SCAP.com Introduction

Aharon Chernin

Unrealized benefits of security standards

- Community

Current status - Developmental

- Website is up
- Mailing lists and forums
- Repository is not live
- We are starting with OVAL, followed by XCCDF and other standards

Repository Features; *Community*

- Build a “meritocracy” where quality and contributions earn rank within the community.
- Highest merit achievers will join the SCAP board to assist in definition approvals
- Definitions are quality rated by users. Definition quality impacts merit.
- Submission age impacts merit. Merit earned from a large one time submission will decay over time.
- Definitions will support discussions
- *Perhaps* - Revenue sharing with highest merit earners

Why do we need another repository?

- Competition is healthy. There should never be a single master repository
- We need a repository that fosters a community
- The community needs a repository that shares the vision of the private sector
- To promote the use of SCAP standards, a repository can be used to generate public contribution
- Features. The security community requires a feature rich standards repository

What powers us…

- Drupal 6.x content management system
  - Powers sites like - Whitehouse.gov, popularscience.com, nasa.gov
  - Less time reinventing the wheel = More time coding an repository
  - OVAL Content is Drupal aware. Meaning, stored in native Drupal formats. == Less code to write
  - I only have to support the custom OVAL management modules that I created
  - Large user contribution and support community

OVAL Repository Features
OVAL Submissions

- OVAL documents XML validated upon upload
- XML is “beautified” automatically
- OVAL definitions are automatically checked against published and unpublished best practices and the results presented to the end user.
- Duplicate content identified
- Automatically change submitted Objects, States, and Variables duplicates to use existing content.
- Submit to Mitre and SCAP.com at the same time

OVAL Repository Features
The Repository

- Full version control
  - Any “accepted” change increments versions on Definitions and Tests
  - Recursive version control. Changing an inventory definition or test will increment impacted definitions version.
- “Diff Viewer”
  - Go back in time and see the changes made to any part of a definition or test.

OVAL Repository Features
The Repository

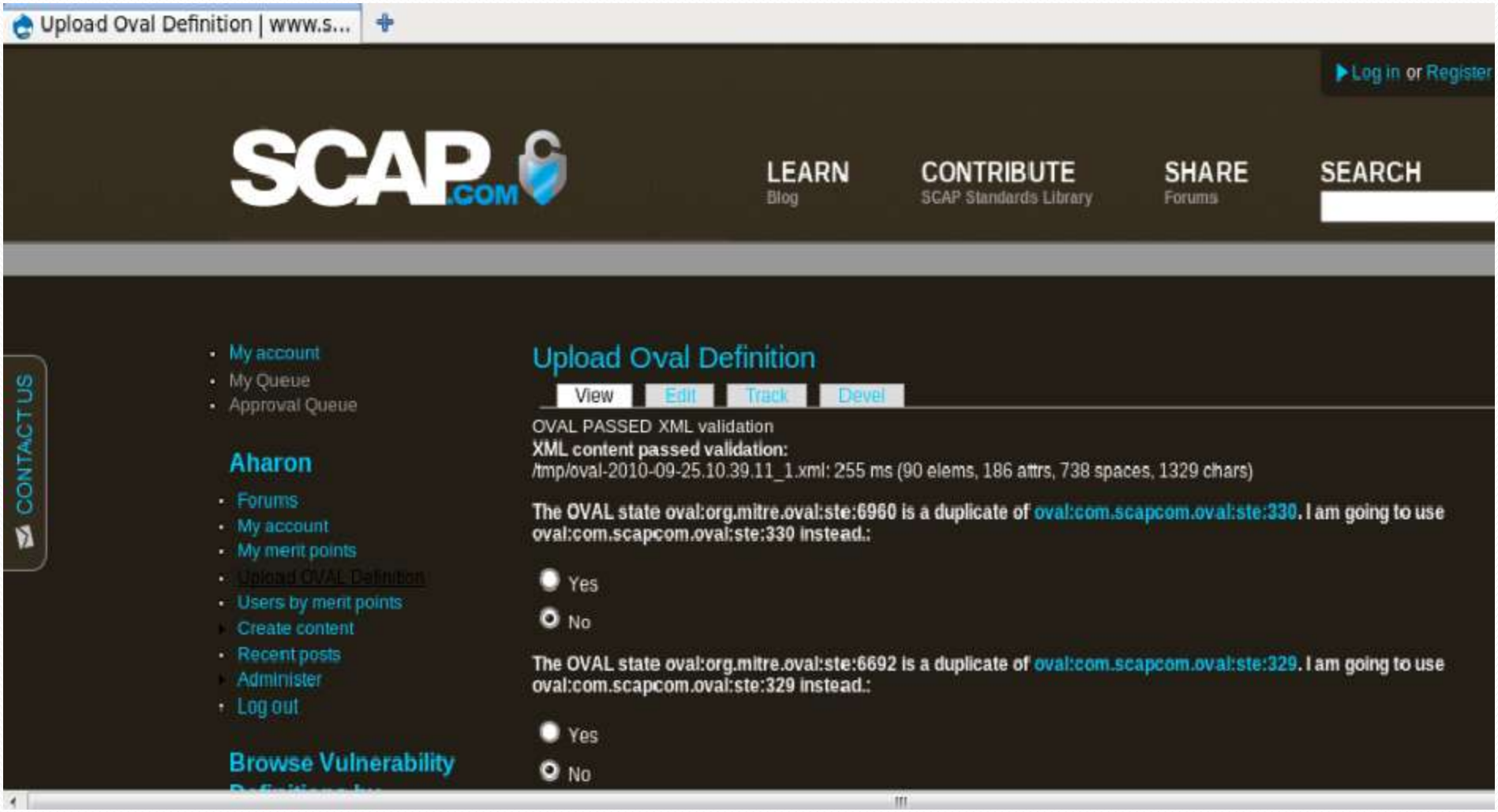
- Duplicate definitions, tests, objects, and states will produce warnings
- Approval Queue
  - Assigned approvers can accept or reject pending or mod_pending definitions
  - View the “Diff View” and “Best Practices” results during review
  - New tests are automatically approved with their definitions
  - Modified tests must be approved by an approver

OVAL Repository Features
The Feed

- New thought processes on OVAL feeds
  - The developer OVAL feed
    - Contains all content regardless of status
    - May contain orphan content
    - May contain multiple versions of content
    - Will be much larger
  - The production OVAL feed
    - Contains only “Accepted” content
    - Has no orphan content
    - No duplicate content (definitions, tests, objects,etc)
    - Latest “accepted” version of content only
    - Will be much smaller
  - Feeds by quality

OVAL Repository Features
The Feed

- Ability to choose Mitre or SCAP.com version methodology
- Ability to select Mitre or SCAP.com status methodology
- Feed builder
  - Build your own feeds


Upload Oval Definition | www.s...
Log in or Register
SCAP.COM
LEARN
Blog
CONTRIBUTE
SCAP Standards Library
SHARE
Forums
SEARCH
CONTACT US
My account
My Queue
Approval Queue
Aharon
Forums
My account
My merit points
Upload OVAL Definition
Users by merit points
Create content
Recent posts
Administer
Log out
Browse Vulnerability
Upload Oval Definition
View
Edit
Track
Devel
OVAL PASSED XML validation
XML content passed validation:
/tmp/oval-2010-09-25.10.39.11_1.xml: 255 ms (90 elems, 186 attrs, 738 spaces, 1329 chars)
The OVAL state oval:org.mitre.oval:ste:6960 is a duplicate of oval:com.scapcom.oval:ste:330. I am going to use oval:com.scapcom.oval:ste:330 instead.:
Yes
No
The OVAL state oval:org.mitre.oval:ste:6692 is a duplicate of oval:com.scapcom.oval:ste:329. I am going to use oval:com.scapcom.oval:ste:329 instead.:
Yes
No

WE NEED HELP

- We need either $$$ or developer support to finish this concept
- The Future…