

## Comment Article

### **Straight Talking – Why you should hack your own systems**

By Fran Howarth, Principal analyst, Quocirca Ltd

The top two threats facing organisations today are web-based applications and end users, according to information security researcher the Sans Institute.

Vulnerabilities affecting web applications account for almost half of the total weaknesses seen, Sans says. They are being exploited to convert trusted websites into malicious servers that can launch client-side exploits that are usually delivered via a web page or an email, such as in phishing scams.

Considering the large number of vulnerabilities that are found in web-based applications, it is of great importance that security is built into applications early on in the software development lifecycle - and that they are tested regularly to identify and remove flaws as soon as possible.

During the development process, tools such as source code analysers will do much to identify flaws in the application code. However, even the best source code reviews will be unlikely to uncover all vulnerabilities.

Therefore the best practice is to take a multi-tiered approach to testing software applications for security flaws, by using static code and dynamic program analysis along with vulnerability assessment and scanning tools, and penetration testing.

Scans and assessments are useful for locating potential risks by pinpointing flaws in the application that have manifested themselves into full blown vulnerabilities. For example, when an application is added to the network, the interactions that it has with other pieces of network infrastructure could cause a vulnerability to arise that could not have been seen from just looking at the source code in isolation.

Penetration tests should then be used to seek out those weaknesses that could most readily be exploited. Sometimes also known as ethical hacking, penetration tests are proactive, authorised attempts to compromise security by using the tools favoured by hackers in order to see how well applications hold up against real-world threats.

Armed with this information, organisations can then prioritise remediation efforts for the threats deemed to be the most critical.

In the early days of penetration testing, many organisations were sceptical about their use. However, the use of penetration testing has increased considerably, especially in the last year, and is now considered a best practice for ensuring applications are secure.

In fact, such tests have become so widely accepted that one of the newer regulations to affect organisations accepting credit card payments - the Payment Card Industry Data Security Standards (PCI DSS) regulation - specifies their use at least once per year.

But penetration tests have a lesser known benefit over and above remediating against flaws contained in applications themselves: they can be used to test the security knowledge and awareness of computer users so they don't inadvertently compromise security through human errors.

Hackers are increasingly using social engineering techniques such as phishing, where an attacker tries to perpetrate fraud by sending out legitimate-looking emails in an attempt to garner personal or financial information from an end user. In its latest Security Threat Report, security vendor Symantec saw a 66 per cent increase in computers that have been identified as hosting one or more phishing websites, probably owing to increased use of automated phishing kits.

## Comment Article

---

Penetration tests allow organisations to set up social engineering attacks, garnering information such as email addresses from vulnerable applications and using wizards and templates to do things such as create an email, associate it with an exploit and send phishing attacks to employees to see how aware they are of security issues and how they respond to such an attack.

In this way, organisations can identify which users are less security-savvy - and may need some training on how to avoid such scams.

Through the use of integrated security testing, organisations are in a better position to protect against two of the greatest threats to their organisations: exploitable vulnerabilities in their web-based applications and errors made by end users.

Just remember: testing is not a one-off task and should be repeated at regular intervals or whenever significant changes are made to applications or networks. Hackers are becoming increasingly sophisticated and have an ever-growing range of automated tools at their disposal to help them perpetrate their deeds.

Security tools and penetration tests in particular allow organisations to think and act like hackers - and hopefully outsmart them.

## Comment Article

---

### About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at  
<http://www.quocirca.com>

# Comment Article

---