REQUEST FOR QUOTATION

for

Vulnerability Assessment & Penetration Testing of Online Alumni Election System

Contents

1 About IBA:

The IBA Karachi today sets a standard that other institutions emulate and serves as a beacon of hope and success for students across the nation. The Institute has gone through major changes over past six decades to embrace a wider set of disciplines in its curricula. During the 10 years, the institute has witnessed massive developments in all areas ranging from IT infrastructure, Technology Enhancement, ERP Implementation, E-Learning Solutions & Digitalization, Accreditations, introducing new Programs, Increasing Research activities and organizing National & International Conferences; thus, changing IBA' s physical and academic landscape.

2 Purpose:

The purpose of this assignment is to hire a competent firm that specializes in conducting penetration testing, vulnerability assessment & Stress Testing of Online Alumni Election System. The selected firm is to conduct the Audit to discover any vulnerabilities / weaknesses / attacks in the website(s), web application(s) & Databases. The Audit should be done by using Industry Standards and as per the Open Web Application Security Project (OWASP) methodology. The main objectives for conducting this Web Application, website security audit, System Stress/load Testing and Vulnerability Assessment / Penetration Testing is to:

A. Identify the security vulnerabilities, which may be discovered in the Web application & Database security audit including cross-site scripting, Broken ACLs/Weak session management, Buffer Overflows, Forceful browsing, CGI-BIN manipulation, Form / hidden field manipulation, Command injection, Insecure use of cryptography, Cookie posing, SQL injection, Server miss-configuration, Well-known platform vulnerabilities, Errors triggering sensitive information leak etc. On the Web Application / database.
B. Requirements and analysis performed to increase overall security posture.
C. Identification and prioritization of various risks to the application & Database.
D. Gain a better understanding of potential website its applications and vulnerabilities.
E. Determine the system on code level & DB structure level that if the current Online Alumni Election system of IBA are secure and evaluate the security.
F. Identify remedial solutions and recommendations for making the Online Alumni Election System secure.
G. Rectify / fix identified potential vulnerabilities, and web application & database vulnerabilities thereby enhancing the overall security and stress testing.

H. Submission of data on Online Alumni Election System to its destination, information needs to be protected from unauthorized access or use.

Scope of Audit:

- Mysql Database Security testing
- PHP based Web Application Security testing of Dynamic Applications
- Vulnerability Assessment of identified IBA servers (both Physical & Virtual Machine)
- Penetration Test of identified IBA servers (both Physical & Virtual Machine)
- Stress Testing of Application & Server level.
- Closure verifications of the findings from the tests, maximum 3 iterations

3 Scope of Work (SOW):

The bidders are requested to conduct Stress Testing, Vulnerability Assessment and Penetration Testing (VAPT) to determine security weaknesses, system loads and vulnerabilities in IBA's servers, applications, and databases.

The auditors will have to carry out an assessment of the vulnerabilities, threat and risks that exist in PHP & MYSQL based web application through private/public network Vulnerability Assessment and Penetration Testing. This will include identifying remedial solutions and recommendations for implementation of the same to mitigate all identifying remedial solutions and recommendations for implementation of the same to mitigate all identified risks, with the objective of enhancing the security of the web applications & databases. The bidder will also be expected to propose a risk mitigation strategy as well as give specific recommendations to tackle the residual risks emerging out of identified vulnerabilities assessment. The Web application should be audited as per the Industry Standards and also as per the OWASP (Open Web Application Security Project) model. The auditor is expected to submit the final audit report after the remedies / recommendations are implemented. The final report will certify the web application as "Certified for Security". All the website security audit reports should contain the details as mentioned at the Audit report.

Total number of IPs/domains to be tested will be up-to Two (Production & DR). The details of IPs will be shared after the award of contract.

The bidder should have proven track record in Information Security domain and have extensive experience of VAPT testing for both, public and private sector organizations.

The scope of the proposed audit tasks is given below. The audit firm / company will be required to prepare the checklist / reports & provide remediation of Vulnerabilities & stress testing.

Task 1: Web Application/Security Audit / Assessment / Database Security

The various check / attacks / Vulnerabilities should cover the following or any type of attacks, which are vulnerable to the web application / Database.

- Vulnerabilities to SQL Injections.
- CRLF injections
- Directory Traversal
- Authentication hacking / attacks
- Password strength on authentication pages
- Scan Java Script for security vulnerabilities
- File inclusion attacks
- Exploitable hacking vulnerable
- Web server information security
- Cross site scripting
- PHP remote script vulnerability
- HTTP Injection
- Phishing a website
- Buffer Overflows, Invalid inputs, insecure storage etc.
- Other any attacks, which are vulnerability to the web applications & Database.

The Top 10 Web application vulnerabilities, which are given below, should also checked from the given websites:

A1 – Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attacks to execute script in the victim's browser which can hijacks user sessions, deface web sites, possibly introduce worms, etc.

A2 – Injection Flaws	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
A3 – Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework, which accepts filename or file from users.
A4 – Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
A5 – Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged- on victim's browser to send a pre authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be powerful as the web application that it attacks.
A6 – Information Leakage and Improper Error Handling	Application can unintentionally leak information about their configuration, internal working, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data or conduct more serious attack.
A7 – Broken Authentication	Account credentials and session tokens are often not protected. Attackers compromise passwords, keys or authentication tokens to assume other users' identities.
A8 – Insecure Cryptographic Storage	Web application rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
A9 – Insecure Communication	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communication.
A10 – Failure to Restrict URL Access	Frequently an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

Task 2: RE-Audit based on the recommendation Report from Task 1

The vendor will be responsible to provide a detailed recommendations report for the vulnerabilities observed from Task 1

Task 3: Re, Re-Audit, if required based on the recommendations Report from Task 2

If vulnerabilities are observed from the re-audit, the vendor has to provide a detailed recommendations report on the vulnerabilities observed or found from Re-audit / Task2. IBA expects that all vulnerabilities will be removed at the Task 3 stage. The audit firm / company must submit a summary compliance report at end of each task and the final report should certify that the website/ web applications/ database (should mention the name of website and/or web application) is "certified for security."

4 Project Deliverables:

The selected firm will be required to submit detailed reports to the IBA Karachi that will categorize each of the bugs/observations based on High, Medium and Low Severity. Provided reports will also recommend mitigating action plan to address the identified issues. All types of reports will provide detailed information on Information security risks, vulnerabilities, and the necessary countermeasures and recommended corrective actions.

5 Project Duration:

The total duration for the completion of this Project will be 10 days from the date issuance of Work Order.

6 Shortlisting Criteria:

In evaluating the relative merits of firms bidding for the project, the evaluation committee will take consideration on below given points:

i. Demonstrated experience in carrying out similar projects, as outlined above.
ii. Must have completed at least 5 projects related to Vulnerability Assessment & Penetration Testing (VAPT) and System Stress/load Testing.
iii. The quality, intelligence, efficiency, sustainability and viability/feasibility of the proposed approach and methodology to be applied for this assignment shall be evaluated by the procuring agency, hence consulting firms are required to prepare a comprehensive document. (Attach all relevant documents)

iv. The quality and relevant experience of individual staff members proposed by the firm including the leadership quality for accomplishment of this assignment shall be minutely examined while shortlisting the consultant by IBA Karachi.

v. The selected firm must have certified professionals who have relevant certifications such as Certified Information System Security Professional (CISSP), Certified Ethical Hacker (C|EH) and Certified Information Systems Auditor (CISA).

vi. The consulting firm must be registered with tax department. (Attach relevant Documents)

vii. The consulting firm must provide names of at least 3 clients along with their contact details for whom the company has completed similar projects.

viii. Please mention the Association / Affiliation/ Partnership/ Certification with relevant bodies / entities like SECP, PSEB, P@SHA, relevant standards of ISO / TQM /CMMI (level), IEEE etc. (Relative grading for shortlisting will be carried out so please mention all kind of association / affiliations/ certifications that the consulting firm may have along with documentary evidence)

7 Confidentiality:

The selected firm would ensure that all the data/Information collected under this project is kept confidential and will be the sole and exclusive property of IBA Karachi. The consulting firm will not, acquire any right, title or interest in or to any of the confidential information collected for this consultancy.