Competition Details

IFSEC

This newly launched annual competition aims to find **the next generation security innovations**. We aim to challenge the brightest minds in security technology **from around the world** to submit radically new ideas and game-changing technologies. The competition aims to uncover the creative capabilities of innovators in **universities** and **small to medium sized enterprises** that apply to security needs.

This competition brings together the world's most promising technological innovations at IFSEC 2011 who will compete against each other in a live judging session. This is a unique opportunity for the chosen entrepreneurs to find capital, industry partners and government customers.

Submitting entry

Your entry has now entered the judging process.

	Questions	Your Answers
mandatory	Question 1 Name:	Question 1 Answer **Colin Watson on behalf of the Open Web Application Security Project (OWASP)**
mandatory	Question 2 Email:	Question 2 Answer **colin.watson@owasp.org**
mandatory	Question 3 Country:	Question 3 Answer **Worldwide (established as a not-for-profit charitable organization in the United States on 21 April 2004, and formally recognized as a 501(c)(3) not-for-profit charitable organization on 10 December 2004)**
	Question 4 Name of Idea/Company:	Question 4 Answer **OWASP AppSensor**
	Question 5 Address:	Question 5 Answer **OWASP Foundation, 9175 Guilford Road Suite #300, Columbia, MD 21046**

What Can I Do?

Question 6 Phone Number:	Question 6 Answer
Question 7 Web address:	Question 7 Answer **http://www.owasp.org/index.php /OWASP_AppSensor_Project**
Question 8 The Year your company/idea was founded (if applicable):	Question 8 Answer **The OWASP Foundation came online on December 1st 2001 it was established as a not-for-profit charitable organization in the United States on April 21, 2004. The AppSensor project was conceived in 2008.**
Question 9 Technology Category: the technology can best be described as fitting into which category?	Question 9 Answer **Intruder Alarms , Integrated Security IP Network Solutions**
mandatory Question 10 Summary of your Innovation Give us a short description of your idea or product. Name three or more reasons why your product is innovative and superior (technically or otherwise).	Question 10 Answer **AppSensor defines a conceptual framework, methodology and example code to implement intrusion detection and automated response into applications. It is used to detect and prevent attacks by criminals, terrorists and others against applications, their data and their users. It identifies and defends against malicious users such as criminals and hackers. There are no other products, or concepts, elsewhere that provide the breadth and depth of application-layer intrusion detection. Responding to attacks does not require later, or offline analysis, since it is undertaken in real time. Some example use cases are:** ***Detecting and preventing an attempt at fraud via an attack on a smart grid electricity meter.** *** Defending a website from hacktivists attempting to find a SQL injection vulnerability.** *** Detecting suspicious behavior by a user in their online banking application, to identify if their computer is compromised with malware.** *** Prevention of attempts by commercial spies to gain unauthorised access to corporate or governmental knowledge from online systems.** *** Detection of attempted modification to electronic data being collected by a physical security device (e.g. CCTV camera, alarm system).** **Since AppSensor has full information on user sessions and the desired business logic of the application, it has a very**

low false positive attack detection rate, and can detect attacks that network firewalls, traditional network/host intrusion detection systems and even generic web applications firewalls cannot detect.

mandatory

Question 11 Benefits to Customer

Name three or more quantitative statements discussing why this idea/product benefits your customer. Tell us who your target market is and what security problem your innovation solves?

Question 11 Answer

*** AppSensor detects attacks in real time that would otherwise go undetected.**
*** AppSensor results in very few false positives because it is instrumented where it has context of the application.**
*** AppSensor responds instantly to attacks, which allows it to stop attacks in progress.**
*** AppSensor reduces operational application risk.**
*** The concepts are free to use or modify, so all progress will directly benefit the \\\"customers\\\".**

The users of AppSensor are groups which build and operate software applications - these are in both private and public sector organisations, including those in the \\\'third sector\\\'. Currently operators of applications rarely know whether their applications are under attack, and conventional security protection systems often provide no protection to application-layer attacks. This is increasingly important for products using digital transmission and control, e.g. other security products running application software. Applications might include embedded systems, SCADA devices, websites, web services and mobile phone applications. Users of AppSensor benefit from visibility into probes and attacks against their applications, and are able to automatically respond to attacks in real time.

mandatory

Question 12 IP Status

Do you own all the necessary IPs? Have you applied for or have been granted a patent? If not, why not?

Question 12 Answer

The copyright holder is the OWASP Foundation. The AppSensor concept and documentation are available under a Creative Commons Attribution-ShareAlike 3.0 License http://creativecommons.org/licenses/by-sa/3.0/ (see http://creativecommons.org/licenses/by-sa/3.0/legalcode for the full license). AppSensor code is published by OWASP under the BSD license. No patent has, or will be applied for, since OWASP\\\'s mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all materials are available under a free and open software license. Therefore, OWASP encourages free use, modification and redistribution under the terms of the license.

mandatory

Question 13 Technology

Describe how the technology works, what the system’s components are and how the product interfaces externally. Explain how your solution could be integrated into a

Question 13 Answer

The AppSensor Project defines an application layer intrusion detection system. AppSensor is embedded inside the application code and uses detection points to identify suspicious and malicious behavior. AppSensor analyses and responds to security events in real time, with responses such as logging a user out, locking their account, disabling part of the application, or changing the way the application works (e.g. by adding delays, or alternative checks).

The power of AppSensor is that it:

larger system or further developed to enhance its value to the targeted customer community. We do not want to know your 'secret sauce' but require enough information for the judges to understand what you are doing and to evaluate its merits and to differentiate you from others in the field.

*** Understands the application context.**
*** Integrates fully with user properties/session.**
*** Knows whether the application is under attack.**
*** Responds to attackers in real time, such as logging them out or locking their account.**
*** Has an extremely low rate of false positives for attack detection.**

The project comprises of a conceptual framework, and guidance for planning and developers:

*** AppSensor, https://www.owasp.org/images/2/2f/OWASP_AppSensor_Beta_1.1.pdf**
*** AppSensor Detection Points, http://www.owasp.org/index.php/AppSensor_DetectionPoints**
*** AppSensor Response Actions, http://www.owasp.org/index.php/AppSensor_ResponseActions**
*** AppSensor Implementation Planning Workbook, http://www.owasp.org/index.php/File:Appsensor-planning.zip**
*** AppSensor Developer Guide, http://www.owasp.org/index.php/AppSensor_Developer_Guide**

The project is programming language, framework and operating system agnostic. The concepts can be implemented in any application, but demonstration code has been written which builds on the ESAPI (OWASP Enterprise Security API) coding framework. This is currently only available in Java. The example code, or the concepts, can easily be built into software in any organisation, and in any language. There is no single way to use AppSensor - it depends upon each organization\\\'s culture:

*** Development practices.**
*** Architectural design patterns.**
*** Use of code libraries and frameworks.**

There are no restrictions, other than defined in the answer to question 12. The objective is to provide value to the software development community, and thus their organizations.

mandatory

Question 14 How does this innovation change the World tomorrow?

Describe why do you think your technology is disruptive for the security industry?

Question 14 Answer

Traditional defensive measure for applications have to guess about the user\\\'s intent and what is acceptable usage. Network firewalls let both malicious and non-malicious traffic through to web applications (e.g. all HTTP traffic to a web site or web application). Network and host intrusion detection and prevention systems are like forensic systems which are trying to look for unusual activity, and often this relates to evidence from a deeper, packet and system level. Even generic web application firewalls have no inherent knowledge about the application\\\'s logic, valid entry points or the roles & permissions of various users. Application-layer intrusion detection and prevention is hardly being used anywhere.

AppSensor combines building security in to development practices with dynamic, real-time detection and response capabilities. The traditional information security world sees these as separate product categories.

As an analogy, consider a high street branch of a retail bank. Why can we catch bank robbers, but not hackers? There are many different controls in the bank - physical ones like thick walls, man traps, a barrier in front of the tellers and a hardened safe inside an inner office, electronic surveillance such as an intruder alarm system, CCTV and panic buttons, human monitoring such as by a guard as well as vigilant staff, and more specific controls such as access control, multi-factor authentication and transaction verification. Internal systems are probably linked to the local police department. If the bank were a web application, it would usually have insufficient external controls, unnecessary partner trust, no real-time analysis, ineffective monitoring, limited security training of operators, single factor authentication, alternative administrative access, and no response capability. Would you bank there? See pages 12 and 13 of this presentation for a visual representation of this analogy: http://www.owasp.org/images /0/06/Defend_Yourself-Integrating_Real_Time_Defenses_into_Online_Applications-Michael_Coates.pdf

This may appear a simple and obvious solution. But it is hardly adopted anywhere. AppSensor exists to help organizations get over the initial hurdle so they can benefit from application-layer intrusion detection and prevention.

Two unique innovations are:

*** AppSensor operates in real time making informed decisions about mis-use.**
*** AppSensor has an extremely low false positive attack detection rate.**

This means that actual attacks can be identified with a very high degree of certainty, and they can be stopped before they have the chance to exploit unknown vulnerabilities. It is a proactive approach that reduces risk.

The pilot work has demonstrated AppSensor can also defend against application worms, like the MySpace Worm (also known as the \\\"Samy worm\\\"). The behavioral monitoring aspects of AppSensor can detect the rate change in a function\\\'s usage (e.g. add a friend), disable the feature dynamically, prevent the spread of the worm, and allow the application to remain otherwise operational while clean-up is undertaken and the vulnerability is corrected or patched. A new online demo has been created at http://michael-coates.blogspot.com/2011/02/live-demo-of-attack-aware-application.html

mandatory

Question 15 Market

Where do you fall within your market? How are you different than other players? Describe the size of the market, its growth potential, demand opportunity and

Question 15 Answer

[NB The OWASP Foundation does not endorse or recommend commercial products or services]

The ideas and concepts in AppSensor exist to a limited extent in some web application firewall products (e.g. Imperva, ModSecurity, Trustwave Breach) although these do not integrate with the code, and do not intelligently detect and defend against attacks. There are also a small number of run-time analysers (e.g. Fortify), but they do not

customer preferences. (Successful applications have described competitors and substitutes, how you position your company/technology in the industry and your relationship with suppliers.)

have the full coverage of AppSensor\\\'s capabilities and are language-dependent. Often intrusion detection and prevention systems are turned off or run in detection-mode only due to the problem of false positives, which AppSensor does not suffer from. The general approach can be included in an ad-hoc manner in some software (e.g. locking an account after multiple failed authentication attempts, raising security events when input validation failures occur). These features are often implemented as discrete processes and some, like the investigation of logs, may be undertaken reactively to incidents or performed largely in a manual way. AppSensor centralizes and formalizes the approach.

OWASP is unique in that it makes all its resources freely available. Therefore the outputs of this work would be available to all software architects, designers and developers. Thus the deliverables identified can be taken by anyone, and applied at any scale of project. Usually the target applications and aspects would be selected based on an assessment of risk. This would be different for each organization and application.

Recent reports by analysts have indicated there is a positive return on investment for building security into software development processes in a formal manner:

*** Security and the Software Development Lifecycle: Secure at the Source, Aberdeen Group**
http://www.aberdeen.com/Aberdeen-Library/6983/RA-software-development-lifecycle.aspx
*** State of Application Security - Immature Practices Fuel Inefficiencies, But Positive ROI Is Attainable, Forrester Research**
http://www.microsoft.com/downloads /en/details.aspx?FamilyID=813810f9-2a8e-4cbf-bd8f-1b0aca7af61d&displaylang=en

We believe this will encourage the uptake of defensive/detective combination technologies like AppSensor in enterprises. The cost of implementation will relate to the planning and execution of the AppSensor concepts, which are free of charge themselves.

mandatory

Question 16 Business Plan

Explain how you intend to reach your market. Be as specific as you can about your strategy in terms of pricing, promotion, selling and distribution.

Question 16 Answer

Our target market (the \\\"customers\\\") are systems architects, designs and development managers. These people have the most influence on software development practices, and without their support, the AppSensor concepts are unlikely to be adopted. We intend to promote the deliverables (defined in the answer to Question 17) at developer-orientated conferences and other events, in the development and security press, and online using blogs and discussion forums.

The outputs are open source and free to the world. If the money invested is in our project, it can benefit everyone, not just big companies willing to buy an expensive commercial product. The investment\\\'s benefits would be multiplied many-fold by the adopters, improving application security, reducing risk, and contributing to stable economies.

mandatory

Question 17 How would you spend the winning prize of $10,000?

How will winning this competition affect the development of your innovation or technology?

Question 17 Answer

Much of the original work was funded with $5,000 from OWASP\\\'s Summer of Code 2008: http://www.owasp.org /index.php/OWASP_Summer_of_Code_2008 (see also the assessment process http://www.owasp.org/index.php /OWASP_AppSensor_Project_-_Assessment_Frame). This culminated in the production of a beta-quality project book. Further voluntary work has been undertaken by a number of project contributors, including the development of an operational prototype written in Java. However, we want to support the completion of the following release-quality deliverables:

*** Update and extend the AppSensor book, to make implementation of AppSensor easier.**
*** Programming to extend ESAPI (Java) demonstration code, so it is possible to plug AppSensor directly into a web application using this framework.**
*** Programming to create ESAPI (PHP) demonstration code since PHP is used so widely due to ease of development and deployment, and can easily contain many vulnerabilities.**
*** Update/create developer guides for each of the above to ensure they are readily understandable, as quickly as possible, by developers.**
*** Write an ESAPI Swingset AppSensor tutorial (Java), to enable those learning ESAPI to learn about AppSensor as they train.**
*** Create and deliver new presentation materials for both technical and business-orientated audiences.**
*** Define a short business case justification guide.**

OWASP would oversee the selection, appointment and assessment of the people who undertake work on the deliverables. OWASP\\\'s assessment criteria will be used:

http://www.owasp.org/index.php/Assessment_Criteria_v2.0

Without this funding, effort will continue to be made by the volunteers, but the GSS award would allow the desired deliverables to be fast-tracked, by making grants to people who work on the deliverables. This is not market-rate employee or contractor rates; but more in line with the way other OWASP grants are provided, as a motivation.

mandatory

Question 18 What do you expect from the mentorship?

How do you intend to get benefit from the offered mentorship? What can it mean practically for your innovations,future?

Question 18 Answer

We would like mentorship to provide a strategic overview to what we are doing — ensuring we are focused on our target market, and that we create deliverables which can be understood, incorporated easily and therefore widely adopted. We would also want mentorship to assist networking opportunities with industry and government to promote the concept. We would especially request help in meetings with software framework/library teams (e.g. ASP.NET) who create very important parts of software infrastructure. This will be a vital part of encouraging adoption, and thus improving the defensive measures in applications.