

## Security Breach Causes PCI SSC to Issue Statement

In response to a recent security breach at the retailer TJX Cos. Inc., who operate the TK Maxx and Marshalls chains, the Payment Card Industry Security Standards Council (PCI SSC) has issued a statement reiterating the importance of all businesses involved in handling payment data to do so with the utmost vigilance and to comply with their recently revised Data Security Standard.

It is thought that the breach at TJX may have resulted in the compromise of millions of credit and debit cards (<http://www.iht.com/articles/2007/01/19/business/data.php>) and could cost the company hundreds of thousands of dollars in fines from regulators and payment associations.

The mission of the PCI SSC, founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, is to enhance payment account security through adoption of the Payment Card Industry's Data Security Standard. The Standard contains twelve sections based around:

- Building and maintaining a secure network;
- Protecting cardholder data;
- Ensuring the maintenance of vulnerability management programs;
- Implementing strong access control measures;
- Regularly monitoring and testing networks; and
- Ensuring the maintenance of information security policies.

It is mandatory for all organisations involved in the storage and processing of payment card information to comply with the Standard. Failure to do so can result in financial or operational consequences being imposed by individual payment brands.

The Data Security Standard currently at version 1.1 (as of February 2007) and supporting information can be found at <https://www.pcisecuritystandards.org/>. Eurotek, in conjunction with our strategic partner Westpoint Limited, a PCI Approved Scanning Vendor, can offer a regular vulnerability assessment service that satisfies the requirements of the Data Security Standard.

## Vulnerabilities increase by 34% !

With the advent of 2007 the Computer Emergency Response Team (CERT) have been able to release their latest vulnerability figures. During 2006 the number of vulnerabilities reported to them rose by 2074, up from 5990 in 2005 to 8064 – an increase of 34%.

## Vulnerabilities explained: Cross-Site Scripting

### What is the impact?

Websites vulnerable to Cross-Site Scripting (abbreviated as XSS) make it possible for attackers to maliciously change the content that visitors see when they follow a specially prepared link. In doing so, login credentials and other information which legitimate visitors have stored on the website may be stolen, or the appearance of the site can be changed in other ways which are damaging.

### How does this work?

Websites consist of HTML code, a mixture of text and "tags" in angle brackets which tell the web browser how to render the page, e.g.: `<font color="red">This text will appear red</font>`

Another such tag is the `<script>` tag, which makes it possible to embed fragments of JavaScript code in a webpage. This code can make the browser perform actions such as showing a popup window, redirecting the user to a different URL, or changing any part of the page currently being viewed. Embedded script code is widely used in websites nowadays to provide modern interactive "web 2.0" features, but it is also vital to XSS attacks as we shall see.

Consider a common website facility such as a search box which allows visitors to search for products in a catalogue. When a user enters a query (e.g. "widgets") and clicks search, the results page often includes the user's original query, e.g. "100 results found for widgets". What if the user enters `widgets<script>alert('Vulnerable')</script>`?

If the website is vulnerable to XSS, the user's query would be included verbatim in the HTML code of the results page, including the `<script>` tag, which would make the user's browser pop up a window containing the text Vulnerable. XSS attacks do not require users to manually visit websites and enter things into search boxes – this can be automated by crafting a URL containing the exploit, e.g.: `http://ww.example.com/search?query=widgets<script>alert('Vulnerable')</script>`

This URL could be contained in an email the attacker sends to intended victims, or placed on another website. When a victim is duped into clicking on the link, this would directly bring up the search results page including the embedded malicious code.

### Why is this a problem?

The pop-up window example used above is harmless: real XSS exploits can include script code that (for instance) submits the user's login cookie for the vulnerable website to the attacker. The victim's stolen cookie can then be used to login to the targeted website as the victim.

Another exploit would be to embed script or HTML code which makes the victim's browser display a spoofed login page instead of the vulnerable website's real content.

Many victims may be duped into entering their login details into this spoofed page, which would then be submitted to the attacker.

Other types of malicious content that could be injected would be inappropriate images or fake news items. This is particularly problematic if the XSS is "persistent", i.e. the website allows users to submit text (including malicious code) that will then be seen by other users.

It is important to note that being vulnerable to Cross-Site Scripting or HTML injection does not mean an attacker can immediately penetrate the security of a website and steal data; rather it makes it possible to craft an exploit which will facilitate theft of credentials or data, or cause other damage if users can be duped into clicking on maliciously crafted links.

### Cross-Site Scripting in the news

Cross-Site Scripting vulnerabilities have recently been disclosed (and fixed) on several Google websites (1),(2). These are all the more critical as Google lets users use a single account across multiple services (such as Gmail

and Google Docs & Spreadsheets), with most of these services storing personal information such as emails, contacts, documents, search histories, etc.

If even one site under the Google domain (google.com) such as base.google.com is vulnerable to XSS, this means that the user's google.com cookie can be stolen and all of that user's data stored on other Google services may be compromised.

PayPal has also had XSS vulnerabilities(3) which are known to have been exploited (4). Maliciously crafted links followed by victims made Paypal.com display spoofed content which prompted users to enter sensitive account details. These spoofs are all the more convincing as they actually appear on the genuine Paypal.com domain which users inherently trust, rather than on spoof domains (such as paypal-accountverify.com) which are commonly used in "phishing" attacks and are more easily recognised as being fake.

Adobe Reader 7, a piece of software for viewing PDF files which is installed on millions of PCs worldwide was also recently found to be vulnerable to an unusual XSS flaw(5). Rather than being a vulnerability in a website, this flaw makes it possible to craft a URL pointing to a PDF file on the local machine or any remote website which can contain script code, which will be executed in the context of the local machine or the remote website.

This means that if the attacker knows the name and location of any PDF file on the victim's computer, and the user (who's using a vulnerable version of Adobe Reader), clicks on a malicious link, this can submit the contents of any file from the user's PC to a remote site. If a website contains a PDF file anywhere, a malicious link can be crafted to this file which is able to steal the user's cookie for that website.

### Cross-Site Scripting: How (not) to fix it

The fundamental issues involved in XSS have been known for over 10 years. Exploits on major sites occurred as early as 1986, however it is still common to find XSS vulnerabilities in new websites and web applications in 2007.

Firewalls offer no or only limited protection against XSS. Most firewalls simply block ports and do not act on the application (HTTP) layer at all; even those that do only offer limited protection, as there are many ways to circumvent automated detection of XSS. SSL encryption (HTTPS) also does not protect against XSS. It simply encrypts data between the user and the web server; this data can still contain malicious code.

The best approach to managing the risk of XSS is first to determine if your web applications are vulnerable to such exploits. This can be achieved with regular vulnerability assessments. These assessments need to be regular as new XSS exploits are being discovered all

the time. Ideally the assessments should follow a blended approach to testing, using a combination of automated tools and manual checking.

Using automated tools alone to detect XSS is prone to both false negative and false positive results.

If your applications are vulnerable to XSS attacks then their source code will need to be modified, which is generally easy to do. The issue that causes XSS vulnerabilities in source code in the first place is often one of education – web developers who are very capable of designing attractive websites may lack awareness of security issues, and so do not take the necessary steps to mitigate against common vulnerabilities such as XSS or SQL injection.

The fundamental technical issue lies in the treatment of user input: input supplied by the user must always be “sanitised” and should never be included verbatim in the output of a website. Characters such as angle brackets (which are required to inject HTML or script tags) can be filtered out or “quoted” (turning > into &gt; and < into &lt;) so that they still appear when viewing the page, but do not work as HTML tags.

These kinds of fixes are easy to implement. Many modern web development frameworks (such as ASP.NET7) also include features which make it very easy to avoid the problem.

(1) **“Google XSS Vuln”**

<http://ha.ckers.org/blog/20061213/google-xss-vuln/>

(2) **“Cross Site Scripting Vulnerability in Google”**

<http://ha.ckers.org/blog/20060704/cross-site-scripting-vulnerability-in-google/>

(3) **“PayPal XSS Exploit available for two years?”**

[http://news.netcraft.com/archives/2006/07/20/paypal\\_xss\\_exploit\\_available\\_for\\_two\\_years.html](http://news.netcraft.com/archives/2006/07/20/paypal_xss_exploit_available_for_two_years.html)

(4) **“PayPal Security Flaw allows Identity Theft”**

[http://news.netcraft.com/archives/2006/06/16/paypal\\_security\\_flaw\\_allows\\_identity\\_theft.html](http://news.netcraft.com/archives/2006/06/16/paypal_security_flaw_allows_identity_theft.html)

(5) **“Cross-site scripting vulnerability in versions 7.0.8 and earlier of Adobe Reader and Acrobat”**

[http://www.adobe.com/support/security/advisories/apsa\\_07-01.html](http://www.adobe.com/support/security/advisories/apsa_07-01.html)

(6) **“Hotmail flaw exposes passwords”** (August 24, 1998)

<http://news.com.com/2100-1033-214787.html>

(7) **“How To: Prevent Cross-Site Scripting in ASP.NET”**

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/PAGHT000004.asp>

## Shouldn't you be taking a serious long term view of your I.T. Security?

According to CERT just over 8000 security vulnerabilities were reported in 2006. That's 670 new vulnerabilities every month, 155 per week, or 22 each day.

The majority of these vulnerabilities are targeting your business critical applications.

Firewalls can do very little to protect against application layer vulnerabilities.

**The Solution:** Our Managed Vulnerability Assessment Services.

To stay on top of these vulnerabilities and ensure they're not exploited take our annual managed vulnerability assessment service. Each month, or more frequently, we will run a comprehensive up-to-date set of non-destructive security tests to determine how vulnerable your key Internet facing business assets are.

Our monthly findings are presented in an easy to view HTML report that contains corrective actions, management overviews and executive trends.

For organisations that want to actively reduce the business risks they face, our managed vulnerability assessment services can provide many benefits:

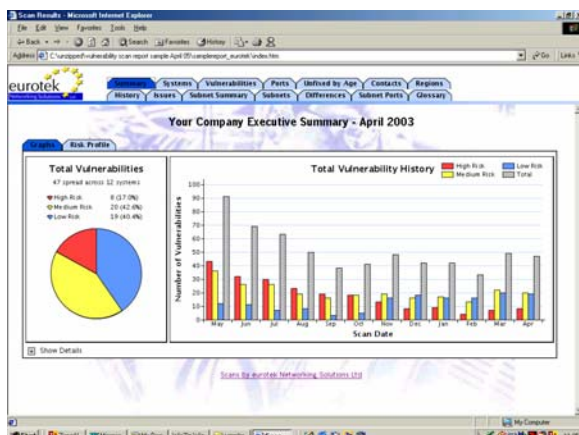
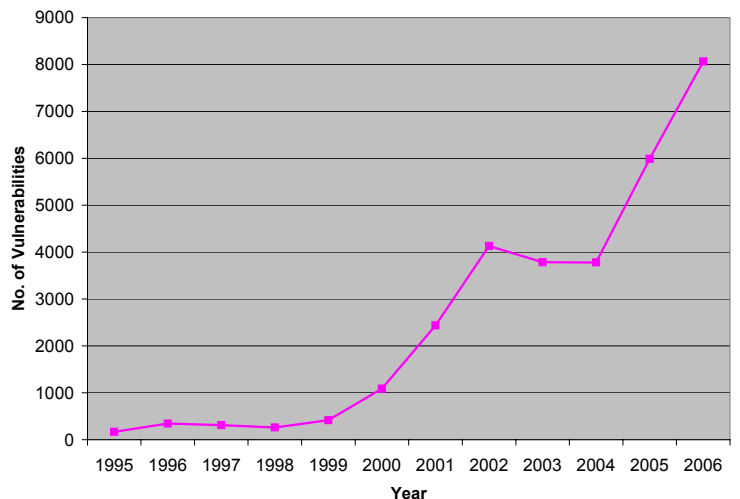
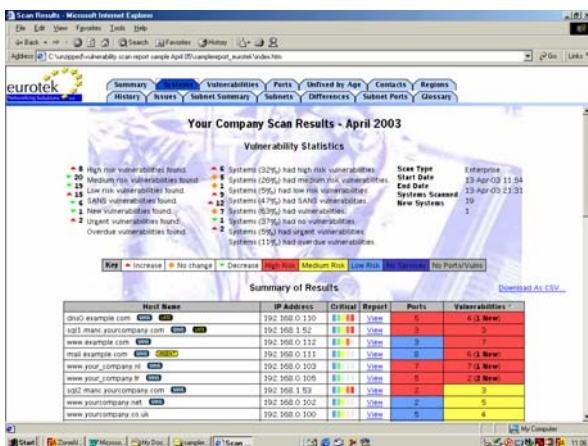
- Ongoing protection against the latest security exploits
- Guards against human error, e.g. developers' software bugs, server or firewall misconfiguration
- Verifies effectiveness of other security controls and policies
- Prevents security breaches and thereby:
  - Protecting your company's reputation, (reducing adverse media coverage, customer dissatisfaction, loss of public confidence etc.)
  - Reduces costs (fewer security incidents from which to recover, fewer compensation or litigation claims etc.)
  - Demonstrates 'best practice' in addressing risk (Turnbull, Basel Capital Accord, ISO17799, Sarbanes Oxley), and meeting Corporate Governance objectives
- More cost effective than doing it 'in-house'
- Frees up staff to concentrate on core business activities
- Very low management overhead

Our Enterprise service is a full vulnerability assessment service examining the vulnerabilities presented by your Internet-reachable systems. The service lasts for one or more years (renewable), and assessments are performed typically every month. Features include:

- Manual verification of target address details before scanning takes place
- Flexible scheduling options for scan commencement
- Blended assessment approach (automated and, manual)
- Full TCP port scan, reliable scanning of well defined UDP services, and ICMP scanning
- Thousands of application layer security tests, each with suggested fixes
- All tests are kept fully up to date and are non-destructive
- 'Crystal box' testing methodology means tests can be customised to suit your environment
- Easy to view HTML report of findings, free from false positives.

**"Eurotek's Network Security services and on-going Vulnerability scanning and reporting have ensured that we keep on top of threats and maintain Data and I.T. integrity"**

**DARREN SMITH : IT OPERATIONS  
THE ROYAL INSTITUTION OF  
CHARTERED SURVEYORS**



**"How vulnerable are you today...tomorrow...next week...next month?"**

For further details on the products and services mentioned in this news letter, plus our full portfolio please visit: [www.euroteknetworking.com](http://www.euroteknetworking.com) or call: 01908- 565608