SAML Signature Validation

Public Sprint Demo

GN5-1 Trust & Identity Incubator

Marko Ivančić
Pavel Břoušek
Niels van Dijk

Tue Jan 23, 2024

Activity description

The goal is to deliver a software or service solution assisting federation operators of NRENs in testing at scale of several core security aspects of Service Providers SAML deployments within federations.

Deployment scenarios (to be confirmed with stakeholders) may include:

- Self-testing by an SP on the route to becoming a production deployment
- (Automated) testing of SP deployment during initial onboarding by FedOps
- (Automated) testing of SP deployment during periodic review by FedOps
- Institution-initiated testing of SP during compliance review, e.g., GDPR compliance, for a service they have a contract with

Focus on the technical implementation of the use cases to be tested, including discussions and potential development of support for FedOps to deploy the test suite. Consider technical, operational, and legal requirements, so we can include them in the designed test suite.

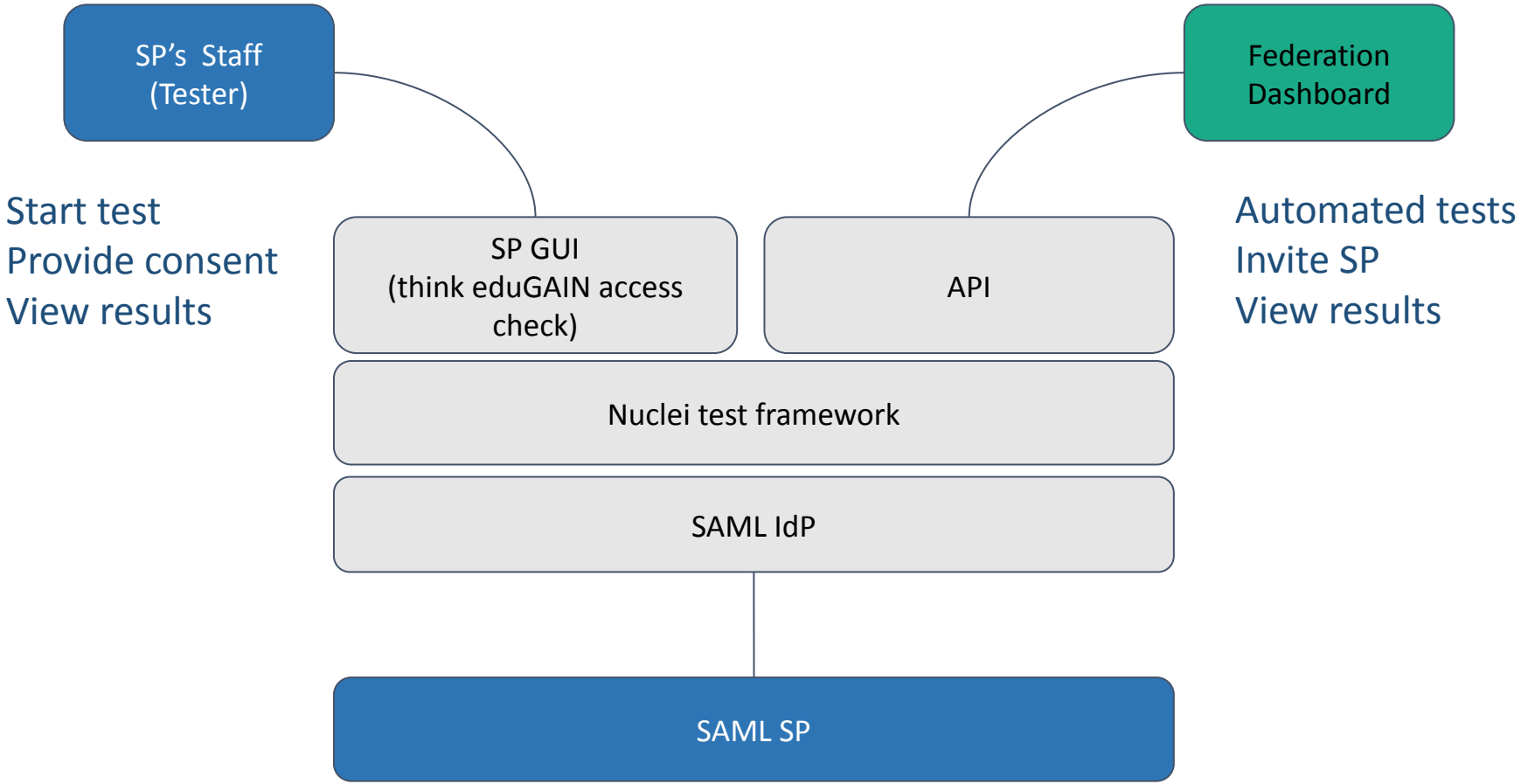
About the use case and deployment scenario

Stakeholder workshop @ GEANT Symposium:

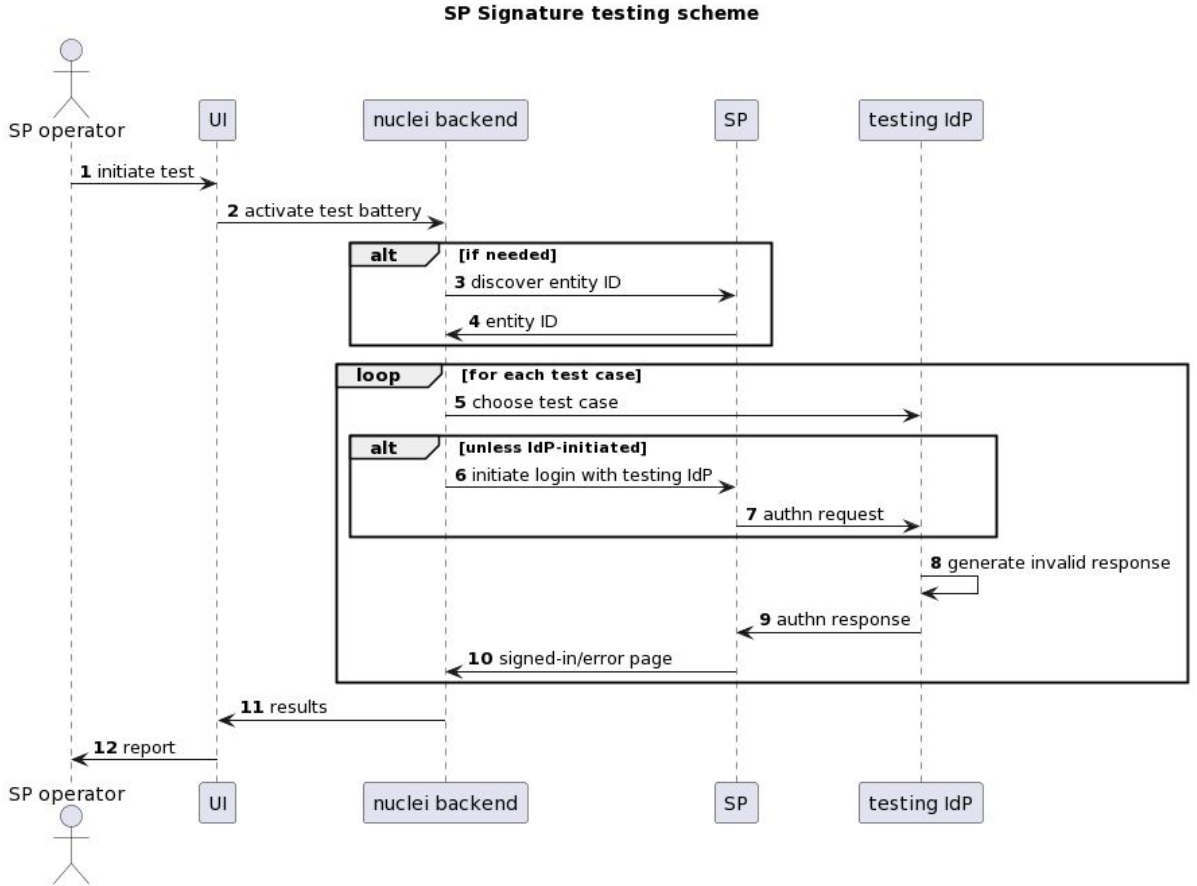
- Core use case: Periodic compliance testing by FedOps
- Secondary: Testing individual SPs (by FedOps, institution or SP itself)

- Deployment scenario: FedOps deploy the tool themselves

Proposed setup



Technical solution



src

Technical solution

Nuclei

- A vulnerability scanner for identifying exploitable weaknesses with a vast library of templates for known vulnerabilities
- Built for automatic detection
- Two relevant scanning modes
  - Raw HTTP (more efficient)
  - Headless (with screenshots)
- Built-in basic modifications (base64, gzip, urlencode…)
  - Cannot directly construct signed XML documents
- Requires an IdP (or a library) for signature generation

Technical solution (nuclei template example)

```
id: incubatorsamltestheadless
info:
  name: Incubator SAML test headless
  severity: low
  tags: headless, extractor
variables:
  filename: '{{replace(BaseURL,"/","_")}}'
  dir: "screenshots"
  testCase: 'invalidSignature'
headless:
  - steps:
        - action: navigate
          args:
            Url: "https://conformance-idp.maiv1.incubator.geant.org/module.php/conformance/test/setup
?testId={{url_encode(testCase)}}&spEntityId={{url_encode(BaseURL)}}"
        - action: waitload
        - action: navigate
          args:
            url: "https://conformance-idp.maiv1.incubator.geant.org/saml2/idp/SSOService.php?spentityid={{url_encode(BaseURL)}}"
        - action: waitload
        - action: screenshot
          args:
          fullpage: "true"
          mkdir: "true"
          to: "{{dir}}/{{filename}}"
    matchers:
      - part: resp
        type: word
        words:
          - "Welcome"
          - "REMOTE_USER = test"
          - "Authenticated"
    extractors:
      - type: kval
        part: extract
        kval:
          - extract
```

Technical solution (nuclei report example)


```
[
  {
        "template-id": "incubatorsamltestheadless",
        "template-path": "/home/brousek/Dokumenty/Incubator/nuclei-templates/saml-headless.yaml",
        "template-encoded": "aWQ6IGluY3ViYXRvcnNhbWx0ZXN0aGVhZGxlc3MKaW5mbzoKICBuYW1lOiBJbmN1YmF0b3IgU0FNTC...",
        "info": {
          "name": "Incubator SAML test headless",
          "author": [
            "pavel brousek"
          ],
          "tags": [
            "headless",
            "extractor"
          ],
          "severity": "low"
        },
        "type": "headless",
        "host": "aai-playground.ics.muni.cz",
        "port": "443",
        "scheme": "https",
        "url": "https://aai-playground.ics.muni.cz/simplesaml/module.php/saml/sp/metadata.php/default-sp",
        "path": "/simplesaml/module.php/saml/sp/metadata.php/default-sp",
        "matched-at": "https://conformance-idp.maiv1.incubator.geant.org/saml2/idp/SSOService.php?spentityid=...",
        "response": "<html xmlns=\"http://www.w3.org/1999/xhtml\"><head>\n...",
        "timestamp": "2023-12-11T00:56:04.298944088+01:00",
        "matcher-status": true
  }
]
```

Technical solution

Test IdP

- SimpleSAMLphp v2.1 instance with configured IdP and custom 'conformance' module (authentication processing filter) that can modify SAML responses sent to trusted SPs
- Static authentication source for automatic authentication with a sample user
- Exposes 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 using custom templates

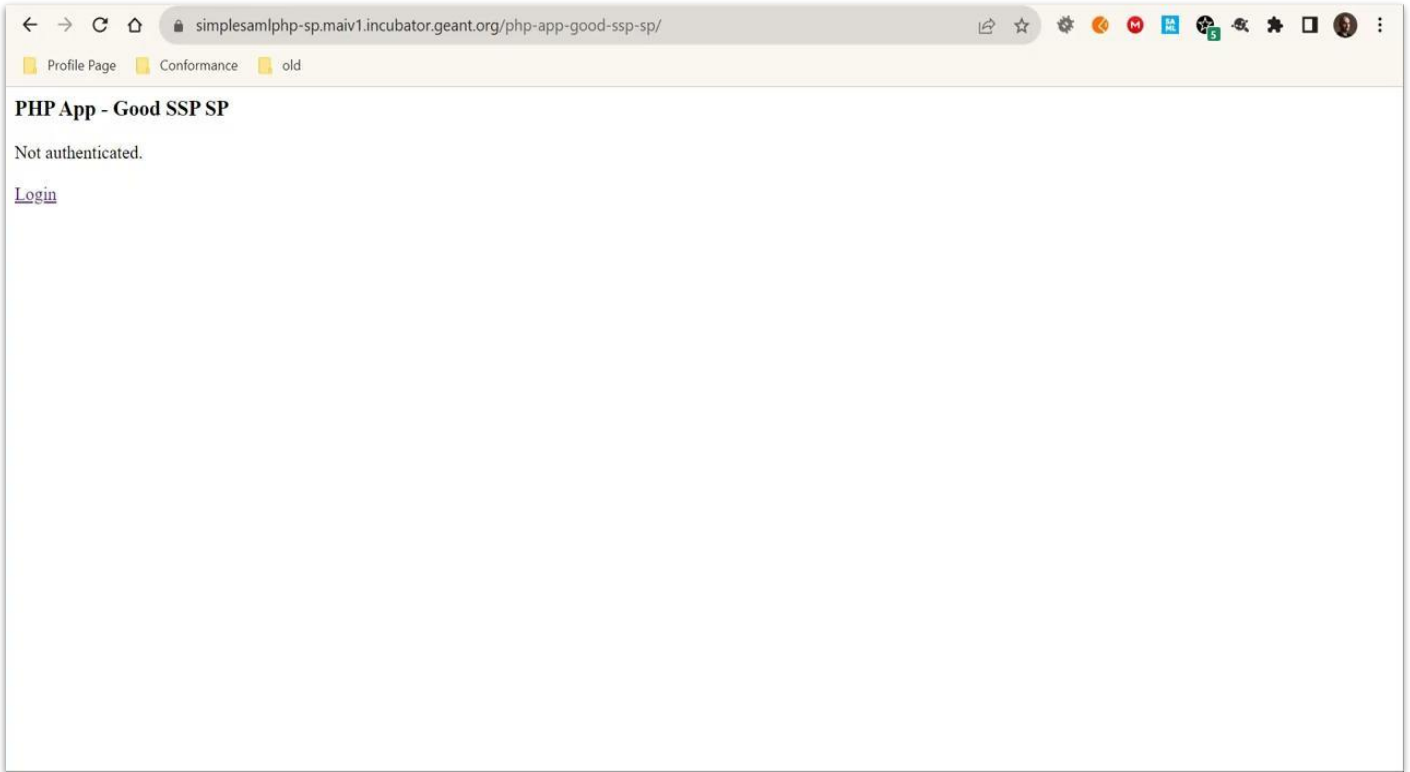
Technical solution

Tested 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

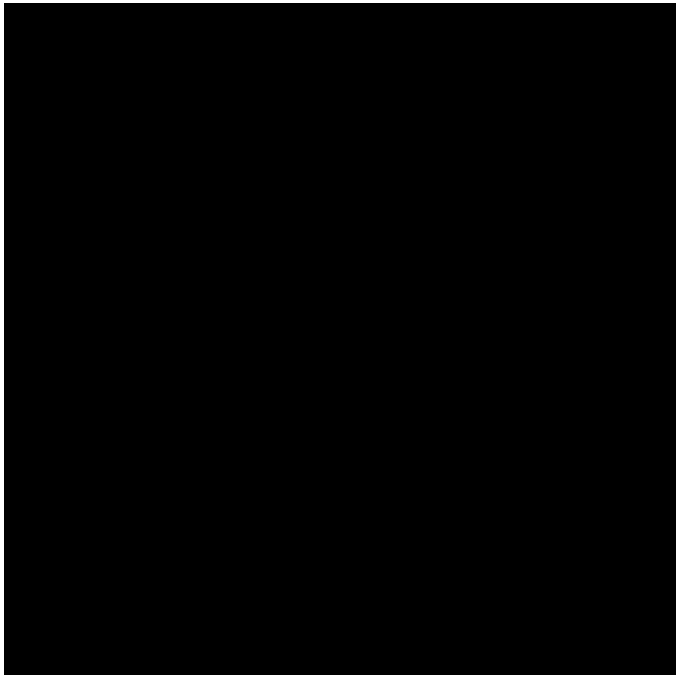
Technical solution

Manual test of the good SP (validates signature) and bad SP (does not validate it)



Technical solution

Using *nuclei* in UI to run the “no signature” test with IdP initiated login for the “good SP” (validates signature)



Thank You

www.geant.org

Co-funded by
the European Union