NTTデータ先端技術株式会社

phpMyAdmin にて任意のコードを実行可能な脆弱性 (CVE-2011-2505, CVE-2011-2506)に関する検証レポート

2011/07/29
NTT データ先端技術株式会社
辻　伸弘
泉田　幸宏
小松　徹也

【概要】

phpMyAdmin にセッション変数内のデータを変更可能な脆弱性（CVE-2011-2505）が発見されました。
この脆弱性は、phpMyAdmin 上の$_SESSION 配列に PHP コードを埋め込むことが可能です。
また、phpMyAdmin に変数を適切に処理しない脆弱性（CVE-2011-2506）が発見されました。
この脆弱性は、コンフィグ作成生成用スクリプトにおいて変数内データを適切に処理しないため、PHP コードを含むファイルを出力可能です。
これらの脆弱性を組み合わせて利用することにより、Web サーバの実行権限で任意の PHP コードを実行可能となります。

今回、この phpMyAdmin の脆弱性（CVE-2011-2505, CVE-2011-2506）を利用した攻撃の再現性について検証を行いました。

【影響を受けるとされているアプリケーション】

影響を受ける可能性が報告されているのは次の通りです。

・phpMyAdmin バージョン 3.3.10.2 未満
・phpMyAdmin バージョン 3.4.3.1 未満

【対策案】

脆弱性が修正されたバージョンである 3.3.10.2、または 3.4.3.1 へとアップグレードを実施いただくことを推奨いたします。

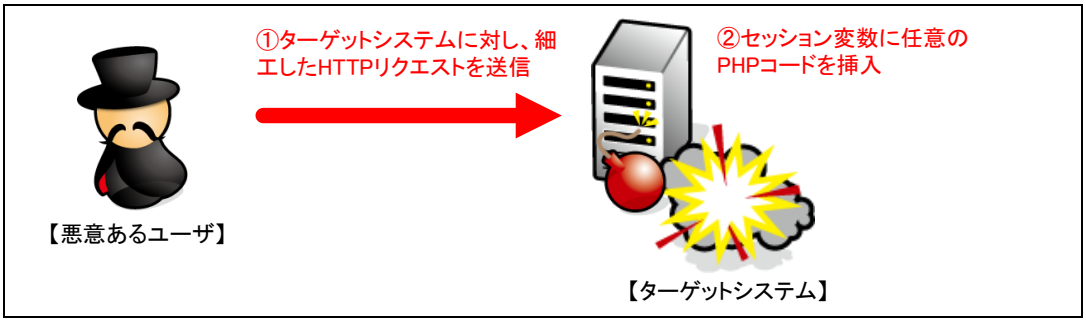
【参考サイト】

CVE-2011-2505
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2505
CVE-2011-2506
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2506

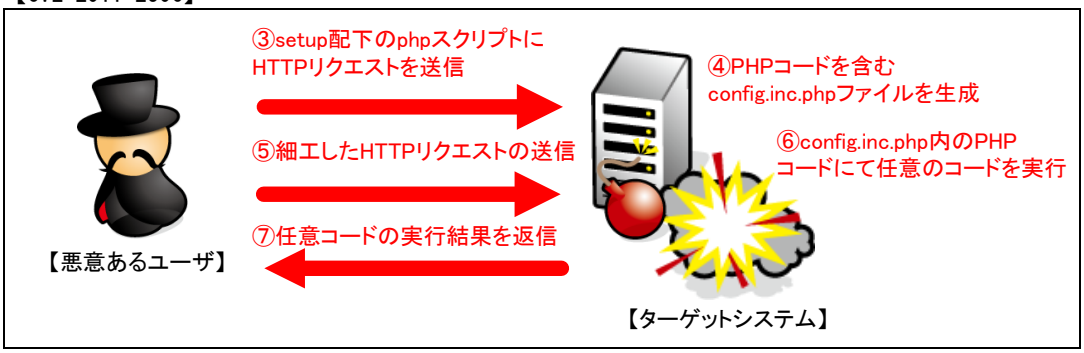
phpMyAdmin - Security - PMASA-2011-5
http://www.phpmyadmin.net/home_page/security/PMASA-2011-5.php
phpMyAdmin - Security - PMASA-2011-6
http://www.phpmyadmin.net/home_page/security/PMASA-2011-6.php

【検証イメージ】

【CVE-2011-2505】



【CVE-2011-2506】



【検証ターゲットシステム】

Debian 6.0.2 上の phpMyAdmin 3.3.10

【検証概要】

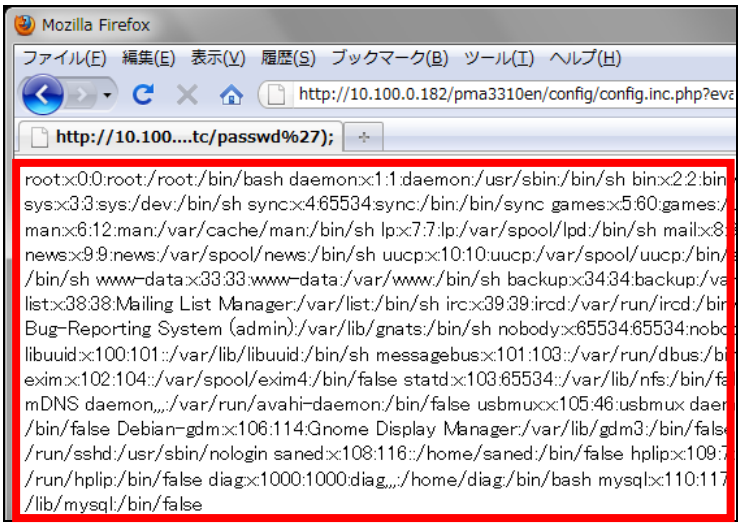
ターゲットシステムに、細工した HTTP リクエストを送信し、セッション変数に PHP コードを挿入します（CVE-2011-2505）。
変数処理に不備のある PHP スクリプトを介して、PHP コードを含むコンフィグファイルを出力し、生成されたスクリプト上で任意のコードを実行します（CVE-2011-2506）。
今回、スクリプトを利用して「/etc/passwd」の表示と任意のコマンドを実行可能なバックドアの設置を検証します。

【検証結果】

下図は、setup スクリプトから作成したコンフィグファイルを利用して、ターゲットシステム上に格納された「/etc/passwd」をブラウザから読みだした結果となります。

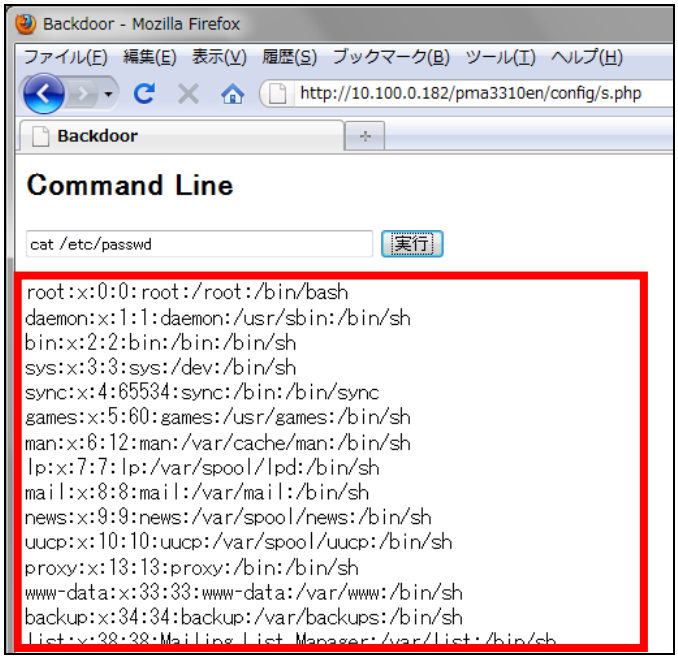
赤枠で示すとおり、ターゲットシステム上に存在する「/etc/passwd」の表示に成功したと判断できます。

「/etc/passwd」の表示



下図は、作成したコンフィグファイルを利用して、任意のコマンドを実行できるスクリプトを設置し、OS のコマンドを実行した結果となります。
赤枠で示すとおり、ターゲットシステム上に存在する「/etc/passwd」の表示に成功したと判断できます。

任意のコマンドを実行可能なバックドアの設置



NTTデータ先端技術株式会社

＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ先端技術株式会社
セキュリティ事業部　営業担当　営業企画グループ
TEL：03-5425-1954
http://security.intellilink.co.jp/