RAPID7 DATA SHEET

Attack Types in InsightAppSec and AppSpider

Rapid7's research and product teams keep up with the latest application security attacks and best practices, so you don't have to. With InsightAppSec and AppSpider, you can go way beyond the OWASP Top Ten to test for over 95 attack types and best practices; you can also create custom checks to address issues and risks that are custom to your environment.

- Anonymous Access
- Apache Struts 2 Framework Checks
- Apache Struts Detection
- Arbitrary File Upload
- ASP.Net Misconfiguration
- ASP.NET Serialization
- ASP.NET ViewState security (ViewState Check)
- Autocomplete attribute/ check
- Blind SQL Injection
- Browser Cache directive (leaking sensitive information)
- Browser Cache directive (web application performance)
- Brute Force (HTTP Auth)
- Brute Force Form based Authentication
- Business Logic Abuse
- Clients Cross-Domain Policy Files
- Collecting Sensitive Personal Information (Personal Sensitive Information)
- Command Injection
- Cookie attributes
- Credentials Over Insecure Channel
- Credentials stored in clear text in a cookie (Password Exposure).
- Cross Origin Resources Sharing (CORS)
- Cross-Site Request Forgery (CSRF)
- Cross-site scripting (XSS), (DOM based Reflected via AJAX Request)
- Cross-site scripting (XSS), (DOM based)
- Cross-site tracing (XST – Web Method)
- CSP Headers
- Custom Directory Module
- Custom Parameter Module
- Custom Passive Module
- Directory Indexing
- Email Disclosure
- Expression Language Injection
- File Inclusion
- Forced Browsing
- Form Session Strength
- FrontPage Checks
- Heartbleed Check
- HTTP Authentication over insecure channel
- HTTP Headers
- HTTP Query Session Check
- HTTP Response Splitting
- HTTP Strict Transport Security (HSTS)
- HTTP User-Agent Check
- HTTP Verb Tampering (Request Method Tampering)
- HTTPS Downgrade
- HTTPS Everywhere
- Information Disclosure in comments
- Information Disclosure in Response
- Information Disclosure in scripts (Script Check)
- Information Leakage In Response
- Java Grinder
- JavaScript Memory Leaks
- LDAP Injection
- Local Storage Usage
- Nginx NULL code
- OS Commanding
- Out of Band Cross-site scripting (XSS)
- Out of Band Stored Cross-site scripting (XSS)
- Parameter Fuzzing
- Persistent Cross-site scripting (XSS) (passive – XSS Persistent)
- Persistent Cross-site scripting (XSS), (active - XSS PersistentActive)
- PHP Code Execution
- Predictable Resource Location (Resource Finder)
- Privacy Disclosure
- Privilege Escalation
- Profanity
- Reflected Cross Site Scripting (XSS,Reflected)
- Reflected Cross Site Scripting Simple (XSS,Simple)
- Reflection
- Reverse Clickjacking
- Reverse Proxy
- Secure and non-secure content mix
- Sensitive Data Exposure
- Sensitive data over an insecure channel
- Server Configuration
- Server Side Include (SSI) Injection
- Server Side Template Injection
- Session Fixation
- Session Strength
- Session Upgrade
- Source Code Disclosure
- SQL Information Leakage (SQL Errors)
- SQL Injection
- SQL injection Auth Bypass
- SQL Parameter Check
- SSL Strength
- Subdomain discovery
- Unvalidated Redirect
- URL rewriting
- Web Beacon
- Web Service Parameter Fuzzing
- X-Content-Type-Options
- X-Frame-Options
- XML External Entity Attack
- XPath Injection
- X-Powered-By
- X-XSS-Protection

Learn more at www.rapid7.com/InsightAppSec.

091418