Webアプリケーションセキュリティ WG

IIJテクノロジー
加藤雅彦

WGのご紹介

- 2004年度 Webセキュリティ調査・検証WGとして発足

- 2004年度の活動
  - 主として攻撃方法とその対策の調査検証
- 2005年度の活動
  - Webアプリケーションセキュリティ WGへ名称変更
  - 啓発コンテンツ、受発注ガイドラインの検討等を行う
- 2006年度の活動
  - ケーススタディによるWebセキュリティ向上コンテンツの作成開始

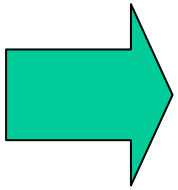
2007年度の目標

- 2006年度の継続として、以下の啓発コンテンツを作成完了させる

「ケーススタディによる
安全なWebサイト構築と運用」

コンテンツの対象・目的

- 対象
  - ユーザ企業
  - 主として中小規模をターゲット
- 目的
  - Webサイトのライフサイクル全般において、セキュリティの重要性への理解を深める



Webアプリケーションセキュリティの認知向上にご利用ください

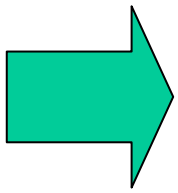
WGの進め方

- 1～2か月に一度のWG開催
  （合計8回開催）
- Webサイトのライフサイクルにあわせ、各フェーズをリレー方式で執筆、メンバーMLで内容をレビュー、リリース

コンテンツ

- JNSA商事がWebサイトを新たに作るというケースを想定
- どのサイトにも標準的にある可能性が高い、「Webでの問い合わせ」「人材募集」をターゲットとした
- 上記のWebサイトを作るために、各サイクルでJNSA商事が行ったこと、その問題点と対策をそれぞれに記述
- 本編の流れは以下の通り
  1. 企画編
  2. 設計編
  3. テスト編
  4. 運用編

詳細はセキュリティ製品バイヤーズガイドへ！



ケーススタディによる安全なWebサイト構築と運用

http://buyers.networkworld.jp/security/

セキュリティ製品バイヤーズガイド

supported by JNSA(日本ネットワークセキュリティ協会)

JNSA会員企業様専用ページへ

製品/サービスディレクトリ

ネットワークセキュリティサービス
- セキュリティ検査・監査・診断サービス
- セキュリティポリシー策定サービス
- セキュリティ教育・トレーニングサービス
- セキュリティコンサルティングサービス
- セキュリティ情報提供サービス
- ウィルス監視サービス
- 不正アクセス監視サービス
- ファイアウォール運用管理サービス
- 電子認証サービス
- コンテンツ監視サービス
- ログ解析
- 損害保険
- 協会／協議会
- その他

アクセス制御／認証
- ワンタイムパスワード
- ICカード／USBトークンデバイス型認証製品
- シングルサインオン製品
- PKI関連製品
- バイオメトリクス
- 検疫
- リスクベース認証

ネットワークセキュリティ
- ファイアウォール／VPN関連製品
- ファイアウォール／VPNログ解析
- 侵入検知／防御
- 統合アプライアンス
- デバイス制御・監視

コンテンツセキュリティ
- ウィルス、スパイウェア対策
- フィルタリング(メール／URL／コンテンツ)
- データベースセキュリティ製品
- フィッシング対策
- シンクライアント
- 文書管理
- 暗号ライブラリ／ツールキット
- アクセス監視、印刷制御

▼文字の大きさ: 標準 大きく

JNSA Press（Web版）：記事一覧

ケーススタディによる安全なWebサイト構築と運用

JNSA技術部会WEBアプリケーションセキュリティWG

運用フェーズ
企画、設計、開発、テストの各フェーズにて様々な問題を抱えたまま、JNSA商事のWebサイトはオープンを迎えました。オープン当初は何のトラブルも発生せず、無事に稼働しているようです。しかし、今まで放置されてきた各フェーズでの問題点はどれもシステムに重大な影響を与えるものばかりです。そしてこれらの多くが運用フェーズに入ってから問題を引き起こします。果たしてJNAS商事のWebサイトはこのまま何事も無く順調に運用されていくのでしょうか・・・？今回は、トラブル発生時における運用フェーズでの問題点やその改善策を検討します。(2008年5月13日)

ケーススタディによる安全なWebサイト構築と運用

JNSA技術部会WEBアプリケーションセキュリティWG

テストフェーズ
今まで企画、設計というフェーズでJNSA商事を見てきましたが、今回はテストフェーズでの状況や問題点、その改善策を検討していこうと思います。今までなんとかスケジュール遅延を起こさずにやってきたJNSA商事ですが、テストフェーズはどうなるでしょうか？(2007年12月19日)

情報セキュリティと仕様のオープン性に関する課題

セコム(株)IS研究所
JNSA PKI相互運用技術WGリーダー　松本　泰

－「IC・IDカードの相互運用可能性の向上に係る基礎調査」から－
(後編)
ICカードのセキュリティの高さの根拠として、よく耐タンパー性などが説明されます。しかし、耐タンパー性や、ICカードで利用されている暗号のアルゴリズム等は、非常に重要な要素ではありますが、それらが評価されているからICカードは安全というのはかなり危ない発想です。それらにより何が保護されているか、どのように保護されているかといったことへの理解がより重要です。(2007年12月5日)

情報セキュリティと仕様のオープン性に関する課題

セコム(株)IS研究所
JNSA PKI相互運用技術WGリーダー　松本　泰

－「IC・IDカードの相互運用可能性の向上に係る基礎調査」から－
(前編)
ICカードのセキュリティの高さの根拠として、よく耐タンパー性などが説明されます。しかし、耐タンパー性や、ICカードで利用されている暗号のアルゴリズム等は、非常に重要な要素ではありますが、それらが評価されているからICカードは安全というのはかなり危ない発想です。それらにより何が保護されているか、どのように保護されているかといったことへの理解がより重要です。(2007年11月21日)

ケーススタディによる安全なWebサイト構築と運用

JNSA技術部会WEBアプリケーションセキュリティWG

ケーススタディによる安全なWebサイト構築と運用

2007年12月19日

JNSA技術部会WEBアプリケーションセキュリティWG

テストフェーズ

今まで企画、設計というフェーズでJNSA商事を見てきましたが、今回はテストフェーズでの状況や問題点、その改善策を検討していこうと思います。今までなんとかスケジュール遅延を起こさずにやってきたJNSA商事ですが、テストフェーズはどうなるでしょうか？
(注:なお、開発フェーズに関しては企画フェーズ初頭で書いたように、すでに安全なWebアプリケーション開発に関するドキュメントが多数出ているため、本連載では割愛させていただきます)

ここまでで色々と問題はあったものの、スケジュールがすでに決まっているということもあり、少々無理をしてでも企画から設計開発へとフェーズを押し進めた結果、なんとか工程どおりに3ヶ月が経過した。開発も完全には終わっていないが、サイトオープンまであと半月と迫っているため、プロジェクトリーダーは開発を続けながら同時にWebサイトのテストを行うこととした。

	1ヶ月目	2ヶ月目	3ヶ月目	4ヶ月目
企画フェーズ	←――→			
設計フェーズ	←―――	―→		
開発フェーズ		←―――	―――→	
テストフェーズ				←―→
サービスイン				▲

1. テスト段階での検討状況

今回の業務アプリケーションを導入するため、関連事業部には出来る限りテストに参加してもらい、問題点を修正してからリリースしたいとプロジェクトリーダーは考えていた。しかし、各事業部は多忙が続いているため、あまり負担をかけるわけにもいかない

そこで、今回新たに導入する人材募集と問い合わせのWebページ開発は単なる機能追加であり開発規模も小さいため、あれこれ検討した末に簡単な内容確認と業務フローの確認だけを行ってもらえるよう、各事業部に依頼することにした。

また、SIベンダーはJNSA商事の業務を熟知しており社内での信頼も厚いことから、受け入れテストは簡単なもので十分だろうと考え、結局のところ以下の機能テストのみを行うということに決めた。

■人材募集

－設計した機能が実装されているかのテスト

- 応募フォームへの入力が可能かを実際に入れてみて確認

コンテンツの反省点

- 概要が中心で、詳細なレベルでの問題洗い出し、対策提示が足りなかった
- 各フェーズの文章ごとに、それぞれ挙げている項目の粒度が異なってしまった (リレー方式の難しさ)
- 主として文章で構成されており、図や絵を多様できなかったため、ぱっと見わかりにくい
- 書き手のバックグラウンドによってこだわるポイントが異なり、解説やストーリーに偏りが出る
- 開発系の話もできれば入れたほうが良かった
- 宣伝がいまひとつ不足していた

まとめ

- 今回ケーススタディという形をとることで、中小規模のユーザ企業が比較的身近にセキュリティを感じることができるコンテンツができた

本コンテンツがユーザ企業のWebセキュリティ向上のヒントになれば幸いです