



 bitexen

2020

Case study: a systematic approach to security becomes a blockchain company standard

kaspersky BRING ON
THE FUTURE



**Blockchain
Security**

Bitexen develops crypto trading solutions by offering multi-platform functionality, both mobile and desktop, as well as an API connection.

www.bitexen.com

FinTech

- Headquartered in Turkey
- Founded in 2018
- Passed Kaspersky Application Security Assessment

In 2020 the Bitexen team took a serious step towards their long-term global goals. They decided to build their solution on a solid foundation by securing their applications during the development process from cyber incidents caused by vulnerabilities, design flaws, and configuration errors.

"We want security to be the gold standard for Bitexen. The competitive advantage we offer to our customers is a seamless experience across different platforms. We have a full range of mobile applications both for iOS and Android, web version, and an API to let customers' algorithms execute orders and complete operations. And all these applications must provide the same level of security for both operations and user assets.

"The flexibility we offer means a bigger amount of code behind the scenes, which, of course, leaves a greater opportunity for threat actors to exploit vulnerabilities. And we do not want security issues to ruin the customer experience," says Yahya Tuğyan Erdem, Partner & CEO at Bitexen Technology Inc.

Challenge

The crypto industry is still in its early years: a definite advantage for early adopters and risk-taking entrepreneurs, but also a time of serious security concerns for asset owners. Large numbers of new crypto exchanges, trading platforms, and other providers for emerging crypto-related services attract users and startups and generate a huge amount of cryptocurrency. In 2019 we already saw criminals stealing 292 mln USD by hacking crypto exchanges.

Yahya Tuğyan Erdem, Partner & CEO at Bitexen Technology Inc, explains: "It is important for crypto trading platforms to earn and keep users' trust. At the moment, the number of crypto exchanges on the market is over 20 000 with cryptocurrency holders constantly switching between them in search of the best trading conditions. Every single cyber incident or even service interruption badly impacts the image of the crypto operation provider.

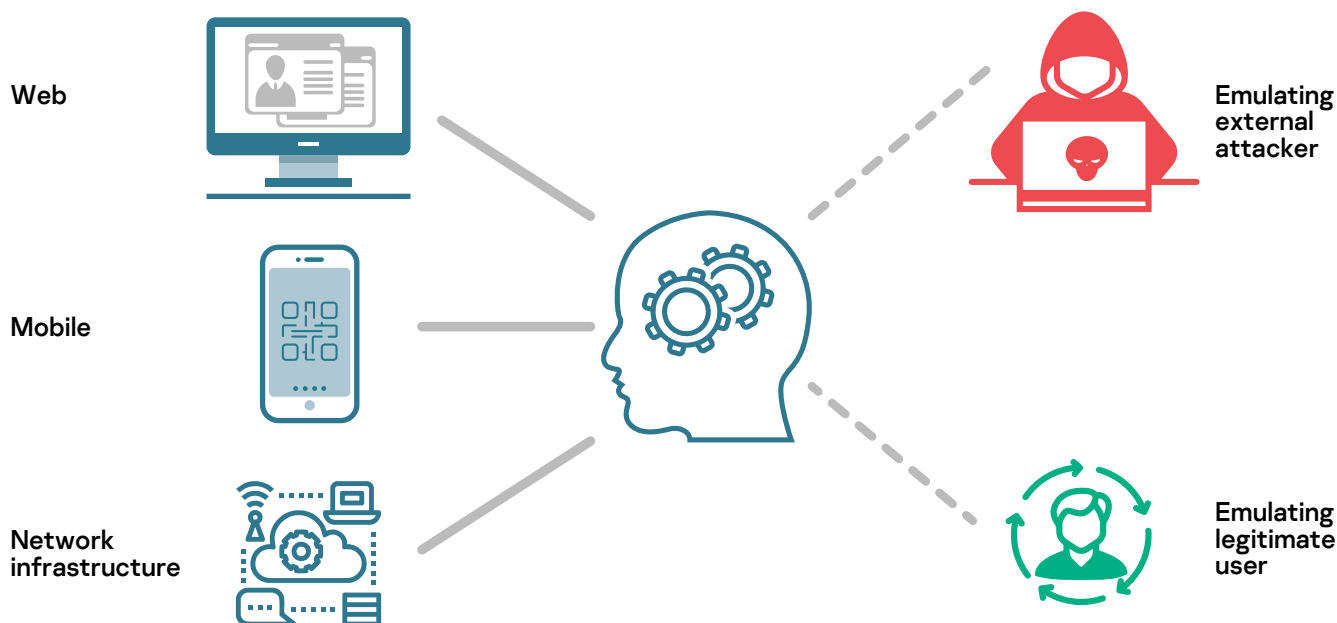
"Moreover, in our industry change is constant. Technology, business models, audience preferences, all change instantaneously and we need to remain flexible. And yet, protecting and securing our end-users is a top priority for the Bitexen team. To achieve this, we collaborated with Kaspersky, a global security pioneer.

"We chose Kaspersky Application Security Assessment to test the Bitexen Cryptocurrency Trading Platform's resistance to cyber-attacks and threats and we are very pleased with our decision and the results," concludes Yahya Tuğyan Erdem.

"Change is constant in the cryptocurrency world. Technology, business models, audience preferences, all change instantaneously and we need to remain flexible. And yet, protecting and securing our end-users is a top priority for the Bitexen team. To achieve this, we collaborated with Kaspersky, a global security pioneer."

Yahya Tuğyan Erdem, Partner & CEO at Bitexen Technology Inc

Application Security Assessment & Pentest



“The assessment included the web application, the iOS and Android apps, as well as pentesting of the external network infrastructure. To simulate real-life scenarios, we chose the pentesting option where vulnerabilities were attacked by both an external attacker without any privileges and an authenticated user.”

Yahya Tuğyan Erdem, Partner & CEO at Bitexen Technology Inc

6 hours

Any eight-character password can be cracked in less than six hours

1.4 mln GBP

The fine British Airways paid after a cross-site scripting attack resulted in leakage of passenger personal data

The security of the entire platform depends on the security of each component

Yahya Tuğyan Erdem says: “It is clear to us that security must be an integral element of our solution. And the security level of the entire platform is equal to the security level of the most vulnerable component. Consequently, the review included the web application, the iOS and Android apps, as well as pentesting of the external network infrastructure.

“To simulate real-life scenarios, we chose the pentesting option where vulnerabilities were attacked by both an external attacker without any privileges and an authenticated user. And this was clearly the right choice,” concludes Yahya Tuğyan Erdem.

Maxim Denizhenko, Security Expert at Kaspersky, explains: “Bitexen has a strong platform where security was addressed throughout the software development cycle. Nevertheless, security assessment revealed a few issues that needed resolution. For one, there was a cross-site scripting vulnerability which often occurs on websites. If left unfixed, the vulnerability allows threat actors to implement external Javascript and gain elevated access privileges to sensitive page content, cookies session, etc.

“The other important finding is the misconfiguration of HTTPS. This error would expose confidential data to hackers if a user, for instance, uses a free Wi-Fi connection controlled by the threat actor,” continues Maxim Denizhenko.

“Kaspersky also recommended 2-factor authentication and a stronger password policy,” Yahya Tugyan Erdem carries on.

“Weak passwords often open the door for brute force attacks. For example, a number of bank customers became victims of this type of attack at the end of 2018,” concludes Maxim Denizhenko.



A winning security attitude

"Being a fintech and startup business it is quite difficult to stay focused properly on security and have the expertise to make sure it functions at 100%, rather than just appear as a line in the technical specification.

"Cooperation with the right partner who can bring such expertise to the table and work in tangent with the development team to address security issues proactively is the key element of a successful security strategy for the companies like us, operating in an industry where security is not your core business, but can still destroy your entire company if not incorporated properly.

"We are glad that we chose to work with the Kaspersky team. They were intelligent, professional, responsive and communications were very smooth," shares Yahya Tuğyan Erdem.

Maxim Denizhenko sums up: "Treating security as an important component and hiring 3rd party professionals to back up internal teams is a great approach for every crypto service provider. It helps to keep digital assets protected and upholds customer trust."

"We are well aware that security is an important component in crypto platform corporate communications to the market. At Bitexen we aim to secure our solution and provide confirmation from 3rd party professional experts. Demonstrable commitment to security builds end-user trust - the most important asset in our business.

"Once we completed the full cycle from receiving the assessment report, studying the recommendations to resolving all the issues, we realized how important it is to have security assessments done regularly. We are committed now to making this a security standard for Bitexen offerings going forward," concludes Yahya Tuğyan Erdem.



Blockchain Security

The ultimate solution package
for securing blockchain-based
technologies

kaspersky.com/blockchain

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

kaspersky

**BRING ON
THE FUTURE**

2020 AO KASPERSKY LAB. ALL RIGHTS RESERVED.
REGISTERED TRADEMARKS AND SERVICE MARKS ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS.