OpenACS and EuroTcl 2025

WU
WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS

Panel 3

Future Directions of NaviServer and OpenACS

Moderation: Gustaf Neumann

JULY 11, 2025

Collected Wishes (1/2)

OpenACS:

- Security level installation modes: high , medium, community.
  This setting will change the default values of many parameters to harden the instance.
- ACS Authentication - password requirements (complexity, aging, length, history)
- CSP handling and centralized reporting
- OACS security posture scan
  - Central page for collecting potential threads in 5.10.1 release (including vulnerability checks for upstream .js packages, automated upgrade support)
  - After release of OpenACS 5.10.1: vulnerability checks for used
    - PostgreSQL client library
    - PostgreSQL server

    Requires NaviServer 5

OpenACS in general

- Drop CVS once and for all, move to GitHub and use all collaboration features there
  (incl. bug tracker, merge requests,...)
- How can we cleanup code/website/documentation
  - Who can decide to delete an outdated wiki page/docu page/package/proc;
  - how can we detect/vote on candidates to be deleted/deprecated/removed from core)

Collected Wishes (2/2)

OpenACS:

- Centralized virus scanner for uploaded files:
  Current state: optional virus scanner based on clamav for XoWiki and derived packages.
- Reports about SQL injections via custom packages using e.g. DataTables.
  Current state: OpenACS has upgrade (local and/or CDN) mechanisms for all included .js packages, but not for custom packages.
  Option: provide a channel for further wishes, automate checks further.
- Request-processor and the “long calls” monitoring for cluster installations
  Current state: slow calls above provided thresholds are classified into slow/medium/good, logs are written per server to a log file, which is analysed from OpenACS. Wanted: centralzed reporting for all node
  Options: write to DB, send in cluster-case to the coordinator (canonical server)
- Oracle support lags behind

NaviServer:

- Secrets management - keys should not in configuration files or on the server machine, but managed by some secrets manager (macOS Keychain, AWS Secrets Manager, Azure Key Vault, Google Secret Manager, …)

  Candidates:

  - .pem certificates containing private keys
  - DB passwords
  - Parameter and cluster secrets in OpenACS

What answers do we have for the big trends?

Big IT-trends

- Mobile computing
- Cloud
- Microservices
- Trust, Risk, Security, Dependability
- Generative AI
- Others?

Realistically

- We can’t shape the trends, but we can’t ignore it either.
- One strength of OpenACS are well-functioning large-scale applications, which need a path for development.