Cybersecurity in a Web 3.0 World

Many individuals and businesses consider Web 3.0 to be the next iteration of the internet. Built on blockchain technology, its semantic architecture facilitates decentralization, personalization, immersion, and a token-driven economy.

What Is Web 3.0?

Overall, it presents many opportunities for companies to enhance their brand engagement and sales through tailored, immersive experiences for consumers. However, these opportunities come with risk, making cybersecurity practices like application security testing a must. Keep reading to find out the benefits of Web 3.0 and how to reduce the risk it brings.

Web 3.0 Opportunities

Web 3.0, also known as the decentralized internet, is a rapidly evolving space with many exciting opportunities for startups and established businesses. Some of the top Web 3.0 trends include gamification (GamiFi), the metaverse, decentralized finance (DeFi), and non-fungible tokens (NFTs). Decentralized autonomous organizations (DAOs) are another Web 3.0 trend that allows for decentralized decision-making and governance.

These trends represent a shift towards a more democratic internet where users have more control over their data and online experiences. The valuation of Web 3.0 blockchain technology in 2023 is close to $3 billion, with a projection of $116 billion by 2030, as per Yahoo Finance.

However, such a market represents not only opportunities for legitimate businesses but also for bad actors.

Cybersecurity for Web 3.0

In the Web 3.0 landscape, cybersecurity is crucial. Decentralized applications (Dapps) rely on distributed networks of nodes and smart contracts to provide trustless, transparent, and immutable services.

Malicious actors have already exploited vulnerabilities in the code, network, or user interface of Dapps. Known breaches include the DAO hack, the Parity multisig wallet bug, DeFi rug pulls, and NFT minting scams. These incidents have resulted in significant losses of funds, reputation, and user confidence for Dapp developers and users.

Application Security Testing for Dapps

To reduce cybersecurity breaches, Dapp developers need application security testing tools that help them identify and fix potential flaws in their code, network, and user interface.

Application security testing tools include static analysis, dynamic analysis, penetration testing, fuzzing, code review, and auditing. These tools help DApp developers ensure that their code is secure, compliant, and optimized for performance and scalability. Additionally, application security testing tools help DApp developers monitor and respond to any emerging threats or attacks in real time.

Analyzing Smart Contract Security

The smart contracts Dapps rely on are software, but the security stakes tend to be even higher than for other types of software. Not only do they directly manipulate funds, but they are also impossible to delete or patch once deployed on the blockchain. Plus, they are a white box to any attacker. For these reasons, there's a lot of attention on smart contract security in the market.

The Enterprise Ethereum Alliance has recently published the first version of EthTrust Security Levels Specification, which draws a lot from the 37 vulnerability categories defined by the Smart Contract Weakness Classification Registry. Regulation, such as the EU's MiCA, also leads to increased focus on security.

So, what's the solution for smart contract security?

First, we need to find and fix security flaws early, before taking the software to production. Second, automation is necessary due to large application portfolios and a shorter time to market.

Static Application Security Testing for Smart Contracts

A range of automated application security testing techniques is available. The most widely used is static application security testing (SAST), which is essentially an automatic source code review.

It makes a lot of sense to use SAST technology for smart contracts. OpenText™ Fortify™ Static Code Analyzer offers SAST in 31+ languages. Its 23.2 release will add support for Solidity-based smart contracts, covering the majority of the SWC registry and EthTrust categories. This capability analyzes

Connect with Us
www.opentext.com

the data that flows through a contract, allowing it, for instance, to spot authentication problems and subtle reentrancy issues.

While point solutions exist for smart contract analysis, smart contracts exist as part of a larger system, including APIs, web, and mobile interfaces. Fortify Static Code Analyzer offers a SAST solution that validates security for the entire system, not just one part of it.

Protect Your Web 3.0 Investments

It's an exciting time to work in Web 3.0. So don't let security risks get in the way. Use SAST to test your Dapps and smart contracts early in the development lifecycle to find and fix issues before they reach production.

To find out how Fortify can help, visit **www.fortify.com**.

About OpenText

OpenText enables the digital world, creating a better way for organizations to work with information, on-premises or in the cloud. For more information about OpenText (NASDAQ/TSX: OTEX), visit **opentext.com**.

Connect with Us

To reduce cybersecurity breaches, Dapp developers need application security testing tools that help them identify and fix potential flaws in their code, network, and user interface.

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.