Web application security services

Why you should participate:

Web applications are subject to various vulnerabilities or attacks that can cause damage, or allow unauthorized access, to data protected by law and/or policy. Failure to perform these scans presents unacceptable risks to individuals, campus units, and the university, and increases the university's liability in the event of a breach.

While automated scanning alone does not mitigate all risks posed by campus web applications, it is a baseline security requirement for all applications that transmit or store PII (personal identity information). This requirement is supported by widely accepted best practices (OWASP Application Security Verification Standard 2009), as well as conclusions and recommendations drawn from breach investigations (Verizon Data Breach Investigation Report 2011, page 66).

How you can participate:

Contact appscanadmins@ucdavis.edu. Please briefly describe your request and the application you would like to scan. Then the AppScan team will contact you to:

• Help outline and document the steps to complete the scanning and remediation.
• Train unit technologists, one-on-one, on how to use AppScan.
• Configure initial application vulnerability scans.
• Coordinate successive runs to verify that the vulnerabilities have been remediated.
• Help identify issues that must be addressed.
• Recommend recharge services for units that might need resources to conduct the application scanning, or to set up the test environment for the scans. (Campus units are responsible for providing a test environment for application scanning.)

What are your responsibilities?

While AppScan administrators can help you with the scanning process, it is up to individual development teams to:

1. Provide and maintain a test environment.
2. Ensure scans are done annually and reviewed periodically.
3. Verify scans are exercising all or most of the application, including all critical functionalities.
4. Verify scans will not impact production or external systems.
5. Mitigate any vulnerabilities that are uncovered.