wizlynx group 侵入テスト

クラウドブリック Webアプリケーションファイアウォール

序文	ウィズリンクスグループ(英名：wizlynx group)は、自動ツール及び手動(マニュアル)によるIT セキュリティテストメソッドを用いて、Web アプリケーション侵入テストを実行することにより、クラウドブリック（Cloudbric）のWebアプリケーションファイアウォール（WAF）のセキュリティ耐性を評価しました。 ウィズリンクスグループは、2020年7月10日(金)から2020年7月13日(月)までインターネット経由でセキュリティ実証解析を実施しています。
対象	クラウドブリックWAFのWebを介した脅威を検出しブロックする性能を実証するため、ウィズリンクスグループの専門家より実施されたセキュリティ評価は、Webアプリケーション侵入テストとWAFベンチマークで構成されています。 侵入テストは、クラウドブリックのWebアプリケーションファイアウォールにより保護された「Giant National Bank」のWebアプリケーションにおいてGreyboxアプローチを使用しオンラインで行われました。 当該のアプリケーションは、テストに使用するウィズリンクスグループにより開発された模擬プログラムであり、既知の脆弱性が含まれています。本評価の目的は、OWASP Top 10に対する当該WAF機能の整合性を評価することにあります。 WAFのベンチマークは、防御率を定義するため、当該WAFを経由した多用な既知の悪性ペイロード（SQLインジェクションやクロスサイトスクリプティング（XSS）等）によって構成されています。
結果	4つの主要な攻撃を通し行われたWAFのベンチマークは、1,738 件すべてのペイロードが、クラウドブリックWAFにより防御されたことを示しました。今回ウィズリンクスグループの脆弱性模擬アプリケーションのWeb侵入テストが明らかにしたことは、クラウドブリックWAFにより、その検証時点においてほぼすべてのOWASP Top 10の脅威に対し、仮想的にパッチ提供していることと同様の効果が得られることを確証するに至りました。唯一の残された脆弱性は、性質上WAFではほぼ検知することは不可能と考えられる、認証や認可のメカニズムに関連するもののみとなりました。

脆弱性の種類	防御したペイロード数	防御率
SQL インジェクション	599 / 599	100 %
クロスサイト スクリプティング (XSS)	600 / 600	100 %
パストラバーサル	20 / 20	100 %
OS コマンドインジェクション	519 / 519	100 %

※ 詳細は、*wizlynx group*による詳細レポートを参照頂けます。

wizlynx group について

ウィズリンクスグループ(英名：wizlynx group)は、倫理と信頼に基づき公正を尊重するスイスのサイバーセキュリティプロバイダであり、ビジネスと企業秘密を効果的に保護するため皆様に役立てられることを理念としており、その存在意義は、サイバーセキュリティと共にあります。その理由は、お客様が当社の情熱と経験から最大限の利益を享受すべきと考え、リスク管理ライフサイクル全体をカバーするサービスポートフォリオを設計しており、その中でも防御について第一義に考えています。ウィズリンクスグループは、CREST登録のペネトレーションテスターを採用し、世界でも数少ないCREST認定の侵入テストサービスプロバイダの１つであります。この高く評価された資格は、ウィズリンクスグループが最高の技術力、ポリシー、プロセスと手順を保持していることをすべてのお客様へ証明しています。

※ 本ペーパーは、wizlynx groupより実施された検証の結果レポートに基づき、作成されたExecutive Summaryを和訳したものです。
文言の解釈に関しましては、英語で作成された原文の方が優先されます。