WhiteHaX WebSite & WebApp Verification Services

WebSite & WebApps are Business Critical: Most Enterprises in the world, large or small, usually have one or more Web-sites for representing their business information and potentially for conducting different sets of business activities through the Internet. A lot of them also rely on internal and external facing web applications, whether developed internally or purchased off-the-shelf. While some Web-sites and Web Apps are simple with only web-based interface, most are much more complex and may make use of back-end processing servers like Authentication, Database, Other types of application processing and transaction servers such as CRM, ERP and others. Given most Web-sites and Web Apps have access to some level of critical data, these sites and Apps usually are a prized target for hackers and malicious users.

Typically, most companies already have some level of security in place for protecting and limiting access to their Web-sites and Web Apps. However, it's still critical to get security verification of such deployed solutions, their respective config policies and the inherent security of the Web-site or Web App. Web Apps are also frequently modified, combine that with vendor s/w updates and configuration/policy changes, these Web-sites and Web Apps, their security and controls on the servers need to be also assessed and verified periodically, to ensure intended protection and enforcement.

Security Verification for WebApp Developers: For software vendors who develop commercial Web Applications as well as Enterprises who have their custom web-based applications, it's even more important to get security verification of the inherent features and implementation of their Web Apps. This allows them to a) reduce potential risk of data compromise at their customer (or internal) deployment, b) avoid the risk of brand-loss and potential liabilities in case if their app causes a breach at a customer (or internally) & c) to provide customers a level of comfort that developer/vendor has done enough security testing on their app. To achieve that, one of the most common method is to add WebApp security verification during the application release cycle i.e. during DevOps, to ensure security verification is part of the application and website release process. Due to the potential for coding errors, it's important for website and WebApp developers to have an external audit of their software performed periodically.

Web-threats: While the simplest form of Web-site attack may be through D/DoS, which could make web-sites and underlying WebApps inaccessible or unavailable for users and for conducting online business, there are many techniques of website and WebApp breaches and exploits. Some of the most common type of web-site breaches are through exploiting known vulnerabilities in web-server and web application software platforms, threats such as SSL exploits, SQL injection, Cross-site scripting and others. However, there are a lot of other advance techniques available for web exploits, which are also now utilized by malicious attackers against web-sites and WebApps, threats such as evading WAF filters evasion, Asynchronous Vuln exploits, XML/XXE exploits etc.

Having these types of attacks and other commonly used web-exploitation techniques, verified through an external web security verification, are a key to successfully ensure that neither business websites nor internally developed WebApps fall prey to such attacks and exploits.

WhiteHaX Web-site and WebApp Verification Services: WhiteHaX Web Verification services utilizes the purpose-built WhiteHaX solution along with other tools and methods to thoroughly verify inherent security of the websites and Web Apps. WhiteHaX first performs web-crawling to build the behavioral model of the Website and/or WebApp. This includes information collected through web-crawl such as types of web components used in developing the website or WebApp, accessible forms and other methods for data processing as well as

potential back-end services utilized such databases etc. Then utilizing this info, it checks hundreds of vulnerabilities, security breach techniques and malicious behavior scenarios against the Website and underlying WebApp, to verify the security of the Website/App and its implementation.

Once the crawl and the verification tests are completed, WhiteHaX then provides a complete verification reports with details of identified security issues as well as based on the type of service, recommend potentially applicable fixes and other suggestions on preventing such security issues from exploits. Some of the attack verification scenarios performed by WhiteHaX include,

- *Web-Crawl:* Crawling the Web App to build a behavioral model then utilize captured details to generate verification of various exploits and threats such as buffer overload, parameter validation, data over-runs, URL manipulation etc.
- *Common Techniques:* Verifying User AUTH and Access Control boundaries; verify commonly used attack techniques like SQL injections, cross-site scripting, SSL attacks, cookie exploits etc.
- *Advance Techniques:* Checking for vulnerability to advance attack techniques such as Privilege escalation, Cross-site forgery, Web-site hi-jacking, XPATH, Shell-shock, Web-app-timing attacks etc. and even more sophisticated techniques such as evading WAF filters, Asynchronous Vuln exploits, XML/XXE exploits, Magic hashes etc.
- *Intrusive Attacks:* While all or most of the above verifications are done non-intrusively on a production site or application, optionally WhiteHaX can also perform intrusive verification of the web-site or WebApp to analyze how an actual attack against them can exploit existing attack surfaces and how deep the penetration may get, including data-exfiltration attempts.

Here are some of the key features of the periodic WhiteHaX Website and WebApp Verification service,

- **Remote verification:** WhiteHaX Website and WebApp verification services are performed remotely. For non-intrusive verification, all the customer needs to provide is a URL to verify the website or WebApp. Web verification service can be performed either on production sites, for sites in staging areas or during DevOps cycles.
- **Periodic Service with Selectable Frequency:** WhiteHaX services are offered as a yearly subscription with selectable frequency such as monthly, quarterly or other frequency as appropriate. It can be pre-scheduled or on-demand (with a reasonable notice period), allowing the flexibility of security verification to be aligned with the need of the business or with DevOps and other development/update cycles.
- **Various Levels:** WhiteHaX Web verification services are offered at various level from a) non-intrusive scan only which helps identify exploitable vulnerabilities and attack surfaces, b) non-intrusive scan with recommendations on how to fix or eliminate found security issues, to c) intrusive scan and attack verification where some attacks are performed on the site or app to verify how deep a security exploit can get.

WhiteHaX Web verification services thus provide a thorough verification of Website and App security. WhiteHaX then delivers a full report of findings with potential severity of each of problems found and where appropriate, provide recommendations on how to fix them. This helps eliminate known exploits, vulnerabilities and other attack-surfaces from the Websites and WebApps. For further information, visit www.WhiteHaX.com/WebServices or contact WebServices@WhiteHaX.com to request datasheet, quote and/or statement-of-work (SoW).