Open Web Application Security Project
June 2008 - Revised

Proposal for

OWASP People Certification Project

DRAFT

For Discussion Purposes

James McGovern

I. Overview

Governments, companies, and educational institutions are doomed to deal with endless streams of software vulnerabilities unless programmers learn to write much more secure code. Part of the charter of OWASP is to assist in making application security visible which requires at its core, dedicated individuals who are savage in the pursuit of excellence.

Several initiatives are underway to improve secure software development skills and knowledge. Oracle, Microsoft, and a few other software companies are conducting short courses for their developers. Consulting firms such as Accenture and Cognizant are investing heavily in teaching secure coding practices to not just security professionals, but all their staff at large. Dozens of universities in the United States, Canada, China, Trinidad and Brazil are creating elective courses on secure software development. Yet, even if all of those initiatives are successful, they are unlikely to affect even two percent of the existing millions of developers already in the work force or those who will be entering the work force over the next five years.

The need for certification in this space is immense. The lack of accountability or at least a way to tell qualified security professionals from those that aren't is difficult. We understand that for traditional software development, applications better compile or they don't go live, developers don't get their bonus and some may even see their employment terminated. In security, there is generally no bar to clear.

Enterprises are under duress in order to translate the requirements of PCI, SoX, HIPAA and other guidance to their daily practice, yet find that those charged sometimes aren't fit for duty. In order to close the gap, they invest significant funding in education and certification. At the highest levels, this is a noble goal; however there is almost always a coupling of certification to courseware where candidates only learn enough to pass a test. For enterprises that don't invest in their employees but do believe in hiring talent on demand, they seek the ability to have a single certification that their recruiting staff can use to filter the great from the masses and the OWASP People Certification Project is the answer to all these concerns and more...

II. Project Goals

The project has six goals:

- Allow employers to rate their developers and architects on security skills so they can be confident that every project has at least one "security master" and all of their developers and architects understand the common errors and how to avoid them.
- Provide a means for buyers of software and systems vendors to measure the secure programming skills of the people who work for the supplier.
- Allow developers and architects to identify their gaps in secure programming knowledge in the language they use and target education to fill those gaps.
- Allow employers to evaluate job candidates and potential consultants on their secure design & development skills and knowledge.

- Provide incentive for universities to include secure software design & development in required computer science, engineering, and programming courses.
- Provide reporting to allow individuals and organizations to compare their skills against others in their industry, with similar education or experience or in similar regions around the world.

III. Requirements

- **Cost**: Certification should be affordable and be cheaper to obtain than others on the market. The proposed certification will be achievable in one exam. The exam will retail for $150.
- **Revenue**: Unlike many of the other OWASP projects, this project will be revenue generating. Proceeds will be 100% allocated to helping local OWASP chapters in their marketing efforts ranging from advertising in local technology publications to providing OWASP branded door prizes.
- **Difficulty**: The security community at large holds OWASP to a higher standard than other security organizations and therefore the exam offered must be more stringent. It is anticipated that the target failure rate for first-time exam takers will hover in the range of 60% to 50%.
- **Characteristics**: When compared to the CISSP, OWASP exam will go much deeper into application security but will remain both software vendor and language agnostic.
- **Timeframes**: This project should have a public certification exam ready by Q4 2008
- **Governance**: The characteristics of how the certification adapts to market conditions over time will be governed by a team of four individuals who are nominated by chapter leaders. The requirements for participation are that the nominated individual should have prior certifications issued by entities such as Microsoft, Cisco, Sun, Oracle, IASA or other bodies. Additionally, we shall have a diversity requirement where one member must be from a Fortune enterprise, one from a government entity, one from a consulting firm and one from a software product vendor.
- **Frequency**: It is anticipated that a volunteer team will create five new questions for each category every six months.

IV. Revenue Sources

The OWASP People Certification Project anticipates deriving revenue in multiple ways:

- **Test Exam Preparation**: Approx 1/2 of all candidates who pursue certification tend to use exam preparation software from firms such as Boson, Transcender and others. It would be this projects intent to establish a relationship with Express Certifications (www.expresscertifications.com) who currently provides the equivalent functionality for the CISSP exam. Typically, an exam preparation vendor would charge a fee of 50% of the actual exam fees. In our scenario, a candidate could take a practice exam for around $75 where in a revenue sharing arrangement would result in approx $30 being remitted to OWASP.

- **Prometric Exams**: There is a guaranteed revenue commitment when entering into a relationship with Prometric of $70K a year (This can be lowered for the first year do to our non-profit status) where Prometric receives $60 to $70 an exam and remits the remainder to OWASP once the revenue target has been fulfilled. If OWASP is wildly successful and has 3,000 people take the exam in the first year, this would result in revenues to OWASP of approx $185,000. if OWASP only achieves a more practical level of 1,000 administered exams, the number would still generate revenue of approx $10K.

- **Logo Apparel**: Candidates will have the opportunity upon passing exam to purchase logo apparel. We will enter into a revenue sharing agreement with same vendor that provides this capability to Microsoft for its MCP program.

V. Exam Categories

Listed below are the anticipated categories for questions that would appear on the exam:

- OWASP Top Ten and 2007 - 10 Questions

- Code Review - 10 Questions

- Logging - 15 Questions. Candidates should be familiar with NIST standards, syslog, event viewer and concepts implemented in frameworks such as Log4J.

- Software Design - 20 Questions - Familiarity with various design patterns, security patterns, modeling security in UML, etc

- Network Security - 20 Questions - While the focus of OWASP is on higher layers of the OSI stack, it is vital that a security professional have understanding of all layers in terms of cause and effect. This exam will ask questions such as what port does ping work over?

- SOA and XML - 20 Questions - Person should be knowledgeable in designing secure WSDL, schemas, etc. Will include stuff that Gunnar Peterson and the iSec Partners guys teaches in their courses

- Cryptography - 20 Questions - Will cover algorithms and when/how to use. Shall also talk about IBE, encrypting XML, key escrow, etc

- Terminology - 20 Questions - Having an understanding of security vocabulary such as pharming, phishing, etc is important. May include stuff related to CWE

- Security Architecture - 20 Questions - Authentication, Authorization, Session Management, etc
- Testing - 20 Questions - Fundamentals of penetration testing, use of Scarab, looking for defaults, de-identifying data, etc
- Lifecycle - 10 Questions - Stuff about SDLC and may cover McGraw, SDL, CLASP, etc
- Logic - 10 Questions - No exam should be strictly question and answer. The exam will present a scenario where the candidate has to choose from multiple solutions.
- Information Security Policies 5 Questions - Governing software creation is important as well. Will talk about characteristics, awareness, compensating controls, legislation such as SoX, HIPAA, PCI, etc

VI. Exam Scoring

Since we are pursuing only one exam with a high level of difficulty, the score will determine multiple levels of certification. Below are the target thresholds for three classification levels.

- **90% or Greater**: Master
- **80% or Greater**: Professional
- **70% or Greater**: Associate

Using this approach has the benefit of keeping test administration fees lower and can actually encourage test candidates to get more familiar with subject areas even when they have achieved passing scores. Additionally, for those who achieve a score of 99% or better, an additional benefit should be free admission to any and all OWASP Conferences for one full year.

The exam will be comprised of between 85 to 95 questions randomly chosen at test time (actual question as well as number of questions) and should take about two hours to complete. Those who pass the test will receive an OWASP branded shirt.

VII. Volunteer Task Assignments

Listed below are the tasks that will be assigned to volunteers.

- **Test Question Creation**: We anticipate needing six to ten volunteers for a period of three months for initial exam creation while stepping back to two or three over the next couple of years.
- **Public Relations**: Announcing the creation of a new exam requires diligence in terms of marketing. We will be seeking an individual knowledgeable in public relations to work with bloggers and industry magazines to help get the word out. Additionally, this individual will work with large software vendors such as Sun, IBM, Oracle, Cisco, HP, EMC to provide additional endorsement. Finally, this individual

will also work with consulting firms such as Accenture, Wipro, BearingPoint, Cognizant and others on a campaign related to each of them getting 100 people certified.

- **Branding**: We will be seeking one individual knowledgeable in branding to help us provide a name for our certification, to create a unique logo and to design branded door prizes.

- **Evangelism**: The word that a new certification is out needs to be championed by someone well-known and respected within the industry. We will need one spokesperson whose role is to encourage others to consider pursuit of this exam. This individual will be the personality behind the certification.

VIII. Demographic Information

Many exams miss out on the opportunity to learn more about their membership and their own backgrounds and interest. The certification exam provides an opportunity to collect meaningful demographic information while also respecting privacy. The exam will minimally collect the following information:

- **Country / Region**: This information is useful in order to provide a fair-share allocation model for door prizes

- **Employer category**: The ability to ascertain whether an exam taker is employed by a government entity, large enterprise, non-profit, consulting firm, student, software vendor, etc will further help us tune the marketing message.

- **Prior certifications**: Knowing whether membership also contains MCSE, CCNP, CISSP or other industry certification will allow us to explore cross-marketing potential.

IX. Contact Information

James McGovern, Enterprise Architect, The Hartford
Hartford CT OWASP Chapter Lead
Email: james.mcgovern@thehartford.com

X. June 2008 Addendum

Below are responses from the community at large and their reactions to the initial proposal along with additional perspectives that address them.

Should exams be proctored?

There are tradeoffs in using an approach such as Prometric over proctored exams. Proctored exams are typically required if you want to attract people from the Federal Government but this comes at the expense of the difficulty in proctoring exams on a worldwide basis. Proctoring is a popular model used by CISSP and other security certifications and if done in alignment with ISO standards could result in higher perception of quality. Proctoring by its very nature, does however make it less convenient for test takers to schedule exams at will and tend to increase exam costs.

Will exams help OWASP increase brand?

At some level, OWASP understands that it is the premier brand in the IT security world. It is reasonable to conclude that partnerships with other organizations may increase visibility but this may come at the expense of reduced credibility. Certification is probably one of the best ways for OWASP to increase visibility to software development professionals that want to understand software security.

Should exams be pass/fail or graded on a curve?

Everyone has their own rationale as to which method is preferred. Reality says that this argument usually arises for security professionals that are on the line of becoming truly competent in software security. The original proposal broke with tradition as practiced by other exams and believes that a curve is a predictor of one's ability and that displaying one's proficiency in terms of levels is the best indicator to not only test takers but those who desire to hire these professionals.

Could you explain more about how the exams will be governed?

There will be several "teams" each with a core set of responsibilities. The first and most important team are those who create exam questions which will primarily be accomplished by a set of volunteers. The second team is responsible for statistical analysis, vetting and quality control of all exam questions. This team may or may not be paid depending on the ability of OWASP to find and recruit individuals with this background. The third team will have administration responsibilities such as coordination of exam dates and locations, candidate tracking and basic public relations responsibilities. We envision this role to be a shared responsibility of paid OWASP employees.

How much funding will you seek from OWASP?

This answer primarily depends on several factors of which the most important is whether exams are proctored or not. If exams are not proctored then funding is minimal and only requires startup funding as contained in original proposal. If proctoring is required, the

funding we seek would come to about $70K for the first year to cover expenses associated with assembling a team to create exams aligned with ISO standards and to hire a part-time exam proctor along with associated travel costs.

There will be some hesitancy for the first candidates to take an exam, since no one has said how difficult it will be via word-of-mouth. How will you overcome this perspective?

We have several ideas on how this is best accomplished. We believe that the first test takers should be nominated to take the test for free (sponsored by OWASP) and chosen based on criteria such as their current level of participation in OWASP, their tenure in the information security profession and whether they have taken certification exams in the past. In order to limit the budget, we propose the following limits:

- OWASP Certification Project Leader (James McGovern) - 20 Nominations
- Each member of the OWASP Board - 10 Nominations
- Each member of the test certification question creation team - 5 Nominations
- Each OWASP Chapter Leader - 2 Nominations

It is anticipated that there will be significant overlap in nominations along with acknowledgement that all nominees may not actually take the exam and therefore the total count of first test takers should not exceed 100.

How can you ensure the security of the exam questions while maintaining OWASP's goal of being open?

There are several perspectives on how to answer this question. Security in terms of whether exam questions are exposed is of primary importance if you are pursuing ISO certification. If this is the case, then following the ISO practices will lead to the right answer. If ISO certification is deemed unimportant, then one has to simply acknowledge that security becomes less of a challenge based on the breadth of information covered which is easily solved based on the law of large numbers. It is easier to remember 50 things than it is to remember 5,000 things.

In terms of how the questions will be created, the current thinking says that each question creation sub-team will have their own electronic working group that will use basic access control. Using simple technologies that can watch for the appearance of questions via Google is also something that can be deployed.

What are the synergies between conferences and certifications?

It is a well-known fact that conference attendance is increased whenever certification exams are offered in conjunction with and at a discount. If OWASP chooses proctored exams, nominates top security professionals who attend and manages to get the Federal Government to participate, it will create a win for both certification and conferences.