Open Web Application Security Project (OWASP)

First Draft 5th March 2009

Digital Britain Report

The UK Government has commissioned a report on Digital Britain concerning how to place Britain at the forefront of the global digital economy. The report's Steering Board is drawing on expertise from across Government, industry and regulators and has invited further contributions since publication of the interim report on January 29th 2009.

The Open Web Application Security Project (OWASP)[1] has created this submission as a contribution to the report. It has been co-ordinated by OWASP's Global Industry Committee[2] in consultation with OWASP's UK chapters in London[3] and Scotland[4].

Discussion

Introduction

OWASP believes good application security is vital to underpin the digital economy and safeguard users.

Fraud

UK Credit and Debit Card fraud is a prime "growth industry" for criminals; up 26% in 2007 (stats for 2008 not out yet)[5]. There is evidence too of a move away from cardholder present fraud, to more internet-based attacks—the main growth being in card-not-present (CNP) fraud, up 37% in 2007[6]. With the introduction of chip and pin in 2006, there has been a further shift in criminals' focus towards transactions where the cardholder is not present; specifically online. This, coupled with the increasing amount of banking and commerce conducted electronically means that the need for secure web applications is greater than ever.

Malware

Distribution of malicious code including viruses, worms, Trojans and spyware, collectively known as malware, used to be mainly undertaken through electronic mail. Spyware and phishing attacks are increasing in particular[7]. It is clear that these attacks are now motivated by monetary gain via an underground economy and criminal organisations[8].

Attacks against applications (e.g. websites and web applications) are the main area in which these sort of attacks are now being carried out[9]. To counter this it is crucial that future applications are designed with the most common risks in mind.

Data Loss

The protection of personally identifiable information, intellectual property and business information is a concern of most organisations, families and individuals. But there are now new ways for information loss, including theft, to occur through digitally connected networks. Web applications are being used to provide access to data that until recently would have been located only deep within an organisation's security perimeter. Now data has effectively been moved outside these defences and is no longer provided adequate protection. It is very difficult to make web applications completely secure, but the many incidents documented illustrate that they are not nearly secure enough[10].

Trust

The Internet and other digital channels are fast becoming the one thing we cannot live without. People are relying on the these channels for fun and education; organisations are relying on these channels to do business; government is engaging with citizens through these channels. But the Internet and other digital channels are insecure. To develop a vibrant digital economy, we need to build trust, and reduce distrust[11]. Without public confidence in the digital systems and processes, our own economic development in these areas will be stifled.

Most computer systems have defects and those exposed on the Internet and other digital channels are at greater risk of exploitation. This affects the systems, applications, the data and the users themselves. We are reliant on the existence of confidence in these channels—without which the sector could collapse. Countries that can improve the standard of software security, will benefit from increased trust.

Online Protection

Applications that are delivered over digital channels (Phone, Internet, TV, etc.) that contain security flaws put the systems, the data, the users at risk.

In order to make Britain the safest place to do business online, our systems and applications must be made more secure. OWASP is working with programming language teams, browser suppliers, framework developers etc. to try to make them more secure by default. But, we need to encourage wider uptake of building security into all stages of the software development process. If Britain can improve the standard of the applications by encouraging secure development practices, rigorous testing and security verification, the digital economy will benefit.

Application security should be approached as a people, process, and technology problem, because the most effective approaches to application security include improvements in all of these areas.

OWASP believes that the development of open standards and guidance is the best way to share knowledge. Organisations that have referenced the defects identified in

OWASPS's Top Ten Project[12] and used the Guide to Building Secure Web Applications[13], Code Review Guide[14] and Testing Guide[15] are using identified good practice to avoid common coding and deployment defects in the software development process.

OWASP members and other contributors are continually updating these guides and developing other tools to help developers, testers, auditors and application owners. They have developed the OWASP Enterprise Security API (ESAPI) Toolkits[16] to help software developers guard against security-related design and implementation flaws, by providing a ready-built, tested and verified modules for common web programming languages.

Organisations should implement security governance measures such as through the adoption of maturity models like one based on the Software Assurance Maturity Model (SAMM)[17]. These need to be tailored to the processes and risks facing each organisation. Once applications are developed, OWASP are committed to providing ways to assess and compare the security aspects. An initiative in this area is an open standard that defines ranges in coverage and levels of rigor to perform application security verifications—the Application Security Verification Standard (ASVS)[18]—which can be used to establish a level of confidence in the security.

Application Security Principles

Overall, the high level principles OWASP believes to be of importance[19] are:

- Apply defence in depth (complete mediation)
- Use a positive security model (fail-safe defaults, minimise attack surface)
- Fail securely
- Run with least privilege
- Avoid security by obscurity (open design)
- Keep security simple (verifiable, economy of mechanism)
- Detect intrusions (compromise recording)
- Don’t trust infrastructure
- Don’t trust services
- Establish secure defaults (psychological acceptability)

These need to be evaluated and interpreted for each particular application in the context of the business process and with consideration of the types of data being collected, used, stored and transmitted.

Digital Britain Report

The online safeguards already identified to protect vulnerable groups and provide informed consent for adults are important. Some of the issues relating to vulnerable groups are facilitated through the use of insecure websites, so improvements in application security also have a knock-on effect in these areas.

However fraud, distribution of malware and data loss can affect anyone. We need to encourage all types of organisations in the UK to identify and adopt good information security governance practices, and in particular ensure their applications are built and evaluated with security in mind.

Specific suggested changes and additions to the Interim report

Section 4.2 Driving Universal Connectivity: Take-up

General
Add a new sentence in the third paragraph after "great content and great services.": "The content and services must not expose the users, systems and data to un-necessary risk.".

Action 21
Insert "safe, secure and" before "designed for ease of use".

Section 5.1 Education and Skills

General
Add a new paragraph after the paragraph relating to the TSB, "Development of digital work-skills requires the appreciation of information security as an aspect underpinning Britain's digital economy. This digital economy relies on trust and the sector can be undermined by lack of security in any part.".

Section 5.3 Online Safeguards

General
The issues discussed above could contribute to the introduction of section 5.3

Tiers
The suggested four tiers of content and information, should be expanded to five. The extra tier is "material potentially harmful to everyone" that would include the likes of malware and web pages/applications that contain security defects which could allow damage to a user, their systems or their data.

Principles
Add a new bullet point "Secure, trusted digital commerce" to the existing three items.

Supporting Guidelines
Add a new bullet point "a safer online experience through the encouragement and uptake of secure software development practices on which OWASP provides a lead".

Action Points
The action points will no doubt be reviewed in the light of additional input since publication of the interim report.

A new action point could address the need to encourage the selection and adoption of secure software design, development, testing and verification methodologies, and for

Governmental organisations, and others, to require verification of the security of their digital applications. The Central Office of Information[20] is a key organisation in the research and development of standards for government websites[21]. The Information Commissioner's Office[22] is particularly active in information privacy matters.

Digital applications found to be lacking in adequate security undermine the confidence in the whole UK digital economy. Encouragement to adopt good application security practices and standards, and incentives to improve security, or reduce defects, would support a safer .UK digital economy.

About OWASP

OWASP is a global open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. OWASP build documents, tools, teaching environments, guidelines, checklists, and other materials to help organisations improve their capability to produce secure code. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security.

OWASP was formed in 2001, in an entirely organic fashion, when a group of security professionals came to realise how terribly insecure the way we develop our web applications was. The initial goal was deemed to be modest: write a guide for developers, which would document secure software development practices. While the initial effort was meant to last a few weeks, it came out to several hundred pages. When released, the OWASP Guide to Building Secure Web Applications was an instant success.

OWASP is a place where good people gather to help increase the awareness of the web application security problems in applications. It's a grass-roots effort, with the driving force being the people who are dealing with these problems every day, and wanting to lend a hand to change the situation for the better. The OWASP Foundation is a not-for-profit entity that ensures the project's long-term success.

OWASP has over 130 local chapters around the world including two in the UK.

OWASP's projects are widely referenced. For example, the OWASP Guide to Building Secure Web Applications is referred to in the Payment Card Industry Data Security Standard (PCI DSS)[23]. OWASP was shortlisted last year for the best security initiative award in Nominet's Best Practice Challenge[24].

References

Note: OWASP does not endorse commercial products or services.

1. Open Web Application Security Project (OWASP)
http://www.owasp.org

2. OWASP Global Industry Committee
http://www.owasp.org/index.php/Global_Industry_Committee

3. OWASP London Chapter
http://www.owasp.org/index.php/London

4. OWASP Scotland Chapter
http://www.owasp.org/index.php/Scotland

5. Fraud Abroad Drives Up Card Fraud Losses, APACS, 3 October 2007
http://www.apacs.org.uk/media_centre/press/03.10.07.html

6. Card Fraud Facts and Figures, APACS
http://www.apacs.org.uk/resources_publications/card_fraud_facts_and_figures.html

7. Information Security Breaches Survey 2008, DBERR, April 2008
http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

8. Report on the Underground Economy, Symantec, 24 November 2008
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf

9. Security threat report: 2009, Sophos
https://secure.sophos.com/security/whitepapers/sophos-security-threat-report-jan-2009-na

10. Web Hacking Incidents Database, Web Application Security Consortium
http://www.xiom.com/whid

11. Distrust and Trust in B2C E-Commerce: Do They Differ? McKnight D, Choudhury V, ACM International Conference Proceeding Series; Vol. 156 Pages: 482-491, 2006

12. Top Ten Project, OWASP
http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

13. Guide to Building Secure Web Applications, OWASP
http://www.owasp.org/index.php/Category:OWASP_Guide_Project

14. Code Review Guide, OWASP
http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project

15. Testing Guide, OWASP
http://www.owasp.org/index.php/Category:OWASP_Testing_Project

16. Enterprise Security API (ESAPI) Toolkits, OWASP
http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

17. Software Assurance Maturity Model (SAMM)
http://www.opensamm.org/

18. Application Security Verification Standard (ASVS), OWASP
http://www.owasp.org/index.php/ASVS

19. Principles, OWASP
http://www.owasp.org/index.php/Category:Principle

20. Central Office of Information
http://www.coi.gov.uk

21. Web Standards and Guidelines, Central Office of Information
http://www.coi.gov.uk/guidance.php?page=188

22. The Information Commissioner's Office

http://www.ico.gov.uk/

23. Payment Card Industry Data Security Standard (PCI DSS) v1.2
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

24. Best Practice Challenge 2008 Winners Brochure
http://www.nominet.org.uk/digitalAssets/34028_Best_Practice_Challenge_winners_booklet.pdf