



## The 7 classic misconceptions regarding Web Application Security

By now it's a known fact: Web applications are hackers' preferred entrance gates at the moment. Nevertheless some experienced administrators are still sticking to a number of misconceptions. This article does away with the seven most frequent ones.

### Misconception #1

«You can't get access to our system through the web.»

Data is often accessed in a targeted, professional manner via secret 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 accessed behind multiple defense lines, web applications today offer 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. Things have changed and it is no longer the case that exploits are written to profit from quarter security loopholes in random targets. Instead an interesting target is brought out of sync using technical manipulations until the desired data can be 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 for three quarters of all web applications.

Targeted data access of this kind cannot be detected via the signature. 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 is in danger if an attack is successful. All systems and interfaces 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 a help site or a company's telephone directory.

Such attacks on the application level have increased with the popularity of Web 2.0 technologies. New, highly dynamic web applications, which distribute content from other users thousand-fold, are popular targets for organized cybercrime groups.

As a recent security report on cyber criminality shows, this problems needs to be taken seriously. The report states that about 25 percent of all companies have already fallen victim to attacks 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's browser and the web application, which only allow valid URLs and as such guard back-end systems against illegal access.

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

## Misconception #2

«Web application security must already be ensured during development.»

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

Components such as the operating system, libraries, middleware, web servers or databases pose their own respective security risks. On top of this, developers can only take into account those risks that are known at the time of application development. However, by the time a project is deployed, it may face attacks which were still unknown during development.

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, pre-installed web application security precautions should be combined with a preceding WAF. Unfortunately, sensible precautions in the application development and the WAF deployment are often played out against each other.

However, companies must realize that the only way to achieve effective and efficient protection is to combine the two.

## Misconception #3

«We encrypt our entire data traffic with SSL (HTTPS) and that is enough.»

The SSL network protocol guarantees safe data traffic between the user's web-browser and the server, but does not safeguard the actual server itself. Protecting the confidentiality and integrity of transferred data via the public, untrustworthy internet is of great importance.

However, hackers also take advantage of this protection to ensure that their attacks reach the company web servers «safely» and in encrypted form.

In order to detect these attacks early enough, SSL-encrypted connections must end at the company boundaries. Powerful WAFs provide the necessary control 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 over multiple levels and then forwarded to the application server.

Only authorized user queries which passed multiple checks can reach the application server via this intermediate stage. Once the authorization has been granted, the WAF can then re-encrypt the data to send it to servers which expect SSL traffic.

Having a WAF assume these security functions decreases server load and as a result also increases application performance.



#### 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 provide an 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. These tests measure 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).

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. They should therefore be conducted once or twice a year.

Updates or patches for newly found vulnerabilities are often not immediately available. By deploying a WAF, 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 an orderly update, while still being protected.

#### Misconception #5

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

This assumption is risky because the operator often works under a false impression of security: According to Gartner, three out of four web applications are open to attacks, whereby three quarters of all attacks today are targeted at web applications.

On top of this, hacker attacks on web applications often don't leave any tracks and remain undetected, because the data is not deleted nor 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 past years, where 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, rather than relying on 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 fulfill the legally binding Compliance Regulations for processing credit card transactions by service providers in the financial or eCommerce sector.

Companies must become aware of the fact, that only the combination of reasonable measures in application development and the use of a Web Application Firewall brings effective and efficient protection.

## Misconception #6

«We were attacked, but no data was stolen.»

Statements of this kind are often reported in the media when a system's weak spots become public.

The problem is that electronic data theft cannot normally be differentiated from normal application access. As a result, the company will not know whether someone had access to sensitive data via a vulnerability for a long time already – after all, this kind of attack does not leave any traces.

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

The most effective protection is therefore provided by proactive systems with multi-level security solutions. The most important filter is the authentication query posed to the user, preceding the applications. This ensures that access is only granted to those authorized to 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, usually in real-time.

But at best, the firewall can only detect simple attacks using predefined signatures. In order to identify 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 beyond pure URL signature filtering must also be able to address application-specific issues such as preceding authentication, cookie protection and URL as well as HTML form protection. 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 so far unknown attacks.