セキュアコーディング勉強会

securecoding.jp

AzureStone（あーじゅ・すとーん）

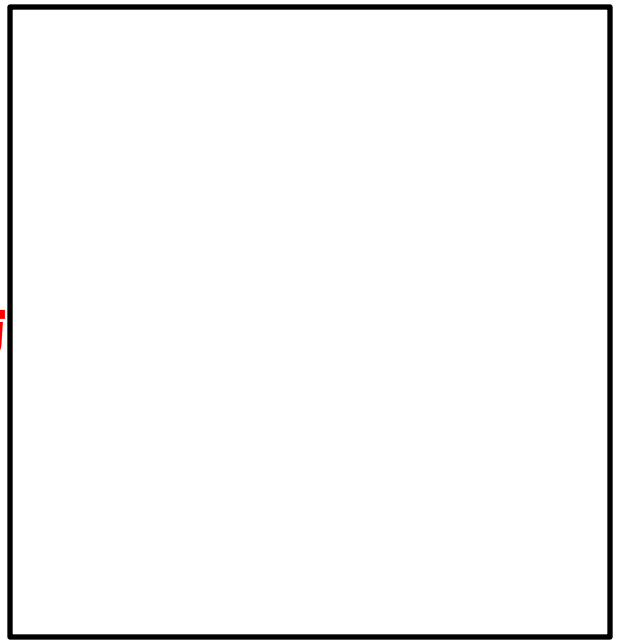
http://www.azurestone.org/

自己紹介

- AzureStone(あーじゅ・すとーん)
- 年齢不詳:何歳に見えます?
- 仕事:システム開発者
  - 開発環境:Linux および Perl および C++
- 執筆活動一年前に多数
  - ハッカージャパン誌 および Software Design 誌
- 住居:こりん星※最近引っ越ししました
  - サーバと生活空間を分離しました。

―昔前の私の状況

- 携帯電話を利用した販促サービスを主とした会社のシステム管理者
- 具体的な業務
  - 社内のセキュリティ対策担当者
  - 情報漏洩確認対応窓口担当者
  - 社内システム管理
- システムを利用するだけの立場



一昔前の私の考え方

- 「セキュア」という名前のついたソフトウェアを使用すればとりあえず問題ない。
  - 例：qmailやOpenBSDの採用
- 「概念」だけ知っていれば大丈夫。
- 「検査」の方法知っていれば大丈夫だ！！
- Windowsは、危険。Linuxなら安全とかいう短絡的発想に基づいていた。

（サニタイズと発言する以上に死語）

現在の私の状況

- システム開発者？
  - コードを書くようになりました
  - OSのセキュリティも見ています
- サポートもしています
  - ある製品のサポートもしています

現在の私の考え方

- 実際、「概念」だけではだめだ！！！
- 多数の脆弱性をつくりこんでしまった。
  - もちろん自分のこと
  - 検査されました。ホワイトボックスとブラックボックスともに・・・。

私の状況の変化

- システム管理者 → システム開発者
- まったくソースコードを読まない環境からソースコードを読む。
- ぷ、ぷぷ、ぷぷぷ、プログラマーじゃないよ！…。
- (;^_^A アセアセ…

真逆な環境

セキュアってなに？

- 現在も答えでていない。
  - 「これは、セキュアなソフトウェアです！」と宣伝するソフトウェアが存在するようだがいったい何をもってセキュアなのかが理解できない。
  - たとえば、●●●●●●とかね。
- 答えが出ていないからこそ、ソースコードを元にそれについて考えてみたい。

そもそもセキュリティなに？

- 機密性
- 完全性
- 可用性

＞＞ｓｋｉｐ

発足の理由

- 前述したように概念を知っているつもりで大丈夫だと安心しコーディングをしたのだが、実際コーディングしてみると脆弱性をたくさん作り込んでしまった。
- 製品（有償）のソースコードを見る機会が増えて見ていくと・・・。自粛

当勉強会の目的・趣旨

- コーディングレベルでいかにセキュアな実装が可能かを勉強することが目的としたセキュアコーディング勉強会です。
  - 例:
    - それソースコードで！
    - それ実装レベルで！
    - それ●●●ライブラリでできるよ！
    - それCPANモジュールで解決できるよ

過去の失敗事例

- office氏事件
  - ちょっとこれは口頭で・・・。
  - (;^__^A　アセアセ…

その結果

- Office氏逮捕・・・。
  - これも口頭で・・・。
  - (;^__^A　アセアセ…

現在、それらを取り巻く状況

- Winny作者逮捕
- 原田ウィルス作成者逮捕
  - 今まで合法とされていたことが合法と認められなくなっている。

    [これはこわい] [これはヤバイ]

やってはいけないこと

- 禁止事項を参照して下さい。
  - http://securecode.g.hatena.ne.jp/keyword/%e7%a6%81%e6%ad%a2%e4%ba%8b%e9%a0%85
- 途中退出や次回参加拒否はありえる

あくまでもソースコードレベル

- 当勉強会は、「セキュアコーディング勉強会」です。名前の通りセキュアなコーディングを勉強する会です。
- 他者の地位・認知度が高い企業に勤めている・大学の教授・自称スーパハカーとかいっさい関係ない。

あくまでもソース(実装)レベル

講師は存在しない

- この勉強会には、講師という概念は存在しません。
  - お客様意識ではなく参加（発言）意識をもってほしいと願っているためです。
- 講師は存在しないが、前に出て喋る人間は、いると思います…。
  - しばらく、AzureStone（あーじゅ・すとーん）が喋ることになるかもしれません…
  - 喋りたい人も募集です。

しかし最低限必要なスキル

- 挨拶をする
  - 「こんばんは！こんばんは！」や「初めまして！」など・・・。**挨拶くらいは**できるようにしてください。

- 禁止事項を閲覧する
  - 参加するからには当勉強会の**趣旨を理解**しかつ禁止事項を**必ず閲覧**しましょう。

実施する内容

- ソースコードレビュー
  - DRYの概念は、別のコミュニティで問うて戴く、あくまでもセキュアかどうか？
- 製品の脆弱性
  - MillwormのExploitCodeを元にどこに脆弱性があったのかを見直す。
  - その他
- 検査方法や自動化テスト
  - 実装した物が、セキュアかどうかを検査する方法
  - 自動化テストの方法

前回（第壱回）勉強会

- 2008年03月21日金曜日
- 19時15分　～　21時15分
- 内容
  - 趣旨の説明
  - 安全にPerlからシステムコマンドを評価する方法

次回（第弐回）勉強会

- 2008年05月30日金曜日
- 19時15分　～　21時15分
- 内容
  - 趣旨の説明
  - PerlのTaintモードについて

まとめ

- 実装レベルで以下にセキュアできるか？どうかを検証する
- 何を持ってセキュアかどうかの答えを出せるようにしていく
- Webに限らずどう脆弱性があるか？
- セキュアなコードを普及させたい！！！！！！
  ！！！！！！！！！！！！！！！！！！！！！！
  ！！！！！！！！！！！！！！！！！！！！！！

お礼

本日は、私の発表を聞いて下さって
誠にありがとうございます。

またこの場を提供して下さった
まっちゃ139の方々
ありがとうございます。

セキュアコーディング勉強会の情報源

- Webサイト
  - http://securecode.g.hatena.ne.jp/
- IRC
  - irc.freenode.net　#securecoding