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
Why OData?

[Diagram showing various technologies and systems connected to 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

Service Document

Feed A

EntityType A

Entry 1
Entry 2
...
Entry N

Feed B

Entity Type B

Entry 1
Entry 2
...
Entry N

Feed C

EntityType C

Entry 1
Entry 2
...
Entry N
Building Blocks

```xml
<?xml version="1.0" encoding="iso-8859-1" standalone="yes"?>
<edmx:DataServices xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservi
    <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="">
      <Property Name="Address" Type="ODataDemo.Address" Nullable="false"/>
      <Property Name="Concurrency" Type="Edm.Int32" Nullable="false" Concurrer
      <NavigationProperty Name="Products" Relationship="ODataDemo.Product_Supp
      <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**

```xml
<EntityType Name="Supplier">
  <Key>
    <PropertyRef Name="ID" />
  </Key>

  <Property Name="ID" Type="Edm.Int32" Nullable="false" />
  <Property Name="Name" Type="Edm.String" />
  <Property Name="Address" Type="ODataDemo.Address" />
  <Property Name="Concurrency" Type="Edm.Int32" />
  <NavigationProperty Name="Products" RelatedEntityName="Product" />
</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**

```xml
<entry m:etag="W/"&quot;0&quot;="/&gt;
  <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" type="application/json" title="Suppliers(0)" />
  <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: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

```xml
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
  - <workspace>
    <atom:title>Default</atom:title>
    - <collection href="Products">
      <atom:title>Products</atom:title>
    </collection>
    - <collection href="Categories">
      <atom:title>Categories</atom:title>
    </collection>
    - <collection href="Suppliers">
      <atom:title>Suppliers</atom:title>
    </collection>
  </workspace>
</service>
```
Service Metadata Document

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

*http://cdn2.bigcommerce.com
Fuzzing OData (One Entity)

Service Metadata Document

Fuzzing Template
Few Oyedata Features

Engage the service

View response here

Pick a template
OYEDATA DEMONSTRATIONS
OFUZZ DEMONSTRATION
ATTACKING ODATA SERVICES

*http://www.securityheavy.com
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/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
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
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

• A Pentester’s Guide to Hacking OData
Find $x$.

Here it is.
THANK YOU!