TechRepublic Japan

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃

サイバー攻撃を知る

- 「中間者攻撃」入門 -- 手口や標的を知り保護対策を学ぶ
- 「Man-in-the-Disk 攻撃」入門 --「Android」を狙う攻撃の手口とその対策
- 「クロスサイトスクリプティング攻撃」入門 -- 脆弱性を悪用する手口と回避方法

TechRepublic Japan

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃

サイバー攻撃を知る

「中間者攻撃」入門 -- 手口や標的を知り保護対策を学ぶ

盗聴、詐称、メッセージの傍受は、通信自体と同じくらい古くからある犯罪だ。私たちの頭の中にある情報以外はすべて、他者によるアクセスが可能だが、誰もがあなたのように善意にあふれているわけではない。

通信の傍受や改ざんは何世紀も前から行われており、インターネットの登場によって、犯罪者は他者のプライベートな通信に自身の関心を差し挟むことがはるかに容易になった。こうした不正行為は、中間者（man-in-the-middle：MITM）攻撃と呼ばれる。日常的に発生し、影響力が強く、壊滅的な損害を与えるサイバー犯罪だ。

本記事では、MITM 攻撃について知っておくべきことを、個人や組織の防衛策とともに紹介する。

中間者攻撃とはどんなものなのか

MITM 攻撃の概念は単純だ。あるコンピュータからのトラフィックを傍受して、トラフィックの読み取りや改ざんの可能性に気づかれないように本来の受信者に送る。

犯罪者は MITM 攻撃を実行することで、自身の暗号通貨ウォレットを挿入して資金を盗むことができるほか、ブラウザを悪意あるウェブサイトにリダイレクトすることや、情報を受動的に盗んで後のサイバー犯罪に利用することなどが可能になる。

第三者によるインターネットトラフィックの傍受はすべて MITM 攻撃と言える。適切な認証を実施しなければ、攻撃者にいとも簡単に傍受されてしまう。たとえば、公共 Wi-Fi ネットワークは MITM 攻撃の発生源になることが多いが、これはルータも接続されるコンピュータも ID を検証しないためだ。

公共 Wi-Fi 攻撃の場合、攻撃者は近くの場所で同一ネットワーク上にいるか、トラフィックを傍受できるコンピュータをそのネットワーク上に配置しておく必要がある。ただし、攻撃者は必ずしも物理的に標的の近くにいる必要はない。トラフィックを乗っ取って、感染が拡大する場所すべてに悪意ある情報を注入できるマルウェア変種が、多数存在する。

MITM 攻撃に対抗するには、何らかのエンドポイント認証を利用する必要があり、これには理論上は偽装不可能な認証キーを使用する TLS や SSL などがある。認証方法は強力になっており、一部のシステムではエンドツーエンドの暗号化が用いられている。

2 要素認証方式は、MITM 攻撃に対するセキュリティ強化の一例だ。パスワードは、アカウントやシステムを保護する手段としての信頼性が一段と低下している。ハードウェアキーやソフトウェアコードなど、別に入力される 2 つめの要素を追加することで、攻撃者によるトラフィックの傍受や暗号化の突破が困難になる。だが、それで暗号化クラッキングを完全に防

こちらは、2019/02/22 に公開された記事（https://japan.techrepublic.com/article/35131033.htm）を再録したものです。仕様等は公開時点のものです。

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃

サイバー攻撃を知る

止できるわけではない。ハッカーは証明書の偽造や、銀行のウェブサイト、ログインポータル、その他の偽サイトを用意して情報を盗むことも多い。

MITM 攻撃は、サイバー軍拡競争の格好の例だ。新しい形式の暗号化が破られると、組織はすぐに新たな暗号化を開発し、それがまた破られる、というサイクルが繰り返されている。

中間者攻撃の有名な例にはどのようなものがあるのか

インターネットの登場以来、有名な MITM 攻撃の例はいくつもあるが、MITM 攻撃が及ぶ範囲の広さと強力さを説明するには、歴史を振り返り、コンピュータが発明されるはるか前に起きた最も強力な MITM 攻撃の 1 つに注目することが重要になる。それがバビントン陰謀事件だ。

1568 年、投獄されたスコットランド女王メアリーの支持者たちは、メアリーに手紙を書き、イングランド女王エリザベス 1 世の暗殺計画への協力を求めた。だが、エリザベスの諜報員がメアリーの返信を傍受し、内容を改ざんして、陰謀者の名前を尋ねた。名前を書き連ねた陰謀者の返信は、再び中間者によって傍受される。これがメアリーと共謀者の処刑へとつながった。

インターネットベースの MITM 攻撃の例も多い。

- Edward Snowden 氏は 2013 年、米国家安全保障局（NSA）の文書を公表し、NSA が Google になりすましていたことを暴露した。NSA はトラフィックの傍受や SSL 証明書の偽装によって、あらゆる人の Google 検索を監視できていた可能性がある。
- Comcast は、自社のウェブトラフィックに JavaScript を挿入することで、サードパーティーサイトがホストしている広告の代わりに自社の広告を表示させていたことが発覚した。
- アドウェアプログラム「Superfish」は、SSL トラフィックをスキャンして証明書をインストールし、それによって安全なトラフィックを傍受してリダイレクトしていたことが分かっている。
- 「Android」スマートフォン向けバンキングアプリの重大な脆弱性によって、多数のアプリが MITM 攻撃に対して無防備な状態に陥った。

他にも多くの例あり、発覚することなく実行される攻撃はさらに多いだろう。だが、それらすべてが 1 つのことに帰結する。MITM 攻撃は起きるものであり、インターネットが存在する限り、企ては今後も続くということだ。

中間者攻撃の標的になりやすいのは誰か

いかなる人物や組織も MITM 攻撃の標的になり得るが、これらの犯罪の多くには、金銭的な利益という共通のテーマがある。銀行やバンキングアプリは、マルウェアベースの MITM 攻撃の標的になることが多い。悪意あるコードは、パケットの窃取、トラフィックの乗っ取り、あるいは安全な接続への侵入を目的に、標的サイトへのトラフィックを検知するまで待つことがある。

とはいえ、金融関連の接続だけがよく狙われるわけではない。セキュリティの突破によって個人的な利益を得られるのなら、攻撃者はあらゆる安全な接続に関心を持つだろう。これには、ソーシャルメディアのアカウントや E コマースサイトの認証情報、機密データベースなどがある。

TechRepublic Japan

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃

サイバー攻撃を知る

モノのインターネット（Internet of Things：IoT）は MITM 攻撃の標的になることが増えており、その背景として、IoT デバイスが急速なペースで成長し、セキュリティが追いついていないという状況がある。IoT デバイスは個人や企業に関する個人識別情報を大量に送信する可能性もあるため、サイバー犯罪者たちにとって、IoT トラフィックの乗っ取りは魅力的だ。

産業用モノのインターネット（Industrial Internet of Things：IIoT）ハードウェアを運用する企業は、セキュリティ対策が手薄で、機密性の高い専有情報に IIoT マシンがアクセスするため、MITM 攻撃のリスクが特に大きい。IIoT システムが MITM 攻撃を受けると、ビジネスの中断、製品の不正操作による強度や安全性の低下、IIoT マシンが製造時に使用する専有情報の盗難が発生するおそれがある。

つまり、インターネット上で機密情報を送信する人は誰でも MITM の標的になる可能性がある。ただし、企業への攻撃のうち、ハッカーが金銭的な利益を得る攻撃や、競合他社が有利になるような攻撃は、甚大な損害が発生する可能性があり、脅威の度合いが大きい。

中間者攻撃にはどのような種類があるのか

自宅や外出先、オフィスでコンピュータを MITM 攻撃から保護するためには、自分が何から身を守っているのかを理解する必要がある。MITM 攻撃のタイプはさまざまで、複数の脆弱性を標的とし、多様な発信源から仕掛けられる。安全を維持するには、どのような種類の MITM 攻撃があり得るのか、そのすべてから身を守るためにどうすべきかを知っておかなければならない。

中間者攻撃には以下のような種類がある。

- **不正アクセスポイント**：正規の公共ネットワークになりすますし、Wi-Fi に自動接続するコンピュータをだますために設置される。多くの場合、こうした不正なネットワークはトラフィックを監視して機密情報を盗む。
- **アドレス解決スプーフィング**：ローカルエリアネットワーク上の悪意あるノードが別のマシンになりすまして被害者を欺き、悪意あるノードに接続させてから、トラフィックを正規のノードに渡す。
- **mDNS スプーフィング**：ネットワークデバイスをだまして、偽のアドレスに接続させる。mDNS は、名前をローカルエリアネットワーク上のアドレスと照合するために使うもので、偽装されると、悪意あるマシンが脆弱なコンピュータや IoT ハードウェアへアクセスできるようになってしまう。
- **DNS スプーフィング**：インターネットユーザーをだまして、本物そっくりの偽ウェブサイトに接続させるために使用されることが多い。オンラインバンキング詐欺や他のアカウント乗っ取り攻撃でよく用いられる手口だ。

中間者攻撃はどうすれば防げるのか

こうした多様な形態の MITM 攻撃から身を守るには、複数の手段が必要であり、それぞれの手段が各形態の攻撃を阻止する上で不可欠となる。

- コンピュータやモバイルデバイスを Wi-Fi ネットワークへ自動的に接続させない。既知の信頼できる Wi-Fi ネットワーク以外には接続しない。
- 自分が管理しているすべてのアクセスポイントで、必ずセキュリティ対策と暗号化を実施する。物理的に近い場所から MITM 攻撃をしかけようとする攻撃者は、効果的なセキュリティによってネットワークから閉め出すことができる。
- 未知の Wi-Fi ネットワークや公共の Wi-Fi ネット

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃

サイバー攻撃を知る

ワークに接続する場合は、必ず VPN を使用してトラフィックを保護する。

- 安全な HTTP 接続（URL が https:// で始まる）を使用しないウェブサイトとは決して機密情報を共有してはならない。
- 2 要素認証に対応しているアカウントでは、必ず 2 つめの認証要素を追加する。
- フィッシング攻撃や、リンクをクリックしてウェブサイトにログインするように求める電子メールに注意する。電子メールが本物か確信を持てない場合は、問題のウェブサイトに手入力でアクセスして、電子メールのリンクを使用せずにログインしよう。それでも確信を持てない場合は、サイトの運営組織に連絡して、正規のメッセージか確認してほしい。
- システムの脆弱性を悪用する MITM 攻撃を防ぐため、OS は必ず最新の状態にする。
- 最新のウイルス対策アプリケーションをインストールして、コンピュータの定期スキャンを設定する。

MITM 攻撃やその他の種類のサイバー犯罪を完全に防ぐことはできないとしても、警戒を怠らなければ、リスクを大幅に低減し、狙うにはあまりに時間がかかる手ごわい標的になることはできる。

TechRepublic Japan

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃

サイバー攻撃を知る

「Man-in-the-Disk 攻撃」入門 --「Android」を狙う攻撃の手口とその対策

Google の「Android」モバイル OS では、長年にわたり相当数のセキュリティ脆弱性が発見されてきた。テクノロジニュースを追っていると、ユーザーと開発者を先進的なサイバー攻撃の危険にさらす新しい脆弱性が、Android の設計のあらゆる場所に潜んでいるように感じることもある。

その一例が、ソフトウェア調査会社 Check Point の研究者による先ごろの発見だ。「Man-in-the-Disk」（MITD）攻撃と名付けられたその攻撃は、Android の外部ストレージ処理の脆弱性を利用して、悪意あるコードを注入する。MITD 攻撃を可能にするエクスプロイトは Android の設計に不可欠なレベルに存在するため、Android ユーザーに深刻な影響を及ぼす。

中間者（Man-in-the-Middle：MITM）攻撃と名前が似ているのは、この 2 つの攻撃に共通点が多いためだ。どちらも不正な目的のためにデータを傍受し、改ざんすることも多い。2 つの攻撃の違いは規模だけだ。

Check Point の研究者は、MITD 攻撃に対して無防備なアプリを多数（Google のような大手ディストリビューターが提供するアプリも含む）発見した。また、このエクスプロイトを利用するアプリを独自に開発することにも成功した。

MITD 攻撃は、Android デバイスに深刻な損害を与えるだけでなく、Android アプリを作成する開発者の評判も大きく傷つける可能性がある。Android デバイスのユーザーも、Android 開発者も、本記事を読み進めて、新たに発見されたこの悪質な攻撃手法について詳しく知ってほしい。

どんなものなのか

Man-in-the-Disk 攻撃と聞いて最初に思い浮かぶのは、中間者（Man-in-the-Middle：MITM）攻撃と名前がよく似ているということかもしれない。それもそのはず、MITD は実質的に MITM の 1 形態だ。

MITM 攻撃は、2 つのエンドポイント間のトラフィックを傍受して、（必ずではないが高い頻度で）改ざんする。MITD 攻撃は同じことをより小さな規模で実行する攻撃で、Android の外部ストレージとインストール済みアプリの間を移動するデータを傍受し、場合によっては改ざんする。

それが何を意味するのかを理解するには、Android デバイスの内部ストレージと外部ストレージが機能する仕組みを知る必要がある。

内部ストレージは各アプリに独占的に割り当てられるもので、他のアプリがアクセスすることはできない。また、サンドボックス化されているため、他のアプリケーションや Android プロセスから隔離されており、他のアプリや Android OS に影響を与えることも、影響を受けることもない。

外部ストレージは、Android デバイスにインストールされているすべてのアプリケーションによって共有される。ダウンロードファイル、写真、その他のメディアやファイルが、1 つの特定のアプリケーション専用のものでない場合は、外部ストレージに保存される。注意したいのは、外部ストレージが取り外し可能とは限らない点だ。Android デバイスの内部メモリ上

こちらは、2019/02/22 に公開された記事（https://japan.techrepublic.com/article/35131478.htm）を再録したものです。仕様等は公開時点のものです。

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃
サイバー攻撃を知る

の独立したパーティションが外部ストレージである場合もある。

MITD 攻撃関連で外部ストレージについて知っておくべき最も重要なことは、アプリは外部ストレージを使って、他のアプリケーションと共有されないデータを自由に保存できるということだ。多くの場合、内部ストレージは限られているため、データを大量に使用するアプリはよく外部ストレージを使って追加ファイルを保存したり、アップデートをプリロードしたり、サイズを小さく見せたり、下位互換性を持たせたりする。

Android アプリが外部ストレージへのアクセスを要求するのはよくあることで、標準的と言ってもいいほどだが、そこに問題が入り込む。

Check Point の報告にあるように、悪意あるアプリは外部ストレージを悪用する能力を十分に備えており、アプリデータを読み取って、外部ストレージからアプリに送信されるデータを改ざんする。悪意あるアプリはそのエクスプロイトを使用して個人データを盗み、他の悪意あるアプリケーションを内部ストレージにインストールし、正規のアプリのコードを破壊して無効化し、コードの注入によってデバイス上での権限を昇格させることができる。

Check Point が説明したプロセスは、同報告にある2つの画像で詳しく解説されている。悪意あるアプリのインストールと、アプリのクラッシュに関する画像だ。

なぜそれほど危険なのか

MITD 攻撃が引き起こす脅威は非常に大きい。これは主に、外部ストレージへのアクセス権を取得することによって Android デバイスを攻撃するからだ。サンドボックス化された専用の内部ストレージスペースの外で何らかの処理を実行する Android アプリ（そのようなアプリは非常に多い）は、外部ストレージへのアクセスを要求する。

Check Point が調査報告で述べているように、外部ストレージへのアクセスは新しいアプリが要求する典型的な権限なので、他の一部の権限要求と違って怪しまれない。ユーザーが「許可」をタップすると、悪意あるアプリは外部ストレージの中身を自由に監視、改ざんできるようになり、さらには他の悪意あるアプリをユーザーに知られずにインストールすることも可能になる。

大半の Android マルウェアと同様に、MITD 攻撃もユーザーに活動の許可を求める。Android ウイルスや攻撃がどれだけうまくコーディングされ、難読化されていても、サンドボックス環境の外側で何かを実行するには、ユーザーの許可が必要だ。

ユーザーは通常、アプリが要求する権限を不審に思っても無視してしまうので、外部ストレージへのアクセスのような一般的な要求は、経験豊富で慎重な Android ユーザーであっても見過ごすことが多い。

誰が影響を受けるのか

MITD 攻撃の危険にさらされるのは、テクノロジを利用する世界の一部の集団、つまり Android 開発者と Android ユーザーだけだ。

この特定のエクスプロイトは、はるかに一般的な中間者攻撃に似ているように思えるかもしれないが、Android が外部ストレージを処理する仕組みに限定された攻撃手法だ。簡単に言うと、Android デバイスを持っていない人、Android デバイス向けのアプリケーションを開発していない人、企業所有の Android デ

こちらは、2019/02/22 に公開された記事（https://japan.techrepublic.com/article/35131478.htm）を再録したものです。仕様等は公開時点のものです。

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃

サイバー攻撃を知る

バイスや BYOD の Android デバイスを管理していない人は、MITD 攻撃について心配する必要はない。

だからといって、他のプラットフォームには同様のエクスプロイトがない、または今後も登場しないというわけではなく、許可を悪用して本来アクセスできない OS の領域に侵入するマルウェアは珍しくない。そうした他の潜在的な攻撃は MITD 攻撃ではないが。

開発者はどうすればアプリを保護できるのか

外部ストレージとそのセキュリティの欠如は、Android の構造の根幹に関わるものだ。それを考えれば、Google が Android を再設計して、MITD 攻撃からの脅威を完全に排除する可能性は低い。

そのため、開発者は必ずアプリで外部ストレージを安全に使用して、データの収集、アプリの破損、マルウェアのサイドロードを防がなければならない。

Google のアプリ開発ガイドのベストプラクティスのセクションには、アプリのセキュリティに関するヒントが多数掲載されており、その多くを MITD 攻撃の防止に応用することができる。

Google は外部ストレージの使用に関して以下のように述べている。

- SD カードなどの外部ストレージに作成されたファイルはグローバルに読み取りと書き込みが可能だ。外部ストレージはユーザーによよって削除されたり、アプリによって変更されたりする可能性があるため、外部ストレージを使用して機密情報を保存してはならない。
- 信頼できないソースからのデータの場合と同じように、外部ストレージからのデータを処理するときは、入力検証を実行する必要がある。
- 読み込みの前に、外部ストレージに実行可能ファイルやクラスファイルを保存しないことを強くお薦めする。
- アプリで外部ストレージから実行可能ファイルを取得する場合は、動的読み込みの前に、ファイルを署名して、暗号により検証する必要がある。

内部ストレージのデータを保護する効果的な方法も記載されている。

- プロセス間通信（IPC）ファイルに対しては、「MODE_WORLD_WRITEABLE」モードや「MODE_WORLD_READABLE」モードの使用を避ける必要がある。これらのモードは、特定のアプリへのデータアクセスを制限する機能やデータ形式の制御に対応していないからだ。
- アプリが直接アクセスできないキーを使用してローカルファイルを暗号化する場合がある。たとえば、キーを「KeyStore」に配置して、端末に保存されていないユーザーパスワードを使用して保護することができる。
- コンテンツプロバイダーを使用して、アプリ間の内部ストレージの読み取りと書き込みのパーミッションを臨機応変に動的に与えることができる。

Check Point は、多くの MITD 脆弱性の原因として、粗末なプログラミングが考えられると指摘する。開発者は懸命に努力して安全なアプリを作成するのではなく、機密性の高いデータを外部ストレージに保存したり、未検証のデータをアプリにロードできるようにしたりしているという。

Google はセキュリティのヒントで多くを語っていないかもしれないが、コードを数行追加するだけで、

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃
サイバー攻撃を知る

ユーザーのセキュリティ、アプリの信頼性、開発者としての評判を大幅に改善できることもある。

Google がこの問題を解決するために Android を再設計する可能性は低いため、同社に代わってセキュリティを補強するのは開発者の役割だ。

ユーザーはどうすればデバイスを保護できるのか

Android ユーザーの方は心してほしい。粗末な作りのアプリは、悪意あるダウンロードから仕掛けられる MITD 攻撃によって不正に操作されるおそれがあり、安全が大いに脅かされている。

「クラッシュしてアプリの防御が無効になると、攻撃者はコードインジェクションを実行して、攻撃対象アプリケーションに与えられた許可を奪い取り、自身の権限を昇格させて、カメラやマイク、連絡先リストなど、ユーザーのデバイスの他の部分にアクセスする可能性がある」。Check Point はこのように指摘する。

非常に大きな危険であるため、保護対策をアプリ開発元任せにすることはできない。Google、Yandex、Xiaomi（どれも MITD 攻撃に対して脆弱なアプリを作っている）といった大手の開発元であっても同じだ。

Android ユーザーは、以下の手順をすべて実施して身を守ってほしい。モバイルデバイスの安全を守るには、総合的な保護が必要だ。

- スマートフォンにマルウェア対策アプリをインストールして、悪意あるアプリに目を光らせ、セキュリティアプリを最新の状態に保つ。
- アプリケーションは、公式の「Google Play」ストア以外の提供元からロードしてはならない。Google Play ストアでもマルウェアが発見されたことはあり、今後も発見されるだろうが、サードパーティーのアプリストアでは、Google が導入している保護対策を利用できず、悪意あるアプリをダウンロードしてしまう可能性が大幅に高まる。
- アプリレビューに目を通して、他のユーザーの意見を確認しよう。レビューの評価が低い、内容がない、同じ内容や似た内容のレビューが繰り返し投稿されている場合は、すべて危険信号だ。
- アプリの権限を確認しよう。アプリの Google Play ストアページで、アプリの説明の下にある「Read More」（もっと見る）をタップして、下にスクロールし、「App Permissions」（アプリの権限）を探す。何かがおかしいと感じたら（たとえば懐中電灯アプリが外部ストレージへのアクセスを要求）、そのアプリをインストールせずに別のアプリを探そう。

ユーザーのデバイスを最前線で保護するのは開発者だが、ユーザーは何もしなくていいわけではない。安全を守るための適切な予防措置を講じれば、Android デバイスの深刻な感染について心配する必要はなくなるはずだ。

TechRepublic Japan

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃

サイバー攻撃を知る

「クロスサイトスクリプティング攻撃」入門 -- 脆弱性を悪用する手口と回避方法

最新の非常に顕著なオンライン脅威が危険であることは簡単に納得できるが、最先端のサイバー攻撃だからといって、古い攻撃と同じくらい広範囲で継続的に発生しているとは限らない。クロスサイトスクリプティング（XSS）を例に考えてみよう。Microsoft が初めて XSS 攻撃を特定して分類したのは 2000 年のことだが、XSS 攻撃の記録はインターネットの最初期にまでさかのぼる。バグ報奨金ホスティングウェブサイト HackerOne は 2017 年 7 月、XSS は同プラットフォームのユーザーが最もよく発見する脆弱性であり続けていると報告している。

クロスサイトスクリプティングの脅威が衰える可能性は低いため、インターネットユーザーとウェブ開発者は XSS がどんなものか、どうすればこのサイバー攻撃を防げるのかを知る必要がある。

どんなものなのか

クロスサイトスクリプティングは、攻撃者がウェブページの脆弱性を悪用して独自のコードを注入したときに発生する。このコードは、認証情報やセッションクッキー、その他の機密データなどのユーザー情報を盗み、サイトに永続的に潜在して複数のユーザーを攻撃することもある。

XSS 攻撃の特徴は、悪用するウェブサイトやウェブアプリが標的ではない点だ。サイトやアプリは攻撃経路にすぎない。XSS 攻撃には、ユーザーのマシン上で実行されるスクリプトが使われる。クライアントサイドスクリプトと呼ばれるものだ。その大半は JavaScript や HTML で記述されるが、クライアントサイドスクリプトに使用できる言語は他にもある。

XSS 攻撃は、反射型攻撃と格納型攻撃の 2 種類に分類される。

反射型攻撃は、短期間の非持続的な攻撃であり、スクリプトなどの埋め込みオブジェクトを排除するサニタイジング（無害化）を適切に実行しないサーバサイドスクリプトを利用する。

反射型 XSS 攻撃を使用する攻撃者は、電子メール、悪意あるウェブサイト、またはその他の場所で、ユーザーにリンクをクリックさせる必要がある。そのリンクには悪意あるスクリプトが含まれており、脆弱なウェブサイトはこれをサニタイジングで除去できないため、スクリプトがウェブサイトからユーザーのコンピュータに送信される。

格納型攻撃は、それほど一般的ではないが、反射型攻撃よりもはるかに危険で破壊的だ。ウェブサイトとのやりとりが最小限である反射型攻撃と異なり、サイトを悪用して、攻撃者が標的のコンピュータ上で実行したい悪意あるスクリプトを保存させる。

格納型攻撃をしかけるには、ウェブサイトがユーザー情報を公共の場所（ソーシャルメディアプラットフォーム、オンラインフォーラム、サードパーティーの小売サイトなど）に格納している必要がある。もっと具体的に言えば、ウェブサイトにサニタイジングされていない HTML を埋め込めるようになっていなけれ

こちらは、2019/02/22 に公開された記事（https://japan.techrepublic.com/article/35131832.htm）を再録したものです。仕様等は公開時点のものです。

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃

サイバー攻撃を知る

ばならず、それによって訪問者は、ページを閲覧するだけで知らないうちに不正なデータにさらされてしまう。反射型攻撃と同様に、感染コンテンツに埋め込まれたスクリプトはユーザーに見えないため、疑いを持たれることはない。

反射型攻撃ではユーザーがリンクをクリックする必要があるが、格納型攻撃ではユーザーによる操作が必要ない。格納型攻撃の例としては、ユーザー名、ブログ投稿、製品の説明、フォーラムへの投稿など、サニタイジングされていないユーザー生成型 HTML コンテンツが許可されるあらゆる場所に XSS を埋め込む攻撃などが考えられる。

どれほど大きな脅威なのか

XSS 攻撃の仕組みは単純で、脆弱なウェブサイトと、JavaScript や HTML に関する基本的な知識さえあれば、ユーザーの生活をかき乱すことが可能になる。つまり、クロスサイトスクリプティングは極めて大きな脅威ということだ。XSS の強い持続性だけで、誰もが不安になるだろう。XSS は 1990 年代中ごろから問題となっており、今なお重大な問題だ。

Positive Technologies による最近の調査では、テスト対象ウェブサイトの 4 分の 3 近くが XSS 攻撃に対して無防備であることが明らかになった。Positive Technologies の調査結果が正しいなら、XSS はインターネットにおいて飛び抜けて悪用されやすい脆弱性ということになる。

XSS 攻撃では、ユーザーの機密データが盗まれる可能性がある。XSS の標的で特に機密性が高い情報が、セッションクッキーだ。セッションクッキーはウェブサイト上でユーザーの ID を検証し、ユーザーがドメイン内の複数のページを訪問する間、ログイン状態を維持できるようにする。

XSS 攻撃者にセッションクッキーを盗まれると、ユーザーのアクティブセッションが複製され、ソーシャルメディアへの投稿、個人情報やアカウント情報の編集、パスワードの変更、クレジットカード情報の取得、銀行振込、E コマースサイトでの商品購入など、そのユーザーがウェブサイト上で実行できるあらゆることが、攻撃者にも可能になってしまう。

主な事例にはどのようなものがあるのか

主要サイトへの XSS 攻撃の証拠は、10 年以上さかのぼっても簡単に見つけられる。成功した XSS 攻撃に関するニュース記事は非常に多く、最初のインシデントから何年も対策が施されなかった攻撃もある。

- 2008 年、Facebook に概念実証 XSS が投稿された。Facebook はその脆弱性を発見後すぐに修正したが、公表される前に悪意ある攻撃の被害者がいたかどうかは分かっていない。
- Twitter の 2010 年の再設計に XSS 脆弱性が含まれていた。元英国首相 Gordon Brown 氏の妻である Sarah Brown 氏が被害に遭い、その脆弱性を知らないうちに 100 万人以上のフォロワーと共有してしまった。このエクスプロイトは、クリックしなくてもマウスオーバーするだけでユーザーをポルノサイトにリダイレクトするものだった。
- eBay ユーザーは長年にわたり、アイテムリストに埋め込まれた XSS スクリプトを扱っていた可能性がある。この問題は 2017 年初頭まで修正されなかった。このケースでは、悪意あるセラーが正規の製品リストにスクリプトを追加して、ユーザーを偽のログインページにリダイレクトし、

認証情報を収集してから、ユーザーを再び正規の eBay ページにリダイレクトしていた。

- British Airways のウェブサイトとモバイルサイトの決済システムを標的とした XSS 攻撃で、同航空会社の予約 40 万件近くが不正にアクセスされた。これらすべての取引で使われたクレジットカードとデビットカードの情報が盗まれたおそれがある。
- 2005 年に MySpace に影響を及ぼした「Samy」ワームは、ユーザーのプロフィールに同ワームの開発者に関する一文を追加した。「samy is my hero」（Samy は私のヒーロー）という文言だ。実害はなかったが、Samy ワームは XSS を利用して 20 時間足らずで 100 万人以上の MySpace ユーザーに感染し、インターネット史上、最速で拡散したワームとなった。
- 米 Yahoo は、電子メール分野での優位が揺らいでいた時期に、多数のセキュリティ問題に直面した。たとえば 2013 年の XSS フィッシング攻撃では、被害者がアカウントを盗まれている。

残念ながら、これらの例は、広く報道された主要なクロスサイトスクリプティング攻撃の一部でしかない。今後、他の XSS 攻撃が発生して個人情報が盗まれることは十分に考えられる（その可能性は非常に高い）。

開発者はどうすればウェブアプリを保護できるのか

自分のプロジェクトが XSS 攻撃の被害に遭ったウェブ開発者は、攻撃を受けやすい脆弱性を放置した自分を責めるしかない。

場合によっては、いくつかの HTML タグをウェブサイトに追加するだけで、簡単に XSS を防げることもある。必ずしもそう簡単にいくわけではないが、まずはエンコーディングという手法を試してみるといいだろう。

エンコーディングは基本的に、ユーザー入力からすべてのコードを取り除き、ウェブブラウザがその入力をデータとしか解釈しないようにするものだ。サーバサイドとクライアントサイドの一方、または両方でユーザー入力をエンコーディングする方法はいくつかあり、それによって HTML、CSS、JavaScript、URL スクリプトがすべて取り除かれ、純粋なテキストとしてレンダリングされる。

だが、ウェブアプリケーションがテキストだけでなくリッチデータの入力も受け入れる必要がある場合など、エンコーディングが最適でないケースもある。

エンコーディングで XSS 攻撃を確実に阻止できるわけでもない。たとえば、入力フィールドに直接入力するのではなく、外部にリンクするユーザー入力が行われる場合、エンコーディングフィルタを通らずに、悪意あるコードが送信されてしまうことが多い。だからといって、エンコーディングは予防策として意味がないわけではなく、検証のような追加の保護手段によって補完する必要がある。

検証は XSS 対策の第 2 の主要な手法だ。ユーザー入力に含まれている可能性のあるコードをすべて排除するのではなく、悪意のあるコードを取り除く。検証は通常、分類とサニタイジングのいずれかの方法で実行する。

分類とは、許可する HTML タグと許可しない HTML タグの種類を指定する方法だ。これは、特定のコマンドをブラックリストまたはホワイトリストに登録することで指定できる。ホワイトリストは、許可するものを最小限に抑え、悪意あるものが漏れる可能

性を排除するため、一般的にブラックリストよりも優れた方法とみなされている。

分類は、ユーザー入力を受け取り時に処理し、「許容可能」または「不適切」のいずれかに区分する。ホワイトリストやブラックリストの基準を満たさない入力はすべて許可されない。

サニタイジングは検証エンジンによって、ユーザー入力の特定の部分が悪意あるものかどうかを判断する。悪意あるものと判断された場合、サイトはその入力を拒否するか、問題のある要素をサニタイジングで除去するかを選択する。

ユーザーが複雑な HTML を利用する必要があるケースでは、入力のサニタイジングが最良の選択肢かもしれない。エンジンが不適切と見なすものをブロックしつつ、ユーザーのコードの大部分を実行することができるだからだ。XSS 攻撃とその対策を解説するサイト Excess XSS は、サニタイジングエンジンでブラックリストによって無効な入力を識別しようとすると、サニタイジングの効果がなくなるので、ブラックリストを使わないように警告する。その代わりに、サニタイジングライブラリとフレームワークによって、徹底的かつ全面的にホワイトリストを利用するアプローチでサニタイジングを実行するように薦めている。

注目を集めている 3 つめのアプローチは、コンテンツセキュリティポリシー（CSP）だ。CSP では、信頼できるドメインから送信されたものでなければ、どんなリソースも（スクリプト、スタイルシート、ファイルなど）実行されない。注入されたスクリプトは、信頼できるドメインから来たものではない可能性が高いため、実行を許可されず、攻撃が阻止される。

World Wide Web Consortium（W3C）は、CSP が検証やエンコーディングの代わりになると考えるべきではない、と述べている。「CSP は多層防御として使うのが最適だ。悪意あるコード注入が引き起こす損害を軽減できるが、入念な入力検証や出力エンコーディングに取って代わるものではない」（W3C）

XSS 対策の他のアプローチには、スクリプトを完全にブロックする、クッキーのセキュリティを強化して IP アドレスに紐付ける、「Google Chrome」「Opera」「Firefox」の 2017 年 11 月以降のバージョンでクッキーに「SameSite=Strict」パラメータの使用を強制する、といったものがある。

どのアプローチをとるべきか分からない場合は、どれが自分のサイトに最適かを調べて確認しよう。確信を持てない場合は、複数の方法を採用するのもいいだろう。

インターネットユーザーはどうすれば身を守れるのか

XSS は主に、サイトを悪用されてユーザーにクロスサイトスクリプトを渡してしまっている開発者の問題だ。これらの脆弱性は無防備なウェブサイトのコードを利用して機能するため、エンドユーザーが XSS 攻撃から身を守るためにできることは多くない。

だからといって、XSS 攻撃防止に関してユーザーにできることが何もないわけではないが、選択肢は限られている。信頼できそうにないウェブサイトに対する防御を強化したい人は、以下のヒントを参考にしてほしい。

- ウェブサイトへのログインを求める電子メールリンクは、絶対にクリックしてはならない。フィッ

中間者攻撃、Man-in-the-Disk 攻撃、クロスサイトスクリプティング攻撃

サイバー攻撃を知る

シングが目的かもしれないし、クロスサイトスクリプトが大量に埋め込まれていて（正規のウェブサイトにつながる場合でも）、金銭を奪われるかもしれない。ログインリンクをクリックするよう求める電子メールを受信したら、そのリンクをたどるのではなく、必ずブラウザを開いてアカウントにサインインするようにしよう。

- 「ScriptSafe」（Chrome） や「NoScript」（Firefox）など、スクリプトをブロックするブラウザアドオンを使おう。これらのアドオンは、手動で許可しない限り、スクリプトの実行を完全にブロックする。これなら XSS 攻撃の実行を阻止できるはずだ。
- ソーシャルメディアの投稿やプライベートメッセージに違和感を覚えたら、リンクをクリックしてはならない。乗っ取られたアカウントは、よくマルウェアの拡散や XSS 攻撃の実行に使われる。それを避けるには、フィッシング電子メールを回避する場合と同じように警戒する必要がある。