HACKTHEBOX

ATTACKING AUTHENTICATION MECHANISMS

CHEAT SHEET

JWT

- Try JWT without a signature
- Set signature algorithm to `None`
- Brute-Force the secret of JWTs protected with symmetric algorithms
- Attempt algorithm confusion for JWTs protected with asymmetric algorithms
- Investigate whether the web application supports additional JWT claims such as
  - `jwk`
  - `jku`
  - `x5c`
  - `x5u`

OAuth

- Investigate if the `redirect_uri` is properly validated
- Investigate if a `state` parameter is present and properly validated
- Investigate for possible XSS vulnerabilities from reflected OAuth parameters

SAML

- Investigate the response to a SAML response when the signature has been removed
- Manipulate the SAML response to explore Signature Wrapping vulnerabilities
- Investigate XML Attacks such as XXE and XSLT Server-side Injection in the SAML XML data