一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

頻繁に悪用される脆弱性の広域スキャンシステムによる検出精度評価に向けて

青山　航大[†]　大塚　瑠莉[†,††] YinMinn Pa Pa[††]　吉岡　克成[†††]

† 横浜国立大学大学院環境情報学府　〒240-8501 神奈川県横浜市保土ケ谷区常盤台 79-7
†† 横浜国立大学大学院先端科学高等研究院　〒240-8501 神奈川県横浜市保土ケ谷区常盤台 79-7
††† 横浜国立大学大学院環境情報研究院/先端科学高等研究院　〒240-8501 神奈川県横浜市保土ケ谷区常盤 79-7
E-mail: †{aoyama-koudai-my,otsuka-ruri-dk}@ynu.jp, ††{yinminn-papa-jp,yoshioka}@ynu.ac.jp

あらまし　広域スキャンシステムは, Web サーバや IoT 機器など, インターネットに接続された様々なデバイスやシステムを調査できるウェブサービスである. これらのシステムは, インターネットを網羅的にスキャンし, 発見されたホスト上で動作するネットワークサービスやアプリケーションの種類, バージョン, 脆弱性情報等を提供する. 本研究では, まず悪用が確認された脆弱性のリストである KEV (Known Exploited Vulnerabilities) カタログと共通脆弱性評価システム CVSS (Common Vulnerability Scoring System) v3.1 に基づき、頻繁に悪用される脆弱性をいくつか選出する. 次に、安全に管理された環境でこれらの脆弱性を有するサービスを動作させ，代表的な広域スキャンシステムである Shodan と Censys がこれらのサービスとその脆弱性を正しく検出できるかを検証する.

キーワード　広域スキャンシステムスキャナー, Shodan, Censys, 脆弱性評価

Towards Evaluating the Detection Accuracy of Internet-Wide Scanners for Frequently Exploited Vulnerabilities

Aoyama KOUDAI[†], Ruri OTSUKA[†,††], Yin MINN PA PA[††], and Yoshioka KATSUNARI[†††]

† Graduate School of Environment and Information Sciences, Yokohama National University
79-7 Tokiwadai, Hodogaya-ku, Yokohama, 240-8501 JAPAN
†† Institute of Advanced Sciences, Yokohama National University
79-7 Tokiwadai, Hodogaya-ku, Yokohama, 240-8501 JAPAN
††† Faculty of Environment and Information Sciences, Yokohama National University / Institute of Advanced Sciences, Yokohama National University　79-7 Tokiwadai, Hodogaya-ku, Yokohama, 240-8501 JAPAN
E-mail: †{aoyama-koudai-my,otsuka-ruri-dk}@ynu.jp, ††{yinminn-papa-jp,yoshioka}@ynu.ac.jp

Abstract　Internet-wide scanning systems are web services that can survey various devices and systems connected to the Internet, including web servers and IoT devices. These systems comprehensively scan the Internet, providing information such as the types, versions, and vulnerability information of network services and applications running on discovered hosts. In this study, we first select several frequently exploited vulnerabilities based on the KEV (Known Exploited Vulnerabilities) catalog, a list of vulnerabilities confirmed to be exploited, and the Common Vulnerability Scoring System (CVSS) v3.1. Next, we operate services with these vulnerabilities in a securely managed environment and verify whether representative internet-wide scanning systems, Shodan and Censys, can correctly detect these services and their vulnerabilities.

Key words　Internet-wide scanners, Shodan, Censys, vulnerability assessment

1. はじめに

インターネットの普及とデジタル化の進展に伴い, 企業や個人が利用するサービスの数は飛躍的に増加している. これにより, サイバー攻撃の手法も多様化・高度化し, 未発見の脆弱性を狙った攻撃が頻発している. 特に, インターネットに公開されたサービスは攻撃者にとって容易にアクセス可能なターゲットとなるため, これらの脆弱性の早期発見と効果的な対策が強く求

められている. Attack Surface Management（ASM）は, 組織が所有する全てのデジタル資産を特定し, それらに存在する脆弱性を明確化し, 修復の優先順位を設定することで, 潜在的な攻撃面を効果的に削減し, サイバー侵害のリスクを最小限に抑えるために不可欠な手法である [1].

しかしながら, セキュリティの研究者やシステム管理者などのサイバーセキュリティの専門家が ASM の一環として Shodan [2] や Censys [3] といったインターネットスキャニングツールを活用しているにもかかわらず, これらのツールが提供する脆弱性情報の信頼性については十分に検証されていない現状がある.

関連研究においては, Li [4] らおよび Bennett ら [5] の研究が存在し, Shodan と Censys のスキャン頻度やポート検出率に焦点を当てた比較がなされているが, 脆弱性検出能力といったセキュリティ面での評価は十分に行われていない. 本研究では, この課題を明確化し,「Shodan と Censys の脆弱性検出はどの程度正確か？」というリサーチクエスチョンを設定した.

本研究では, 以下の 2 つの観点から Shodan と Censys の脆弱性検出能力を評価した. 第一に, 悪用された場合に被害が深刻となる脆弱性（CVSS スコア [7] が V3.1 で 9 以上）および実際に攻撃に利用された脆弱性（Known Exploited Vulnerabilities, KEV [6]）を持つ Web サービス（Apache HTTP Server, Nginx）の脆弱性について検証した. 第二に, Web サービスの各バージョンに存在する既知の脆弱性についても調査を行った. 例えば, Apache 2.4.50 には, 既知の脆弱性が 32 個存在しており, それら全てをスキャナーが検知できているかを調査した.

これらの評価を行うために, Docker コンテナを用いて Apache と Nginx をインターネット上で動作させ, グローバル IP アドレス 1 つに対して 1 つのサービスバージョンを割り当てて運用した. 各サービスにおいて, CVSSv3.1 スコア 9.0 以上かつ KEV カタログに登録された脆弱性を含むバージョンを 20 種類選択し, 正解データとして CVE Details, National Vulnerability Database (NVD) [8], および各サービスの公式ドキュメントを用い, 各バージョンに存在する脆弱性を判定した. 具体的には, CVSS スコアが V3.1 で 9 以上の脆弱性および実際に攻撃に利用された脆弱性（KEV）を対象とし, さらに選定した各バージョンに存在する全ての脆弱性についてスキャナーの検知結果を確認した. 第一の脆弱性カテゴリーを CVSS スコアが V3.1 で 9 以上の脆弱性および実際に攻撃に利用された脆弱性とし, 第二の脆弱性カテゴリーを各バージョンに存在する全ての脆弱性とする.

実験の結果, 第一の脆弱性カテゴリーにおいては, Shodan および Censys の両ツールともに Nginx に存在する脆弱性において見落としや誤検知がないことが判明した. しかし, Apache に存在する脆弱性に対して, Shodan と Censys のスキャン結果は, 誤検知や見逃しが存在した. 具体的には Shodan では, 3 つのバージョンで誤検知し, 16 個のバージョンでは, 1 つの脆弱性を見逃した. 一方で, Censys では, 1 つのバージョンで誤検知し, 16 個のバージョンで 2 つ, 3 つのバージョンで 1 つの脆弱性を見逃した. 一方, 第二の脆弱性カテゴリーにおいては, Shodan と Censys どちらも, Apache と Nginx に関して見逃した脆弱性が存在した. Shodan では Nginx, Censys では Apache の脆弱性を多く見逃していた. また, Apache HTTP Server のスキャン結果に関して, Censys の誤検知は 1 件のみであったが, Shodan は用意した 20 バージョン全て, 10 件以上の脆弱性を誤検知した.

本研究の貢献は以下の通りである. 第一に, Shodan と Censys のサービスごとの脆弱性検出能力を明らかにした. 第二に, これらのサービスによって検出される脆弱性の種類および検出精度の差異を示し, これにより脆弱性の確認の際に Shodan や Censys を選定する際の参考となる知見を提供した.

2. 関 連 研 究

広域スキャンシステムの比較研究において, Shodan と Censys の性能評価が複数の研究で報告されている.

Li ら [4] は, スキャン頻度の比較評価を行い, HTTPS ポートに対して Censys が 1 日間隔, Shodan が 9 日間隔でスキャンを実施し, HTTP ポートでは Censys が 2 日間隔, Shodan が 10 日間隔であることを明らかにした. さらに, サポートするプロトコル数においても, Shodan が 185 種類, Censys が 34 種類と Shodan の方が多くのプロトコルをサポートしており, 両エンジンの特性の違いが示された. Bennett ら [5] は, 世界 5 地域（サンノゼ, 東京, モントリオール, パリ, サンパウロ）に VM を設置し, FTP, SSH, HTTP, HTTPS の 4 つのサービスに対する 47 日間の実証実験を実施した. その結果, 両エンジンが 24 時間以内に検索結果を更新でき, 1 日あたりのスキャン回数は Shodan が 176 回, Censys が 411 回であることを示した.

これらの研究により, Shodan と Censys の基本的な性能の違いが明らかになった一方で, 脆弱性検知能力や検出精度などのセキュリティ面での評価は十分に行われていない. 本研究では, この点に着目した評価を行うことで, 広域スキャンシステムの新たな知見の提供を目指す.

3. 調 査 手 法

本研究では, リサーチクエスチョン「Shodan と Censys の脆弱性検出はどの程度正確か？」に基づき, Shodan と Censys の脆弱性検出能力を評価するための実験を実施した. 本節では, サービスの選定理由, 脆弱性に基づく選定方法, 実験環境の準備手順, およびデータ収集方法について詳細に述べる.

3.1 サービスの選定

本研究では, インターネット上で広く利用され, 過去に深刻な脆弱性が報告されている Web サーバである Apache HTTP Server および Nginx を対象とした. これらのサービスは無償で利用可能であり, Docker などのコンテナ技術を用いることで複数のバージョンを容易に設定できるため, 再現性の高い実験環境構築に適している. また, W3Techs [9] の調査によれば, Apache HTTP Server と Nginx が Web サーバ市場でトップ 2 のシェアを占めており, 実務的にも重要な評価対象であることから選定した.

3.2 脆弱性に基づくバージョン選定方法

サービス選定後, 各サービスに関してバージョンを選定する. 選定の際には, Known Exploited Vulnerabilities catalog(KEV) と Common Vulnerability Scoring System(CVSS) を基準とする.

KEV は, 米国 CISA (Cybersecurity and Infrastructure Security

Agency) が公開している, 過去および現在において実際に攻撃が行われていることが確認された脆弱性を中心にリスト化したカタログである.

CVSS は, 脆弱性の重大性を数値化する標準的な評価スキームであり, 攻撃ベクトルや影響範囲など複数の要因を統合して 0.0〜10.0 の数値スコアを与える仕組みである. スコアが 0.0 から 10.0 まで設定されており, スコアが大きくなるにつれて, 攻撃者が悪用した場合の被害が重大化しやすい脆弱性となる. 今回, CVSS に関しては, Common Vulnerability Scoring System Version 3.1 を使用する.

各サービスに対して 20 のバージョンを選定し, その中に KEV に登録されている脆弱性が存在してるバージョンや, CVSS スコアが 9.0 以上の脆弱性があるバージョン, そしてパッチ適用済みのバージョンを混在させた. バージョンごとに存在している脆弱性を確定する際は, CVE-Details, 各サービス公式ドキュメント, および National Vulnerability Database（NVD）を参照し, 確認した.

具体的には, Apache HTTP Server や Nginx において KEV に該当する脆弱性が含まれるバージョン（例：Apache HTTP Server 2.4.49）を複数ピックアップし, 実際に攻撃された事例がある CVE を調査対象に含めることで, 「実際にサイバー攻撃に狙われている脆弱性」が見落とされないかを重視した. さらに, CVSS v3.1 で 9.0 以上（Critical）の脆弱性を持つバージョンを選定し, 潜在的に高リスクな脆弱性の検出能力を評価した. また, 同一マイナーバージョンでもパッチ適用によって脆弱性が修正されているバージョンを 1〜2 種含めることで, 誤検知が起きないかを評価するための対照群とした.

このように 20 バージョンという上限を設定したのは, サービスごとのリリース履歴をすべてカバーしようとすると解析対象が膨大になり, 実際に Docker 上で動かして評価するコストが莫大になるためである. 一方で, 2〜3 バージョンしか用意しないと, 重要な脆弱性パターンを見落とすか, パッチ済み・未パッチ両方を包括できない恐れがある. 結果的に, KEV 該当の脆弱性を持つバージョン, CVSS 高リスク脆弱性を持つバージョン, 安定版パッチ済みバージョン, 最新版などが混在する形でバージョンを選定し, 合計 20 に収束させる形が妥当と判断した. 選定したバージョンの一覧を図 1 に示す.

Apache	nginx
2.2.32	1.0.15
2.2.34	1.4.7
2.4.2	1.6.3
2.4.6	1.8.1
2.4.10	1.10.3
2.4.18	1.11.13
2.4.32	1.12.2
2.4.33	1.14.0
2.4.34	1.14.2
2.4.37	1.15.12
2.4.41	1.16.1
2.4.47	1.18.0
2.4.48	1.20.0
2.4.50	1.20.2
2.4.51	1.21.4
2.4.52	1.21.6
2.4.57	1.22.0
2.4.58	1.22.1
2.4.60	1.23.4
2.4.62	1.27.2

図 1: 評価実験に用いたサーバプログラムのバージョン

3.3 実験環境の準備

実験には, フィルタフリーネットワークを用いた. フィルタフリーネットワークとは, 特定の IP レンジを使用し, 外部からのアクセスを制限しないネットワーク環境を指す. 本研究では, フィルタフリーネットワークを構築し, 外部からのアクセスを制限しない環境を整備した. これにより, Shodan および Censys によるスキャンが正確に行われることを保証した.

さらに, Docker コンテナが悪用された場合に備え, iptables [10] という linux に実装されているパケットフィルタリング型のファイヤーウォールの機能を設定し, 確立された通信以外の通信は遮断するようにした. また, 確立された通信に関してはポート 80 での通信のみを許可し, それ以外のポートは拒絶している. さらに, 確立された通信以外では外部への通信ができないように設定した.

3.3.1 Docker の準備

本研究では, 軽量な仮想化技術である Docker を活用し, Apache HTTP Server および Nginx の各バージョンをインターネット上で動作させる環境を構築した. グローバル IP アドレス 1 つに対して 1 つのサービスバージョンを割り当て, 各サービスの 20 種類のバージョンをデプロイした. 各バージョンは HTTP ポート（ポート 80）で動作させ, 統一されたアクセス条件下での検証を行った.

具体的には, グローバル IP アドレスを各サービスに 20 個ずつ割り当て, 計 40 個のコンテナを運用した. これにより, 各サービスの異なるバージョンが同時に運用され, Shodan および Censys によるスキャンが各バージョンごとに独立して行われる環境を実現した. また, Docker コンテナに対して Privilege 権限を付与しないように設定し, セキュリティリスクを低減した.

3.4 データ収集方法

3.4.1 正解データ収集方法

広域スキャンサービスが正しく検知できているか評価するには, 各サービスの各バージョンに存在する脆弱性, すなわち正解データとの照合が不可欠である.

正解データとしては, CVE-Details [11] から取得した脆弱性リストや NVD, 公式のドキュメントを用いた. 具体的には, CVE-Details の API を活用し, Apache HTTP Server および Nginx の各バージョンが保持する CVE 情報を取得し, それらをバージョン単位で JSON ファイルとして保存した. この JSON ファイルには, 各バージョンに紐づくすべての CVE ID が含まれており, 本研究の評価においては「スキャナーが, この JSON ファイル内の CVE を検知できるか」が主たる基準となる. つまり, Shodan や

Censys が検知した脆弱性リスト（CVE タグなど）と正解データを比較することで, どの程度正確に脆弱性を検出・報告できているかを定量的に検証する.

3.4.2 Shodan / Censys からのスキャンデータ収集

テストベッドとして構築した Docker コンテナ上のサービス（前述の複数バージョン）をインターネットに公開し, 2024 年 10 月 6 日から 2024 年 11 月 20 日までの約 1 か月半にわたって, Shodan および Censys からのスキャンデータを収集した. 具体的には, 両スキャナーの API を用い, 毎日 2 回（12 時間おき）API 呼び出しを行い, 最新のバナー情報や脆弱性情報（CVE ID）が含まれる JSON データを取得した. 取得したデータには, スキャナーが検出したポート番号, サービスのバージョン, そして該当する脆弱性（CVE ID）の一覧が含まれる.

最終的には, 観測期間中に得られた複数回のスキャン結果のうち最新の情報を用いて正解データとの照合を実施した. たとえば, Shodan が 10 月某日にバージョン誤認を起こしていても, 後日のスキャンで修正される可能性があるため, 最新データを用いることでスキャナーの最新の検知性能を評価できるように配慮した.

以上の方法により, (1) 事前に確立したバージョン別の脆弱性情報（正解データ）と, (2) 実際に Shodan および Censys が報告する脆弱性データを照合することで, サービスのバージョンや脆弱性の深刻度ごとに見逃した脆弱性数や誤検知した脆弱性数などの指標を算出し, スキャナーの脆弱性検出能力を総合的に評価する.

4. 評 価 方 法

(1) 深刻な脆弱性の検知状況の評価

この評価では, 実際に攻撃に利用された, またはリスクが高い脆弱性（CVSSv3 スコア 9.0 以上または KEV 登録）のうち, どれだけ正しく検知できるかを重視する. 評価は, 以下の 3 つの観点に基づく.

（1） **正しい検知:** 正解データに含まれる深刻な脆弱性を正しく検知できた場合.

（2） **見逃し:** 正解データに含まれる深刻な脆弱性を検知できなかった場合.

（3） **誤検知:** 正解データに含まれない脆弱性のうち, CVSSv3 スコア 9.0 以上または KEV 登録されているものを誤って報告した場合.

例として, あるバージョンに以下の脆弱性が存在するとする：

- CVE-2023-A（CVSSv3 9.2）
- CVE-2023-B（KEV 登録）
- CVE-2023-C（CVSSv3 7.5）

スキャナーが以下の脆弱性を報告した場合：

- CVE-2023-A
- CVE-2023-C
- CVE-2023-X（存在しない脆弱性, CVSSv3 9.1）
- CVE-2023-Y（存在しない脆弱性, CVSSv3 7.5）

この場合, 深刻な脆弱性の評価では, 正しい検知は 1 件（CVE-2023-A）, 見逃しは 1 件（CVE-2023-B）, 誤検知は 1 件（CVE-2023-X）と評価される.

なお, CVE-2023-C および CVE-2023-Y は深刻な脆弱性には該当しないため, 本評価では考慮しない.

(2) 各バージョンに存在する全脆弱性の検知状況の評価

各バージョンに存在する全ての脆弱性について, CVSS スコアのカテゴリ（Critical, High, Medium, Low）ごとの検知状況を評価する. この評価では, 以下の観点に基づく.

（1） **正しい検知:** 正解データに含まれる脆弱性を正しく検知できた場合.

（2） **見逃し:** 正解データに含まれる脆弱性を検知できなかった場合.

（3） **誤検知:** 正解データに含まれない脆弱性を誤って報告した場合.

同じ例において, CVSS スコアのカテゴリ別評価では, 正しい検知は 2 件（CVE-2023-A および CVE-2023-C), 見逃しは 1 件（CVE-2023-B), 誤検知は 2 件（CVE-2023-X および CVE-2023-Y）と評価される. この評価方法では, CVSS スコアに関係なく, すべての脆弱性の検知状況を評価対象とする点が, 前述の深刻な脆弱性の評価方法と異なる.

5. 実 験 結 果

5.1 深刻な脆弱性に対する検知結果

Apache HTTP Server に存在する, 深刻な脆弱性の検知結果を図 2 に示す. 図 2 は, 横軸に Apache HTTP Server のバージョン（2.2.32 から 2.4.62), 縦軸に脆弱性の数を示している. 各バージョンについて, 灰色のバーは実際に存在する脆弱性の数（Expected Vulnerabilities), 青色のバーは Shodan が検知した脆弱性の数 (Shodan Detected), 薄い赤色のバーは Shodan が検知できなかった脆弱性の数（Shodan undetected), 赤色のバーは Shodan による誤検知の数（Shodan False Positive）を示している. 同様に, オレンジ色のバーは Censys が検知した脆弱性の数（Censys Detected), 薄い赤色のバーは Censys が検知できなかった脆弱性の数（Censys undetected), 赤色のバーは Censys による誤検知の数（Censys False Positive）を表している.

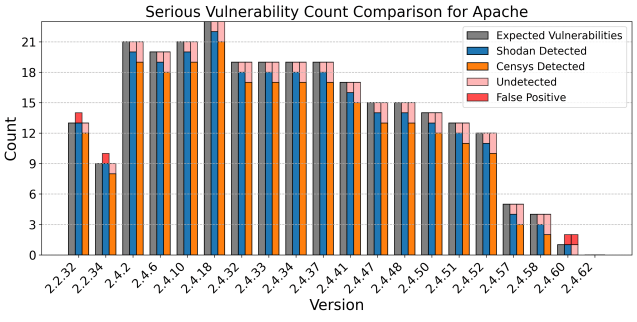

図 2: 深刻な脆弱性に対する検知結果:Apache

Shodan は, バージョン 2.2.32, 2.2.34, 2.4.60 において誤検知が確認された. また, 2.4.2〜2.4.58 までのバージョンでそれぞれ 1 件の見逃しが確認された. 見逃しがおきたバージョンは全て同一の脆弱性で CVE-2024-38475 であることが判明した. それ以

外の脆弱性については, 正しく検知した.

一方, Censys は調査対象の 20 バージョンのうち, 脆弱性が存在しない 2.4.62 を除く 19 バージョンにおいて, 脆弱性の見逃しが確認された. バージョン 2.2.32, 2.2.34, 2.4.60 では, それぞれ 1 件の見逃しが確認され, 2.4.2〜2.4.58 ではそれぞれ 2 件の見逃しが確認された. バージョン 2.2.32〜2.4.60 で見逃された脆弱性は共通しており CVE-2024-40898 であった. また, この脆弱性に加え, バージョン 2.4.2〜2.4.58 では, 全て同一の脆弱性で CVE-2024-38475 であることが判明した. さらに, バージョン 2.4.60 において 1 件の誤検知が観察された.

Nginx に存在する, 深刻な脆弱性の検知状況を図 3 に示す（図 2 と同様の形式）.

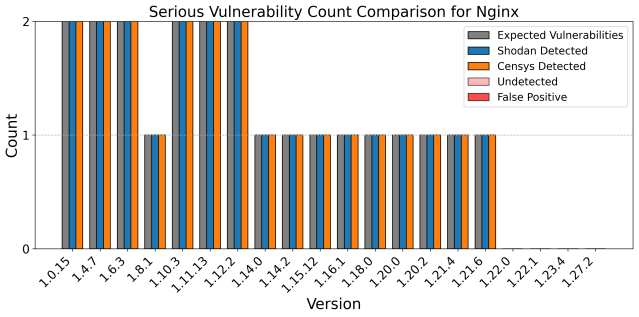

図 3: 深刻な脆弱性に対する検知結果:Nginx

Shodan と Censys は全てのバージョンにおいて完全に検知結果が一致した. 両スキャナーとも, 存在する深刻な脆弱性を全て正しく検知し, 見逃しや誤検知は観測されなかった.

5.2 各バージョンに存在する全脆弱性の検知結果

Apache HTTP Server における全脆弱性の検知状況を図 4 に示す. 図 4 は, 横軸に Apache HTTP Server のバージョン（2.2.32 から 2.4.62), 縦軸に脆弱性の数を示している. 各バージョンについて, 左から順に実際に存在する脆弱性（Expected Vulnerabilities), Shodan の検知結果, Censys の検知結果を示している. 脆弱性は CVSS スコアに基づき以下の色で分類している：

（1） **Critical (CVSSv3 ≥ 9.0):** 赤色
（2） **High (7.0 ≤ CVSSv3 < 9.0):** オレンジ色
（3） **Medium (4.0 ≤ CVSSv3 < 7.0):** 黄色
（4） **Unknown (CVSSv3 スコアがない脆弱性):** 緑色
（5） **検知できなかった脆弱性:** 薄いピンク (Undetected)
（6） **誤検知した脆弱性:** 灰色 (False Positive)

Shodan では, すべてのバージョンにおいて誤検知が確認された. 特に, 脆弱性が存在しないバージョン 2.4.62 においても脆弱性が存在すると誤検知された.

一方, Censys では Shodan と比較して誤検知が少なく, バージョン 2.4.60 での 1 件のみ確認された.

さらに, Shodan および Censys のいずれのスキャナーにおいても, 脆弱性の見逃し（Undetected）が存在することが明らかとなった. 特に, Censys では見逃された脆弱性の数が Shodan よりも多い傾向が見られた. Apache の各バージョンにおける Shodan の脆弱性の見逃し数/見逃し率, 図 5 に, Censys の脆弱性の見逃し数/見逃し率を図 6 に示す.

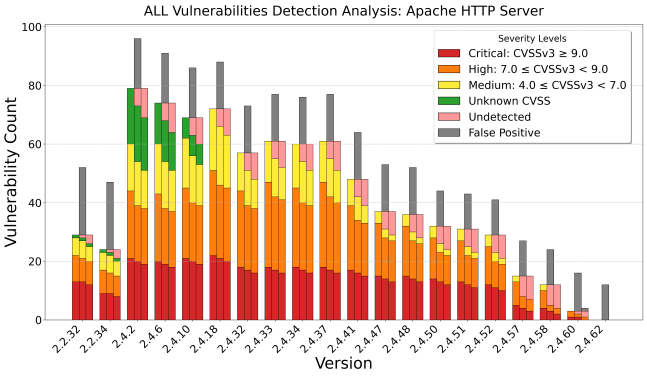

図 4: 各バージョンに存在する全脆弱性の検知結果:Apache

Version	UNKNOWN	MEDIUM	HIGH	CRITICAL	Total
2.2.32	0/1 (0.0%)	0/6 (0.0%)	1/9 (11.1%)	0/13 (0.0%)	1/29 (3.4%)
2.2.34	0/1 (0.0%)	0/6 (0.0%)	1/8 (12.5%)	0/9 (0.0%)	1/24 (4.2%)
2.4.2	0/19 (0.0%)	1/16 (6.2%)	4/23 (17.4%)	1/21 (4.8%)	6/79 (7.6%)
2.4.6	0/14 (0.0%)	1/17 (5.9%)	4/23 (17.4%)	1/20 (5.0%)	6/74 (8.1%)
2.4.10	0/7 (0.0%)	1/17 (5.9%)	4/24 (16.7%)	1/21 (4.8%)	6/69 (8.7%)
2.4.18	-	1/21 (4.8%)	4/29 (13.8%)	1/22 (4.5%)	6/72 (8.3%)
2.4.32	-	1/13 (7.7%)	4/26 (15.4%)	1/18 (5.6%)	6/57 (10.5%)
2.4.33	-	1/14 (7.1%)	4/29 (13.8%)	1/18 (5.6%)	6/61 (9.8%)
2.4.34	-	1/15 (6.7%)	4/27 (14.8%)	1/18 (5.6%)	6/60 (10.0%)
2.4.37	-	1/14 (7.1%)	4/29 (13.8%)	1/18 (5.6%)	6/61 (9.8%)
2.4.41	-	1/9 (11.1%)	4/22 (18.2%)	1/17 (5.9%)	6/48 (12.5%)
2.4.47	-	1/4 (25.0%)	4/18 (22.2%)	1/15 (6.7%)	6/37 (16.2%)
2.4.48	-	1/4 (25.0%)	4/17 (23.5%)	1/15 (6.7%)	6/36 (16.7%)
2.4.50	-	1/4 (25.0%)	4/14 (28.6%)	1/14 (7.1%)	6/32 (18.8%)
2.4.51	-	1/4 (25.0%)	4/14 (28.6%)	1/13 (7.7%)	6/31 (19.4%)
2.4.52	-	1/4 (25.0%)	4/13 (30.8%)	1/12 (8.3%)	6/29 (20.7%)
2.4.57	-	2/2 (100.0%)	4/8 (50.0%)	1/5 (20.0%)	7/15 (46.7%)
2.4.58	-	2/2 (100.0%)	4/6 (66.7%)	1/4 (25.0%)	7/12 (58.3%)
2.4.60	-	-	1/2 (50.0%)	0/1 (0.0%)	1/3 (33.3%)
Total	**0/42 (0.0%)**	**18/172 (10.5%)**	**66/339 (19.5%)**	**16/273 (5.9%)**	**100/826 (12.1%)**

図 5: Shodan の脆弱性の見逃し数/見逃し率:Apache

Version	UNKNOWN	MEDIUM	HIGH	CRITICAL	Total
2.2.32	0/1 (0.0%)	1/6 (16.7%)	1/9 (11.1%)	1/13 (7.7%)	3/29 (10.3%)
2.2.34	0/1 (0.0%)	1/6 (16.7%)	1/8 (12.5%)	1/9 (11.1%)	3/24 (12.5%)
2.4.2	1/19 (5.3%)	3/16 (18.8%)	4/23 (17.4%)	2/21 (9.5%)	10/79 (12.7%)
2.4.6	1/14 (7.1%)	3/17 (17.6%)	4/23 (17.4%)	2/20 (10.0%)	10/74 (13.5%)
2.4.10	0/7 (0.0%)	3/17 (17.6%)	4/24 (16.7%)	2/21 (9.5%)	9/69 (13.0%)
2.4.18	-	3/21 (14.3%)	4/29 (13.8%)	2/22 (9.1%)	9/72 (12.5%)
2.4.32	-	3/13 (23.1%)	4/26 (15.4%)	2/18 (11.1%)	9/57 (15.8%)
2.4.33	-	3/14 (21.4%)	4/29 (13.8%)	2/18 (11.1%)	9/61 (14.8%)
2.4.34	-	3/15 (20.0%)	4/27 (14.8%)	2/18 (11.1%)	9/60 (15.0%)
2.4.37	-	3/14 (21.4%)	5/29 (17.2%)	2/18 (11.1%)	10/61 (16.4%)
2.4.41	-	3/9 (33.3%)	4/22 (18.2%)	2/17 (11.8%)	9/48 (18.8%)
2.4.47	-	2/4 (50.0%)	4/18 (22.2%)	2/15 (13.3%)	8/37 (21.6%)
2.4.48	-	2/4 (50.0%)	4/17 (23.5%)	2/15 (13.3%)	8/36 (22.2%)
2.4.50	-	2/4 (50.0%)	4/14 (28.6%)	2/14 (14.3%)	8/32 (25.0%)
2.4.51	-	2/4 (50.0%)	4/14 (28.6%)	2/13 (15.4%)	8/31 (25.8%)
2.4.52	-	2/4 (50.0%)	4/13 (30.8%)	2/12 (16.7%)	8/29 (27.6%)
2.4.57	-	2/2 (100.0%)	4/8 (50.0%)	2/5 (40.0%)	8/15 (53.3%)
2.4.58	-	2/2 (100.0%)	4/6 (66.7%)	2/4 (50.0%)	8/12 (66.7%)
2.4.60	-	-	1/2 (50.0%)	1/1 (100.0%)	2/3 (66.7%)
Total	**2/42 (4.8%)**	**43/172 (25.0%)**	**67/339 (19.8%)**	**34/273 (12.5%)**	**146/826 (17.7%)**

図 6: Censys の脆弱性の見逃し数/見逃し率:Apache

図 5 より, 次のことが言える. UNKNOWN レベルの脆弱性については, 全バージョンにおいて見逃し数は 0 件であった. Medium レベルの脆弱性については, 全体で 172 件中 18 件が見逃されており, 特にバージョン 2.4.57 と 2.4.58 では, それぞれ 2 件中 2 件が見逃されていた. High レベルの脆弱性については, 全体で 339 件中 66 件が見逃されており, バージョン 2.4.52 では 13 件中 4 件が見逃されていた. Critical レベルの脆弱性については, 全体で 273 件中 16 件が見逃されており, バージョン 2.4.58 では 4 件中 1 件が見逃されていた.

一方で, Censys では図 6 より, 次のことが言える. UNKNOWN レベルの脆弱性については, 全体で 42 件中 2 件が見逃されていた. Medium レベルの脆弱性については, 全体で 172 件中 43 件が見逃されており, 特にバージョン 2.4.57 と 2.4.58 では, それぞ

れ 2 件中 2 件が見逃されていた. High レベルの脆弱性については, 全体で 339 件中 67 件が見逃されており, バージョン 2.4.52 では 13 件中 4 件が見逃されていた. Critical レベルの脆弱性については, 全体で 273 件中 34 件が見逃されており, バージョン 2.4.60 では 1 件中 1 件が見逃されていた.

Shodan と Censys の結果を比較すると, Censys の方が全体的に見逃した脆弱性数が多い傾向が確認された. 特に, Medium レベルの脆弱性において, Censys では Shodan よりも 25 件の脆弱性を見逃した. Critical レベルの脆弱性においても, Censys では 18 件多く見逃した. これらの結果から, Apaceh に関しては, Censys は Shodan に比べて脆弱性を見逃す数が多いことが判明した. Nginx における全脆弱性の検知状況を図 7 に示す（図の形式は図 4 と同様).

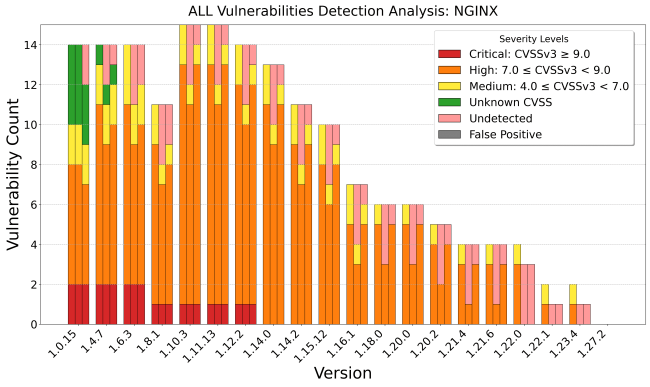

図 7: 各バージョンに存在する全脆弱性の検知結果:Nginx

Nginx は, Apache HTTP Server の結果とは異なり, Shodan および Censys において誤検知は見られなかった. 一方で, Apache と同様に, Shodan および Censys ではほとんどのバージョンにおいて脆弱性の見逃しが存在した. しかし, Apache とは異なり, Shodan では Censys よりも多くの脆弱性が見逃されていることが明らかとなった. Nginx の各バージョンにおける Shodan の脆弱性の見逃し数/見逃し率, 図 8 に, Censys の脆弱性の見逃し数/見逃し率を図 9 に示す.

Version	UNKNOWN	MEDIUM	HIGH	CRITICAL	Total
1.0.15	0/4 (0.0%)	0/2 (0.0%)	0/6 (0.0%)	0/2 (0.0%)	0/14 (0.0%)
1.4.7	0/1 (0.0%)	0/2 (0.0%)	2/9 (22.2%)	0/2 (0.0%)	2/14 (14.3%)
1.6.3	-	1/3 (33.3%)	2/9 (22.2%)	0/2 (0.0%)	3/14 (21.4%)
1.8.1	-	1/2 (50.0%)	2/8 (25.0%)	0/1 (0.0%)	3/11 (27.3%)
1.10.3	-	1/2 (50.0%)	2/12 (16.7%)	0/1 (0.0%)	3/15 (20.0%)
1.11.13	-	1/2 (50.0%)	2/12 (16.7%)	0/1 (0.0%)	3/15 (20.0%)
1.12.2	-	1/2 (50.0%)	2/11 (18.2%)	0/1 (0.0%)	3/14 (21.4%)
1.14.0	-	1/2 (50.0%)	2/11 (18.2%)	-	3/13 (23.1%)
1.14.2	-	1/2 (50.0%)	2/9 (22.2%)	-	3/11 (27.3%)
1.15.12	-	1/2 (50.0%)	2/8 (25.0%)	-	3/10 (30.0%)
1.16.1	-	1/2 (50.0%)	2/5 (40.0%)	-	3/7 (42.9%)
1.18.0	-	1/1 (100.0%)	2/5 (40.0%)	-	3/6 (50.0%)
1.20.0	-	1/1 (100.0%)	2/5 (40.0%)	-	3/6 (50.0%)
1.20.2	-	1/1 (100.0%)	2/4 (50.0%)	-	3/5 (60.0%)
1.21.4	-	1/1 (100.0%)	2/3 (66.7%)	-	3/4 (75.0%)
1.21.6	-	1/1 (100.0%)	2/3 (66.7%)	-	3/4 (75.0%)
1.22.0	-	1/1 (100.0%)	2/2 (100.0%)	-	3/3 (100.0%)
1.22.1	-	1/1 (100.0%)	-	-	1/1 (100.0%)
1.23.4	-	1/1 (100.0%)	-	-	1/1 (100.0%)
Total	**0/5 (0.0%)**	**16/30 (53.3%)**	**32/122 (26.2%)**	**0/10 (0.0%)**	**48/167 (28.7%)**

図 8: Shodan の脆弱性の見逃し数/見逃し率:Nginx

Shodan は, 図 8 より, UNKNOWN レベルの脆弱性については, バージョン 1.0.15 で 4 件中 1 件が見逃されており, 全体で 5 件中 1 件が見逃されていた. Medium レベルの脆弱性について

Version	UNKNOWN	MEDIUM	HIGH	CRITICAL	Total
1.0.15	1/4 (25.0%)	0/2 (0.0%)	1/6 (16.7%)	0/2 (0.0%)	2/14 (14.3%)
1.4.7	0/1 (0.0%)	0/2 (0.0%)	1/9 (11.1%)	0/2 (0.0%)	1/14 (7.1%)
1.6.3	-	1/3 (33.3%)	1/9 (11.1%)	0/2 (0.0%)	2/14 (14.3%)
1.8.1	-	1/2 (50.0%)	1/8 (12.5%)	0/1 (0.0%)	2/11 (18.2%)
1.10.3	-	1/2 (50.0%)	0/12 (0.0%)	0/1 (0.0%)	1/15 (6.7%)
1.11.13	-	1/2 (50.0%)	0/12 (0.0%)	0/1 (0.0%)	1/15 (6.7%)
1.12.2	-	1/2 (50.0%)	0/11 (0.0%)	0/1 (0.0%)	1/14 (7.1%)
1.14.0	-	1/2 (50.0%)	0/11 (0.0%)	-	1/13 (7.7%)
1.14.2	-	1/2 (50.0%)	0/9 (0.0%)	-	1/11 (9.1%)
1.15.12	-	1/2 (50.0%)	0/8 (0.0%)	-	1/10 (10.0%)
1.16.1	-	1/2 (50.0%)	0/5 (0.0%)	-	1/7 (14.3%)
1.18.0	-	1/1 (100.0%)	0/5 (0.0%)	-	1/6 (16.7%)
1.20.0	-	1/1 (100.0%)	0/5 (0.0%)	-	1/6 (16.7%)
1.20.2	-	1/1 (100.0%)	0/4 (0.0%)	-	1/5 (20.0%)
1.21.4	-	1/1 (100.0%)	0/3 (0.0%)	-	1/4 (25.0%)
1.21.6	-	1/1 (100.0%)	0/3 (0.0%)	-	1/4 (25.0%)
1.22.0	-	1/1 (100.0%)	2/2 (100.0%)	-	3/3 (100.0%)
1.22.1	-	1/1 (100.0%)	-	-	1/1 (100.0%)
1.23.4	-	1/1 (100.0%)	-	-	1/1 (100.0%)
Total	**1/5 (20.0%)**	**16/30 (53.3%)**	**6/122 (4.9%)**	**0/10 (0.0%)**	**23/167 (13.8%)**

図 9: Censys の脆弱性の見逃し数/見逃し率:Nginx

は, 全体で 30 件中 16 件が見逃されており, 見逃し率は 53.3% となっている. 特に, バージョン 1.18.0 から 1.23.4 では, それぞれ 1 件中 1 件が検知されていた. High レベルの脆弱性については, 全体で 122 件中 6 件のみが見逃されており, 見逃し率は 4.9% と低かった. Critical レベルの脆弱性については, 存在した 10 件全てが正しく検知され, 見逃しは発生しなかった.

一方で, 図 9 より, Censys では UNKNOWN レベルの脆弱性については, 全ての脆弱性が正しく検知され, 見逃しは発生しなかった. Medium レベルの脆弱性については, Shodan と同様に全体で 30 件中 16 件が見逃されており, 見逃し率は 53.3% であった. High レベルの脆弱性については, 全体で 122 件中 32 件が見逃されており, 見逃し率は 26.2% となっている. 特に, バージョン 1.21.4 と 1.21.6 では, それぞれ 3 件中 2 件が見逃されていた. Critical レベルの脆弱性については, Shodan と同様に 10 件全てが正しく検知され, 見逃しは発生しなかった. Shodan と Censys の結果を比較すると, High レベルの脆弱性の検知において Shodan の方が優れていることが確認された. Shodan は 122 件中 6 件（4.9%）の見逃しであったのに対し, Censys では 122 件中 32 件（26.2%）を見逃していた. Medium レベルの脆弱性については, 両者とも同じ見逃し数（30 件中 16 件）であった. Critical レベルの脆弱性については, 両者とも見逃しがなく, 完全な検知を達成していた. これらの結果から, Nginx に関しては, 特に High レベルの脆弱性の検知において Shodan の方が優れていることが判明した.

6. 考　　察

6.1 スキャナー間の比較

Shodan と Censys を比較すると, Apache では Censys が Shodan よりも多くの脆弱性を見逃している一方, Nginx では Shodan が Censys よりも多くの脆弱性を見逃していた. これは, 各スキャナーが異なるスキャン手法やデータベースを使用しているため, Web サーバごとに異なる検知性能を示す結果となったと考えられる. 具体的には, Shodan は誤検知の頻度が高いものの, 深刻な脆弱性の検知性能が高い. これは, Shodan が積極的なスキャン手法を採用している可能性を示している. その結果として誤検知が増加する一方で, 高深刻度の脆弱性を確実に検知できる能力が高いことが確認された. 一方, Censys は誤検知が少ないものの, 脆弱性の見逃しが多い傾向が見られた. これは, より保守

的なスキャン手法や判定基準を採用している可能性を示唆している.

さらに, Shodan に関しては, 検知した脆弱性に「verified（検証済み）」と「unverified（未検証）」の 2 種類が存在する [12]. Unverified な脆弱性は, 収集したメタデータに基づいて推測された脆弱性であり, 例えば古いバージョンの Apache が動作している場合, そのバージョンに関連する既知の脆弱性を関連付けている. 一方, verified な脆弱性は, Shodan が実際に検証を行って確認した脆弱性である. 今回の研究では, Shodan をブラックボックスとして扱い, verified/unverified の区別を考慮せずに通常の状態で検知結果を評価した. これにより, Shodan の検知結果における誤検知や見逃しの実態を純粋に評価することが可能となったが, 一方で verified に区分される脆弱性のみに限定した場合の検知精度は今回の結果とは異なることが予想される. さらに, 実運用においてはサーバのバージョン情報を秘匿した運用が行われる場合も多いが, このような状況での検知精度評価は今後の課題とする.

6.2 実務的提言

本研究の結果を踏まえると, 広域スキャンシステムの実運用においては, Shodan と Censys の特性を理解した上で目的に応じた使い分けが求められる. まず, 両スキャナーとも深刻な脆弱性（Critical レベル）についてはおおむね高い検知率を示したが, Apache HTTP Server の一部バージョンで Censys が見逃しを起こすなど, わずかな差異が確認された. Shodan は積極的なスキャン手法によって緊急度の高い脆弱性をより確実に捉える一方で, 誤検知の可能性が否定できない. そのため, 運用時には Shodan が報告する「verified / unverified」の脆弱性を丁寧に区別し, 特に unverified な項目については追加検証を行うことが望ましい. また, 誤警報を含むリスクを考慮し, 常に二次確認のフローを用意することで, 過剰な対応コストを抑えつつ重大な脆弱性を見落とさない運用が期待できる.

一方で, Censys は全体として誤検知が少なく, 初期スクリーニング時の誤報リスクを最小化できる利点がある. しかし, 見逃しが散見されることから, 定期的なスキャン結果のレビューや他ツールとの併用が不可欠となる. 深刻度の高い脆弱性は問題なく検出できる場合が多いものの, 一部のバージョンや新規に報告された脆弱性に関してデータベース対応が遅れることもあり得るため, 結果に対する継続的な追跡と検証が望ましい.

総合的には, Shodan と Censys を相互補完的に活用することが最適解となる可能性が高い. 両者の結果を照合することで, 見逃しや誤検知を相互に補完し合い, 全体的な検出精度を高めることができる. さらに, NVD 等の脆弱性データベースの更新状況を定期的にチェックし, CPE 未登録の脆弱性や新たに公表された脆弱性への対応を迅速に把握しておくことも重要である. こうした運用方針を徹底すれば, 高深刻度だけでなくその他の脆弱性に対してもより正確な検知と対処が可能となり, 組織のセキュリティリスク低減に寄与すると考えられる.

7. おわりに

7.1 まとめ

本研究では, Apache HTTP Server と Nginx を対象に Shodan および Censys の脆弱性検知能力を評価した. その結果, Shodan は全バージョンで誤検知が観察された一方, 深刻度の高い脆弱性を的確に検知する能力に優れていることが確認された. 特に深刻な脆弱性については見逃しを最小化できる反面, 運用の場面では誤警報を適切にふるい分ける工夫が不可欠である. 一方の Censys は誤検知がほとんど見られないにもかかわらず, 中程度から高深刻度の脆弱性を取りこぼす傾向が見られた. これらの特徴は, 特に Apache HTTP Server で顕著に表れ, 最新の脆弱性情報がスキャナー側で未登録の場合などに見逃しや誤検知が生じることが分かった. また, Nginx に関しては両スキャナーとも誤検知が起こらなかったが, 脆弱性の見逃しが依然として発生し, Shodan は Censys よりも多くの脆弱性を捉えきれなかったケースが散見された. これらの結果を踏まえると, サービスごとにスキャナーの検知性能に違いがあり, バージョンや脆弱性情報の更新状況によっても結果が変動することが確認できた.

Shodan が積極的なスキャンを行うことで深刻な脆弱性を検出できる反面, 誤警報の多さという課題を抱える. 一方, Censys は保守的な手法によって誤検知を抑えているが, 見逃しを起こしやすいことが明らかになった. したがって, 脆弱性管理においては両者の長所を活かし, 短所を補完し合う運用を組み合わせるのが有効だと考えられる. たとえば, 重大度の高い脆弱性をできるだけ見落としたくない場面では Shodan の積極的検知を活用し, 基本スクリーニングで誤報をできるだけ減らしたい状況では Censys の結果を優先するなど, 目的や運用ポリシーに合わせた使い分けが重要である.

7.2 今後の課題

今後の研究においては, 評価対象とするスキャナーの種類を増やし, より多様なツールを比較分析することが重要である. これにより, 各スキャナーの検知性能の違いや特徴をより包括的に理解することが可能となる. また, 評価対象とするサービスやそのバージョン数を拡大することで, 異なる環境下でのスキャナーのパフォーマンスを詳細に検証することが求められる. 特に, 異なる種類のウェブサーバーやアプリケーションに対する脆弱性検知能力を評価することで, スキャナーの汎用性や特定のサービスに対する適応性を明らかにすることが期待される. さらに, 評価基準の拡充も今後の課題として挙げられる. 脆弱性の検知精度だけでなく, スキャナーのスキャン速度, リソース消費量, ユーザビリティなど, 多角的な評価基準を導入することで, 実務におけるスキャナー選定の指針を提供することが可能となる.

謝辞 この成果の一部は, 国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP24003）の結果得られたものです.

文　献

[1] 経済産業省 商務情報政策局 サイバーセキュリティ課, ASM (Attack Surface Management）導入ガイダンス, https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

(参照 2025.2.3)
[2] Shodan. https://www.shodan.io/ (参照 2025.2.3)
[3] Censys. https://censys.io/ (参照 2025.2.3)
[4] Li et al.,“A Survey on Cyberspace Search Engines,”In CNCERT 2020, CCIS 1299 (pp. 206–214). (参照 2025.2.3)
[5] Bennett, C., Abdou, A., & van Oorschot, P. C.,“Empirical Scanning Analysis of Censys and Shodan,”Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb), 2021. (参照 2025.2.3)
[6] Cybersecurity and Infrastructure Security Agency (CISA). Known Exploited Vulnerabilities Catalog. https://www.cisa.gov/known-exploited-vulnerabilities-catalog (参照 2025.2.3)
[7] FIRST.“Common Vulnerability Scoring System SIG.”https://www.first.org/cvss/ (参照 2025.2.3)
[8] National Institute of Standards and Technology (NIST), National Vulnerability Database. https://nvd.nist.gov/ (参照 2025.2.3)
[9] W3Techs,“Web Server Usage Statistics,”https://w3techs.com/technologies/overview/web_server (参照 2025.2.3)
[10] Netfilter,“Netfilter User's Guide,”https://www.netfilter.org/projects/iptables/index.html (参照 2025.2.3)
[11] CVE Details. https://www.cvedetails.com/ (参照 2025.2.3)
[12] Shodan,”Understanding Shodan Vulnerability Assessment.”https://help.shodan.io/mastery/vulnerability-assessment (参照 2025.2.3)