GINRŌ GUARD

CapsuleCorp

脆弱性診断・ペネトレーションテスト報告書

日付: 2025年8月26日
プロジェクト: CCorp-2025-08-A
セキュリティアナリスト: ベルクール　バティスト
版数: 1.0

機密保持通知

本報告書には機微で特権的かつ機密性の高い情報が含まれています。本書の機密性を保護するため、取り扱いに細心の注意を払ってください。本報告書の公開は、CapsuleCorp の評判を損ない、または CapsuleCorp に対する攻撃を助長する可能性があります。GINRŌ GUARD は、本情報の使用に起因する特別、偶発、付随、または結果的損害について一切の責任を負いません。

免責事項

本評価は、契約範囲内の全ての脆弱性を必ずしも露見させるものではありません。本報告書は、特定時点（ポイントインタイム）での CapsuleCorp 環境に対する評価結果の要約です。評価期間中に環境へ変更が加えられた場合、結果に影響する可能性があります。

目次

経営層向け要約

GINRŌ GUARD は 2025/08/16 から 2025/08/28 にかけて、CapsuleCorp の社内ネットワークに対してセキュリティ評価を実施しました。本ペネトレーションテストは、外部の脅威主体が CapsuleCorp の社内ネットワークへのアクセスを試みるシナリオを模擬しました。本評価の目的は、CapsuleCorp のインフラに存在する脆弱性を発見・特定し、それらの是正方法を提案することです。評価範囲内で合計 **5** 件の脆弱性を確認し、その深刻度別内訳は以下の通りです。

重大	高	中	低	情報
1	**1**	**1**	**1**	**1**

最も深刻な脆弱性は、攻撃者に顧客アカウント乗っ取りの機会を与えます。機密性・完全性・可用性を確保するため、本書「指摘事項」セクションで示す是正・対応策の実装を推奨します。
なお、本評価は契約範囲内の全脆弱性を必ずしも明らかにするものではありません。評価期間中の環境変更は結果に影響する場合があります。

推奨事項

法令順守の不備など、技術的脆弱性以外であっても重大な事業上の失敗につながり得る事項が確認された場合は、経営陣へ速やかにエスカレーションすることを推奨します。

診断概要

確認されたセキュリティの強み

GINRŌ GUARD は、CapsuleCorp のネットワークにおいてセキュリティを大きく高めている以下の強みを確認しました。これらの統制が継続的に有効であることを確保するため、今後も監視を継続してください。

- リクエストレート制限は適切に構成され、期待どおりに機能しています。

改善が必要な領域

ネットワークのセキュリティをさらに向上させるため、GINRŌ GUARD は以下の対応を推奨します。これらを実装することで、攻撃者が CapsuleCorp の情報システムに対する攻撃を成功させる可能性を低減し、また攻撃が成功した場合の影響を軽減できます。

短期的な推奨事項

事業リスクを最小化するため、GINRŌ GUARD は可能な限り早期に以下の対応を実施することを推奨します。

- SQL インジェクションを防止するため、パラメータ化クエリを使用する。
- DOM に挿入する前に、信頼できない入力をすべてサニタイズおよびエンコードする。

長期的な推奨事項

GINRŌ GUARD は、緊急の事業リスクは伴わないが是正が難しい課題について、今後 6か月以内に以下の対応を実施することを推奨します。

- Webアプリケーションファイアウォール（WAF）の導入
- 決済ビジネスロジックのセキュリティを確保するためのバックエンド（サーバー側）検証の実装

スコープ

本評価は、提案依頼書および正式な書面合意で定義されたスコープに基づいて実施しました。

ネットワーク

サブネット	備考
10.0.1.0/24	CapsuleCorp 本社ネットワーク
10.0.2.0/24	日本（東京）拠点ネットワーク

Web アプリケーション

名称	種別	URL
CapsuleCorp website	Web アプリ	https://www.capsule.web

提供された認証情報

CapsuleCorp は、以下の認証情報とアクセスを評価円滑化のため提供しました。

項目	備考
テストアカウント	devbobtest@capsule.web・認証が必要な機能

テスト手法

GINRŌ GUARD のテスト手法は、情報収集、対象評価、脆弱性実行の三段階で構成されています。情報収集段階では、CapsuleCorp のネットワークシステムに関する情報を収集しました。対象情報の精緻化と価値評価のため、ポートスキャンなどの列挙手法を用いました。続いて対象評価を実施し、GINRŌ GUARD は CapsuleCorp のネットワークに存在する脆弱性を攻撃者が悪用する状況を模擬しました。このフェーズでは、通常業務に支障を与えない方法でシミュレーションを行いながら、脆弱性の証跡（エビデンス）を収集しました。次ページの図は、この手法を図示した概念図です。


1
PLANNING
Establish scope
Research assets
Confirm targets
TARGET ACQUISITION
Network scanning
OS Fingerprint
Banner grabbing
2
3
PRE-EXPLOITATION
Assess vulnerabilities
Customize attack tools
Confirm targets
EXPLOITATION
Leverage vulnerabilities
Execute payloads
Establish system access
4
5
POST-EXPLOITATION
Escalate privileges
Lateral movement
Network Pivoting
REPORTING
Evidence collection
Findings write-down
Risk assessment
6

区分定義

リスク区分

深刻度	CVSS スコア	DESCRIPTION
重大	9-10	当該脆弱性は組織に対し即時かつ重大な脅威をもたらし、緊急の是正対応が必要です。悪用された場合、事業・財務・評判に壊滅的な損害を引き起こす可能性があります。
高	7-10	当該脆弱性は組織に対し緊急性の高い脅威であり、是正対応を優先すべきです。
中	4-6	悪用が現実的に可能で、業務機能に顕著な支障を生じさせるおそれがあります。可能な限り早期に是正することが望まれます。
低	2-3	組織にもたらす脅威は軽微です。存在を記録し、可能であれば是正してください。
情報	1	直ちに明確な脅威を示すものではありませんが、業務プロセスが望ましくない挙動となる、または会社の機微情報が露出する可能性があります。

リスクマトリクス

	影響度		
悪用可能性	最小	中程度	大
起こりにくい	情報	低	中
あり得る	低	中	高
起こりやすい	中	高	重大

悪用可能性の区分

区分	説明
起こりやすい	悪用手法が広く知られており、公開ツールのみで実行可能。低スキルの攻撃者や自動化ツールでも比較的容易に悪用できる。
あり得る	悪用手法は知られており公開ツールでも実行可能だが、設定や調整が必要。基盤システムの理解が求められる。
起こりにくい	基盤システムに対する深い理解や高度な技術が必要。特定の条件が整わないと成立しない場合がある。

事業影響の区分

影響度	説明
大	重要業務が組織全体で大きく中断する可能性があり、重大な財務的損失を招くおそれがある。
中程度	一部の業務に目立つ支障を生じさせる可能性があるが、財務または運用への影響は限定的。
最小	影響は一部の利用者にとどまり、日常的な業務に大きな支障を生じにくい。

指摘事項

#	指摘事項名	スコア	リスク
1	認証回避	10	重大
2	DOM 型クロスサイトスクリプティング	8	高
3	アクセス制御の誤設定	6	中
4	robots.txt による機微情報の露出	3	低
5	サーバーバージョンの開示	1	情報

並び順・リスクスコアの降順

1 - 認証回避

リスク	重大
CVSS V3.1 スコア	10
対象 **URL**	http://capsule.web/#/login

セキュリティ上の影響

CapsuleWeb のログインフォームは、入力処理の不備とサーバー側検証の欠如により、認証回避に脆弱です。メールアドレス欄に SQL ロジックを注入することで、基盤のクエリを常に真を返すように改変でき、パスワード検証を完全に迂回できます。

この脆弱性により、未認証の攻撃者でも管理者権限でアプリケーションへアクセスし、登録ユーザー情報などの機微データが露出します。

悪用可能性: 起こりやすい

悪用は容易で高度な知識を要しません。単一の細工入力でログイン機構を回避できるため、悪用難度は低いと評価されます。

事業影響: 大

正当な資格情報なしに管理機能へ全面アクセスを許す結果となります。ユーザーアカウントの閲覧・変更、さらなる権限昇格の可能性も含まれます。この欠陥は認証レイヤーを根本から無効化し、機密性と完全性の全面的な喪失につながります。II

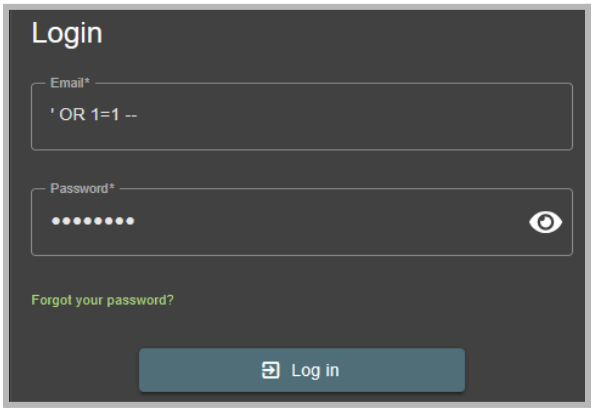
参考情報
- OWASP Top 10: Injection (A03:2021)
- CWE-89: SQL Injection

是正・対応策

- SQL インジェクション防止のため、パラメータ化クエリを必ず使用する。
- ログイン入力項目にサーバー側の厳格な入力検証を追加する。
- データベースアカウントの権限を最小権限に制限する。
- 詳細なエラーメッセージを利用者へ表示しない。

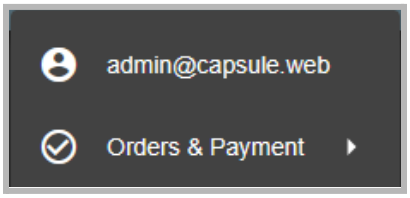
検証手順・PoC

1 - ログインページを開く: http://capsule.web/#/login

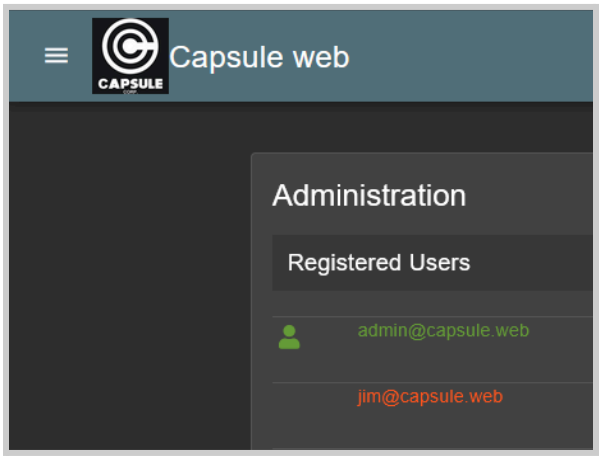


- Email 欄に次のペイロードを入力する: ' OR 1=1 –
- 任意のパスワードを入力する(無視される)。
- フォームを送信する。

2 - ログインが成功し、アプリケーションは攻撃者を管理者ユーザーとして認証する。



3 - /administration ページにアクセス可能となり、機微情報が露出し、攻撃者に管理者権限が付与される。



2 - DOM 型クロスサイトスクリプティング

リスク	高
CVSS V3.1 スコア	8.1
対象 **URL**	http://capsule.web/#/search?q=

セキュリティ上の影響

CapsuleWeb の検索機能は、クライアント側 JavaScript における入力処理の不備により、DOM ベースのクロスサイトスクリプティング（XSS）に脆弱です。`innerHTML` などの関数でサニタイズされていないクエリパラメータがそのまま DOM に反映され、攻撃者が任意の JavaScript を挿入できます。

この脆弱性により、被害者のブラウザで悪意あるスクリプトを実行され、セッションクッキーの窃取、アカウント乗っ取り、または認証済みユーザーになりすました操作が行われる可能性があります

悪用可能性: あり得る

ログイン済みユーザーを細工した URL に誘導する必要があります。高度な知識は不要で、ペイロードは被害者のブラウザで自動的に実行されるため、悪用は可能です。

事業影響: 大

成功した場合、セッションハイジャックが可能となり、アプリケーションの機密性と完全性が損なわれます。攻撃者はユーザー（管理者を含む）になりすまし、機微情報を流出させ、特権操作を実行できます。認証情報の使い回しやセッション共有がある環境では、システム全体の侵害に発展するおそれがあります。

参考情報:
- OWASP Top 10: Cross-Site Scripting (A03:2021)
- CWE-79: Improper Neutralization of Input During Web Page Generation

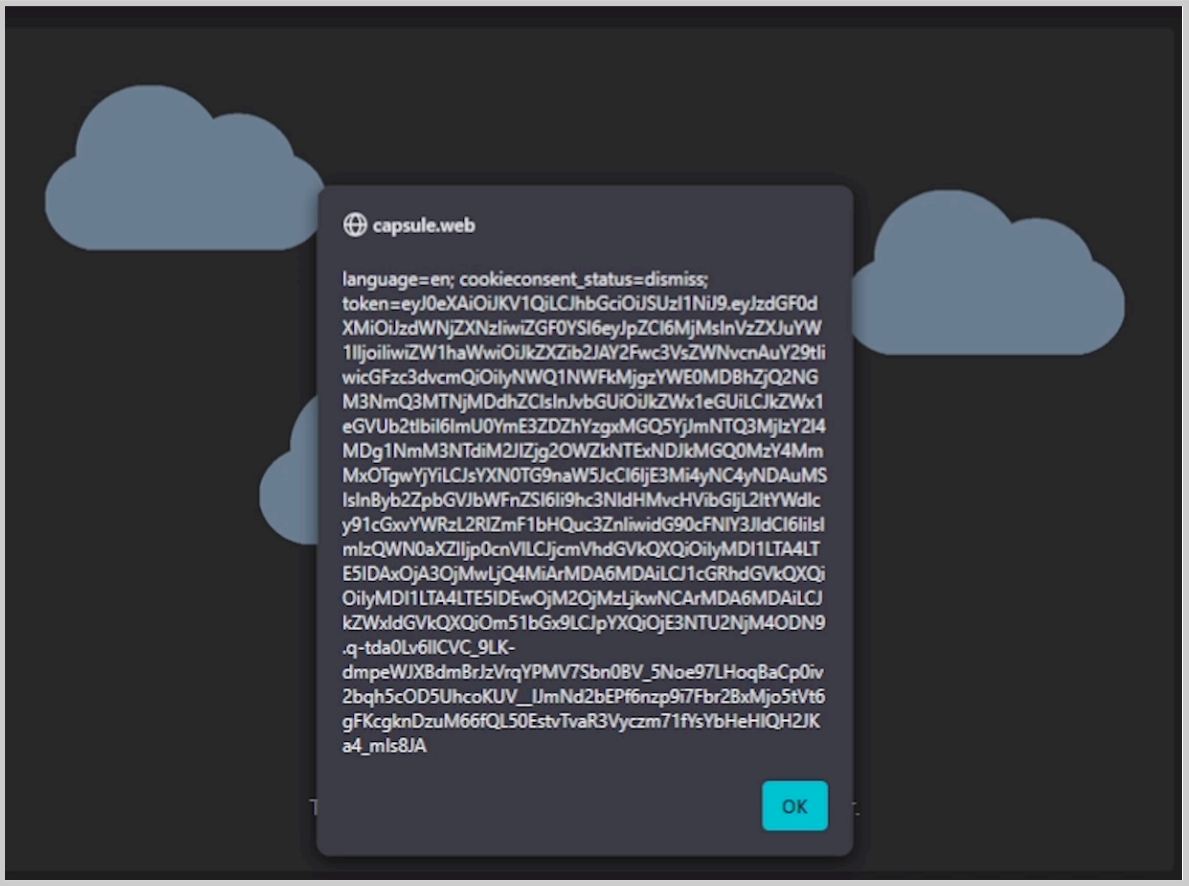
是正・対応策

- DOM に挿入する前に、信頼できない入力をすべてサニタイズおよびエンコードする。
- `innerHTML`、`document.write`、`eval` などの不適切な関数の使用を避ける。
- `textContent` や `setAttribute`など安全な DOM APIを使用する。

検証手順・PoC

1 - 検索ページへ移動する:
http://capsule.web/#/search?q=<img src=1 onerror=alert(document.cookie)>

2 - ペイロードがサニタイズされずに DOM に反映されます。実際の攻撃では、`alert()` を被害者のセッショントークンを外部送信する悪意あるコードに置き換えることで、アカウント乗っ取りが可能になります。



付録A - 使用ツール

ツール	説明
BurpSuite	Webアプリケーションのテストに使用。
Metasploit	脆弱なサービスの悪用および脆弱性スキャンに使用。
Nmap	ホストのポートスキャンに使用。
Nuclei templates	脆弱性・誤設定・露出データの検出に使用。
Sublist3r	指定ドメインのサブドメイン発見に使用。
Amass	ネットワークマッピング、資産発見、サブドメイン列挙に使用。

表A.1: 評価で使用したツール

付録B - エンゲージメント情報

クライアント情報

クライアント	CapsuleCorp
主担当者	DevBob, ***CTO***
メール	Devbob@capsulecorp.com
承認者	以下の人物は、エンゲージメントのスコープ変更および条件の修正を承認できます。 • CapsuleCorp - Dev Bob • GINRO GUARD - Baptiste Bellecour

連絡先情報

氏名	ベルクール　バティスト
住所	日本 東京都〈伏せ字〉
電話	070-3450〈伏せ字〉
メール	baptiste@ginro-guard.com