OWASP UK Chapters

Formal Response to Browser Standards for Public Sector Websites

The government's Central Office of Information (COI) draft document on browser standards for public websites underwent public consultation from 5th September to 17th October 2008:

COI - Browser Standards Consultation version 0.13
http://www.coi.gov.uk/guidance.php?page=200

The OWASP Scotland and London Chapters developed and submitted the following joint response to COI on 16th October 2008.

About OWASP

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organisations to develop, purchase, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. OWASP advocates approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas. OWASP can be found at http://www.owasp.org

OWASP has over 130 local chapters around the world. Both the UK chapters (London and Scotland) have collaborated to create this joint response.

Introduction

We welcome the work on web standards and guidelines, in particular the understanding that websites have to be cross-platform and that the COI document should "provide a method for creating a reasonable list of browsers for testing".

The 7th Data Protection Principle of the Data Protection Act, which appears in COI's list of 'legal issues' http://www.coi.gov.uk/guidance.php?page=164, recommends publishing organisations to take a 'risk-based approach to security matters'. So, whilst the over-riding objective is to publish information and ensure everyone can see it, public sector and other organisations still have an obligation to secure it.

Cross-platform support, including security, should be built into all stages of website

development, testing and operation i.e. throughout the software development life cycle. The support of particular browsers and platforms should be built-in and not reliant on additional coding which could introduce additional vulnerabilities. All data submitted by users and returned to them should be validated and secured, and where appropriate encryption used to protect sensitive data (such as log in forms) and for transfer.

A key issue is that while the website should be supported in popular browsers, this is not sufficient for testing purposes. Developers/programmers needs to realise that people will try and access the content using "non-browser" tools to look for vulnerabilities and the website should be secure enough to protect users and itself from such threats. This requires testing beyond "popular browsers".

OWASP has produced a Top 10 Guide to the most critical web application security flaws which is referenced by many leading government, financial (e.g. Payment Card Industry Data Security Standard), and corporate standards and is the Gold standard for web application security. Two other reference points for website owners and developers are the OWASP Guide to Building Secure Web Applications and the OWASP Testing Guide.

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

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

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

Suggested amendments to the document

Paragraph 30: Add text "The critical security flaws identified in the OWASP Top Ten Project must be protected against in all browsers and tools, regardless of popularity."

Paragraph 40: Add text "The website should be developed using practices such as those detailed in the OWASP Guide to Building Secure Web Applications and tested for security using the OWASP Testing Guide." and "Users critical data (passwords, account numbers, cash relative data, etc) must be encrypted as defined in standard security policies."

Paragraph 41: Add a bullet point "Security - Is the user, their system and their data secure?"

Paragraph 46: Add bullet points "Manipulation and addition/removal of form, URL, cookie and other header parameter values" and "Business logic"

Appendix A: Add at end "Security issues must also be tested with no assumptions of browser type."

Appendix B: Add to template table "Manipulation and addition/removal of form, URL, cookie and other header parameter values" and "Business logic"