ARE YOUR ENTERPRISE AND ITS APPLICATIONS IN SAFE HANDS?

Infosys®
Navigate your next

Insecure Application – an open invitation to hackers

Writing an insecure application code is no less than leaving the master key under the doormat.

Not all the developers consider the security aspect while building an application. Different studies and surveys show that **approximately 75% of the cyber-attacks happen due to an insecure application containing the insecure code.**

Being exposed to the outside world, applications have become a leading vector for cyber-attacks. In this hour of need, an enterprise really needs to be assured of the quality of the source code that goes in the application.

If you ponder your application isn't coded the way it should be and perhaps on the hit list of hackers, you need not to panic. We have the solution for you.

How can Infosys help you become "secure"?

Infosys developed Security Testing framework, in collaboration with HPE solution, **integrates the process of Fortify security code scans with existing QA builds** for applications and uncovers all the potential application security issues.

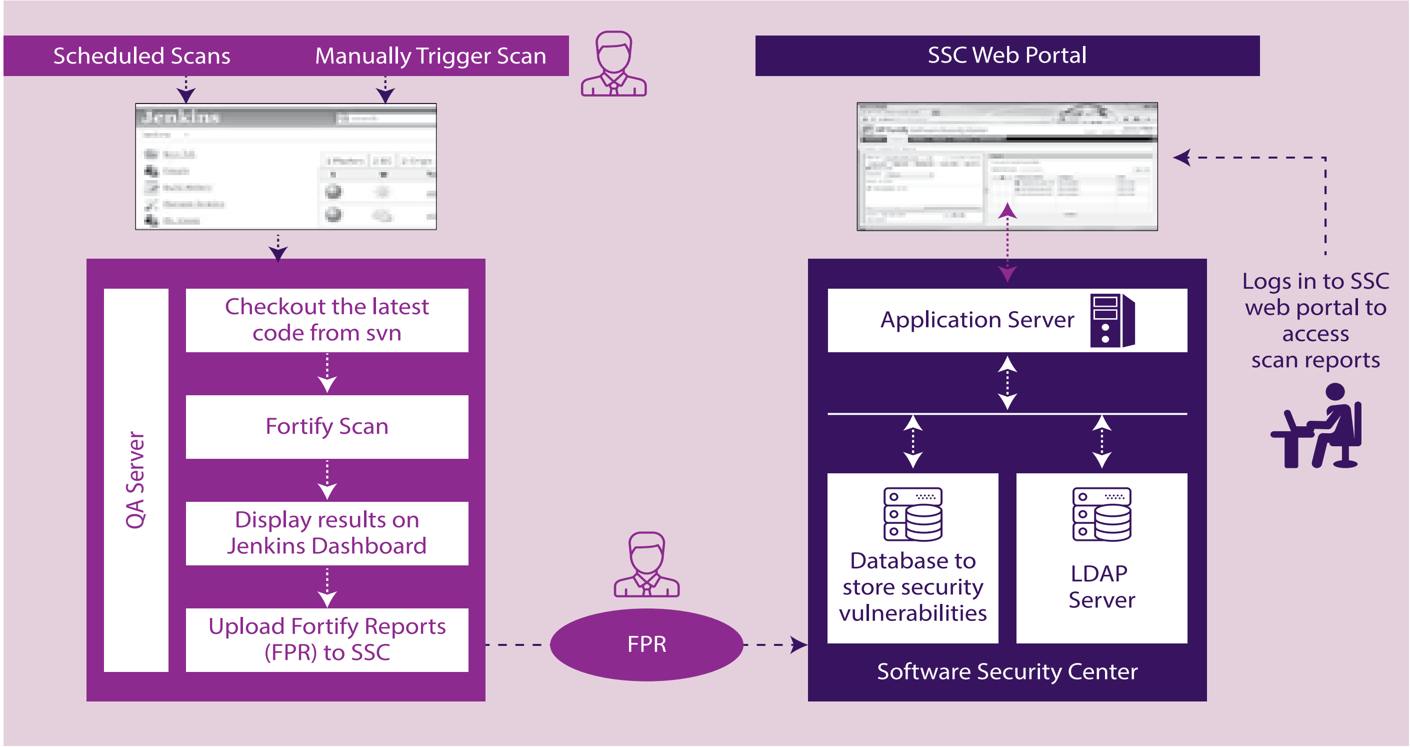
The framework addresses the perennial problem of false positive removal from scan results by using the Infosys developed filter sets and thereby, **eliminating thousands of false positives in a fraction of time.** With this, the framework assures to provide a **quick turn around on critical and high security issues via a centralized application (Fortify Software Security Centre).** Authorized users (Developers/ Managers) can login to Fortify Software Security Centre portal to monitor the scan results, make comparative analysis and strategies for issue resolution.

Why should you choose our solution?

- On-demand scan to uncover vulnerabilities.
- Alert for new high confidential, high severity issues on weekly basis.
- Regularly patching and updating all third party library/ components using OWASP dependency checker.

Infosys HPE Fortification Solution

Infosys HPE collaborated Security Testing approach is better than the conventional Secure Code Analysis approach carried out on a desktop. In the Desktop approach, the Security Analyst has to download the application source code on his desktop and run the security scan. This leads to additional time and effort for false positive elimination during the rescan. Our testing solution helps to overcome this by managing the scan results in a systematic and efficient manner.


Scheduled Scans
Manually Trigger Scan
Jenkins
QA Server
Checkout the latest code from svn
Fortify Scan
Display results on Jenkins Dashboard
Upload Fortify Reports (FPR) to SSC
FPR
SSC Web Portal
Application Server
Database to store security vulnerabilities
LDAP Server
Software Security Center
Logs in to SSC web portal to access scan reports

*Software Security Center (SSC) – A browser based product that stores all the Fortify Reports (FPR) and security vulnerabilities.

Top 10 Benefits

- Customized shell script automates the build and scan process for all applications
- Facilitates continuous integration process with Jenkins and run periodic scans
- Capability to perform efficient scan by filtering blacklisted rules and reduce scan time.
- Provide options to filter vulnerabilities before & after scan with minimum/zero false positives
- Provides user to opt for multiple filters based on the type of the code.
- Provides Custom Rule to improvise vulnerability detection
- Reduced effort in false positive elimination during rescan via the Fortify 'Merge option'
- Provides options to add custom recommendation for security vulnerabilities
- Support for memory tuning based on the complexity of the applications
- Improves the Scan quality and performance by allowing the user to control the "cut off" point to limit the analyzers

Infosys Key Accelerators and Differentiators

- Over 100+ certified security consultants (CEH, OSCP, GPEN, CISSP, CISA, etc.)
- Strategic partnership with HP
- In house repository (Application Security Assessment tool, Security Checklists and Guidelines)
- Dedicated Infosys Center of Emerging Technology Solution (iCETS) security CoE team to drive innovations in the security domain

Success story with one of our esteemed clients

Client Overview	The Client is an American multinational technology company that designs, develops and sells consumer electronics computer software and online services.
Business Drivers / Needs	Enhance comprehensive security assessment by implementing static analysis of source code for key applications Identify and remediate vulner abilities in applications early in the software development lifecycle to reduce costs, improve efficiency, and enhance application security Lack of processes for security assessment Support for “shift left” approach by identifying and mitigate vulnerabilities earlier in the lifecycle
Infosys Solutions	As a solution for the above needs on the static code analysis , Infosys team had performed initial assessment on various SCA tools and came up with a best approach to build a framework “Fortification”, an integrated solution that performs static code analysis using HP Fortify .The framework triggers scan, perform analysis , generates report and upload the results in SSC. Infosys team created an optimized filter sets to capture only the relevant vulnerabilities during the scan phase .Hence reducing manual effort by 60% Setup a one stop centralized portal (Software Security Center) for vulnerability management Quick turn around on scan results with Critical, High and most probable issues with almost zero false positive tolerance Provide developers with different scan mode on demand basis and facilitate to filter the issues pre & post scan Schedule weekly scan for 50+ applications to alert for new vulnerabilities Enhanced developer awareness of secure coding practices Detailed line-of-code guidance and remediation on identified vulnerabilities
Value Delivered	Ability to perform static analysis for 50+ applications with more than 100 million lines of codes scanned till date Reduced risk Significant reduction in vulnerabilities at code level enhances the protection of consumer information and reduces the company’s risk Ability to uncover 1000+ security vulnerabilities with the support of various Fortify rule sets comprising Dataflow, Structural, Configuration and Semantic issues. Critical / high security issues were detected & mitigated at early stage in QA Process

For more information, contact askus@infosys.com

Infosys®
Navigate your next