

アクセス制御機構の機能不全を 検出・検証するシステム

株式会社 ソフテック

SofTek

内容

- ◆ はじめに
- ◆ 開発目標
- ◆ 機能説明
- ◆ 今後の課題
- ◆ まとめ



はじめに

Webシステムに関する現状

Webシステムの
利用頻度増加

電子政府/電子商取引サイトなど
ますます高まる依存度



Webシステムの
脆弱性が潜在化

脆弱な状態での稼動サイトも存在
個人情報漏洩、成りすましの危険性



十分な検出ツール
が存在しない

開発段階でアクセス制御における欠
陥(セッション管理等)が検証できない

効率的な検査を実現するためには？

- ◆ アクセス制御機構の検査システムの開発
 - これまでの問題点
 - 手作業で...外部の監査作業で...
 - アクセス制御機構の欠陥を検査するツールが無い
- ➡ これを改善！

- アクセス制御の欠陥の検出・検証が可能
- 検査効率の大幅な向上
- 開発側と発注側でのクロスチェック



開発目標

開発目標

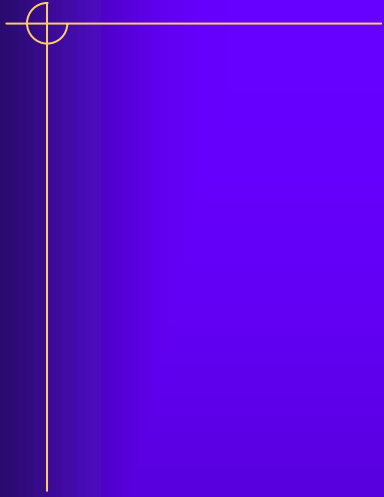
Webシステムにおけるアクセス制御機構の機能不全を検査可能なシステムの開発

- アクセス制御機構の機能不全の検知・検証システムの開発
- 欠陥を有する評価用デモWebサイトソフトウェアの開発

開発効果

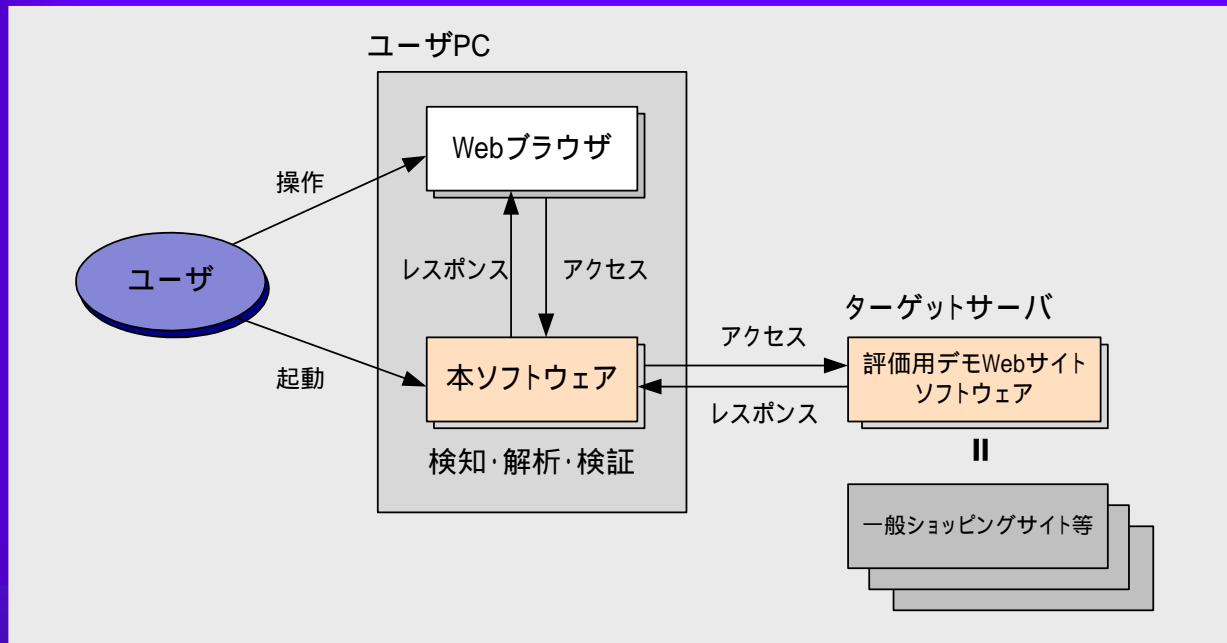
Webシステムの開発段階でWebサイトの脆弱性を事前に検証可能

デモサイトの公開によるアクセス制御機構の欠陥の実際を理解してもらうための啓蒙作業が可能



機能説明

システム概要

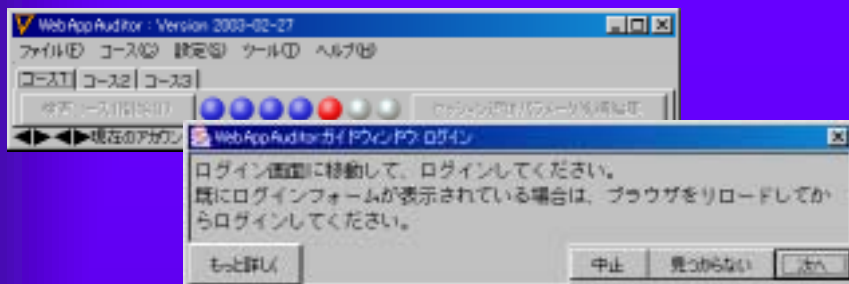


- プロキシサーバとして動作するシステムであり、利用者はシステムからの案内に従いWebサイト上をアクセスすることで検出・検証に必要な情報の収集・記録を行う。
- 収集・記録されたアクセスデータに対する分析結果から、アクセス制御機構の機能不全による欠陥の確認を行う。

開発機能

- ◆ リクエスト/レスポンス記録機能
 - 個人情報に関する送受信データを記録
- ◆ 分析・検出機能
 - 送受信データを元にしたアクセス制御機構の機能不全に対する分析・検出
- ◆ 検証機能
 - 送受信データを手動で変化させた場合の分析・検出結果による検証

機能概要



- 検査コース選択
(情報収集範囲が異なる3コース)
- 操作ガイド表示
(データ収集に必要なアクセスを指示)
- 分析結果表示
 - セッション追跡パラメタ(セッションID)検出
 - セッション追跡パラメタ(セッションID)データ内容検証
(記録したアクセス内容の編集/再生/オリジナルとの比較)
 - 検出した脆弱項目/脅威度/検出理由 など
- 分析結果詳細表示
 - 検出状況一覧
 - セッション追跡パラメタ(セッションID)遷移分析情報 など
- 記録情報からの Cookie 属性推測

The image shows a Microsoft Internet Explorer browser window displaying a table titled '検出状況一覧' (Detection Status Overview). The table has four columns: '状況' (Status), '検出項目名称' (Detection Item Name), '概要' (Summary), and '脅威度' (Severity). The table lists various vulnerabilities such as 'アクセス制御の欠如' (Lack of access control), 'ユーザ識別の欠如' (Lack of user identification), '多重認証の欠如' (Lack of multi-factor authentication), etc. Each row includes a severity score and a risk level. The table is as follows:

状況	検出項目名称	概要	脅威度
未検出	アクセス制御の欠如	ログイン手続きをスキップして、誰でも他人に成りすますことができます。	90% 100
検出	ユーザ識別の欠如	正権の手続きでログインしたユーザであれば、他人に成りすますことができます。	100% 100
検出	多重認証の欠如	セッション/ハイジャック攻撃が可能な状況では、個人情報が漏れます。	70% 10
検出	異なるセッションで同一セッション追跡IDの使用	セッション追跡IDを再利用される危険性が高くなります。	90% 20
検出	脆弱なセッション追跡パラメタ	他人に成りすますことができる可能性があります。	90% 20
未検出	30秒間の短いセッション追跡パラメタ	ログイン手続きをスキップして、誰でも他人に成りすますことができます。	100% 90
検出	脆弱なセッション追跡パラメタ	ログイン手続きをスキップして、誰でも他人に成りすますことができます。	90% 95
未検出	URL/クッキーによるセッション追跡	セッション/ハイジャック攻撃の実現可能性が高い方式です。	100% 50
未検出	外部サイトへのリンクでセッション追跡パラメタが渡り、セッションが変更される	外部サイトへのリンクをたどるとセッション追跡パラメタが変更される状態になっており、セッションをハイジャックされる危険性があります。	100% 100
未検出	cookie によるセッション追跡	クロスサイトスクリプティング脆弱性やブラウザのセキュリティホールに頼る方式です。	100% 20
未検出	永続的cookieの使用	cookieを盗まれる危険性が高くなります。	100% 10



今後の課題

成果物の普及

◆ 広報・啓蒙活動のアプローチ

- 評価用デモWebサイトを利用したデモサイトの構築による一般社会への啓蒙と発言を積極的に行う。

◆ セキュリティ市場へのアプローチ

- 弊社のセキュリティ関連のチャネルを利用して販売を行っていくための検討を行う。

成果物の実用化

◆システム自体の利便性の向上

- 現在のレベルを使いこなすには、ある程度のスキルが要求される。
- GUI、操作性、ヘルプ画面の充実等



まとめ

まとめ

- ◆ 行政や民間のインターネット向けサービスで使用されるWebアプリケーションについて、そのセキュリティ上の欠陥を検出、検証するソフトウェアの開発を行った。
- ◆ 従来より、Webサーバの脆弱性やCGIプログラムの既知の脆弱性を検査するソフトウェアは商用化されていたが、ログイン機能を持つWebアプリケーションのアクセス制御機構の欠陥を自動的に検査するソフトウェアはこれまでに存在しておらず、本開発はそれを実現した。
- ◆ 電子政府の安全性を確保するため経済産業省が、「情報セキュリティ監査制度」を推進しているが、そのセキュリティ監査においても、本ソフトウェアが有効に活用されるものと期待している。