

APPLICATION SECURITY TESTING (AST) INTELLIGENCE

The global application security testing industry is changing. Applications and application programming interfaces are critical to every facet of our private and corporate daily lives. To meet this changing paradigm, Edgescan offers continuous **Dynamic Application Security Testing (DAST)** integrated with deep dive, business logic **penetration testing** through our Edgescan advanced license. This combination of production-safe, automated and manual testing on one platform, allow enterprises to tackle the ever-increasing demand for accurate and useful Application Security Testing (AST) intelligence. Details of our DAST and Business Logic Penetration Testing services below.

EDGECAN ESSENTIALS/STANDARD / (DAST)

	APPLICATION ASSESSMENT	
All OWASP Top 10 (2013, 2017) vulnerabilities	HTTP caching control	OS command injection
Application framework - known vulnerabilities (spring / struts / zend / django / .net, etc.)	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, time based, Boolean conditional, MySQL, MSSQL, Oracle, etc.
Cross site scripting (XSS) – reflected / stored	Improper output encoding / content type encoding	Unsecured session cookie
Data / information leakage	Improper file system access control	URL redirect security
Directory indexing	Insufficient SSL / TLS / transport layer protection	XML attribute security, XML external entities
DOM XSS	Integer overflows	XML injection and schema security
File path traversal	LDAP injection	XPath injection

EDGESCAN VULNERABILITY INTELLIGENCE

ADDITIONAL SECURITY INTELLIGENCE

Alerting on all notable events SMS & email (this is programmable and can be raised against any event)	Enumeration of internet facing hosts by address and hostname.	<i>Host-tagging</i> to add greater clarity to reports and vulnerability display. Tag IPs with customised IDs to help with asset identification.
Document OS and software versions on all systems managed by Edgescan.	Continuous IP Monitoring: An asset register of all hosting systems and associated live services across all servers managed by Edgescan.	Identify unnecessary and insecure services and ports which are live on your systems.
Auto Web Application Firewall (WAF) Rule Generation. Edgescan will generate WAF rule scripts to virtually patch against application vulnerabilities.	Edgescan vulnerability intelligence integrates with other security and business systems through it's open API.	Role based access for segregation of asset data and separation of critical remediation intelligence.

EDGESCAN ADVANCED (PENETRATION TESTING)

In addition to the Edgescan Standard (DAST) testing (above), penetration testing attempts to discover issues which scanners generally don't detect. The discovery of such issues is unique to Penetration Testing or using an Edgescan Advanced license as the issues are contextual and require human intelligence to discover and exploit.

DEEP DIVE PENETRATION TESTING

Anti-automation assessment	Credential / ID / session prediction.	Session fixation / expiration weakness
Brute force	Horizontal authorisation weakness (peer-to-peer)	Weak password recovery
Business logic weakness / functional abuse / state logic weakness	Insecure indexing / direct object access	



IRL: +353 (0) 1 6815330
 UK: +44 (0) 203 769 0963
 US: +1 646 630 8832

Sales and general enquiries:
sales@edgescan.com

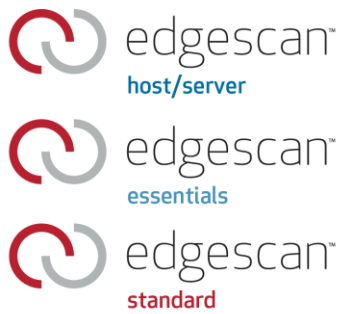
View our latest

**2020 VULNERABILITY
 STATISTICS REPORT**

at edgescan.com

EDGESCAN

TRADITIONAL
VULNERABILITY
SCANNING



AUTOMATED

HYBRID

MANUAL

VULNERABILITY SCAN

MANUAL VERIFICATION

PENETRATION TEST

ABOUT EDGESCAN

Edgescan is a vulnerability management service (SaaS) which continuously identifies cybersecurity vulnerabilities across the full stack.

Edgescan provides continuous system visibility and provides support to understand, priorities and mitigate cyber security risks on a continuous basis.

Edgescan significantly reduces the cost of ownership while increasing cybersecurity resilience and interoperability significantly.

- Technical & logical security assessment
- Multiple scanning engines
- Expert manual verification & risk rating
- Trending / metrics / reporting
- Continuous security visibility & intelligence
- Fullstack security (network & application layer)



IRL: +353 (0) 1 6815330
UK: +44 (0) 203 769 0963
US: +1 646 630 8832

Sales and general enquiries:
sales@edgescan.com

View our latest

**2020 VULNERABILITY
STATISTICS REPORT**

at edgescan.com