

User Manual2

Version: Final (2025-09-29) — Matches the shipped system: React UI, Express API, Python scan engine (TCP), Supabase.

AT-AT — Comprehensive User Manual

Table of Contents

1. [Overview](#)
2. [Quick Start](#)
3. [Signing In & Account Access](#)
 - o 3.1 [Login](#)
 - o 3.2 [Create an Account](#)
 - o 3.3 [Forgot / Reset Password](#)
4. [Home](#)
5. [Dashboard](#)
 - o 5.1 [Metrics](#)
 - o 5.2 [Running Scans](#)
 - o 5.3 [Quick Actions](#)
6. [Managing APIs](#)
 - o 6.1 [Add API \(manual\)](#)
 - o 6.2 [Import OpenAPI \(JSON/YAML\)](#)
 - o 6.3 [Endpoints & Details](#)
 - o 6.4 [Tags & Flags](#)
 - o 6.5 [Sharing](#)
 - o 6.6 [Scheduling Scans](#)
7. [History & Reports](#)
8. [Settings](#)
9. [Help, Privacy & Terms](#)
10. [Troubleshooting](#)

11. [FAQ](#)
 12. [Keyboard & Productivity Tips](#)
 13. [Glossary](#)
-

1. Introduction

APIs have become a critical component of modern software systems, enabling seamless data exchange and integration across applications. However, this growing reliance on APIs also increases their exposure to security threats such as unauthorized access, data breaches, and injection attacks. The API Threat Assessment Tool provides a comprehensive solution for identifying, analyzing, and mitigating these risks. This manual introduces the tool, outlines its features, and guides you through its installation, configuration, and usage to ensure your APIs remain secure and compliant with industry standards.

1.1. Purpose of the Tool

The API Threat Assessment Tool is designed to help developers, security analysts, and system administrators identify, assess, and mitigate potential security risks in APIs. With the increasing reliance on APIs for application integration and data exchange, ensuring their security is critical to prevent data breaches and maintain system integrity.

1.2. Why It's Important

APIs are a common target for cyberattacks, such as injection attacks, broken authentication, and data exposure. This tool addresses these threats by providing automated scanning, threat detection, and actionable security recommendations.

1.3. Key Features

- Users can import an API specification either by uploading a YAML or JSON file or by entering API details manually.
- Add and manage endpoints and tags to ensure all relevant parts of the API are included in the assessment.
- Scan the API against the OWASP Top 10 API Security Risks, either all at once for a complete assessment or individually for targeted checks.
- Generates a comprehensive security report after each scan, highlighting vulnerabilities and providing

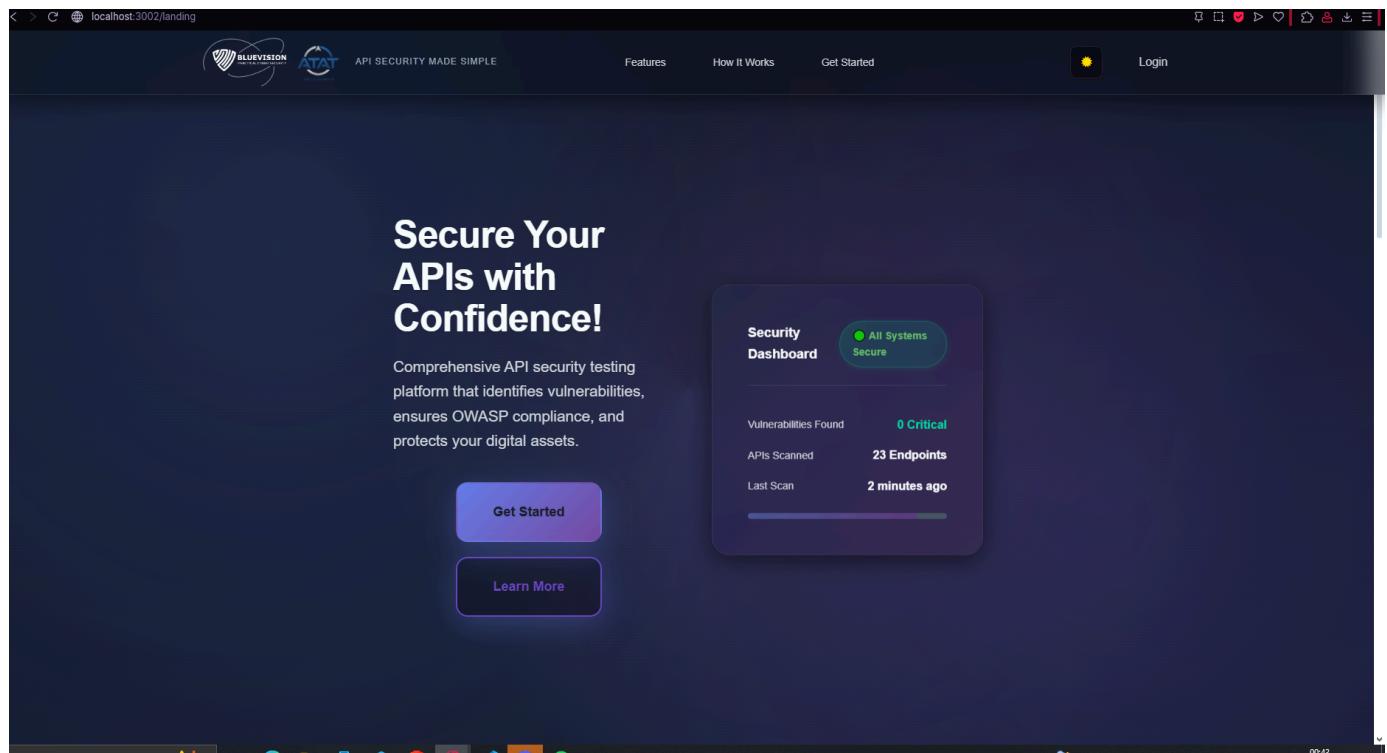
actionable recommendations. • Ability to select specific security checks based on your organization's priorities or compliance requirements. API Threat Assessment Tool – User Manual

1.4. Scope of the Manual

This manual will guide you through the configuration and usage of the API Threat Assessment Tool, enabling you to protect your APIs from common and emerging threats effectively. NB – For ease of use, Chrome and Microsoft Edge browsers are recommended.

- **You bring:** your API spec (OpenAPI).
- **AT-AT provides:** guided workflows for **importing, scanning, reviewing results, tagging/flagging, and sharing** summaries.

Supported browsers: latest Chrome or Edge (recommended).

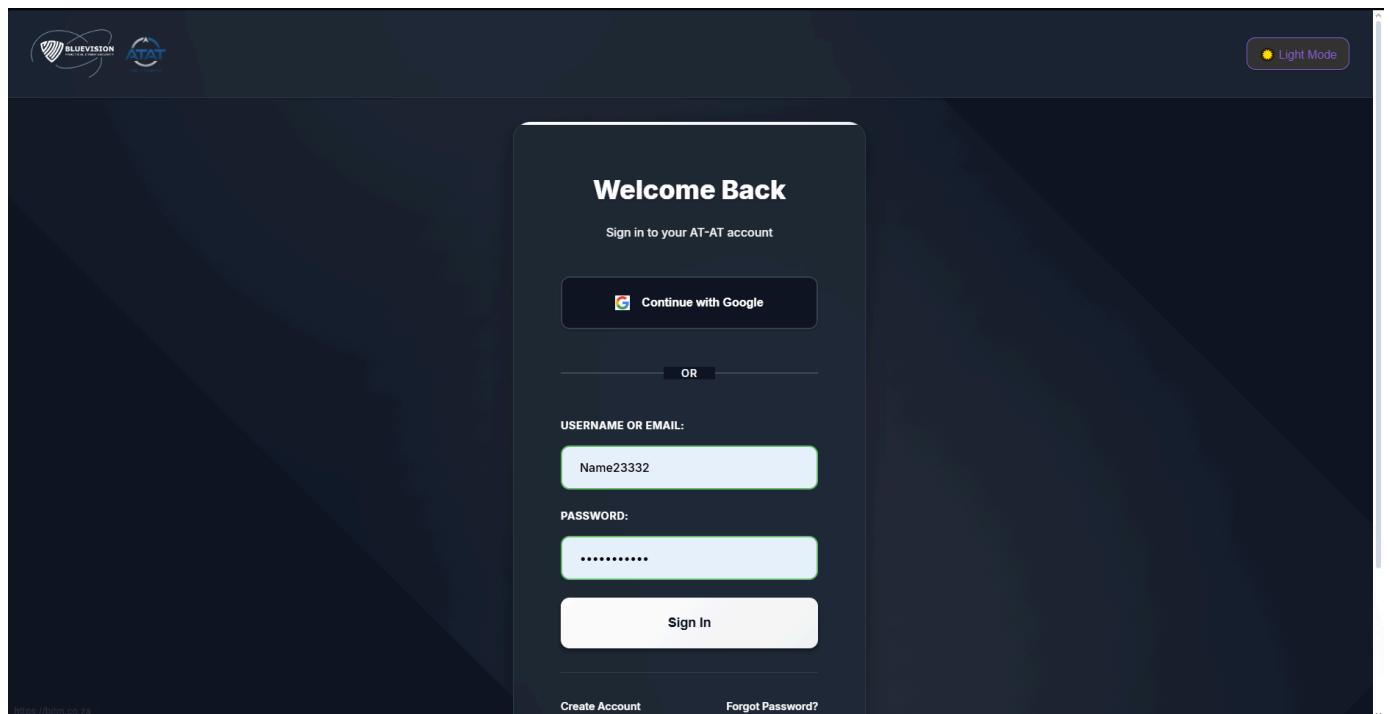


Quick Start

1. **Sign in or create an account.**
2. **Import** your API (OpenAPI JSON/YAML) or **Add API** details manually.
3. **Start a scan** using a profile/check set.
4. **Monitor progress** and **view results**.
5. Use **tags/flags** to triage; **share** summaries if needed.

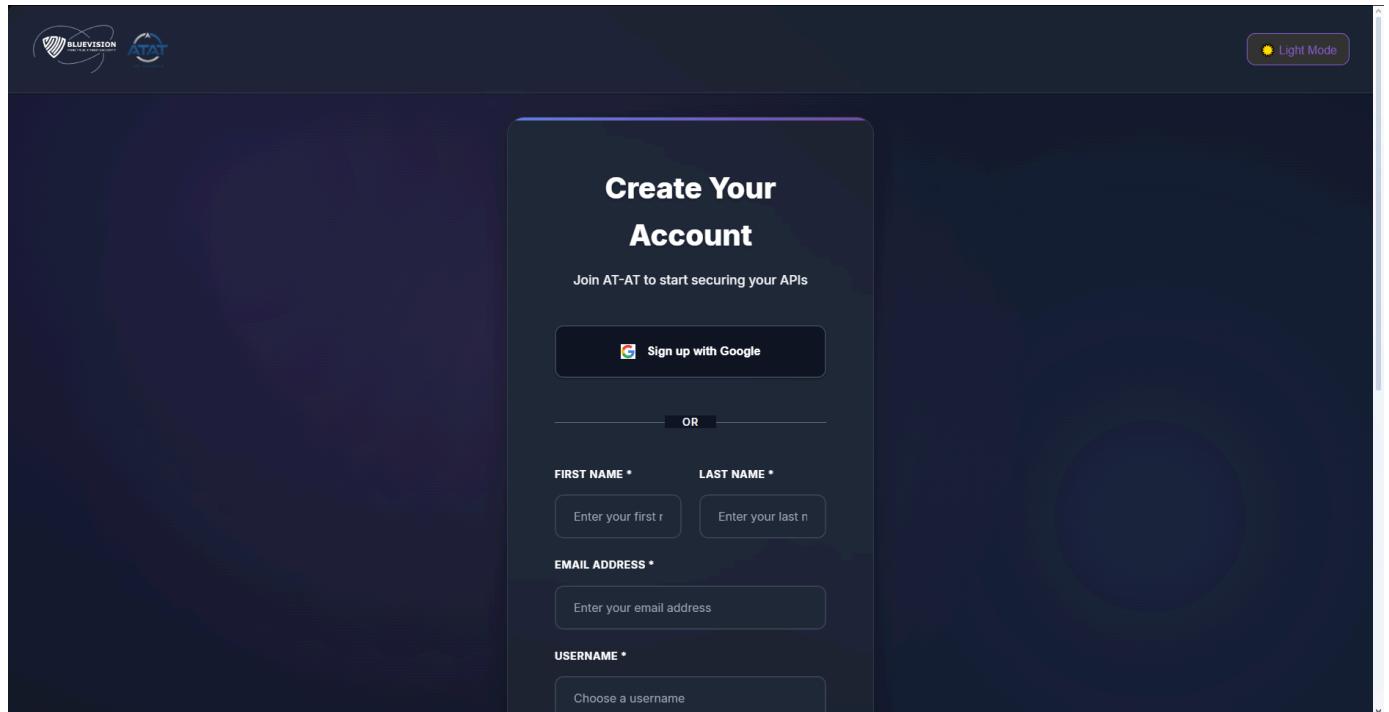
Signing In & Account Access

Login



- Enter **email/username** and **password**.
- Use **Forgot password** if you can't sign in.
- New here? Click **Create account**.

Create an Account



- Provide **first name**, **last name**, **email**, **username**, and **password**.

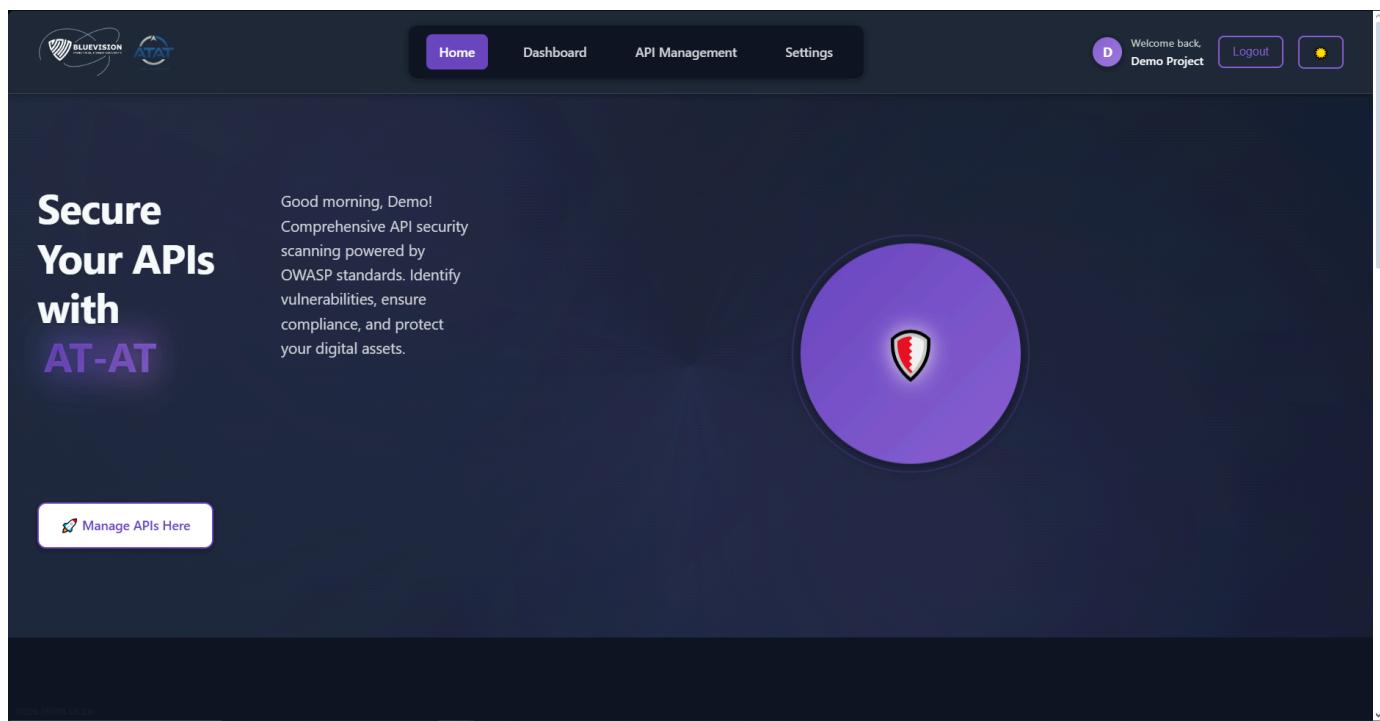
- Accept **Terms & Conditions** to complete registration.

Forgot / Reset Password

- **Forgot:** request a reset link; the app returns a generic success message (prevents user enumeration).
- **Reset:** open the link from your email and set a **new password**.
- Tokens are **one-time** and expire after **60 minutes**.

Home

The Home screen centralizes your primary actions.



- **Run a Scan** — launch the scan flow.
- **Explore Templates** — browse preconfigured check sets.
- **View Reports** — open recent results.
- **Manage APIs** — add/import and configure your APIs.

Dashboard

The Dashboard aggregates key indicators and provides shortcuts to run scans or view reports.

The screenshot shows the BlueVision Security Dashboard. At the top, there are two logos: 'BLUVEVISION' and 'AT&T'. The navigation bar includes links for Home, Dashboard (which is highlighted in purple), API Management, and Settings. On the right, there's a welcome message 'Welcome back, Demo Project', a 'Logout' button, and a yellow circular icon with a question mark.

Security Dashboard

Good morning, Demo! Here's an overview of your API security posture.

Key metrics displayed:

- Total APIs Managed: 6
- Total Scans: 9
- Vulnerabilities: 282
- Critical Alerts: 0

Weekly Activity

Metrics

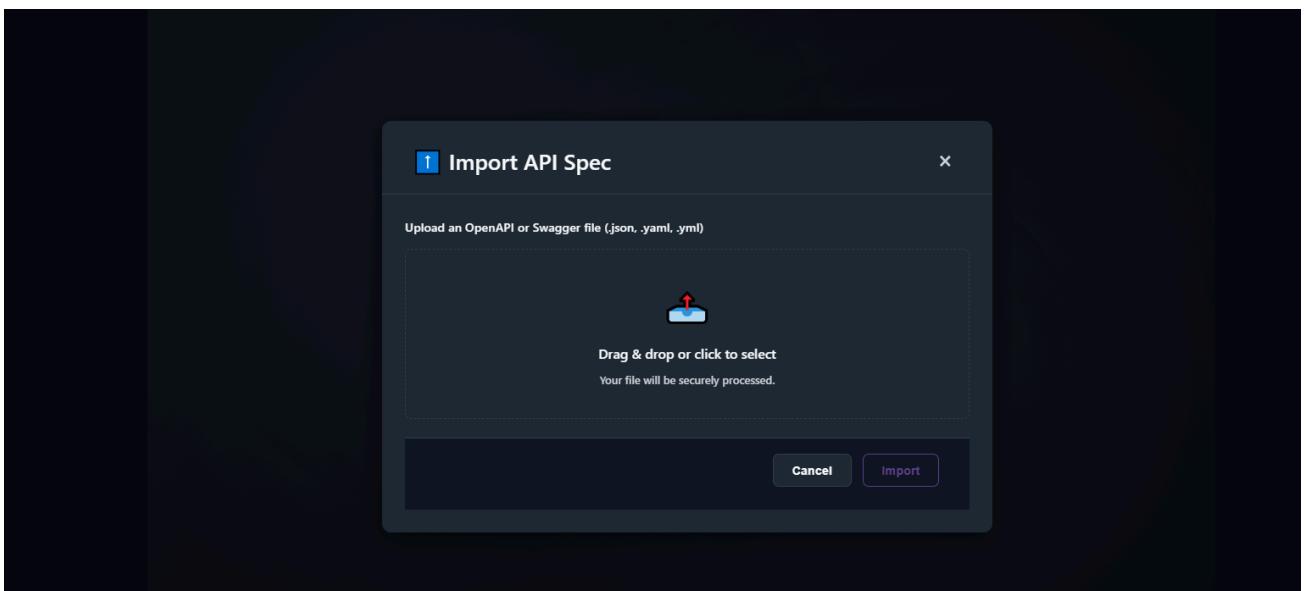
See high-level stats, recent activity, and quick links to frequent actions.

Running Scans

Configure a Scan

From Dashboard or API pages:

1. Select an **API**.

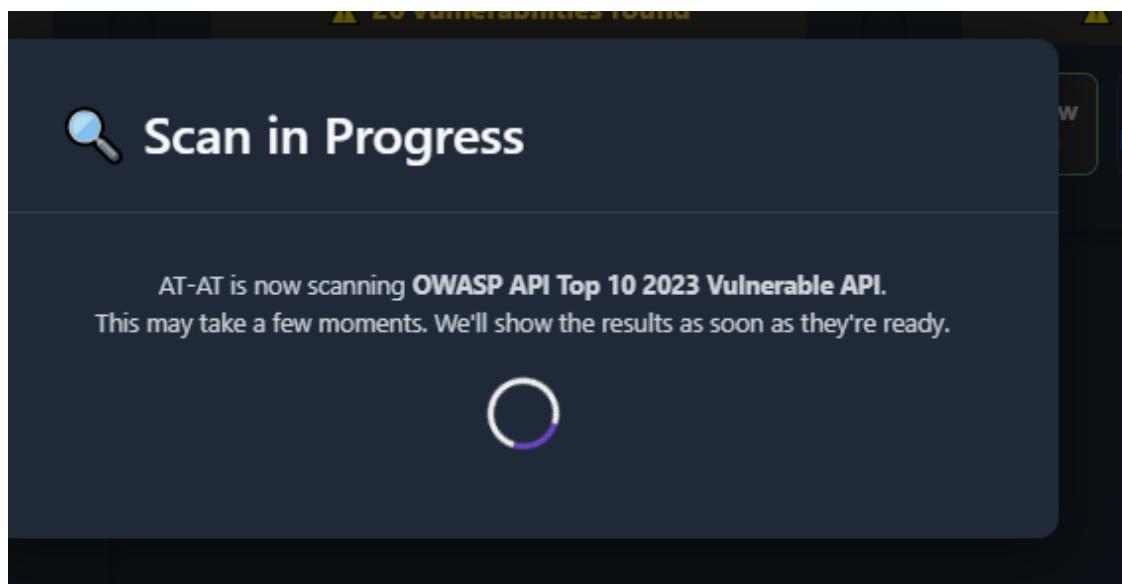


2. Choose a **profile** or **checks**.

3. Click **Start Scan**.

Monitor Progress

- Watch status updates during execution.



Quick Actions

- **Manage APIs** — go to API management
- **Scan Templates** — open template library
- **Account Settings** — update your profile
- **Documentation** — open help resources

Managing APIs

Centralize all the APIs you assess: import, edit, and organize.

The screenshot shows the 'API Management' section of a web application. At the top, there are navigation links for 'Home', 'Dashboard', 'API Management' (which is highlighted in purple), and 'Settings'. On the right side, there's a user profile with a blue circle icon, the text 'Welcome back, Demo Project', a 'Logout' button, and a yellow circular icon. The main area features a dark background with a central banner containing the text 'API Management' in large white letters. Below the banner is a sub-section with the text 'Centrally manage your API endpoints, configure security scans, and monitor your API ecosystem.' and a 'Import API Spec' button. At the bottom of the screen, there are three large, semi-transparent buttons with icons: a keyhole for 'Edit Details', a heart for 'Share Access', and a calendar for 'Schedule Scan'.

Add API (manual)

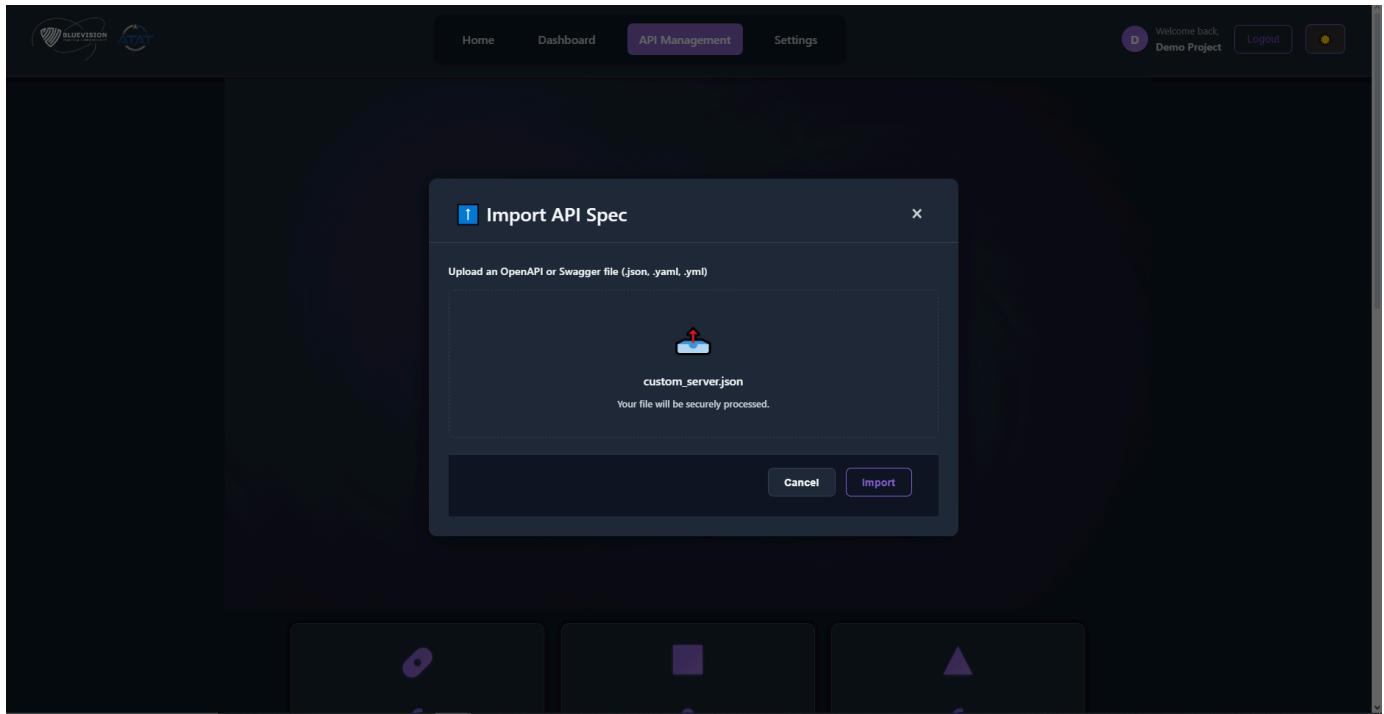
Click **Add API** and enter the basics:

- **Name, Base URL, Description** (optional)

The screenshot shows a modal dialog titled 'Manage API: OWASP API' with a subtitle 'Top 10 2023 Vulnerable API'. The dialog has a dark background and contains the message 'Select a configuration option to proceed.' Above this message are three rounded rectangular buttons: 'Edit Details' (with a pencil icon), 'Share Access' (with a heart icon), and 'Schedule Scan' (with a calendar icon). At the bottom of the dialog, there is a red-bordered box containing a warning titled 'Danger Zone' with the text 'This action is permanent and cannot be undone.' A large red button at the bottom with a trash can icon and the text 'Delete this API' is prominently displayed.

Import OpenAPI (JSON/YAML)

Import a **.json** or **.yaml/.yml** OpenAPI file. The app validates file type/size and parses endpoints.



Tips

- Keep your spec valid (use an OpenAPI linter if possible).
- Large specs import faster if you remove unneeded examples/schemas.

Endpoints & Details

Review endpoints derived from your spec: method, path, parameters, and descriptions.

📁 Endpoints for OWASP API Top 10 2023

X

Vulnerable API

GET /

Read Root

GET /api/BOLA/profile/{user_id}

Get User Profile

GET /api/BOLA/{user_id}/invoice/{invoice_id}

Get User Invoice

GET /api/BOLA/purchase

Get Purchase

GET /api/BOLA/ticket

Get Ticket

POST /api/BKEN_AUTH/login

Login

POST /api/BKEN_AUTH/reset-password

Tags & Flags

Use **tags** to categorize, and **flags** to highlight priority items.

▶ Configure Flags for Scan

X

Search by method or path...

GET /

BOLA BKEN_AUTH BOPLA URC BFLA UABF
 SSRF SEC_MISC IIM UC API SKIP

GET /api/BOLA/profile/{user_id}

BOLA BKEN_AUTH BOPLA URC BFLA UABF
 SSRF SEC_MISC IIM UC API SKIP

GET /api/BOLA/{user_id}/invoice/{invoice_id}

BOLA BKEN_AUTH BOPLA URC BFLA UABF
 SSRF SEC_MISC IIM UC API SKIP

GET /api/BOLA/purchase

BOLA BKEN_AUTH BOPLA URC BFLA UABF
 SSRF SEC_MISC IIM UC API SKIP

GET /api/BOLA/ticket

BOLA BKEN_AUTH BOPLA URC BFLA UABF
 SSRF SEC_MISC IIM UC API SKIP

← Prev

Page 1 of 2

Next →

Cancel

Start Scan

[Privacy Policy](#)

[Terms of Service](#)

[Documentation](#)

[Contact Us](#)

Sharing

Share summaries where appropriate (e.g., to your team).

Share "OWASP API Top 10 2023 Vulnerable API" ×

Currently Shared With

- K1LLSHOT_007henrumatthis@gmail.com

read

[Revoke](#)

Share with New User

User Email Address

user@example.com

Permission Level

Read-Only

[Cancel](#)

[Share API](#)

Scheduling Scans

Schedule recurring scans if your build supports it.



Scheduled Scanning for OWASP API Top 10 2023



Vulnerable API

A scan is currently scheduled to run **daily**.

Next run is estimated for:

9/30/2025, 12:48:23 AM

[Disable Schedule](#)

View Results & Reports

When complete, open the report to inspect findings.

Scan Report for OWASP API Top 10 2023

X

Vulnerable API

31

Total Vulnerabilities

15

High Severity

15

Medium Severity

1

Low Severity

Scanned on: 9/29/2025, 2:46:33 AM

Duration: 2.43 seconds

HIGH 1. Broken Object Level Authorization

/api/BOLA/profile/2 +

Description:

Endpoint allows us to access data of other users by tampering with id's

Recommendation:

Properly authenticate before returning data

Method:

GET

CVSS Score:

10

Full Evidence:

Method: GET
Path: /api/BOLA/profile/2
Parameters: {}

HIGH 1. Broken Object Level Authorization

/api/BOLA/1/invoice/1 +

Download Report

Close

- Group by **risk/test** or **endpoint**.
- Drill down to see **evidence** and guidance.
- Export **HTML/JSON** where available. (*PDF export is not part of this build.*)

History & Reports

Browse past scans, filter by API or date, and re-open reports.

The screenshot shows a dark-themed web interface for managing scan history. At the top, there's a header with a document icon and the text "Scan History for OWASP API Top 10 2023". Below the header, the title "Vulnerable API" is displayed. In the center, there's a summary box containing the date "9/29/2025, 2:46:33 AM" and the ID "f31e66573f4b4f4e856ee3b310098422". To the right of the ID are three buttons: "View", "Executive Report", and "Technical Report". A close button ("X") is located in the top right corner of the main content area.

Tip: Use tags/flags to curate a shortlist for review meetings.

Settings

Update your profile, change your password, and adjust preferences.

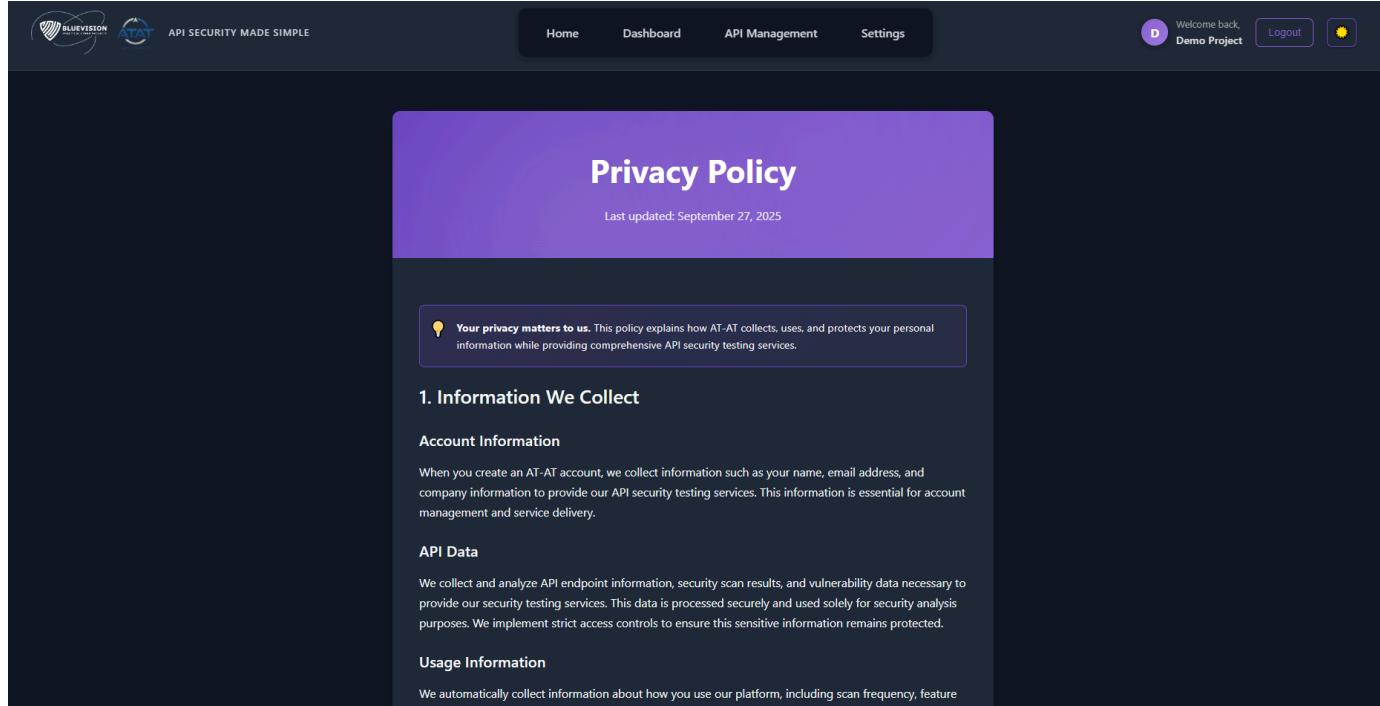
The screenshot shows a dark-themed settings page. At the top, there's a navigation bar with links for "Home", "Dashboard", "API Management", and "Settings" (which is highlighted). On the far right of the top bar, there's a user profile icon with "Welcome back, Demo Project" and "Logout" buttons. Below the top bar, there's a large sidebar with the title "Account Settings". To the right of the sidebar, there's a text message: "Good morning, Demo! Manage your account preferences, security settings, and notification options." At the bottom of the page, there are four tabs: "Profile", "Notifications", "Security", and "Preferences".

- **Profile:** name, email (verification may be required for changes)
- **Security:** change password
- **Preferences:** theme and UI options
- **Notifications:** enable/disable categories

Help, Privacy & Terms

Access help resources and review your legal documents.

Privacy Policy



The screenshot shows the 'Privacy Policy' page. At the top, there's a dark header bar with the BlueVision AT-AT logo, the tagline 'API SECURITY MADE SIMPLE', and navigation links for 'Home', 'Dashboard', 'API Management', and 'Settings'. On the right, there's a user profile icon with 'D' and 'Welcome back, Demo Project', a 'Logout' button, and a sun icon. The main content area has a purple header 'Privacy Policy' and a sub-header 'Last updated: September 27, 2025'. Below this is a callout box with a lightbulb icon and the text: 'Your privacy matters to us. This policy explains how AT-AT collects, uses, and protects your personal information while providing comprehensive API security testing services.' The main content is divided into sections: '1. Information We Collect', 'Account Information', 'API Data', and 'Usage Information'. Each section contains descriptive text and a small note at the bottom.

Privacy Policy

Last updated: September 27, 2025

Your privacy matters to us. This policy explains how AT-AT collects, uses, and protects your personal information while providing comprehensive API security testing services.

1. Information We Collect

Account Information

When you create an AT-AT account, we collect information such as your name, email address, and company information to provide our API security testing services. This information is essential for account management and service delivery.

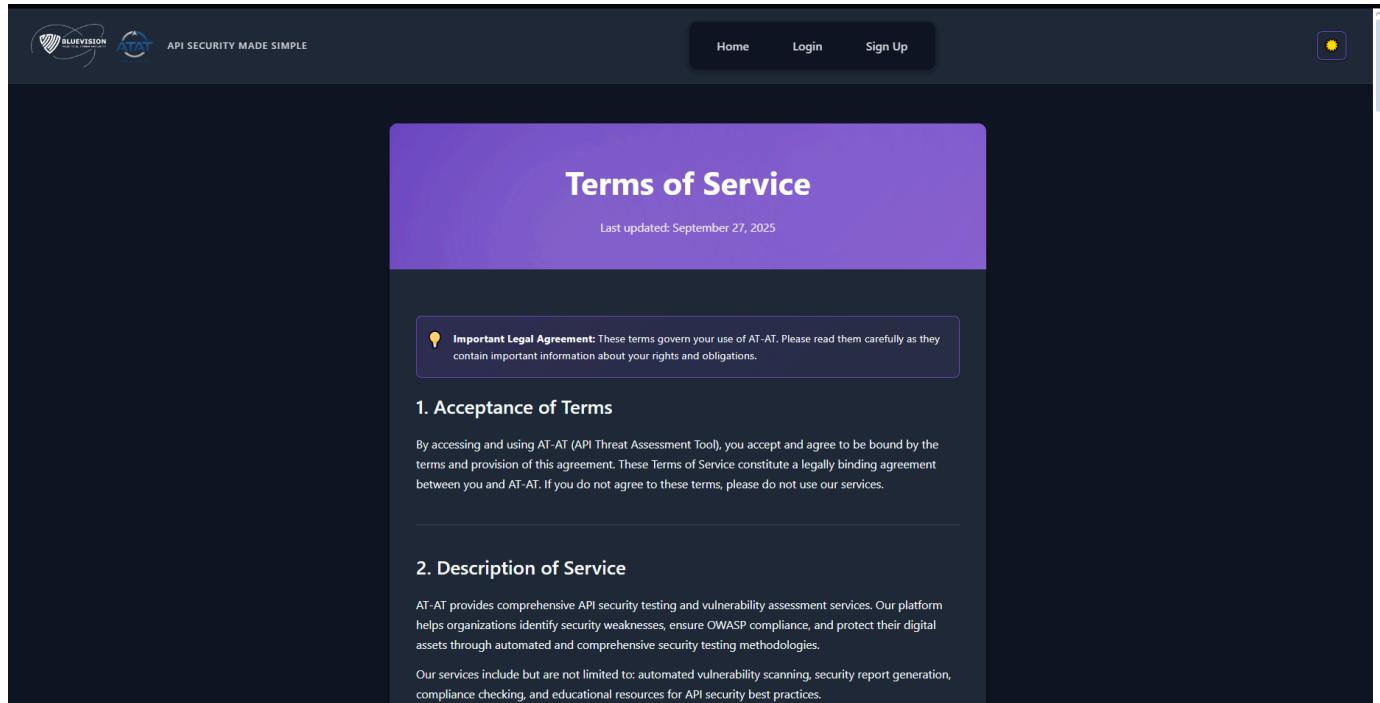
API Data

We collect and analyze API endpoint information, security scan results, and vulnerability data necessary to provide our security testing services. This data is processed securely and used solely for security analysis purposes. We implement strict access controls to ensure this sensitive information remains protected.

Usage Information

We automatically collect information about how you use our platform, including scan frequency, feature

Terms of Service



The screenshot shows the 'Terms of Service' page. It has a similar dark header bar with the BlueVision AT-AT logo, tagline, and navigation links ('Home', 'Login', 'Sign Up'). On the right, there's a user profile icon with 'D' and 'Welcome back, Demo Project', a 'Logout' button, and a sun icon. The main content area has a purple header 'Terms of Service' and a sub-header 'Last updated: September 27, 2025'. Below this is a callout box with a lightbulb icon and the text: 'Important Legal Agreement: These terms govern your use of AT-AT. Please read them carefully as they contain important information about your rights and obligations.' The main content is divided into sections: '1. Acceptance of Terms' and '2. Description of Service'. Each section contains descriptive text and a small note at the bottom.

Terms of Service

Last updated: September 27, 2025

Important Legal Agreement: These terms govern your use of AT-AT. Please read them carefully as they contain important information about your rights and obligations.

1. Acceptance of Terms

By accessing and using AT-AT (API Threat Assessment Tool), you accept and agree to be bound by the terms and provision of this agreement. These Terms of Service constitute a legally binding agreement between you and AT-AT. If you do not agree to these terms, please do not use our services.

2. Description of Service

AT-AT provides comprehensive API security testing and vulnerability assessment services. Our platform helps organizations identify security weaknesses, ensure OWASP compliance, and protect their digital assets through automated and comprehensive security testing methodologies.

Our services include but are not limited to: automated vulnerability scanning, security report generation, compliance checking, and educational resources for API security best practices.

Contact Us



Contact Us

We're here to help! Reach out to us for any questions, support, or feedback regarding the AT-AT platform.

💡 Need help? Choose the appropriate inquiry type below for faster response times, or contact us directly for general questions.

Get in Touch

Primary Contact

Email: atissue.capstone@gmail.com
We typically respond within 24-48 hours during business days.

[Send General Inquiry](#)

Inquiry Types

To help us route your inquiry efficiently, please select the appropriate category:

Troubleshooting

I can't log in

- Check your email/username and password.
- Use **Forgot password** to reset credentials.

Import failed

- Ensure the file is **.json** or **.yaml/.yml**.
- Validate your spec (OpenAPI 3.x recommended).
- Large specs: remove excessive examples or unused schemas.

No results after starting a scan

- Confirm the **engine** is running (if self-hosted).
- Re-open the **History** tab to check status; refresh if needed.

Screens look different

- You may be on a newer build; this manual targets the final Demo-4 release.

FAQ

Q: Do I need an OpenAPI file?

A: Yes. Scans are driven by your uploaded spec (JSON/YAML).

Q: Can I export PDF?

A: Not in this build. Use **HTML/JSON** exports where available.

Q: Are role-based permissions supported?

A: This build uses **JWT** on selected routes; fine-grained RBAC is out of scope.

Q: Can I schedule scans?

A: If your environment enables scheduling, the UI provides a Schedule option (see screenshot).

Keyboard & Productivity Tips

- **Search (/) or Ctrl/Cmd+K:** jump to features.
 - **Use tags/flags:** group hot items for triage.
 - **Open results in a new tab:** keep context while reviewing multiple endpoints.
-

Glossary

- **OpenAPI:** a standard for describing REST APIs.
 - **Endpoint:** an API method+path (e.g., GET /users).
 - **Tag/Flag:** labels to organize and prioritize items.
 - **Profile/Checks:** sets of security tests to run.
 - **Report:** the findings produced after a scan.
-

End of manual.