Progress®

Are you Vulnerable?

Configuring PAS for OpenEdge

Anil Kotha

Software Engineer, Principal

Nov 14, 2023

In 2022, it took an average of 277 days—about 9 months—to identify and contain a breach.

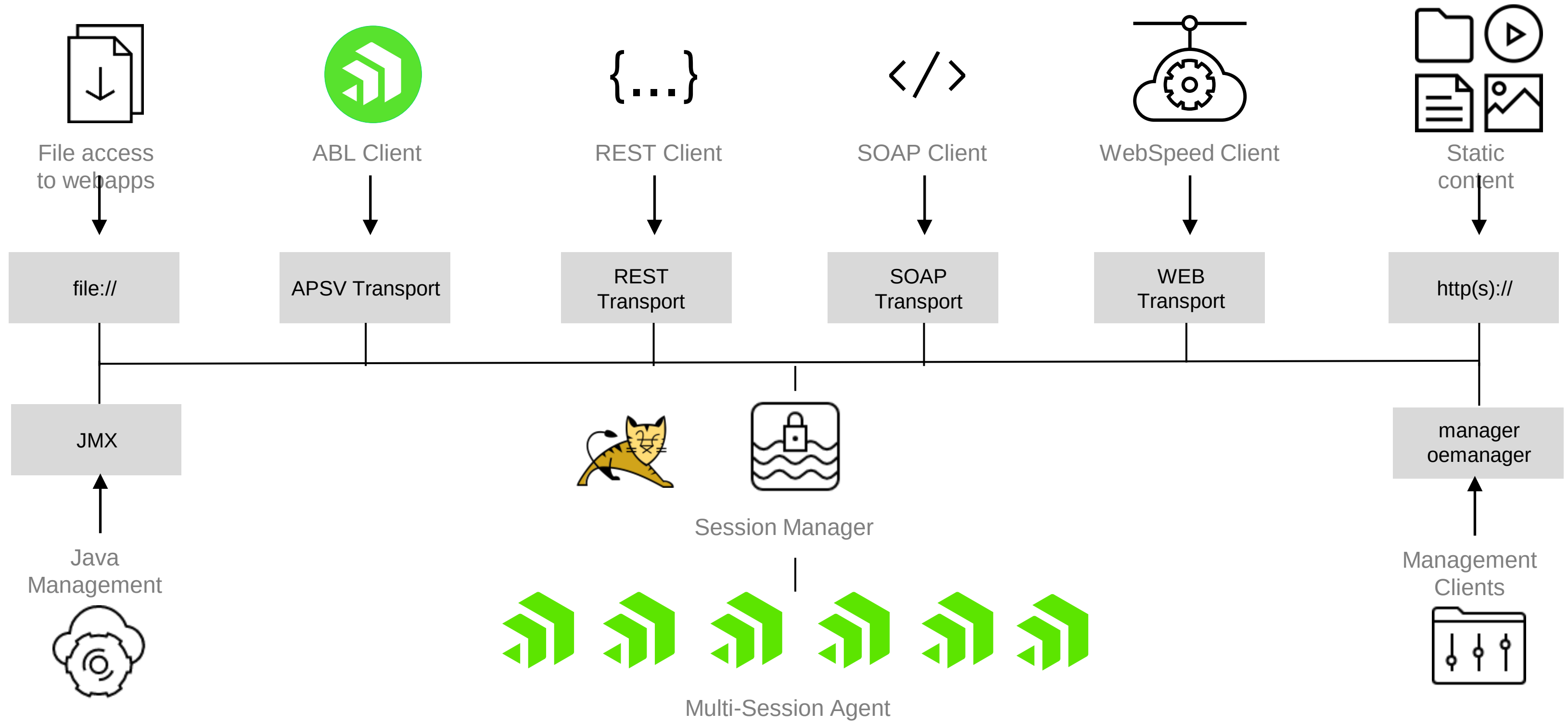
US$ 4.45M

Global Average Total Cost per Data Breach

OpenEdge Enhanced Architecture

Progress Application Server (PAS) for OpenEdge

Scalable, Secure and Standards Based



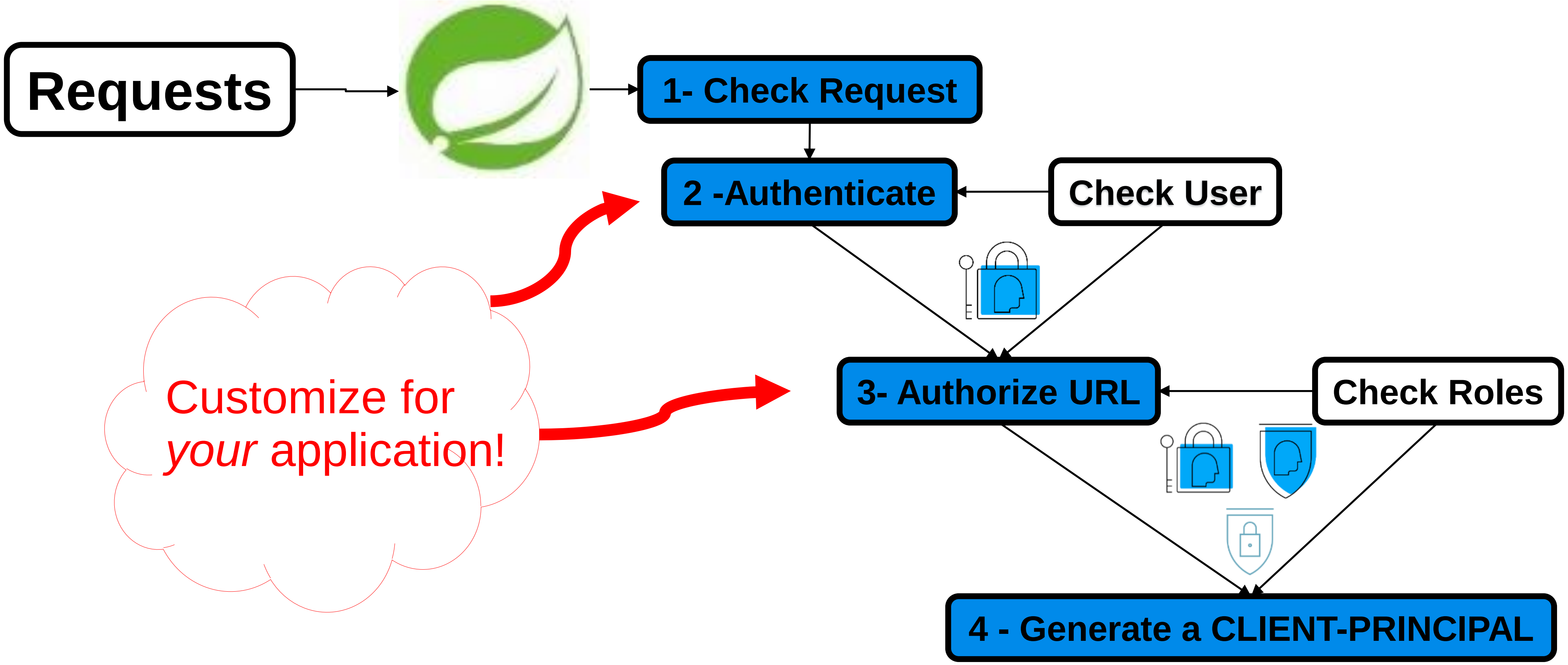
What you will learn

- Don’t use the defaults
- You’re probably disclosing too much
- Use secure protocols where you can
- Limit the pathways into your server
- Think about non-Tomcat security too

Don’t use the defaults

Change the defaults

Configure strong authentication and authorization



Requests

1- Check Request

2 -Authenticate

Check User

3- Authorize URL

Check Roles

4 - Generate a CLIENT-PRINCIPAL

Customize for
your application!

Change the defaults

Check the PASOE security model

```
proenv> tcman.sh config psc.as.security.model

     psc.as.security.model=production
```

- If the security model is “development”, create a new production instance before going live

```
     tcman create -Z prod …
```

Change the defaults

Change the default ports

- In CATALINA_BASE/conf/catalina.properties

```
# port #s used by server.xml
psc.as.http.port=8810
psc.as.https.port=8811
```

Change the defaults

Disable or protect the shutdown port

- In CATALINA_BASE/conf/catalina.properties

```
# port #s used by server.xml
psc.as.shut.port=8812     // Setting to -1 disables
psc.as.shut.pwd=SHUTDOWN  // If not disabled, use strong pwd
```

Change the defaults

Change the Tomcat password

- Update the CATALINA_BASE/conf/tomcat-users.xml
- Update the admin credentials in the OpenEdge Management Console

- Use the SecretKeyCredentialHandler for the User Database

https://docs.progress.com/bundle/openedge-security-and-auditing/page/Secure-the-Tomcat-Manager-and-OpenEdge-Manager-web-applications.html

You’re probably disclosing too much!

Don’t disclose too much!

Be careful with status

- Development server has a default home page that display status
  - Don’t deploy in production
- Make sure status responses are off
  - `statusEnabled=0 in openedge.properties`
- Each transports (REST/SOAP/WEB) have their own individual status pages.

Don’t disclose too much!

Don’t advertise the server type

- Make sure the X-Powered-By HTTP header is disabled

```
server.xml <Connector xpoweredBy=“false” />
```

- Get rid of the Server HTTP Header
  - Default value of this header for Tomcat 4.1.x to 8.0.x is Apache-Coyote/1.1.

```
server.xml <Connector server=“SomeGenericValue” />
```

From 8.5.x onwards this header is not set by default.

- Do not return unnecessary headers that are not mandatory by clients.

Use secure protocols where you can

Secure Protocols

HTTPS

- Enable TLS

  https://docs.progress.com/bundle/pas-for-openedge-management/page/Configure-a-PAS-for-OpenEdge-instance-for-TLS.html

- Enforce HTTPS – either reject HTTP or redirect users to HTTPS

  https://community.progress.com/s/article/How-to-redirect-Progress-application-server-for-OpenEdge-PASOE-http-calls-to-https

- Use HTTP Strict Transport Security (HSTS) to protect against MITM

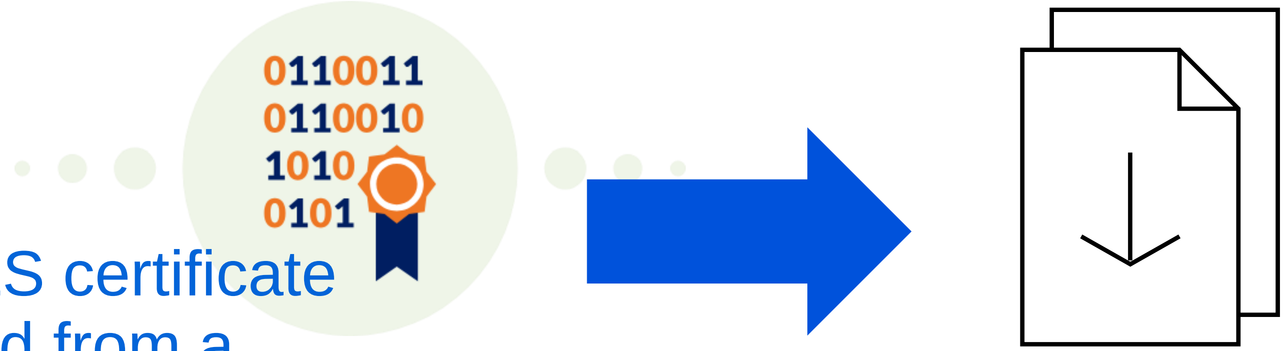
  In CATALINA_BASE/conf/catalina.properties

  ```
  http.spring.headers.hsts=true
  ```

Secure Protocols

Use valid SSL/TLS certificates

- Add a valid key/certificate to your PASOE instance



SSL/TLS certificate obtained from a Certificate Authority (CA)

CATALINA_BASE/conf/
tomcat-keystore.p12

- Do NOT rely on the key/certificate sent by OpenEdge for testing

$DLC/servers/pasoe/conf/Keystore.README

Limit the pathways into your server

Limit pathways into your server

Get rid of unused applications

- Disable unused transports (openedge.properties)

```
[oepas1.ROOT.APSV]
 adapterEnabled=0
```

- Disable unused connectors (server.xml)

```
tcman feature HTTP=off
```

- Disable unused HTTP methods (oeablSecurity.csv)

```
"/apsv/**","GET","hasAnyRole('ROLE_PSCUser')"
```

- Remove unused apps (examples, servlets, doc, manager, host manager)

Limit pathways into your server

Remove unused content

- Remove all of the ABL web app /static/ files provided as samples, unless your ABL application uses them
- Get rid of $DLC/servers/pasoe/archive (security scans sometimes flag)
- Copy off $DLC/servers/redist

Limit pathways into your server

Use the noaccess ROOT application

- A ROOT webapp is always required
- Default for PASOE is a single ABL webapp
- Consider noaccess ROOT when more than one ABL app
  - Allows an unambiguous URL space
  - Replaces the root with a very secure configurable webapp

See the noaccess.README in the pasoe/extras/noaccess.war

Limit pathways into your server

Protect JMX access

- Tomcat (and PASOE) exposes much data and control
- If enabled, needs to be considered an administrator access
- Recommendations from Apache

1. configuring a strong password for all JMX users
2. binding the JMX listener only to an internal network
3. limiting network access to the JMX port to trusted clients
4. providing an application specific health page for use by external monitoring systems

Limit pathways into your server

Configure the Remote Address Valve

- Any administrative application should be protected by the RemoteAddrValve

```
CATALINA_BASE/webapps/<webapp>/META-INF/context.xml
CATALINA_HOME/conf/context.xml and server.xml
```

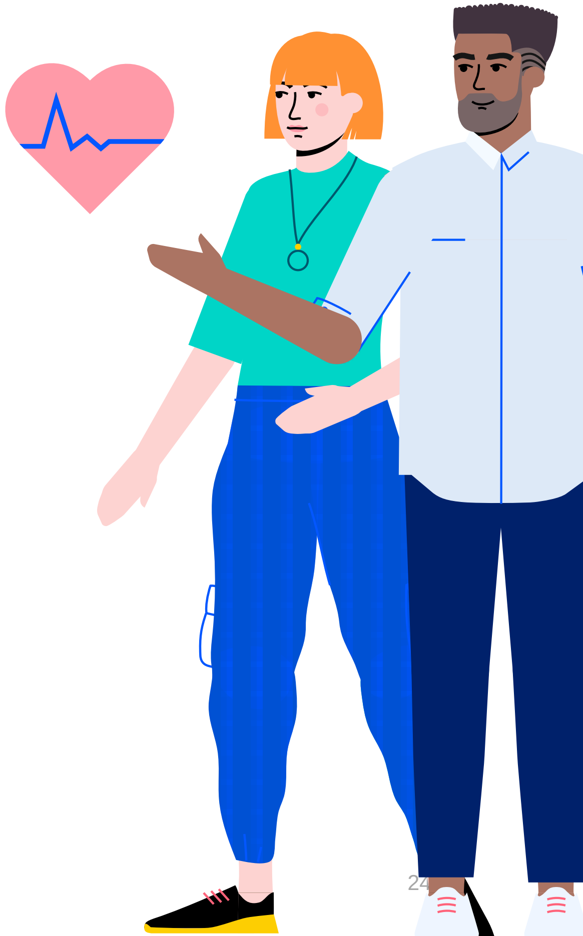
Example: limiting access to localhost (e.g. for manager or oemanager)

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
       allow="127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:0:1"/>
```

Limit pathways into your server

Don’t forget the management paths

- If you use OEE/OEM/OECC – deny access to the manager & oemanager web apps deployment operations.
- In general, do not permit Tomcat on-line deployments and reloads of changed web apps in a production environment.



Think about Non-Tomcat security too

Non-Tomcat configuration

Use a non-root user

- Create a dedicated user for the PASOE processes
- Don’t use a Windows privileged service account
- Minimum necessary permissions
  - e.g. no remote login for the PASOE user

Non-Tomcat configuration

Restrict file permissions

- Loose file-system permissions are often convenient for admins
  - But… disclose too much about application, users, etc.
- Make NOT world readable, no group write access
- Appropriate umask so logs get NO world access
- Example (your requirements may be different)
  - Files owner root, group pasoe (except logs, temp, work -> owner pasoe)
  - Root can read/write. Group can read/execute. World no permissions
  - Bad actor can't change config, deploy new or modify ABL applications

Non-Tomcat configuration

Monitor your PAS for OpenEdge server

- Spikes in authorization or authentication failures
- Unusual levels of access log errors
- Keep an eye on the logs
- Running services and processes

57% of cyberattack victims report that their breaches could have been prevented by installing an available patch

ServiceNow / Ponemon Institute study, 2018

Non-Tomcat configuration

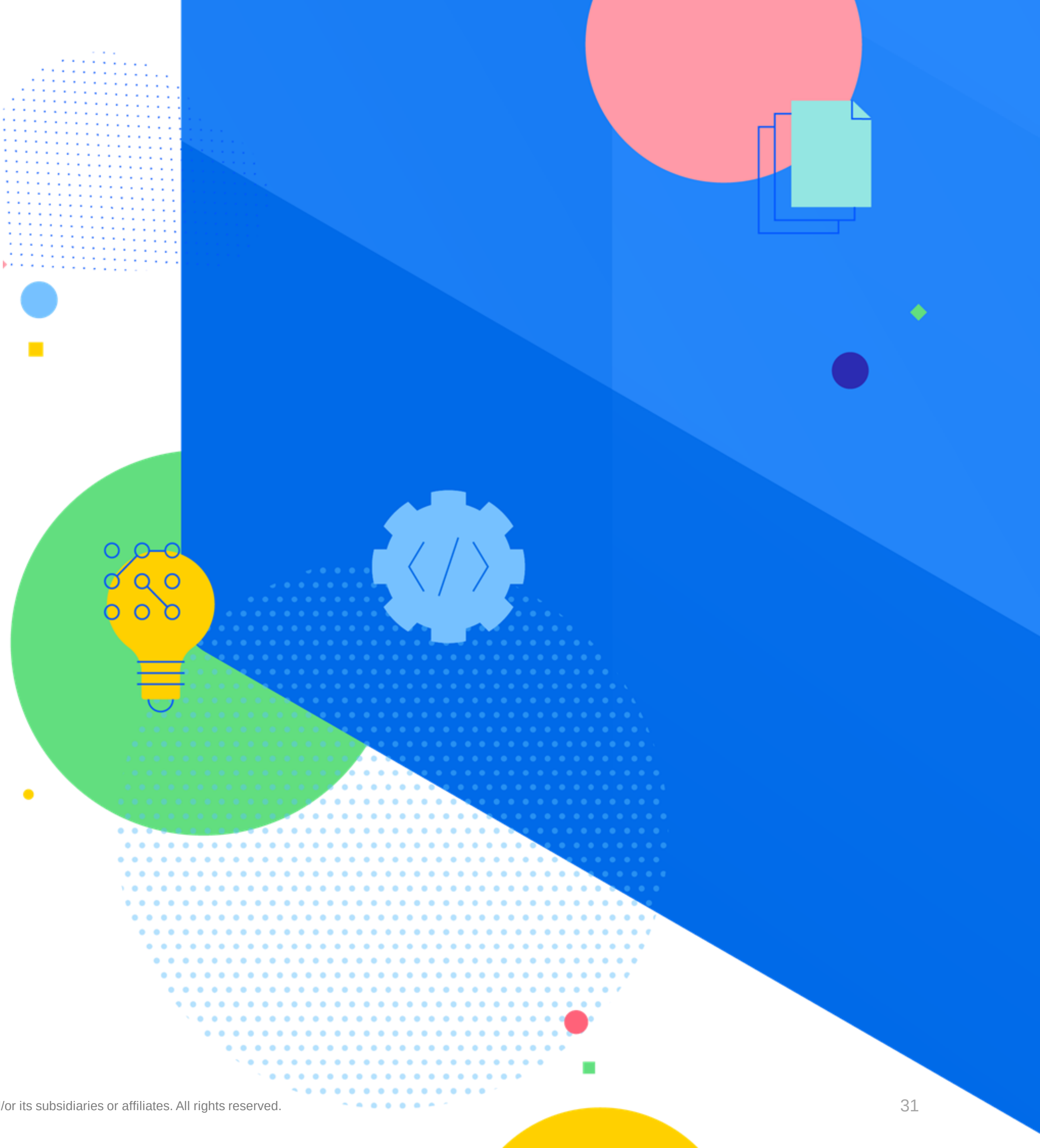
Stay up to date with the latest OpenEdge

- Much more difficult (and sometimes impossible) to patch older releases
- Security patches
- New security features

- Stay current with Java security updates
- OS security updates

What did we learn?

- Don’t use the defaults
- You’re probably disclosing too much
- Use secure protocols where you can
- Limit the pathways into your server
- Think about non-Tomcat security too
- Monitor and stay up-to-date



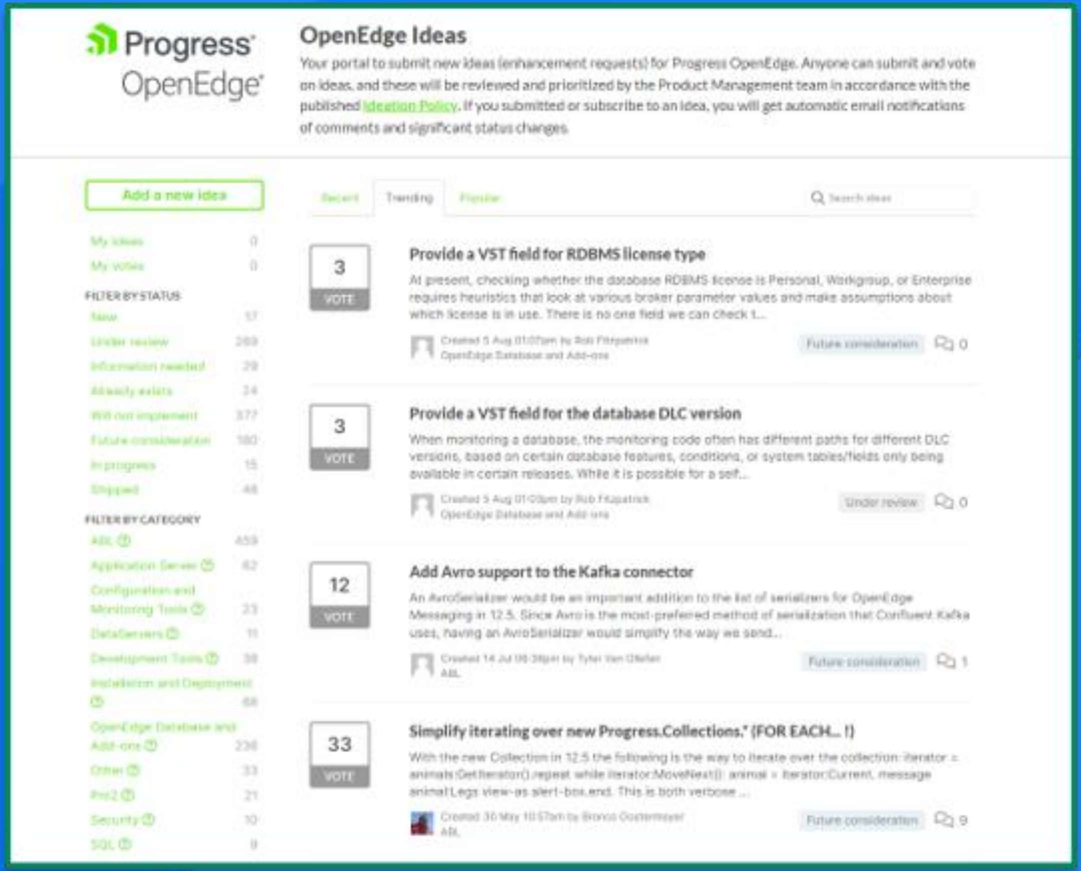
Where can I learn more?

Installation	• See extensive descriptions in $DLC/servers/pasoe/conf/oeablSecurity.properties.README
Documentation	• OpenEdge content portal at https://docs.progress.com • Spring Security, see https://spring.io/projects/spring-security • Ask a question on https://stackoverflow.com with the spring-security tag
Webinars	• 3rd Party Identity Providers and OAuth2
Education	• OAuth2 https://www.rfc-editor.org/rfc/rfc6749 • OpenID Connect https://openid.net/connect/faq/ • SAML2 https://docs.oasis-open.org/security/saml/v2.0/
Training	• Progress OpenEdge AppServer Administration

Don’t See Your Favorite Feature?

Submit and vote on ideas!

https://openedge.ideas.aha.io/



Progress OpenEdge

OpenEdge Ideas

Your portal to submit new ideas (enhancement requests) for Progress OpenEdge. Anyone can submit and vote on ideas, and these will be reviewed and prioritized by the Product Management team in accordance with the published Ideation Policy. If you submitted or subscribe to an idea, you will get automatic email notifications of comments and significant status changes.

My ideas	0
My votes	0
FILTER BY STATUS	
New	17
Under review	269
Information needed	29
Already exists	24
Will not implement	377
Future consideration	180
In progress	15
Shipped	48
FILTER BY CATEGORY	
ABL	459
Application Server	62
Configuration and Monitoring Tools	23
DataServers	11
Development Tools	38
Installation and Deployment	68
OpenEdge Database and Add-ons	236
Other	33
Pro2	21
Security	10
SQL	8

3 VOTE

Provide a VST field for RDBMS license type

At present, checking whether the database RDBMS license is Personal, Workgroup, or Enterprise requires heuristics that look at various broker parameter values and make assumptions about which license is in use. There is no one field we can check t...

Created 5 Aug 01:07pm by Rob Fitzpatrick
OpenEdge Database and Add-ons
Future consideration 0

3 VOTE

Provide a VST field for the database DLC version

When monitoring a database, the monitoring code often has different paths for different DLC versions, based on certain database features, conditions, or system tables/fields only being available in certain releases. While it is possible for a self...

Created 5 Aug 01:03pm by Rob Fitzpatrick
OpenEdge Database and Add-ons
Under review 0

12 VOTE

Add Avro support to the Kafka connector

An AvroSerializer would be an important addition to the list of serializers for OpenEdge Messaging in 12.5. Since Avro is the most-preferred method of serialization that Confluent Kafka uses, having an AvroSerializer would simplify the way we send...

Created 14 Jul 06:36pm by Tyler Van Olleter
ABL
Future consideration 1

33 VOTE

Simplify iterating over new Progress.Collections.* (FOR EACH... !)

With the new Collection in 12.5 the following is the way to iterate over the collection: iterator = animals:GetIterator().repeat while iterator:MoveNext(): animal = iterator:Current. message animal:Legs view-as alert-box.end. This is both verbose ...

Created 30 May 10:57am by Bronco Oostermeyer
ABL
Future consideration 9

Join the CVP!

OpenEdge Customer Validation Program

Actively influence the developer experience and future enhancements of Progress OpenEdge!

Get Access to:

Roadmap surveys
Usability reviews
Pre-release software

Virtual open houses
Quarterly objectives
Sprint reviews

https://www.progress.com/openedge/customer-validation-program

Progress®