The Computerworld Honors Program

Honoring those who use Information Technology to benefit society

Final Copy of Case Study

Status:
Laureate

Year:
2013

Organization Name:
NASA Office of the Chief Information Officer, Information Security Division

Organization URL:
http://www.nasa.gov/offices/ocio/itsecurity/index.html

Project Name:
Web Application Security Program (WASP)

Please select the category in which you are submitting your entry:
Safety & Security

Please provide an overview of the nominated project. Describe the problem it was intended to solve, the technology or approach used, how it was innovative and any technical or other challenges that had to be overcome for successful implementation and adoption. (In 300 words or less.)

NASA has a diverse Information Technology (IT) infrastructure that encompasses over 4,000 Web applications providing communication and data to partners around the globe. Malicious actors use web applications as a gateway to attack NASA's infrastructure. In an effort to address this challenge, the NASA OCIO established a Web Application Security Program (WASP) to focus on assessing the security posture of the agency's web applications. The WASP team conducts automated and manual testing across the enterprise to identify critical vulnerabilities. The WASP team works with the IT Security stakeholders to ensure remediation of vulnerabilities, and provides vulnerability scanning tools for stakeholders. The WASP team employs innovative, custom methods enabling discovery and remediation of enterprise vulnerabilities prior to exploitation by

malicious actors. As a result the actions have significantly reduced the attack surface available to threat actors thereby improving the agency's security posture.

When was this project implemented or last updated? (Please specify month and year.) Has it incorporated new technologies and/or other innovations since its initial deployment? (In 300 words or less.)

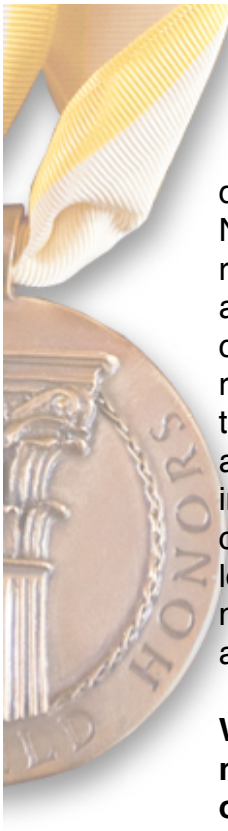
The program was launched in June 2012. Since program inception, the WASP team has developed significant innovations, including extending the commercial scanning tools used to find key features on web applications, which allows the subject matter experts to focus their attention on manual testing. The features of the scanner has been extended to find CGI scripts, Java Applets, PHP Pages, and PII collection in web forms. These features are red flags for locations in web applications where vulnerabilities normally exist. The enhanced features free the analysts to focus on finding specific vulnerabilities through manual testing. The WASP team continues efforts to refine the scanning tool.

Is implementation of the project complete? If no, please describe the project's phases and which phase the project is now in. (In 300 words or less.)

Implementation of the project is not yet complete. During the inception phase of the program the WASP team took time and effort to coordinate with system and network administrators and web application teams across the enterprise to ensure that scanning activity did not interfere with NASA's mission. The NASA WASP scanning activities are being implemented in phases with approximately three centers being added in each phase. As Centers are incorporated, automated scanning and manual testing activities are incorporated into the Agency's continuous monitoring framework. The team is systematically moving this critical program into an operations and maintenance (O&M) phase for the initial Centers that have under gone web application testing. By June 2013, implementation should be complete across NASA's enterprise, and the project will be fully in an O&M mode of operations.

Please provide at least one example of how the technology project has benefited a specific individual or organization. Feel free to include personal quotes from individuals who have directly benefited from the work. (In 300 words or less.)

In the short period (six months) since the program's inception, the WASP team has identified 27 critical and 37 high-risk vulnerabilities across all of NASA. Examples include: The discovery and mitigation of vulnerabilities that would have resulted in the potential loss of a significant number of complete PII records. The



discovery and mitigation of vulnerabilities could have resulted in exposure of NASA credentials. The program identified the vulnerabilities that could have resulted in the direct compromise of multiple NASA servers by external threat actors, and collaborated with the Centers to remediate the findings. This collaboration resulted in reduced lag time between vulnerability discovery and remediation. The Chief Information Security Officer (CISO) at one center noted that this program provided a critical capability for the Agency. The Deputy CISO at another center said he was impressed with the results, in particular this innovative web application security approach found numerous vulnerabilities that current tools and techniques were unable to identify. In addition, to ensure the longevity of the mitigations and to secure NASA's enterprise the team provided multiple NASA Centers with tools and training necessary to perform web application security training at the Center level.

Would this project be considered an innovation, a best practice or other notable advancement that could be adopted by or tailored for other organizations and uses? If yes, please describe that here. (In 300 words or less.)

Innovation: Through this project, the WASP team adapted and enhanced industry best practices across the NASA enterprise. Specifically, the commercial scanning tool used was extended to detect applications with particular properties, such as CGI scripts, Java applets, PHP pages, and interesting parameters. This allows the manual testing to be better focused. We are not aware of anyone else using such a hybrid approach with custom scanner extensions for web application testing. Additionally, the test team is developing tools to mine data from the raw data to guide manual test efforts. This innovation has allowed the program to use a small team of subject matter experts, resulting in lower cost and improved finding for the agency.