Top 100 Blockchain Websites Receive Worrying Cyber Ratings… Are Investors and Users at Risk?

Cybersecurity is a critical concern for businesses and investors alike, and the emerging blockchain industry is no exception. Recent cybersecurity ratings of blockchain websites have revealed that many platforms are operating with low cyber ratings, potentially putting investors at risk.

A blockchain is a digital ledger that enables secure and transparent transactions, with cryptocurrency being one of the most popular applications. However, blockchain technology is not immune to cyber threats, including hacking and data breaches. With millions of dollars at stake, investors and traders need to have confidence in the security of the platforms they use.

Unfortunately, recent cybersecurity assessments have revealed that many blockchain websites have some concerns. Cybersecurity firm, Cygienic.com, conducted an analysis of the **top 100 blockchain websites by Market Cap** and found the following:

Cygienic Cyber Rating

30% websites ranged between **C+ and B**.

Hosting Malware Software

15 websites hosting servers were registered as infected with or distribute Malware software - this may be a shared server, supported by an external provider, or a dedicated blockchain server – the attack opportunity here is sending Malware to users connecting to their servers.

Poor Security Certs (SSL)

57 websites had SSL cert vulnerabilities ranging from out-of-date SSL certs to a low-grade security cert purchase – this means data transferred from the user to the server could be compromised.

Email Spoofing Protection

21 domains failed to meet basic email SPF security settings – the attack opportunity here is to impersonate or spoof a staff email address to convince other staff or clients to trick them into a cyberattack.

Webpage Security Headers

67 websites failed to meet basic webpage security header configuration – this means the site has a much higher chance of being compromised due to limited security features settings on each page – the attack opportunity is cyberattack can inject malicious code into the sever you connect to.

Open Network Ports

4 websites have potential open network ports that could be targeted by cyberattacks – the attack opportunity here is to find a weakness in the open port service or a vulnerability to gain access to the server.

Critical & High Vulnerabilities

3 websites have critical & high infrastructure vulnerabilities – these are potential exposure points for cyberattacks – the attack opportunity here is to use a known technique to compromise the known vulnerability to gain access to the server and data.

The report highlights several issues that put investors at risk, including weak encryption, and insufficient network security. Additionally, some blockchain websites were found to be using outdated software that could easily be exploited by cybercriminals.

Investors and traders should take note of these findings and carefully evaluate the security of any blockchain platform before using it to buy, sell or trade cryptocurrencies. Cybersecurity should be a top priority for any blockchain website, and investors should look for platforms with high ratings and strong security protocols.

As the blockchain industry continues to grow, it is essential that businesses and investors take cybersecurity seriously. By prioritizing security and working to address vulnerabilities, blockchain websites can help build trust and confidence in this emerging technology.

For more information on the cybersecurity ratings of blockchain websites, please contact support@cygienic.com