PHP Conference2002

WEBシステムセキュリティ with PHP 2002夏版

岡田 良太郎

日本PHPユーザ会

有限会社テューンビズ
株式会社テックスタイル
http://techstyle.jp/
riotaro@techstyle.jp
slashdot okdt

August 17, 2002

- はじめに

- UNIX は 米国およびその他の国における米国X/Open, Inc.の登録商標です。
- Linux はLinus Torvalds の米国およびその他の国における登録商標あるいは商標です。
- X Window System は、X Consortium, Inc.の商標です。
- ZENDはZend Technologies, Ltdの商標です。
- Red Hat は、米国 Red Hat Software, Inc. の登録商標です。
- その他、記載されている会社名、製品名は各社の登録商標または商標です。
- 本資料の著作権は岡田良太郎に帰属します。

August 17, 2002

TechStyle

セキュリティ3要素と脅威

- 機密性：対象（人）、内容（データ）の関係を保証
  - ユーザID、管理権限、パーソナリゼーション
    - 脅威：顧客データ漏洩，ID不正利用
- 完全性：正確な伝達
  - メール、メッセージ
    - WEBサイト改ざん, ウイルス感染, 盗聴, なりすまし
- 可用性：期待されるときはいつでも応じられる
  - パフォーマンス、アベイラビリティ
    - DoS対策,サーバダウン, タイムアウト
- つまり、「安全に安定して動きゃいい」ってことか！

TechStyle

PHPプログラムと環境

TechStyle

チェック順（例）をイメージ

1. PortScanして開きポートをチェック – 20,22,80,8080,… 2. 開きポートごとにExploitアタックを発射 – Linux(ICMP), telnet, OpenSSH, Apache, … → サーバダウン（DoS/DDoS） → バッファオーバフロー,侵入成功 （ユーザ情報/システムファイルの取得）	PHP環境
3. HTTP/HTTPSをブラウザでつんつん – FORMにタグを埋め込んでみる クロスサイトスクリプティング – FORMにシェルエスケープ文字を入れてみる – URLなどを渡しているようなら、別のドメインを入れてみる – 不正に(？)ファイルを取得	コンテンツプログラム

TechStyle

PHPプログラムのセキュリティ

TechStyle

青本の述べる注意点

- ファイル命名、ディレクトリ配置
- includeするリモートURL
- HTMLタグチェック
- SQLクエリ文字列
- 認証のすり抜け
- 認証情報の漏洩
- Referrerチェック
- ファイルアップロード
- シェルコマンドの実行

TechStyle

FORMの基本

- なにをFORMで扱うか
  - Hiddenを使うな
  - URLを渡すな
  - FORMに入る時点でCookie有効チェックをしろ
- データの扱い方
  - Referrerをチェック(完全な信頼性はない)
  - 危険文字のエスケープ
  - XSS対策

TechStyle

スペシャルキャラクタの影響

- ピリオド、カンマ、セミコロン、スラッシュ、！などに特別な意味がある
- Buffer Overflow攻撃にも用いられる

→ データクリーニングの必要性

  - popenのパラメータに突っ込むケース
  - ファイルオープン
  - SQL文に足しこむケース
  - シェルに突っ込むケース
    - exec, shell_exec, passthru, system
- XSS対策のために、必殺技（実験中）をこっそり。

TechStyle

データクリーニング関数例

- ereg_replace(“[^0-9]”,””,$data)
  - クリーニングの基本
- addslashes($data)
    - addcslashes (string str, string charlist)
  - クオート（single,double）, バックスラッシュ、NULL文字などをスラッシュ付加
- quotemeta($data)
  - .+?[^](*)$ などをquoteする
- escapeshellcmd($data)
  - メタ文字をエスケープする

TechStyle

コーディング上の注意

- パラメータデータに注意すべき関数
  - include, readfile, fopen, file, link, unlink, symlink, rename, rmdir, chmod, chown, chgrp, exec, system, passthru, popen (など)
- safe_mode による制限
  - 指定ディレクトリ、指定権限でしか動作しない
  - php*.ini により、サイト全体に対して
- 文字列関連、制御コード系
  - サイズチェック、データクリーニング
- コネクションプーリング (p関数)
  - すなおにアベイラビリティのためのものだと割り切る

TechStyle

PHP環境を考える

TechStyle

速いマシンは必要か？

- PHPスクリプトがメインの環境では
  - 主なボトルネックはCPUです。
    - スタティックなHTMLあるいは画像では、メモリーとネットワークがボトルネックになります。
  - 例えば遅いPentium 400Mhzマシンはスタティックな HTMLページでT3回線 (45Mbps) を費やし尽くします。
    - CPUパワーに余力があり、ネットワークの帯域が問題の場合
      - mod_gipや zlib.output_compression を利用

TechStyle

php.ini

- php.iniを制するものはPHPを制す！？
- セーフモード
  - safe_mode = On（gidにより読み書きできるファイルを制限できる）
  - safe_mode_exec_dir = /(php実行ディレクトリ制限)
- open_basedir
  - phpスクリプトからアクセスできるディレクトリを制限できる
- max_execution_time
  - phpのタイムアウト時間を設定できる（ビジー時のアベイラビリティ）
- memory_limit
- upload_tmp_dir

TechStyle

php.ini

- register_grobals
  - Offを推奨
    - EGPCS(Environment、GET、POST、Cookie、Server)変数を自動的にグローバル変数として登録するかどうかを指定する設定項目
- variables_order
  - デフォルトは“EGPCS”の順。
    - EGPCS変数のパースの順番を指定する設定項目。この5つの頭文字の順番でパースされるため、頻度の高い順に並べると良い。サーバ変数(E,S)関連を前にもっていけというアドバイスも(青本)。

TechStyle

システムアップデート

- データセンタ運用者の一言

  ああ、PHP
  アップデートしすぎじゃねーのか…

  フジモト…

TechStyle

PHP4.2.0/4.2.1のセキュリティホール

- 7/22リリースしたて
  - 先月PHPカンファレンス、今月でよかった…
- 問題
  - HTTP POSTリクエストによって送信されてきたMIME ヘッダを解析処理する部分。
    - 具体的には
      - ユーザーエージェントから「multipart/formdata」リクエストとして送られてきたものを変数とファイルに区別する処理で、入力データのチェックが不十分なところがあり、悪意あるデータを送り込まれることにより、セキュリティホールにつながる影響を受けることになる。

TechStyle

PHP4.2.0/4.2.1のセキュリティホール

- 対応
  - PHPを、この問題を修正した新バージョン、4.2.2にバージョンアップする
    - 今後、それぞれのLinuxディストリビューションメーカーらから提供されるアップデートパッケージを適用する（現時点ではまだ提供されていない）。
  - HTTP POSTリクエストを制限する
    - Apacheの場合は、設定ファイル内（httpd.conf）あるいはドキュメントルートの.htaccessファイルに

```
<Limit POST>
  Order deny,allow
  Deny from all
</Limit>
```

TechStyle

最新事情 – 重要なアップデート

- Apache (2002/6/20)
- OpenSSH(2002/6/26)
- Resolver(2002/7/10)
- Sendmail(2002/6/25)
- Samba(2002/6/19)

…

TechStyle

PHPセキュリティを学ぶ

TechStyle

リソース

- PHPマニュアル
  - 第4章セキュリティ
    - http://www.php.net/manual/ja/security.php
  - CHM形式のドキュメントに結構感動
- Suggested Methods of Using PHP Security
  - http://www.sans.org/infosecFAQ/sysadmin/PHP_sec.htm
- PHP4徹底攻略実践編
- PHPデスクトップリファレンス
  - ISBN4-87311-034-3

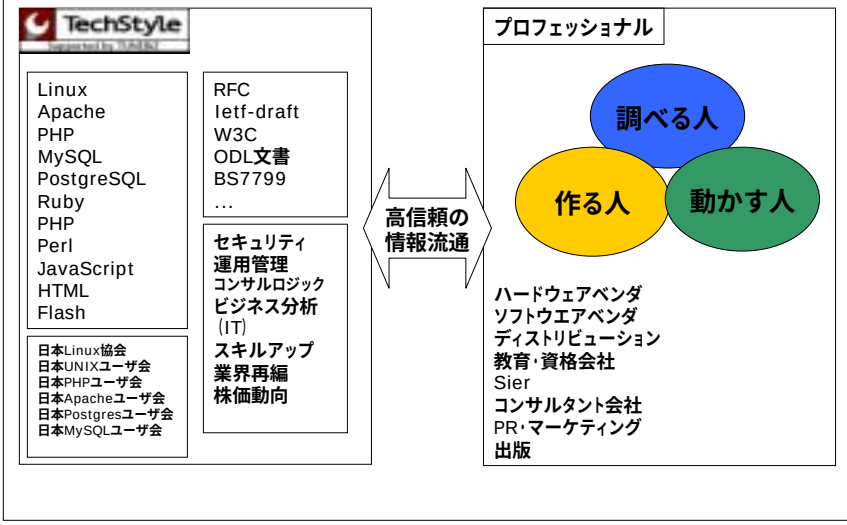
TechStyle

またお目にかかりましょう

- 今回話せなかったこと
  - Securityクラス
  - 設計ポリシーによる防衛
  - OS（カーネル）やWEBサーバとPHPパフォーマンスの関係
  - 開発環境の整備とバリエーション（M社DW）
- この話の続き（？）
  - Linux Conference(9月17日)
  - TechStyle Web Development Seminar(10月)
  - Internet Week(12月くらい)
  - 来年のPHPカンファレンス（未定？）

TechStyle情報サービス

http://techstyle.jp/



Thank You

Please feel free to mail me

riotaro@techstyle.jp

TechStyle

クロージング

- 今年のPHPカンファレンスを振り返って
- 来年のPHPカンファレンスに向けて
- 謝辞