# OWASP

# Web application security badges

Presented at OWASP London on 3rd April 2008 by Colin Watson

Today's e-commerce websites are labelled with numerous badges/seals to indicate compliance to security, identity, privacy, SSL and other objectives and standards. The 'security badges' are of particular interest, but what are they checking and can they be trusted?

## 1 Introduction

Web application designers and owners have always been attracted to buttons and labels. These were originally limited to declaring the site would work with particular web browsers or matched some World Wide Web Consortium (W3C) standard for web page markup or accessibility guideline. Some went so far as to badge the type of software used for the application or server.

This labelling has continued unabated. In addition to the above, third parties are now offering certification schemes for various security concepts:

- privacy
- secure sockets layer (SSL) certificate validity / SSL use
- identity
- code of practice
- code signing
- reviewed
- policy compliance
- vulnerability tested
- safety for children.

The “vulnerability tested” schemes are of interest since there are many ways to test this, and it is not immediately clear whether these are testing network or application vulnerabilities, or the extent of the tests, or the guarantees offered.

# 2 Badges and claims

The schemes are mainly used on e-commerce enabled websites – no major banking websites have been found which use these. Also, North American websites are much more likely to use the schemes; in some cases websites by the same company in other regions do not have the security labelling. Many of the statistics that are quoted include US dollar values, so it is difficult to tell whether the research has been undertaken in other regions and cultures. One badge scheme is displayed on some shopping search engines.

Seven labelling schemes were identified which appeared to fall into the "vulnerability tested" category. Of these, one is no longer available to join although its badges still appear on some websites. Another was called "security verified" but it was actually a combination identity/SSL badge – not any form of vulnerability assessment.

The remaining five schemes that associate themselves with the security/safe/anti-hackers sphere have been examined. These are variously referred to as trust marks, security badges or certifications. All the schemes comprise of three components:

- automated testing of compliance
- visible date-stamped badge
- method to verify the badge (e.g. a certificate)

and the scheme operators list benefits such as:

- attract shoppers who look for these badges
- greater confidence/trust in the business operator
- increase conversion rate (turn more visitors into purchasers)
- associate the website with a secure and trusted brand
- users have assurance their payment card information is safe
- greater peace of mind for users.

Websites which pass the tests are encouraged to display the badges in a prominent position – towards the upper top left of the screen on the site's home page, catalogue and payment pages. The scheme operators state:

> "… our … security scan ensures web sites, servers, routers, firewalls and Internet-connected devices are free of known vulnerabilities and pass the SANS Top 20 Internet Security Vulnerabilities as defined by SANS, the FBI and FedCIRC"
>
> "… a site that has passed … has also met the security scanning standards of Visa, MasterCard, American Express, and Discover"
>
> "… mark to appear only when a web site's current security status meets the highest published government standards"

> "… our security seals are backed by the latest advances in website scanning technology, vulnerabilities reporting portal – and our own ever-vigilant specialists"
>
> "… certification can make the difference as to whether or not they will make purchases at your site"
>
> "… set and forget - after the simple configuration process, … will help make sure your servers are secure and will prove this fact to your customers"

Testimonials, comparative trials and independent reports do appear to support these claims, but what are the website's owners and users actually getting?

# 3 Comparison

All the schemes rely on the website owner supplying relevant network addresses correctly. If a website or application spans multiple network addresses, all of these should be examined, although it is up to the website owner to identify these. Therefore it is quite possible for the security badge to be displayed on a website where some parts of it have not been tested.

The labelling schemes were operated against a public-facing test website which included registration, restricted access areas, an administration facility and some parts of the site required the use of SSL. The single web server IP address was submitted. The website was not subject to traffic management such as load balancing, nor protected by a web application firewall ("layer 7" firewall) although it did sit behind a stateful network layer firewall – a typical arrangement for many simpler website hosts.

Vulnerability scans need expert interpretation. All five schemes reported the website was not vulnerable after some false positives, where vulnerabilities are detected incorrectly, such as information disclosure had been removed. In one of the tests, the scan identified an issue which would only have been possible if the server was running a different operating system. Three of the schemes also provided information on the network scanning requirements for Payment Card Industry Data Security Standard (PCI DSS) indicating that the website (network) was compliant. Interestingly two of these were actually aborting their scans due to the firewall blocking their source IP addresses during aggressive port scans, so they did not actually complete their tests.

Only two of the schemes undertook any form of application vulnerability testing – the others were performing network-type vulnerability testing. The schemes used Nmap, DNS queries, tracerouts, pings and scanners based on Nessus and Nikto. These are tools used by security professionals, but manual web application testing would perform additional tests.

Of the two schemes which undertook application vulnerability testing, both tried to enumerate additional unlinked resources but only one actually attempted to modify input data and add additional parameters. Neither had the extent and depth of modern desktop "web application scanner" tools.

Apart from regular daily automated scans to determine scheme compliance, four allowed manually initiated scans with the ability to modify some parameters. There

was no consistency in what could be configured.

# 4 Trust

The labelling relies on the schemes being trusted by website users. There are no certification authorities such as with SSL certificates, so the schemes either need a recognisable name or high market share for this to occur. However, the majority of internet users don't understand, or want to know about, certification authorities.

There is no consistency between the various schemes - they do not provide identical findings when tested on the same website. The testing can easily be incomplete or unfinished. There is no-one verifying these badges mean anything. Therefore, they may be undermining the efforts of other security practitioners.

Some of the badge services are provided by companies who are also an Approved Scanning Vendor (AVS) under the PCI DSS. PCI DSS has certainly raised the profile of security issues with the many organisations that handle payment card data and the security badge businesses have been quick to extend their offerings into this area.

Websites displaying the badges have not necessarily passed all the current tests and some sites displaying the badge have been hacked. Although most of the schemes remove the badge when a daily scan finds a problem, in some cases, it can take more than a week to lose the badge status, although repeated infringements are likely to be frowned upon due to the potential effect on the labelling scheme's brand. There is also a risk that problems on someone else's website could undermine confidence in the labelling scheme and thus have a negative effect on another website's performance.

These badges say nothing about malicious insiders or external malicious users who may access privileged information and use it in an unauthorised manner. The labelling schemes say themselves that they cannot guarantee 100% security and state something like "99.9% secure" but it's not clear how that is calculated. There is also a degree of interpretation allowed for some vulnerabilities – once a vulnerability has been identified, a website owner can request for it to be nulled if they consider it a false positive or invalid in some way. It is not impossible to envisage a future complaint to the Advertising Standards Authority about the labelling claims on UK e-commerce websites.

It is true that security organisations often state that "99% of all network exploits leverage known vulnerabilities" but in the web application world where almost every e-commerce website is coded differently, these statistics make little sense. Users do not differentiate and perhaps are concerned with the overall security of the website (including the application, network and hardware), not solely network exploits.

# 5 Conclusions

The schemes are useful - they could identify many vulnerabilities at a very competitive cost. But the results need careful consideration, perhaps adjustment, and interpretation to prevent misunderstandings and ensure the website owner doesn't have a false sense of security. A website which has one of these security badges is not necessarily vulnerability-free (or even fully tested). In the same way, an e-

commerce application which complies with the PCI DSS doesn't necessarily mean it is immune to payment card data theft. The schemes should be configured and used with care with all the help on offer to ensure they are checking what's expected.

The main problem appears to be with the marketing message. Despite the badges appearing on website pages, most of the schemes are not testing for application vulnerabilities. Therefore there is a difference between the impression that most website users (and some owners) will have compared with the reality. In addition, the labelling schemes seem to suggest "safety from hackers" – a promise which cannot be delivered. With time, it is almost always possible to find another vulnerability.

Other types of labelling schemes for privacy, identity, certificate validation and so on, dilute the security message and website users are probably not necessarily able to tell the difference easily.

There are some notable scanning vendors who do not offer any form of security labelling. Therefore it is likely that other security vendors may enter the market, and these will probably be more focused on application testing, although it would add further fragmentation to the market.

In the meantime, the current security labelling schemes are therefore primarily marketing tools, not necessarily evidence of good security practices or of websites safe to use. They will be of use to online retailers whose names are less well known or whose competitors are already labelled. Robust website security requires applying security thinking to all stages of planning, design, development, testing and operation – not security labelling.

# 6 References and further reading

1. PCI Certification doesn't make a website harder to hack

http://jeremiahgrossman.blogspot.com/2007/06/pci-certification-doesnt-make-website.html

2. 'Hacker Safe' seal: Web site shield, or target?

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9057878

3. Picking Apart The Hannaford Breach- What Might Have Happened

http://securosis.com/2008/03/18/picking-apart-the-hannaford-breach-what-might-have-happened/