

PLUMBING THE PLUMBER: A PLAYBOOK FOR INTEGRATION SERVERS



WHOAMI?



Ryan "Roll4Combat" Bonner

https://x.com/BadAt_Computers

<https://www.linkedin.com/in/roll4combat/>



Guðmundur "GummiKalli" Karl Karlsson

<https://x.com/gummikalli3>

<https://www.linkedin.com/in/gummikalli/>

WHAT ARE WEBMETHODS?

- Central Integration Hub
- Connects Anything Anywhere
- Data Transformation
- **Sketchy** undocumented plumbing of the corporate world

A unified integration approach for enhanced productivity

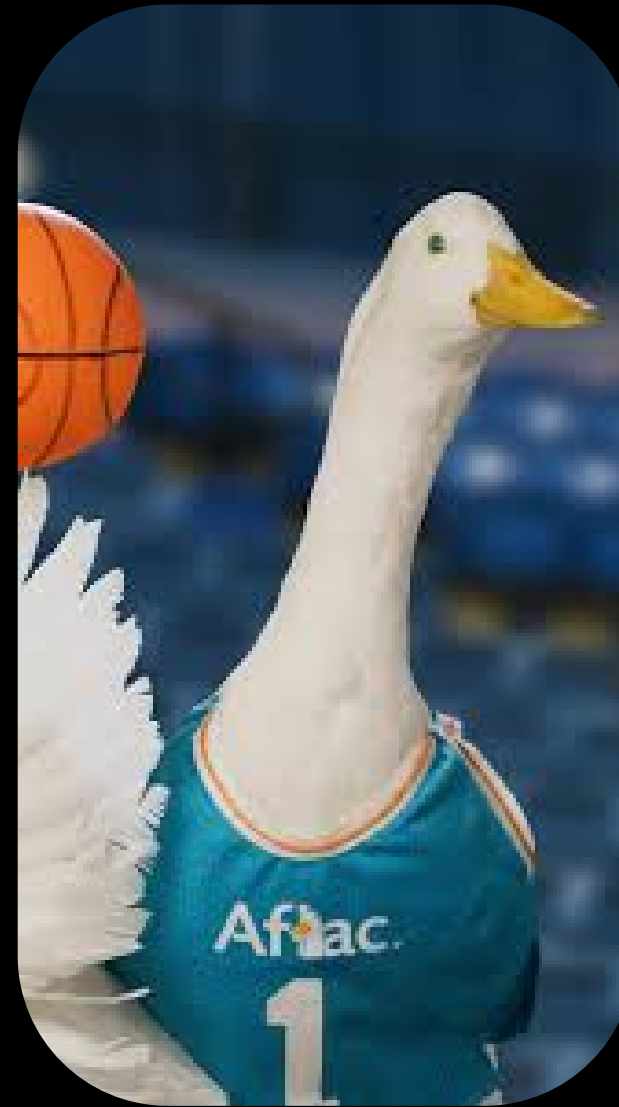
Enterprises today demand more than ever from their tech stacks amid a rush of rapid change, driven by business imperatives to derive value from AI; the increasing sprawl of APIs, Kafka and in-memory data grids; and ongoing waves of digital transformation. Yet most tech stacks strain under the compounding demands, unable to evolve into an AI-ready foundation for innovation.

IBM webMethods Hybrid Integration provides comprehensive development, deployment, management and monitoring of diverse integration patterns across on-premises and

SPOTTED IN THE WILD

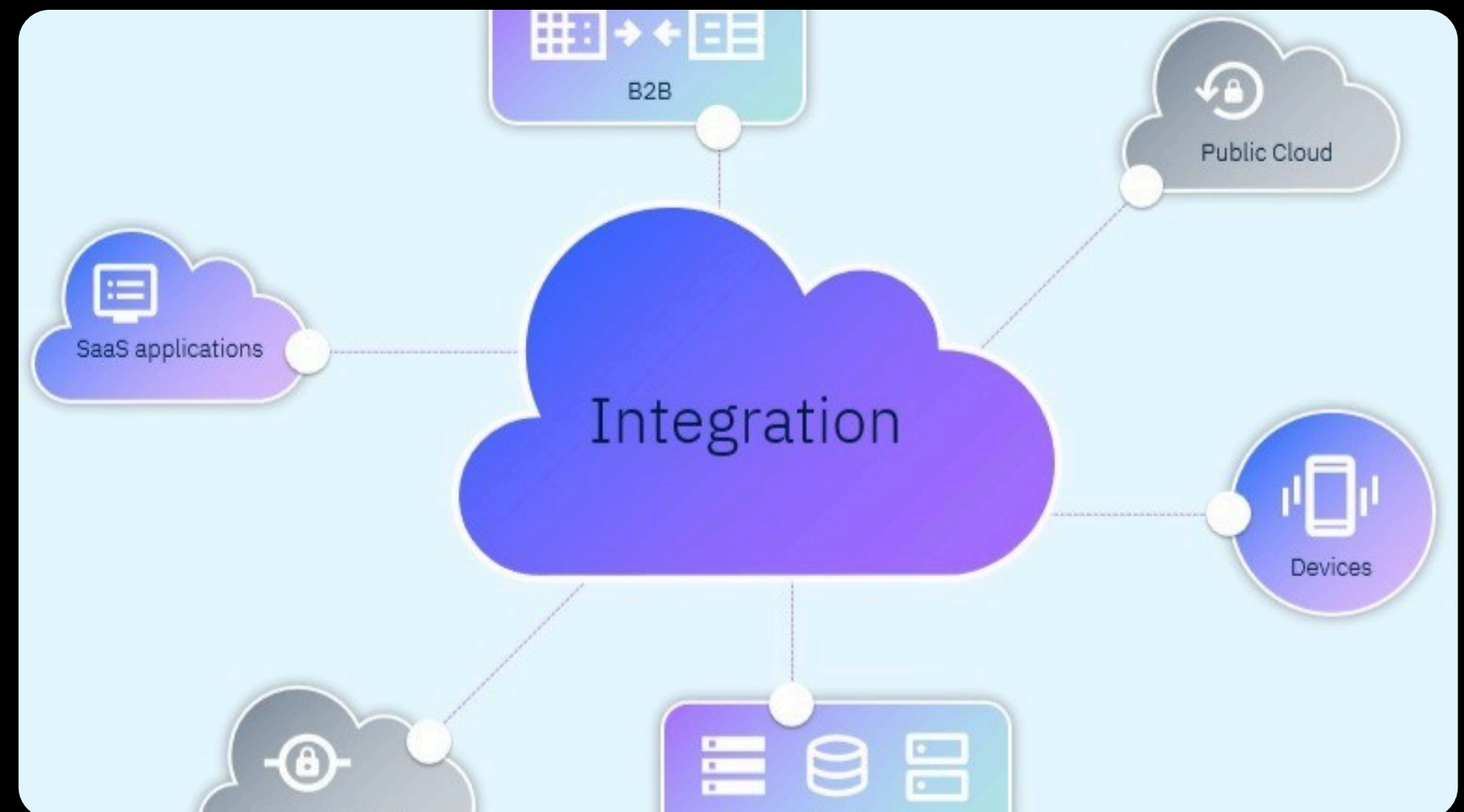


Google



WHY SHOULD WE CARE?

- Found in Banking, Telecom, **Healthcare**, Government, and Insurance.
- Processes financial transactions, integrates patient **health records** and manages global supply chains.
- A central point of failure for things we rely on daily



STARTING THE HUNT



SECURITY THROUGH OBSCURITY-AS-A-SERVICE

- Deep understanding required private, expensive training
- In 2015, it was around \$8,000 per person
- Security model = If we don't tell anyone how it works, no one can hack it



READING DOCUMENTATION



ibm-wm-transition

ibm-wm-transition has 156 repositories available.
Follow their code on GitHub.



Home | Software AG Product Documentation

 softwareag.com

SO BORING READING DOCUMENTATION



IBM webMethods Integration

With IBM webMethods Integration, turn your data and services into experiences everyone will love with application integration for everyone and...

 ibm.com / Sep 24, 2024

CASTING A WIDE NET

- Shodan
- FOFA
- CENSYS
- ZOOMEYE
- Google



SHODAN

- "WWW-Authenticate: Basic realm="Integration Server""
- http.html:"WmRoot"
- ssl.cert.subject.cn:"Integration Server"
- http.html:"Software AG"

TOTAL RESULTS

613

TOP COUNTRIES



United States	333
Germany	42
Netherlands	37
China	26
Korea, Republic of	23
More...	

TOP PORTS

 View Report

Product Spotlight: Fre

20.23.152.184 

Microsoft Corporation

 Netherlands, Amsterdam

cloud

35.209.11.174 

logistics.com

174.11.209.35.bc.googleusercontent.com

Google LLC

 United States, Council Bluffs



cloud

ZOOMEYE

- Wider Port Scanning - 3800
- Integration with Seebug vuln database
- Better coverage in Asian Markets

"Integration Server" && (iconhash="c5665614132b8bfc64f024d4bb0f6d3a")

"Integration Server" × && (iconhash = "c5665614132b8bfc64f024... × Not satisfie

About 975 results (Nearly year: 532 results) 0.148 seconds

Icon(1):  Select All

Result Report Maps


"Integration Server"

"Integration Server" × Not satisfied with the search, try [ZoomEyeGPT](#)

About 10,335 results (Nearly year: 2,718 results) 2.228 seconds

Icon(99):           More Sel

Result Report Maps

 [129.24.172.149:443](#)  

[129.24.172.149](#)  [Data update](#)

 [United States, Texas, Port A...](#)

Hostname: [oraweb02-int.unm.e...](#)

Organization: [University of New ...](#)

ASN: [AS3388](#)

Title: [The Business Page](#)

 2025-08-03 09:40

Header

Body

SSL


Ha


HTTP/1.1 200 OK
Date: Sun, 03 Aug 2025 02:00:00 GMT
Server: Apache
Last-Modified: Mon, 14 Oct 2024 17:19:5
ETag: "37c6-624730b51f991"
Accept-Ranges: bytes
Content-Length: 14278
Connection: close
Content-Type: text/html; charset=UTF-8

FOFA

- Rule-based fingerprinting engine
- Asset correlation
- `icon_hash="-234335289"`



icon_hash="-234335289"



Favicon(1):  999+ [Select all](#)


 all



1,489 results (839 unique IP) ,64 ms ,Keyword Search.
Nearly year results, click to view [all](#) results.

TOP FID	
yAiKat...	947
XT/yz...	230
0FC01...	94
DZWel...	48
tWe1O...	26

TOP COUNTRIES/REGIONS	
>> US 	426
CN 	160

 <https://142.34.52.23>  XT/y... 413

Integration Server Administrator
142.34.52.23
 Canada / British Columbia / Victoria
ASN: 15830
Organization: Equinix (EMEA) Acquisition E...
2025-08-04

Header
HTTP/1.1 200
Connection: cl
Content-Lengt
Cache-Control
Content-Type:
Pragma: no

CENSYS

- Quality data
- Query Assistance
- Certificate Issues
- Attack Surface Management

The screenshot displays the Censys search interface. At the top, a search bar contains the query "webmethods" with a green checkmark icon. Below the search bar, there are two tabs: "Search Results" (active) and "Report Builder".

On the left side, there is a sidebar with icons for user profile, search, and a stack of documents. The main content area is divided into two sections:

ASSET TYPES

Asset Type	Count
Hosts	920
Certificates	535
Web Properties	2.8K

SOFTWARE VENDORS

Vendor	Count
cloudflare	2.8K
f5	1.7K
amazon	593
microsoft	441
openresty	83

Below the vendors list is a "More" link with a dropdown arrow.

On the right side, the search results summary shows: "RESULTS: 4,262 • DURATION: 0.61s". Below this, a specific result is highlighted for IP "20.227.18.170: 443" with the label "WEB PROPERTY".


The details for this property are as follows:

HTML Title	404 Not Found
Browser Trust	Trusted ✓
Software	Nginx

Below the details, there is a section titled "MATCHED FIELDS" with a dashed line separator. It lists several fields and their values:

Field	Value
web.cert.names	2em-az-au.webmethods.io
web.cert.names	2em-az-eu.webmethods.io
web.cert.names	2em-az-us.webmethods.io
web.cert.names	al-az-us1.webmethods.io
web.cert.names	al-az-us2.webmethods.io
web.cert.parsed.subject.common_name	tal-az-au.webmethods.io

who uses webmethods?




InfoClutch

https://www.infoclutch.com › middleware-software › w...

webMethods Customers List

Companies that use webMethods ; Amway, www.amway.com, 15000, \$8 Billion ; Freddie Mac, www.freddiemac.com, 7284, \$23 Billion.




Enlyft

https://enlyft.com › ... › Business Process Management

Companies using WebMethods and its marketshare

4580 companies use WebMethods. WebMethods is most often used by companies with 50-200 employees & \$>1000M in revenue. Our usage data goes back 9 years and 9 ...




TheirStack.com

https://theirstack.com › technology › webmethods

List of companies using WebMethods in United States

Download a list of 622 companies that use WebMethods in United States which includes industry, size, location, funding, revenue...




ReadyContacts

https://www.readycontacts.com › target-account-profiling

Software AG WebMethods Customer List

Apr 11, 2025 — Ready's comprehensive database of Software AG WebMethods user list provides detailed contact information for businesses who use it.



Companies that use WebMethods
















Integrations Platform-as-a-Service (iPaaS)

2,760 companies

See allGet alerted

List of companies using WebMethods

Technology is any of WebMethodsAdd FilterAPIExport

Company	Country	Industry	Employees	Revenue	Technologies
 Aflac	 United States	Insurance	18K		 WebMethods
 Vodafone	 United Kingdom	Telecommunications	144K	\$	
 CGI	 Canada	It Services And It Consulting	89K	\$	
 VISEO	 France	It Services And It Consulting	2.8K	\$	
 Bristol Myers Squibb	 United States	Pharmaceutical Manufacturing	39K	\$46B	 WebMethods
 OpenText	 Canada	Software Development	23K	\$3.5B	 WebMethods

WebMethods's usage

Integrations Platform-as-a-Service (iPaaS)

The confidence of Aflac using WebMethods is high

The technology was mentioned in 88 job postings between Jun 07, 2022 and Sep 10, 2024.

CT LOG SCANNING - GUNGNIR

- Not every server is meant to be public.
- Even a hidden server needs a valid SSL/TLS certificate
- We can monitor these logs in real-time to see every new certificate as it's created for any domain in the world.

```
roll14combat ~ /BugBounty/Tools 22:43
→ gungnir | grep -iE webmethods
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
int-dr-aks-01-az-us.webmethods-stage.io
```

<https://github.com/g0ldencybersec/gungnir>

PUTTING IT ALL TOGETHER



INTEGRATION_SURFER

- Takes a list of IP's & Domains
- Integration Server Identification
- Tests default credentials
- FFUF each one with about 5100 API endpoints

```
> ./Integration_Surfer.sh integration_ips.txt finaltest.txt
Processing input file for domains and IPs...
Resolved 522 unique IP addresses

=====
INTEGRATION SURFER v1.0
=====

Choose your surfing operation:
1. Integration Server Detection (tests 9 endpoints)
2. Default Credential Testing (tests 6 credentials)
3. Fuzzing (runs ffuf over everything)
4. Run All Tests (detection + credentials + fuzzing)
5. Test Credentials and Fuzz (skip detection, assume good data)
6. Detection + Credentials only (no fuzzing)
7. Detection + Fuzzing only (no credentials)

Enter your choice (1-7): 6
Selected: Detection + Credentials only (no fuzzing)
Integration server monitor started (PID: 67900)

Total domains to surf: 522
```

```
* cat credentials_results.txt | grep -i success
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: Administrator:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: Administrator:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: Administrator:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: Administrator:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_SYSUSER:manage
SUCCESS - Credentials worked: WEBM_CLUSTERUSER:man
```

<https://github.com/Roll4Combat/IntegrationSurfer>

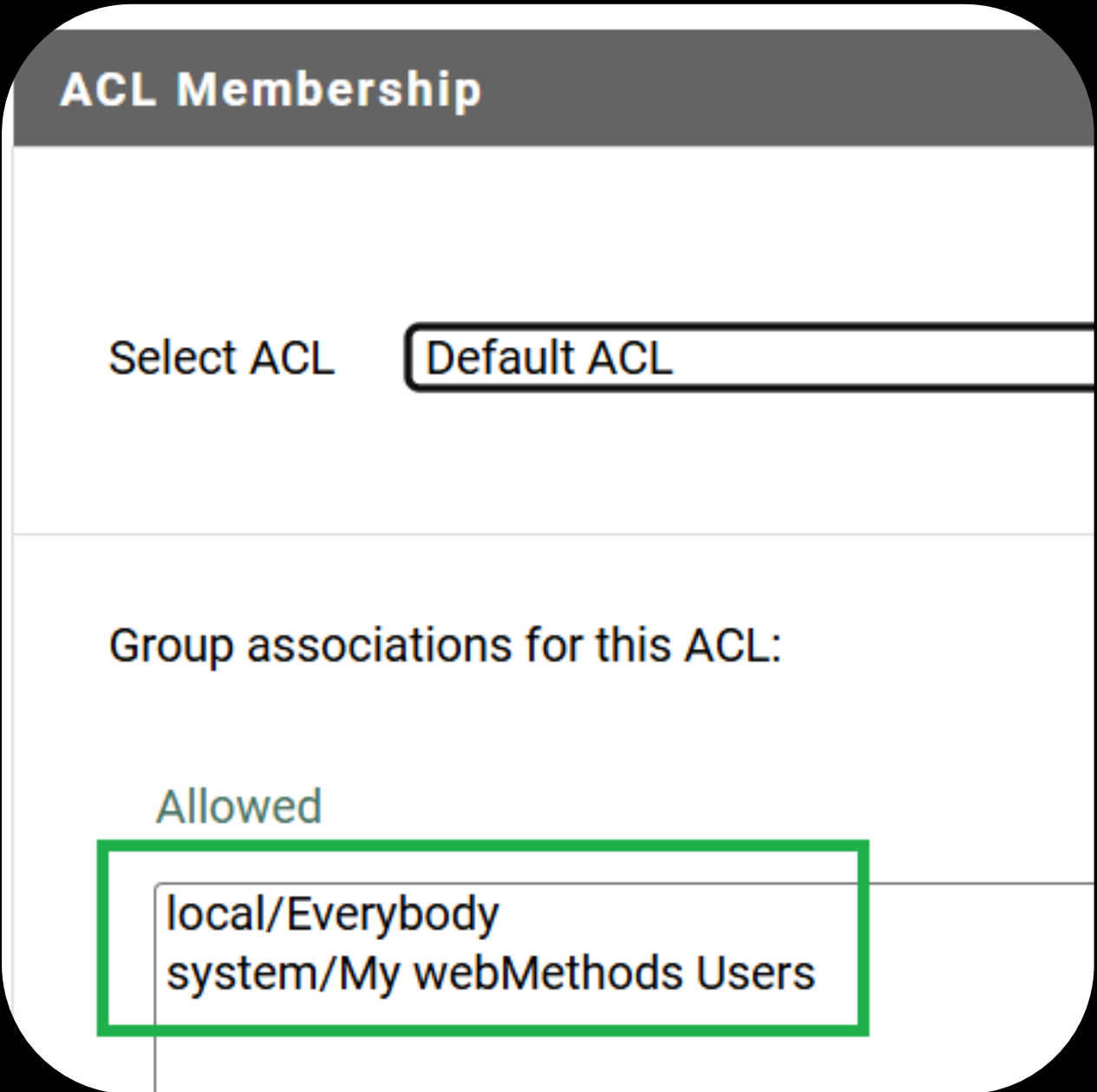
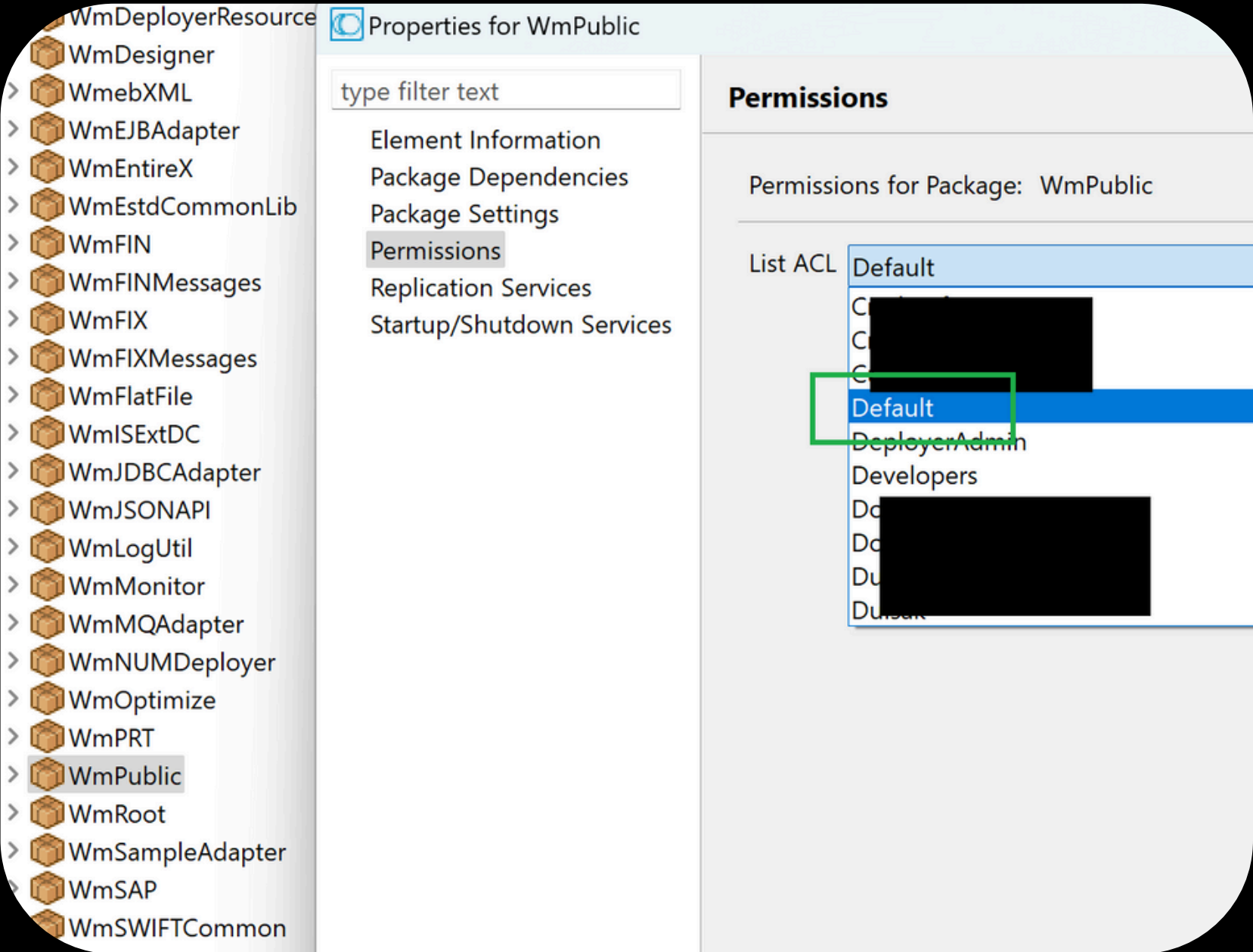
WAIT A MINUTE.....

- 200 = successfully ran
- 500 = We can run it with fixed formatting.....

```
pub.security.keystore:setKeyAndChain [Status: 500, Size: 160  
pub.security.outboundPasswords:listKeys [Status: 200, Size:  
pub.security.outboundPasswords:getPassword [Status: 500, Siz  
pub.security.outboundPasswords:removePassword [Status: 500,  
pub.security.outboundPasswords:setPassword [Status: 500, Siz  
pub.security.outboundPasswords:updatePassword [Status: 500,
```













DEVELOPER MISTAKES!




WMPUBLIC?

And hundreds more...

	pub.file:bytesToFile
	pub.file:checkFileExistence
	pub.file:copyFile
	pub.file:deleteFile
	pub.file:getFile
	pub.file:listFiles
	pub.file:moveFile
	pub.file:readerToFile
	pub.file:streamToFile
	pub.file:stringToFile

FINDING SERVICE NAMES

 Documentation


Search in IBM webMethods B2B Trading Networks

IBM webMethods B2B Trading Networks <

Change version

11.1.0 ▾

☒ Show full table of contents

 Filter on titles

Admin Folder

Archive Folder

Charting Folder

Delivery Folder

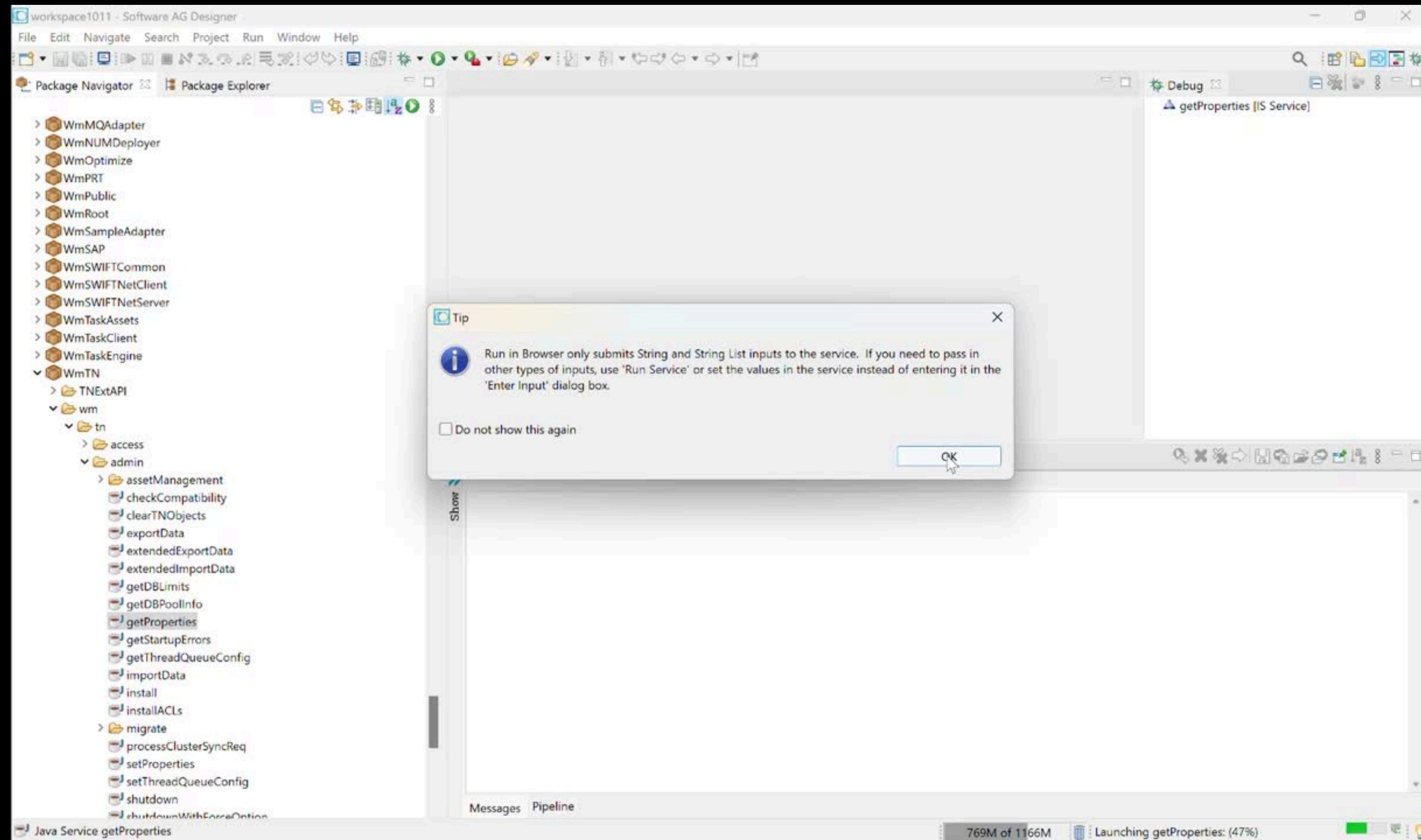
Dictionary Folder

Summary of Elements in this Folder

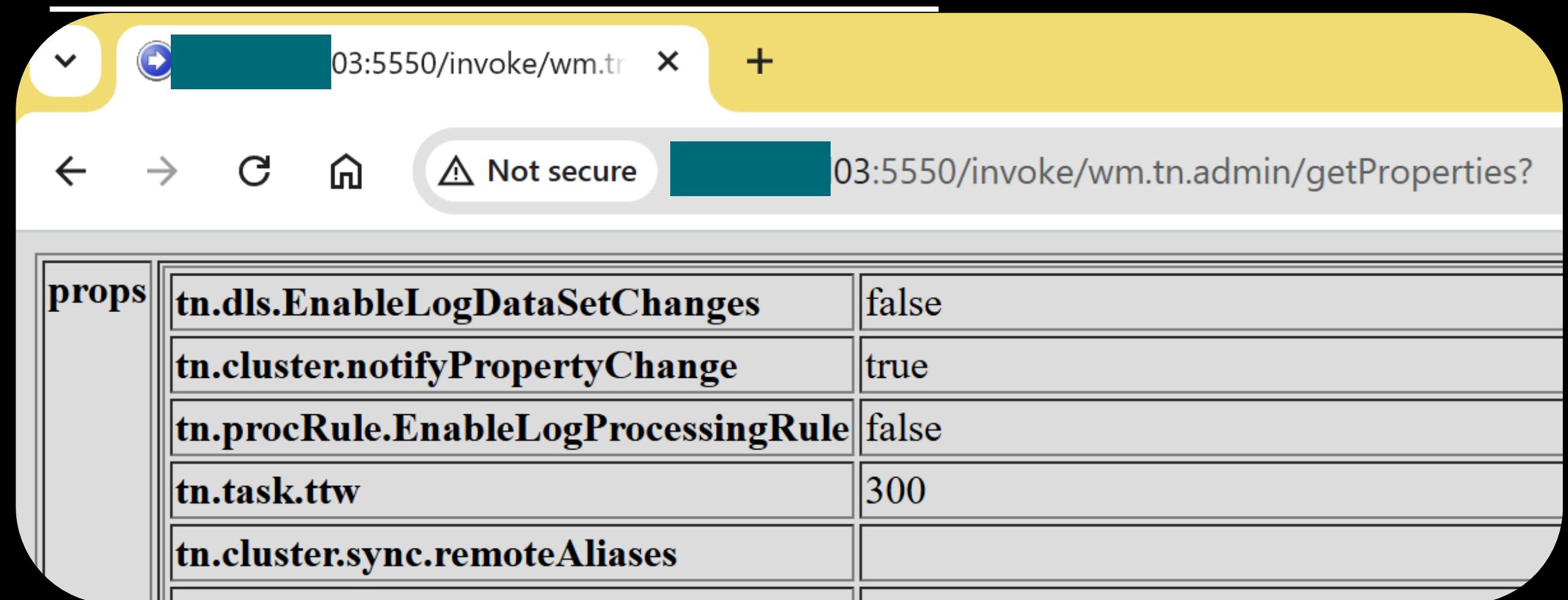
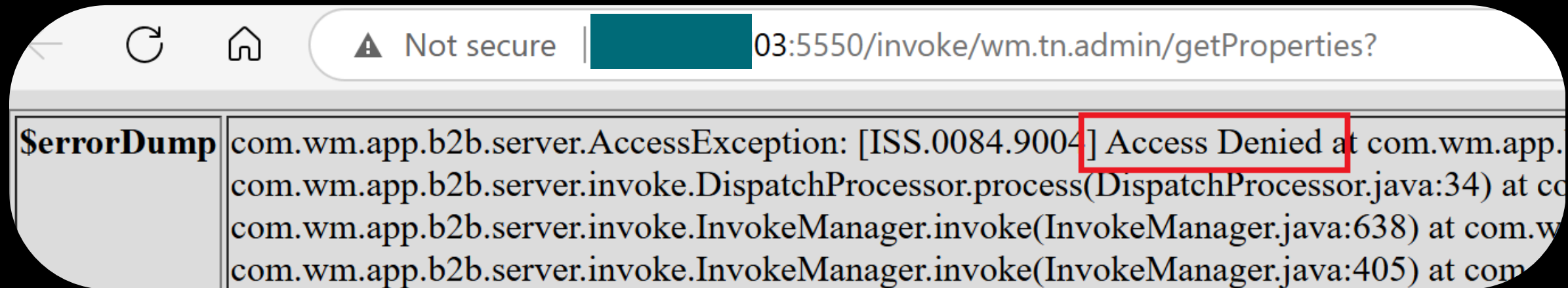
The elements that are available in this folder are listed in the following table:

Element	Description
wm.tn.admin:exportData	Exports data from the Trading Networks database.
wm.tn.admin:extendedExportData	Exports data from the Trading Networks database by either saving the data to an export file or by generating sources for solution deployment through IBM webMethods Deployer. Provides extensions for each asset type and an option to filter the asset type based on internal IDs.
wm.tn.admin:extendedImportData	Imports data from the supplied XML or binary file containing Trading Networks data by either saving the data from an export file or by generating sources for solution deployment through IBM webMethods Deployer. Provide

/INVOKE?FUCKED=TRUE

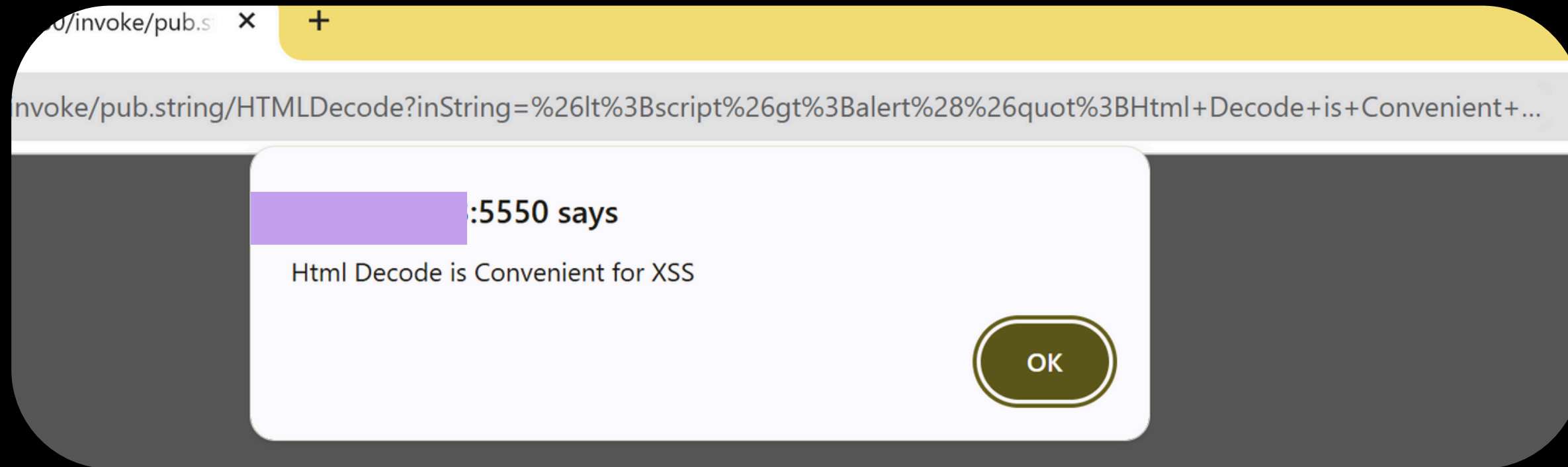


FUZZ ALL THE THINGS!



WM.SERVER.ADMIN:SHUTDOWN

FINDING EXPLOITS



Contact	
Delivery	
PartnerID	
Protocol	ftp
PrimaryAddr	MBoolean true
Host	
Port	
Location	docType/TypeName%_%value bizdoc/InternalID%.dat.asc
UserName	
Password	
CustomData	
DestinationID	
NativeProtocol	
CustomDataString	
B2BInterface	
B2BService	

PUB.UTILS:EXECUTEOSCOMMAND

FUZZ PROPRIETARY SERVICES

CompanyName.ProjectName.Pub:GetAllCustomersData

THE WINS, LOSSES, AND TAKEAWAYS

- Offered multiple jobs by some giant companies
- Turned in 80ish reports to bug bounty programs, VDP's, and direct email
- We only touched maybe 10 % of possibilities
- Assume we can use a similar methodology on others

THANK YOU



<https://defendiceland.is>



<https://securing.dev/>



@xssdoctor



@unltycyb3r



@DanielMiessler
<https://danielmiessler.com/>



@GOLDEN_infosec



@JHADDIX
ARCANUM-SEC.COM