OCTOBER 2021

API Security Questionnaire

A guide to hardening third-party APIs

Presented by the member banks of the ***Alloy Labs Alliance***
In collaboration with ***Crowe LLP***

ALLOY LABS ALLIANCE

Crowe

Cybersecurity is an increasingly important topic for bank leaders.

75%

of all credential abuse attacks against the financial services industry targeted APIs directly.

(Source: Akamai)

62%

of organizations have no or just a basic strategy in place for API security.

(Source: Salt Security)

The number of cyber attacks continues to rise, and the sophistication of those attacks is escalating. Further, customers are demanding data portability, open networks that enable connections to third party applications, and new products that require banks to partner with fintechs to integrate new offerings into their existing systems. To address these security challenges in modern software head-on, application programming interfaces (APIs) need to be developed with security in mind.

The members of the Alloy Labs Alliance ("Alliance") — a consortium of innovative community and midsize banks — are keenly attuned to this tension. The bankers involved in the Alliance's Cybersecurity Center of Excellence ("Cyber group") identified the need to secure third-party APIs that are used to connect systems and transfer data as a priority. To that end, the group co-created API security focus points.

Co-Creating API Security Focus Points

By organizing in a Center of Excellence, the cybersecurity leaders from a dozen banks were able to come together for regular, monthly working sessions. Alloy Labs runs several Centers of Excellence covering a wide array of topics. The goal of every group is to share the knowledge and workload required to develop tangible resources that can be used at each of the members' institutions internally.

For this project, the Cyber group enlisted the help of the Alliance's consultant, Crowe, LLP, a public accounting, consulting, and technology firm.

Crowe worked with the Alliance's Cyber group through a series of discussions. These discussions focused on the API Top 10 list of security vulnerabilities developed by the Open Web Application Security Project® (OWASP) as a framework. The resulting questionnaire is comprised of over forty security questions broken down into two categories: initial/ongoing due diligence and event-driven due diligence.

Using This Questionnaire

This questionnaire is for informational purposes only. It is designed to provide considerations for a bank's approach to hardening third party APIs, though each institution is responsible for establishing its own policies in accordance with their unique needs and risk policies.

These questions may aid in banks' efforts to craft their own API security strategies. The questionnaire can be used to solicit information from vendors and technology providers about the security of their APIs. It can also be provided to a bank's internal teams to help them gauge connectivity requests before they're submitted to the bank's security team. Finally, the questions may aid in banks' efforts to craft their own API security strategy strategies.

API Security Questionnaire

Initial/Ongoing Due Diligence Questionnaire

General API Security	
Initial Vendor Questions	1. What is the process to perform API security reviews? 2. Is manual code security testing on APIs performed by qualified personnel with expertiseN in both development and code security? 3. Who is allowed to provision and manage access to the API? 4. Is data encrypted in transit within the API for both request and response?
OWASP API Security	
Broken Object Level Authorization	1. How is separation of data for multiple clients established and maintained? (Only if hosted) 2. Are user/client identifiers randomized and/or protected to prevent guessing or enumeration?
Broken User Authentication	1. What methods of API authentication are available? (OAuth2, OpenID, SAML, OAuth, JWT, TLS, Basic Auth) 2. Is MFA available to protect API access?
Excessive Data Exposure	1. Do access controls allow for control over what data a user receives when making an API request? 2. What sensitive data or PII will be accessible through API requests?
Lack of Resources & Rate Limiting	1. Is a limit in place to restrict the rate of API requests? 1a. Can this limit be changed based on business need? 2. Is a file or payload size limit in place throughout the API?

Broken Function Level Authorization	1. How is access to admin connections provisioned and established? 2. What additional security controls are available to protect administrative sessions?
Mass Assignment	1. Is a method for bulk upload of data available? 1a) What format is this data expected to be in? (JSON, XML, CSV)
Security Misconfiguration	1. Is HTTPS enabled for all APIs? 2. Are either TLS 1.2 or 1.3 used for Encrypting all APIs used? 3. Are security reviews performed for all systems supporting APIs? (Only if hosted) 4. Is IP control available to control access to the API?
Injection	1. Is documentation available for all API calls including request and response information? (Swagger Documentation or equivalent)
Improper Assets Management	1. Are multiple versions of the API available for external use? (Test, Prod, Old) (Only if hosted) 1a. If multiple versions are available, is a life cycle document maintained with EOL dates? 2. What systems and software will be required to support the API? (Windows Server, SQL, etc.) (Only if on-premise)
Insufficient Logging & Monitoring	1. Are failed and successful login attempts logged and available for review? 2. Are administrative activities logged and available for review? (Account creation, Account disabled, Change of user access) 3. Is user activity logged and available for review? 4. Is alerting available on failed security checks or inappropriate user activity?

Additional/Event-Driven Due Diligence

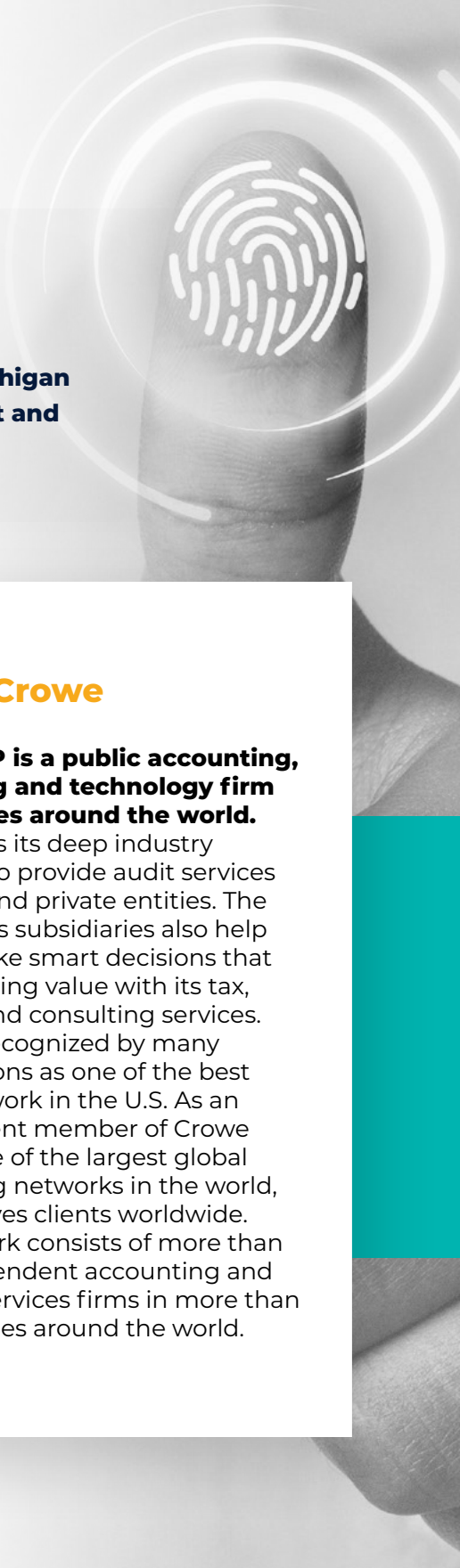
General API Security	
Initial Vendor Questions	1. Has a penetration test been performed against the API? 1a. Have any issues identified been addressed?

OWASP API Security	
Broken Object Level Authorization	1. Are IDs used to determine resource access? (/api/client1/financial_info) 1a. Can these IDs be easily guessed or brute forced?
Broken User Authentication	1. Can unused methods of authentication be disabled? 2. Is a method available for sessions to be terminated causing the token to be invalid? 3. Can MFA or other additional security be configured on specific high risk commands?
Excessive Data Exposure	1. Are schemas reviewed on a regular basis to remove any unnecessary data from responses?
Lack of Resources & Rate Limiting	1. Is DoS protection in place for the API and supporting systems? (Only if hosted) 2. Are checks in place to monitor for high compression ratios on uploaded files?
Broken Function Level Authorization	1. Does all admin functionality require confirmation of authorization through additional access checks?
Mass Assignment	1. Are properties configured to read-only where possible in object schemas and how are these values reviewed?

Security Misconfiguration	1. Are vulnerability scans run on a regular basis against underlying systems and the API? (Only if hosted) 2. What is the timeframe in which identified issues are patched or addressed?
Injection	1. Is all input validated, filtered and sanitized before being utilized or stored?
Improper Assets Management	1. Is an inventory maintained of all systems that are in place to support API functionality? (Only if hosted) 2. Is an API firewall in place to controls and monitor API calls? (Only if hosted)
Insufficient Logging & Monitoring	1. Can logs be exported or forwarded on a regular basis to support other logging or SIEM platforms? 2. Are logs on the system in a read only format and/or are changes to the logs alerted on?

Special thanks to the Alloy Labs member banks that participated in developing this tool:

- **American State Bank**
- **American State Bank & Trust**
- **Citizens & Northern Bank**
- **Capital Community Bank**
- **Columbia Bank**
- **Gate City Bank**
- **Horicon Bank**
- **Liberty Bank**
- **Locality Bank**
- **Mercantile Bank of Michigan**
- **Union Bank of Vermont and New Hampshire**



About the Alloy Labs Alliance

Alloy Labs is a member-driven shared innovation lab that helps banks operationalize innovation. Leveraging the network effects of over 50 institutions, our members are able to reduce risks, lower costs, and shorten the time between ideas and results. We do this by generating proprietary insights, developing partnerships, and making strategic investments. Alloy Labs also operates The Concept Lab, a reverse accelerator that helps banks cement relationships with startups accepted into the program, and the Alloy Alchemist Fund, a strategic investment group that invests in startup partners. For more information visit www.alloylabs.com.

About Crowe

Crowe LLP is a public accounting, consulting and technology firm with offices around the world. Crowe uses its deep industry expertise to provide audit services to public and private entities. The firm and its subsidiaries also help clients make smart decisions that lead to lasting value with its tax, advisory and consulting services. Crowe is recognized by many organizations as one of the best places to work in the U.S. As an independent member of Crowe Global, one of the largest global accounting networks in the world, Crowe serves clients worldwide. The network consists of more than 200 independent accounting and advisory services firms in more than 130 countries around the world.