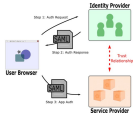
Bypassing SAML Authentication

Security Assertion Markup Language

B.Dhiyaneshwaran

AGENDA

- What is SAML ? 

- Flow of SAML 

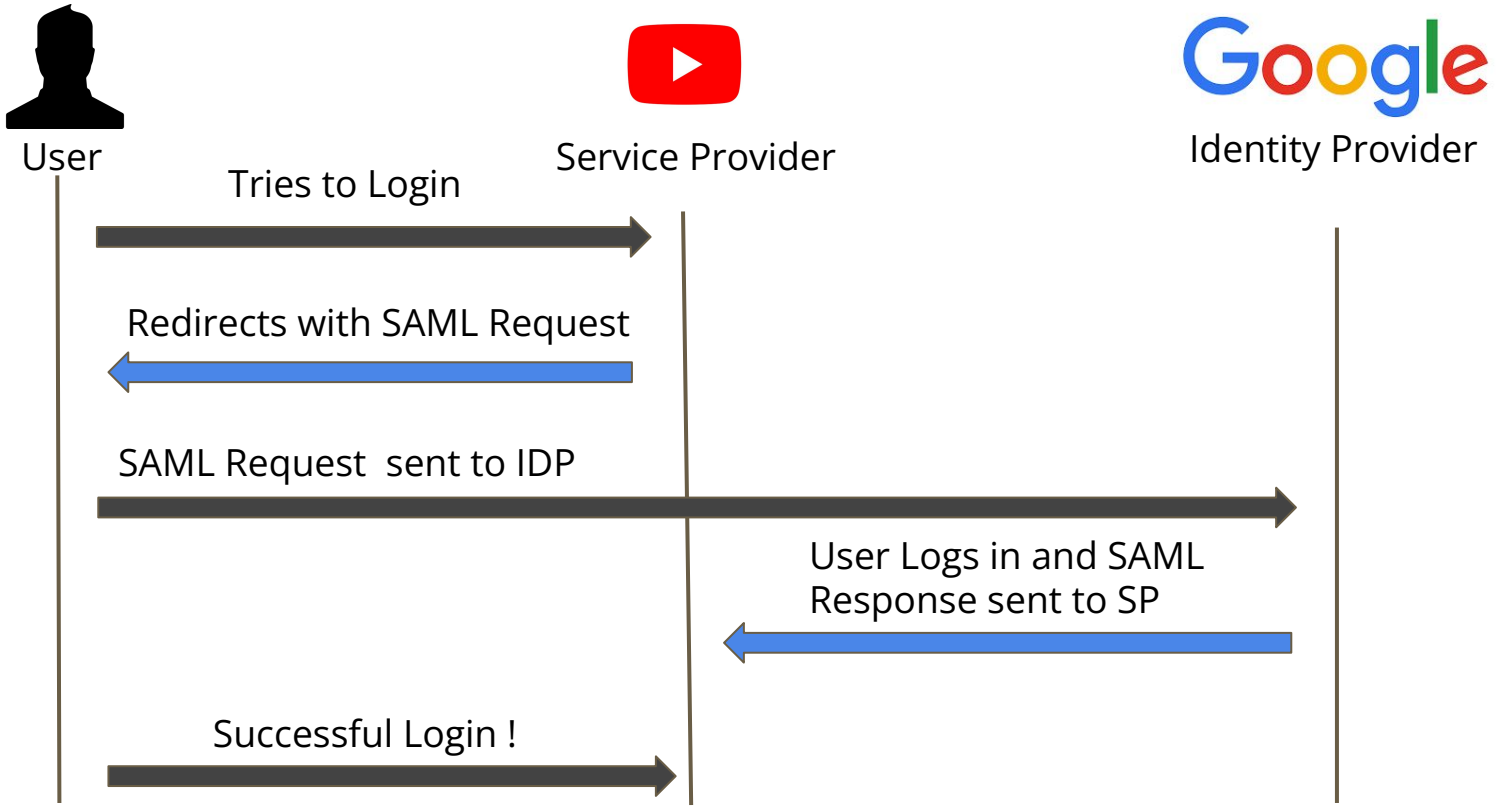
- SAML Response 
- Live Demo 

- Remediation 

What is SAML ?

The companies which uses SAML has a single login page and configure all the web application in a way that their users can login to the application using the Single Sign On.

Flow of SAML


User
Service Provider
Google
Identity Provider
Tries to Login
Redirects with SAML Request
SAML Request sent to IDP
User Logs in and SAML
Response sent to SP
Successful Login !

SAML Response

Assertion

```
<SAMLResponse>
    <Issuer>https://idp.com/</Issuer>
    <Assertion ID="id1337">
        <Subject>
            <NameID>user@lucideustech.com</NameID>
        </Subject>
    </Assertion>
```

Signature

```
<Signature>
    <SignedInfo>
        <CanonicalizationMethod Algorithm="xml-c14n11"/>
<Reference URI="id1337"/>
    <SignatureValue>
    JouQHKvwh64PSjlOjo+XVGGsLIIEyHV+I+F2nCq+dfgE=
    </SignatureValue>
<Signature>
</SAMLResponse>
```

Demo Time

Scenarios :

The Main goal is to bypass the **SSO** get the “admin” rights and delete the complaints.

Test Cases :

- Nothing Configured
- Signature Not Checked
- CVE-2017-11427

Remediation

- Validate Message Confidentiality and Integrity
- Validate Protocol Usage
- Validate Signatures
- Validate Protocol Processing Rules
- Input Validation
- Cryptography

Reference

- SAML Security
- A Breakdown of the New SAML Authentication Bypass Vulnerability
- Hacking SAML. Bypassing authentication using the… | by Vickie Li | The Startup
- Bypassing SAML 2.0 SSO with XML Signature Attacks • Aura Information Security Research Blog
- Bypassing SAML Authentication for Begineers
- yogisec/VulnerableSAMLApp: Vulnerable SAML infrastructure training applicaiton

Lab can be accessed at

http://68.183.41.129:8000/

Happy Hacking !!!