CGI-Park 受信名人におけるセキュリティー対策

受信名人では、悪意のある攻撃者からシステムや個人情報を保護するため、厳重なセキュリティー対策を施しています。その対応策として、現在主流となっている下記の攻撃手法に対してどのような対策を講じているかご説明します。
また、仮に新たな攻撃手法が確認され、受信名人に新たなセキュリティーホールが見つかった場合でも、すぐに修正パッチを公開することで、被害の拡大防止に全力で取り組んでいます。

1. SQLインジェクション対策

- **解説**

  データベースと連携したウェブアプリケーションの多くは、利用者からの入力情報を基にデータベースへの命令文を組み立てています。ここで、命令文の組み立て方法に問題がある場合、攻撃によってデータベースの不正利用をまねく可能性があります。このような問題を「SQLインジェクションの脆弱性」と呼び、問題を悪用した攻撃を、「SQLインジェクション攻撃」と呼びます。

- **対策**

  受信名人はデータベースを利用していないアプリケーションのため、SQLインジェクション攻撃による影響は受けません。

2. OSコマンド・インジェクション

- **解説**

  ウェブアプリケーションによっては、外部からの攻撃により、ウェブサーバのOSコマンドを不正に実行されてしまう問題を持つものがあります。このような問題を「OSコマンド・インジェクションの脆弱性」と呼び、問題を悪用した攻撃手法を、「OSコマンド・インジェクション攻撃」と呼びます。

- **対策**

  受信名人の機能では、外部からの入力値からOSコマンドを実行できる設計になっていないため、OSコマンド・インジェクション攻撃を受ける心配はありません。

3. パス名パラメータの未チェック／ディレクトリ・トラバーサル

- **解説**

  ウェブアプリケーションの中には、外部からのパラメータにウェブサーバ内のファイル名を直接指定しているものがあります。このようなウェブアプリケーションでは、ファイル名指定の実装に問題がある場合、攻撃者に任意のファイルを指定され、ウェブアプリケーションが意図しない処理を行ってしまう可能性があります。このような問題の一種を「ディレクトリ・トラバーサルの脆弱性」と呼び、この問題を悪用した攻撃手法の一つに、「ディレクトリ・トラバーサル攻撃」があります。

- **対策**

  外部からのパラメータでウェブサーバ内のファイル名を直接指定するような実装は行なっていないため、ディレクトリ・トラバーサル攻撃を受ける心配はありません。

4. セッション管理の不備

- **解説**

  ウェブアプリケーションの中には、セッションID（利用者を識別するための情報）を発行し、セッション管理を行っているものがあります。このセッションIDの発行や管理に不備がある場合、悪意のある人にログイン中の利用者のセッションIDを不正に取得され、その利用者に成りすましてアクセスされてしまう可能性があります。この問題を悪用した攻撃手法を、「セッション・ハイジャック攻撃」と呼びます。

- **対策**

  CGI-Park全製品において、管理画面のセッション管理にはセッションIDは利用しておらず、Cookieによる暗号化された情報でユーザ認証を行なっており、Cookieの改竄やセッション・ハイジャック攻撃を受ける心配はありません。

5. クロスサイト・スクリプティング

- **解説**

  ウェブアプリケーションの中には、検索のキーワードの表示画面や個人情報登録時の確認画面、掲示板、ウェブのログ統計画面など、利用者からの入力内容やHTTPヘッダの情報を処理し、ウェブページとして出力するものがあります。ここで、ウェブページへの出力処理に問題がある場合、そのウェブページにスクリプトなどを埋め込まれてしまいます。この問題を「クロスサイト・スクリプティングの脆弱性」と呼び、この問題を悪用した攻撃手法を、「クロスサイト・スクリプティング攻撃」と呼びます。クロスサイト・スクリプティング攻撃の影響は、ウェブサイト自体に対してではなく、そのウェブサイトのページを閲覧している利用者に及びます。

- **対策**

  受信名人で動作している公開ページ側の入力フォームからの入力情報は、すべてタニサイジング処理を施しているため、HTMLタグなどのウェブページの表示に影響する特別な記号文字（「<」、「>」、「&」など）は、HTMLエンティティ（「<」、「>」、「&」など）に置換されるため、クロスサイト・スクリプティング攻撃による影響は受けません。

6. メールの第三者中継

- **解説**

  ウェブアプリケーションの中には、利用者が入力した商品申し込みやアンケートなどの内容を、特定のメールアドレスに送信する機能を持つものがあります。一般に、このメールアドレスは固定で、ウェブアプリケーションの管理者以外の人は変更できませんが、実装によっては、外部の利用者がこのメールアドレスを自由に指定できてしまう場合があります。この問題を悪用した攻撃は、「メールの第三者中継」と呼びます。

- **対策**

  受信名人において、問い合わせフォームの自動返信メールの宛先は、入力フォームから受け付けたメールアドレスになりますので、第三者のメールアドレスを入力された場合、意図しないメールが第三者に送信されてしまうことはあります。

  しかし、この「メールの第三者中継」の攻撃者の意図は、そのシステムを利用した迷惑メー

ル送信の踏み台にすることなので、自動返信の宛先を1件だけ第三者に設定しただけでは攻撃として成立しません。また、自動返信先のメールアドレスは、メールアドレスの文法チェックを行なっているため、メールアドレス以外の文字が入力された場合は、エラーを返すようになっています。そのため、メールヘッダーの改竄などで意図しないメールを送信してしまう心配はありません。
さらに、自動返信メールを送信しないように設定することもできますので、そうすれば「メールの第三者中継」に対する驚異はなくなります。