

SGS 報告書番号: SHCS250400018907

試験報告書 (テストレポート) ペネトレーションテスト (侵入テスト) OWASP REST
アセスメント

SHCS250400018907 報告書参照番号

実施者 (氏名 + 署名): Scott Cao / Sualt lao ,

承認者 (氏名 + 署名): Bruce Shen / Bruce Shen

発行日: 2025-06-16

有効期限: /

総ページ数: 10

試験実施機関: SGS-CSTC Standards Technical Services (Shanghai) Co., Ltd.

住所: 588 West Jindu Road, Xinqiao, Songjiang, 201612 Shanghai, China

申請者名: Shanghai Gaoxian Automation Technology Development Co., Ltd

住所: Floor 10, Building D, NO 666, ShengXia Road China(Shanghai)

試験規格: ペネトレーションテスト (OWASP REST アセスメント チートシートへの参
照)

試験報告書フォーム番号: EEC_OWASP REST B

試験報告書フォーム作成元: SGS-CSTC

マスターTRF: 2022-12-30

品目受領日: 2025-04-23

品目実施期間: 2025-04-23 から 2025-06-16 まで

試験結果: 脆弱性は見つかりませんでした

本報告書における試験結果は、試験対象にのみ関連するものであり、提出されたサーバー
機器の技術文書に基づいています。技術の発展に伴いリスクは変化するため、時間の経
過とともに機器の安全性が損なわれる可能性があります。製品セキュリティライフサイ
クルの一環として、販売、製造、製造委託した製品および提供するサービス内のセキュリ
ティ脆弱性を継続的に監視、特定、および修正することは、サプライヤー/製造元の責任で
す。

本試験報告書は、SGS の一般的な配送条件 (要請に応じて入手可能、および
www.sgs.com でアクセス可能) に基づいて発行されています。そこに定義されている責
任の制限、補償、および管轄権の問題に注意が向けられます。別段の定めがない限り、
(a) 本文書に示されている結果は試験されたサンプルのみを指し、(b) 当該サンプルは 3
ヶ月間保管されます。本文書は、SGS の事前の承認なしに、全文以外の複製を行うこと
はできません。

SGS は製品に関連する技術文書を確認し、それに応じて試験計画、評価内容、および評価
要件を設計しました。評価の前に、試験計画は申請者によって確認、受け入れ、および承

認められました。

本文書は、Company（当社）が、裏面に印刷されている、または要請に応じて入手可能な、あるいは <http://www.sgs.com/en/Terms-and-Conditions.aspx> でアクセス可能な「サービスの一般条件」に従って発行するものであり、電子形式の文書については、<http://www.sgs.com/en/Terms-and-Conditions/Terms-e-Document.aspx> にある「電子文書の利用規約」に従うものとします。そこに定義されている責任の制限、補償、および管轄権の問題に注意が向けられます。本文書の保持者は、ここに記載されている情報が、当社の介入時点のみにおける、かつクライアントの指示（ある場合）の範囲内での当社の見解を反映していることを通知されます。当社の唯一の責任はクライアントに対するものであり、本文書は取引の当事者が取引文書に基づくすべての権利および義務を行使することを免除するものではありません。本文書は、当社の事前の書面による承認なしに、全文以外の複製を行うことはできません。本文書の内容または外観の不正な変更、偽造、または改ざんは違法であり、違反者は法律の最大限の範囲で起訴される可能性があります。別段の定めがない限り、本試験報告書に示されている結果は試験されたサンプルのみを指し、当該サンプルは 30 日間のみ保管されます。

評価方法は、申請者がビデオ会議を通じて関連技術者にサーバー機器を操作させ、SGS の評価者が申請者から提供されたデータを確認してサーバー機器を評価するというものです。本報告書の内容または外観の不正な変更、偽造、または改ざんは違法であり、違反者は法律の最大限の範囲で起訴される可能性があります。

製品の説明

製品名：Autonomous Scrubber（自律型スクラバー / 自動床洗浄機）

商標：/

製造元：Shanghai Gaoxian Automation Technology Development Co., Ltd

モデル/タイプ参照：Scrubber 50 MD / Scrubber 50 MR / S1 PRO M / SW1

試験の要約：

CRITICAL（致命的）	HIGH（高）	MEDIUM（中）	LOW（低）
0	0	0	0

一般備考：N/A（該当なし）

分類の定義：リスク分類

レベル	スコア	説明
Critical	10	脆弱性は組織に即座の脅威をもたらします。悪用に成功すると、組織に永続的な影響を与える可能性があります。修復は直ちに実施されるべきです。

レベル	スコア	説明
High	7-9	脆弱性は組織に緊急の脅威をもたらし、修復を最優先すべきです。
Medium	4-6	悪用に成功する可能性があり、ビジネス機能の顕著な混乱を招く可能性があります。この脆弱性は、可能な限り速やかに修復されるべきです。
Low	1-3	脆弱性が組織にもたらす脅威は、無視できるほど微小または最小限です。この脆弱性の存在を記録し、可能であれば修復すべきです。
Informational	0	これらの発見は組織に対する明確な脅威はありませんが、ビジネスプロセスが望ましくない形で動作したり、会社に関する機密情報が明らかになったりする可能性があります。

悪用可能性の分類

可能性	説明
Likely（可能性が高い）	悪用方法が広く知られており、一般に入手可能なツールを使用して実行できます。スキルの低い攻撃者や自動化ツールでも、最小限の困難さで脆弱性を悪用することに成功する可能性があります。

可能性	説明
Possible（可能性がある）	悪用方法が広く知られており、公開ツールを使用して実行できる可能性があります。設定が必要です。悪用に成功するには、基礎となるシステムへの理解が必要です。
Unlikely（可能性が低い）	悪用には、基礎となるシステムへの深い理解や、高度な技術スキルが必要です。悪用に成功するには、正確な条件が必要となる場合があります。

ビジネス影響の分類

影響度	説明
Major（重大）	悪用に成功すると、組織全体で重要なビジネス機能に大規模な混乱が発生し、重大な財務的損害が生じる可能性があります。
Moderate（中程度）	悪用に成功すると、重要ではないビジネス機能に重大な混乱を引き起こす可能性があります。
Minor（軽微）	悪用に成功しても、影響を受けるユーザーはごくわずかであり、日常の

影響度	説明
	ビジネス機能に大きな混乱は生じません。

修復難易度の分類

難易度	説明
Hard (困難)	修復には、時間を要する基礎システムの広範な再設定が必要な場合があります。修復により、通常のビジネス機能が中断される場合があります。
Moderate (普通)	修復には、時間がかかるか、またはコストがかかる、軽微な再設定や追加が必要な場合があります。
Easy (容易)	修復は、ほとんど困難を伴わずに、短時間で達成できます。

SGS 評価結果 (ASSESSMENT FINDINGS) :

番号	発見事項	リスクスコア	リスク	修正
1	(空白)	/	/	/

1- セキュリティログなし (Without Security log)

RISK	/
悪用可能性 (Exploitation Likelihood)	/
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	/

- セキュリティへの影響 (Security Implications) N/A (該当なし)
- 分析 (Analysis) テスト中、評価者は機器の内部にセキュリティログが存在し、さまざまな機密性の高い操作情報が記録されていることを確認しました。このログ情報により、セキュリティインシデントが発生した場合にリスクの発生源を迅速に特定し、ネットワークセキュリティリスクを低減することができます。
- 推奨事項 (Recommendations) ログイン・ログアウトやパスワード変更などの機密性の高い操作を含む、ネットワークセキュリティログ機能を追加してください。

2- ロジックポート検出 (Logic Port Detection)

RISK	/
悪用可能性 (Exploitation Likelihood)	/
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	/

- セキュリティへの影響 (Security Implications) N/A (該当なし)
- 分析 (Analysis) 評価者は、ポートを調査することにより、デバイスに外部へ露

出した脆弱なインターフェースが存在するかどうかを確認しようと試みました。担当者がNmap ツールを使用して確認したところ、デバイスに外部へ露出したサービスやポートは存在しないことが判明しました。これは、デバイスがオープンなサービスを提供するサーバー側としてではなく、クライアントとしてのみ機能していることを示しています。インターフェースの確認結果は以下の図の通りです。

【画像内テキスト】

Login with Password (パスワードでログイン)

1, 2, 3, 4, 5, 6, 7, 8, 9, AC, 0, [戻る]

After five incorrect password entries, the machine will be locked (パスワード入力を5回間違えると、マシンがロックされます)

Login

I have read and agree to the [Privacy Agreement] ([プライバシー規約]を読み、同意しました)

Plaintext

C:\Users\caowang>nmap -sS 192.168.50.90 [cite: 385]

Starting Nmap 7.97 (<https://nmap.org>) at 2025-06-16 13:31 +0800 [cite: 386]

Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan [cite: 387]

SYN Stealth Scan Timing: About 21.00% done; [cite: 387]

ETC: 13:35 (0:03:12 remaining) [cite: 388]

Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan [cite: 388]

SYN Stealth Scan Timing: About 22.00% done; [cite: 388]

ETC: 13:35 (0:03:11 remaining) [cite: 389]

Stats: 0:00:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan [cite: 389]

SYN Stealth Scan Timing: About 23.50% done; [cite: 389]

ETC: 13:35 (0:03:06 remaining) [cite: 390]

Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 up), 1 undergoing SYN Stealth Scan [cite: 390]

SYN Stealth Scan Timing: About 24.40% done; [cite: 390]

ETC: 13:35 (0:03:03 remaining) [cite: 391]

Nmap scan report for 192.168.50.90 [cite: 391]

Host is up (0.24s latency). [cite: 392]

All 1000 scanned ports on 192.168.50.90 are in ignored states. [cite: 393]

Not shown: 1000 filtered tcp ports (no-response) [cite: 394]

MAC Address: AC:D9:29:E6:18:DE (Quectel Wireless Solutions) [cite: 395]

Nmap done: 1 IP address (1 host up) scanned in 242.59 seconds [cite: 396]

Nmap スキャン結果

- 推奨事項 (Recommendations) 開発中または使用中に、不要なポートや機能を閉じてください。

3- アクセス制御 (Access Control)

RISK	
悪用可能性 (Exploitation Likelihood)	/
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	/

- セキュリティへの影響 (Security Implications) N/A (該当なし)
- 分析 (Analysis) 評価中、アセッサーはログインパスワードが設定されているデバイスに対し、ブルートフォース (総当たり) 攻撃を用いて侵入を試みました。評価者が誤ったパスワードを使用してログインを試みたところ、5 回試行した後にデバイスのログイン機能が無効化され、30 分後に再度試行する必要がある状態になりました。不正アクセスからデバイスを保護するために、アンチ・ブルートフォース (総当たり防止) メカニズムがデバイス上に存在しています。

(以下、画像内文字の文字起こし部分：1, 2, 3, 4, 5, 6, パスワード入力を 5 回間違えるとマシンがロックされます, 9, ログイン, プライバシー規約へ, アカウントロックのヒント, AC, 0)

【画像内テキスト】

00:29:57

Robot is locked, try again after 30 minute (ロボットがロックされました。30 分後にやり直してください)

00:29:57 ロボットがロックされました。30 分後にやり直してください

- 推奨事項 (Recommendations) ロックのヒント (Locking Tips)：累積的なペナルティメカニズムを通じて、総当たり防止メカニズムを使用し、不正アクセスを防止してください。

4- 画面自動ロック (Screen Auto Lock)

RISK	/
悪用可能性 (Exploitation Likelihood)	
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	/

- セキュリティへの影響 (Security Implications) N/A (該当なし)
- 分析 (Analysis) テスト中、評価者はデバイスに自動画面ロックメカニズムが存在

し、自動ロック時間がユーザーによって管理されていることを確認しました。デフォルトでは、デバイスは15秒で自動的にロックされます。自動ロックメカニズムの使用は、ユーザーがログインしている間に他のユーザーによって不正アクセスされるリスクを防ぐための効果的な方法です。

- **推奨事項 (Recommendations)** 自動ログアウトメカニズムを設計することは、ユーザーがログアウトせずにマシンを離れた場合の不正な攻撃の可能性を効果的に防ぎます。

5- アプリケーション自動起動 (Application Auto Start)

RISK	/
悪用可能性 (Exploitation Likelihood)	/
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	/

- **セキュリティへの影響 (Security Implications)** N/A(該当なし)
- **分析 (Analysis)** 評価者はテストプロセス中に、デバイスの起動後、直接アプリケーションページに遷移することを確認しました。評価者はオペレーティングシステム (OS) に入ることができず、デバイスの一般ユーザー権限を取得することもできません。また、デベロッパーモードの有効化や adb デバッグの有効化といった、デバイス上での機密性の高い設定や操作を行うこともできませんでした。
- **推奨事項 (Recommendations)** アプリケーションが自動的に起動するように設計することで、デバイスの権限が乱用されるのを防ぐことができます。

6- ショートカットキーの使用 (Shortcut Key Usage)

RISK	/
悪用可能性 (Exploitation Likelihood)	/
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	/

- **セキュリティへの影響 (Security Implications)** N/A (該当なし)
- **分析 (Analysis)** 評価者はテスト中に、Android のショートカットキーやショートカットジェスチャーを使用して、OS に侵入したり設定ページを呼び出したりすることを試みました。一般的なショートカットジェスチャーが試みられましたが、デバイスは効果的な応答を示しませんでした。これにより、デバイスへの不正なアクセスが不可能な状態が確保されていることが確認されました。また、評価者は USB ポートを介してキーボードやマウスなどの接続を試みましたが、システムはデバイスへのアクセスを拒否しました。

- 推奨事項 (Recommendations) アプリケーションが自動的に起動するように設計することで、デバイスの権限が乱用されるのを防ぐことができます。

7- インジェクションテスト (Injection Test)

RISK	/
悪用可能性 (Exploitation Likelihood)	/
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	/

- セキュリティへの影響 (Security Implications) N/A (該当なし)
- 分析 (Analysis) 評価者は、デバイス上に多くの入力ボックスがあることを確認し、インジェクション攻撃を試みました。試行中、すべての入力ボックスが、指定された文字のみのユーザー入力を許可するように制限されていることが判明しました。キーボードも無効化されていたため、評価者は外部キーボードを使用した入力を行うことができませんでした。したがって、評価者はデバイスがインジェクション攻撃に対して耐性があると結論付けました。
- 推奨事項 (Recommendations) ユーザー入力を厳格にフィルタリングしてください。

SGS 8- パスワード更新のダブルチェック (Password Update Double Check)

RISK	/
悪用可能性 (Exploitation Likelihood)	/
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	

- セキュリティへの影響 (Security Implications) N/A (該当なし)
- 分析 (Analysis) 評価者は、ユーザーがログインしているものの監視されていない状態をシミュレートし、不正なパスワード更新操作を行おうと試みました。評価者は、パスワードの更新などの機密性の高い操作に対して、二段階検証機能が設定されていることを確認しました。これは、ログイン状態であっても現在のデバイスのログインアカウントのパスワードによる二段階検証を要求し、その検証が合格した後にのみユーザーがパスワードを更新することを許可するものです。これにより、パスワード更新メカニズムの安全性が効果的に保護されます。
- 推奨事項 (Recommendations) 不正な更新を避けるために、パスワードの更新には二重の検証 (ダブルバリデーション) を要求してください。

9- パスワード更新のダブルチェック (Password Update Double Check) (※注: 原文ママ。項目のタイトルが8番と同じになっていますが、内容は通知メカニズムに関するものです)

RISK	/
悪用可能性 (Exploitation Likelihood)	/
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	/

- セキュリティへの影響 (Security Implications) N/A (該当なし)
- 分析 (Analysis) 評価中、評価者はデバイスがユーザー通知メカニズムを無効化しており、機密情報の漏洩や機密性の高い操作の実行を減少させていることを確認しました。
- 推奨事項 (Recommendations) N/A (該当なし)

10- パスワード更新のダブルチェック (Password Update Double Check) (※注: こちらも原文ママ。項目名が重複していますが、内容は9番と同様です)

RISK	/
悪用可能性 (Exploitation Likelihood)	/
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	/

- セキュリティへの影響 (Security Implications) N/A (該当なし)
- 分析 (Analysis) 評価中、評価者はデバイスがユーザー通知メカニズムを無効化しており、機密情報の漏洩や機密性の高い操作の実行を減少させていることを確認しました。
- セキュリティへの影響 (Security Implications) N/A (該当なし)

11- USB テスト (USB Testing)

RISK	/
悪用可能性 (Exploitation Likelihood)	/
ビジネス影響 (Business Impact)	/
修復難易度 (Remediation Difficulty)	/

- セキュリティへの影響 (Security Implications) N/A (該当なし)
- 分析 (Analysis) 評価者は、FaceDancer ツールを使用して USB インターフェースのファジングテスト (※予期しないデータを入力するテスト) を実施しましたが、クラッシュは発生しませんでした。手動テストを組み合わせた結果、USB ではキーボードやマウスなどの周辺機器といった不要なドライバーが無効化されていることも判明しました。これにより、デバイスのハードウェアインターフェースにおけるサイバーセキュリティのリスク面 (アタックサーフェス) が縮小されました。

- 推奨事項 (Recommendations) 不要なハードウェアポートを無効化してください。

付録 I- 製品写真 (Appendix I - Product Photos) 7

(※各写真のキャプション)

- 製品概要 (Product overview)
- 製品概要 (Product overview)
- 製品概要 (Product overview)
- 製品概要 (Product overview)
- 製品概要 (Product overview)
- 製品概要 (Product overview)
- 製品概要 (Product overview)
- 製品概要 (Product overview)

SGS グループ (SGS SA) メンバー

TRF 番号 EEC_OWASP REST B

報告書終了 (End of Report)