

# [REVS] Security Considerations for Web-based Applications

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0018.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 02/06/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 6 Feb 2005 17:59:42 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Security Considerations for Web-based Applications

---

## SUMMARY

The white paper linked here suggest several rules-of-thumbs to handle common risks to web sites and web-based applications. The paper focuses on ways to design a web based system to be better protected against common risks such as: Phising, Cross-Site-Scripting, SQL Injection and more.

## DETAILS

### Understanding the Threat:

Attackers have an ever increasing number of vectors in which they can manipulate poorly thought-out and implemented online services. The consequences of this ranges from the erosion of customer confidence in the online offering, through to the manipulation and eventual compromise of the hosting environment. To understand the necessity of improving the processes in which an organization selects host names for their Internet services or references URL's within a web-based application, a study of key threats and the attack vectors that abuse them is required. This section focuses upon the techniques currently used by attackers to construct their attack.

### Which Threats?

Depending upon an attacker's motivation and the sophistication of the online service, there are a large number of threats which an organization may be exposed to. However, by focusing upon the threats that can make use of poorly implemented host naming procedures or web-application URL referencing, the number becomes more manageable. Threats that traditionally make use of poor host naming and URL referencing include:

- \* Phishing – use of an electronic message (e.g. email, web banner advertising, instant messaging) to socially engineer a customer into following a disguised or obfuscated URL. The URL leads to a host controlled by the attacker in which they seek to harvest customer authentication details. See *The Phishing Guide* by the author for a comprehensive analysis of this threat.
- \* Cross-site Scripting – manipulation of a web-application's URL designed to cause an attackers code (hosted at an alternative site) to be executed within the customers web-browser. The attacker may choose to inject malicious content with the purpose of discrediting an organization, or seek to actually compromise the customer's host.
- \* Preset Session Hijacking – the hijacking of a customer's interactive session after they have authenticated themselves using a SessionID specified by an attacker within an insecure URL. The attacker subsequently gains interactive access to the logged in session and may carryout application functions as if they were the real customer.
- \* Bot-Net Building – similar to Phishing however, the attacker's purpose is to compromise the customers host and install a remotely controllable agent rather than merely harvest authentication details. Depending upon the nature of the bot installed, the attacker may also monitor all network traffic and subsequently capture customer authentication details used for multiple online services.
- \* Mistyped Names – many customers mistype host names and registered domains. An attacker may register permutations of an organizations domain to capture these mistypes and direct them to an application of their choice. This alternative application may be used to discredit the organization or seek to impersonate it with the aim of capturing customer authentication details.
- \* SQL Injection – abuse of poor data handling processes that causes an attackers code submitted through a URL to be executed by the applications backend database server. Through this vector, an attacker may choose to steal or corrupt the data contained in the database, or seek to compromise the database host.

### Best Practices:

The secret to protecting against all of the threats and attack vectors explained in the previous section is by adopting a robust and comprehensive defense-in-depth posture. While there are no silver bullets

Securiteam: [REVS] Security Considerations for Web-based Applications

in information security, the inclusion of well thought out and implemented best practices can significantly contribute to an organizations ability to thwart many aspects of these attacks. In many cases, it is often the adoption of the simplest and most basic security best practices that have the greatest impact in helping to secure an organization and the multiple Internet-based services it offers.

At a fundamental level, the process of keeping host names as simple and recognizable as possible combined with the use of short URL's for referencing application components can appreciably contribute to the overall security of an organization's online service. Customers and clients must be able to tell at a glance exactly which service offering they are connecting to, and have confidence that they are not succumbing to a fraudulent link.

Obtaining the Paper:

The paper can be found at:

<<http://www.ngssoftware.com/papers/NISR-BestPracticesInHostURLNaming.pdf>>  
<http://www.ngssoftware.com/papers/NISR-BestPracticesInHostURLNaming.pdf>

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.ngssoftware.com/papers/NISR-BestPracticesInHostURLNaming.pdf>>  
<http://www.ngssoftware.com/papers/NISR-BestPracticesInHostURLNaming.pdf>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.