XACML: Exercise

Questions

Given the XACML policy and access request below, determine the access response.

Access Request

```xml
<Request>
  <Attributes
    Category="urn:oasis:names:tc:xacml:3.0:subject-category:access-subject">
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
      <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#string">
        Alice
      </AttributeValue>
    </Attribute>
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
      <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#string">
        accountant
      </AttributeValue>
    </Attribute>
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
      <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#string">
        engineer
      </AttributeValue>
    </Attribute>
  </Attributes>
  <Attributes
    Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:xpath">
      <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#string">
        order
      </AttributeValue>
    </Attribute>
  </Attributes>
  <Attributes
    Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
      <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#string">
        make
      </AttributeValue>
    </Attribute>
  </Attributes>
</Request>
```
Access Control Policy

<PolicySet
   xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
   PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permitoverrides"
   PolicySetId="RPS:manager:role">
   <Target>
      <AnyOf>
         <AllOf>
            <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  manager
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
         </AllOf>
      </AnyOf>
   </Target>
   <PolicySetIdReference>PPS:manager:role</PolicySetIdReference>
</PolicySet>

<PolicySet
   xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
   PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permitoverrides"
   PolicySetId="RPS:engineer:role">
   <Target>
      <AnyOf>
         <AllOf>
            <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  engineer
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
         </AllOf>
      </AnyOf>
   </Target>
   <PolicySetIdReference>PPS:engineer:role</PolicySetIdReference>
</PolicySet>

<PolicySet
   xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
   PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permitoverrides"
PolicySetId="RPS:accountant:role">
<Target>
<AnyOf>
<AllOf>
<Match

MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
<AttributeDesignator MustBePresent="false"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</Match>
</AllOf>
</AnyOf>
</Target>
</PolicySetIdReference>PPS:accountant:role</PolicySetIdReference>
</PolicySet>

PolicySetIdReference>PPS:accountant+engineer:role</PolicySetIdReference>
</PolicySet>

<PolicySet
xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides"
PolicySetId="RPS:accountant+engineer:role">
<Target>
<AnyOf>
<AllOf>
<Match

MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
<AttributeDesignator MustBePresent="false"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</Match>
<Match

MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">engineer</AttributeValue>
<AttributeDesignator MustBePresent="false"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</Match>
</AllOf>
</AnyOf>
</Target>
</PolicySetIdReference>PPS:accountant+engineer:role</PolicySetIdReference>
</PolicySet>
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides"
    PolicySetId="RPS:employee:role">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
            DataType="http://www.w3.org/2001/XMLSchema#string">
            employee
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
            AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <PolicySetIdReference>PPS:employee:role</PolicySetIdReference>
</PolicySet>

<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides"
    PolicySetId="PPS:manager:role">
  <Target />
  <Policy
    PolicyId="permission:manager:role"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
    <Target />
    <Rule RuleId="R:manager" Effect="Permit">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:function:string">
              <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">
                order
              </AttributeValue>
              <AttributeDesignator
                MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:attribute-category:resource"
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">
                approve
              </AttributeValue>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
  </Policy>
</PolicySet>
<AttributeDesignator
    MustBePresent="false"
    Category="urn:oasis:names:tc:xacml:1.0:attribute-category:action"
    AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
    DataType="http://www.w3.org/2001/XMLSchema#string"/>
</Match>
</AllOf>
</AnyOf>
</Target>
</Rule>
</Policy>
</PolicySet>

<PolicySet
    xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides"
    PolicySetId="PPS:engineer:role">  
    <Target/>
    <Policy
        PolicyId="permission:engineer:role"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
        <Target />
        <Rule RuleId="R:engineer" Effect="Permit">
            <Target />
            <AnyOf>
                <AllOf>
                    <Match
                        MatchId="urn:oasis:names:tc:xacml:1.0:function:function:string">
                        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                            order
                        </AttributeValue>
                        <AttributeDesignator
                            MustBePresent="false"
                            Category="urn:oasis:names:tc:xacml:1.0:attribute-category:resource"
                            AttributeId="urn:oasis:names:tc:xacml:1.0:resource-id"
                            DataType="http://www.w3.org/2001/XMLSchema#string"/>
                    </Match>
                    <Match
                        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                            make
                        </AttributeValue>
                        <AttributeDesignator
                            MustBePresent="false"
                            Category="urn:oasis:names:tc:xacml:1.0:attribute-category:action"
                            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                            DataType="http://www.w3.org/2001/XMLSchema#string"/>
                    </Match>
                </AllOf>
            </AnyOf>
        </Target>
    </Rule>
</PolicySet>
<PolicySet>
  <PolicySetIdReference>PPS:employee:role.xml</PolicySetIdReference>
</PolicySet>

<PolicySet
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides"
  PolicySetId="PPS:accountant:role">
  <Target />
  <Policy
    PolicyId="permission:accountant:role"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
    <Target />
    <Rule RuleId="R:accountant" Effect="Permit">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:function:string">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                order
              </AttributeValue>
              <AttributeDesignator
                MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:attribute-category:resource"
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                pay
              </AttributeValue>
              <AttributeDesignator
                MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:attribute-category:action"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
  </Policy>
</PolicySet>

<PolicySet
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides"
  PolicySetId="PPS:accountant+engineer:role">
  <Target />
</PolicySet>
<Policy
  PolicyId="permission:accountant+engineer:role"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permitoverrides">
  <Target />
  <Rule RuleId="R:accountant+engineer" Effect="Permit">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:function:string">
            <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">
              order
            </AttributeValue>
            <AttributeDesignator
              MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:1.0:attribute-category:resource"
              AttributeId="urn:oasis:names:tc:xacml:1.0:resource-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">
              modify
            </AttributeValue>
            <AttributeDesignator
              MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:1.0:attribute-category:action"
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
</Policy>

<PolicySetIdReference>PPS:accountant:role.xml</PolicySetIdReference>
</PolicySet>

<PolicySet
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permitoverrides"
  PolicySetId="PPS:employee:role">
  <Target />
  <Policy
    PolicyId="permission:employee:role"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permitoverrides">
    <Target />
    <Rule RuleId="R:employee" Effect="Permit">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:function:string">
              7
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
  </Policy>
</PolicySet>
<AttributeDesignator
    MustBePresent="false"
    Category="urn:oasis:names:tc:xacml:1.0:attribute-category:resource"
    AttributeId="urn:oasis:names:tc:xacml:1.0:resource-id"
    DataType="http://www.w3.org/2001/XMLSchema#string"/>
</Match>
<Match
    MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#string">
        read
    </AttributeValue>
    <AttributeDesignator
        MustBePresent="false"
        Category="urn:oasis:names:tc:xacml:1.0:attribute-category:action"
        AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
        DataType="http://www.w3.org/2001/XMLSchema#string"/>
</Match>
</AllOf>
</AnyOf>
</Target>
</Rule>
</Policy>
</PolicySet>