SYNOPSYS®

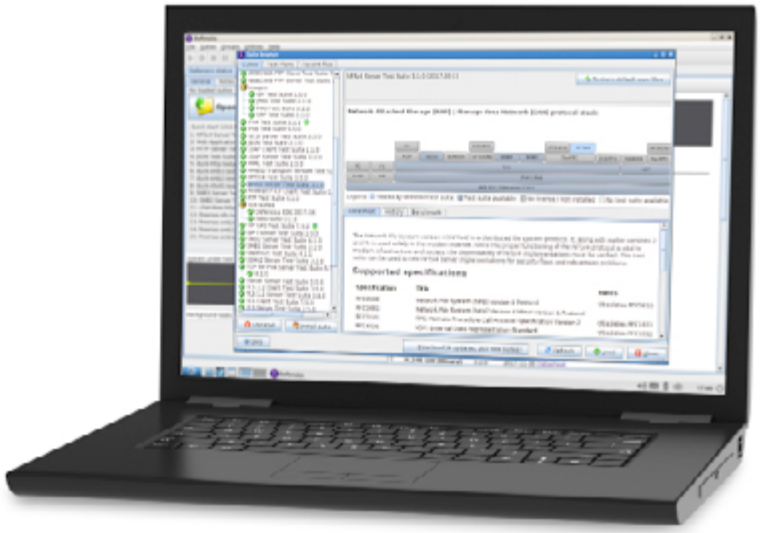
Defensics

ファジング・テスト

外部調達か内製かを問わず、ビジネスを支えるソフトウェアの脆弱性を洗い出し、ソフトウェアの堅牢性とシステムの相互運用性を高めます。

概要

Defensics® ファジング・テストは、ソフトウェアのセキュリティ脆弱性を効果的かつ効率的に検出、修正する包括的かつ強力な自動ブラックボックス・ソリューションです。体系的かつインテリジェントなアプローチを取り入れたネガティブ・テストにより、市場投入スケジュールや運用コストに影響を与えることなく製品の革新性とソフトウェア・セキュリティを両立できます。

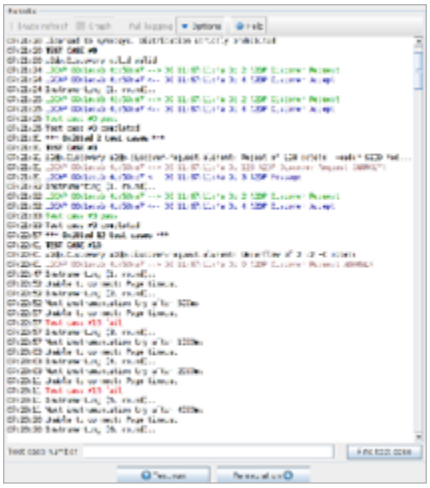


Defensics は論理的なユーザー・インターフェースを採用。画面の指示に従って手順を実行するだけで高度なファジング・テストを簡単に実行できます。

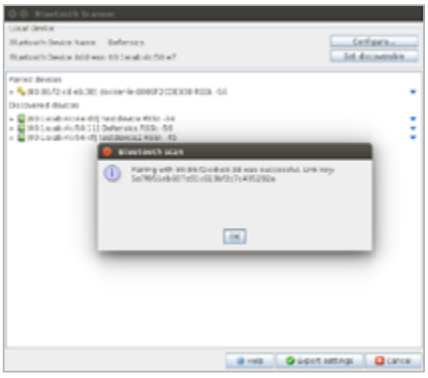
主な機能

インテリジェントなファジング・エンジン

Defensics エンジンにはインターフェース、プロトコル、ファイル・フォーマットなど入力タイプに関するナレッジが事前にプログラムされています。このため、入力タイプ内での通信を司る規則を深く理解し、その入力タイプに特有のセキュリティ脆弱性を突くような、ターゲットを絞り込んだテスト・ケースを送り込むことができます。このインテリジェントで体系的なアプローチによるファジング・テストにより、コストやセキュリティを犠牲にすることなくテスト時間を短縮できます。



Defensics のレポート。メッセージ・シーケンス・ログを利用して異常な応答の根本原因を突き止めることができます。



Defensics には Device Explorer などテスト・プロセス全体を自動化する機能が用意されており、ユーザーによる面倒な設定は不要です。

シノプシスのファジング・テストがこれまでに検出した未知の脆弱性の一覧は、こちらをご覧ください。

包括的なファジング・ソリューション

250 を超えるビルド済みのインテリジェントなテスト・スイートが用意されており、人手でテストを作成しなくてもすぐにファジング・テストを開始できます。テスト・スイートは、新しい入力タイプ、仕様、RFC を反映して常に更新されています。

- 各テスト・スイートは、メッセージ・シーケンスを微調整してカスタマイズできます。データ・シーケンス・エディタを使用すると、デフォルトの定義済みテスト・スイートに含まれないコーナー・ケースも網羅できます。
- 更に拡張性が必要な場合は、テンプレート・ファザーを使用します。Universal Data Fuzzer（ファイル・フォーマット・テンプレート・ファザー）と Traffic Capture Fuzzer（プロトコル・テンプレート・ファザー）は、ユーザーが用意したサンプル・ファイルをリバースエンジニアリングしてテスト・ケースを生成します。
- 独自 / カスタム入力タイプを使用する場合は Defensics SDK で専用のテスト・スイートを作成できます。Defensics SDK は一部のトランスポート層をサポートしており、インストルメンテーションが付属します。

あらゆる開発ライフサイクルに適合

Defensics には、ほとんどすべてのテクノロジやプロセス環境への適合を可能にするワークフローが含まれます。伝統的な SDL であれ CI 開発ライフサイクルであれ、Defensics は早期段階で開発に組み込むことができるため、最小限のコストで脆弱性を捕捉して修正できます。独自の開発ライフサイクルを使用している場合は、シノプシスの経験豊富なプロフェッショナル・サービス・チームがファジング・テスト・チェックポイントの特定からファジング・テストのメトリクス定義、ファジング・テスト成熟度プログラムの確立までをお手伝いします。

Defensics は開発プロセスに適合するだけでなく、周辺テクノロジとの連携も容易です。API およびデータ・エクスポート機能を利用してデータを共有することでレポート作成および解析の幅が広がるなど、Defensics を完全なプラグアンドプレイ方式で利用できます。

大量の詳細データを含むレポートにより効率的な修正をサポート

- コンテキスト化されたログ：Defensics とテスト対象システムの間のプロトコル・パスおよびメッセージ・シーケンスを詳細に記録した修正ログにより、各脆弱性のトリガと技術上の影響を容易に特定できます。
- 脆弱性マッピング：Defensics には各脆弱性を CWE などの業界標準規格およびインジェクション・タイプにマッピングする機能があり、必要な情報をすぐに見つけて修正できます。
- 問題の再現：Defensics では脆弱性トリガが 1 つのテスト・ケースにまで絞り込まれるため、問題を再現して正しく修正されているかどうかを検証できます。
- 修正パッケージ：暗号化した修正パッケージを生成してソフトウェア・サプライヤに渡すことにより、サプライチェーン全体で安全かつ協調的な修正が可能です。

自動化によるスケーラブルなファジング・テスト

テスト・ターゲットのスキャンから接続先のレイヤ数の決定まで、Defensics には豊富な API が用意されており、あらゆるニーズに応じた柔軟でスケーラブルな自動化が可能です。

- 単一機器のテスト
- 毎回同じテスト・プランを実行できるように、繰り返し可能なオートメーションをセットアップ可能
- 最新のスケーラブルな仮想化技術によりテスト時間を短縮

Defensics | テスト・スイート・カタログ

Authentication（認証）、Authorization（許可）、Accounting（課金やユーザーのアクセス情報の収集）(AAA)
- Diameter クライアント・サーバー
- EAPOL サーバー
- Kerberos サーバー
- LDAPv3 クライアント・サーバー
- RADIUS クライアント・サーバー
- TACACS+ クライアント・サーバー
- MACsec サーバー

アプリケーション
- FIX
- JSON フォーマット
- Web アプリケーション
- WebSocket クライアント・サーバー
- XML SOAP クライアント・サーバー
- XML ファイル
- XMPP サーバー

バス・テクノロジ
- CAN Bus
- CAN FD

セルラー・コア
- BICC/M3UA
- GRE
- GTP Prime
- GTPv0
- GTPv1 クライアント・サーバー
- GTPv2-C クライアント・サーバー
- PMIPv6 クライアント・サーバー
- S1AP
- SCTP クライアント・サーバー
- SMPP
- SMS (SMPPインジェクション)
- SMS (ファイル・インジェクション)
- X2-AP
- MAP

コアIP
- DHCP/BOOTP クライアント・サーバー
- DHCPv6 クライアント・サーバー
- DNS クライアント・サーバー
- FTP クライアント・サーバー
- HTTP クライアント・サーバー
- HTTP/2 サーバー
- ICAP サーバー
- IPv4 パッケージ
  - ARP クライアント・サーバー
  - ICMP
  - IGMP
  - IPv4
  - TCP for IPv4 クライアント・サーバー
- IPv6 パッケージ
  - ICMPv6
  - IPv6
  - TCP for IPv6 クライアント・サーバー
- SOCKS クライアント・サーバー

電子メール
- IMAP4 サーバー
- MIME
- POP3 サーバー
- SMTP クライアント・サーバー

汎用
- Traffic Capture Fuzzer
- Universal ASN.1 BER サーバー
- Universal Fuzzer

ICS
- 60870-5-104 (iec104) クライアント・サーバー
- 61850/Goose/SV
- 61850/MMS クライアント・サーバー
- BACNET
- CIP サーバー
- COAP
- DNP3 クライアント・サーバー
- MQTT クライアント・サーバー
- Modbus マスター
- Modbus PLC
- OPC UA サーバー
- Profinet DCP
- Profinet PTCP クライアント・サーバー

リンク・マネジメント
- LACP (802.3ad)
- STP/RSTP/MSTP/ESTP

メディア
- アーカイブ・パッケージ
  - GZIP
  - JAR
  - ZIP
- オーディオ・パッケージ
  - MP3
  - MPEG4 (M4A/MP4)
  - OGG
  - WAV
  - Windows Media (WMA/WMV)
- イメージ・パッケージ
  - GIF
  - JPEG
  - PNG
  - TIFF
- ビデオ・パッケージ
  - H.264 ファイル Suite
  - H.264 RTP フォーマット
  - MPEG2-TS
  - MPEG4 (M4A/MP4)
  - OGG
  - Windows Media (WMA/WMV)
- vCalendar
  - vCard

医療
- DICOM サーバー
- HL7v2 サーバー

広域イーサネット
- BFD
- CFM (802.1ag, Y.1731)
- E-LMI (MEF-16)
- Ethernet (802.3, 802.1Q)
- GARP (802.1D)
- LLDP (802.1AB)
- OAM (802.3ah)
- PBB-TE サーバー
- Synchronous Ethernet (ESMC)

PKI（公開鍵基盤）
- CMPv2 クライアント・サーバー
- CSR

遠隔管理
- CWMP (TR-69) ACS
- CWMP (TR-69) CPE
- IPMI サーバー
- Netconf test suite
- PCP サーバー
- SNMP trap
- SNMPv2c サーバー
- SNMPv3 サーバー
- SSHv1 サーバー
- SSHv2 サーバー
- Syslog
- TFTP サーバー
- Telnet サーバー

ルーティング
- BGP4+ クライアント・サーバー
- DVMRP パッケージ
  - DVMRPv1
  - DVMRPv3
- IS-IS
- LDP
- MPLS サーバー
- MSDP
- NHRP
- OSPFv2
- OSPFv3
- Openflow コントローラ
- Openflow スイッチ
- PIM-SM/DM
- RIP

- RIPng
- RSVP
- TRILL サーバー
- VRRP

ストレージ
- CIFS/SMB サーバー
- DCE/RPC サーバー
- FCOE + FIP クライアント・サーバー
- NFSv3 サーバー
- NFSv4 サーバー
- Netbios サーバー
- SMBv2 クライアント・サーバー
- SMBv3 クライアント・サーバー
- SunRPC サーバー
- iSCSI クライアント・サーバー

時刻同期
- IEEE1588 PTP クライアント・サーバー
- NTP クライアント・サーバー

VoIP
- H.323 クライアント・サーバー
- MGCP サーバー
- MSRP サーバー
- RTP/RTCP/SRTP
- RTSP クライアント・サーバー
- SIP UAC
- SIP UAS (+TT)
- SIP-I サーバー
- STUN クライアント・サーバー
- TURN クライアント・サーバー

VPN
- DTLS クライアント・サーバー
- IKEv2 クライアント・サーバー
- IPSec
- ISAKMP/IKEv1 クライアント・サーバー
- L2TPv2/v3 クライアント・サーバー
- OCSP クライアント・サーバー
- SCEP
- SSTP
- TLS/SSL クライアント・サーバー
- X.509v3 Certificates

無線
- Bluetooth LE パッケージ
  - ATT クライアント・サーバー
  - アドバタイズ
  - HOGP ホスト
  - Health
  - プロファイル
  - SMP クライアント・サーバー
- Bluetooth パッケージ
  - A2DP
  - AVRCP
  - BNEP
  - HFP AG/Unit
  - HSP AG/Unit
  - L2CAP
  - OBEX-サーバー
  - RFCOMM
  - SDP
- Wi-Fi AP パッケージ
  - 802.11 WLAN AP
  - 802.11 WPA AP
  - WPA Enterprise
- Wi-Fi Client パッケージ
  - 802.11 WLAN Client
  - 802.11 WPA Client

5G テクノロジー
- GTPv2-C クライアント・サーバー
- S1AP/NAS クライアント・サーバー
- GTPv1 クライアント・サーバー
- E1AP クライアント・サーバー
- NGAP/NAS クライアント・サーバー
- X2AP クライアント・サーバー
- XNAP クライアント・サーバー
- PFCP クライアント・サーバー
- F1AP クライアント・サーバー

モニタリング / エンジン機能

インストルメンテーション
- 有効ケース
- Syslog
- エージェント
- SNMP
- テスト実行ごとのカスタム・スクリプト

SafeGuard チェッカー
- アンプ攻撃
- 認証バイパス
- ブラインドLDAPインジェクション
- ブラインドSQLインジェクション
- 証明書の妥当性検査
- RRSIGレコードの署名者名の圧縮
- クロスサイト・リクエスト・フォージェリ
- クロスサイト・スクリプティング
- 有効ケースに比べ過剰なクッキー
- Heartbleed
- 情報漏洩
- 不十分な乱数性
- LDAPインジェクション
- 不正な形式のHTTP
- リモート実行
- SQLインジェクション
- 予期しないデータ
- 保護されていない認証情報
- 弱い暗号

各種アノマリ
- ASN.1/BERアノマリ
- 認証情報アノマリ
- ディープ・パケット・インスペクション
- EICARアンチウイルス・テスト・ファイル
- GTUBE（Generic Test for Unsolicited Bulk Email）
- 制御プレーン・インジェクション・アノマリ
- 整数アノマリ
- ネットワーク・アドレス・アノマリ
- オーバーフロー・アノマリ
- アンダーフロー・アノマリ

注: テスト・スイートは頻繁に追加されます。最新のリストについてはお問い合わせください。

シノプシスの特色

シノプシスのソフトウェア インテグリティ グループは、企業が安全で高品質のソフトウェアを構築し、リスクを最小限に抑えながらスピードと生産性の最大化に貢献します。シノプシスは、アプリケーション・セキュリティのリーダーであり、静的解析、ソフトウェア・コンポジション解析、動的解析ソリューションを提供しており、独自のコード、オープンソース・コンポーネント、およびアプリケーションの動作における脆弱性や不具合を迅速に見つけて修正します。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社
〒 158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス

TEL: 03-6746-3600
Email: sig-japan@synopsys.com