



# CASE STUDY

CRYPTOCURRENCY  
EXCHANGE  
SECURITY  
AUDIT



# About the Client

---

The client is a global personal finance company, which allows people to easily buy and spend Bitcoin and other currencies. With over 70,000 customers, they have processed over \$100m worth of transactions.

They provide simple tools to manage digital currencies and use multi-factor authentication (e.g. password plus SMS verification) to ensure their customers' bitcoins are safe, even if their password is compromised. As an additional layer of protection, they store the majority of customer bitcoin holdings offline.

# Why is Security Paramount?

Decentralised currencies are traded in centralised exchanges. If an exchange is hacked, it leads to massive losses which cannot be recovered through forks (soft and hard). Trust on a cryptocurrency exchange is absolute.



## NICEHASH

Nearly \$64m in bitcoin was stolen by hackers who broke into Slovenian-based bitcoin mining marketplace NiceHash.

BITFINEX

## BITIFINEX

The breach of the Bitcoin exchange platform, caused 120,000 units of bitcoin, which was valued at \$72 million at the time, to be stolen.

enigma

## ENIGMA

The de-centralized platform had its website and a number of social accounts compromised with the perpetrators netting nearly \$500,000 in digital coin.



# Exclusive Tests

1

Two factor authentication bypass

2

Session Hijacking

3

Authorisation & authentication bypass

4

Phishing Resilience

5

OWASP Top 10

6

WASC 40

7

Data encryption assessment

8

DNS attack resilience

9

DoS and DDoS resilience

10

Cloud Security



# Engagement Overview

A quick overview of the engagement.

7

BUGS  
IDENTIFIED

- API Security Testing - 2 Low severity.
- Web Application Security Testing - 1 high and 4 low severity.

12

WHITE HATS

Hackers engaged.

450

END POINTS

Tested thoroughly.

# SECURE YOURSELF!

+91 80 4150 1408

info@entersoftsecurity.com

[www.entersoftsecurity.com](http://www.entersoftsecurity.com)

