WATSON HALL

Watson Hall Ltd

London 020 7183 3710
Edinburgh 0131 510 2001

info@watsonhall.com
www.watsonhall.com

TOP 10

Top 10 website security issues

the website security issues to tackle first

Website security (also referred to as web application security, or webappsec) is a broad field, but most websites have common security issues that need to be addressed, regardless of the particular technologies used or functions deployed.

Terms of use

This top 10 list is provided free of charge and without any warranty. Use of this top 10 list is subject to the terms of use displayed on our website at http://www.watsonhall.com/terms/

Each top 10 list may need to be amended for the particular website project's requirements, functionality and environment.

References

You may want to review all our top 10 website security lists at http://www.watsonhall.com/methodology/top10s.pl. The latest links to details of information security related legislation, codes of practice, organisations, initiative and standards can be found on the Watson Hall website at http://www.watsonhall.com/security/

1 Validation of input and output data

All data used by the website (from users, other servers, other websites and internal systems) must be validated for type (e.g. numeric, date, string), length (e.g. 200 characters maximum, or a positive integer) and syntax (e.g. product codes begin with 2 letters and are followed by 5 digits) and business rules (e.g. televisions can only cost between £100 and £2000, an order can contain at most 20 items, daily credit limit must not be exceeded). All data written as output (displayed) needs to be safe to view in a browser, email client or other software and the integrity of any data that is returned must be checked. Utilising Asynchronous JavaScript and XML (AJAX) or Adobe Flex increase complexity and the possible attack vectors.

2 Direct data access (and theft)

If data exists, it can potentially be viewed or extracted. Avoid storing data that you do not need on the website and its database(s) – for example some data relating to payment cards should never be stored. Poorly developed systems may allow access to data through SQL injection

compromises, insufficient input and output data validation (see No 1 above) or poor system security.

3 Data poisoning

If user's can amend or delete data inappropriately and this is then used to update your internal systems, business information is being lost. This can be hard to detect and it is important that the business rules are examined and enforced to validate data changes to ensure poisoning is not occurring. If poisoning is not detected until well after it has occurred, it may be impossible to recover the original data.

4 Malicious file execution

Uploaded files or other data feeds may not be what they seem. Never allow user-supplied input to be used in any file name or path (e.g. URLs or file system references). Uploaded files may also contain a malicious payload so should not be stored in web accessible locations.

5 Authentication and session management

Websites rely on identifying users to provide access permissions to data and functions. If authentication (verification of identity, registration and logging in), authorisation (granting access rights) and session management (keeping track of the identity of a logged in user while they browse a website) can be circumvented or altered, a user could access resources they are not allowed to. Beware especially of how password reminders, remember-me, change password, log out and updating account details are handled, how session tokens are used and always have login forms on dedicated and encrypted (SSL) pages.

6 System architecture and configuration

The information system architecture model should address the sensitivity of data identified during the requirements and specification phase of a website project. This may entail having separate web, application and database servers or involve clustering, load balancing or virtualisation. Additional security issues can be created through the way the live environment is configured. Sufficient and safe logging, monitoring and alerting facilities need to be built in to allow audit.

7 Phishing

Phishing, where users are conned into believing some other entity is or belongs to your own organisation (email messages and websites are the most common combination), is best tackled through user education but the way the website is designed, its architecture and how it communicates with users can reduce the risk.

8 Denial of service

Whilst malicious users might try to swamp the web server with a vast number of requests or actions that degrade its performance (filling up logs, uploading large files, undertaking tasks that require a lot of memory repeatedly) denial of service attacks include locking out valid user accounts or be caused by coding problems (e.g. memory leaks, resources not being released).

9 System information leakage

Web servers, errors, staff, partner organisations, search engines and rubbish can all be the source of important information about your website – its technologies, business logic and security methods. An attacker can use such information to their advantage so it is important to avoid system information leakage as far as possible.

10 Error handling

Exceptions such as user data validation messages, missing pages and server errors should be handled by the code so that a custom page is displayed that does not provide any system information to the user (see No 9 above). Logging and alerting of unusual conditions should be enabled and these should allow subsequent audit.

Why Watson Hall?

Watson Hall helps United Kingdom organisations design, develop, implement and operate websites and web applications securely, by undertaking threat modelling, vulnerability assessments, developing information security management programmes, providing advice on development best practice and performing security testing.

To discuss any security matters in confidence and without obligation, telephone us on 020 7183 3710 or use the enquiry form on our website at http://www.watsonhall.com/form/

Watson Hall Ltd is a limited company registered in England no 6004969 at North Bastle, Gatehouse, Northumberland, NE48 1NG, United Kingdom.