

Framework for Application Security Testing



September 11th, 2018



Create thousands of security tests from existing functional tests ...automatically

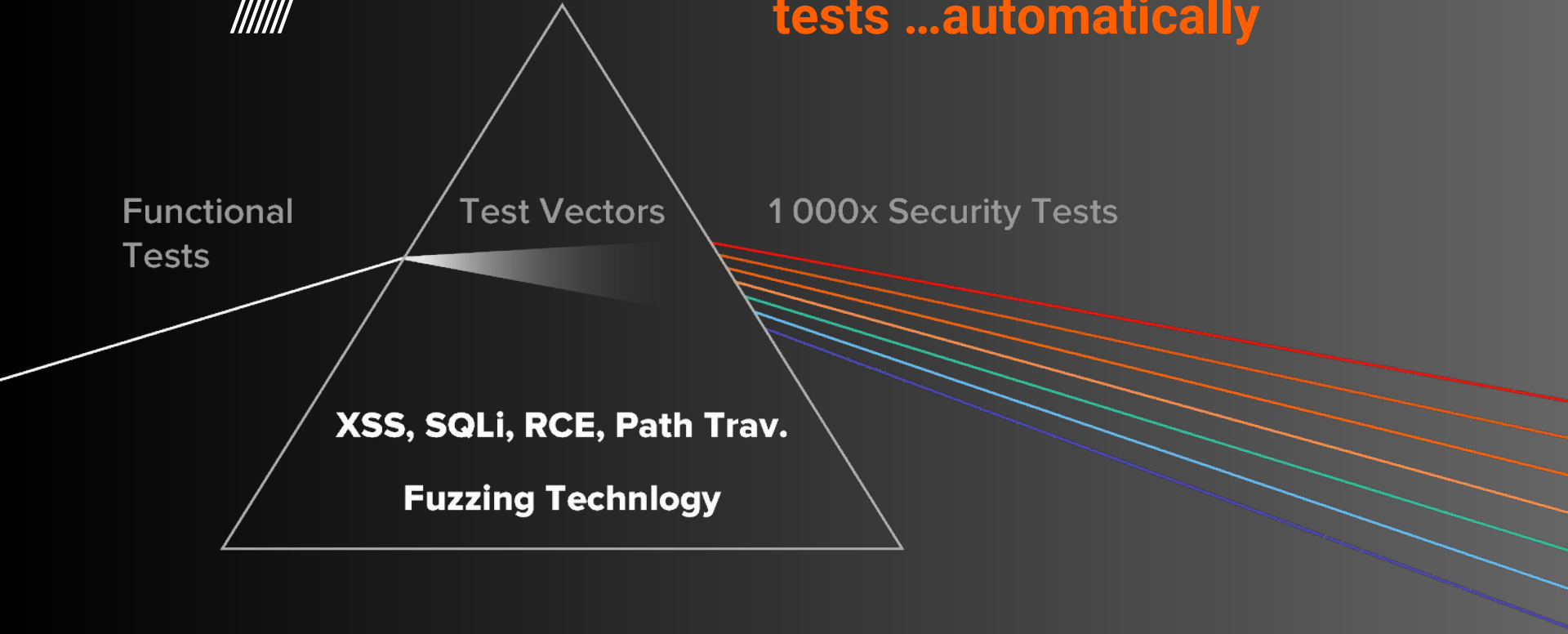
Functional Tests

Test Vectors

1 000x Security Tests

XSS, SQLi, RCE, Path Trav.

Fuzzing Technlogy



Wallarm FAST – enables secure CI / CD



“

Wallarm FAST has many cool features to help DevOps teams strike the delicate balance between the security of the application and the very short release cycles.

Chris Rodriguez

SENIOR ANALYST

F R O S T  S U L L I V A N

Finds Issues BEFORE Software is Deployed

Results may include:

- vulnerabilities of known types such as OWASP Top 10
- unknown and zero-day vulnerabilities with a fuzzer
- vulnerabilities in XML, REST, JSON, SOAP, Base64 and protocols with nested encoding (no configuration required to parse it)
- API/endpoint behavioral anomalies

Generating Tests

FAST

A

- **Capture a baseline** from QA or production traffic, with FAST acting as a proxy
- **Create security tests** by inserting XSS, PTRAV, RCE or SQLi vector into all or specified web API parameters for every endpoint
- **Create thousands of tests** by applying fuzzing governed by regular expressions
- **Specify test pass criteria** to detect anomalies
- **Policy for generating tests** can be defined out of band by the security team

Running Tests

FAST



B

- Generated tests run automatically
- Running tests and retrieving results is easily automated via API for CI / CD integration
- Authentication/credentials can be inherited from the requests, defined in a test automation framework or provided by a proxy
- Rate of testing and termination criteria are explicitly defined
- Automation and reporting are well suited for regression testing

Actionable intelligence

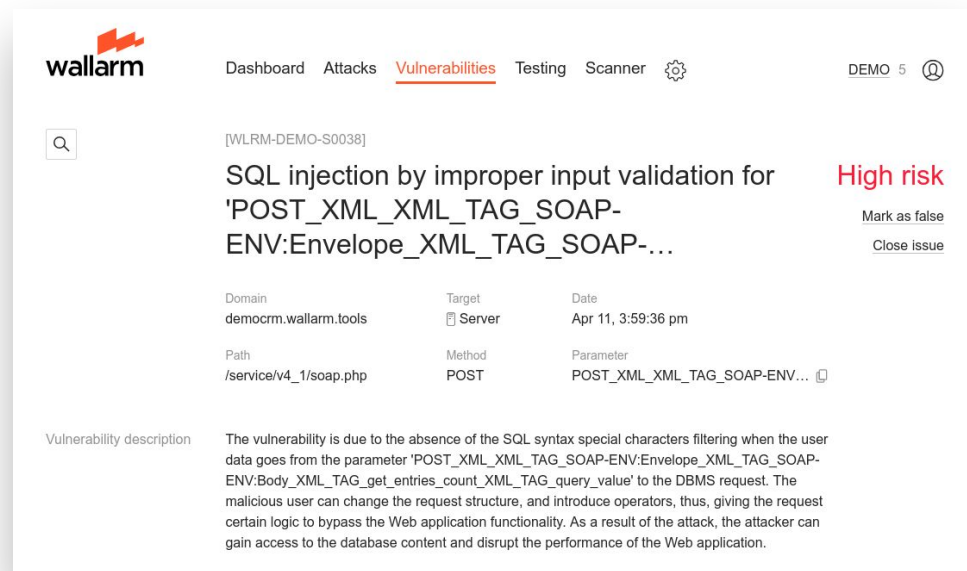
Provides actionable detailed information for every issue found:

- original (baseline) request
- test that found vulnerability
- detailed vulnerability description
- example exploit

Results are integration-ready with REST API

Allows security team to apply their expertise with leverage without slowing down CI / CD pipeline

Developers and QA execute tests within their existing test automation flow



The screenshot displays the Wallarm dashboard interface. At the top, there is a navigation bar with the Wallarm logo and menu items: Dashboard, Attacks, Vulnerabilities (highlighted), Testing, Scanner, and a settings gear icon. On the right side of the dashboard, it shows 'DEMO 5' and a user profile icon. Below the navigation bar is a search bar. The main content area displays a vulnerability report for '[WLRM-DEMO-S0038]'. The title of the issue is 'SQL injection by improper input validation for 'POST_XML_XML_TAG_SOAP-ENV:Envelope_XML_TAG_SOAP-...' and it is marked as 'High risk'. To the right of the title are two buttons: 'Mark as false' and 'Close issue'. Below the title, there is a table with three columns: Domain, Target, and Date. The Domain is 'democrm.wallarm.tools', the Target is 'Server', and the Date is 'Apr 11, 3:59:36 pm'. Another table below shows Path, Method, and Parameter. The Path is '/service/v4_1/soap.php', the Method is 'POST', and the Parameter is 'POST_XML_XML_TAG_SOAP-ENV...'. At the bottom, there is a 'Vulnerability description' section with a detailed text description of the issue.

Dashboard Attacks **Vulnerabilities** Testing Scanner ⚙️ DEMO 5 👤

[WLRM-DEMO-S0038]

SQL injection by improper input validation for 'POST_XML_XML_TAG_SOAP-ENV:Envelope_XML_TAG_SOAP-...' **High risk**

Mark as false
Close issue

Domain	Target	Date
democrm.wallarm.tools	Server	Apr 11, 3:59:36 pm

Path	Method	Parameter
/service/v4_1/soap.php	POST	POST_XML_XML_TAG_SOAP-ENV...

Vulnerability description

The vulnerability is due to the absence of the SQL syntax special characters filtering when the user data goes from the parameter 'POST_XML_XML_TAG_SOAP-ENV:Envelope_XML_TAG_SOAP-ENV:Body_XML_TAG_get_entries_count_XML_TAG_query_value' to the DBMS request. The malicious user can change the request structure, and introduce operators, thus, giving the request certain logic to bypass the Web application functionality. As a result of the attack, the attacker can gain access to the database content and disrupt the performance of the Web application.

Start testing within minutes

Register for a new FAST account
<https://fast.wallarm.com/signup>

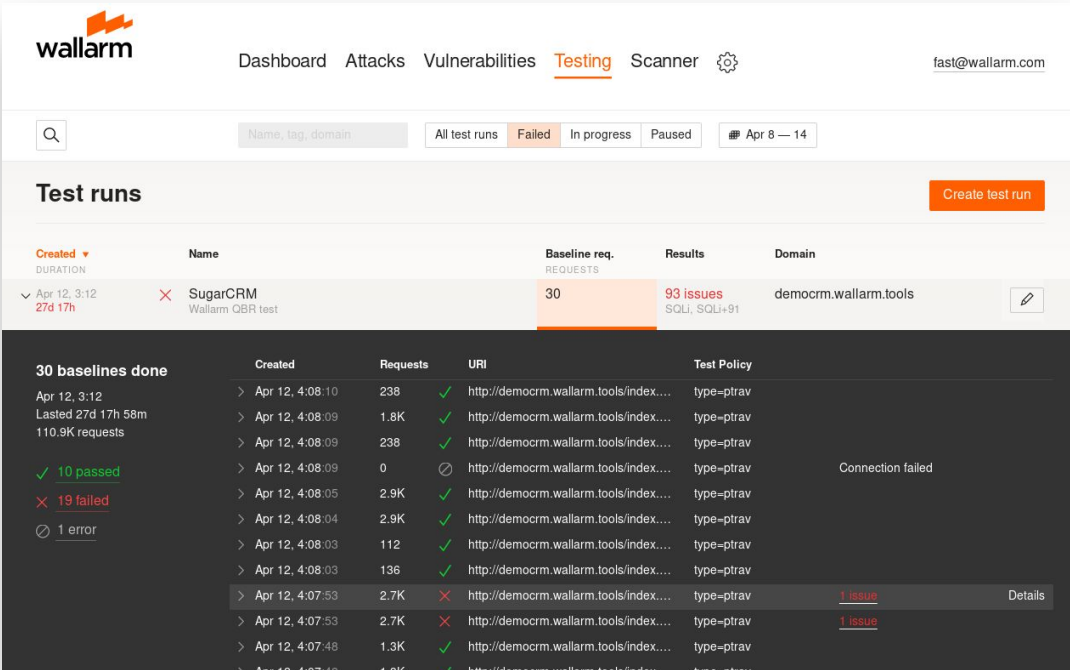
Define a new TestRun in Wallarm Console

Pull wallarm/fast-proxy from a Docker Registry

Configure your browser, Selenium or shell to use wallarm-proxy

Start functional and automated security testing

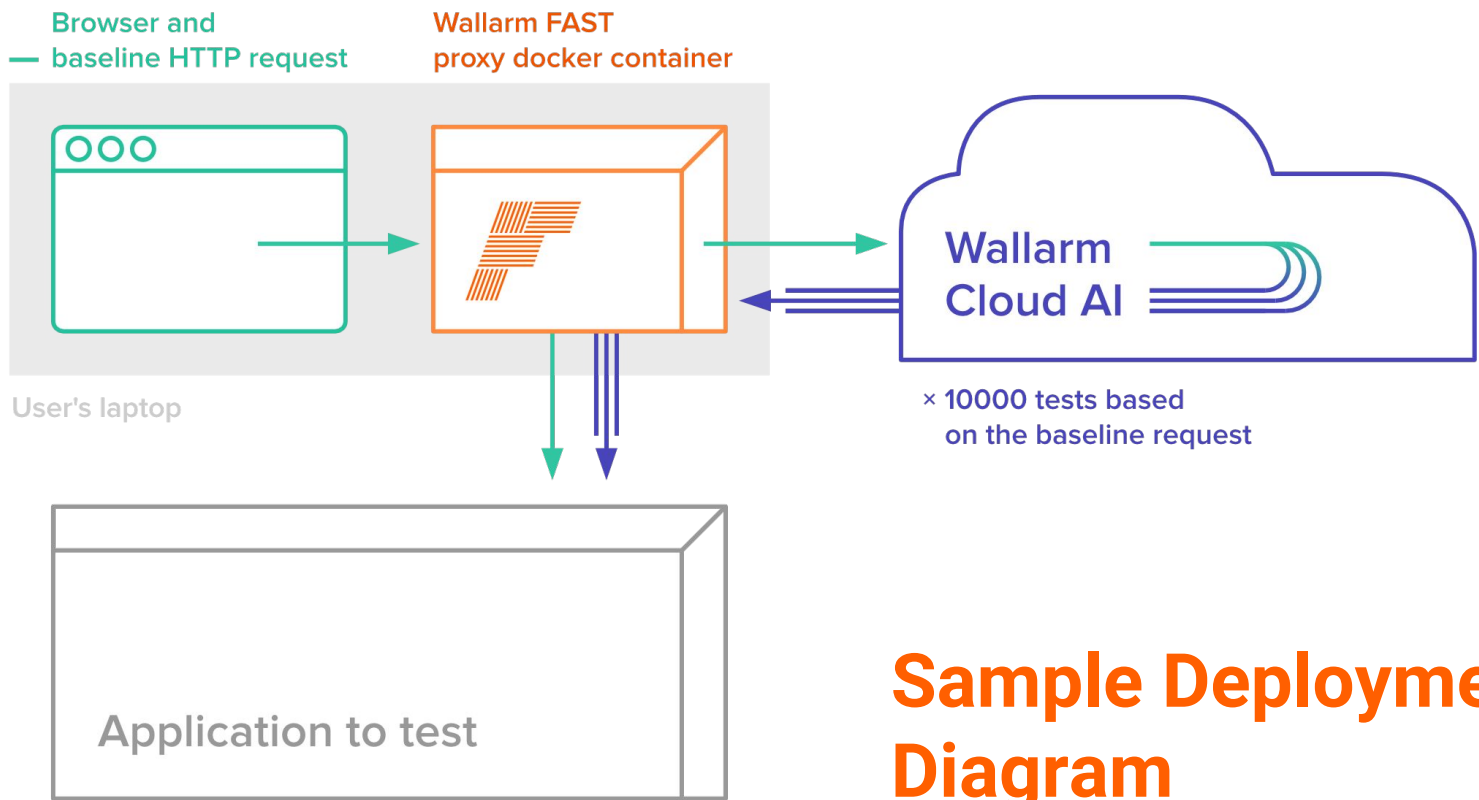
It's that easy!



The screenshot displays the Wallarm console interface. At the top, the Wallarm logo is on the left, and navigation links for Dashboard, Attacks, Vulnerabilities, Testing (highlighted), and Scanner are in the center. The user email fast@wallarm.com is on the right. Below the navigation is a search bar and filters for test runs: All test runs, Failed (selected), In progress, and Paused. A date filter shows Apr 8 — 14. The main section is titled "Test runs" and includes a "Create test run" button. A table lists test runs, with one selected: "SugarCRM" (Wallarm OBR test) created on Apr 12, 3:12, with a duration of 27d 17h. It shows a baseline requirement of 30 requests and 93 issues (SQL, SQLi+91) for the domain democrm.wallarm.tools. Below this, a detailed view shows "30 baselines done" with a list of requests, including their creation time, request count, status (passed/failed/error), URI, and test policy.

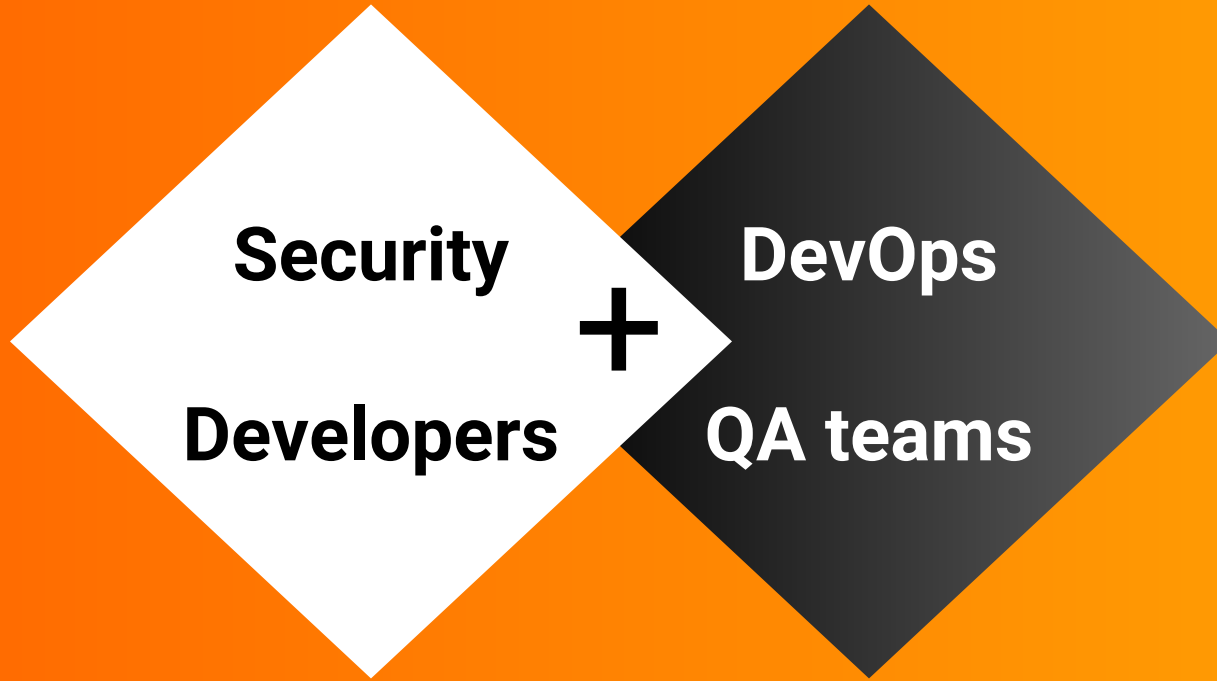
Created	Name	Baseline req.	Results	Domain
Apr 12, 3:12 27d 17h	SugarCRM Wallarm OBR test	30	93 issues SQL, SQLi+91	democrm.wallarm.tools

Created	Requests	URI	Test Policy
Apr 12, 4:08:10	238	http://democrm.wallarm.tools/index...	type-ptprav
Apr 12, 4:08:09	1.8K	http://democrm.wallarm.tools/index...	type-ptprav
Apr 12, 4:08:09	238	http://democrm.wallarm.tools/index...	type-ptprav
Apr 12, 4:08:09	0	http://democrm.wallarm.tools/index...	type-ptprav Connection failed
Apr 12, 4:08:05	2.9K	http://democrm.wallarm.tools/index...	type-ptprav
Apr 12, 4:08:04	2.9K	http://democrm.wallarm.tools/index...	type-ptprav
Apr 12, 4:08:03	112	http://democrm.wallarm.tools/index...	type-ptprav
Apr 12, 4:08:03	136	http://democrm.wallarm.tools/index...	type-ptprav
Apr 12, 4:07:53	2.7K	http://democrm.wallarm.tools/index...	type-ptprav 1 issue Details
Apr 12, 4:07:53	2.7K	http://democrm.wallarm.tools/index...	type-ptprav 1 issue
Apr 12, 4:07:48	1.3K	http://democrm.wallarm.tools/index...	type-ptprav
Apr 12, 4:07:48	1.3K	http://democrm.wallarm.tools/index...	type-ptprav



Sample Deployment Diagram

Who is FAST for?



Licensing

Personal non-transferable license

- 30 days trial license
- \$79/mo after
- Limited to single simultaneous test run & 1000 base-lines per month

Pen-tester productivity license

Contact us

DevOps team license

Coming in Q3

Wallarm Ecosystem for Application & API Security

**Adaptive AI Platform
enables dev/QA
and production
application & API
security**

Attack blocking

Scanning

Testing

**Adaptive real
time web and API
protection**

**Automated CI/CD
integrated security
testing**

Application Security powered by AI



Other Wallarm products

Wallarm attack mitigation for applications and APIs (NG WAF)

- protection against full spectrum of threats: OWASP Top 10, bots, app abuse and DDoS
- Works in full blocking mode (ultra-low false positives)
- AI-powered detection and bespoke security rules

Wallarm scanner for operational security testing

Additional FAST resources

fast.wallarm.com/signup

[Demo video](#)

[Marketing video](#)

[Data Sheet](#)

[Evaluation guide](#) [Test policy guide](#)

Try it for yourself today

```
$docker run wallarm/fast
```

About Wallarm

Founded in 2013

Headquartered in Silicon Valley

Backed by prominent VCs

Y Combinator, Partech Ventures, Runa Capital

Profiled in analyst's reports as one
of 12 leading WAF providers

Frost & Sullivan

“White hat” security DNA

Experienced team of managers and advisors

Protects 150M+ users
at 120+ customers from startups
to Fortune 500

