CSO Conference *& Awards*

Produced by CSO | IDC

FioriDAST

Reinvent dynamic security scans for modern Web-based Cloud applications

Matthias Ems, SAP SE
Vladislav Dexheimer, SAP SE

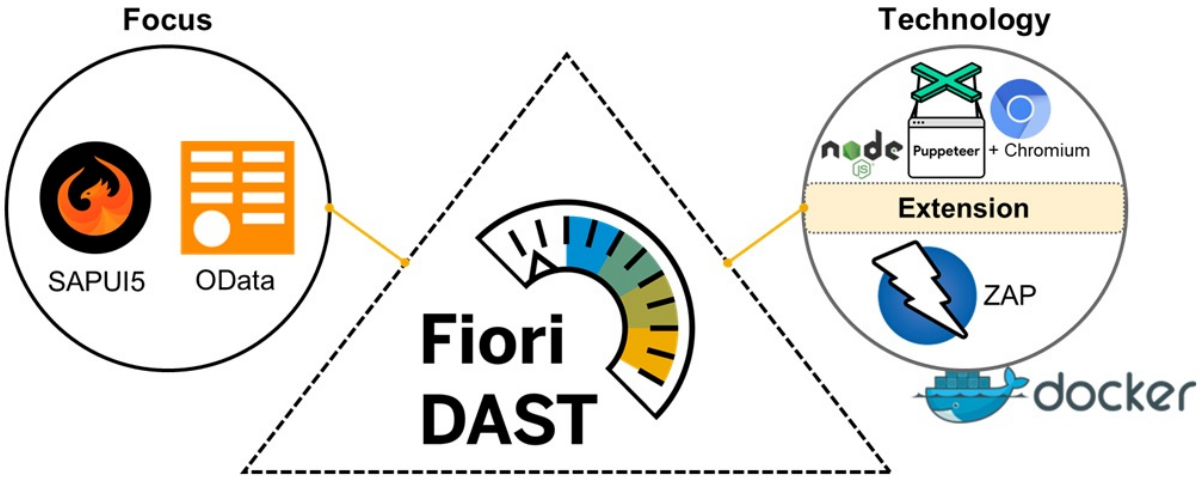
CSO Conference & Awards | SAP
Produced by CSO | IDC

Context & Challenges

- SAP delivers business software with many Web applications, especially within the SaaS ERP “SAP S/4HANA Cloud Public Edition”
- Code scans (SAST) cover only a subset of vulnerabilities and are blind to security issues like misconfigurations and authorization check inconsistencies
- Penetration testing comes late in the lifecycle and doesn’t fully scale (→ shift left)
- Other dynamic security test (DAST) tools lack in-depth capabilities for SAP-specific UI and API technologies
- High-level automation and scalability is a must due more than 1000 applications in scope

Solution Overview

In-house security tool for **automated exploration and attacks** against **application interfaces at runtime** aiming to detect **Web-related vulnerabilities**



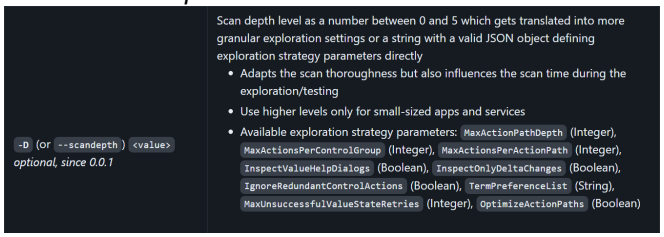
Capabilities

1. Configuration & Orchestration

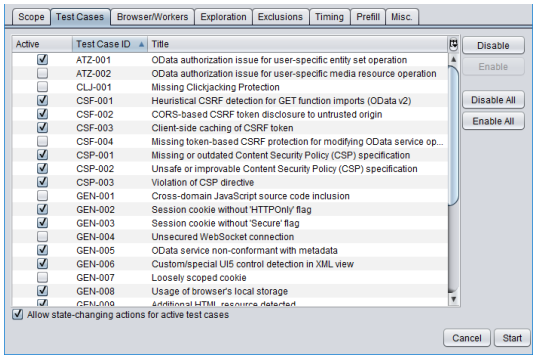
Customizability via UI, API, CLI

...

Command-line parameters



Test case selection



Filtering and amendments of alerts

```
# Local browser storage usage will be ignored by external.server.com
url(*https://external.server.com*)&test(GEN-008):confidence(f);
# Missing Clickjacking protection will be considered as a high risk
test(CLJ-001):risk(h);
# Solution for CSRF-related alerts in path /services/v1/ will be adjusted
url(*/services/v1/*)&test(CSF):solution(Check if anti-CSRF token is applied);
```

Capabilities

1. Configuration & Orchestration

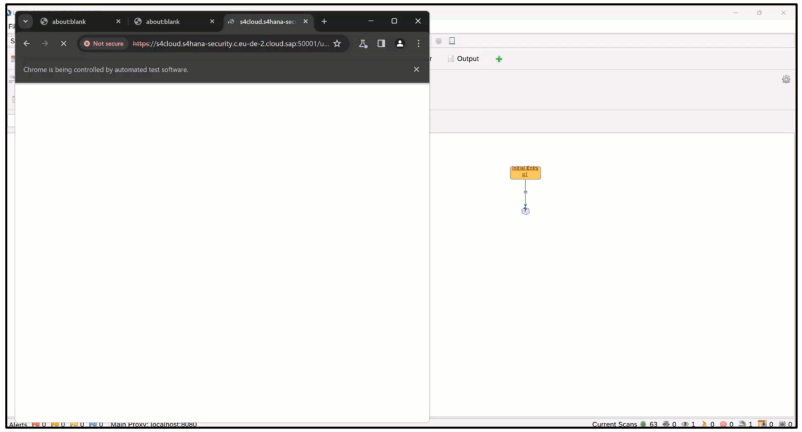
2. Exploration

Transparent Authentication

Web App Crawling

API Spidering

…



Capabilities

1. Configuration & Orchestration

2. Exploration

3. Security Testing

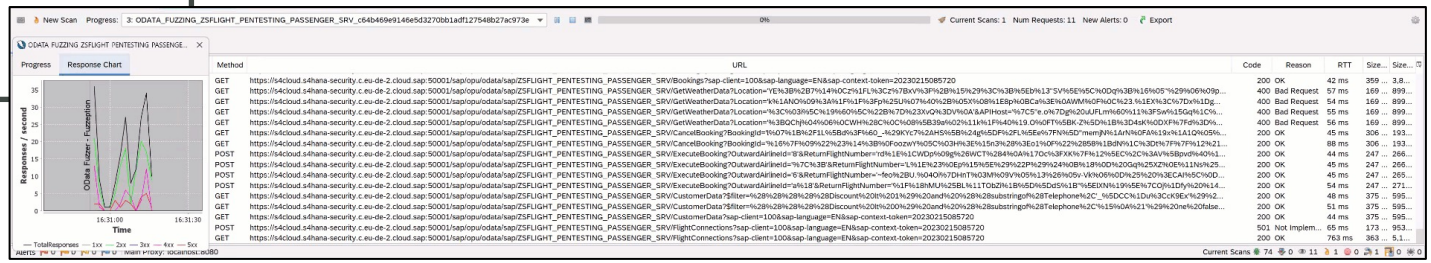
Client-side XSS

API Fuzzing

Insufficient Authorization Checks

Information Disclosure

…



Capabilities

1. Configuration & Orchestration

2. Exploration

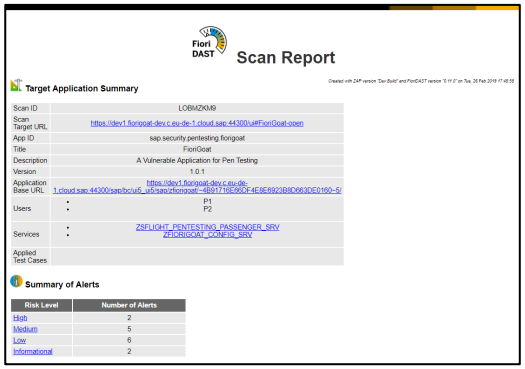
3. Security Testing

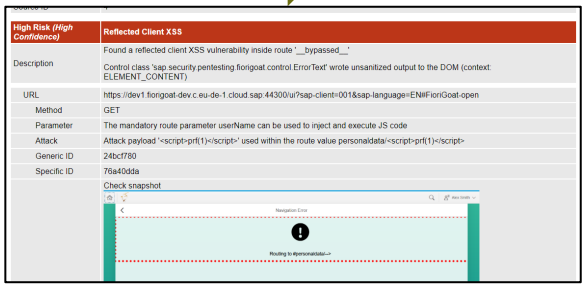
4. Reporting

Optimized Reporting

Different formats (XML, SARIF, PDF)

…





Achievements & Takeaways

- Automated scanning of > 600 applications in SAP S/4HANA Cloud daily with well-defined audit and correction processes (customer trust in SAP security)
- Broad tool adoption within other product areas at SAP
- Tool improvements via feedback loop from different channels

- Certain business challenges can only be tackled by custom/specialized solutions
- High efforts and engineering resources are required but the benefits can be paramount with automation in mind

Credits

- Management support
- International core team
- Cybersecurity students
- Close network of SAP security experts
- (Early) Adopters