

Web Application Security, The Importance of an Independent Assessment

Background	1
What are the key threats?	2
When should you perform a WASA?	3
How will a WASA help improve your application and organisational security?	4
Why Activity?	5
More Information	5

Background

Web applications are becoming more sophisticated and increasingly technically complex. They range from dynamic Internet and Intranet portals, such as e-commerce sites and partner extranets, to HTTP-delivered enterprise applications such as document management systems and ERP applications. The availability of these systems and the sensitivity of the data that they store and process are becoming critical to almost all major businesses, not just those, which have online e-commerce stores.

This diversity in the use and the sensitivity of information that needs to be protected introduces a distinct set of risks and security challenges into the corporate environment. The Gartner Group states, "Today over 70% of attacks against a company's web site or web application come at the 'Application Layer' not the Network or System Layer." The cost of a successful attack and the subsequent compromise of the application to any organisation can be significant both financially and in damage to reputation. The risk of compromise has risen with the increased complexity of web applications, the growing interest in security breaches by both the media and regulatory bodies and the proliferation of different groups of potential attackers.

Web applications and their supporting infrastructure and environments use diverse technologies and can contain a significant amount of bespoke and customised code. The very nature of their feature rich design and their ability to collate, process and disseminate information over the Internet or from within an Intranet makes them a popular target for attack. Also, since the network security technology market has matured and there are fewer opportunities to breach information systems through network based vulnerabilities; hackers are increasingly switching their focus to attempting to compromise applications.

Security breaches and successful attacks executed by malicious attackers have recently been a favourite media topic. The smallest of breaches, that historically may well have gone unnoticed by the wider public, are now often widely publicised, greatly increasing the risk to an organisation's reputation.

Web Application Security

The UK Government, in direct response to the recent spate of publicised security breaches and the resultant mood of distrust from the public towards the storage and processing of their data, has initiated the process of revising the Data Protection Act.

The proposed changes include legislation to increase the accountability of organisations and individuals; as well as the introduction of a criminal offence in the case of demonstrable neglect towards information security or repeated data breaches.

In addition, regulatory bodies such as the Information Commission and the Financial Services Authority (FSA) are calling for UK and EU legislation to require the public disclosure of significant security breaches that result in the loss of personal information and data.

There are also now a wide range of potential groups of attackers, with differing motivations, ranging from individuals looking simply to compromise systems driven by a passion for technology and a 'hacker' mentality; focused criminal organisations seeking potential targets for financial proliferation; political activists motivated by personal or group beliefs; to disgruntled employees and system administrators abusing their privileges and opportunities for a variety of goals.

As the level of threat and the potential organisational exposure to application-based attacks increases it is critical that organisations incorporate application security into their information security strategy and risk assessment processes. Through understanding the threats and performing a programme of assessment of application level vulnerabilities, an organisation can provide evidence to regulators, customers and partners that they are effectively managing the risk that their corporate applications pose.

The remainder of this paper sets out the key threats that your web application(s) face, together with their impact on your organisation. The paper then details how you can address these threats with an independent Web Application Security Assessment (WASA).

What are the key threats?

Web applications that store and process sensitive and personal information are typically exposed to five generic threats:

- **Authentication Bypass** giving access to the application and its stored and processed data via the circumvention of authentication controls.
- **Privilege Escalation** giving unauthorised access to the application and its stored and processed data via the circumvention of access controls.
- **Loss or Modification of Data** resulting in the integrity of the applications data store being compromised.

- **Compromise of Interconnected Systems** resulting from exploitation of a trusted path through an insecure application in order to leverage access to otherwise unexposed corporate or partner systems and data.
- **Denial of Service** resulting in the unavailability of the applications resources.

Successful exploitation of any of these threats and the loss, modification or destruction of your applications data could lead to:

- Modification, leakage or destruction of your sensitive customer or organisational data.
- Loss of service and therefore loss of revenue through unavailability of the application.
- Loss of organisational reputation and customer confidence.
- Fines from the Information Commissioner or other regulatory bodies.
- Loss of revenue.

It is therefore critical to perform an assessment of web applications both prior to their roll out and on a regular basis to ensure that any and all specific application threats are understood and remediated.

When should you perform a WASA?

You should consider performing a WASA on all external and internal web applications that store and process sensitive corporate information. The decision as to which web applications to test should be driven by a security risk assessment.

Many organisations trust their application providers and developers to have implemented effective application security. Although many developers use standard frameworks and take application security seriously, their primary aim is functionality and delivering a working application. There is no substitute for an independent assessment from an organisation that is focused on security.

When considering whether to perform a WASA the questions you should ask are:

- Does the application store and process personal information that is covered by the Data Protection Act?
- Does the application store and process financial information?
- Does the application store and process sensitive corporate information?

- Does the application require user authentication and/or multiple levels of access control to restrict the viewing and/or modification of the application or its data?
- Does the application connect to other applications or systems within your organisation?
- Does the application connect to other applications or systems outside your organisation?
- Does a third party provider manage the application?
- Did a third party provider develop the application?
- Is the application bespoke to your organisation, developed for a specific purpose?

If the answer to any of these questions is yes then you should strongly consider a WASA.

How will a WASA help improve your application and organisational security?

Specifically a Web Application Security Assessment will help your organisation:

- Validate the effectiveness of security controls within an application.
- Understand and identify potential breach points.
- Benchmark an application's security posture.
- Provide confidence in any third-party software to ensure it is fit for purpose before purchase or deployment.
- Identify and eliminate errors in the applications prior to deployment to reduce the cost and risk of remedial efforts.
- Provide significant value as part of a standard development QA and testing process.
- Provide input into the organisational security risk assessment process on the key threats and vulnerabilities within an application or suite of applications.
- Aid in protecting brand identity by avoiding loss of consumer confidence and business reputation.
- Protect intellectual property and prevent financial loss ensuing from a real and successful attack.
- Demonstrate compliance and conformity with Industry, Government and regulatory bodies enabling organisations to operate in regulated markets.

Web Application Security

Why Activity?

- Activity uses proven and repeatable methodologies that build on recognised Industry Standard approaches such as CHECK, Council of Registered Ethical Security Testers (CREST), Open Source Security Testing Methodology (OSSTM) and Open Web Application Security Project (OWASP).
- Activity is a CREST member company and as such assessment methodologies and processes have been assessed independently to ensure that they provide the required level of quality and skills in the provision of security testing services.
- Activity consultants have an average of over 5 years security testing and consultancy experience in providing security services to HMG and private sector clients.
- We have a wide range of experience in testing applications of all sizes and shapes, from e-commerce applications to collaborative working applications, document management systems and enterprise CRM systems.
- Activity's internal processes and systems have been certified to ISO 9001 for Quality and ISO 27001 for security, giving confidence to clients that Activity provides a consistent and quality focused service to clients.

More Information

For more information contact:

Activity
25 Hercules Way
Aeropark, Farnborough
Hampshire
GU14 6UU

Tel 01252 377321
Fax 01252 377670
Email info@activityim.com
Web www.activityim.com