SERVICE DEFINITION DOCUMENT
WEB APPLICATION PENETRATION TESTING

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

About JUMPSEC

JUMPSEC is a UK-based cyber security consultancy, established in 2012, with a proven track record in offensive testing, incident response, managed detection, and advisory services for both public and private sector organisations. Our work is led by skilled professionals with extensive experience in red teaming, security engineering, and incident response, ensuring that our services are rooted in real-world knowledge and practical expertise.

We place a premium on assurance. Our teams include CHECK and CREST-qualified penetration testers, as well as NCSC CIR-approved incident responders and NCSC CIE-accredited Incident Managers, enabling us to deliver a wide range of government-level security engagements. We have deep experience deploying and managing Microsoft security technologies such as Microsoft Defender and Sentinel, particularly within regulated environments. Our approaches and documentation are consistent with recognised standards including the NIST Cyber Security Framework, CIS Controls and CAF, and our reporting is clear and purposeful, catering to both technical specialists and executive decision-makers.

Clients use JUMPSEC to achieve three outcomes:

- to reduce the risk of significant security incidents
- to speed up the detection and containment of threats, and
- to demonstrate robust governance to stakeholders such as boards, auditors, and insurers

Our services are transparent and collaborative—clients are given clear scopes, well-defined engagement terms, daily updates during testing, and strong evidence to support their security posture. We prioritise remediation advice based on business impact, not just automated scan results.

Protecting client data is at the heart of our operations. JUMPSEC acts as a data processor under UK GDPR and DPA, adheres to principle-of-least-privilege access, and only retains evidence for periods agreed with clients. Where necessary, our personnel hold BPSS or SC clearance, and we can provide reports and artefacts in accessible formats to meet WCAG 2.1 AA standards.

Our public sector experience covers central and local government, healthcare, education, and critical national infrastructure. In the private sector, we support clients in finance, manufacturing, logistics, and technology. We often deliver projects alongside complementary services, such as red and purple teaming, detection engineering, and incident response retainers, to drive measurable improvements and tangible returns.

We continually refine our services to address the evolving needs of our clients, frequently developing tailored solutions to unique challenges. Our approach is adaptable and shaped by each client's specific situation, so the best way to understand how we can help is to discuss your needs directly with us before RFP release.

This overview outlines JUMPSEC's broad capabilities and demonstrates how our expertise can be applied to deliver practical, threat-focused security for your organisation. To find out more about how we can address your cyber security requirements, please get in touch for a straightforward conversation.

Example use cases

Local authority — Citizen portal access control

We scheduled a test that specifically targeted account boundaries in a housing and benefits portal. JUMPSEC assessors demonstrated IDOR and identified weak role checks, which exposed citizen records. We focused our actions on enforcing object-level authorisation, applying stricter input handling, and setting testable acceptance criteria. On re-testing, JUMPSEC confirmed we successfully blocked enumeration and correctly scoped data restricted by roles.

Central government — Case management and FOI portal

JUMPSEC modelled civil servant, contractor, and citizen roles during the assessment. We surfaced broken access control in draft case notes, identified verbose errors, and discovered insecure redirects after sign-in. As a result, JUMPSEC hardened session handling, enforced stricter role policies, and implemented secure redirects. We verified that our actions correctly isolated roles and produced cleaner audit trails for disclosure reviews.

Charity — Donations and volunteer management platform

We reviewed donor and volunteer workflows and found mass assignment vulnerabilities on profile updates, weak rate-limiting on password resets, and JWT validation gaps. JUMPSEC prioritised schema allow-listing, centralised token checks, and implemented per-endpoint throttling. In follow-up testing, we confirmed that authorisation remained stable and observed reduced abuse of sensitive fields.

University — Research repository and supervision tools

We assessed file services and supervisor dashboards, where JUMPSEC identified issues such as broken access control, path traversal through upload handlers, and inadequate audit trails. We introduced strict authorisation, implemented safe file handling, and ensured that all actions were traceable. During re-testing, JUMPSEC confirmed that research artefacts were properly isolated and upload workflows proved resilient.

Service Overview

JUMPSEC conduct manual-first testing to identify exploitable design and implementation weaknesses in web applications. Assessment covers authentication, authorisation, input handling, session integrity, and business logic. Findings are reproducible and prioritised, with practical guidance suitable for engineering backlogs and governance packs.

Objectives

- Identify and validate exploitable security weaknesses with evidenced impact
- Provide reproducible proof, clear remediation steps, and secure design patterns
- Reduce recurrence by addressing root causes in controls and workflows
- Support governance with risk-based prioritisation and traceable outcomes

Approach

Testing reflects data sensitivity, user roles, integration scope, and regulatory context. Activities run in safe environments and approved windows using non-destructive techniques. Representative accounts and datasets are used to demonstrate impact without affecting production.

Method

- **Plan —** confirm objectives, scope, data classes, environments, and windows
- **Test —** assess authn/authz, input validation, session management, and logic flows
- **Validate —** demonstrate impact using controlled data and reproducible steps
- **Debrief —** classify severity, document fixes, and outline secure patterns
- **Improve —** optional re-test to confirm remediation and prevent regression

Deliverables

- Executive summary highlighting key risks and priorities
- Technical report with evidence (requests/responses, screenshots, payloads) - OWASP ASVS and OWASP Top 10 for coverage and taxonomy, CWE/CVSS for classification and severity assignment. Secure development patterns referenced for prevention
- Issue register (CSV/XLSX) with severity, owners, and due dates
- Optional re-testing and letter confirming remediation status

Outcomes and benefits

- Lower application risk across common and logic-based weaknesses
- Backlog-ready remediation tasks with clear acceptance criteria
- Improved build quality through secure patterns and guardrails
- Governance artefacts suitable for audit and assurance reviews

Pricing model

Fixed price per application/scope or time-and-materials aligned to SFIA. Price drivers include auth complexity, integration count, environment availability, required artefacts, and optional re-testing.

Timelines

- Planning and access: 3–5 working days
- Execution: per agreed scope and complexity
- Report issue: 5–10 working days after evidence freeze
- Optional re-test: typically 30–60 days post-remediation

Security and assurance

Practitioner-led delivery using peer-reviewed methods and internal QA. Evidence is reproducible and traceable. Reports and artefacts are available in accessible formats

Team and roles

- **Engagement Lead.** Scope, governance, quality management, and stakeholder alignment.
- **Application Security Tester(s).** Testing and evidence capture.
- **Coordinator.** Logistics, participant comms, evidence handling, and action tracking.

Buyer responsibilities

- Provide environments, test accounts/roles, and representative data
- Supply documentation, integration details, and change window approvals
- Arrange third-party consents where integrations or suppliers are in scope

JUMPSEC responsibilities

- Operate within rules of engagement and change control
- Use non-destructive techniques and agreed abort criteria
- Secure handling and time-boxed retention of data and artefacts

Data protection and privacy

The buyer is data controller; JUMPSEC acts as processor. Only minimum necessary evidence is collected and retained. Secure transfer, strict access control, and agreed retention periods apply. Artefacts are returned or securely destroyed on completion.

Constraints and assumptions

- No denial-of-service or production data modification
- Third-party participation requires prior written approval
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- API Penetration Testing
- Secure SDLC / DevSecOps Assessment
- Source Code Review

Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

0333 939 8080

hello@jumpsec.com

www.jumpsec.com