



# Attacking OData

- **Gursev Singh Kalra**

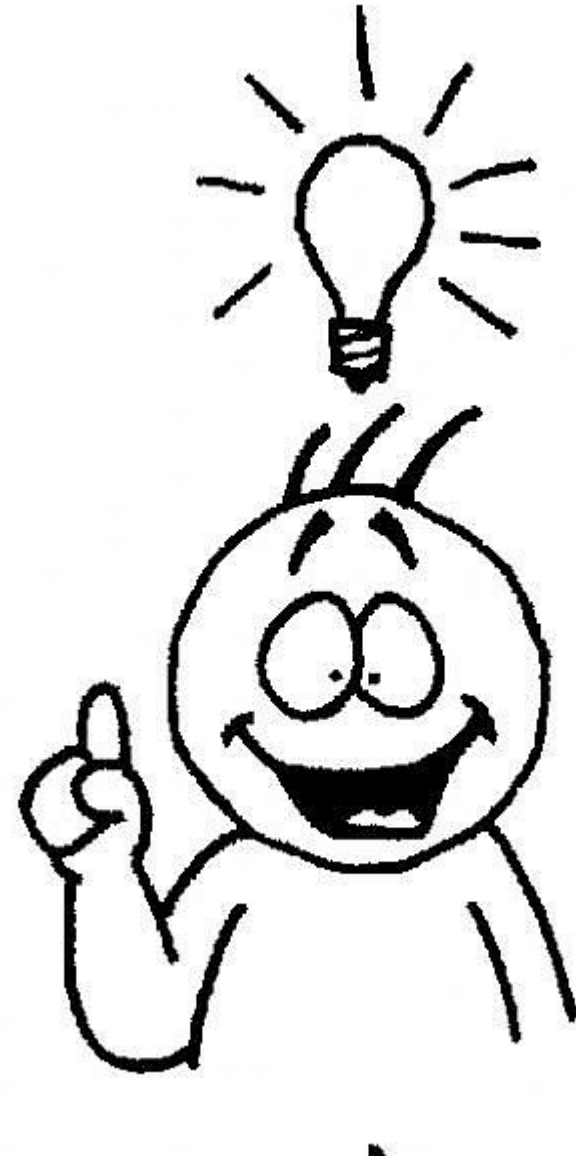
Principal Consultant

McAfee, Foundstone Professional Services

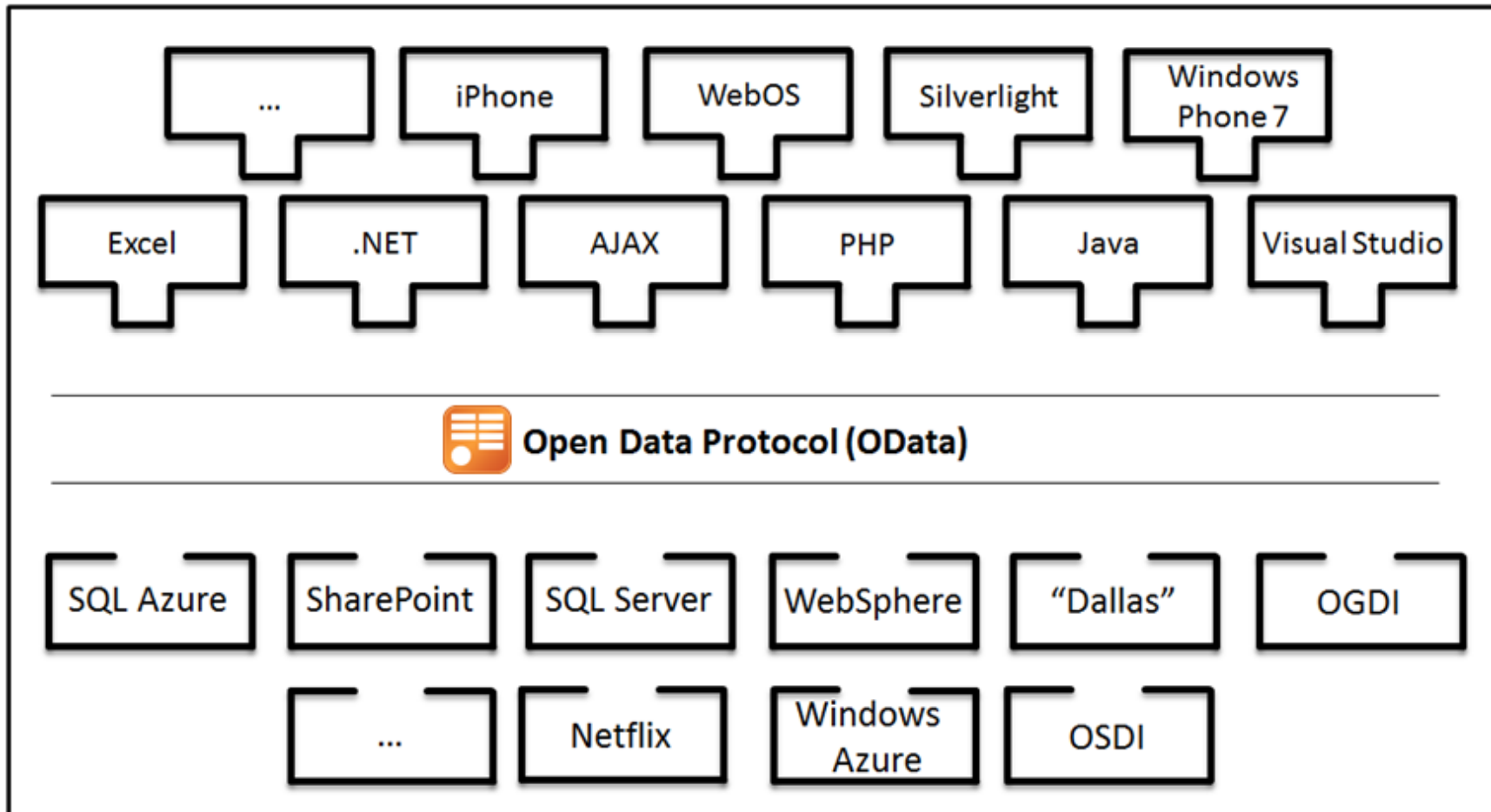
# Agenda

- OData Primer
- Oyedata for OData Assessments
- Oyedata Demonstrations
- Ofuzz Demonstration
- Attacking OData Services

# ODATA PRIMER



# Why OData?



\* <http://geekswithblogs.net>

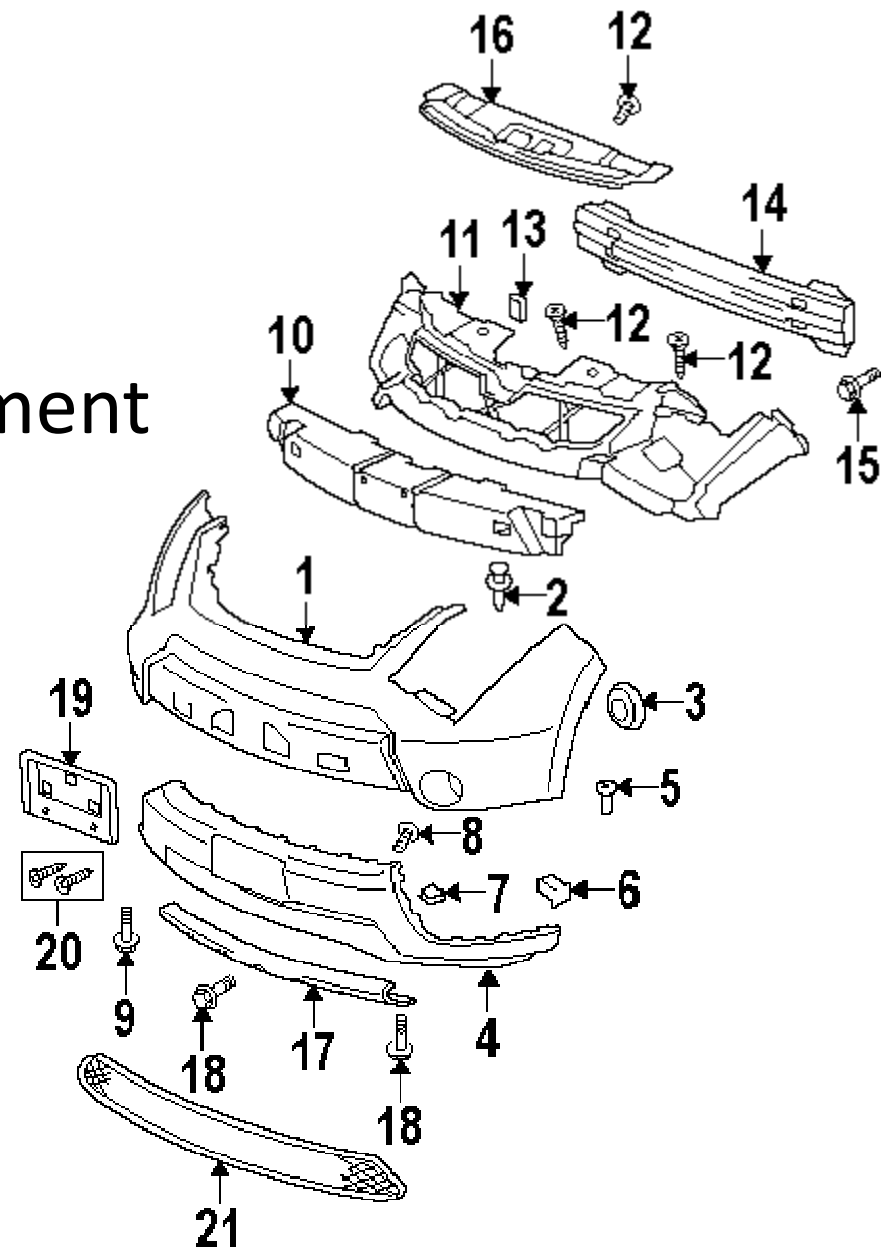
# What is OData?



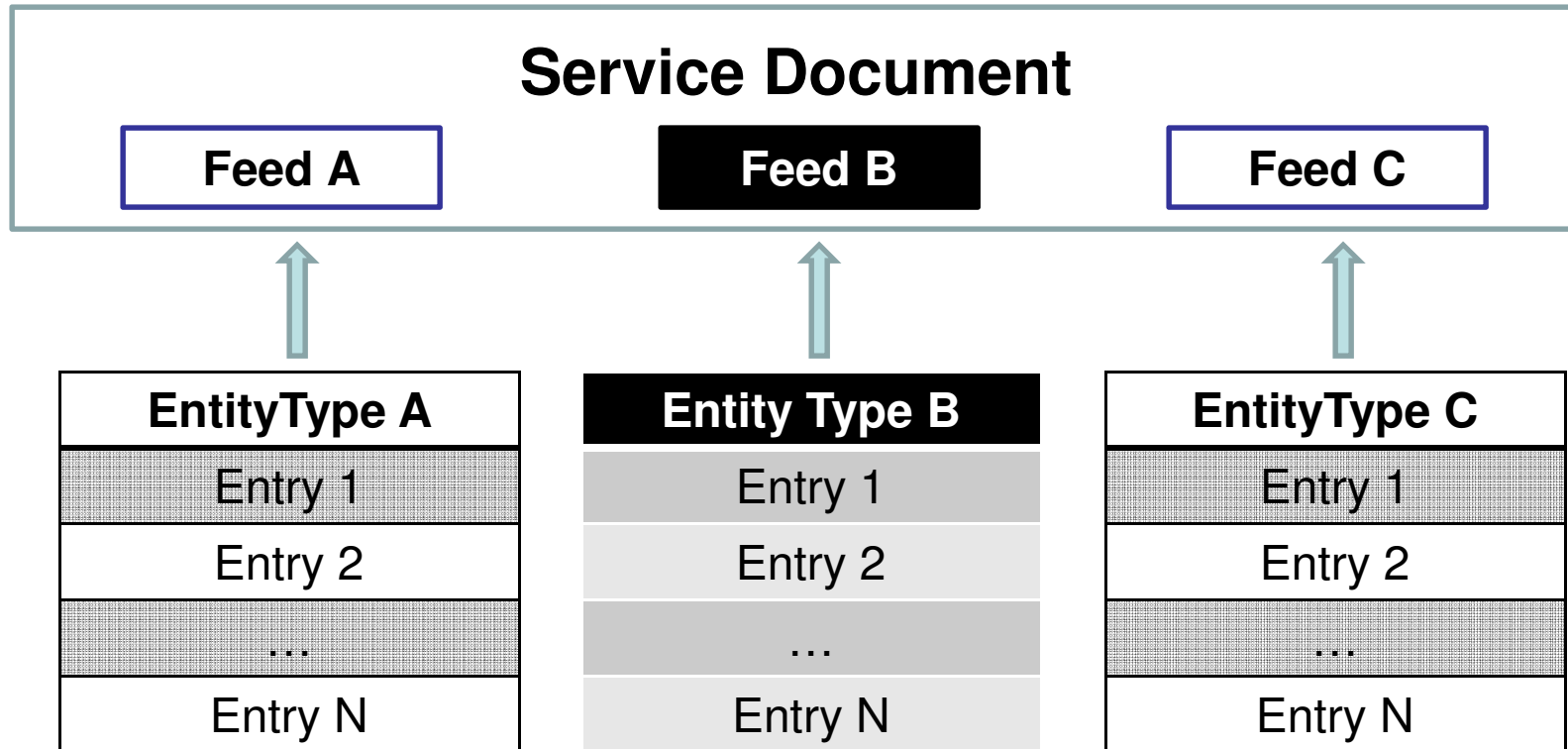
- Query and Update Data over the Web.  
JDBC/ODBC for the Internet
- Resources identified using Uniform Resource Identifiers (URIs)
- HTTP based RESTful data services
  - Relies on PUT, POST, DELETE and GET methods
- Adopted by Microsoft, IBM, SAP etc...

# O - Overwhelming

- Open Data Protocol
- Service Metadata Document
- Entries and Entity Types
- EDMDataTypes, CSDL
- Service Document
- Service Operations
- Complex Types
- Feeds, **more...**



# Entity Types, Feeds & Service Doc



# Building Blocks

```
<?xml version="1.0" encoding="iso-8859-1" standalone="yes"?>
<edmx:Edmx Version="1.0" xmlns:edmx="http://schemas.microsoft.com/ado/2007/06/edmx"
  <edmx:DataServices xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices"
    <Schema Namespace="ODataDemo" xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices"
      <EntityType Name="Supplier">
        <Key>
          <PropertyRef Name="ID" />
        </Key>
        <Property Name="ID" Type="Edm.Int32" Nullable="false" />
        <Property Name="Name" Type="Edm.String" Nullable="true" m:FC_TargetPath="m:Name" />
        <Property Name="Address" Type="ODataDemo.Address" Nullable="false" />
        <Property Name="Concurrency" Type="Edm.Int32" Nullable="false" Concurrency="true" />
        <NavigationProperty Name="Products" Relationship="ODataDemo.Product_Supplier" />
      </EntityType>
      <ComplexType Name="Address">
        <Property Name="Street" Type="Edm.String" Nullable="true" />
        <Property Name="City" Type="Edm.String" Nullable="true" />
        <Property Name="State" Type="Edm.String" Nullable="true" />
        <Property Name="ZipCode" Type="Edm.String" Nullable="true" />
        <Property Name="Country" Type="Edm.String" Nullable="true" />
      </ComplexType>
```



# Entity Type and Entry

## Entity Type

```
<EntityType Name="Supplier">
  <Key>
    <PropertyRef Name="ID" />
  </Key>
  <Property Name="ID" Type="Edm.Int32" Nullable="true" />
  <Property Name="Name" Type="Edm.String" />
  <Property Name="Address" Type="ODataDemo.Address" />
  <Property Name="Concurrency" Type="Edm.Int32" />
  <NavigationProperty Name="Products" Relationship="SupplierProducts" />
</EntityType>
<ComplexType Name="Address">
  <Property Name="Street" Type="Edm.String" />
  <Property Name="City" Type="Edm.String" />
  <Property Name="State" Type="Edm.String" />
  <Property Name="ZipCode" Type="Edm.String" />
  <Property Name="Country" Type="Edm.String" />
</ComplexType>
```

## Entry

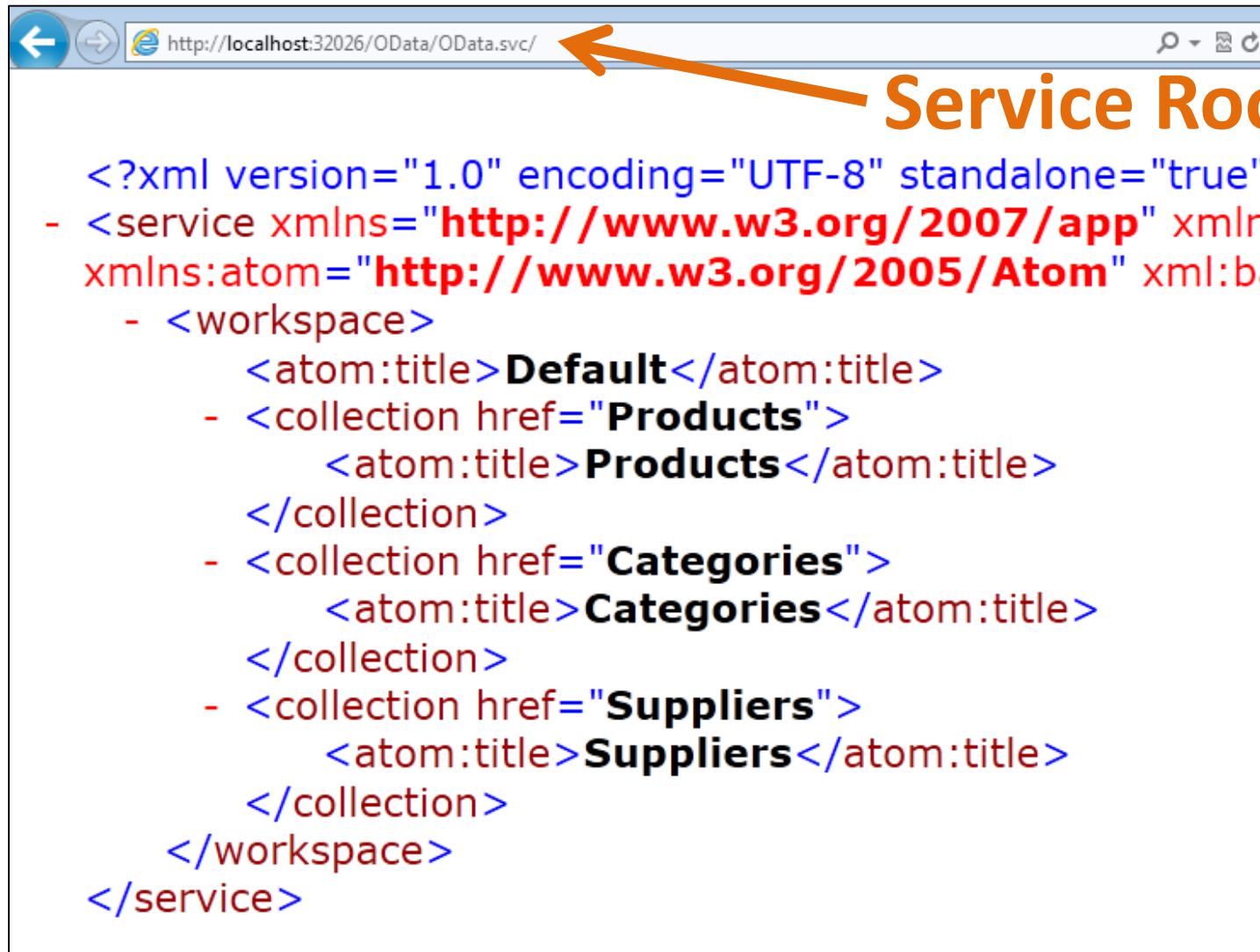
```
<entry m:etag="W/"0"">
  <id>http://localhost:32026/OData/OData.svc/Suppliers(0)</id>
  <title type="text">Exotic Liquids</title>
  <updated>2012-11-09T05:20:22Z</updated>
  <author>
    <name />
  </author>
  <link rel="edit" title="Supplier" href="Suppliers(0)" />
  <link rel="http://schemas.microsoft.com/ado/2007/08/dataservice/operations/insertentity" title="Create" href="Suppliers(0)" />
  <category term="ODataDemo.Supplier" scheme="http://schemas.microsoft.com/ado/2007/08/dataservice/schemas/ODataDemo" />
  <content type="application/xml">
    <m:properties>
      <d:ID m:type="Edm.Int32">0</d:ID>
      <d:Name>Exotic Liquids</d:Name>
      <d:Concurrency m:type="Edm.Int32">0</d:Concurrency>
      <d:Address m:type="ODataDemo.Address">
        <d:Street>NE 228th</d:Street>
        <d:City>Sammamish</d:City>
        <d:State>WA</d:State>
        <d:ZipCode>98074</d:ZipCode>
        <d:Country>USA</d:Country>
      </d:Address>
    </m:properties>
  </content>
</entry>
```

# Feeds

- Collection of Typed Entries
- An OData Service can have one or more feeds
- Service Document lists all top-level Feeds

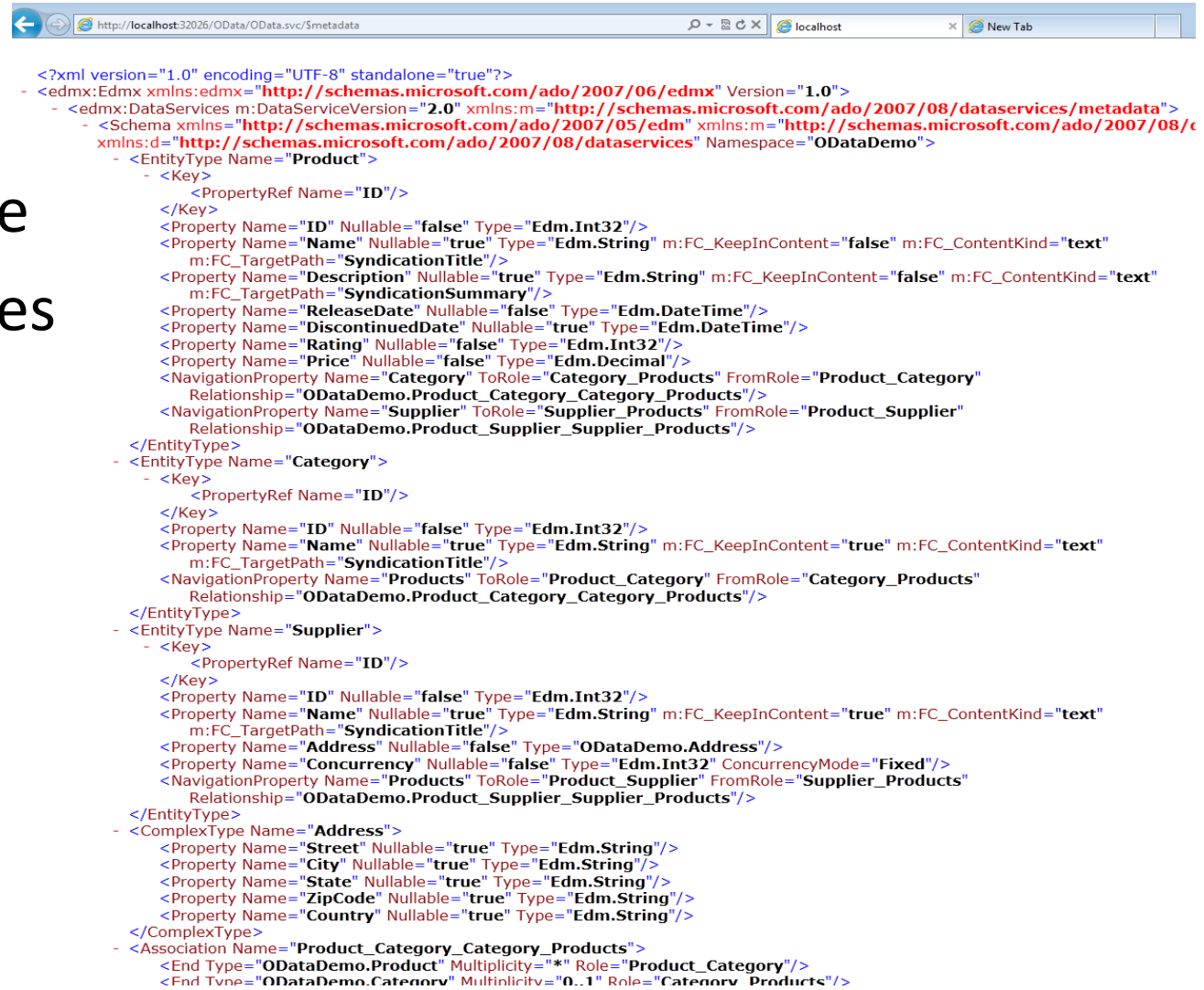


# Service Document



# Service Metadata Document

- **\*DNA\*** of an OData Service
- CSDL describes Data Model
- **/\$metadata**



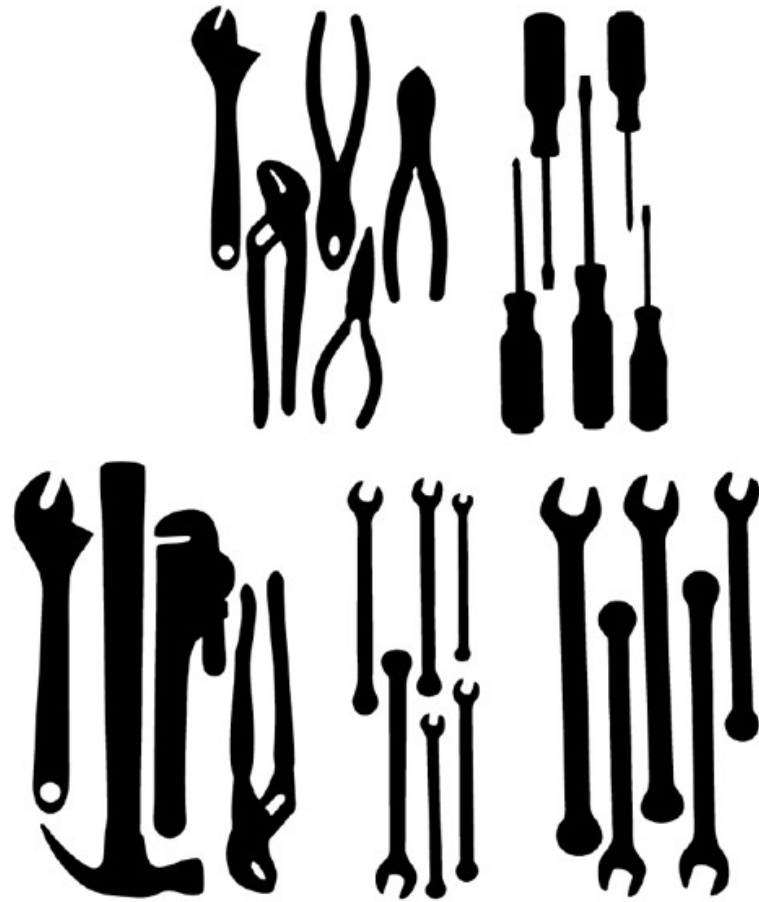
```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <edmx:Edmx xmlns:edmx="http://schemas.microsoft.com/ado/2007/06/edmx" Version="1.0">
  - <edmx:DataServices m:DataServiceVersion="2.0" xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata">
    - <Schema xmlns="http://schemas.microsoft.com/ado/2007/05/edmx" xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices" Namespace="ODataDemo">
      - <EntityType Name="Product">
        - <Key>
          <PropertyRef Name="ID"/>
        </Key>
        <Property Name="ID" Nullable="false" Type="Edm.Int32"/>
        <Property Name="Name" Nullable="true" Type="Edm.String" m:FC_KeepInContent="false" m:FC_ContentKind="text" m:FC_TargetPath="SyndicationTitle"/>
        <Property Name="Description" Nullable="true" Type="Edm.String" m:FC_KeepInContent="false" m:FC_ContentKind="text" m:FC_TargetPath="SyndicationSummary"/>
        <Property Name="ReleaseDate" Nullable="false" Type="Edm.DateTime"/>
        <Property Name="DiscontinuedDate" Nullable="true" Type="Edm.DateTime"/>
        <Property Name="Rating" Nullable="false" Type="Edm.Int32"/>
        <Property Name="Price" Nullable="false" Type="Edm.Decimal"/>
        <NavigationProperty Name="Category" ToRole="Category_Products" FromRole="Product_Category" Relationship="ODataDemo.Product_Category_Category_Products"/>
        <NavigationProperty Name="Supplier" ToRole="Supplier_Products" FromRole="Product_Supplier" Relationship="ODataDemo.Product_Supplier_Supplier_Products"/>
      </EntityType>
      - <EntityType Name="Category">
        - <Key>
          <PropertyRef Name="ID"/>
        </Key>
        <Property Name="ID" Nullable="false" Type="Edm.Int32"/>
        <Property Name="Name" Nullable="true" Type="Edm.String" m:FC_KeepInContent="true" m:FC_ContentKind="text" m:FC_TargetPath="SyndicationTitle"/>
        <NavigationProperty Name="Products" ToRole="Product_Category" FromRole="Category_Products" Relationship="ODataDemo.Product_Category_Category_Products"/>
      </EntityType>
      - <EntityType Name="Supplier">
        - <Key>
          <PropertyRef Name="ID"/>
        </Key>
        <Property Name="ID" Nullable="false" Type="Edm.Int32"/>
        <Property Name="Name" Nullable="true" Type="Edm.String" m:FC_KeepInContent="true" m:FC_ContentKind="text" m:FC_TargetPath="SyndicationTitle"/>
        <Property Name="Address" Nullable="false" Type="ODataDemo.Address"/>
        <Property Name="Concurrency" Nullable="false" Type="Edm.Int32" ConcurrencyMode="Fixed"/>
        <NavigationProperty Name="Products" ToRole="Product_Supplier" FromRole="Supplier_Products" Relationship="ODataDemo.Product_Supplier_Supplier_Products"/>
      </EntityType>
      - <ComplexType Name="Address">
        <Property Name="Street" Nullable="true" Type="Edm.String"/>
        <Property Name="City" Nullable="true" Type="Edm.String"/>
        <Property Name="State" Nullable="true" Type="Edm.String"/>
        <Property Name="ZipCode" Nullable="true" Type="Edm.String"/>
        <Property Name="Country" Nullable="true" Type="Edm.String"/>
      </ComplexType>
      - <Association Name="Product_Category_Category_Products">
        <End Type="ODataDemo.Product" Multiplicity="*" Role="Product_Category"/>
        <End Type="ODataDemo.Category" Multiplicity="0..1" Role="Category_Products"/>
      </Association>
    </Schema>
  </edmx:DataServices>
</edmx:Edmx>
```

# Service Operations

- Remotely Invoked Custom Functions
- Accept Primitive Data Via GET or POST
- Return primitives, complex types, feeds or a void



*\*<http://img.ehowcdn.com>*



## OYEDATA AND OFUZZ

# Fuzzing OData (One Entity)

## Service Metadata Document

```
<EntityType Name="Title" m:HasStream="true">
  <Key>
    <PropertyRef Name="Id"/>
  </Key>

  <Property Name="Id" Type="Edm.String" Nullable="false" MaxLength="128" Unicode="true" FixedL
  <Property Name="Name" Type="Edm.String" Nullable="true" MaxLength="Max" Unicode="true" Fixed
  <Property Name="ShortName" Type="Edm.String" Nullable="true" MaxLength="Max" Unicode="true"
  <Property Name="Synopsis" Type="Edm.String" Nullable="true" MaxLength="Max" Unicode="true" F
  <Property Name="ShortSynopsis" Type="Edm.String" Nullable="true" MaxLength="Max" Unicode="tr
  <Property Name="AverageRating" Type="Edm.Double" Nullable="true"/>
  <Property Name="ReleaseYear" Type="Edm.Int32" Nullable="true"/>
  <Property Name="Url" Type="Edm.String" Nullable="true" MaxLength="Max" Unicode="true" FixedL
  <Property Name="Runtime" Type="Edm.Int32" Nullable="true"/>
  <Property Name="Rating" Type="Edm.String" Nullable="true" MaxLength="Max" Unicode="true" Fix
  <Property Name="DateModified" Type="Edm.DateTime" Nullable="false" m:FC_TargetPath="Syndicat
  <Property Name="Type" Type="Edm.String" Nullable="true" MaxLength="Max" Unicode="true" Fixed
  <Property Name="WebsiteUrl" Type="Edm.String" Nullable="true" MaxLength="Max" Unicode="true"
  <Property Name="NetflixAplId" Type="Edm.String" Nullable="true" MaxLength="Max" Unicode="tru
  <Property Name="TinyUrl" Type="Edm.String" Nullable="true" MaxLength="Max" Unicode="true" Fi
  <Property Name="BluRay" Type="Netflix.Catalog.v2.DeliveryFormatAvailability" Nullable="false
  <Property Name="BoxArt" Type="Netflix.Catalog.v2.BoxArt" Nullable="false"/>
  <Property Name="Dvd" Type="Netflix.Catalog.v2.DeliveryFormatAvailability" Nullable="false"/>
  <Property Name="Instant" Type="Netflix.Catalog.v2.InstantAvailability" Nullable="false"/>

  <NavigationProperty Name="Disco" Relationship="Netflix.Catalog.v2.Title_Disco" FromRole="Title
  <NavigationProperty Name="Season" Relationship="Netflix.Catalog.v2.Title_Season" FromRole="T
  <NavigationProperty Name="Series" Relationship="Netflix.Catalog.v2.Title_Series" FromRole="T
  <NavigationProperty Name="Movie" Relationship="Netflix.Catalog.v2.Title_Movie" FromRole="Tit
  <NavigationProperty Name="AudioFormats" Relationship="Netflix.Catalog.v2.TitleAudioFormat_Ti
  <NavigationProperty Name="Awards" Relationship="Netflix.Catalog.v2.TitleAward_Title" FromRol
  <NavigationProperty Name="ScreenFormats" Relationship="Netflix.Catalog.v2.TitleScreenFormat_
  <NavigationProperty Name="Languages" Relationship="Netflix.Catalog.v2.Language_Titles" FromR
  <NavigationProperty Name="Cast" Relationship="Netflix.Catalog.v2.Person_TitlesActedIn" FromR
  <NavigationProperty Name="Directors" Relationship="Netflix.Catalog.v2.Person_TitlesDirected"
  <NavigationProperty Name="Discs" Relationship="Netflix.Catalog.v2.Title_Discs" FromRole="Tit
  <NavigationProperty Name="Episodes" Relationship="Netflix.Catalog.v2.Title_Episodes" FromRol
  <NavigationProperty Name="Genres" Relationship="Netflix.Catalog.v2.Genre_Titles" FromRole="G
  <NavigationProperty Name="Seasons" Relationship="Netflix.Catalog.v2.Title_Seasons" FromRole=
</EntityType>
```

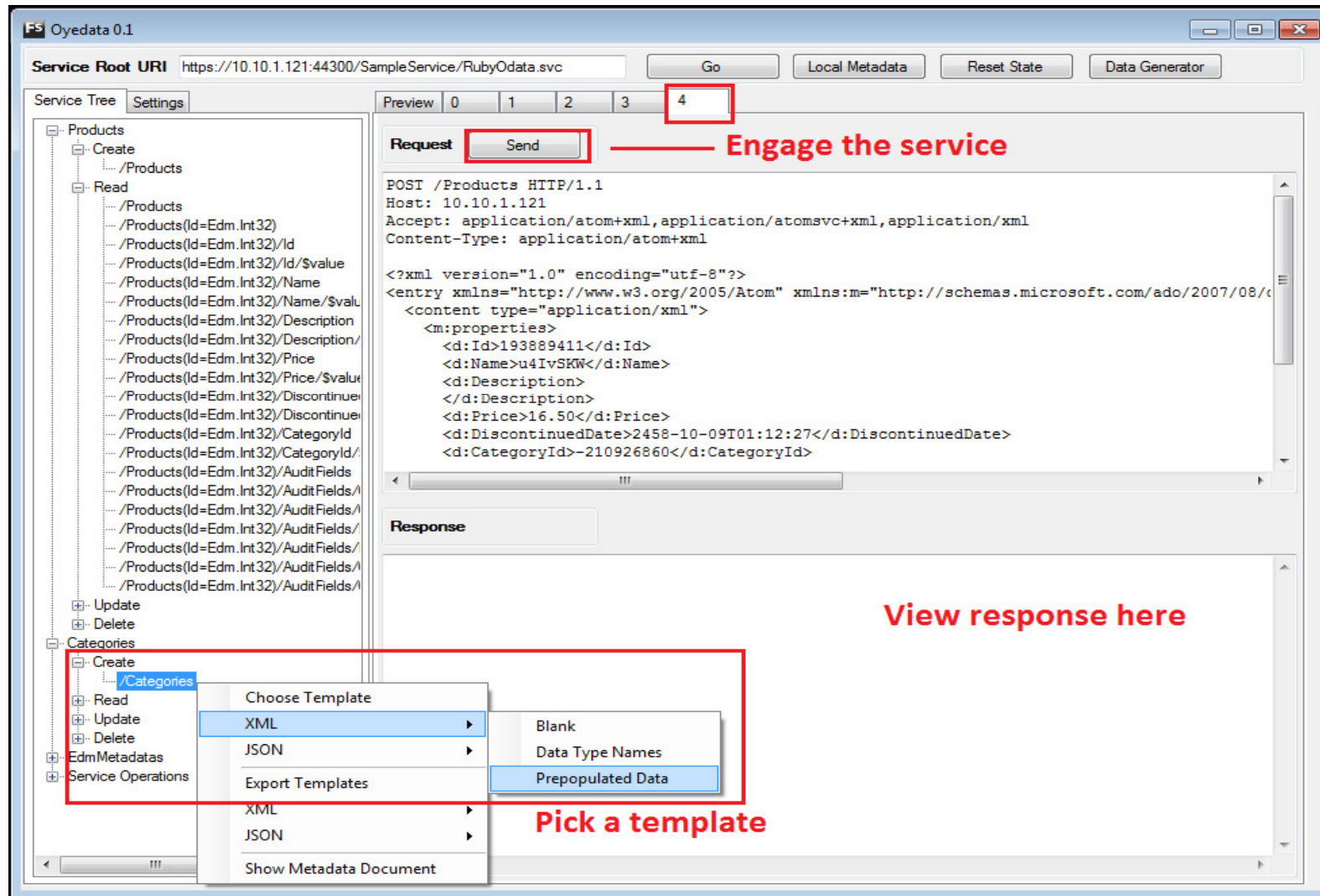


## Fuzzing Template

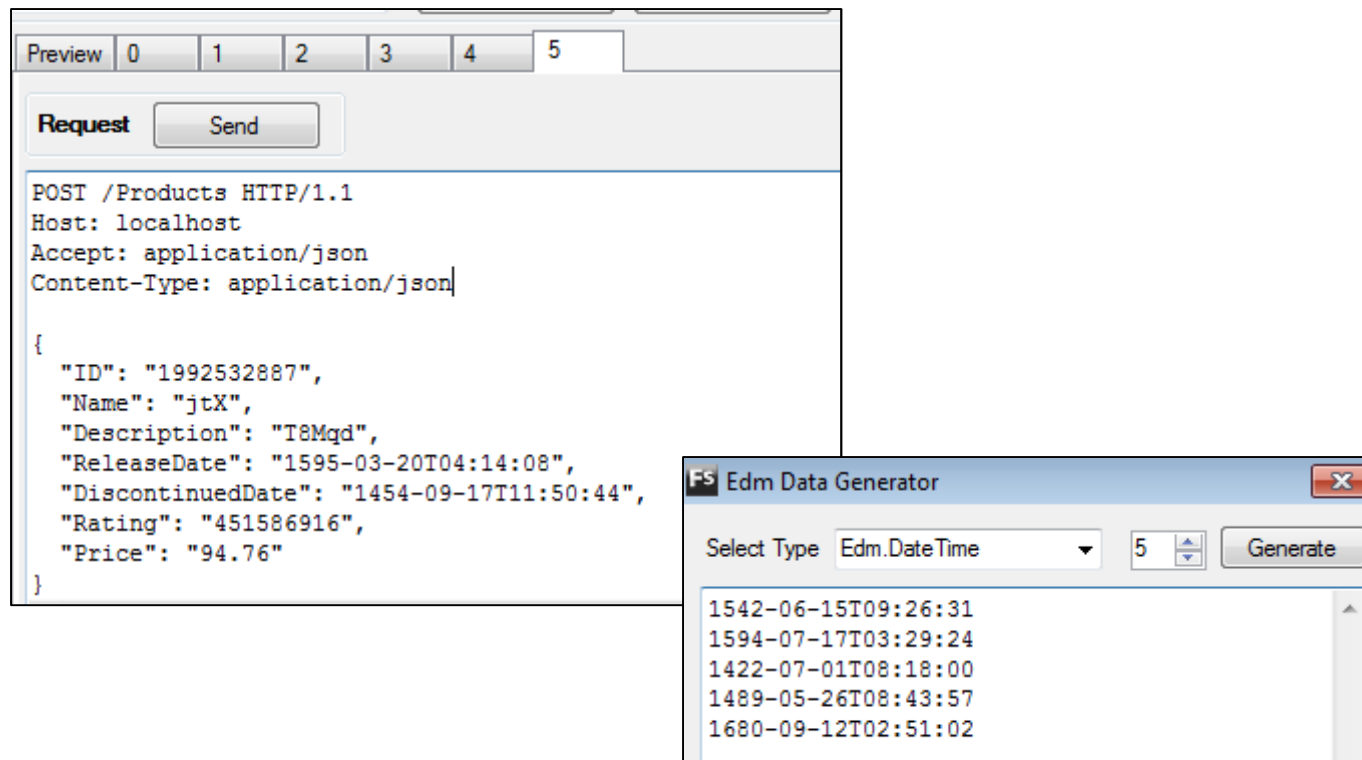
```
<?xml version="1.0" encoding="utf-8"?>
<entry xmlns="http://www.w3.org/2005/Atom" xmlns:m="http://schemas.microsoft.com/ado/2007/08/datas
  <content type="application/xml">
    <m:properties>
      <d:Id> Edm.String* </d:Id>
      <d:Name> Edm.String^ </d:Name>
      <d:ShortName> Edm.String^ </d:ShortName>
      <d:Synopsis> Edm.String^ </d:Synopsis>
      <d:ShortSynopsis> Edm.String^ </d:ShortSynopsis>
      <d:AverageRating> Edm.Double^ </d:AverageRating>
      <d:ReleaseYear> Edm.Int32^ </d:ReleaseYear>
      <d:Url> Edm.String^ </d:Url>
      <d:Runtime> Edm.Int32^ </d:Runtime>
      <d:Rating> Edm.String^ </d:Rating>
      <d:DateModified> Edm.DateTime </d:DateModified>
      <d:Type> Edm.String^ </d:Type>
      <d:WebsiteUrl> Edm.String^ </d:WebsiteUrl>
      <d:NetflixAplId> Edm.String^ </d:NetflixAplId>
      <d:TinyUrl> Edm.String^ </d:TinyUrl>
      <d:BluRay>
        <d:Available> Edm.Boolean </d:Available>
        <d:AvailableFrom> Edm.DateTime^ </d:AvailableFrom>
        <d:AvailableTo> Edm.DateTime^ </d:AvailableTo>
        <d:Rating> Edm.String^ </d:Rating>
        <d:Runtime> Edm.Int32^ </d:Runtime>
      </d:BluRay>
      <d:BoxArt>
        <d:SmallUrl> Edm.String^ </d:SmallUrl>
        <d:MediumUrl> Edm.String^ </d:MediumUrl>
        <d:LargeUrl> Edm.String^ </d:LargeUrl>
        <d:HighDefinitionUrl> Edm.String^ </d:HighDefinitionUrl>
      </d:BoxArt>
      <d:Dvd>
        <d:Available> Edm.Boolean </d:Available>
        <d:AvailableFrom> Edm.DateTime^ </d:AvailableFrom>
        <d:AvailableTo> Edm.DateTime^ </d:AvailableTo>
        <d:Rating> Edm.String^ </d:Rating>
        <d:Runtime> Edm.Int32^ </d:Runtime>
      </d:Dvd>
      <d:Instant>
        <d:Available> Edm.Boolean </d:Available>
        <d:AvailableFrom> Edm.DateTime^ </d:AvailableFrom>
        <d:AvailableTo> Edm.DateTime^ </d:AvailableTo>
        <d:HighDefinitionAvailable> Edm.Boolean </d:HighDefinitionAvailable>
        <d:Rating> Edm.String^ </d:Rating>
        <d:Runtime> Edm.Int32^ </d:Runtime>
      </d:Instant>
    </m:properties>
  </content>
</entry>
```



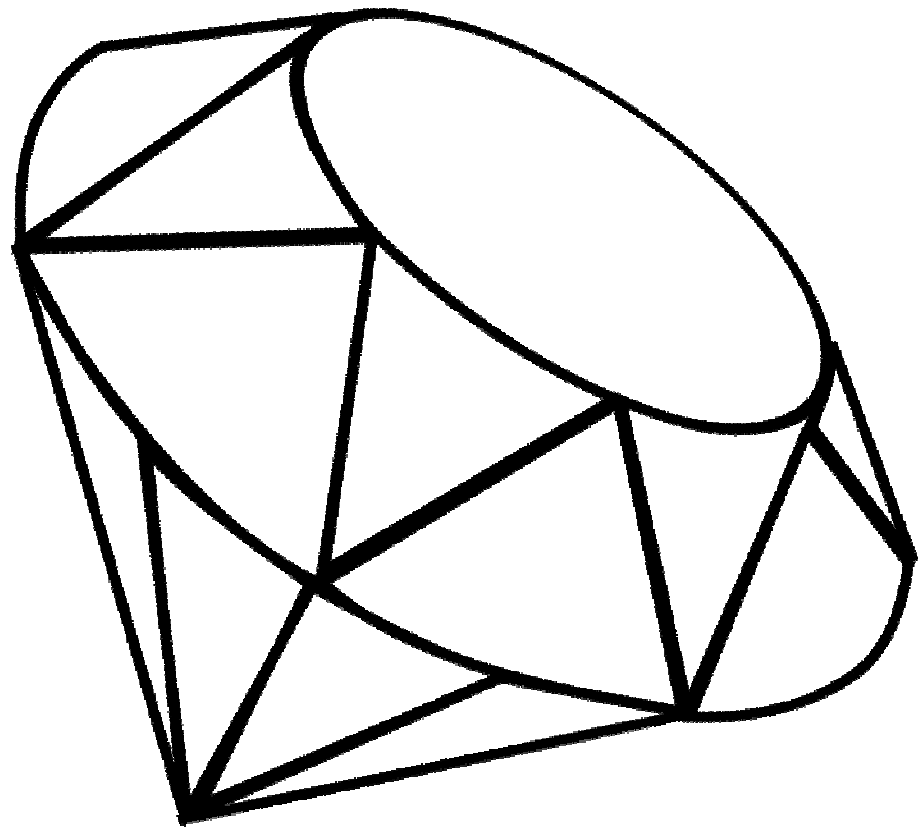
# Few Oyedata Features







# OYEDATA DEMONSTRATIONS



# OFUZZ DEMONSTRATION



# ATTACKING ODATA SERVICES

# OData on Security

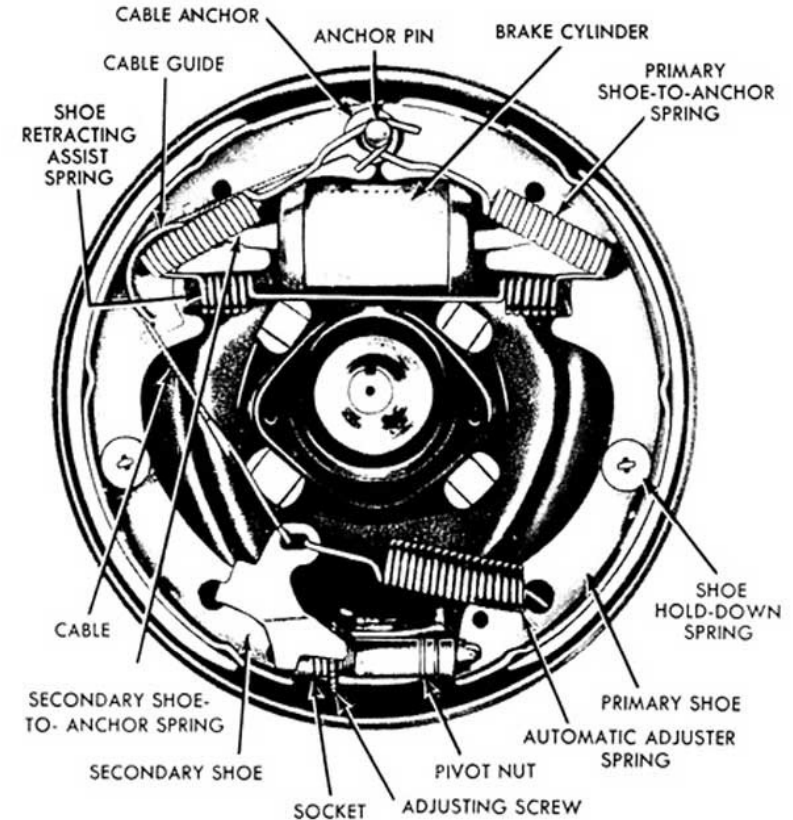
- No Security Specifications
- Based on HTTP, AtomPub, and JSON
- Security considerations for several technologies involved



*\*<http://bowtielaw.files.wordpress.com>*

# Enumeration

- Service Document
- Service Metadata Document
- Tools (Oyedata, Linqpad, etc...)
- HTTP Methods
  - PUT and DELETE



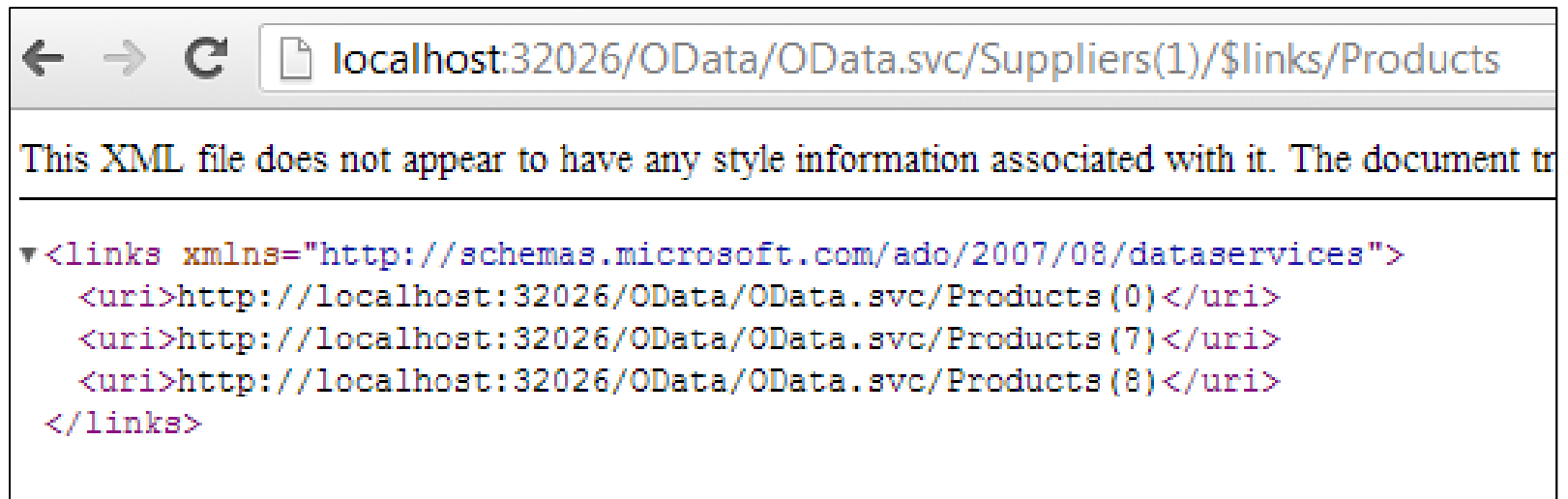
# HTTP Verb Tunneling

- Allows to tunnel HTTP methods with POST
- Can be abused to execute unauthorized verbs

```
POST /Products(1) HTTP/1.1
Host: localhost:32026
Accept: application/atom+xml,application/atom+xml
X-HTTP-METHOD: DELETE
Content-Type: application/atom+xml
```

# Navigation Properties

- `http://localhost:32026/OData/OData.svc/Suppliers(1)/Products`
- Can be used as a springboard to other Entry Type's additional data




The screenshot shows a web browser window with the address bar containing the URL `localhost:32026/OData/OData.svc/Suppliers(1)/$links/Products`. Below the address bar, a message states: "This XML file does not appear to have any style information associated with it. The document tr". The main content area displays an XML snippet:

```
<links xmlns="http://schemas.microsoft.com/ado/2007/08/dataservices">  
  <uri>http://localhost:32026/OData/OData.svc/Products(0)</uri>  
  <uri>http://localhost:32026/OData/OData.svc/Products(7)</uri>  
  <uri>http://localhost:32026/OData/OData.svc/Products(8)</uri>  
</links>
```

# System Query Options

- Control the amount and type of data returned by the OData service.
- **\$select, \$format, \$expand, \$filter, \$orderby** etc...
- Assess like regular web application parameters



```
<?xml version="1.0" encoding="iso-8859-1" standalone="yes"?>
<feed xml:base="http://localhost:32026/OData/OData.svc/" xmlns:d="http://schemas.microsoft.com/ado/2007/08/data/services/metadata"
  xmlns:m="http://schemas.microsoft.com/ado/2007/08/data/services/metadata"
  <title type="text">Products</title>
  <id>http://localhost:32026/OData/OData.svc/Products</id>
  <updated>2012-11-12T04:31:20Z</updated>
  <link rel="self" title="Products" href="Products" />
  <entry>
    <id>http://localhost:32026/OData/OData.svc/Products(0)</id>
    <title type="text">Bread</title>
    <summary type="text">Whole grain bread</summary>
    <updated>2012-11-12T04:31:20Z</updated>
    <author>
      <name />
    </author>
    <link rel="edit" title="Product" href="Products(0)" />
    <category term="ODataDemo.Product" scheme="http://schemas.microsoft.com/ado/2007/08/data/services/metadata" />
    <content type="application/xml">
      <m:properties>
        <d:ID m:type="Edm.Int32">0</d:ID>
      </m:properties>
    </content>
  </entry>
```



# Assessing OData Operations

- Key Enumeration and Entry Access
- Individual Property Access
- Write and Update operations (POST & PUT)
- Delete operations (DELETE)
- Service Operations

# Data Validation and Error Handling

- Can be performed as per regular WAPT
- Malformed JSON and XML requests
- Database Integrity Checks

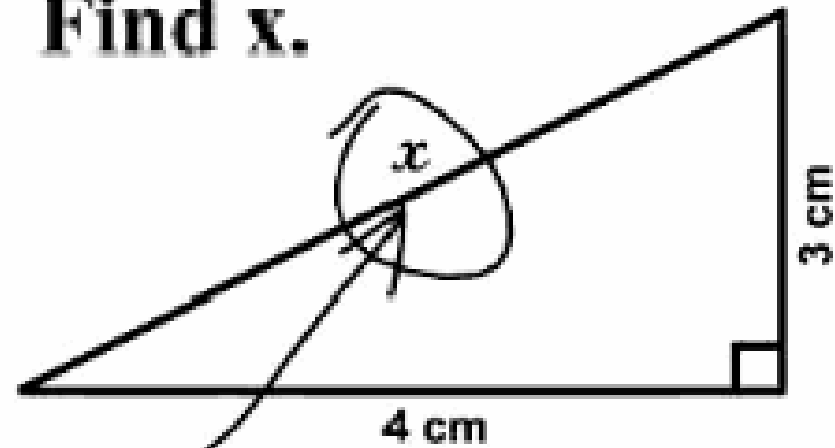
# Additional Considerations

- Access File Systems, Databases, CMS and others...
- Framework Generates Tons of Dynamic Code
- SQLi, Remote File Access, XPath Injection and Framework Specific Vulnerabilities

# Further Reading and References

- Official OData website
  - <http://www.odata.org>
- Oyedata
  - <http://www.mcafee.com/us/downloads/free-tools/oyedata.aspx>
- A Pentester's Guide to Hacking OData
  - <http://www.mcafee.com/us/resources/white-papers/foundstone/wp-pentesters-guide-to-hacking-odata.pdf>

**Find  $x$ .**



*Here it is*



**THANK YOU!**