GOT OWASP?

https://www.owasp.org/index.php/Japan

The OWASP Internet of Things Top 10 - 2014

I1 安全でないウェブインターフェース

アカウントリストの漏洩、ロックアウト機構の欠如、ユーザのクレデンシャル情報が弱い場合、ウェブインターフェースは安全とは言えません。
特に、内部ネットワークのユーザのみが使用すると考えられているウェブインターフェースの多くは安全性が低くなっています。しかし、内部ユーザからの脅威は外部ユーザからの脅威に相当する危険性があります。ウェブインターフェースの問題は、XSSなどの脆弱性を特定できる自動テストツールを活用しながら手作業で確かめていくことで容易に見つけることができます。

I2 欠陥のある認証・認可機構

パスワードが脆弱で、しかもその保護が不十分である場合、認証・認可機構に欠陥が生じます。内部ネットワークのユーザのみが使用し、外部ネットワークのユーザからはアクセスされないことを前提としている場合、ほとんどのインターフェースにこのような欠陥が見られます。認証・認可機構の問題の多くは、自動テストツールでも、手作業でも容易に見つけることができます。

I3 安全でないネットワークサービス

安全でないネットワークサービスは、バッファオーバーフロー攻撃や、ユーザがデバイスを使えなくするサービス妨害(DoS)攻撃の影響を受けやすくなります。また、他ユーザに対するDoS攻撃では、安全でないネットワークサービスを悪用されることがあります。ポートスキャンやファジングツールで検知することで、安全性を確認できます。

I4 通信路の暗号化の欠如

通信の暗号化を行わないと、LANやインターネットで通信されるデータを誰からでも見られるようになります。LANのトラフィックは内部の限られた人にしか見られないため通信路の暗号化が不要だと考える人もいるでしょうが、ワイヤレスネットワークでは、設定の不備があれば誰にでもトラフィックを見られるようになります。この問題の多くは、ネットワークトラフィック上で、実際に読めるデータを調べることで容易に見つけることができます。また自動化ツールでSSLやTLSのような常識的な暗号化通信が適切に実装されているかを調べることができます。

I5 プライバシー

プライバシーの問題は、収集した個人情報の保護が適切でない場合に発生します。デバイスのセットアップ時にユーザから収集するデータを分析することで、プライバシーの問題を検知できます。また、自動化ツールでパターンを特定して検索することで、個人情報や機微情報の収集状況を確認できます。

I6 安全でないクラウドインターフェース

ユーザの認証情報やアカウントリストを推測しやすい場合、クラウドインターフェースは安全とはいえません。クラウドインターフェースへの接続内容をレビューし、その通信がSSL接続を用いているかどうか、さらにパスワードリセット機構がアカウントの有効性を見せて結果的にアカウントのリスト化につながってしまうものとなっていないかなどを確認することにより、安全性を確認することができます。

I7 弱いモバイルインターフェース

推測しやすいユーザ認証情報やアカウントリストを取得可能である場合、モバイルインターフェースは安全とはいえません。ワイヤレスネットワークへの接続やSSL接続の有無、パスワードリセット機構がアカウントリスト作成につながるかどうかなどを確認することでモバイルインターフェースの安全性を確認できます。

I8 セキュリティ設定の不備

セキュリティ設定の不備は、ユーザにデバイスのセキュリティ設定についてのスキルがないか、不足している場合に生じます。
また、ウェブインターフェースの設定画面で、緻密なアクセス権限の設定ができない場合、たとえば強力なパスワードの使用を必須にすることができない場合などにも生じます。手動で設定画面をレビューし、これらのオプションの存在を調べることで確認できます。

I9 ソフトウェア・ファームウェアの問題

更新できないデバイスは、それ自体がセキュリティ欠陥です。デバイスに脆弱性が発見されたら、そのデバイスは更新できなければなりません。また、肝心のソフトウェアやファームウェアのアップデートの配信において、ネットワーク接続が保護されていない場合も安全とは言えません。また、ソフトウェアやファームウェアに認証情報など機微情報がハードコーディングされている場合も安全ではありません。この問題を発見するには、アップデート時のトラッフィックをチェックしたり、バイナリエディタなどを使いアップデートファイルそのものに関心を誘う情報が含まれていないかを分析します。

I10 物理的な問題

攻撃者がデバイスを取り外すことで、記録媒体や、そこに保存されているデータにアクセスできる場合、物理的な脆弱性が存在すると言えます。また、USBなど外部ポートが設定やメンテナンス用の機能としてアクセスできる場合にも、物理的なセキュリティの問題になります。

OWASPの成果物は、無料で自由にご利用になれます。

- **脆弱性とリスク**: OWASP Top 10 / OWASP Mobile Top 10
- **セキュリティテスト**: ASVS / Testing Guide
- **開発ガイドライン**: Developer Guide / Cheatsheets
- **ゲーム形式の勉強ツール**: Snakes and Ladders

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

designed by Asterisk Research, Inc.

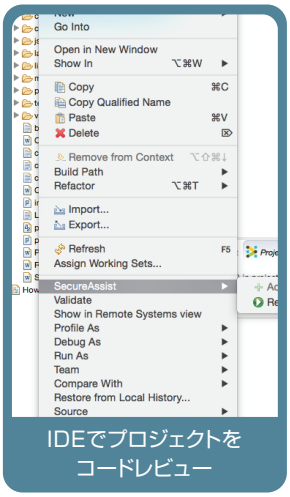
TRY SecureAssist

http://secureassist.jp/downloads

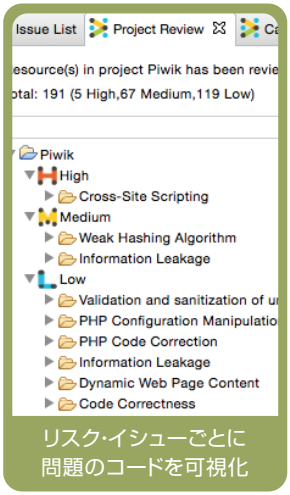
そりゃ誰も、問題のあるコードを作りたくはありません。

…セキュア開発は習得が困難。しかも開発にはスケジュールとコストのプレッシャーが強い。
でも、後で問題が発覚してからの対応では、修正するコストもリスクも高くつくのはわかります。

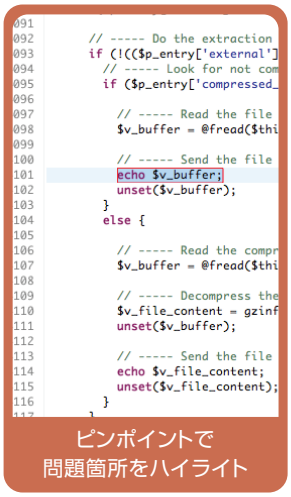
答え 開発段階で素早く問題コードを見つけ、すぐに修正し、再発を防ぐ仕組みが有効。



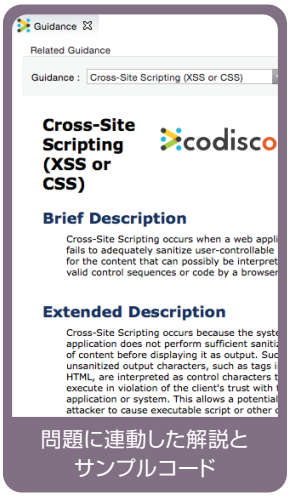
IDEでプロジェクトを
コードレビュー



リスク・イシューごとに
問題のコードを可視化



ピンポイントで
問題箇所をハイライト



問題に連動した解説と
サンプルコード

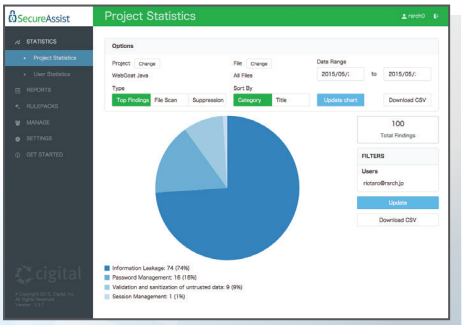
OWASPなど、参考資料への
リンクも提供

OWASP Top 10 2010/2013、IoT Top 10やCWE/SANS Top 25 2011 対策はもちろんのこと、セキュアコーディングの最新のテストケースとガイドを搭載。 PCI DSS準拠にも有効です。

入力値検証 / 出力値エンコーディング	安全でないデータの取り扱い	適切なコーディング手法
クロスサイトスクリプティング(9)	安全でないデータの保存(6)	スレッドAPI(3)
SQLインジェクション(4)	機微情報の漏洩(11)	Struts設定の不備(11)
Path マニピュレーション(2)	貧弱な暗号の利用(8)	不適切なエラー処理(3)
DoS 攻撃(6)	信頼境界の違反(9)	ログの取り扱い(2)
ファイル入出力(2)	未検証のリダイレクトや転送(2)	クッキーのセキュリティ(3)
未検証のユーザ入力(5)		リソースの取り扱い(3)

※2015年時点のテスト項目カテゴリです。定期的に更新されます。

管理機能 Enterprise Portal は、プロジェクトの継続的な品質管理に役立ちます。



- プロジェクトの整理と品質の情報収集
- ルールやガイドのカスタマイズと配信
- 利用者グルーピング、ライセンス管理(最小構成20 ID)

対応する言語

Java .NET PHP

対応する開発環境

Eclipse
Visual Studio
RAD
Spring Tool Studio
NEW IntelliJ

SecureAssist

事後対応から開発プロジェクトを解放しましょう。このツールははるかに安価で、導入は容易です。
IDEプラグインの全機能は30日間無料で試用できます。
今すぐご活用ください。

sales@rsrch.jp
03-6380-9133

Asterisk Research, Inc.