



# The 7 classic misconceptions about Web Application Security

**Although in the meantime word has got around that web applications are the favoured entrance gates for hackers at the moment, some experienced administrators are still sticking to their misjudgments. The following article does away with the seven classic misconceptions.**

## **Misconception #1**

**“Our web applications do not allow any access to our systems.”**

Data is often accessed in a targeted or professional manner in secret and via hidden paths - web applications in particular give hackers diverse opportunities for data theft and are therefore among their preferred targets today. This is hardly surprising because web applications, by their very definition, provide an electronic interface to data and transactions.

While in the past confidential information and critical transactions could only be retrieved from behind multiple defense lines, web applications today give a direct access route - even to a company's most important information. So there is no other place where hackers are closer to their desired target than with web applications. All it takes is just one weak spot on any level for them to be able to launch successful attacks.

Targeted information theft is therefore now the order of the day, unlike in the past. Things have changed and it is no longer the case that exploits are written that steer towards security loopholes in random targets. Instead an interesting target is brought out of sync using technical manipulations until such a point as that the required data has been extracted. Even classic manipulation methods such as forceful browsing, cross-site-scripting, SQL/ command injections or the exploitation of business logic weak spots can result in successful attacks with three quarters of all web applications.

Targeted data access of this kind cannot be detected via the signature and reactive security protection systems such as an IDS (intrusion detection system) or IPS (intrusion prevention system) cannot prevent such attacks. One of the greatest misunderstandings

here is that it is not just the data used by the web application that are in danger if an attack is successful. All systems and interfaces that are linked to the web application are potentially affected.

It is not uncommon that a company's entire internal data can be stolen via a seemingly harmless web application, such as for example, a help site or a company's telephone book.

Attacks of this kind on the application level have increased with the popular Web 2.0 technology. These highly dynamic web applications, which distribute contents from other users thousand fold, are increasingly being used by organized cybercrime groups.

A current security report on cyber criminality shows that this problems needs to be taken seriously. The report states that about 25 percent of all companies have already fallen victim to various attacks that were initiated from Web 2.0 sites such as Xing, MySpace or Facebook.

Effective protection against unauthorized data access is provided by so-called web application firewalls (WAFs) between the user and the web application which only allow valid URLs and as such guard backend systems against illegal access.

---

1... Sophos-Security Threat Report - July 2009 update:  
<http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jul-2009-na-wpus.pdf>



# The 7 classic misconceptions about Web Application Security

## Misconception #2

“The web applications’ security must be ensured at the development stage.”

Of course application developers cover security aspects such as logic, precise authentication or data processing in the development. However, in the subsequent deployment the solution is always part of a more complex IT landscape upon which the developer no longer has any influence.

Connected components such as the operating system, libraries, middleware web servers or a database pose their own respective security risks. On top of this, developers can only take account of those risks that are known at the time of application development. However, by the time a project is deployed, it may be faced with attacks on the web applications which were still unknown during the development period.

Although remedies can be provided with software updates and new application versions, the security precautions can often not be updated fast enough. In order to be able to react quickly and safely to unforeseen threats, preinstalled web application security precautions should be combined with a preceding WAF. Unfortunately, often sensible precautions in the application development and the WAF deployment are played off against each other. However, companies must realize that the only way of achieving effective and efficient protection is to combine the two.

## Misconception #3

“We encrypt our entire data traffic with SSL (HTTP/S) and that is enough.”

The SSL network protocol guarantees safe data traffic between the user, or the web-browser and the server, but does not safeguard the actual server itself. It is incredibly important to protect the confidentiality and integrity of transferred data on the public, untrustworthy internet.

Hackers also take advantage of this protection and this is how their attacks reach right up to the company web server “safely” and in encrypted form.

In order to detect these attacks early enough SSL-encrypted connections must end - at the latest - at the company boundaries. Powerful WAFs provide the required controls at this point.

As a guarding authority between the user and the application the WAF initially stops the incoming data traffic before it is filtered and forwarded using a multilevel routine.

Only authorized user queries that have been subjected to multiple checks can reach the web server via this intermediate stage. Once the authorization has been granted the WAF can send the SSL-encrypted data on if the backend server knows to expect SSL queries. If a WAF assumes these security functions, then the load on the server is relieved and as a result the applications’ performance on the server increased, for example.



# The 7 classic misconceptions about Web Application Security

## Misconception #4

"Our systems always work with the latest patch versions and we run an automatic scan on a regular basis, so all lights are green."

Automatic scanners give a fundamental overview of weak spots in a company's IT - they do not, however, detect most of today's attacks on web applications.

Hackers may still have penetrated the web applications undetected despite inconspicuous scanner results. The use of a professional penetration test is therefore recommended in order to uncover any targeted data theft. A test of this kind measures the security level of the application environment, but should also always incorporate checks for manual attacks which are based on reverse engineering (exploitation of knowledge about internal system structures) and be conducted once or twice a year.

Automatic security scanners and penetration tests check the current status of a system architecture and are always only snapshots, i.e. they do not provide any proactive system protection.

The corresponding updates or patches are often not directly available for customer-specific weak spots.

By deploying WAFs companies can react directly to a detected leak in the sense of "virtual patching" and block unauthorized server queries.

This gives a company the time to implement a orderly update in the background.

## Misconception #5

"Our web applications are secure; nothing has ever happened here."

This presumption is risky because the user often labours under false security.

According to Gartner, three out of four web applications is open to attack, whereby three quarters of all attacks today are targeted at web applications.

On top of it all, hacker attacks on web applications often don't leave any tracks and remain undetected because the data does not disappear or is not changed - all applications continue to function normally and no system accesses are recorded.

Current perceptions still seem to be shaped by the viruses and Trojans from years gone by when an attack always resulted in obvious consequences.

The aim of current attacks is to steal data without being detected. There are no previously known signatures for targeted attacks of this nature. Dynamic protection that is adapted to a specific application and not thousands of reactive, often outdated signatures is required here in order to be able to counter these attacks.

In addition to general data protection, security solutions with PCI DSS protection also fulfil the legally binding Compliance Regulations applied for processing credit card transactions by service providers in the financial or eCommerce sectors.



# The 7 classic misconceptions about Web Application Security

## Misconception #6

"We have been subject to attacks, but no data was stolen."

Statements of this kind are often reported about in the media when a system's weak spot becomes public.

The problem is that electronic data theft cannot normally be differentiated from normal application access. As a result, the company cannot know if someone has been copying data electronically via a weak spot for a long time already - after all, this kind of attack does not leave any tracks.

Unlike viruses or Trojans which were still in circulation a few years ago, the systems are not affected by these targeted attacks and continue to run as normal for the user.

So the most effective method is the proactive system protection with security solutions that have several security levels. The most important filter is the authentication query posed to the user which precedes the applications. This ensures that access is only granted to authorized people who can then interact with the application server.

The next important level is the dynamic filtering which only allows valid server queries without relying on signatures. Accesses and data requests can also be traced precisely via the registered ID numbers using a reporting function. Condition: A reverse proxy server has to be installed in front of the web application servers and intercept network connections and network protocols such as SSL.

## Misconception #7

"We already use a reverse proxy server and deploy the best and most expensive firewalls, even two different ones one behind the other."

Network firewalls check the data traffic to the web server or rather, the signatures and protocols of the user queries to the server, in real-time if possible.

But at best, the firewall can only detect simple attacks using predefined signatures. In order to identify the hacker attacks, which are normally camouflaged, a firewall must at least be able to access encrypted data, which is usually not the case. Effective protection for web applications which goes beyond pure URL signature filtering must also be able to address application-specific issues such as preceding authentication, cookie protection and URL address protection as well as HTML forms too. The access route via manipulated URLs must also be blocked. Only web application security solutions which filter all queries and data at the access point to web applications on multiple levels -both statically and dynamically - provide proactive protection against hitherto unknown attacks.