Testing for insecure SAML signature validation
Trust & Identity Incubator Final Demo

Demo, Online
02 Mai 2024

Public (PU)
**Activity description**

The goal of the activity is to deliver a (software or service) solution that assists federation operators of NREN federations in testing at scale of several core security aspects of Service Providers SAML deployments within their federation.

Deployment scenarios, to be confirmed with stakeholders, might include:

- Self-testing by an SP as part of the route towards becoming a production deployment
- (Automated) Testing the SP deployment as part of the initial onboarding into the federation by FedOps
- (Automated) Testing the SP deployment as part of periodic review by FedOps
- Institution initiated testing of SP as part of compliance review, e.g. wrt GDPR compliance, for a service they have a contract with

This topic should include the technical implementation of the use cases we would like to test against. In addition it needs to discuss and if need be develop a means to support FedOps to deploy the testsuite both technically and operationally.

Next to technical and operational requirements we need to understand as well as potential legal aspects, so we can include all of these in the design of the test suite.
About the use case and deployment scenario

Stakeholder workshop @ GEANT Symposium

- Core use case:
  - Periodic compliance testing by FedOps
  - Secondary: Testing individual SPs (by FedOps, institution or SP itself)
- Deployment scenario: FedOps deploy the tool themselves
- Test cases: Idp Initiated

First public sprint demo

- Test cases: Add SP initiated
- Better reporting
Topic background - IdP vs. SP-initiated login

- two ways to start the authentication
  - IdP-initiated (“unsolicited”)
    - starts at IdP endpoint
  - SP-initiated
    - various forms (login button, automatic login, …)
    - mostly SP-specific (difficult to automate in large scale)
    - we have leveraged two standard endpoints
      - [Service Provider Request Initiation Protocol](#)
        - in eduGAIN mostly Shibboleth SPs
      - [Identity Provider Discovery Service](#) response endpoint
        - Shibboleth SP, SimpleSAMLphp, SATOSA, …
Nuclei test

```
src
```
Conformance IdP + nuclei flow

Manual test via Conformance IdP UI

1. Initiate test
2. Activate test battery

Loop:
   - For each test case
   - 3. Choose test case

Alt. [unless IdP-initiated]
   - 4. Initiate login with testing IdP
   - 5. Authn request

6. Generate invalid response
   - 7. Authn response

8. Signed-in/error page

9. Results

10. Report

Fed/SP operator
Conformance IdP
Nuclei
SP

Src
Conformance IdP

- SimpleSAMLphp 'conformance' module that can modify SAML responses sent to trusted SPs
  - https://github.com/cicnavi/simplesamlphp-module-conformance
- Provides UI for running tests, viewing results …
- Exposes API endpoints for manual or programmatic actions:
  - Defining the next test for the SP (valid response, without a signature, with an invalid signature, etc.)
  - Provisioning SP metadata trusted by the Test IdP
  - Running nuclei tests
  - Fetching results in JSON format
- Enables bulk testing using SimpleSAMLphp cron feature
- Provides SP Consent feature (sending email challenge to SP contacts)
- Static authentication source for automatic authentication with a sample user
Test SPs

- Good and bad SP deployments (SPs that validate or not validate signatures)
- Two SimpleSAMLphp SPs
  - Bad SP has a hardcoded modification to skip signature checks
- Two Keycloak SPs
  - Bad SP has a configuration option not to validate signatures
- Two Shibboleth SPs
  - Bad SP has a configuration option not to validate signatures
Test Environment

- Live demo
Activity results

- **Nuclei templates and workflows**
  - IdP-initiated login
  - SP-initiated login
    - via [Service Provider Request Initiation Protocol](#)
    - via [Identity Provider Discovery Service](#) response endpoint

- **Conformance module for SimpleSAMLphp**
  - Signature generation for manual testing and nuclei
  - Running single tests from UI
  - Bulk testing (via cron module)
  - API
  - SP metadata registration / provisioning

- **Prepared deployment** (using docker compose)
  - conformance IdP, database, nginx and https (Let’s encrypt)
  - configuration not included (e.g. metadata sources)
Thank You