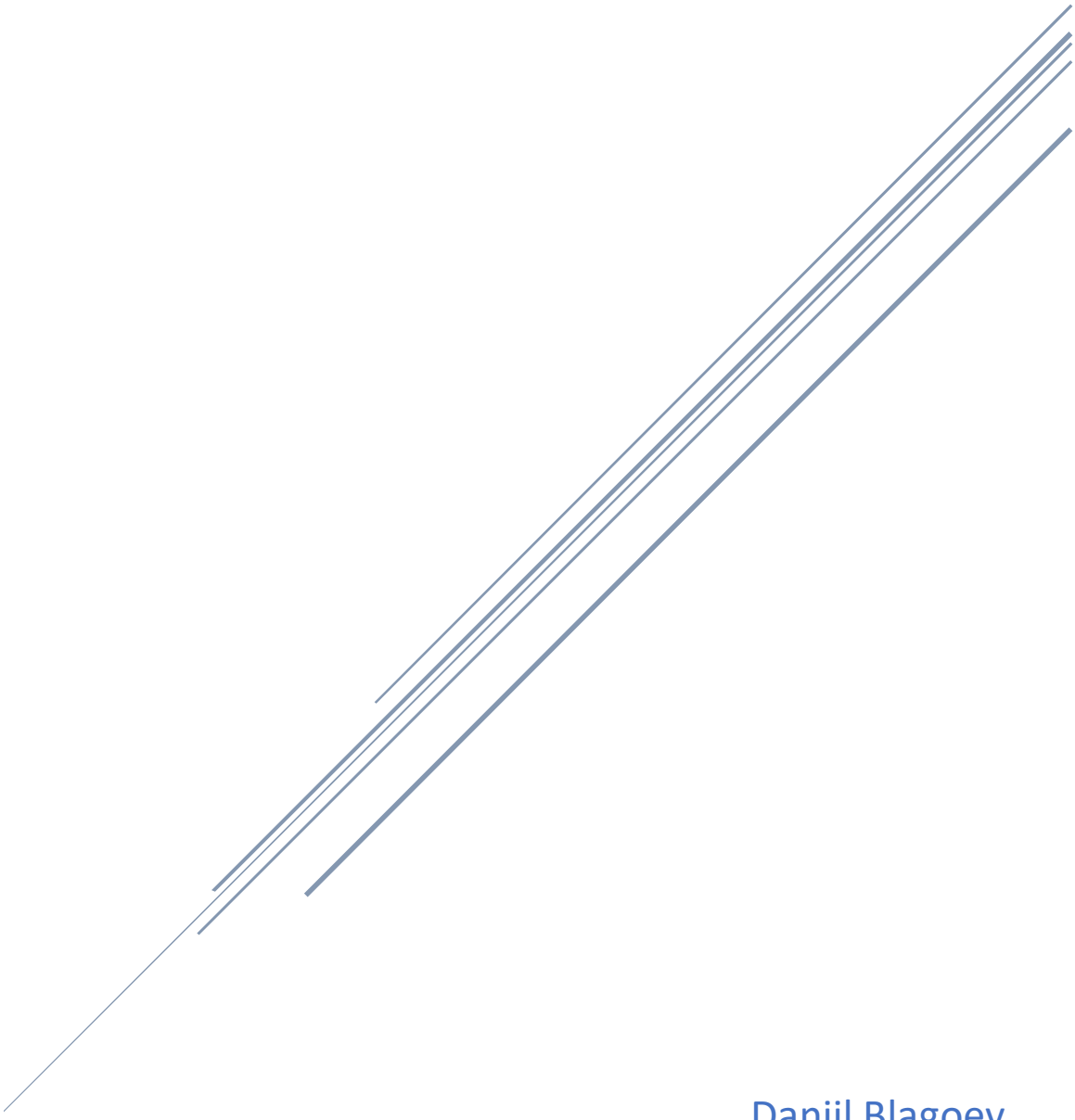
BITBY

Security report document



Daniil Blagoev
Software Engineering Semester 3

	Likelihood	Impact	Risk	Actions possible	Planned
A1: broken access control	Low	Severe	Medium	N/A, fixed	Yes
A2: cryptographic failure	High	Severe	High	Encrypt all of the sensitive user information	Yes
A3: injection	High	Severe	High	Input validation	Yes
A4: insecure design	Medium	Low	Medium	Limit resource consumption by user or service	Yes
A5: security misconfiguration	Medium	Mediu m	Medium	Handle errors properly to avoid leaked stack traces, etc.	Yes
A6: vulnerable and outdated components	Medium	Mediu m	Medium	N/A, fixed	Yes
A7: identification and authentication failures	Medium	High	High	Take defensive measures against credential stuffing	N/A

A8: software and data integrity failures	High	Medium	High	Ensure libraries and dependencies are consuming trusted libraries	N/A
A9: security logging and monitoring failures	High	High	High	Log auditable events	N/A
A10: server-side request forgery	Medium	High	High	Sanitize and validate all user data	Yes

Reasoning

A1:

The likelihood of broken access control is low because ByBit uses authentication and authorization practices for necessary functionalities. The impact is severe because a crypto exchange contains very sensitive user information.

A2:

The likelihood of cryptographic failures is high because ByBit only encrypts its users' passwords for now. The impact is severe because the personal information contained in the system is very sensitive.

A3:

The likelihood of injection is high because ByBit does not have much time invested into preventing it. The impact is severe because the data in the system is related to finances and is of great importance.

A4:

The likelihood of insecure design is medium because ByBit does use unit, integration and system testing, but it could take more defensive measures to prevent attacks of this nature.

A5:

The likelihood of security misconfiguration is medium because ByBit it does not have most of the listed risks from this type of attack such as: unnecessary features are enabled or installed, software is outdated, etc.

A6:

The likelihood of vulnerable and outdated components is medium because frameworks and dependencies are regularly kept up to date and ByBit uses no outdated software.

A7:

The likelihood of identification and authorization failures is medium because ByBit does implement some measures against such attacks, but more improvements could be made.

A8:

The likelihood of software and data integrity failures is high because ByBit has not invested time into building up defenses against such attacks.

A9:

The likelihood of security logging and monitoring failures is high because ByBit has not invested time into building up defenses against such attacks.

A10:

The likelihood of server-side request forgery is medium because ByBit takes measures against some of the risks like not sending raw data to clients for example.

Conclusion

In summary, ByBit has some very basic security mechanisms in place, which are definitely not enough for a real crypto exchange. More layers of defense would be implemented if ByBit were to head into the real world of crypto exchanges.