SAML Tools of the Trade & Vulnerability Prevention

After discussing multiple vulnerabilities in SAML implementations, let us discuss what tools we can use to simplify the vulnerability identification and exploitation process. Furthermore, we will briefly explore how to prevent SAML-based vulnerabilities.

Tools of the Trade

SAML Raider is an extension for BurpSuite that we can use to identify and exploit vulnerabilities in SAML implementations. We can install it from the BurpSuite App Store under Extensions > BApp Store.

After installing the extension, it automatically highlights requests containing SAML-related data in the HTTP proxy tab:

image

To explore more functionalities provided by SAML Raider, let us send the request sending the SAML response to the service provider to Burp Repeater. As we can see, SAML Raider adds a new tab to the request in Burp Repeater:

image

Clicking on the SAML Raider tab and then on SAML Message Info displays some general information about the SAML data as well as the decoded XML data at the bottom of the window:

image

In the SAML Attacks tab, we can exploit all vulnerabilities discussed in this module. We can execute a signature exclusion attack by clicking the Remove Signatures button. SAML Raider automatically removes the ds:Signature node from the SAML response. Furthermore, we can execute XXE and XSLT attacks, as well as all eight variants of signature wrapping attacks:

image

SAML Raider will adjust the SAML response accordingly and re-encode the XML data. All we have to do after selecting an attack in SAML Raider is to re-send the request in Burp Repeater. This simplifies vulnerability identification and exploitation greatly since we no longer have to decode and re-encode the SAML response XML data manually.

image