Institute of Business Administration Karachi
Leadership and Ideas for Tomorrow

Scope of Work

RFQ–4245–12931–Vulnerability Assessment & Penetration Testing

Network Infrastructure, Servers, Databases, Web Applications and Mobile Application

1. Introduction and Objectives

The objectives of the engagement are to:

- Identify exploitable vulnerabilities in the in-scope network infrastructure, servers, applications, mobile application and databases before attackers can exploit them.
- Evaluate security configurations, access controls, patch levels and the effectiveness of firewall and Web Application Firewall (WAF) protections.
- Assess vulnerabilities from external (internet) and internal (IBA network) perspectives using black-box and grey-box approaches, as agreed with IBA ICT.
- Rate findings by severity and business impact, recommend practical remediation, and verify closure through revalidation.

2. Technical Scope

2.1 Network Components, Core Switches and Routers

- Identify vulnerabilities across in-scope routers, core switches and associated network management interfaces; conduct controlled penetration testing for exploitable weaknesses.
- Review configuration hardening against applicable Service Provider and recognized security benchmarks; assess outdated firmware, unnecessary services and insecure management protocols.
- Review administrative access, authentication, authorization, remote management exposure, management-plane segmentation and logging.
- Assess router access controls and configuration weaknesses and evaluate resilience against common network attacks using non-disruptive methods.

2.2 Network Firewalls

- Review firewall security posture, rules, security zones, NAT and access-control policies for excessive permissions and unauthorized access paths.
- Identify unnecessary open ports, exposed management services, weak administrator access and insecure protocols.
- Evaluate IPS/detection and blocking policies, security logging, alerting and visibility using safe validation techniques.

- Review policy effectiveness against common network attacks without conducting disruptive traffic or denial-of-service tests.

2.3 Web Application Firewall (WAF)

- Assess security configuration and protection policies of the physical WAF device.
- Safely validate protection against common web attacks, including SQL injection and cross-site scripting (XSS).
- Confirm that public-facing applications pass through the WAF from both external and internal access paths, and test for unauthorized direct access to backend servers bypassing the WAF.
- Review reverse-proxy configuration, SSL/TLS, security logging, alerting, attack-blocking controls and access policy effectiveness.
- Coordinate all production WAF tests with IBA ICT; disruptive testing requires prior written approval.

2.4 Physical Servers and Server VMs

- Assess operating-system and application patch levels, unsupported versions, security hardening and unnecessary or exposed services on all listed physical servers and VMs.
- Review administrative access, authentication, privileges, remote-management exposure, network segmentation and relevant security event logging.
- Evaluate risks to hosting infrastructure and the security configuration of web servers, including SSL/TLS, security headers and exposed directories where applicable.

2.5 Web Applications and Hosting Web Servers

- Assess the web applications listed for vulnerabilities, from external and internal perspectives.
- Test authentication, authorization and session management, including role-based access across student, faculty, staff, applicant, alumni and administrator accounts.
- Assess the applications against the OWASP Top 10:2025 and the OWASP Web Security Testing Guide (WSTG).
- Test APIs used by the applications against the OWASP API Security Top 10.
- Test business logic specific to each application (e.g. admission form submission, fee and payment flows, HR records access).
- Test file upload, report and document download functions for unauthorized access and malicious file handling.
- Verify that each application is protected by the Fortinet WAF on internal and external access paths, and test for direct access to backend servers that bypasses the WAF.
- Test the hosting web server configuration, including SSL/TLS settings, security headers and directory exposure.
- Identify PHP versions and assess the October 2026 PHP remote code execution vulnerabilities CVE-2026-109618 and CVE-2026-109619 ("PHP2Shell"), where applicable. Fixed releases are PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35; earlier branches must be patched by backport or upgraded.

- Verify PHP security patch levels, unsupported versions, exposed configuration (e.g. phpinfo, display_errors) and vulnerable third-party extensions, frameworks and dependencies.
- For Windows-based servers, verify applicable updates for the October 2026 Brotli decoder vulnerability CVE-2026-111497 ("HTTP2Shell"), covering PHP, curl, Node.js, .NET and any other components that bundle Brotli 1.0.3 to 1.2.0.

2.6 Mobile Application (IBA Alumni App)

- Assess the application against the OWASP Mobile Top 10 and the OWASP Mobile Application Security Verification Standard (MASVS), using the OWASP Mobile Application Security Testing Guide (MASTG).
- Perform static analysis of the application package for hard-coded secrets, API keys, insecure configuration and vulnerable libraries.
- Perform dynamic analysis covering local data storage, certificate validation, transport security and session handling.
- Test the backend APIs used by the app for authentication, authorization (including access to other users' records) and input validation.
- Review privacy aspects, including requested permissions and personal data sent to third-party services.

2.7 Database Security

- Review database access controls, privileges, default and shared accounts, and password policies for the in-scope database instances.
- Review database security configuration and patch levels against Service Provider and CIS benchmarks.
- Review network exposure of database listeners and confirm databases are reachable only from authorized application hosts.
- Assess the application-to-database connection, including stored credentials, least-privilege application accounts and exposure to SQL injection.
- Review database auditing, backup protection and encryption of data in transit and at rest.

3. Documentation and Reporting

- Provide an executive summary suitable for non-technical stakeholders and a detailed technical report covering each affected asset, vulnerability, impact, evidence and recommended remediation.
- Classify each finding by severity using CVSS v3.1 or v4.0 and describe the relevant business impact.
- Provide non-sensitive proof of successful penetration where applicable, including screenshots and representative requests/responses.
- Deliver a separate revalidation report after remediation showing fixed, partially fixed and outstanding findings.
- Securely delete IBA data, credentials and evidence held by the Service Provider after final report acceptance and confirm deletion in writing.

4. Rules of Engagement

- Agree testing windows and blackout periods with IBA ICT prior to kickoff, avoiding admission, registration and examination periods.
- Define safe testing limits and excluded/restricted systems before execution. Denial-of-service, load testing and other disruptive attacks are excluded unless specifically approved in writing.
- Coordinate production WAF, firewall, network and critical server testing with IBA ICT; stop and escalate if service instability is detected.
- Use only IBA-authorized accounts and testing source IP addresses disclosed in advance; do not access, alter or exfiltrate real student, staff or alumni data beyond the minimum proof required.

5. Legal and Compliance Considerations

- Comply with applicable laws and regulations, including the Prevention of Electronic Crimes Act (PECA) 2016.
- Obtain written authorization from IBA and all necessary permissions from relevant teams before testing. The final target list and rules of engagement must be formally approved before testing begins.
- Sign an NDA covering access to configurations, credentials, network diagrams, findings and other sensitive information.

6. Communication and Escalation

- Appoint named points of contact from IBA ICT and the Service Provider, with agreed progress and findings communication channels.
- Define incident response and emergency escalation contacts for unforeseen events or service disruption.
- Notify IBA ICT of critical vulnerabilities within 24 hours of discovery, without waiting for the final report.

7. Post-Testing Support

- Provide clarification and reasonable assistance to IBA ICT teams implementing remediation.
- Include two revalidation cycles after remediation at no additional cost, with separate written results for each cycle.

8. Bill of Quantity

#	Applications / Services	Qty
1	Routers	2
2	Core switches	2
3	Network firewalls	2

#	Applications / Services	Qty
4	Web Application Firewall (WAF) (physical device)	1
5	Physical hardware / servers	6
6	Server VMs	10
7	Web Applications / Portals	5
8	Mobile Application (IBA Alumni App, incl. backend APIs)	1
9	Database Instances	6
10	Revalidation after remediation	2 cycles

Service Providers shall quote per line item, specify the total effort in person-days, identify testing tools and methodology, and provide a proposed timeline from kickoff to final report. Final asset inventory and test windows shall be approved by IBA ICT before commencement.