edgescan™

PROFESSIONAL DATASHEET

When to use Professional:

- Authenticated Testing
- Web Application Testing
- Network Layer Testing
- Manual validation for all results
- Recommended Assessment for less critical authenticated applications
- Recommended for use on permanent applications with authentication enabled

What you also get:

- Includes all edgescan Essentials features but also includes authenicated testing to simulate a “logged in” attacker
- Expert Support - Support and access to analysts
- False positive free vulnerability intelligence
- On-demand, continous or scheduled assessments
- On-demand retests
- Reliable on-demand metrics & KPIs
- Massively scalable
- Very cost effective
- Flexible Reporting
- Production Safe
- 100,000+ Full-Stack vulnerability tests
- 56,000 + CVE checks

Vulnerability Scanning

OWASP Top 10 (2013,2017) Vulnerabilities	HTTP Caching Control	OS Command injection
Application framework with known vulnerabilities	HTTP Header Injection	Persistent session cookie
Autocomplete attribute	HTTP only session cookie	Remote file inclusion (RFI)
Buffer overflow	HTTP response smuggling	SANS Top 25 Software Errors
Content spoofing / HTML hacking	HTTP response splitting / pollution	Server-side Injection
Cookie access control	Improper input handling	SQL Injection: error based, Union-based
Cross site scripting (XSS) - Reflected	Improper Encoding or Escape of Output	Unsecured session cookie
Cross site scripting (XSS) - Stored	Integer Overflows	XML injection and schema security
Cross site scripting (XSS) - DOM	Improper file system access control	URL redirect security
Data / Information leakage	Insufficient SSL / TLS protection	XML attributes security, XML external
Directory Indexing	LDAP Injection	XPath Injection
File path traversal	-	SQL Injection: Boolean-based, Time-based