API Discovery

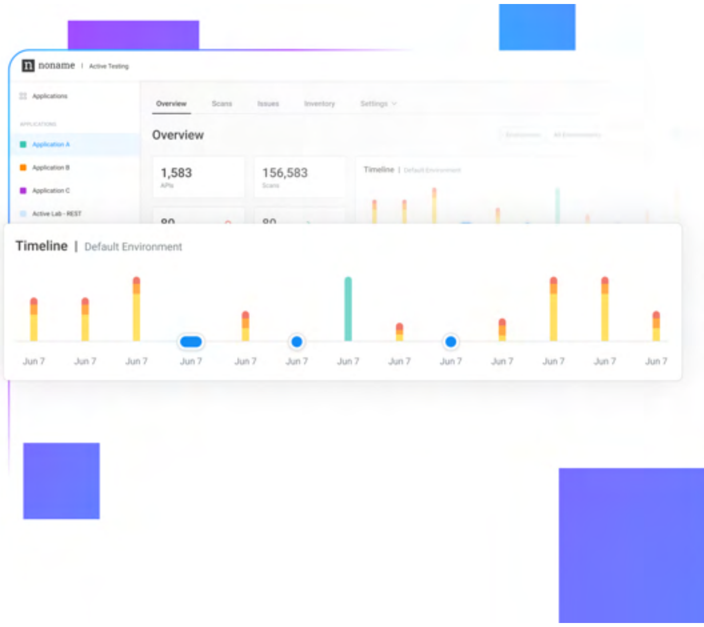
API Posture Management

API Runtime Protection

API Security Testing

Security Testing

API Security Testing goes a long way in avoiding API breaches by preventing security vulnerabilities from ever reaching production environments. Noname Active Testing focuses on finding and remediating API security vulnerabilities during the development phase of the SDLC, before they can be exploited.



Why you need API Security Testing

The earlier you catch security vulnerabilities, the better. From both a cost perspective and remediation angle, it is much easier to correct issues during the development process of the API than after it has been released into production and is being actively used. It allows organizations to more confidently and efficiently deliver applications to the business and remain competitive securely.

Noname Security API Security Testing

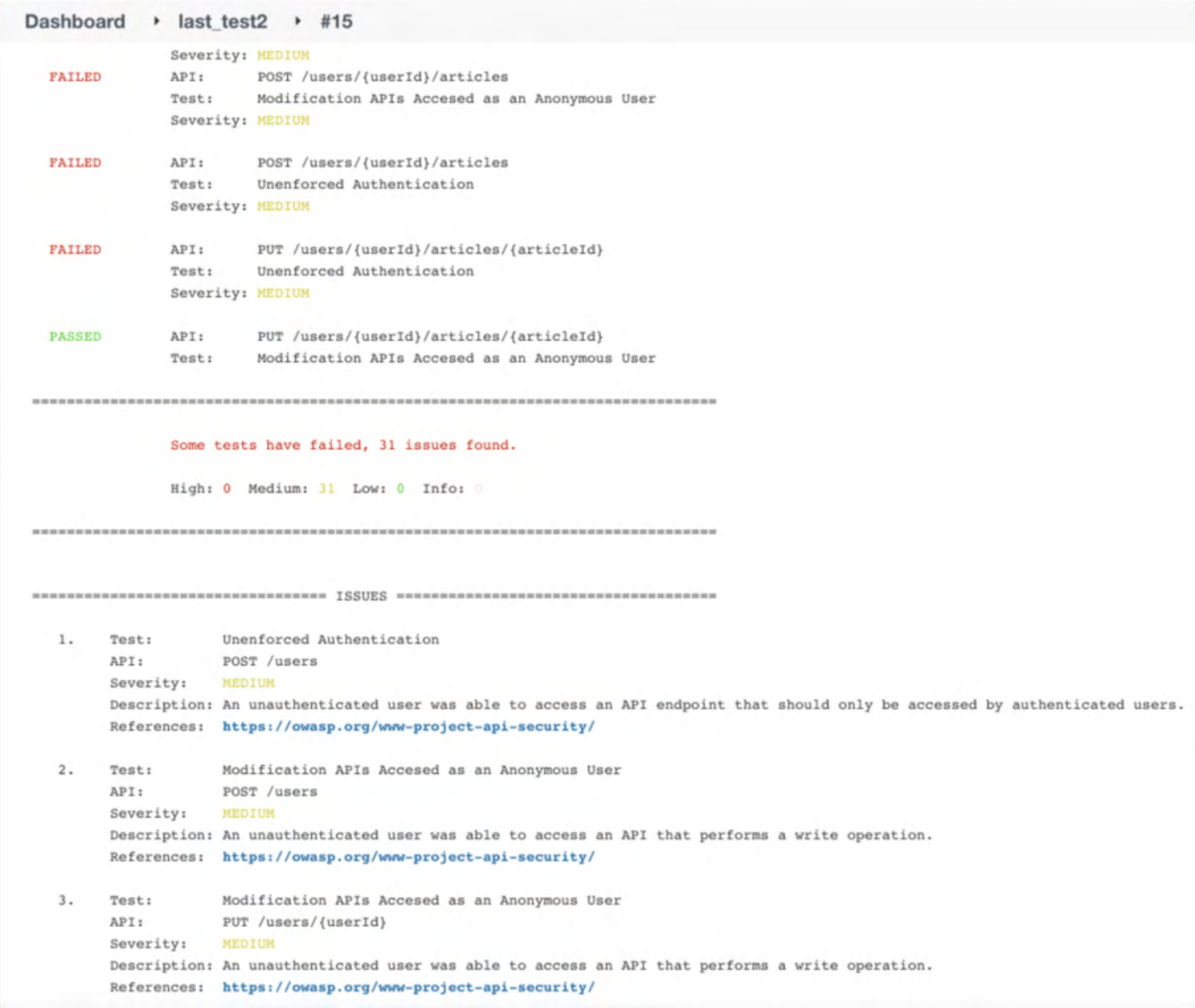
Noname ensures that no API is left untested. We brought years of experience in production API security over to a pre-production solution to uncover sophisticated API security vulnerabilities using API-specific tests resulting in findings commonly missed by existing DAST solutions. Our world-class auto-reachability ensures all pieces of the API endpoints are sufficiently tested for vulnerabilities and remediations presented. Active Testing seamlessly integrates with existing developer workflows using CI/CD tooling to avoid unnecessary workflow changes or delays in testing for API security.

Using Noname Security Active Testing, you can:

- ✓ Reduce remediation costs by 10x to 100x by finding issues earlier
- ✓ Reduce refactoring costs
- ✓ Improve code quality without sacrificing speed
- ✓ Increase revenue by accelerating time to market

Remediation

Security vulnerabilities exposed through Active Testing will automatically be exposed to the development team either during the build process or via integrations with tools like Jira. With vulnerabilities exposed in context, developers can efficiently remediate issues immediately instead of refactoring after sensitive data have been put at risk or exploited.



Dashboard ‣ last_test2 ‣ #15

```
                Severity: MEDIUM
  FAILED        API:      POST /users/{userId}/articles
                Test:     Modification APIs Accesed as an Anonymous User
                Severity: MEDIUM

  FAILED        API:      POST /users/{userId}/articles
                Test:     Unenforced Authentication
                Severity: MEDIUM

  FAILED        API:      PUT /users/{userId}/articles/{articleId}
                Test:     Unenforced Authentication
                Severity: MEDIUM

  PASSED        API:      PUT /users/{userId}/articles/{articleId}
                Test:     Modification APIs Accesed as an Anonymous User

===============================================================================

                Some tests have failed, 31 issues found.

                High: 0  Medium: 31  Low: 0  Info: 0

===============================================================================


================================== ISSUES =====================================

   1.    Test:        Unenforced Authentication
         API:         POST /users
         Severity:    MEDIUM
         Description: An unauthenticated user was able to access an API endpoint that should only be accessed by authenticated users.
         References:  https://owasp.org/www-project-api-security/

   2.    Test:        Modification APIs Accesed as an Anonymous User
         API:         POST /users
         Severity:    MEDIUM
         Description: An unauthenticated user was able to access an API that performs a write operation.
         References:  https://owasp.org/www-project-api-security/

   3.    Test:        Modification APIs Accesed as an Anonymous User
         API:         PUT /users/{userId}
         Severity:    MEDIUM
         Description: An unauthenticated user was able to access an API that performs a write operation.
         References:  https://owasp.org/www-project-api-security/
```

About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across four pillars — Discovery, Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in London.

nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371