SWAMP Demo for OWASP Omaha & InfraGard

Notes from the OWASP Omaha Dec 2014 chapter meeting and SWAP demo
12/18/14, as prepared by Allyson Miller

WebEx screencast available at

- Please forward these notes to anyone else who would like them.
- Meeting recording and WebEx player: https://app.box.com/s/8hfh2be846i6bmqja0fm
- Note: The mir-swamp.org SWAMP website will be down for maintenance from 2-4pm today (Thurs. 12/18/14), so please try us out and register later this evening or tomorrow!

Attendees:

- Pat Beyer (SWAMP Project Manager)
- Ally Miller (SWAMP Admin)
- Darrell Dwelley (SWAMP Assurance Analyst/Lead Programmer)
- John Rogers
- Michael D'Alfonso
- Zac Fowler
- Jim Manico
- Tom Brennan
- Others from OWASP-Omaha

SWAMP Project Overivew

- Went live in Feb 2014
- SWAMP is hosted at the Morgridge Institute for Research in Madison, WI
- We're a collaboration of 4 organizations
    - Morgridge (non-profit, private, research institute)
    - 3 universities
        - Indiana University (Cybersecurity, help desk)
        - University of Illinois at Urbana-Champaign (Identity Management)
        - University of Wisconsin-Madison (Chief Scientist, tool integration)
    - ~30 employees total, 17 at Morgridge
- DHS project, no-cost
- Languages supported now: Java source, Java byte code, C/C++, Python
    - Android/mobile is coming in January
    - PHP, Javascript, more to come…
- A variety of open source tools.
- Partnerships with 4 commercial tool vendors:
    - Parasoft (C/C++test and Jtest are available now)
    - GrammaTech (Code Sonar, coming soon)
    - Veracode (coming soon)
    - Red Lizard (Goanna, coming soon)

- Any open-source developer or educator/student can use open source and commercial tools for free!
- Wanting to promote testing of open-source code, since it's incorporated into other products
- SWAMP hosts 400 packages (including NIST Juliet Test Suite) with known vulnerabilities to use to test against software assessment tools you develop
- The strength of the SWAMP is that you can run your code against multiple tools at the same time and view a standardized report of results from all the tools in one place (CodeDx results viewer from Secure Decisions).
- We maintain tools, perform updates, etc. for you
- Secure environment

Progress of Open-Sourcing SWAMP

- We are completing our internal code review now. Will have SWAMP out for open-source in January.

Installing an Independent SWAMP Environment

- January's open-source publication is very raw. Illinois is working on testing the process and documentation of setting up their own SWAMP environment.
- Later open-source offerings will be better documented and easier to deploy
- Open-source tools will come with it.
- Commercial tool hooks would be there, but you would need to work out an agreement with commercial tool vendors before using their tools.

Funding and Future of the SWAMP

- Fully funded by DHS S&T directorate through Sept 30, 2017.
- Morgridge is committed to keeping SWAMP running as it is now. The intent is to keep SWAMP open and free.
- Funding opportunities will be pursued for after DHS funding ends.
- Possibility of getting some funding from Morgridge and commercial vendors. Morgridge would continue hosting hardware.

Hardware

- 700 cores
- Equipped to handle and manage/scale up to 700 cores
- Physically secured data center
- Red Hat RHEL 6.6
- AlienVault for secure logging
- When assessments are built, they are built with a package of software against a selected tool and OS/platform. We run assessments in a secure VM in our back-end environment. Once the assessment completes, the VM disappears and results are standardized and available in our native or CodeDx viewer.
- All hardware is SWAMP-dedicated.

Other DHS Projects

- There are other SWAMP-esque projects in DHS but mostly just single tools. We are multiple tools and a secure environment.
- Car Wash environment at DHS to develop and test applications

- We are talking with other DHS projects that could link in to the SWAMP.

Case Studies

- We have had good feedback from users, but we don't track details of what our users do. We are working on developing metrics to collect anonymized data for analysis. Working on getting case studies to share.
- 400 users
- 1200 assessments per week
- Integrated with Bowie State curriculum.
- Xcellus did penetration testing for the SWAMP and is using us for their testing now.

Privacy

- We have an agreement with the US Government. It does not have the rights to the software that is uploaded into the SWAMP. Morgridge is committed to protecting data. Privacy Policy and Whitepaper.
- Only a couple of SWAMP staff members could get to your code for support purposes and would require approval to do so. Also, the hardware that accesses the code conceals user data so it's not easy to determine what's being run when assessments are being performed.

Data Persistence

- Data persists as long as users leave it in the SWAMP as part of their project.
- Deleting code in projects or deleting user accounts will remove the code. It is not stored elsewhere.

Testing of the SWAMP Itself

- Darrell performs some application testing, uses OWASP Zap for web-front end.
- Middle-ware/back-end is done by the Infrastructure team at Morgridge and by the cybersecurity team at Indiana.
- We "eat our own dog food". Any code we run that's supported in the SWAMP is also run through the SWAMP.
- We do a week of active security and development testing prior to each release. This is a different team doing testing, aside from the developers.
- We do a yearly external test for the security of both our facility and site. (Xcellus is a DHS contractor. Last done in Feb/March 2014. Finding a new contractor for next year.)
    - Pat will review what outcomes of this can be shared/made publicly available.
- We have a very active, creative, and robust cybersecurity team and third party involvement.

SWAMP Demo

- Log in with GitHub credentials or create an account with us
- You do everything through a Project. Projects can be private or shared with others. Projects have owners who have overall control.
- Upload your code in a Package, specifying the tool(s) to run against, and the platform. You may specify versions of packages, tools, and platforms.
- You can run assessments once or schedule runs (daily, weekly, monthly).
- You can pull code from public GitHub repositories. We're working on figuring out private repositories and other repos besides GitHub.

- View results from multiple tools in a single results viewer, CodeDx.
    - CodeDx shows results with line of code, CWE value, severity/priority, etc.
    - Comments are stored and are available to other people as you work through.

Platform selection

- We intend to support as many platforms as we can.
- Open-source were first.
- We will be adding Android, iOS, OS X, and Windows.
- Can run your packages against multiple platforms.

No Build

- We offer a no-build option for raw source code analysis without linking/compiling everything.

Tools

- The tools offered are as robust as possible, with filtering available in the viewer.

Feedback

- If you are a user and would like something added (tool, package, platform, language, etc.), PLEASE TELL US! We take user needs into account with our development schedule.
- Support@continuousassurance.org