



B7 Selected Technical Security Considerations of the OData Protocol

Tuesday, March 24 2015

2:00 PM

John Willson

IT Architect

DSSLtd.com



Presentation will be
available at:

www.misti.com/download

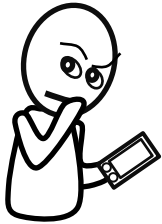
Download password is available in your Show Guide

Selected Technical Security Considerations of the OData Protocol

“open by default, secure by design”

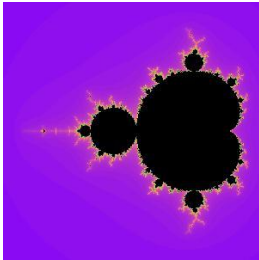
Overview

“open by default, secure by design”



- Your Presenter
- Open Data & OData
- OData Dependencies
- Common Attack Vectors
- Well Formed OData
- Housekeeping

John Willson

- Software technologist { first language Fortran II in 1968 – current language C#; first web experience Mosaic 1994 – current DNS/HTTPS; ... }
- IT architect { Visio 2 - Client-Server; Mindjet Data Sharing Protocol; ... }
- Consultant { KPMG 1979; current DSS Ltd.; ... }
- {

}
- Open data evangelist



JSON OData's Emerging State

- Open data and OData
- Other major data exchange protocols
- Rapid OData adoption





OData's Emerging State



[DATA](#) [TOPICS](#) [IMPACT](#) [APPLICATIONS](#) [DEVELOPERS](#) [CONTACT](#)

The home of the U.S. Government's open data

Here you will find data, tools, and resources to conduct research, develop web and mobile applications, design data visualizations, and more.

GET STARTED

SEARCH OVER 155,386 DATASETS



BROWSE TOPICS



Agriculture



Climate



Education



Energy



Finance



Geospatial



Global
Development



Health



Jobs & Skills



Public Safety



Science &
Research



Weather



OData's Emerging State



DATA TOPICS IMPACT APPLICATIONS DEVELOPERS CONTACT

DATA CATALOG

/ Datasets Organizations ?

Federal datasets are subject to the U.S. Federal Government **Data Policy**. Non-federal participants (e.g., universities, organizations, and tribal, state, and local governments) maintain their own data policies. Data policies influence the usefulness of the data. [Learn more](#) about how to search for data and use this catalog.



Order by:
Relevance

Datasets ordered by Relevance

You are searching in the list of datasets. [Show results in entire Data.gov site.](#)

Filter by location

Clear

Enter location...



Map data CC-BY-SA by [OpenStreetMap](#)
Tiles by [MapQuest](#)

Dataset Type

A-Z

1-9

Clear All

non-geospatial (1)

Topic Categories

A-Z

1-9

Clear All

1 dataset found for "odata"

census_tracts_odata2

City of San Francisco — census_tracts_odata2

CSV

application/rdf+xml

JSON

XML

1 dataset found for "odata"

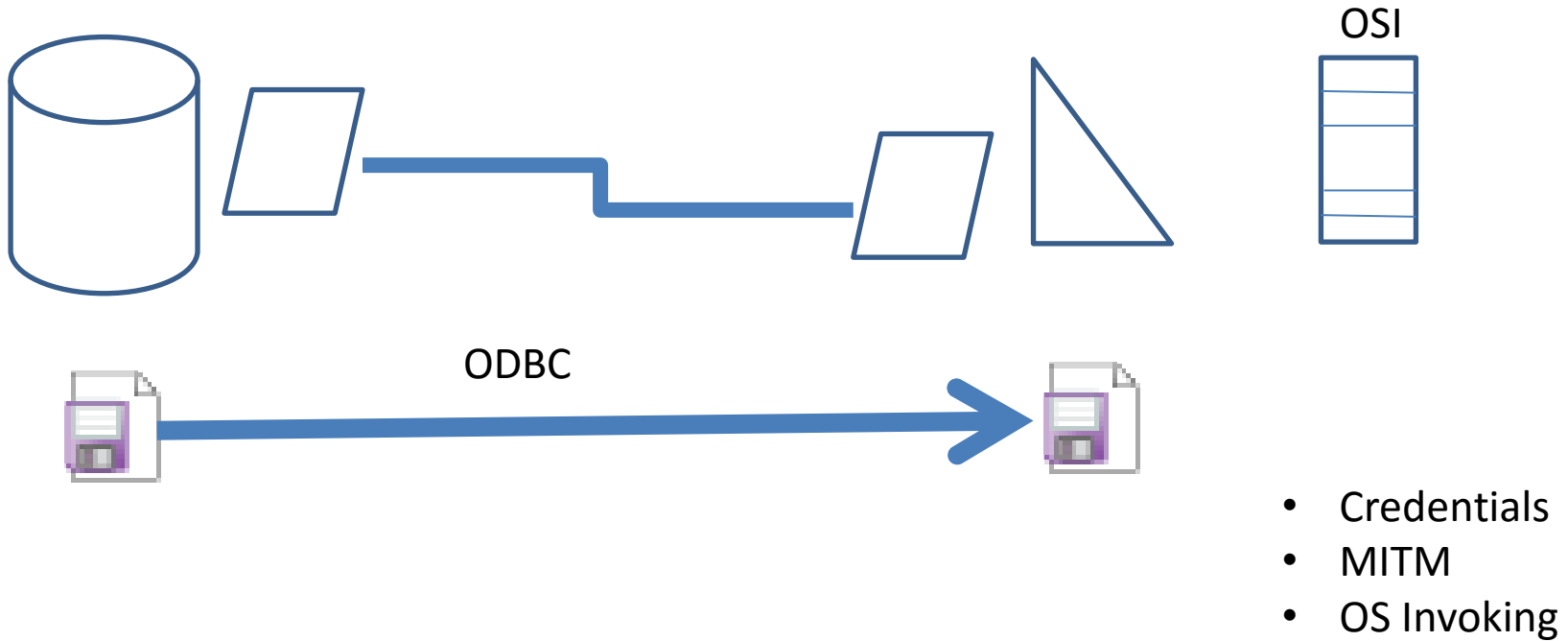
You are searching in the list of datasets. [Show results in entire Data.gov site.](#)

You can also access this registry using the API (see [API Docs](#)).

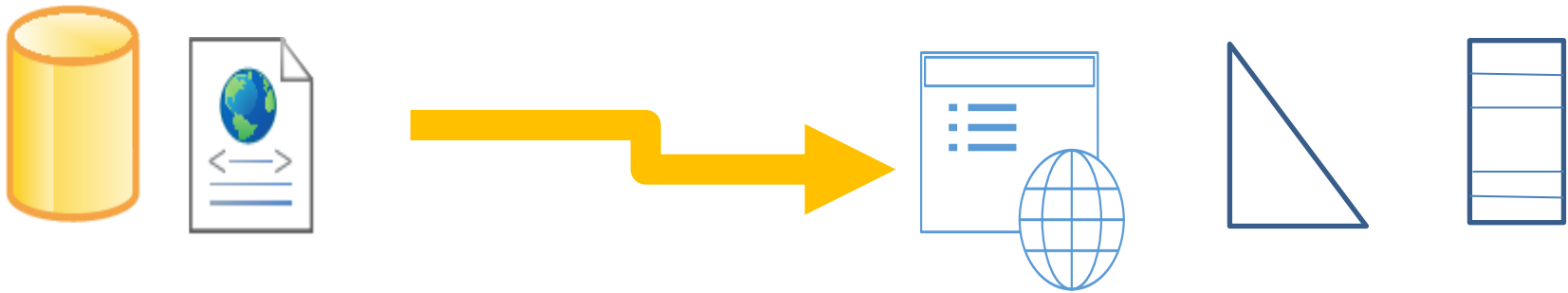
Didn't find what you're looking for? [Suggest a dataset here.](#)

City

Pre HTTP (1995)



HTTP/s (Web1)

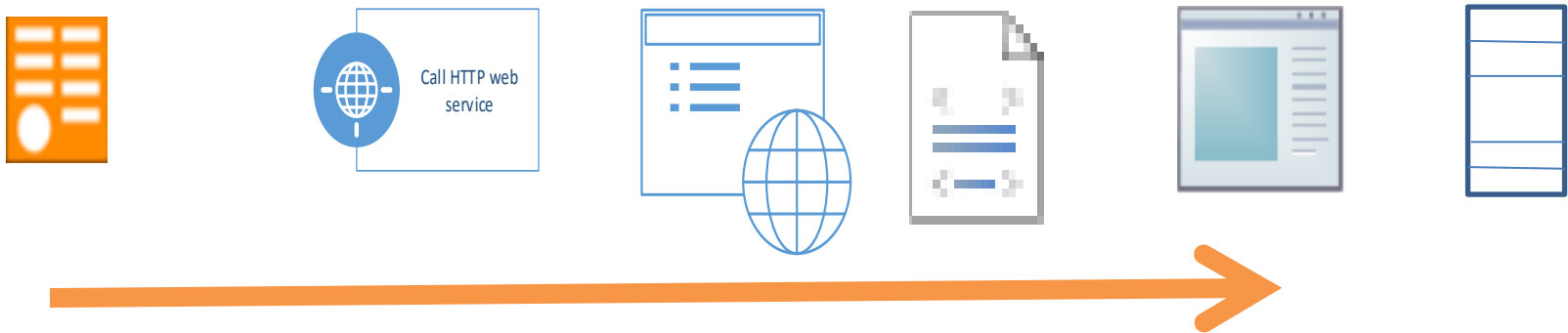


FTP / Compression / Ad hoc JS / Home Grown



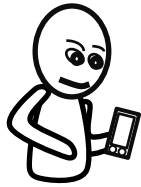
- DOS
- Injection
- MITM

Example OData Web Application



Level 1 Minimal Conformance
Level 2 Intermediate Conformance
Level 3 Advanced Conformance

- XSS
- Injection
 - JS
 - SQL
- DOS
- HTTP Parameter Overload
- MITM



Demo Discussion

 OData web service

bing  7°   50    

y00okq76ck.database.windows.net > [MyC5] > Query(Untitled1.sql) * ion@y00okq76ck Log off Help

MyC5

My Work (2) 

Query(Untitled1.sql)

[dbo].[C5EnterpriseGoals]

New Query Open Save As Run Actual Plan Estimate... Stop

```
select * from C5EnterpriseGoals
```

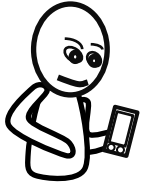
Messages Results

1 17 Row(s)

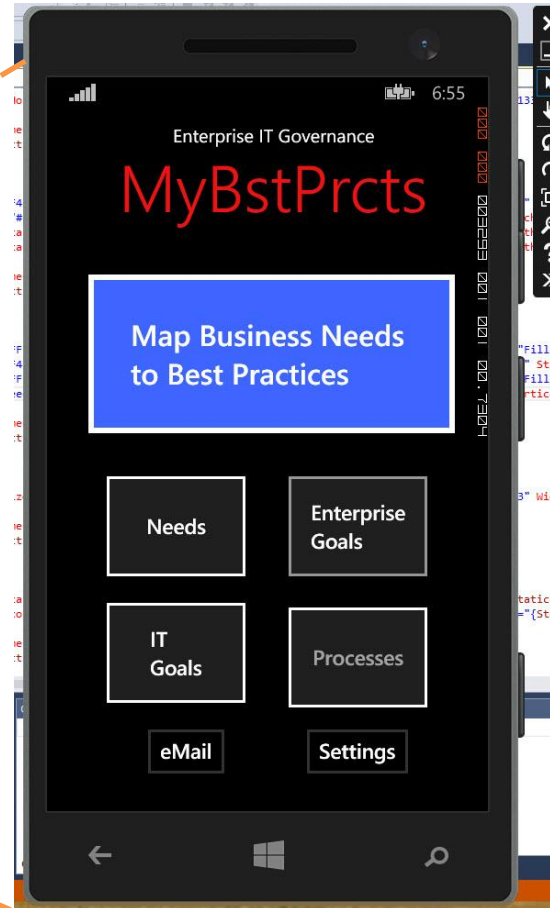
ID	EGoalID	tblKey	Description
1	E1	1	Stakeholder value of...
2	E2	2	Portfolio of competitive...
3	E3	3	Managed business risk...
4	E4	4	Compliance with external...
5	E5	5	Financial transparency
6	E6	6	Customer oriented service...
7	E7	7	Business service continuity...
8	E8	8	Agile responses to a...
9	E9	9	Information based strategic...
10	E10	10	Optimisation of service...
11	E11	11	Optimisation of business...
12	E12	12	Optimisation of business...
13	E13	13	Manged busines change...
14	E14	14	Operational and staff...
15	E15	15	Compliance with internal...
16	E16	16	Skilled and motivated people
17	E17	17	Product and business...

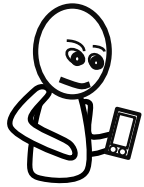
Overview Administration Design

Demo Discussion



OData web service





Demo Discussion

bing database.windows.net > [MyCS] > Query(Untitled1.sql) * ion@y00okq76ck Log off Help

MyCS

My Work (2) ☯

Query(Untitled1.sql)

[dbo].[CSEnterpriseGoals]

```
select * from CSEnterpriseGoals
```

Messages Results

1 17 Row(s)

ID	EGoalID	tblKey	Description
1	E1	1	Stakeholder value of...
2	E2	2	Portfolio of competitive...
3	E3	3	Managed business risk...
4	E4	4	Compliance with external...
5	E5	5	Financial transparency
6	E6	6	Customer oriented service...
7	E7	7	Business service continuity...
8	E8	8	Agile responses to a...
9	E9	9	Information based strategic...
10	E10	10	Optimisation of service...
11	E11	11	Optimisation of business...
12	E12	12	Optimisation of business...
13	E13	13	Manged busines change...
14	E14	14	Operational and staff...
15	E15	15	Compliance with internal...
16	E16	16	Skilled and motivated people
17	E17	17	Product and business...

Overview Administration Design

Enterprise IT Governance

8:36

MyBstPrcts

Map Business Needs to Best Practices

Needs Enterprise Goals

IT Goals Processes

eMail Settings

← Windows Search



Demo Discussion

<https://data.environment.alberta.ca/Services/Land/LandRec.svc/>

[https://data.environment.alberta.ca/Services/Land/LandRec.svc/\\$metadata/](https://data.environment.alberta.ca/Services/Land/LandRec.svc/$metadata/)

[https://data.environment.alberta.ca/Services/Land/LandRec.svc/Projects?\\$select=*](https://data.environment.alberta.ca/Services/Land/LandRec.svc/Projects?$select=*)



Demo Discussion

root payload recipe



Get Water Licenses Example

[https://environmentuat.internal.gov.ab.ca/Services/WaterUseReportingDataQuery/WURDQService.svc/GetSummaries?stakeholderName=''&apvID=''&fileNumber='27529'&priority=''&allocationTypeKey=0&quarterSection=''§ion=0&township=0&range=0&meridan=0®ionKey=0&districkKey=0&municipalityKey=0&riverBasinCode=''&subBasinKey=0&waterBodyKey=0&reportingIntervalKey=0&industryActivityKey=0&specificPurposeCode=''&licenseAmountFrom=-1M&licenseAmountTo=-1M&reportDateFrom=datetime'2000-01-01T00:00:00'&reportDateTo=datetime'2013-02-27T00:00:00'&\\$inlinecount=allpages](https://environmentuat.internal.gov.ab.ca/Services/WaterUseReportingDataQuery/WURDQService.svc/GetSummaries?stakeholderName=''&apvID=''&fileNumber='27529'&priority=''&allocationTypeKey=0&quarterSection=''§ion=0&township=0&range=0&meridan=0®ionKey=0&districkKey=0&municipalityKey=0&riverBasinCode=''&subBasinKey=0&waterBodyKey=0&reportingIntervalKey=0&industryActivityKey=0&specificPurposeCode=''&licenseAmountFrom=-1M&licenseAmountTo=-1M&reportDateFrom=datetime'2000-01-01T00:00:00'&reportDateTo=datetime'2013-02-27T00:00:00'&$inlinecount=allpages)



Demo Discussion

root



Get Water Licenses Example

You are not authorized to view this page

The Web server you are attempting to reach has a list of IP addresses that are not allowed to access the Web site, and the IP address of your browsing computer is on this list.

Please try the following:

- Contact the Web site administrator if you believe you should be able to view this directory or page.

HTTP Error 403.6 - Forbidden: IP address of the client has been rejected.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to [Microsoft Product Support Services](#) and perform a title search for the words **HTTP** and **403**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **About Security**, **Limiting Access by IP Address**, **IP Address Access Restrictions**, and **About Custom Error Messages**.

OData Dependencies

The screenshot shows a web browser window with the URL <http://services.odata.org/validation/>. The page header includes "pha Release - v0.1" and navigation links: "Home | [About](#) | [Roadmap](#) | [Feedback](#)". The main heading is "Open Data Protocol" with the subtitle "Service Validation Tool". Below this, there are two tabs: "By Uri" (selected) and "By Direct Input". A text input field contains the URL "https://data.environment.alberta.ca/Services/Land/LandRec.svc/" and a "Validate" button. Under the input field, there are radio buttons for "AtomPub/XML", "JSON-Min", and "JSON-Full", and a checkbox for "Crawling". Below these are three radio buttons for "OData v1.0 and v2.0 service endpoint", "OData v3.0 service endpoint", and "OData v4.0 service endpoint". A yellow banner at the bottom of the form area says "Validation complete." Below the form, a link says "You can see a list of all rules [here](#)." A section titled "Results (13 of 13 rules executed. 3 errors, 2 warnings.)" contains a list of validation results with green checkmarks and yellow warning icons. The results are: "The root URL of a data service that implements the AtomPub protocol SHOULD identify the service document. [Specification] [Section: 2.2.6.2.7]", "A data service SHOULD represent all available collections in a single <app:workspace> element. [Specification] [Section: 2.2.6.2.7]", "AtomPub Service Documents MUST be identified with the 'application/xml' media type. [Specification] [Section: 2.2.3.7.1]", and "A data service SHOULD expose a conceptual schema definition language (CSDL) based metadata endpoint that describes the structure and organization of all the resources exposed as HTTP endpoints. [Specification] [Section: 2.2.3.7.2]".

pha Release - v0.1

Home | [About](#) | [Roadmap](#) | [Feedback](#)

Open Data Protocol

Service Validation Tool

By Uri By Direct Input

<https://data.environment.alberta.ca/Services/Land/LandRec.svc/> Validate

☒ AtomPub/XML ☐ JSON-Min ☐ JSON-Full

☐ Crawling

☐ OData v1.0 and v2.0 service endpoint

☐ OData v3.0 service endpoint

☒ OData v4.0 service endpoint

Validation complete.

You can see a list of all rules [here](#).

Results (13 of 13 rules executed. 3 errors, 2 warnings.)

- ✓ The root URL of a data service that implements the AtomPub protocol SHOULD identify the service document. [Specification] [Section: 2.2.6.2.7]
- ✓ A data service SHOULD represent all available collections in a single <app:workspace> element. [Specification] [Section: 2.2.6.2.7]
- ✓ AtomPub Service Documents MUST be identified with the 'application/xml' media type. [Specification] [Section: 2.2.3.7.1]
- ⚠ A data service SHOULD expose a conceptual schema definition language (CSDL) based metadata endpoint that describes the structure and organization of all the resources exposed as HTTP endpoints. [Specification] [Section: 2.2.3.7.2]

- A lot of other standards
- Wide use and acceptance

OData Dependencies

```
▼<service xmlns:atom="http://www.w3.org/2005/Atom" xmlns:app="http://www.w3.org/2007/app" |
```

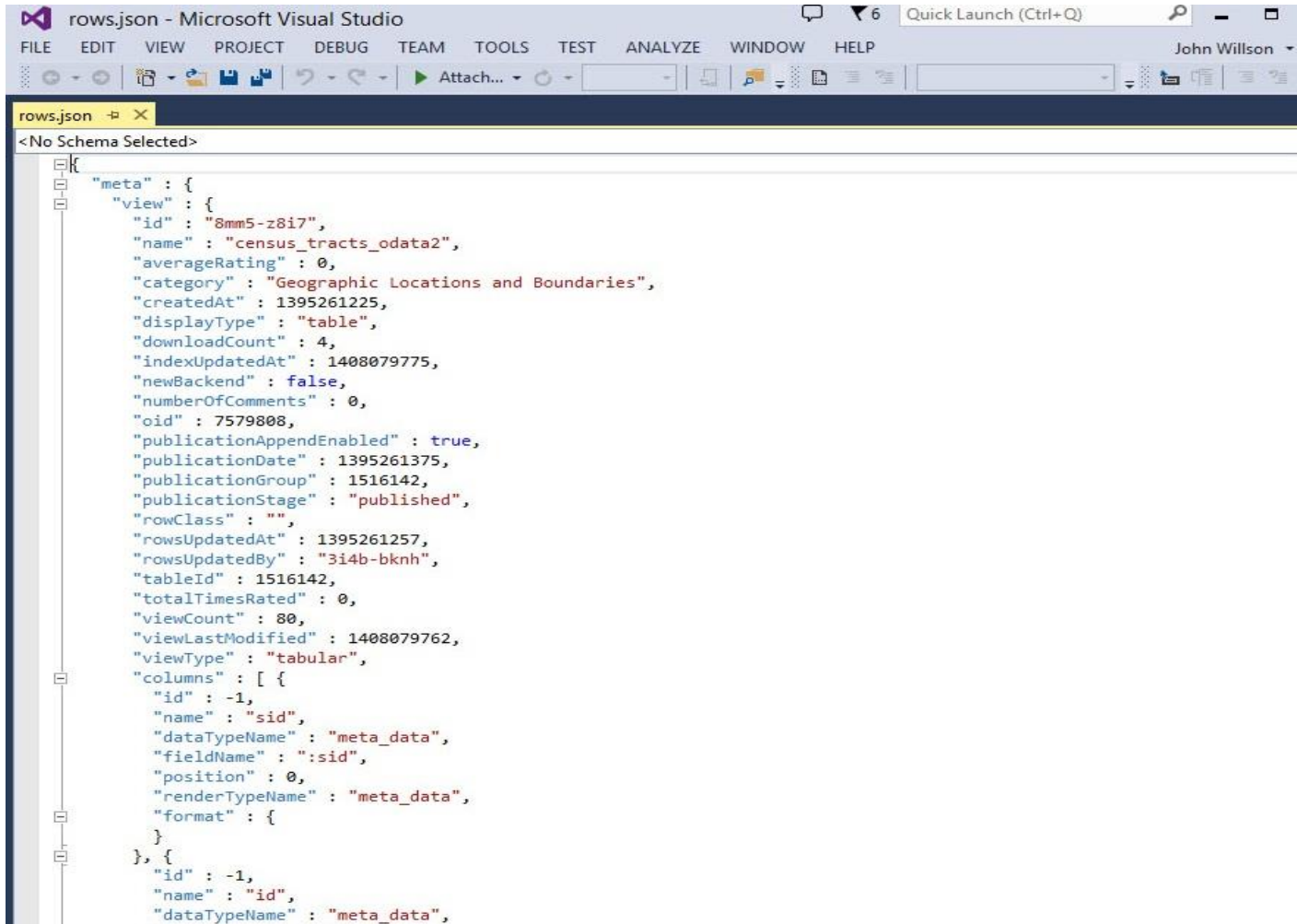
```
xmlns="http://www.w3.org/2007/app" xml:base="http://almaexpensereporting.alberta.ca/ExpenseReportService.svc/">
```

```
▼<workspace>  
  <atom:title>Default</atom:title>  
  ▼<collection href="ExpenseCategories">  
    <atom:title>ExpenseCategories</atom:title>  
  </collection>  
  ▼<collection href="ExpenseTypes">  
    <atom:title>ExpenseTypes</atom:title>  
  </collection>  
  ▼<collection href="Expenses">  
    <atom:title>Expenses</atom:title>  
  </collection>  
</workspace>  
</service>
```

OData Dependencies

```
C:\Users\DSSLtd\AppData\Local\Microsoft\Windows\INetCache\IE\2BWDWZVU\ro
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
html5_validator_tool.txt example.js nodevars.bat npm.cmd rows.rdf
1 <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:rdfs="http://www
2 <rdf:Description rdf:about="http://data.sfgov.org/resource/_8mm5-z8i7/1">
3   <socrata:rowID>1</socrata:rowID>
4   <rdfs:member rdf:resource="http://data.sfgov.org/resource/_8mm5-z8i7"/>
5   <ds:polygon_number>1</ds:polygon_number>
6   <ds:point_order>0</ds:point_order>
7   <ds:longitude>-122.44092</ds:longitude>
8   <ds:latitude>37.77364</ds:latitude>
9   <ds:tractce10>016500</ds:tractce10>
10  <ds:aland10>370459</ds:aland10>
11  <ds:geom><geo:SpatialThing>
12    <geo:lat>37.7736350001552</geo:lat>
13    <geo:long>-122.44092200025</geo:long></geo:SpatialThing></ds:geom></rdf:Descrip
14 <rdf:Description rdf:about="http://data.sfgov.org/resource/_8mm5-z8i7/2">
15   <socrata:rowID>2</socrata:rowID>
16   <rdfs:member rdf:resource="http://data.sfgov.org/resource/_8mm5-z8i7"/>
17   <ds:polygon_number>1</ds:polygon_number>
18   <ds:point_order>1</ds:point_order>
19   <ds:longitude>-122.44257</ds:longitude>
20   <ds:latitude>37.77342</ds:latitude>
21   <ds:tractce10>016500</ds:tractce10>
22   <ds:aland10>370459</ds:aland10>
23   <ds:geom><geo:SpatialThing>
24     <geo:lat>37.7734240003174</geo:lat>
25     <geo:long>-122.442565000474</geo:long></geo:SpatialThing></ds:geom></rdf:Descri
26 <rdf:Description rdf:about="http://data.sfgov.org/resource/_8mm5-z8i7/3">
```

OData Dependencies

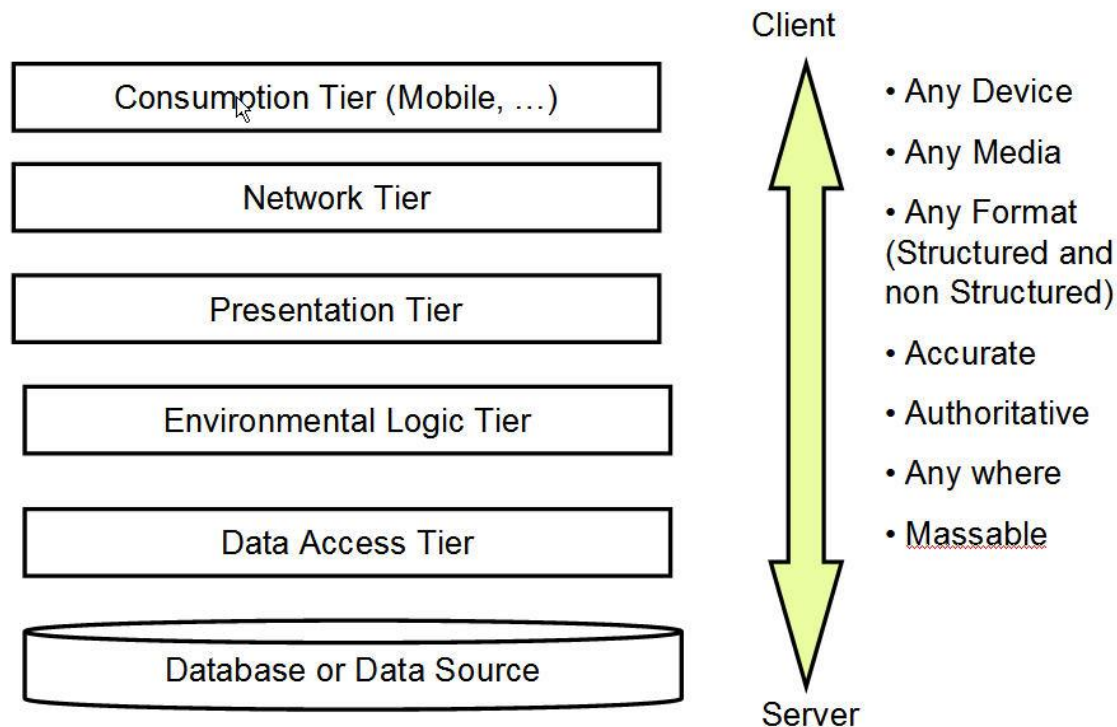


```
rows.json - Microsoft Visual Studio
FILE EDIT VIEW PROJECT DEBUG TEAM TOOLS TEST ANALYZE WINDOW HELP John Willson
rows.json <No Schema Selected>
{
  "meta": {
    "view": {
      "id": "8mm5-z8i7",
      "name": "census_tracts_odata2",
      "averageRating": 0,
      "category": "Geographic Locations and Boundaries",
      "createdAt": 1395261225,
      "displayType": "table",
      "downloadCount": 4,
      "indexUpdatedAt": 1408079775,
      "newBackend": false,
      "numberOfComments": 0,
      "oid": 7579808,
      "publicationAppendEnabled": true,
      "publicationDate": 1395261375,
      "publicationGroup": 1516142,
      "publicationStage": "published",
      "rowClass": "",
      "rowsUpdatedAt": 1395261257,
      "rowsUpdatedBy": "3i4b-bknh",
      "tableId": 1516142,
      "totalTimesRated": 0,
      "viewCount": 80,
      "viewLastModified": 1408079762,
      "viewType": "tabular",
      "columns": [ {
        "id": -1,
        "name": "sid",
        "dataTypeName": "meta_data",
        "fieldName": ":sid",
        "position": 0,
        "renderTypeName": "meta_data",
        "format": {
        }, {
        "id": -1,
        "name": "id",
        "dataTypeName": "meta_data",

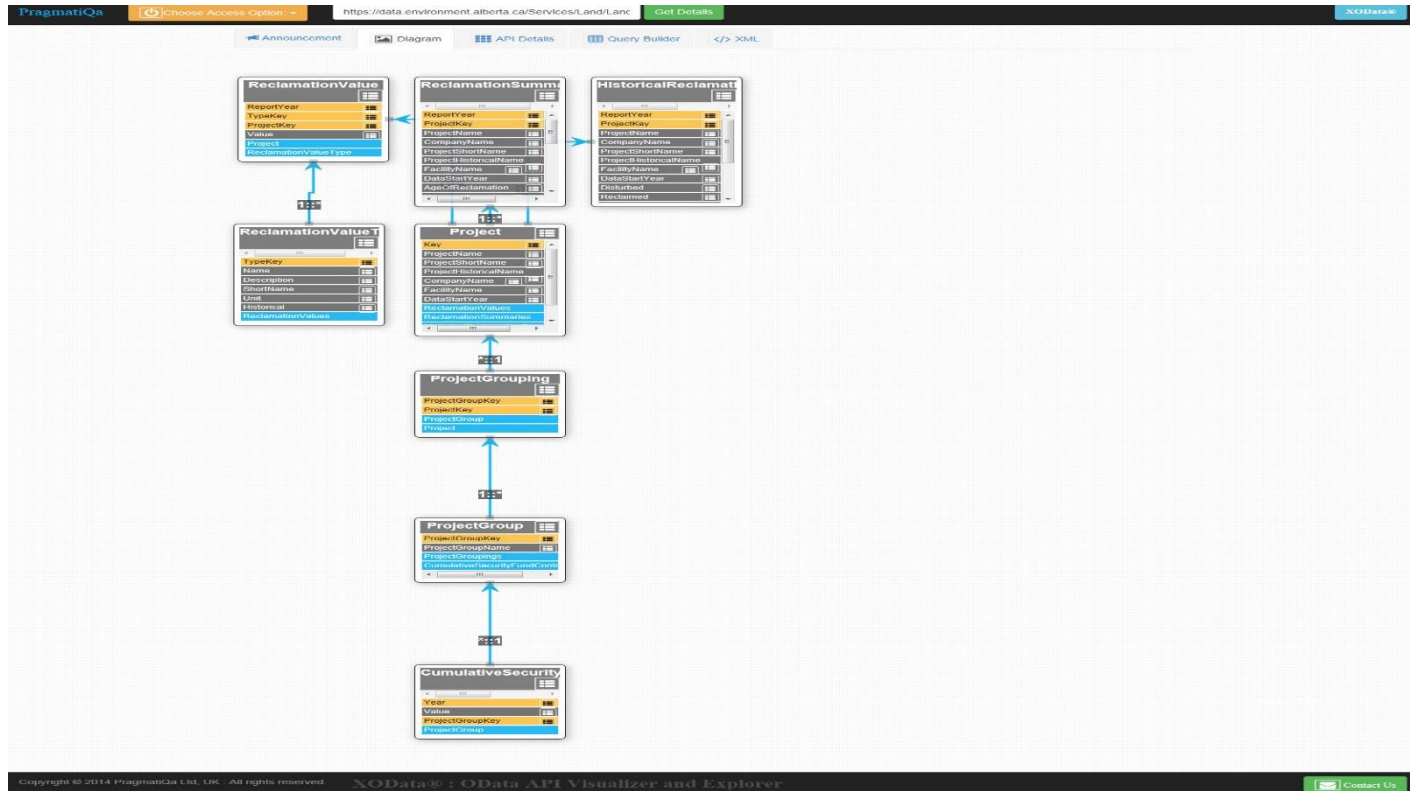
```

Example Business Solution Stack

Odata Interaction Stack

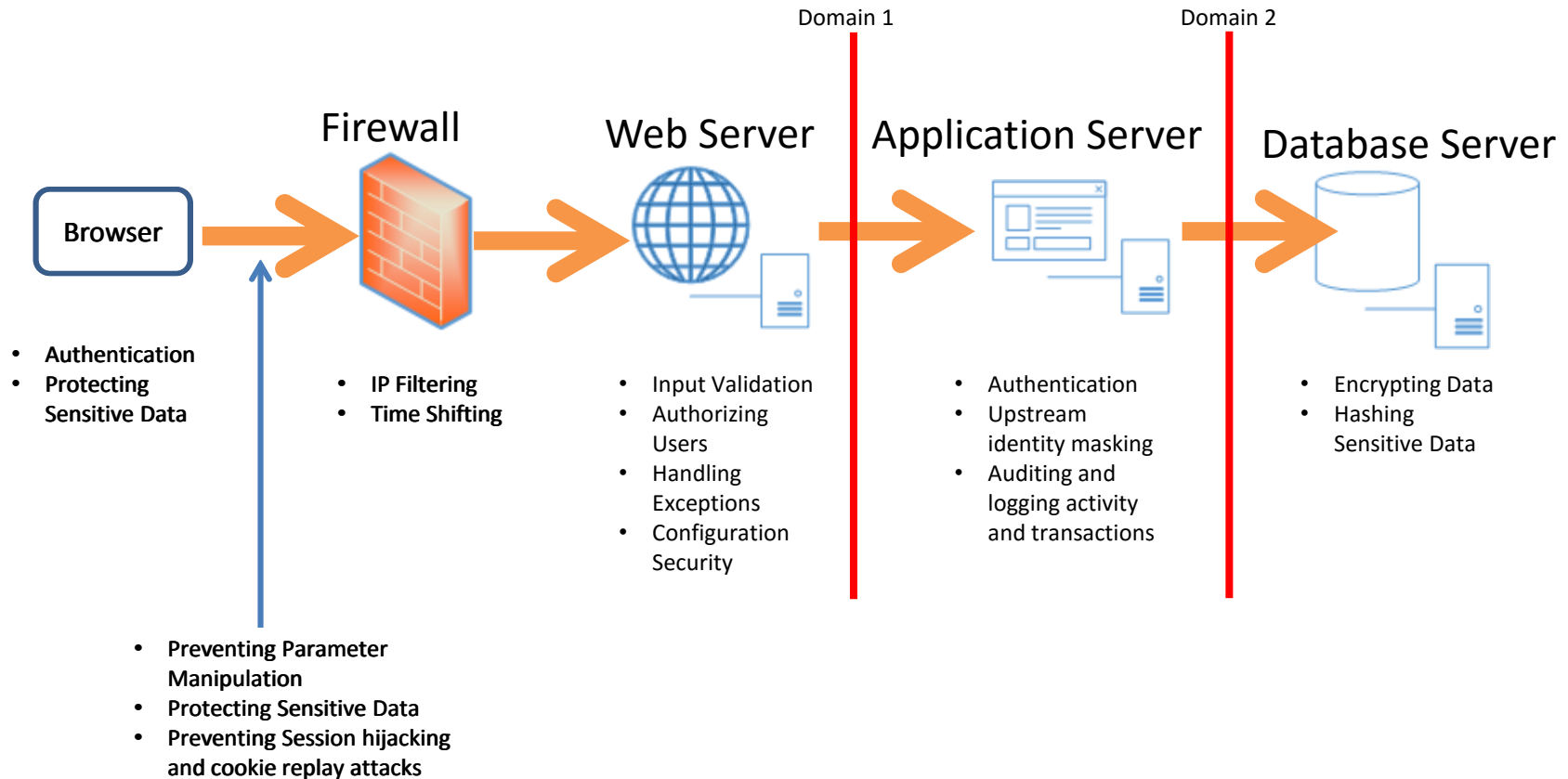


OData.org Tool xodata



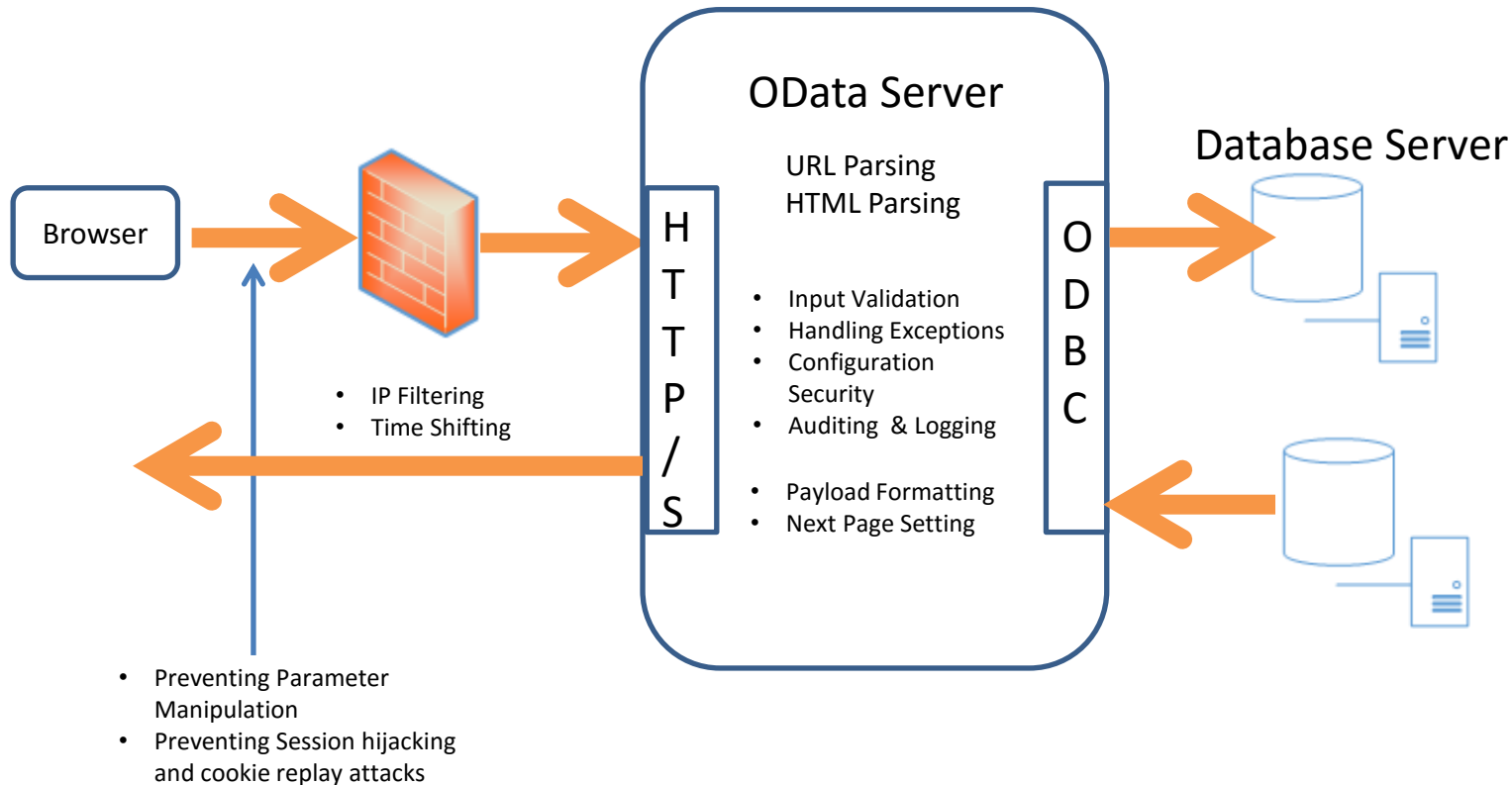
[http://pragmatika.com/xodata/?url=https://data.environment.alberta.ca/Services/Land/LandRec.svc/\\$metadata/](http://pragmatika.com/xodata/?url=https://data.environment.alberta.ca/Services/Land/LandRec.svc/$metadata/)

Conceptual Web APP Security Architecture*



* .NET Application Architecture Guide, 2nd Edition modified Figure 3

Example Conceptual OData Security Architecture



Common Attack Vectors



- XSS
- Injection
 - JS
 - SQL
- DOS
- HTTP Parameter Overload
- MITM

- Reputation lost
- Data Corruption / Masking
- Misleading

- Confidential Data Disclosure
- Outage (opportunity loss)
- Credential Theft

Common Attack Vectors



- XSS

Browser executed scripts to malicious alternative website masking as friendly website.

- Injection

- JS

Browser executed scripts likely on the consuming device controlling dynamically binding only during the current session – although may persist through cookie packing.

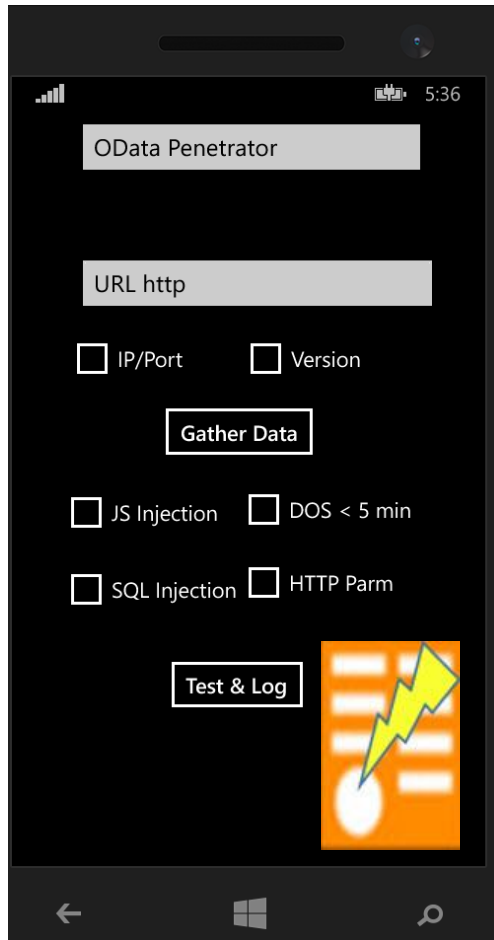
- SQL

Browser executed scripts likely imbedding on the producer data base and persisting through SQL manipulation.

- HTTP Parameter Overload

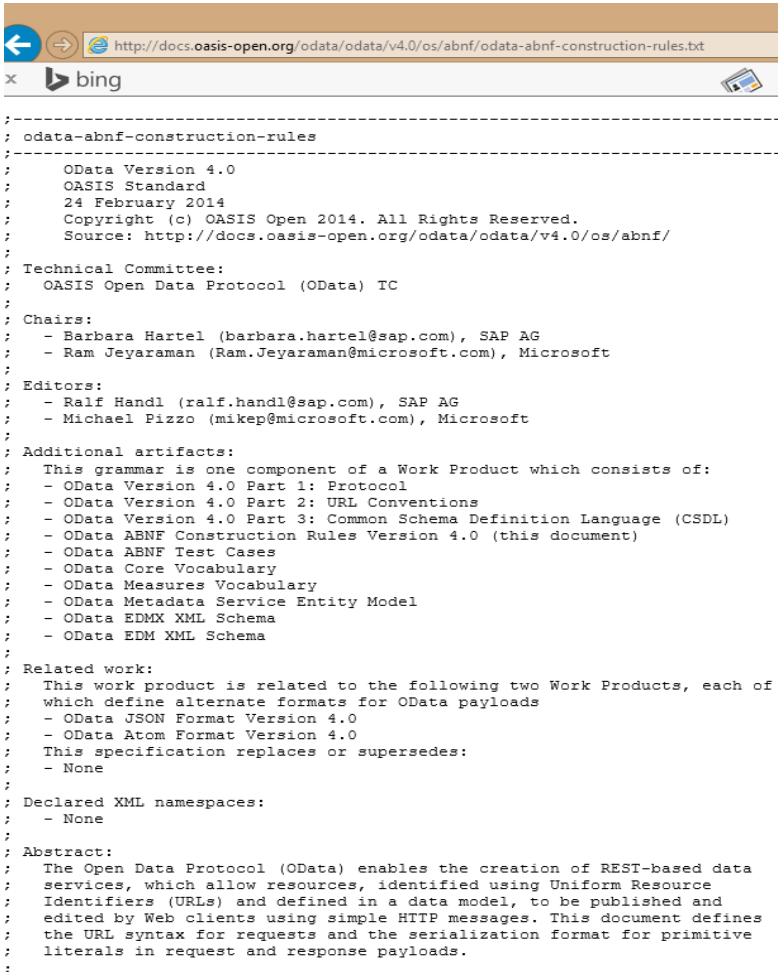
<http://www.codeproject.com/Articles/818408/Web-Application-Security-Vulnerabilities?msg=4909477#xx4909477xx>

Future Tool Speculation

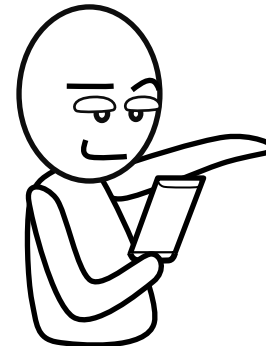


- Return if JSON or ATOM
- URL length check
- Non ABNF OD character use
- Unicode Use
- Special character use %20, 00, NUL, ' %27...
- HTTP error status codes use
- Degrade by multiple requests – processing queries \$TOP, \$OrderBy, \$Skip, \$Count, ...
- Multiple \$SELECT in one URL

ABNF



```
<TestCase Rule="odataRelativeUri"
Name="Query -
crossjoin"><Input>$crossjoin(Customers,Count
ries)?$expand=Customers($select=Name),Cou
ntries($select=Name)&$filter=Customers/Coun
tryCode eq Countries/CountryCode and
Countries/Name eq 'USA'</Input></TestCase>
```



OData Well Formed URLs

- ABNF



- WFF (well formed) OData URL;
- ABNF legitimate;
- No invalid characters or character combinations.

URL character parsing using Regex.



- Possible WFF OData URL;
- Code inserted within URL;
- Attempt to make unusual server or client supervisory event.

Black hat pattern matching.
Keyword counting.
Special character checking.



- Possible WFF OData URL;
- Code appended usually after a character(s) that attempt to make unusual server or client supervisory event;

Cascading operation checking.

- In firm extensions

\$Encrypt / \$Decrypt
\$Compress / \$Uncompress

Summary

- OData is a powerful, feature rich data exchange protocol with few security surprises.
- Standard security practices of COBIT and risk management apply to the business solutions that use OData as a component.
- OData version 4 is an emerging standard in a world of open web standards.
- Major attacks involving OData can be defended using routine security approaches for web services.
- There is a lot of security help for OData and a large body of resources on stream already.

Q & A





THANK YOU!

John Willson,

jwillson@dssltd.com

Please Remember To Fill Out Your Session
Evaluation Forms!

Acknowledgements

Name	Organization
Odata Technical Committee	OASIS
Ralf Handl	SAP
Stefan Drees	Independent
Mikael Pizzo	Microsoft
Ram Jeyaraman	Microsoft
Ed Bourne	Blackberry
Susan Malaika	IBM
Judy Heilman	Compass
Ashley Snelgrove	Silver Creek
Mike Hebert	iomer

Selected Tools

1	<u>http://docs.oasis-open.org/odata/odata/v4.0/os/abnf/</u>
2	<u>http://odatavalidator.codeplex.com/</u>
3	<u>http://metasapiens.com/sesame/data-browser/</u>
4	<u>http://download.cnet.com/OData-Browser/3000-2124_4-75231698.html</u>
5	<u>http://www.mcafee.com/us/downloads/free-tools/oyedata.aspx</u>
6	<u>http://www.telerik.com/download/fiddler</u>
7	<u>https://www.wireshark.org/download.html</u>

Selected URLs

1	<u>Home OData - The Protocol for REST APIs</u>
2	<u>DSS Ltd</u>
3	<u>Home MS Open Tech</u>
4	<u>OASIS Advancing open standards for the information society</u>
5	<u>The Open Group</u>
6	<u>World Wide Web Consortium (W3C)</u>
7	<u>OWASP</u>
8	<u>ISACA</u>
9	<u>MIS Training Institute</u>
10	<u>semantic odata Search Results Community and Business Groups</u>
11	<u>Welcome — Association for Computing Machinery</u>
12	<u>IEEE - The world's largest professional association for the advancement of technology</u>