SQA CONSULTANT

Inventing the future....

# Making your Web Application Secure

White paper - August 2014


# Table of Contents

# Introduction

The increased use of web applications and online information sharing creates convenience and more opportunities for clients and organizations. However, this also introduces the risk of information exposure even to the extent of risking individual's financial information. This exposure attracts more and more hackers to perform targeted and varied attacks on web applications. To minimize the success of these attacks, government companies and private organizations are updating the regulations to ensure comprehensive security testing and audits of web applications prior to release. Both, the threats and the regulatory requirements, increase the necessity of security testing. In this white paper we will be focusing on various aspects of security testing of web applications. Major topics include:

- The reasons and importance of security testing, its relation to software development process, and how often testing should be performed.
- The OWASP Top 10 web application vulnerability list and its relation to other security standards and regulatory requirements.
- Security testing techniques and its types
- How SQA Consultant team contributes towards securing your application.

# Why web application security is important?

Any online system requires protection at multiple levels of network and application layers. All the different stages, for their protection, require unique set of tools, techniques and expertise. The security of network to system layers is a reasonably old area of online and offline systems. For protection of these layers, many tools and techniques are available, like firewall, anti-viruses, network distribution, etc. If these tools are correctly configured (which also requires testing and verification) then these layers become reasonably secure. Also, organizations and managers are generally aware of these vulnerabilities and therefore are ready to invest in protection of these layers.

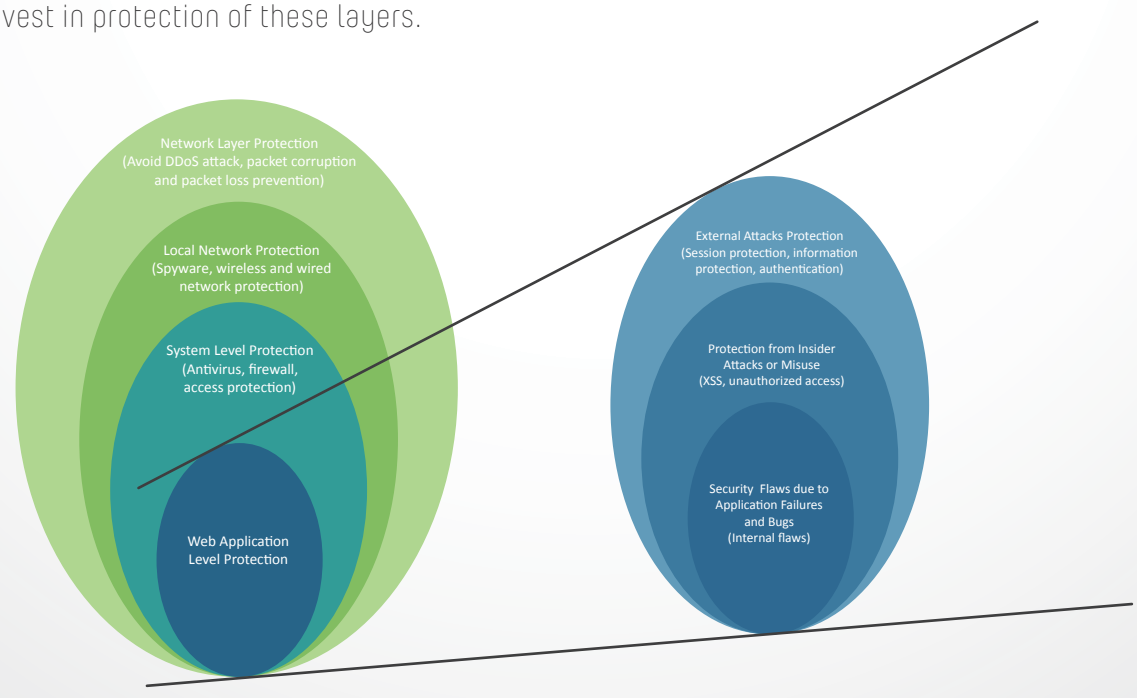



Figure 1 - Protection layer classification and web application layer details

On the other hand, web applications are relatively new area and an exponentially growing field. Due to strict budget and time constraints, application designers and developers do not have enough time to consider all aspects of product security.

The Web Application Security Consortium (WASC) estimated in early 2009 that 87% of all websites were vulnerable to attack. In another independent analysis run by Acunetix, 70% of websites are at immediate risk of being hacked.

The awareness of developers and managers about vulnerabilities, even the known ones, is quite low. Due to this limited awareness and large growth, according to Web Application Security Consortium (WASC) estimates, in 2009 the 87% of all web sites were vulnerable to attacks.
When a comparison is made of web application layer attacks to system attacks, application security testing becomes of even more importance because of the following reasons:

- Web application attacks are simple in nature as compared to the complex nature of system attacks.
- Vulnerabilities of application expose data of multiple users that can be misused as compared to when an individual user's system is compromised.

So, it is better to perform security checks on your application and strengthen it against any possible attack than to take risks.

As per the analysis performed in 2007 by CSI (Computer Crime and Security Survey) a web security breach costs as much as $350,424. This cost can be saved by making security testing an integral part of our testing cycle.

# What makes your application secure?

Just like software quality assurance process, the software security assurance also requires a complete set of management activities that are integrated with software development process of the organization. Following are the two major parts of application security assurance:

## Identify security management and testing activities

The set of activities that are performed to ensure software security includes, but is not limited to, security testing. Selecting a correct and complete set of activities ensures security of any application. Therefore, the identification of these activities is one of the most critical success factors for any security assurance project. These sets of activities depend upon the application type, organization requirements and compliance requirements. The standards related to information security and IT security, (like PCI DSS, ISO 27000 series, ITIL, ASVS) define set of security requirements, security control areas, implementation processes and frameworks. The set of activities and the depth of each activity vary for each standard. However the generic set of activities, that would be required for any security plan, is depicted in Figure 2.

Defining and extracting activities based on security requirements of application, organization's standards, and perfectly integrating them with SDLC can guarantee the security of products.

## Integrate security testing activities with organization's current process

After identifying the testing activities according to the organizational and security standard requirements, these activities should be integrated with the current project development process. A simple activity list and its relation with general process are depicted in Figure 2.


Figure 2 - Application security project activities aligned with software development life cycle

## How frequently should a security check be run?

Even if security testing is an integral part of the development life cycle, it is important that security checks are frequently run on the environment.

The frequency of security testing depends on the following factors:

- The sensitivity of data involved in your application
- Type of threat, virus, function library updates etc.
- Security standard compliance requirements
- The budget allocated for security testing

One important point here is to make sure that the development and testing plan is flexible enough to cater to any unforeseen circumstances e.g. a new and critical vulnerability detected. In such case of emergency, the team should be ready for an emergency testing patch to secure the application. For example, in case a global security breach has affected many applications, an emergency testing sprint would have to be run to secure your application from its effects and handle the issue if the application is affected.

As per PCI Security Standard Council:
"Penetration testing should be performed at least annually and anytime there is a significant infrastructure or application upgrade or modification (for example, new system component installations, addition of a sub-network, or addition of a web server)."

## What is OWASP and what constitutes its Top 10 vulnerability list?

Open Web Application Security Project (OWASP) is a not-for-profit charitable organization whose focus is to improve software security. Their mission is to help individuals and organizations in improving the software security by providing following information:

- Knowledge of vulnerabilities and scope of their threat.
- Tools and techniques to identify them.
- Preventive measures that need to be integrated in the application.
- Free and open source tools and frameworks developed by OWASP participants that can be used for
  - o Understanding of vulnerabilities
  - o Security testing of applications
  - o Secure development support frameworks for different platforms (ESAPI)
- Guidelines, processes and standards including
  - o Application Security Verification Standard (ASVS)
  - o Software Assurance Maturity Model (SAMM)
  - o Testing guide
  - o Development guides and cheat sheets
  - o Top 10 vulnerabilities list

OWASP: A community dedicated to software security by providing security standards, security requirements, development and testing guidelines, and free and open source tools for testing and development support.

OWASP Top 10 provides important guideline about the most critical web application security flaws. It was first released in 2003 and since then a new version of the document is released after every three years with updated priorities of these Top 10 risks. The OWASP Top 10 list is made by contribution of security experts from all over the world. The Top 10 list document provides following information:

- Vulnerability description
- Sample vulnerability and sample attack
- Guidelines on how to avoid these vulnerabilities
- References to OWASP and other related articles

Underlying concept is that if you are able to prevent Top 10 risks successfully, then you have reduced a lot of security breaches as well as future maintenance cost.

The security policies, risk assessment policies and risk treatment plans in the security audit activity list are extracted from the OWASP Top 10 document and its references.

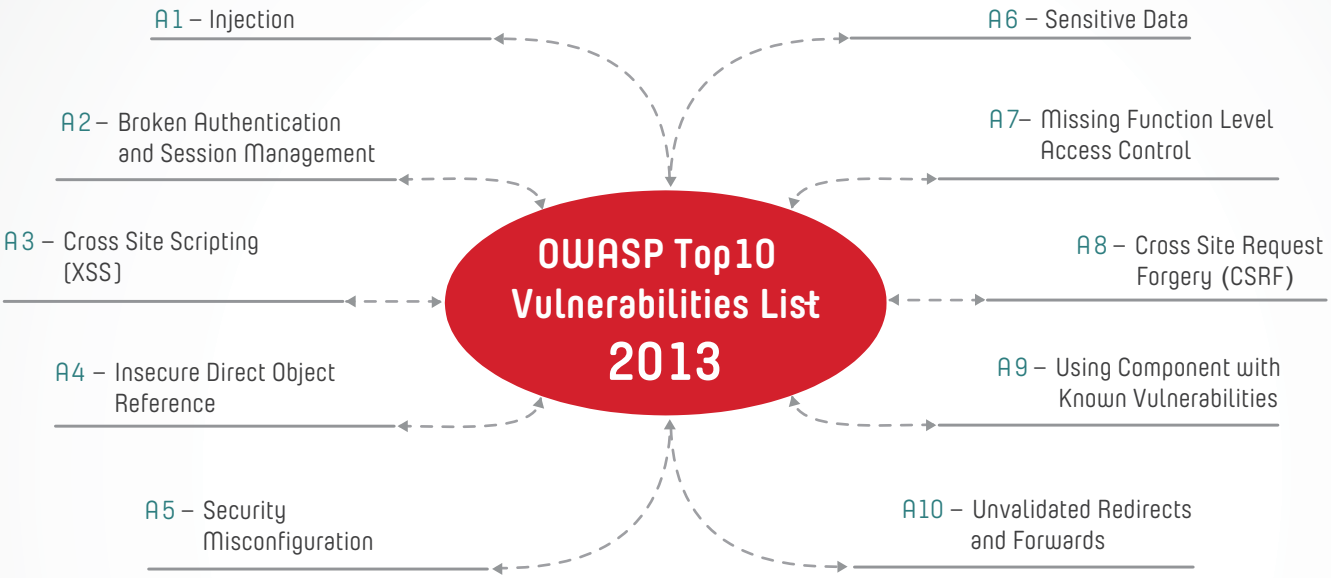



Figure 3 - Vulnerabilities list based on OWASP Top 10 project -2013

# How vulnerability list relates with other standards?

The OWASP Top 10 vulnerability list provides the basic, most important and extensive step towards making the application secure. Hence, many organizations and standards relate to the OWASP vulnerability list. It can be easily said that the compliance to Top 10 vulnerability list becomes the first step towards any security standard compliance. Following table lists different security standards and their relation with OWASP Top 10

| Standard and Organizations | Description | Relation with OWASP Top 10 List |
|---|---|---|
| ASVS | A standard developed by OWASP that lists the requirements for web applications | The requirements of ASVS and Top 10 list overlap and therefore Top 10 list forms the basis of ASVS |

| | | |
|---|---|---|
| Gramm-Leach-Bliley Act (GLBA) | An act provided by US Federal Trade Commission (FTC) which specifies requirements of security, privacy, safeguard and protection | For web application section they recommend protection from OWASP Top 10 vulnerability list |
| National Security Agency NSA | A government organization that focuses on protecting U.S. national security systems | Refer OWASP Top 10 in their web application security overview |
| ISO 27000 Series | ISO 27000 series provides different security control areas, security requirements. However, none of them are specific to web application | The requirements and security policies for control areas related to web application can therefore be extracted from OWASP Top 10 list |
| ITIL | ITIL provides framework for software development and includes security requirements but it is not specific to web application | The requirements and security policies related to web application can therefore be extracted from OWASP Top 10 list |
| PCI DSS | Any organization or application that deals with money transactions and credit card data handling has to comply with PCI DSS | The requirement section 6 of PCI DSS deals with web application part of the complete project and its requirements. This section overlaps with Top 10 list of OWASP |
| FFIEC | A council that heads different law enforcement organizations and acts like Electronic Fund Transfer Act, Regulation (EFTA) | FFIEC guidelines for authentication overlap the requirements for authentication and session management of OWASP Top 10 |

Many other organizations and standards that define security requirements in terms of confidentiality, protections, privacy and integrity do not particularly deal with requirements for web applications. In these scenarios the security policies for web application can be obtained from OWASP Top 10 vulnerability list and its references.

# What constitutes security testing and what are its types?

The security testing and risk assessment activity, just like any other testing, is a set of tests that evaluate the standing of an application against a set of criteria. As discussed in previous sections, the scope, security requirements and risk criteria are based on application requirements, standards requirements, and organizational requirements. Defining and planning risk assessment policy is an important activity before starting actual security testing. In order to plan the testing activities one needs to understand the different types of testing. We will discuss the testing categories based on two criteria: Security Testing Method and Security Testing Depth.

## Security testing types based on testing method

### Manual Testing

In manual testing a human resource directly executes tests based on assessment criteria and analyzes its results. This is among the most powerful and effective techniques available in any type of testing.
Manual testing may include checking vulnerability lists, reviewing the design document, reviewing the code and analyzing the data storage.

**Advantages:**

1. It is most comprehensive and flexible testing.
2. Requires minimum supporting technologies.
3. Early introduction in SDLC.
4. Scenario identification based on application functionality.

**Considerations:**

1. Manual testing consumes a lot of time.
2. Depends on testers' thought process, skills and testing effectiveness.
3. All input validations cannot be tested due to time constraints.
4. Cannot totally replace automated testing.

### Automated Testing

Automated security testing can be used to test security requirements using minimum human interaction. The security testing can be automated in different ways i.e.
1. Use automated parsers that parse through your application and identify vulnerabilities.
2. Automate functionality based scenarios using web application automation tools.

**Advantages:**

1. Reduces testing time.
2. Increases test coverage.
3. Reduces dependency on skills of testers.

**Considerations:**

1. Parsers do not cover application functionality and business scenarios.
2. Automating functionality related testing incurs development and maintenance cost.
3. Cannot totally replace manual testing especially related to new scenarios and vulnerabilities.

# Security testing types based on testing scope

### Penetration Testing

In this type of testing, tester is given minimal or no information of the application to be tested. This requires exploring application interfaces through public IP analysis, open port analysis, host system analysis, communication protocol analysis and social engineering.

**Advantages:**

1. Can be fast (and cheap)
2. Requires a relatively lower skill-set
3. Tests the code that is actually being exposed

**Considerations:**

1. Introduced too late in the SDLC
2. Limited testing scope
3. Does not give complete picture as the limited time available to tester is normally not applicable to hackers.

### Authorized Internal Testing

In this type of testing the testers are given complete access to application including its user interface, administrative interface and databases. The tester has complete understanding of application and its business logics.

**Advantages:**

1. This helps find maximum vulnerabilities in limited time
2. It is the minimum requirement of security testing based on OWASP recommendations

**Considerations:**

1. Requires complete application understanding
2. Requires clear definition of security policies and requirements to be tested

### White Box Testing

Security standards like ASVS and PCI DSS have different level of security requirements based on application functionality. In higher security levels, it is required to perform complete code analysis. The code analysis can contain static and dynamic analysis. The purpose could be to review cryptographic techniques, field validations, authorization checks, branch coverage and statement coverage.

**Advantages:**

1. It is the most comprehensive security testing coverage
2. Increases test coverage
3. Reduces dependency on skills of testers
4. Early introduction in SDLC
5. Early identification of issues

**Considerations:**

1. Highly skilled testing staff required
2. In practical scenarios, source code deployed might not be the one reviewed

# How to balance security techniques and types?

Due to different types of available testing techniques, it also becomes an important task to understand which techniques are best suited for an application. In general, there is no correct or incorrect answer to this question. However after compiling the application requirements and/or standard compliance requirements one needs to develop a balanced approach. The balanced approach is the one that integrates with a complete SDLC and therefore can perform security testing and verification activities based on current phase of the SDLC. Even in SDLC the security testing needs to be performed in correct percentage to identify maximum issues at earlier stages and increase security testing efficiency. According to the OWASP testing guide following is the proportion of test effort in different phases of SDLC:

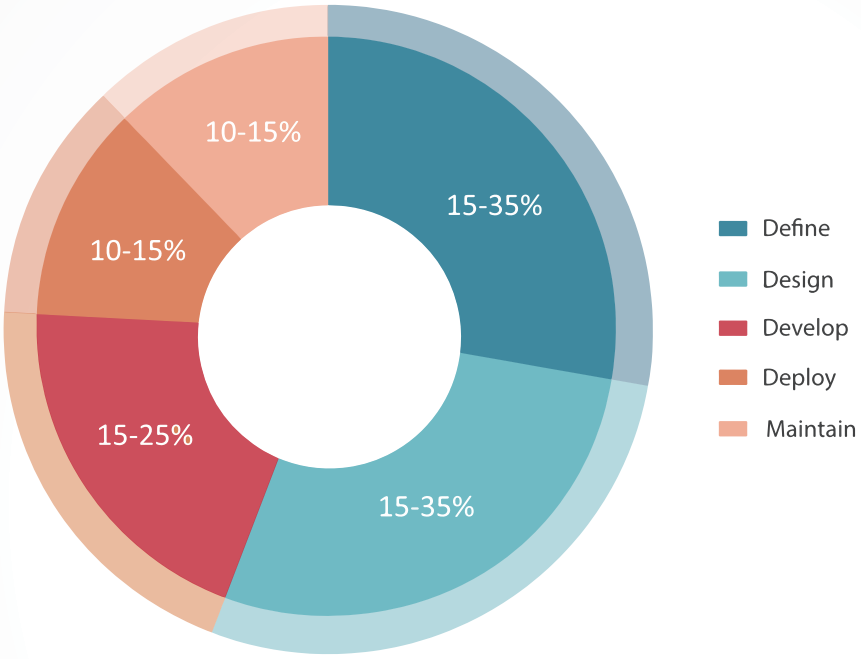



Figure 4 - Security test efforts proposed by OWASP in proportion to software development life cycle

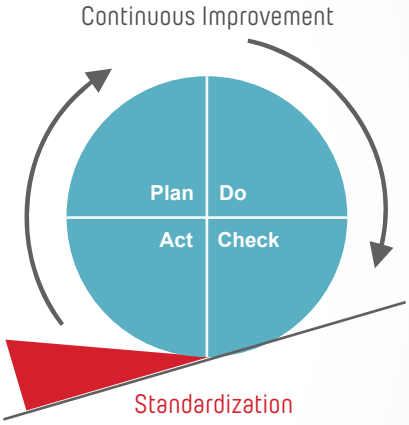
# What are the common misconceptions of security testing?

There are organizations that fail to secure their applications despite investing their time and resources in security testing of their applications. Such organizations are usually the victim of some misconceptions related to the security of web applications. Following are the major misconceptions identified by security experts and OWASP, that need to be addressed for ensuring secure applications:

- Securing of system and network through firewalls and antiviruses is not sufficient for security application.
- Without approval of project managers and stakeholders, complete security testing is not possible.

- Developers themselves create security requirements during design phase of the project. Instead the security requirements should be based on some internationally recognized set of rules.
- Performing security testing without understanding complete process, requirements and techniques is not possible.
- Most commonly performed testing is penetration testing, but it does not give a complete picture of application security.
- Sometimes even when security testing process is used, it is not well integrated with SDLC and therefore does not achieve its purpose with maximum efficiency.
- One time security testing is not sufficient for application security. Application should be tested annually, for any major functionality change or when a critical vulnerability is identified.
- Security testing is normally considered independent of application functionality. However, it needs to be tested whether business logics can be bypassed or not.
- Automated web parsing tools are not sufficient for security testing as they cannot identify business logics.
- Introduction of security testing at later stages results in more effort and less comprehensive issue list.

# How we contribute towards security of your application?



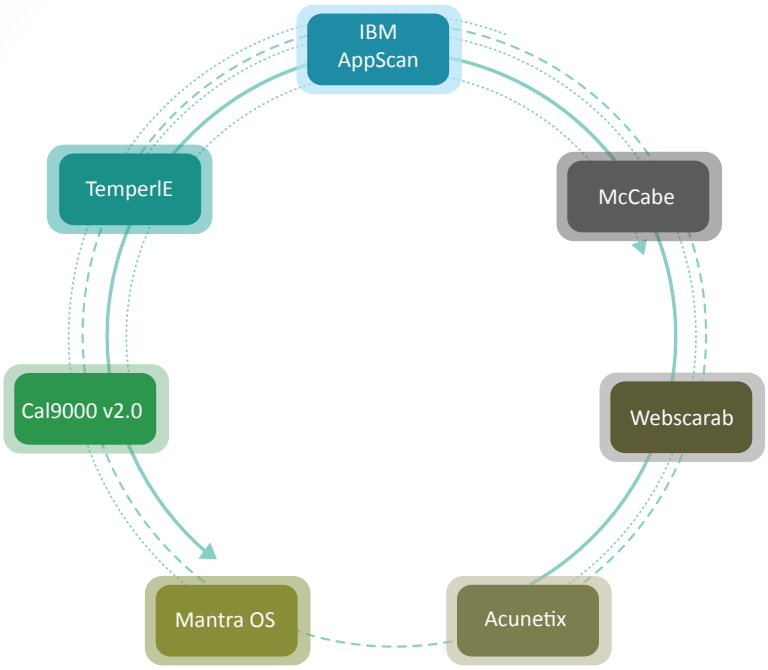

SQA Consultant team's security testing services ensure a complete and comprehensive application security based on any of the clients requirements. Keeping in mind the entire spectrum of risks, nature of application and available testing techniques we help our clients in following activities by using Plan-Do-Check-Act process:

- Identifying security standards, laws and regulations that apply to the application scope
- Conveying importance of web application's security across teams, managers and stakeholders
- Creating a maintainable and scalable framework
  - o Process suggestions based on current SDLC of the organization
  - o Suggesting required testing types and conducting any type of testing
- Gathering security requirement based on
  - o Application functionality requirements
  - o Any security standard compliance requirements
- Generating concise and detailed test report
  - o Efficient testing and issue reporting
  - o Helping developers and managers in understanding the reported issues, their risk level and their possible fixes.
- Conducting internal audits for compliance to well acclaimed standards
- Mitigating critical failure factors in order to achieve maximum results

SQA Consultant team has the skills and capability to help your organization in any of the above mentioned activities with the best quality.
In the past we have performed following activities for our clients:

- Identifying standards and laws applicable to non-financial web application in US.
- Defining security testing process for clients
- Defining requirements based on OWASP Top 10 list
- Writing test cases applicable to application based on OWASP Top 10 list
- Penetration testing and full access testing for web application
- White box testing and code reviews for safety critical applications
- Generating comprehensive and detailed issue reports

SQA Consultant team has previously used following major set of tools for the purpose of security testing:




# Conclusion

Web application security is critical because the system and network level security techniques do not completely protect user's data. Achieving web application security should not be considered as a trivial task and organizations should fully commit to the security project. In order to achieve this, organizations should understand their unique security requirements and relevant security testing techniques before moving forward with security project. The security testing activities also need to be well integrated with software development cycle and software testing cycle.
The security testing process and requirements should be developed after thorough research of internationally available standards and set of rules. In the field of web application, OWASP Top 10 vulnerability list and related projects provide a comprehensive set of requirements. Therefore, compliance with Top 10 list can be considered as a main goal for any web application security project.
SQA Consultant team can provide support to your organization in all activities ranging from understanding international standards to comprehensive testing and process integration. Our focus is to mitigate common errors made during software testing and provide efficient and successful implementation of security testing process. We also help organizations in internal audits before they apply for external standard certification.

SQA CONSULTANT

Inventing the future....

# Contact Us

Explore ways to use our expertise in growing your business while establishing a valuable partnership with us.

Contact our consultants at:

Phone: +1.412.533.1700 (Ext: 585)
E-mail: info@sqaconsultant.com
Website: www.sqaconsultant.com