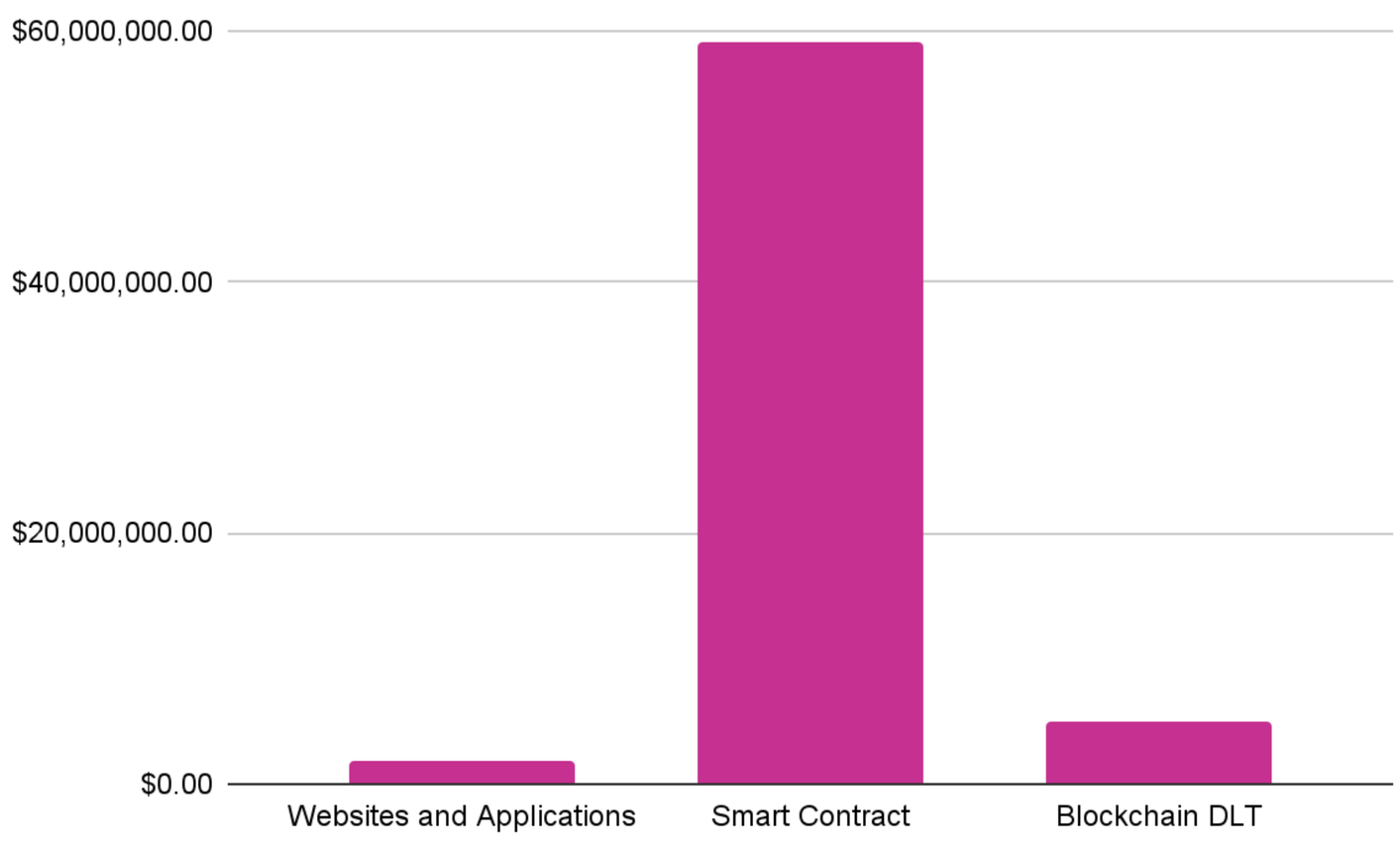
- Vulnerabilities reported in Smart Contracts lead with a total of 728 submissions, accounting for 58.3% of paid reports.
- Websites and Applications total 488 submissions, representing 39.1% of the total paid reports by type.
- Blockchain/DLT total 32 submissions, representing 2.6% of the total paid reports by type.



Immunefi Bounty Payments Analysis

Payments by Type

- Smart Contracts take the lead with a total $59,113,273 in bounty payments, accounting for 89.6% of the total amount paid to whitehats.
- Blockchain/DLT total $4,890,910, representing 7.4% of the total whitehat payouts paid to whitehats.
- Websites and Applications total $1,914,811, representing 2.9% of the total whitehat payouts.

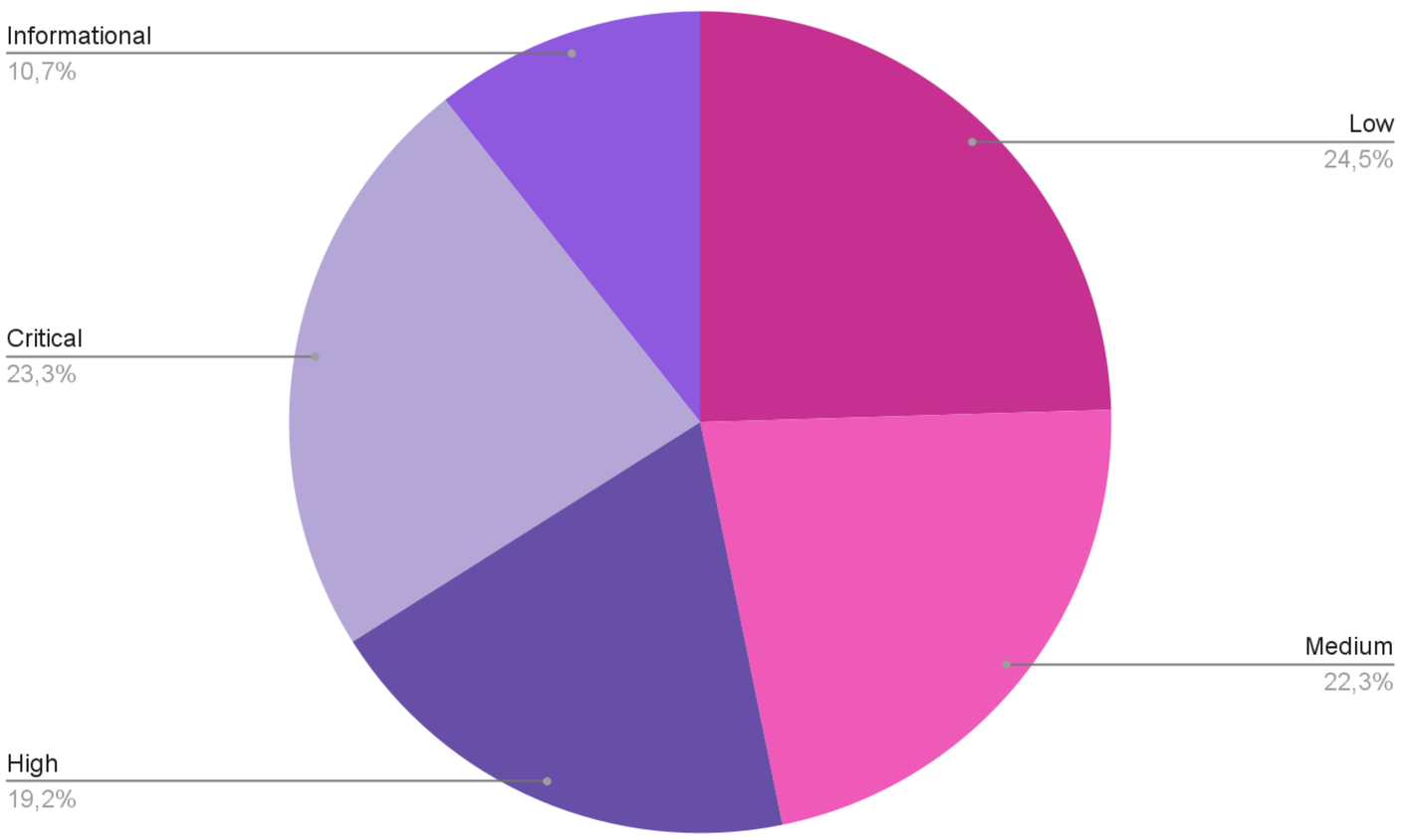


Immunefi Bounty Payments Analysis

Severity

Low and critical severity reports take the lead, with 48.9% of the total paid bug reports.

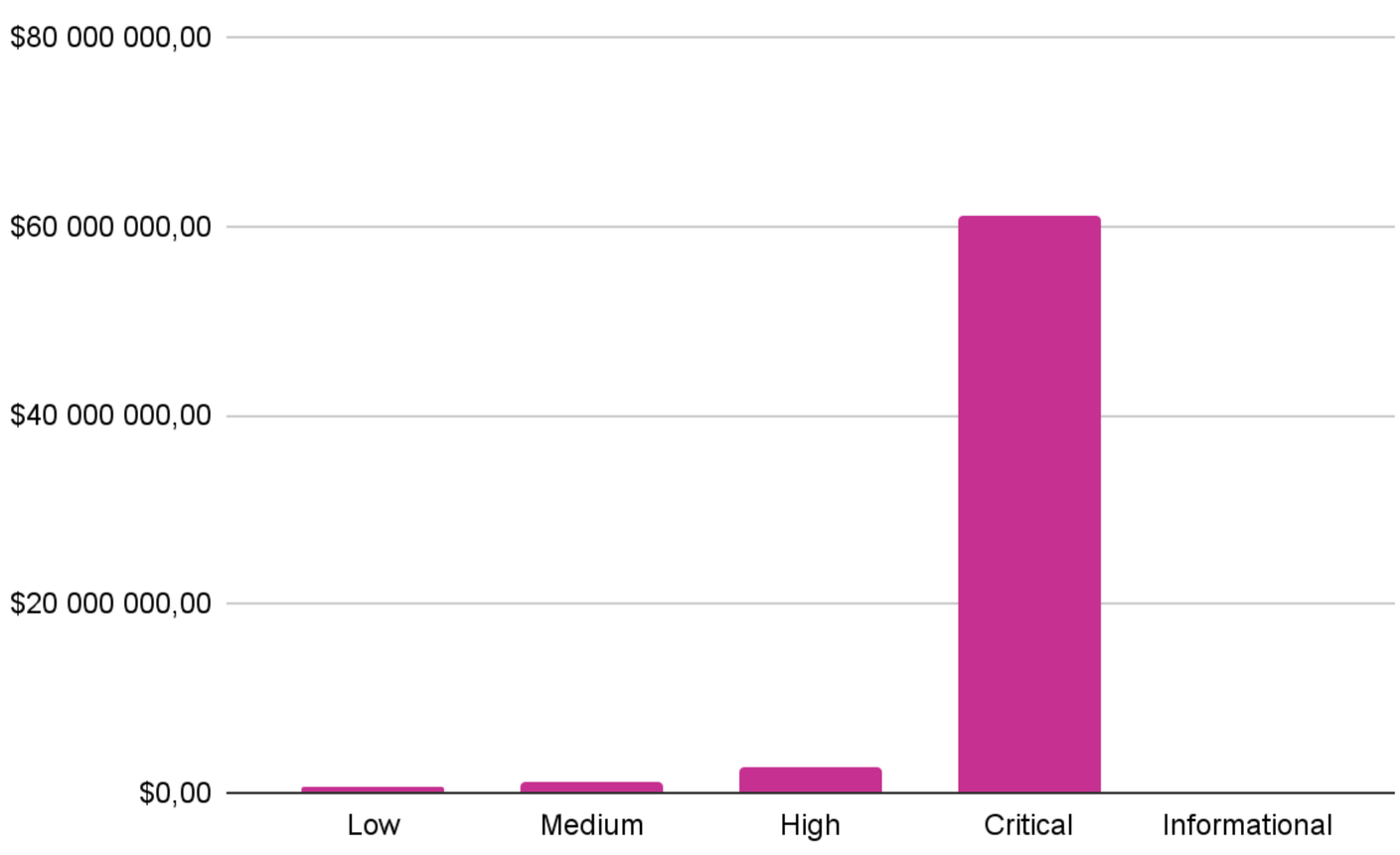
- Low severity bug reports total 306, representing 24.5% of submitted vulnerabilities, across paid reports.
- Medium severity bug reports reports total 278, representing 22.3% of submitted vulnerabilities, across paid reports. An example of a medium vulnerability report includes the potentially exploitable Denial of Service (DoS) bug on Balancer.
- High severity bug reports total 240, representing 19.2% of submitted vulnerabilities, across paid reports. Examples of high vulnerability reports include Pods Finance, for a logic error that allowed for theft of yield or abuse of the rewards system on the protocol, and Mushrooms Finance, for a MEV (miner-extractable value) attack with flash bots.
- Critical bug reports total 291, accounting for 23.3% of submitted vulnerabilities, across paid reports. Examples of critical vulnerability reports include Wormhole, Aurora, Moonbeam, and Polygon, where significant amounts of user funds were directly at risk.
- Vulnerabilities classified as Informational account for 10.7% across 133 paid reports.



Immunefi Bounty Payments Analysis

Payments by severity

- Critical vulnerabilities take the lead with a total of $61,155,773, accounting for 92.7% of all bounties paid out.
- High vulnerabilities total $2,875,627, representing 4.3% of the total bounties paid out.
- Medium vulnerabilities total $1,149,623, representing 1.7% of the total bounties paid out.
- Low vulnerabilities total $511,637, representing 0.7% of the total bounties paid out.
- Vulnerabilities classified as Informational account for 0.3% of the total, amounting to $207,854 in bounty rewards paid out.



Ransom Analysis

Sometimes, a project gives an offer to the malicious hacker that they can keep a percentage of the stolen funds as long as they return the rest, in exchange for the project not legally pursuing the hacker.

Overview

Multichain
Returned
$1 million
Ransom
$150.000

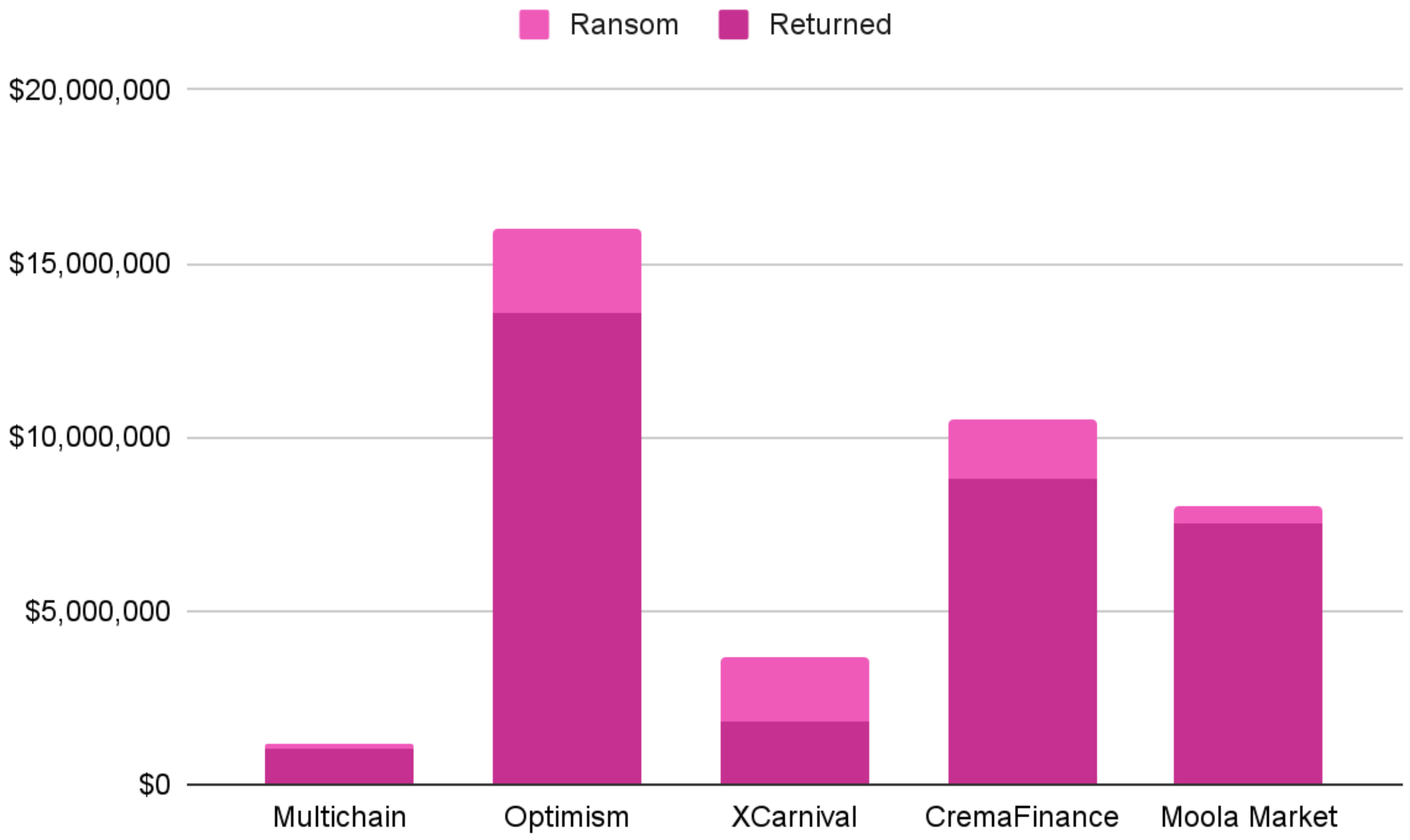
Optimism
Returned
$13.6 million
Ransom
$2.4 million

XCarnival
Returned
$1.8 million
Ransom
$1.85 million

Crema Fin.
Returned
$8.8 million
Ransom
$1.68 million

Moola Market
Returned
$7.5 million
Ransom
$500,000

In total, malicious hackers have returned **$32,700,000** illicitly gained from DeFi protocols across 5 specific situations in 2022. Hackers kept **$6,445,000** in total ransom payments.



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 **$144 million** in available bounty rewards.

Supported projects

Trusted by established, multi-billion dollar projects like Chainlink, Wormhole, MakerDAO, Compound, Synthetix, and more, Immunefi now supports 301 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.

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 $144M in rewards available on Immunefi — the leading bug bounty platform for web3.

https://immunefi.com/