Submission #74
==========
Please enter the full title of the initiative you would like to enter.
Cornucopia

Please choose the category which best fits your initiative
Making the internet a safer place

What is the URL of your site?
https://www.owasp.org/index.php/OWASP_Cornucopia

Logo
owasp_logo.eps (http://nia.nominet.org.uk/sites/default/files/webform/owasp_logo.eps)

==========
Question 1: Outline the initiative that you are entering into the Nominet Internet Awards.

Cornucopia is a card game for website developers which helps them derive software security requirements. The game's goal is to identify relevant threats and thus mitigations, but players are motivated by the desire to win (for each threat identified and each hand won). But at the same time they are learning about application security and helping to create a safer and more secure website or web application.

The card deck has five suits named after software security principles (data validation & encoding, authentication, session management, authorisation and cryptography), and a final suit for everything else called "Cornucopia".

The first draft was developed in late 2012 by Colin Watson, to help train Agile website developers for a client. In 2013 Colin donated the game as a project to the vendor neutral, not-for-profit organisation, the Open Web Application Security Project (OWASP).

During recent months Colin has presented and played the game at six events in Edinburgh, London and Manchester. He is hoping to promote the game in other towns and cities. Like all OWASP projects, the game is free of charge and all materials are published with an open source licence, allowing anyone to use, modify and improve it.

==========
Question 2: How is your initiative making a difference and how does it meet the criteria for the category you are entering?

Threat modelling can be difficult and rather dull. The initiative was designed to help make this more fun, and to make it very relevant to websites and web applications, which are being created and updated at a phenomenal rate in the UK.

Most breaches are caused by attacks targetting application software directly. And almost every business in the UK is responsible for custom software in the form of a website, whether it be a few informational pages, an e- commerce shop, or a business process portal. These websites often have weaknesses in them that can lead to damage to individual users (e.g. malware), and the organisations that own them (e.g. data breach), undermining trust in the online environment.

Through using the game and examining potential attacks to derive security requirements, and making sure these are implemented, this combats online crime by making it harder for criminals and others to exploit software weaknesses gaining access to user and business data. This helps maintain, and possibly improve online trust, and certainly helps protect less experienced people online.

==========
Question 3: What did you set out to achieve with your initiative and how did you meet your targets?

The motive was to contribute to improvements in online safety by helping people create more secure web sites. The initial intention was to provide interesting and memorable training to web developers.
To minimise the initial cost, the original deck was created as a print-your-own word processing document, laid out to fit onto pre-scored "business card" printer sheets available from many stationers.
[Source document: http://bit.ly/SeGCQz ]

Fortunately the idea has taken off and a UK company has gifted the creation of professional print-ready artwork files. They have also donated printed decks, in a quirky package, which are available free of charge.

[Image of cards: http://bit.ly/1o7tvLa ]
[Request a free deck: http://bit.ly/1knYvCX ]

The criteria for success were twofold. Firstly whether developers, rather than information security specialists, find the game helpful, and secondly whether the game reduces software vulnerabilities. Feedback from software developers who have played the game say it has increased their engagement in threat modelling activities. It has been described as "the coolest project", "great fun" and "wonderful". Additionally it does appear to be helping to discover security issues, with possible problems being identified in some developers' own live websites – even during first use of the game.

==========
Question 4: How do you plan to develop your initiative further?

The internet is global and UK citizens and businesses can be affected by security and safety issues elsewhere. The threats against software are the

same everywhere so the project wants to make them more easily usable by people whose first language is not English.

Whilst English language skills are considered vital for information security professionals, this is not the case for the target audience, developers. OWASP volunteers have already offered to translate the game into Japanese and French; these and other languages will be made up into word processing and print-ready documents, and published free of charge like the current deck.

The plan is also to create a mobile app specific version. The threats are different for mobile apps and it would make sense to have a separate deck. Feedback at presentations from developers in the UK's financial services industry has suggested that a “web services” version of the game is desirable. Again this will require a different set of attacks and cross-references.

Furthermore, while presenting in Manchester one attendee expressed his desire to create another version of Cornucopia aimed at helping young people identify online safety threats. This is currently under discussion.

==========
Question 5: Why should your initiative win a Nominet Internet Award?

Cornucopia has been transformed from a personal project to much more. It seems that nothing else has managed to get developers so interested in information security concepts and issues. People love to get their hands on a deck, and use it. Gamification has lead to better engagement.
It benefits players' organisations by reducing vulnerabilities. By developing more secure websites and web applications it contributes to making the online economy safer for the UK’s internet users and economy.

Moreover, last year the a new information supplement for the PCI Data Security Standard was published, and there is a reference to Cornucopia. This and a software security podcast interview with Colin Watson in early 2014 have catapulted it into the limelight. Due to its generic, technology and vendor agnostic content, Cornucopia has been picked up enthusiastically by people around the world.

Demand for information about the game and how to use it be has been enormous. In the last couple of months Cornucopia is now being used in other countries and it is encouraging to see how a UK initiative can be adopted more widely. This has been facilitated by the increased visibility it gains from being an OWASP project.
==========