

[REVS] Best Practices for Secure Development

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0090.html>

From: support@securiteam.com

Date: 10/31/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [REVS] Best Practices for Secure Development

Message-Id: <20011031154638.89796138BF@mail.der-keiler.de>

Date: Wed, 31 Oct 2001 16:46:38 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Best Practices for Secure Development

SUMMARY

The following is an introduction to an excellent article written by Razvan Peteanu on the best practices that should be taken by whoever is planning on building a system that will be accessible through the Internet (or Intranet) and as such will be exposed for a possible attack.

DETAILS

Motivation:

The following referenced document is intended as a guideline for developing secure applications. It is not about how to configure firewalls, intrusion detection, DMZ or how to resist DDoS attacks. In short, it is not about infrastructure and network security. Compared to a year ago, the availability of consolidated material intended for developers has definitely improved but effort is still required to make the developer community more security-aware.

One part of the reason for this lack of security awareness is that traditionally, developers have worked on systems for environments where hacking was not considered a real threat: internal systems, call centers, software for home use, and Intranets. The complexity (and sometimes the

Securiteam: [REVS] Best Practices for Secure Development

unfriendliness) of the applications were adding to the barrier of entry. There may have been occasional exceptions with disgruntled insiders, sometimes with embarrassing outcomes, but they could be dealt with at HR level and the example prevented others from attempting it again.

However, as the Internet has become more and more commercial (after all, this is where the .com comes from), web sites becomes more and more an application. B2C and B2B e-commerce became the buzzwords. There has also been talk about e-government. Cost efficiency has also pushed the market towards an online access only, while traditional channels such as mail or faxes are scrapped. This makes sense for many reasons, but it also brings security to a very personal level. Leaked credit cards are a nuisance but a call to the credit card company can cancel a lost card and repudiate the transactions. Leaked health or credit information has long-lasting effects on the victims and this brings an enormous responsibility on the shoulders of the e-service promoters.

It has also put a pressure on the development community to switch to Internet technologies. Because of lack of security training in traditional programming books and courses, these developers have not been prepared to build systems that withstand a focused attack. And it is not their fault. A single chapter about security in a programming book is not enough, just as one cannot properly learn survival techniques in a single chapter of a mountaineering guide. Such limited coverage also fails to convey the mindset and the skills of the attacker.

We hope this document will fill some of the gap. Do not expect though to be "the only security document you'll ever need". It is and will continue to be a work in progress and your feedback is highly appreciated. Also, make sure you read the other works on this topic (see the Other Resources section). It does not matter where good practices are learnt from as long as they are learnt. You may also find an amount of overlap between this and the other documents. This is expected – after all, "best practices" are not relevant unless they are shared. This document is less intended to be about secure coding as about how building secure systems should be addressed at a slightly higher level.

We will not stay away from code, though but in most cases, we will point the reader to dedicated resources.

The full article is available from:

<http://members.home.net/razvan.peteanu/best_prac_for_sec_dev4.pdf>
http://members.home.net/razvan.peteanu/best_prac_for_sec_dev4.pdf.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:razvan-peteanu@home.com>>
Razvan Peteanu.

=====

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:

Securiteam: [REVS] Best Practices for Secure Development

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.

- **Previous message:** support@securiteam.com: "[NEWS] Downloaded Applications Can Execute Without Warning on Mac IE 5.1 for OS X"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)