2022 年 06 月 30 日

サービス＆セキュリティ株式会社 e-Gate センター

WordPress のプラグイン「WP Contacts Manager」における SQL インジェクションの脆弱性とその対策について

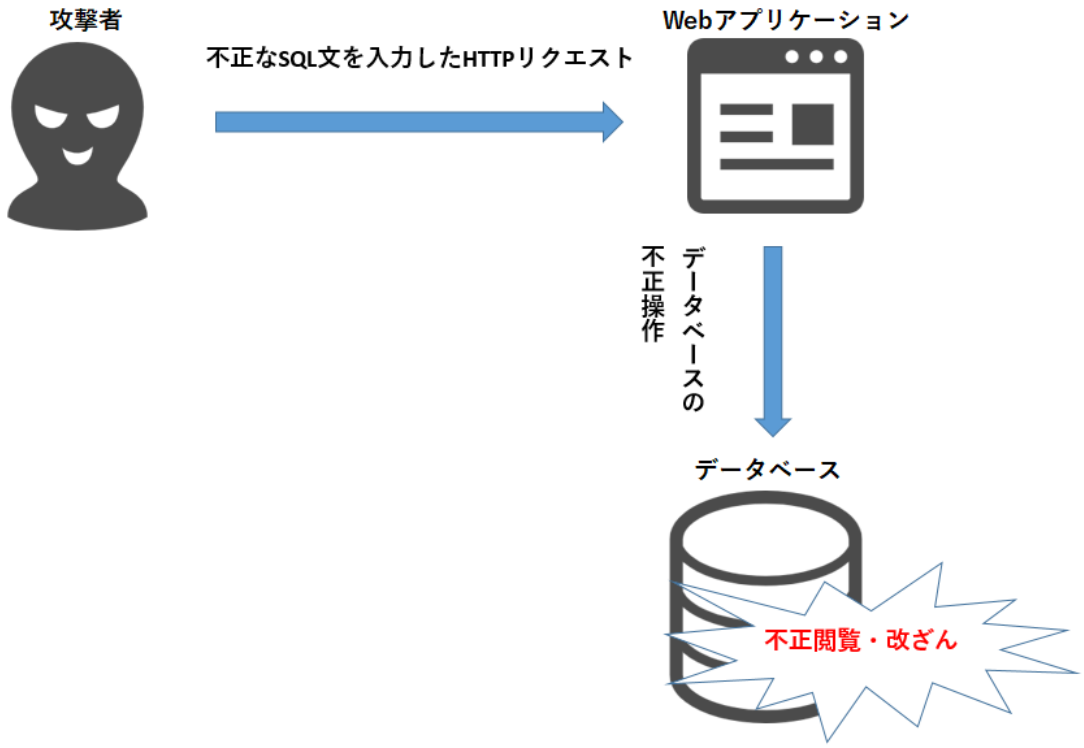
1. 概要

2022 年 5 月、WordPress 向けプラグイン「WP Contacts Manager」において、SQL インジェクションの脆弱性(CVE-2022-1014)が報告されました。この脆弱性の悪用により、データベースへの攻撃が認証不要で可能なため、CVSS 3.1 にてベーススコア「9.8 CRITICAL」と高い数値となっています。SQL インジェクションは古典的な脆弱性でありながら、現在でも多数報告され続けており、発生する被害も大きいことから、今回は改めて SQL インジェクションについて対策の必要性の観点で説明し、併せてオープンソースソフトウェアの対策についてご紹介いたします。

2. SQL インジェクションとは

Web アプリケーションは、ユーザが入力した値を元にデータベースにアクセスし、情報の参照や更新などを行う場合があります。ユーザが入力した値が仕様想定外の場合には、エラー処理や入力値を文字列として扱うなどの処理を行います。SQL インジェクションとは、このような処理の欠如を原因として、攻撃者が入力した SQL 文によるデータベースの不正な閲覧や改ざんを可能とする脆弱性、またはその攻撃を指します。

攻撃者が Web アプリケーションに対して SQL インジェクションで攻撃する場合を図にすると次のようになります。



【図 1 】SQL インジェクションの概要

攻撃例：認証を回避してのログイン

■通常のログイン

利用者がログイン画面からユーザ ID、パスワードにてログインを実行する場合

①ユーザ ID「user1」、パスワード「password1」を入力してログインを実行する。

②リクエストの入力値から SQL 文「SELECT * user_table FROM WHERE user='user1' and pass='password1'」が Web アプリケーションにて作成される。

③上記 SQL 文がデータベースにて実行され、ユーザ ID とパスワードが一致していることを確認しログインが成功する。

■SQL インジェクションを使用しての不正ログイン

攻撃者がログイン画面からパスワードを入力せずに不正ログインする場合

①攻撃者がユーザ ID「user1」、パスワード「' or '1' = '1」を入力してログインを実行する。

②リクエストの入力値から不正な SQL 文「SELECT * user_table FROM WHERE user='user1' and pass='' or '1' = '1'」が Web アプリケーションにて作成される。

③上記 SQL 文をデータベースにて実行され、パスワードの入力なしで不正なログインが成功する。

（この SQL 文はパスワードの入力がなくても毎回、正しい結果になる）

3. 攻撃による影響

攻撃が成功した場合、次のような影響が発生する場合があります。

・データベース内の情報を攻撃者が入手し、アカウントや氏名、住所などの個人情報が外部に漏えいする。

・データベース内の情報を攻撃者に改ざんや削除される。

・データベース内のユーザ ID とパスワードを使用するログイン認証にて不正にログインし、Web サイトを改ざんされる。

このように被害が大きくなるケースが多いのがこの脆弱性の特徴ですので Web アプリケーション開発時から対策をとることが重要となります。

4. 今回脆弱性が報告された WordPress のプラグインにおける脆弱性について

WordPress とはコンテンツマネジメントシステム(CMS)の一つで、Web アプリケーション開発の専門知識がなくても比較的容易に Web ページを作成することができるオープンソースソフトウェアです。Web 技術調査サービス「W3Techs」の調査では WordPress の世界でのシェアは 6 割以上、日本国内でのシェアは 8 割を超えています。WordPress はプラグインを使用することで必要な機能を追加することが可能で、WordPress と同様にプラグインも多用されています。

今回脆弱性が公表された「WP Contacts Manager」も、氏名やメールアドレスなどの管理機能を持つ WordPress 用プラグインの一つです。

WordPress とプラグインは無償で利用可能なものが多く、世界でのシェアも高いことから、攻撃者の標的にもなりやすく、これまでに WordPress 及びプラグインの脆弱性は多数報告されています。

WordPress の脆弱性をついた攻撃については過去に弊社の e-Gate セキュリティニュースで取り上げております。詳細は下記ニュースをご参照ください。

・注意喚起：WordPress の脆弱性を突いた攻撃の増加について

https://www.ssk-kan.co.jp/topics/topics_cat05/?p=11795

5. オープンソースソフトウェアの対策

オープンソースソフトウェア利用時の SQL インジェクション対策としては以下が考えられます。

■開発時の対策

・オープンソースソフトウェアを使用する場合は、既知の脆弱性の存否を確認する。

オープンソースソフトウェアやプラグインなどを利用する場合、利用するバージョンを確認した上で JVN(脆弱性対策情報データベース）などを活用して、すでに公開されている脆弱性の存否を確認する。

JVN の URL　https://jvndb.jvn.jp/

公表されている脆弱性はあくまでも過去に発見された脆弱性ですので、まだ発見・公表されていない脆弱性（ゼロデイ脆弱性）が無いとも限りません。そのため、使用する機能について下記の対策をとることをお勧めします。

・プリペアドステートメントを使用する

ユーザからの入力値を反映させて SQL 文の文字列を作成するときに、通常の文字列連結を使用せずに、プリペアドステートメントを使用して SQL 文を組み立てる。

・エスケープ処理をする

シングルクォート「'」、バックスラッシュ「¥」など SQL の構文を変化させられる特殊記号に対してエスケープ処理を行う。

・入力値を検証する

ユーザからの入力値を検証し不要な文字が含まれる場合には SQL 文を実行せず、エラーを出力する。

・詳細なエラーメッセージを非表示にする

エラーメッセージにデータベースの種類やエラーの原因、SQL 文等の詳細な情報が含まれると、攻撃につながる有用な情報となったり、攻撃結果の出力箇所となったりするため、表示しないようにする。

・データベースのアカウント権限を最小限にする

攻撃を受けた際の被害をなるべく小さく抑えるために、Web アプリケーションがデータベースに接続する際に使用するアカウントの権限を最小限にする。

■運用時の対策

・バージョンを管理する

オープンソースソフトウェアなどは新しい脆弱性が発見・公表されることがあるため、現在利用中のバージョンでの新しい脆弱性の有無などを前述の JVN など活用して定期的に確認する運用体制を整える。

・WAF を導入する

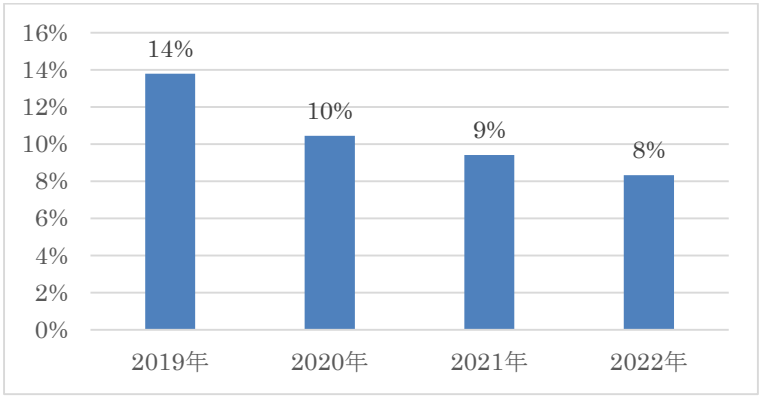
WAF などのセキュリティ機器を導入して、開発時の対策に漏れがあった場合にも攻撃を検知、防御できるようにする。

今回は開発時の対策と運用時の対策について列挙しました。

このような対策をとり、被害を最小限にする取組が重要となります。

6. e-Gate の脆弱性診断サービスについて

当社診断サービスでも SQL インジェクションについては毎年 10%前後検出されています。検出数は減少していますが、検出され続けていることが分かります。この傾向から完全に取り除くことが難しい脆弱性であることが考えられます。SQL インジェクションは被害が大きいことから、万が一にも脆弱性が混入しないよう開発が必要だと当社は考えます。



【図 2】2019 年 1 月～2022 年 6 月に実施した Web アプリケーション診断全案件のうち
SQL インジェクションが検出された案件の割合

e-Gate の脆弱性診断サービスでは、お客様のシステムの脆弱性存否を診断し、検出されたリスクへの対策をご提案させていただいております。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

7. 参考

・NVD
CVE-2022-1014
https://nvd.nist.gov/vuln/detail/CVE-2022-1014

・独立行政法人情報処理推進機構（IPA）
安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity-HTML-1_1.html

安全な SQL の呼び出し方
https://www.ipa.go.jp/security/vuln/websecurity.html#sql

・W3Techs
https://w3techs.com/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標または商標です。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp