|  |  |
| --- | --- |
| ナンバリング | {report\_number} |
| 日付 | {report\_date} |

**{target\_host}**

**プラットフォームAPIファジー検出レポート**

Version 1.2

2020年12月

© 2020 Packer FuzzeR团队

Poc-Sir、KpLi0rn、Liucy、RachesseHS、Lupin-III

* **著作権表示**

Packer Fuzzerテストレポート（以下、このレポートと呼びます）テンプレートの著作権は、Packer Fuzzer開発チーム（以下、チームと呼びます）に属し、法律で保護されています。 チームには、このレポートテンプレートを変更および解釈する権利があります。 このレポートテンプレートの内容を変更する場合、対応する著作権ステートメントを保持する必要があります。 チームの許可なしに、Packer Fuzzerツール（以下、このツールと呼びます）を商用目的で使用することは一切できません。 上記の声明に違反する個人または企業の場合、チームは法的責任をさらに追求する権利を留保します。

* **該当ステートメント**

このレポートは、このツールによって検出されたすべてのターゲットシステムに適用されます。安全な場所に保管し、ターゲットシステムの所有者の許可なしに送信しないでください。

* **免責事項**

このレポートは、ユーザーのテスト結果に基づいてツールによって自動的に生成されるレポートであり、レポートの内容はチームの立場や意見を表すものではありません。 このツールによって提供される検出機能の普及および使用によって引き起こされる直接的または間接的な結果および損失は、ユーザー自身の責任であり、チームはこれについて責任を負いません。 このツールを使用するときは、ユーザーおよびターゲットシステムが配置されている国の関連する法律および規制に従ってください。

* **改訂記録**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **バージョン番号** | **更新日** | **改訂者** | **変更ログ** | **承認者** |
| 1.0 | 2020/8/9 | Liucy | 无 | Poc-Sir |
| 1.2 | 2020/12/18 | Liucy | Add More | Poc-Sir |

**一．レポートの概要**

スキャンされたプラットフォーム：{target\_host}

入力されたパラメータ値：{target\_url}

このスキャンは{scan\_type}スキャンモードを使用し、スキャンIPとして{scan\_ip}を使用します。これには合計で{scan\_time}秒かかります。

スキャン時間：{start\_time}

スキャン完了時間：{end\_time}

このスキャンで合計{api\_num}個の有効なAPIインターフェースが見つかりました。

合計{js\_num}個の関連するJSファイルが見つかりました：

{js\_list}

高リスク{vuln\_h\_num}、中リスク{vuln\_m\_num}、低リスク{vuln\_l\_num}など、合計{vuln\_num}個のセキュリティ脆弱性が発見されました。 彼らです：

{vuln\_list}

追加のCookie情報は：{extra\_cookies}

追加の送信ヘッダー情報は：{extra\_head}

**このツールによる分析後、ターゲットプラットフォームのセキュリティリスクレベルは：**{sec\_lv}

**二．脆弱性の詳細**

{vuln\_deta}

**三．APIリスト**

{api\_list}

**四．安全アドバイス**

{suggest\_foryou}

**五．追加の内容**

extra

**六．付録**

* **脆弱性の説明**

CORSの脆弱性：クロスドメインのリソース共有により、ブラウザーの同一生成元ポリシーが緩和され、ブラウザーを介して異なるWebサイトと異なるサーバー間の通信が可能になります。ユーザーがCORS設定vuln.comを含むWebサイトにログインし、同時に攻撃者から提供されたリンクevil.comにアクセスするとします。 evil.com Webサイトはvuln.comにリクエストを送信して機密データを取得します。ブラウザが情報を受信できるかどうかは、vuln.comの設定によって異なります。 vuln.comがAccess-Control-Allow-Originヘッダーで構成されており、それが予期されている場合、それを受信することが許可されます。それ以外の場合、同じ生成元のポリシーのため、ブラウザーはそれを受信しません。

不正アクセスの脆弱性：名前が示すように、インターフェースへの不正アクセスは、認証を要求せずに、対応するビジネスロジック機能に直接アクセスして操作することができます。これは通常、認証ページの欠陥、認証なし、不適切なセキュリティ設定などが原因で発生します。

機密情報漏えいの脆弱性：情報漏えいは、WebサイトページまたはJSファイル内の機密情報の漏えいを指します。この機密情報を通じて、攻撃者はサーバーにさらに侵入することができます。

水平方向の超権限の脆弱性：超権限の脆弱性とは、アプリケーションが現在のユーザー操作のIDと権限を厳密に検証しないため、ユーザーが自分の管理権限の範囲を超えて機能を操作できるため、ユーザーが操作できない一部の動作を操作することを指します。権限レベルを超えると、同じレベルのユーザーが、名前、携帯電話番号、連絡先住所、個人情報、注文記録など、お互いの機密情報にアクセスすることになります。同時に、同じ権限を持つ他のユーザーとして、削除、追加、変更などの特定の機能を実行することもできます。

SQLインジェクションの脆弱性：SQLインジェクションの脆弱性の理由は、Webサイトアプリケーションが、書き込み時にユーザーがサーバーに送信したデータの有効性（タイプ、長さ、ビジネスパラメーターの合法性など）を検証せず、ユーザーが入力したデータを検証しなかったためです。ローカルの特殊文字フィルタリングにより、ユーザーの入力がデータベースに直接実行され、SQLステートメントの元の設計の予想される結果を超え、SQLインジェクションの脆弱性が発生します。

脆弱なパスワードの脆弱性：Webサイトの管理および運用担当者のセキュリティ意識が不十分であるため、便宜上、パスワードを忘れないようにするために、覚えやすいパスワードを使用するか、システムのデフォルトパスワードを直接使用します。攻撃者はこの脆弱性を利用して、アプリケーションシステムまたは管理システムに直接侵入することで、システム、Webページ、およびデータを改ざんおよび削除し、システムおよびユーザーデータを不正に取得し、サーバーを落下させる可能性さえあります。

任意のファイルアップロードの脆弱性：アプリケーションシステムは、ファイルアップロード機能でユーザーがアップロードしたファイルのタイプ、形式、およびコンテンツの合法性をチェックし、攻撃者に悪意のあるスクリプトファイルまたは予期しないWebshel​​l（.php、.jsp、aspなど）をアップロードさせます。 HTMLファイル、SHTMLファイルなどのファイルをフォーマットします。同時に、ディレクトリジャンプなどの文字を使用したり、アップロードディレクトリを制御して、ファイルをWebディレクトリまたは任意のディレクトリに直接アップロードしたりすることができます。これにより、リモートサーバーで任意の悪意のあるスクリプトファイルが実行される可能性があります。アプリケーションのシステム権限を直接取得します。

* **脆弱性レベル**

このレポートには、低リスク、中リスク、高リスクの3つの脆弱性レベルが組み込まれています。 中でも、リスクの高い脆弱性のタイプには、弱いパスワードの脆弱性、任意のファイルアップロードの脆弱性、SQLインジェクションの脆弱性が含まれます。 ：CORSの脆弱性。

このうち、信頼度が「低」の検出結果は、脆弱性レベルの被害を自動的に軽減し、すでに脆弱性レベルが最低の場合はダウングレードされません。 たとえば、特定の脆弱性は次のとおりです。SQLインジェクションの脆弱性。これはリスクの高い脆弱性であるはずですが、その信頼度は「低い」ため、リスクは中程度の脆弱性に自動的にダウングレードされます。

* **リスクレベル**

このレポートには、スコアリング評価モデルを使用して、リスクなし、低リスク、中リスク、高リスクの4つのリスクレベルが組み込まれており、対応するスコアレベルは0、5、10、18です。 対応する脆弱性グレードのポイントは、低リスクの場合は1ポイント、中リスクの場合は2ポイント、高リスクの場合は6ポイントです。 たとえば、スキャンで合計1つの高リスク、2つの中リスク、および5つの低リスクの脆弱性が見つかり、スコアの計算方法は次のとおりです。1x 6 + 2 x 2 + 5 x 1 = 15（ポイント）、スコアは10より大きく、 18未満なので、リスクレベルは「中程度のリスク」です。

**（レポートの終わり、下は空白）**