# OWASP RFQ Project V1

Project Sponsored by: ProactiveRISK

## SUGGESTED INFORMATION TO PROVIDE[edit]

To receive proposals that are comparable it is important to provide clear information to proposing parties about the scope of verification activities.

Information to provide for each application to be subject to verification:

1. Lines of code (Required for verification efforts where source code review will be involved; recommended in all cases in order provide background information about the scale of the application being assessed. Freely-available software such as CLOC http://cloc.sourceforge.net/ can be used to calculate the number of lines of code. It is also helpful to provide further information about how the lines of code count was determined – for example a raw count of the lines of code or a count of non-comment source statements)

2. Number of dynamic pages (Some form of this is required for verification efforts where manual penetration testing will be involved. It is recommended in all cases in order to provide background information about the scale of the application being assessed. In calculating the number of dynamic pages, it is important to focus on the number of pages with unique functionality. For example, the URLs /show_product.jsp?id=1 and /show_product.jsp?id=2 likely refer to only one unique dynamic page)

3. List of user roles with role descriptions (Recommended for all verification efforts in order to provide business context for any vulnerabilities identified)

4. Brief description of the application and its architecture. This is less important for applications with a basic web application architecture (web server, application server, database server...) but more important for applications with non-standard architectures such as those using thick clients, web services or integration with legacy systems.

5. Level of verification desired (Failing to provide guidance on the level of verification desired can result in suppliers providing inconsistent proposals that vary wildly in price):

a) dynamic vulnerability scanning

b) static analysis

c) manual penetration testing

d) manual code review

e) threat modeling

f) security architecture review

g) malicious code analysis

6. Frequency or duration during which verifications should be performed. Do you want a single verification or would you like multiple verifications to be performed over a period of time?

# SUGGESTED RFP QUESTIONS[edit]

## Company Background[edit]

1. Provide a brief overview of products and/or services offered.

2. How many years has your company been in business? Please list any major milestones such as significant acquisitions or the introduction or elimination of relevant lines of business.

3. Describe your experience with applications of a similar size, scope, complexity, and vertical as the applications to be verified.

4. Describe your experience with the languages, frameworks, libraries, and other technologies that comprise the applications to be verified.

5. Describe your level of involvement in the application security community, in organizations such as the Open Web Application Security Project (OWASP) and the Web Application Security Consortium (WASC).

6. Describe any other relevant background information about your organization and your qualification to provide the request product/service.

## Application Security Verification Methodology[edit]

1. Describe your methodology for all the verification techniques to be used:

a) dynamic vulnerability scanning

b) static analysis

c) manual penetration testing

d) manual code review

e) threat modeling

f) security architecture review

g) malicious code analysis

2. Describe the steps required from our organization in order to prepare for and execute an application verification.

3. If multiple techniques are used, how will they be used together in the verification effort?

4. Provide your thoughts on why performing this security verification is important to our organization.

5. Describe your desired interaction with software developers, security staff, and business owners during the verification process.

## Security Coverage[edit]

1. Describe the vulnerability and security control coverage provided by your verification efforts. Where possible include references to the OWASP ASVS,WASC 24 Broad Classes of Attacks, and the OWASP Top 10

2. Describe the different levels of rigor that you offer for the verification effort. What are the differences in security coverage between these levels?

3. Are you currently able to test for Cross-Site Request Forgery (CSRF) and HTTP Response Splitting?

4. Provide guidance on the level of coverage included in your proposal. What are potential gaps in coverage for the current proposal and what steps could be taken to address them?

5. Does your solution meet PCI 6.6 standards?

## Application Coverage[edit]

1. How does your product/service baseline an application?

2. How do you tune your product/service to verify an application most effectively?

3. What methods do you use to ensure coverage of the entire application?

4. How do you verify with a customer that you are providing thorough coverage of the targeted application?

5. What potential gaps are there between your proposed solution and the platform and architecture of the application being verified? (For example if the target application contains both web pages and web services and your testing does not cover web services this would indicate a gap)

## Risk Evaluation[edit]

1. Describe your process for determining the specific likelihood and business impact of vulnerabilities you discover.

2. How do you limit the reporting of false positives?

3. Describe your approach for combining similar risks so that they can be easily understood and remediated.

## Differentiators[edit]

1. What is the most challenging aspect of your verification efforts?

2. What about your approach is unique and why is that important to us?

## Scope[edit]

1. Approximately how long does it take to implement your product/service?

2. Specifically, how does your solution scale for multiple websites?

3. What performance impact should testing have on applications being tested? What steps are taken to minimize the impact of testing on the performance of applications during the testing process?

4. Does your product or service allow for on-demand / ad hoc testing? What is the lead time required to initiate testing?

## Security[edit]

1. Describe exactly how you will protect our information, including all information about our application and any risks discovered, while it is in your custody. Please describe your network security, information storage security, and need-to-know processes.

2. Please provide information on the trustworthiness of individuals who will have access to our information as part of the verification.

3. Please describe how information necessary for the verification will be exchanged securely.

4. Please describe how our information will be purged from your systems when the verification is complete.

5. Please describe how our information is kept separate from the risk information of other customers.

6. Please provide evidence that your systems are protected against attack.

## Burden[edit]

1. Describe any personnel requirements from our organization. How many personnel are needed? What are their skill sets and experience levels?

2. Describe exactly what materials we will be expected to provide to support the verification efforts.

## Reporting Interface[edit]

1. Describe exactly how risks will be written up, including:

a) title

b) location (URL and/or line of code)

c) specific vulnerability description

d) risk likelihood, business impact, and severity

e) code snippets

f) specific remediation recommendations

2. Describe the risk model you use as well as how it can be customized for our corporate standard.

3. Describe your reporting interface using criteria such as ease of use, clarity, comprehensiveness, how reporting components are organized, etc.

4. How does your product or service provide timely updates on any new web application risks identified? Are alerts delivered to authorized personnel? If so, how are they delivered and under what conditions?

5. Do you provide historical trending reports that track open/closed risks and the ongoing remediation process?

6. Can assessment reports be generated to reflect the risk status of individual web applications, as well as the security health of all web applications?

7. Can your reports be tailored and adapted for viewing by various levels of management, internal/external auditors, security specialists, etc.?

8. Does your solution provide an API so that risks can be exported into other applications, such as CRM apps, bug tracking systems, SIEMs? Are there any canned scripts or standard integrations that exist? With which applications?

9. Do your reports contain specific recommendations for application developers, tailored for the exact problem in the code?

10. How do you provide timely and reliable reporting of risks for ongoing visibility, measurement, and management?

11. How frequently do you provide enhancements to your reporting interface? What is the process?

12. How do developers know if they have successfully remediated a risk?

## Innovation[edit]

1. Describe any recent innovations your company has introduced to lower costs or improve service for your customers.

2. How do you identify new classes of vulnerabilities and test for them?

3. How are you able to uncover and test for new attack techniques that can be used to exploit known classes of risks?

4. How do you test new technologies (e.g. new versions of Flash) for risks?

## Integration[edit]

1. What standard data formats will your product/service export or provide?

2. What other technologies (for example, Web Application Firewalls) does your product/service integrate with? What benefits do these integrations provide? How do the integrations work?

## Benefits[edit]

1. How do you make the remediation process more efficient?

2. Describe the balance of internal and external resources in an ideal application security program.

3. Can you deliver accurate results and diminish/eliminate false positives, thus making the verification process more efficient?

4. Are you able to demonstrate a positive ROI and increased benefits to management? How?

5. Are you able to influence secure coding techniques / reduce time spent debugging? How?

6. Explain why we would realize a competitive advantage by doing business with your company?

## Supporting Services[edit]

1. Describe any training or eLearning options available associated with the verification effort.

2. Do you offer remediation support to software development groups?

3. Is strategic consulting support available to support our application security program.

## Customer Support[edit]

1. Can you describe the process in place whereby customers interact with your internal service and support? What are the escalation procedures?

2. Do you provide tracking of all trouble tickets that have been opened and are they tracked through resolution?

3. Do you offer any kind of Service Level Agreement?

## Pricing/Licensing Options[edit]

1. Explain your pricing model.

2. What are the terms associated with your product or service? Please include a sample Software License Agreement or Master Services Agreement template.

3. Are there other costs we should be made aware of? If consulting or training costs are involved, how do you charge for these services?