A Virtual Hacker to Secure your API

Solution Overview

The State of API Insecurity

There are 26 to 50 APIs in a typical modern application, and up to thousands of APIs in enterprise applications. But when did you last use a single app in your day-to-day work? Imagine now the number of APIs transferring your data while using those apps. To create a more vivid image, consider that large enterprises rely on as many as 25,000+ APIs. Therefore, saying that APIs extend the modern organization's attack surface is, indeed, an understatement.

At the end of 2022, there was a 400% increase in API attacks in just a few months. Research in 2023 showed that 92% of organizations faced an API incident within the last year. 60% had to mitigate the consequences of at least one API data breach. 63% of the overall HackerOne bug bounty rewards had to do with API security vulnerabilities.

The threat actors' focus is shifting increasingly to APIs, and that's for good reasons. API attacks:

- Give relatively easy access to invaluable user and organization data.
- Are cost-effective both in terms of time and money.
- Require remote, modest technical expertise.

No organization has been exempted from API exploits, from tech giants such as Twitter and Facebook to telcos such as T-Mobile and Optus to crypto exchanges such as Kronos Research. The consequences have ranged from financial losses and hefty fines to a severely affected reputation due to the leakage of sensitive user data.

So, the number of APIs in use is exploding, as are the API attacks. How can you fend off your assets against the threats innate to the inevitable increase in API use?

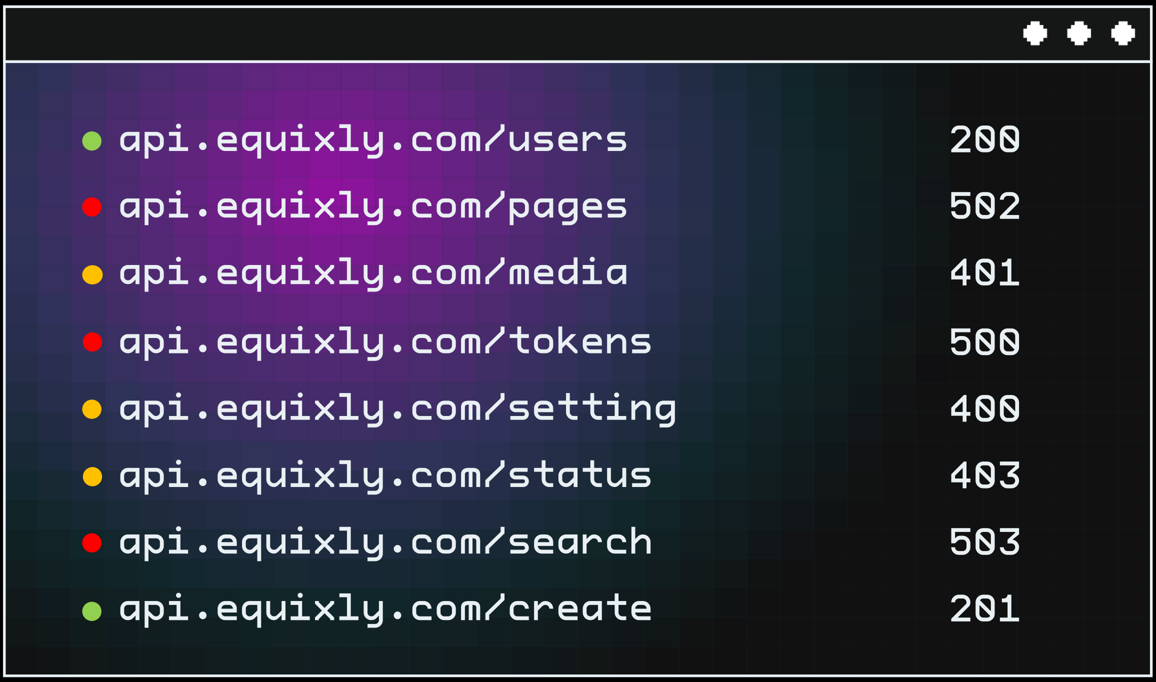
A Virtual Hacker

To protect APIs from hackers, you must see them through the eyes of hackers.

Equixly makes that possible via its AI-powered scanning abilities. It probes through your APIs, looking for nuanced logic flaws and subtle vulnerabilities in addition to those that simply cry to be discovered, just as a hacker would.

Equixly is a virtual hacker that takes the best of both worlds, the human and the machine, and unites them. It uses the same principles humans adhere to when attacking APIs: Equixly approaches APIs methodically to map out vulnerabilities specific to a given API, attempting to exploit them later in the process with your approval.

Like machines, thanks to its proprietary AI-driven algorithm, it does massive, automated work highly efficiently, saving precious time and resources. Its tests are easily repeatable, consistent, and independent of external factors such as expertise level, which are all among the grandest advantages of automated hacking, in this case, ethical hacking, that is, penetration testing.



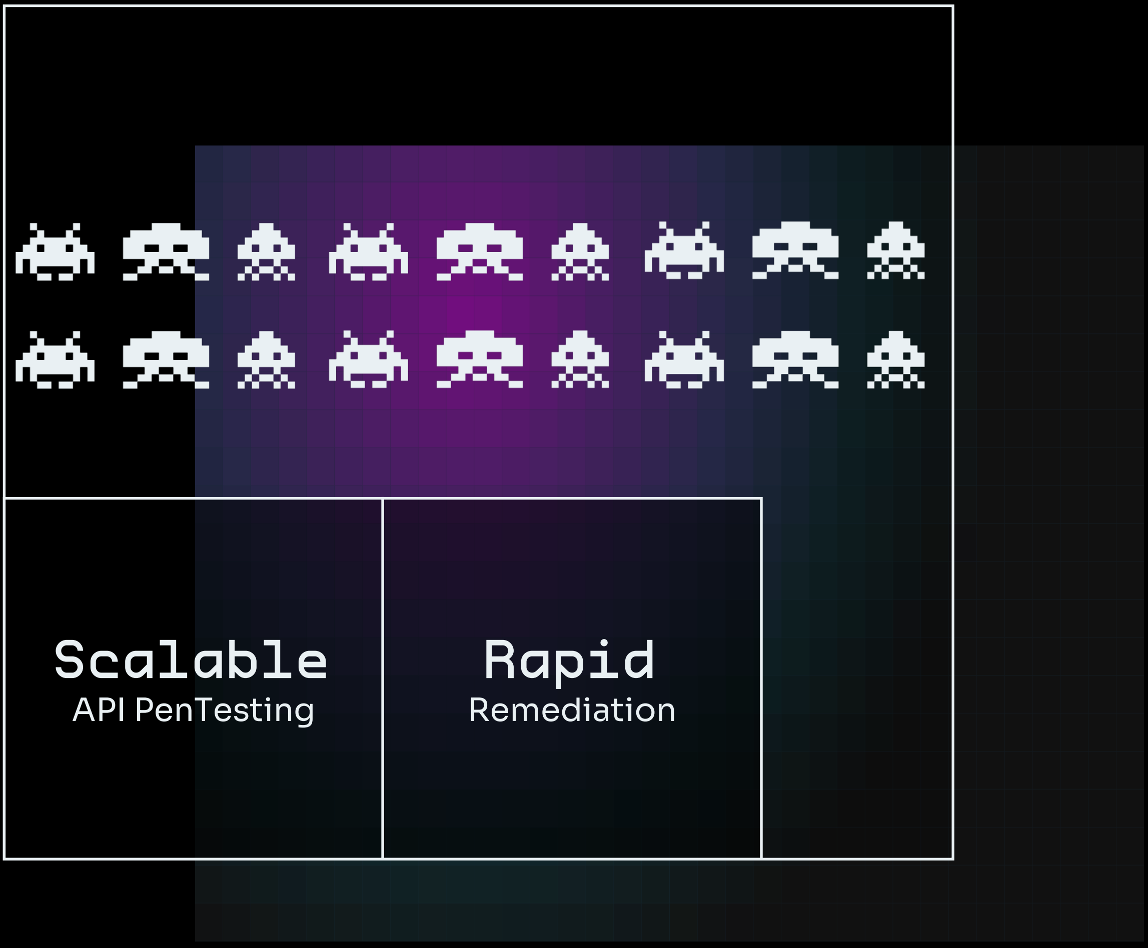
```
🟢 api.equixly.com/users      200
🔴 api.equixly.com/pages      502
🟡 api.equixly.com/media      401
🔴 api.equixly.com/tokens     500
🟡 api.equixly.com/setting    400
🟡 api.equixly.com/status     403
🔴 api.equixly.com/search     503
🟢 api.equixly.com/create     201
```

Test Continuously

However, hacking APIs with the consent of their owners is a late battle strategy. To win not just the battle but the war against API attackers, you must start at the beginning—in development.

Equixly fully endorses the shift-left testing approach. Accordingly, its creators developed it so you can integrate security testing early into the SDLC (software development life cycle) and continuously test throughout development. Equixly can test every new line of code at your convenience. The only code left untested is the one you never wrote.

By allowing you to test for vulnerabilities in development, Equixly can preclude the possibility of major flaws in production and help you avoid security fiascos that disrupt business continuity and require costly reparations in production.



Scalable
API PenTesting

Rapid
Remediation

Attack Your APIs

You can deploy Equixly to attack and shock-test your APIs in two ways: gray box and black box scenarios.

In the gray box scenario, the virtual hacker requires:

- The API base URL
- An API definition, i.e., OAS file in JSON or YAML format
- Setting up user profiles for testing purposes

Relying on the OAS file, Equixly investigates a myriad of API requests and responses. It shows summarized results in a straightforward and well-ordered dashboard, but you can also examine specific scans and issues separately for more details.

Equixly requires setting up user profiles to facilitate testing for vulnerabilities such as Broken Object Level Authorization (BOLA) and Broken Function Level Authorization (BFLA).

Speaking of BOLA and BFLA, the virtual hacker launches attack tests using the latest OWASP Top 10 API Security Risks list. This list of the most severe and common API vulnerabilities is the result of thorough research on API exploits in the wild, which OWASP continuously updates.

It's crucial to know that Equixly, as an automated penetration testing solution, widens the scope of attacks and testing. In our experience and calculations, a midsized API application with 40 endpoints takes as many as 154 hours (about six and a half days) to test approximately 40% of the inputs. Equixly goes far beyond this 40%, testing your APIs comprehensively and, more importantly, in a much shorter time.

In the black box scenario, the base URL and OAS file are still necessary, but Equixly does not receive access to user profiles. That implies that the results of black box attacks can be narrower in scope. However, if the virtual hacker discovers an existing critical authentication vulnerability, it could access a broader range of API information and produce better results.

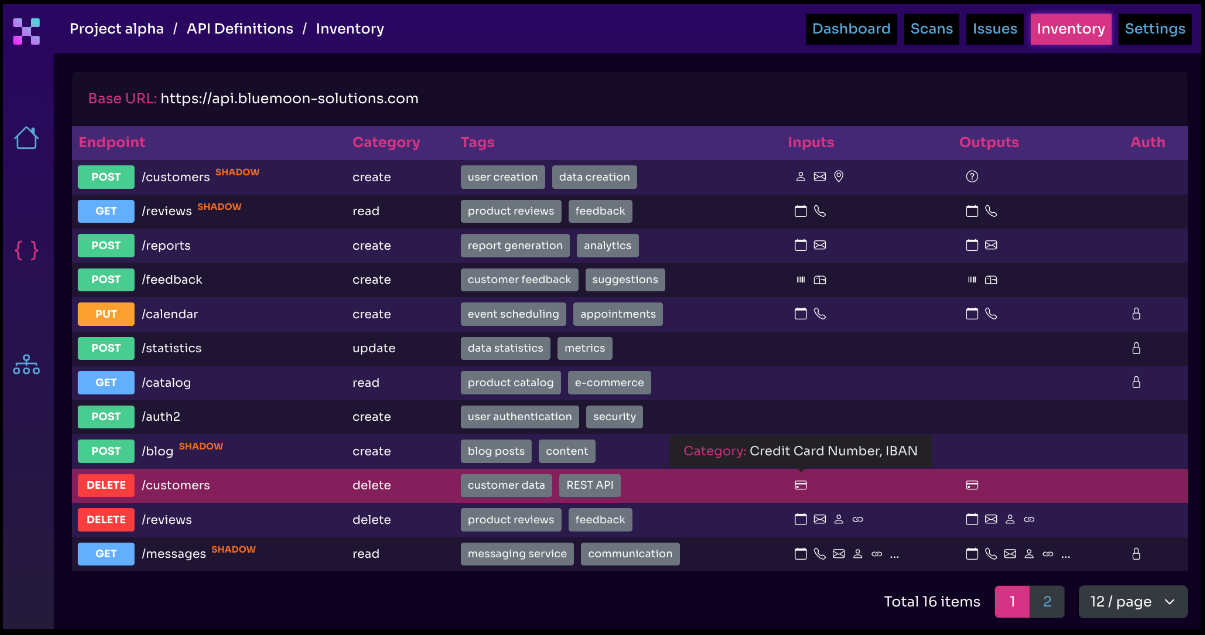
SOLUTION OVERVIEW

Map Your Attack Surface

Visibility is among the most desirable qualities in cybersecurity, and API security is no exception. If you know precisely how many APIs you have, their exact purpose, and what kind of data passes through their endpoints, you work with visible assets you can efficiently protect.

Equixly helps you discover shadow endpoints, which allows you to create a tidy inventory of the APIs in your information environment. It has a separate section where you can see these discoveries.

But Equixly doesn't stop there. It provides information on the data that traverses your endpoints, giving insight into which of them operate with sensitive data. Those endpoints may require stricter security measures and sturdier protection mechanisms, so it's always good to refer to Equixly for precise data classification.



Base URL: https://api.bluemoon-solutions.com

Endpoint	Category	Tags	Inputs	Outputs	Auth
POST /customers SHADOW	create	user creation, data creation	👤 ✉ 📍	?	
GET /reviews SHADOW	read	product reviews, feedback	📅 ☎	📅 ☎	
POST /reports	create	report generation, analytics	📅 ✉	📅 ✉	
POST /feedback	create	customer feedback, suggestions	▮▮▮ 🪪	▮▮▮ 🪪	
PUT /calendar	create	event scheduling, appointments	📅 ☎	📅 ☎	🔒
POST /statistics	update	data statistics, metrics			🔒
GET /catalog	read	product catalog, e-commerce			🔒
POST /auth2	create	user authentication, security			
POST /blog SHADOW	create	blog posts, content			
DELETE /customers	delete	customer data, REST API	💳	💳	
DELETE /reviews	delete	product reviews, feedback	📅 ✉ 👤 🔗	📅 ✉ 👤 🔗	
GET /messages SHADOW	read	messaging service, communication	📅 ☎ ✉ 👤 🔗 ...	📅 ☎ ✉ 👤 🔗 ...	🔒

Category: Credit Card Number, IBAN

Total 16 items 1 2 12 / page

API Inventory in Equixly’s Dashboard

Simplify Compliance

Every organization strives to achieve continuous compliance with international and regional regulations and general security standards. Equixly would be an incomplete solution if it didn't offer mechanisms for you to comply with GDPR, PCI DSS, CCPA, APPs, and other regulations and standards.

There's no secret, and there are no shortcuts to compliant APIs. You use a purpose-built solution such as Equixly to find vulnerabilities in development and production and remedy them. A secure API that doesn't leak sensitive data is the best testimony to your determined compliance efforts. But you also need proof in black and white for auditors and regulators.

Equixly covers this aspect with its simple reporting model, which enables you to generate password-protected PDF reports that include:

- Scan overview
- Data classification
- Security issues breakdown
- Detailed information on the found security issues

The reports allow you to track changes over time and provide evidence that you have remedied issues between two reports.

Contact us

MEET US

Equixly – Local Office
Via E. Torricelli, 8A
37135 Verona (VR),
Italy

Equixly – HQ
Via del Tiratoio, 1
50124 Florence (FI),
Italy

WRITE US

General questions
info@equixly.com

Sales Team
sales@equixly.com

VISIT US

Website
https://equixly.com/

Blog
https://equixly.com/blog/

CALL US

Book a meeting
https://meet.equixly.com/