

Build safe and reliable APIs with Secure Pro in Ready! API

In the connected world, APIs dominate the landscape. Traditional security testing just isn't good enough to handle the added surface area, vulnerabilities, and increasing complexity of modern APIs. You need tools built for APIs by API experts with over a decade of open source experience.

Secure Pro is a powerful approach to API security, combining data-driven testing with automated scanning capabilities to empower teams of testers to seamlessly check the safety of their APIs as part of their existing continuous delivery process. Make sure your teams deliver safe APIs with tools that:

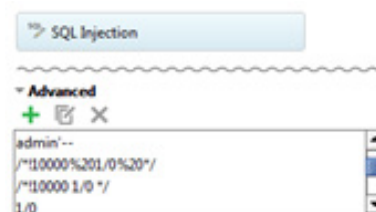
- Test the security of both REST and SOAP services
- Catch server-side configuration errors resulting from invalid data
- Check for sensitive file exposure on servers
- Validate that tests do not contain weak authentication

With Secure Pro, you can catch vulnerabilities in time to do something about it, producing APIs that are safe by default.

Secure Pro in Ready! API includes:

Injection Attacks (SQL, XPath)

Protect against malicious code injection. SQL injection can expose and damage your critical data. Malformed XPath can cause parsers on your server to cough up sensitive configuration



HTTP Method Fuzzing

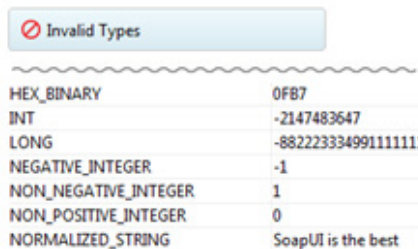
- GET (In definition)
- POST (In definition)
- PUT
- DELETE
- PATCH

REST Specific Security Scans (HTTP Method Fuzzing)

Your API descriptors might say that certain requests are accepted, but what happens when you post something unacceptable; instead of a GET, how about POST, PUT, or DELETE? Don't let these loose ends cause data integrity problems in the production environment.

Invalid Types (XML and JSON)

Know what your APIs do with junk data. Ready! API understands JSON data structures and can test to see what happens when data posted doesn't match the expected value types.



Invalid Types	
HEX_BINARY	0FB7
INT	-2147483647
LONG	-8822233349911111111
NEGATIVE_INTEGER	-1
NON_NEGATIVE_INTEGER	1
NON_POSITIVE_INTEGER	0
NORMALIZED_STRING	SoapUI is the best

Sensitive Files Exposure



/.ssh/id_rsa	Sensitive SSH infor...
/.ssh/id_rsa.bak	Sensitive SSH infor...
/.ssh/id_rsa.old	Sensitive SSH infor...
/.ssh/id_rsa~	Sensitive SSH infor...
/.htaccess	May contain pass...
/.htaccess.bak	May contain pass...

Sensitive File Exposure

Are there files on the server where your API is deployed that expose sensitive information? Automatically scan and detect exposed configuration, permissions, and user list files left on the server by other processes.

Cross-Site Scripting

Check for common vulnerabilities in posting Javascript and HTML code snippets to your APIs. Will your web service inappropriately accept these malicious bits, or will it successfully reject them?

Cross Site Scripting

```
";!--" <XSS> = &{()
<SCRIPT SRC=http://soapui.org/xss.js> </SCRIPT>
<IMG SRC="javascript:alert('XSS');">
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert('XSS')>
```

Weak Authentication

- Strategy
- Apply to Failed TestSteps
- Run only once

Weak Authentication

How are credentials used in your requests, and are there any known vulnerabilities in how your tests are authenticating? Use Secure Pro to find out what may be missing from your authentication process.

Secure Pro pricing starts for as little as \$249/year. Contact a sales representative for full details.

Ready! API is the industry's most widely recognized API quality management platform, built on open source technology, empowering developers and testers to deliver reliable, scalable and safe web services.

