OWASP RFP CRITERIA v 1.1

Project Sponsored by : **ProactiveRisk.**

Table of Contents.

1.0 Introduction

The purpose of this project is to simply provide an objective list of important set of questions companies should utilize when they issue a **Request For Proposal for Web Application Security Projects**.

A **Request For Proposal**, (RFP) is a call made by an organization soliciting for bids by service providers or vendors to meet a need and it is often done by documents.

The information provided in RFPs are important and when you create an RFP for an Application Security Verification project , emphasis should be on providing clear information about the scope of verification activities and evaluation criteria so prospective service providers and vendors can submit proposals that are comparable.

You also need to provide adequate background information about the company soliciting for bids and other relevant information that can ensure that the project life cycle is successful. Also it is important that prospective service providers or vendors provide detailed information that helps the client to make an informed decision on who is the best fit for the project.

Usually this information may include standard questions such as proposed Application Security Verification methodologies for defined tasks, relevant project experience etc. Others may include Security Coverage, Risk Evaluation Process , Reporting Techniques etc.

We outline in subsequent sections detailed information that should be provided for each application that is subject to verification in an Application Security Verification project.

2.0. Recommended Information the Client should provide to Service Providers/Vendors.

2.1 Lines of code. Lines of Code (LOC) or sometimes referred to as Source Lines of Code (SLOC) is a prerequisite for any verification task that involves the review of source code. This software metric (LOC) provides information about the scale of the program under review. There are software packages on the public domain such as LocMetrics on *http://locmetrics.com* or CLOC on *http://cloc.sourceforge.net/* which can be used to count the number of lines of code. Additional information about LOC such as if the count included commented source code or not is also beneficial

2.2 Number of dynamic pages. Information about the number of dynamic pages is advisable as it provides insights about the scale of the application under assessment. It is important for verification efforts that involved manual penetration testing. When estimating the amount of dynamic pages, pay attention to pages with unique functionality or purpose. If you have urls like:

i. /display_results.php?rs=1 ,

ii. /display_results.php?rs=2 ,

iii./display_results.php?rs=3 ,

You need to ensure that you confirm if they refer to a single unique dynamic page or not.

2.3 An Inventory of user roles and role descriptions. The catalog of user roles is endorsed for all verification efforts as it furnishes business context for vulnerabilities (if any) established.

2.4 Brief Application Summary and Application Architecture. This is mission critical for applications with non-standard architectures such as those using thick clients, web services or integration with legacy systems but not so paramount for applications with a

standard web application architecture (web server, application server, database server setup).

2.5 Degree of verification expected. To manage or prevent suppliers providing erratic bids that vary in figures or timelines, there is a need to provide definitive guidance on the level of verification desired. This should include requirements for or on:

a. Dynamic vulnerability scanning.

b. Manual code review.

c. Manual penetration testing.

d. Static analysis.

e. Security architecture review.

f. Malicious code analysis.

g. Threat modeling.

2.6 The frequency or duration for performing verification. It is important to indicate if you want a single verification exercise or if you want several many verification exercises executed within a specified time-frame.

3.0. Recommended RFP Questions.

3.1 Company Background.

a. Summarize the product(s) or service(s) provided by your company.

b. How long has your company been providing products or services relevant to this project? Please provide any relevant information about major milestones such as significant acquisitions, mergers or the introduction or elimination of relevant lines of business.

c. Please provide succinct information your past experience with applications of a similar scope, complexity, and vertical as the applications to be verified in this project.

d. Outline your familiarity and experience with the frameworks, libraries, languages and other relevant technologies that comprise the applications to be verified.

e. Are you involved with organizations or stakeholders in the application security community, such as the **Open Web Application Security Project (OWASP) and the Web Application Security Consortium (WASC)?** if yes , what roles do you play ?

f. Provide other helpful background information about your organization and your qualification to supply the required product/service.

3.2 Application Security Verification Methodology.

a. Outline , in clear details your proposed methodology for all the verification techniques to be utilized:

i. Dynamic vulnerability scanning.

ii. Malicious code analysis.

iii. Manual code review.

iv. Manual penetration testing.

v. Security architecture review.

vi. Static analysis.

vii. Threat modeling.

b. What would you require from the client to prepare for and successfully execute an application verification exercise?

c. Would you be using multiple techniques for this project ? If yes how will you combine these in the verification exercise?

d. Describe your proposed level of communication/ interaction with software development teams , security experts, and business process owners during the verification process.

3.3 Security Coverage.

a. Explain the vulnerability and security control coverage that is provided by your verification efforts. Where relevant, supply references to the **OWASP ASVS,WASC 24 Broad Classes of Attacks,** and the **OWASP Top 10.**

b. Provide the different levels of efforts that you will provider for the verification effort. What are the differences in security coverage between these levels?

c. Presently, are you able to test (precisely) for Cross-Site Request Forgery (CSRF) and HTTP Response Splitting?

d. What are potential gaps in coverage for the current proposal and what steps would you take to mitigate the gaps?

e. Does your solution meet current PCI 6.6 standards?

3.4 Application Coverage.

a. How effectively does your product/service baseline an application?

b. How do you adjust your product/service to verify an application most effectively?

c. What methods or techniques do you use to ensure coverage of the entire application?

d. How do you corroborate with a customer that you are providing accurate coverage of the targeted application?

e. What potential gaps (if any) exists between your proposed solution and the platform and architecture of the application under verification? A case in point - if the target application

contains both web pages and web services and your testing does not cover web services this would indicate a gap.

3.5 Risk Evaluation.

a. Outline your risk evaluation process for establishing the probable vulnerabilities you might discover and it's business impact.

b. What is your procedure for managing the reporting of false positives?

c. Outline your procedures for categorizing similar risks for easy absorption and rectification.

3.6 Differentiators.

a. What aspect of the verification process do you find most challenging (if any)?

b. Tell us why your approach towards this project is exceptional or singular. How and why is this important to the client?

3.7 Scope.

a. What are the time estimates for implement your product/service in a similar verification exercise?

b. How does the proposed solution scale for multiple websites?

c. What are the advised steps for curtailing the impact of testing on the performance of applications during the testing process?

d. Indicate if your product or service provisions for on-demand / ad hoc testing.

e. What is the lead time required to initiate testing?

3.8 Security.

a. What are your procedures for protecting client's information made available to you? Outline in detail your network security, information storage security, and need-to-know policy.

b. Describe the level of confidence you have in staff that would have access to our information in this project.

c. Outline the techniques and policies for information exchange between you (the vendor) and us (the client) during this exercise.

d. Describe your procedure for deleting and purging information from your systems at the completion of this project.

e. How would you compartmentalize our information from the risk information belonging to your other clients?

f. Outline (with tangible evidence) that your systems and network is protected from attacks.

3. 9 Burden.

a. Outline any resource (human) requirements from our organization. This should include technical/operational skill sets and experience.

b. Specify in details the requirements you require from us to execute the verification exercise.

3.10 Reporting Interface.

a. Outline your risk documentation structure. This should include:

i. The Title.

ii. The Location (URL and/or line of code).

iii. Specific vulnerability description.

iv. Risk likelihood, business impact, and severity.

v. Code snippets.

vi. Specific remediation recommendations.

b. Explain the risk model you utilize. How can it be customized to meet your client's standards and expectations?

c. Explain your reporting interface employing criteria such as the learning curve, how reporting components are structured, etc.

d. How do you or your product or services deliver (important) updates on new identified web application risks?

e. What trend and historical reports do you provide that monitor identified/open/closed risks and the ongoing remediation exercise?

f. Is it possible to generate status reports to show the risk status of separate web applications, and the overall security health of all web applications?

g. Are these reports customizable for different stakeholders i.e. management.

h. Do you have any standard scripts or standard integration that are bundled with your solution? If yes indicate the applications.

i. Do your reports provide specific directions for application developers, attuned to the exact problem in the code?

j. What is your process for timely and reliable reporting of risks for stakeholders?

k. How often is your reporting interface updated? What process do you follow for this updates?

l. What benchmark exists for developers to know if they have successfully re-mediated a risk?

3.11 Innovation.

a. Are there any recent innovations or products your firm has delivered that has resulted in improved service delivery for clients?

b. What is your process for identifying new categories of vulnerabilities and test for this?

c. What is your process of identifying new attack techniques that can be used to exploit known vulnerabilities?

d. What is your process for testing new technologies (e.g. new versions of Flash) for vulnerabilities?

3.12 Integration.

a. What are the standard data formats your product/service produce or export?

b. What other relevant technologies (for example, Firewall Applications) does your product/service integrate with?

c. How will the integration work and what benefits will they bring?

3.13 Benefits.

a. How can you increase the efficiency of the remediation process?

b. In your opinion, what is the balance of internal and external resources in an ideal application security program?

c. Can you provide precise results and diminish/eliminate false positives ?

d. Can provide a proof of concept for a positive Return on Investment (ROI) and an increase in benefits to management?

e. Do you have the capacity to influence secure coding techniques / reduce time spent debugging? If yes , How?

f. Outline the technical and business advantage we would gain from working with you in this project.

3.14 Supporting Services.

a. Explain any knowledge transfer process or procedure i.e training , platforms etc you will provide with the verification effort.

b. What remediation support do you provide to software development teams?

3.15 Client Support Details.

a. Outline your client or customer support framework . What are the of support levels you provide and what are the escalation procedures?

b. Do provide a ticket raising and tracking system ? How are your open tickets tracked and closed?

c. What Service Level Agreement(SLA) do you offer ?

3.16 Pricing/Licensing Information.

a. What terms or conditions are linked to the product or service ?Do you have a sample Software License Agreement we can review ?

b. Describe clearly your proposed pricing model.

c. Outline clearly other cost implications which are attached to this bid and requires our attention.

d. Do you provide pro-bono training or consulting services or attach costs to them? If yes what are the charges attached to them?