

---

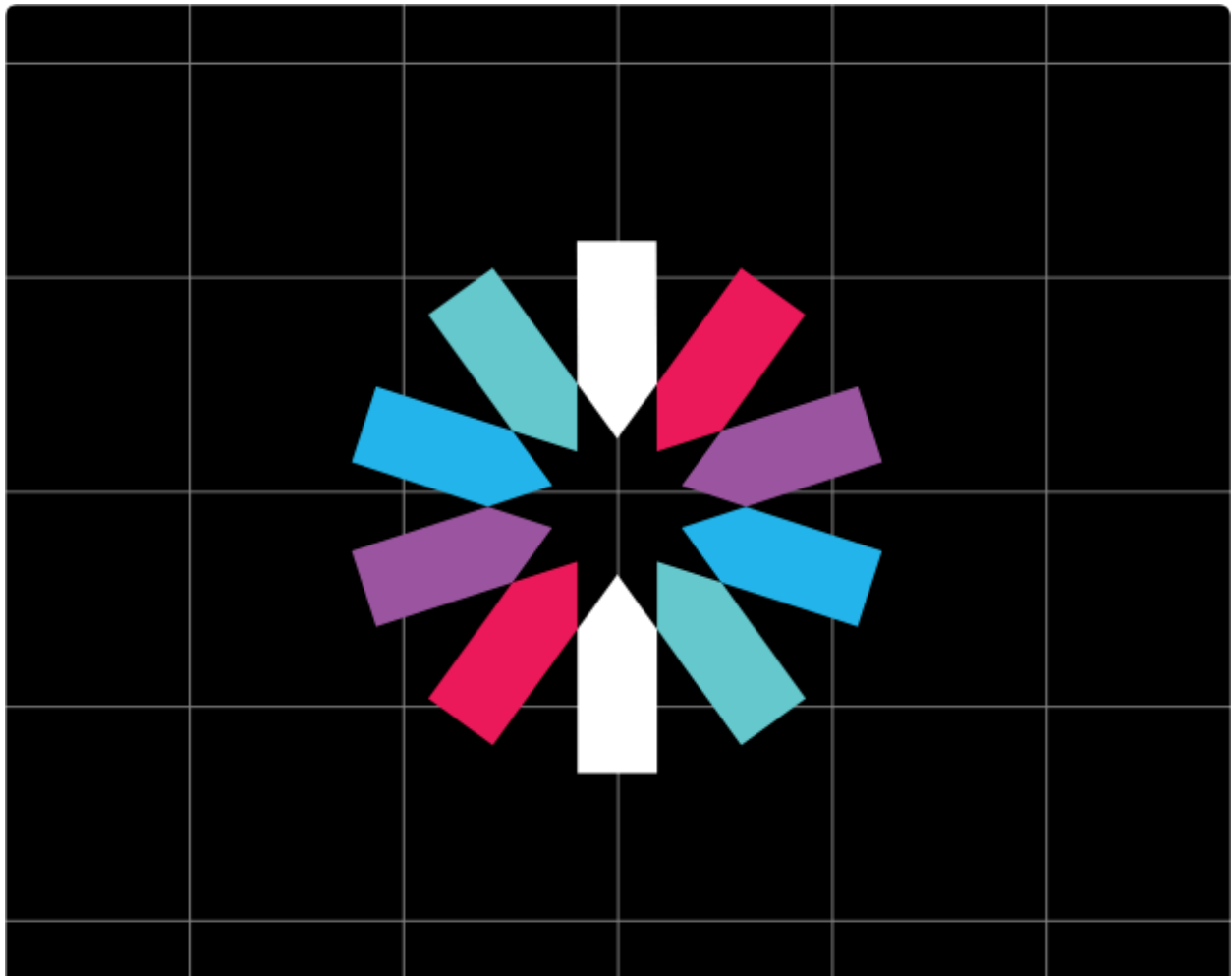
# QUOCCABANK

## Vulnerability Report 2

Simon Nguyen [REDACTED]

Haibing [REDACTED]

Felix [REDACTED]



# Table of Contents

<b>Table of Contents</b> .....	<b>1</b>
<b>Executive Summary</b> .....	<b>4</b>
<b>Summary of Results</b> .....	<b>4</b>
<b>Risk Matrix</b> .....	<b>5</b>
Threat Agent Factors.....	5
Vulnerability Factors.....	5
Technical Impact Factors.....	6
Business Impact Factors.....	6
<b>Results</b> .....	<b>8</b>
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').....	8
Instances.....	9
NetQuocca2.....	9
Reproduction.....	9
OWASP Risk Rating.....	10
Remediation.....	10
Report V2.....	10
Reproduction.....	11
OWASP Risk Rating.....	11
Remediation.....	12
Science Today 2.....	12
Reproduction.....	12
OWASP Risk Rating.....	13
Remediation.....	13
Support V2.....	14
Reproduction.....	14
OWASP Risk Rating.....	15
Remediation.....	15
CWE-113: Improper Neutralisation of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting').....	16
Instances.....	16
Report.....	16
Reproduction.....	16
OWASP Risk Rating.....	18
Remediation.....	19

CWE-352: Cross-Site Request Forgery (CSRF).....	20
Instances.....	20
Layoffs.....	20
Reproduction.....	20
OWASP Risk Rating.....	21
Remediation.....	21
CWE-472: External Control of Assumed-Immutable Web Parameter.....	23
Instances.....	23
Clients 1.....	23
Reproduction.....	23
OWASP Risk Rating.....	24
Remediation.....	25
CWE-434: Unrestricted Upload of File with Dangerous Type.....	26
Profile V1.....	26
Reproduction.....	26
OWASP Risk Rating.....	27
Remediation.....	27
CWE-646: Reliance on File Name or Extension of Externally-Supplied File.....	28
Instances.....	28
Profile V2.....	28
Reproduction.....	28
OWASP Risk Rating.....	29
Remediation.....	29
CWE-180: Incorrect Behaviour Order: Validate Before Canonicalize.....	30
Instances.....	30
Clients 2.....	30
Reproduction.....	30
OWASP Risk Rating.....	31
Remediation.....	31
CWE-85: Doubled Character XSS Manipulations.....	32
Instances.....	32
Science Today Query.....	32
Reproduction.....	32
OWASP Risk Rating.....	33
Remediation.....	33
CWE-656: Reliance on Security Through Obscurity.....	34
Instances.....	34
Relax Unlocks.....	34
Reproduction.....	34

OWASP Risk Rating.....	35
Remediation.....	35
CWE-184: Incomplete List of Disallowed Inputs.....	36
Instances.....	36
Engineering.....	36
Reproduction.....	36
OWASP Risk Rating.....	37
Remediation.....	37
CWE-1395: Dependency on Vulnerable Third-Party Component.....	38
Instances.....	38
Jobs.....	38
Reproduction.....	38
OWASP Risk Rating.....	39
Remediation.....	40
CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition').....	41
Instances.....	41
Relax in-app purchases.....	41
Reproduction.....	41
OWASP Risk Rating.....	43
Remediation.....	44
<b>Glossary.....</b>	<b>45</b>
<b>References.....</b>	<b>45</b>
<b>Appendix.....</b>	<b>46</b>
Jobs.....	46