Flawnter DAST SSO Security Testing Guide

The Flawnter DAST SSO security testing feature will scan for security vulnerabilities on service provider. Currently it supports SAML2 protocol for the SSO. Authentication JSON file is required for the scanner.

Note: The SSO IdP password must be test account. Do not use production credentials. We also recommend having minimum 1-2 minutes SSO token expiration time to give enough time for the scanner to complete the test.

Authentication File

The authentication file is JSON file with information required to authenticate with IdP and also pass to the SSO security testing of service provider.

id - This should be “auth”.
version - This should be 1 unless we publish newer version of the authentication file.
type - The type should be “sso”.
idp - This is the identity provider the SSO is using. Supported values are: okta.
appname - The name of the app (service provider) the identity provider uses.
appid - The app (service provider) id.
relaystate - The SAML relay state that is passed to the service provider. Leave it empty if there is none.
success_token - This is a unique text that is returned in the response by the service provider after successful SSO authentication. The scanner will use this to determine successful login while testing.
login_url - This is the login URL of the identity provider.
content_type - The content type of the data passed to login to IdP.
rawdata - The raw data used in the request body for the login to IdP.
data - The data used in the form of key and value. If using this then rawdata must be empty.

Below is sample JSON file.


```
{
  "id": "auth",
  "version": 1,
  "type": "sso",
  "idp": "okta",
  "appname": "myapp",
  "appid": "ugHR37Hwgh54Ewzop",
  "relaystate": "ERGUWFYTBUKWFTUJERGRET",
  "success_token": "login success",
```

```
  "login_url": "https://mydomain.okta.com/api/v1/authn",
  "content_type": "application/json",
  "rawdata": "{\"password\":\"jrpjnbv843\",\"username\":\"test@example.com\"}",
  "data": []
}
```