45分で分かる
安全なWebアプリケーション開発のための
発注・要件・検収

2009年9月4日

HASHコンサルティング株式会社
徳丸　浩

本日お話しするテーマ

- セキュア開発をベンダーに促すにはどうすればよいか
- セキュア開発においてコストを低減するには
- セキュア開発の要件定義はどう考えればよいか
- セキュア開発で大切な3つのこと
  - セキュリティ要件とセキュリティバグ
  - 開発標準と教育
  - セキュリティテスト
- セキュリティテストツールとしての「ウェブ健康診断仕様」

Copyright (C) 2009 HASH Consulting Corp.

徳丸浩の自己紹介

- 経歴
  - 1985年 京セラ株式会社入社
  - 1995年 京セラコミュニケーションシステム株式会社(KCCS)に出向・転籍
  - 2008年 KCCS退職、HASHコンサルティング株式会社設立
- 経験したこと
  - 京セラ入社当時はCAD、計算幾何学、数値シミュレーションなどを担当
  - その後、企業向けパッケージソフトの企画・開発・事業化を担当
  - 1999年から、携帯電話向けインフラ、プラットフォームの企画・開発を担当
    Webアプリケーションのセキュリティ問題に直面、研究、社内展開、寄稿などを開始
  - 2004年にKCCS社内ベンチャーとしてWebアプリケーションセキュリティ事業を立ち上げ
- その他
  - 1990年にPascalコンパイラをCabezonを開発、オープンソースで公開
    「大学時代のPascal演習がCabezonでした」という方にお目にかかることも
- 現在
  - HASHコンサルティング株式会社　代表　http://www.hash-c.co.jp/
  - 京セラコミュニケーションシステム株式会社　技術顧問　http://www.kccs.co.jp/security/
  - 独立行政法人情報処理推進機構　非常勤研究員　http://www.ipa.go.jp/security/

Copyright (C) 2009 HASH Consulting Corp.

責任と契約について

- Webアプリの脆弱性の責任は発注者か開発者か
  - 発注者に責任というのが主流のよう
  - ただし、判例があるわけではないので要注意
- 経産省の「モデル契約書」では、以下のような記述がある

> なお、本件ソフトウェアに関するセキュリティ対策については、具体的な機能、遵守方法、管理体制及び費用負担等を別途書面により定めることとしている（第50 条参照）。**セキュリティ要件をシステム仕様としている場合には**、「システム仕様書との不一致」に該当し、本条の「瑕疵」に含まれる。

> （セキュリティ）
> 第50 条 乙が納入する本件ソフトウェアのセキュリティ対策について、甲及び乙は、その具体的な機能、遵守方法、管理体制及び費用負担等を協議の上、別途書面により定めるものとする。

- 発注者は自衛のために要求仕様にセキュリティ用件を盛り込んでおくべき
  - 「発注者のための・・・」
  - 「ウェブ健康診断仕様」によるテストに合格すること、と記述する手もありか

Copyright (C) 2009 HASH Consulting Corp.

RFI/RFPの書き方アプローチ

- パターン1:提案を求める
  - 要求も提案も曖昧になりがち
    - 要求の例:セキュリティに留意して開発すること
    - 提案の例:セキュリティには万全の体制で臨みます
- パターン2:詳細な仕様を出す
  - 「安全なWebサイトの作り方」に準拠せよ
  - 「発注者のためのWebシステム／Webアプリケーション セキュリティ要件書」に準拠せよ
- パターン3:検査仕様を提示する
  - 第三者に検査させる
  - 発注者が自ら検査する(後述)

Copyright (C) 2009 HASH Consulting Corp.

RFI/RFPの書き方

- 漠然としたものは効果が薄い
- 脆弱性の名前を列挙する方法
  - XSS、SQLインジェクション【略】の対策を施すこと
  - 対策の「質」を問うことは難しい
- 実装方式を指定する方法
  - 例：SQLアクセスの際はPrepared Statementを使用すること
  - 既存ソフトの流用やフレームワークの使用に制限が生じると、コスト増の要因になり得る
- 検収の方法を指定する
  - 例：弊社の指定する脆弱性検査会社の試験に合格すること
  - コストは高くなる
  - 検査会社の検査内容がグレーなので、開発会社にとってはリスク
  - 「ウェブ健康診断仕様」の応用【後述】

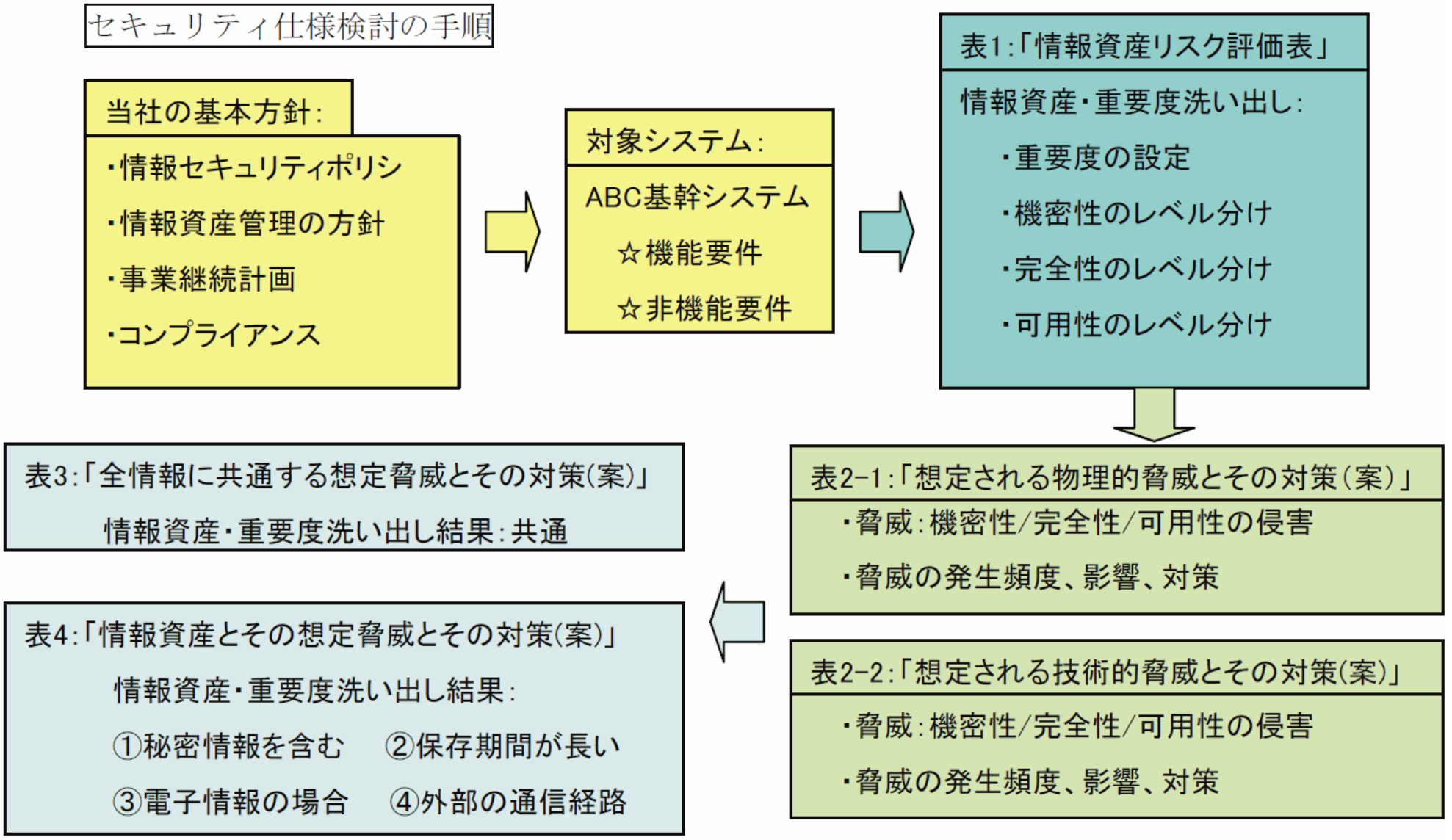
Copyright (C) 2009 HASH Consulting Corp.

提案する方法

- 基本はベンダーに提案してもらう
  - 開発言語、ミドルウェア、フレームワークを考慮したセキュアな開発体制を提案してもらう
  - セキュリティ的な機能の提案
  - 脆弱性を作り込まない体制の提示を求める
  - セキュリティ検査にパスできる根拠を説明してもらう
- 納品物としてセキュリティ検査結果を添付してもらう
  - 今後、納品検査としてのセキュリティ検査は必須とすべき
- 検収時の検査として自らもセキュリティ検査を実施する
  - 「Web健康診断仕様」による検査を自ら実施する（一種の抜き取り検査）
  - 予算に余裕があれば、第三者に検査してもらう

Copyright (C) 2009 HASH Consulting Corp.

従来言われてきたセキュリティ仕様策定プロセス



経済産業省「モデル契約書」別紙3より引用 http://www.meti.go.jp/policy/it_policy/softseibi/index.html#05

資産洗いだし・リスク分析・対策の例

表-1:「情報資産リスク評価表」

情報資産名	情報提供元（もしくは情報先）情報システム	外部	情報提供先（もしくは情報元）情報システム	外部	保管場所	保管形態	保管期間	秘密情報	機密性	完全性	可用性	重要度
○○情報	社員		文書保存システム		文書保存システム	ー	5年	×	Ⅲ	Ⅰ	Ⅲ	Ⅱ
△△情報	ABC基幹システム		ABC基幹DB		ABC基幹DB	電子媒体	5年	○	Ⅲ	Ⅰ	Ⅲ	Ⅱ
××情報	外部委託業者	○	ABC基幹DB		ABC基幹DB	電子媒体	5年	×	Ⅲ	Ⅰ	Ⅲ	Ⅱ

～ 以下略 ～

表2-2:「想定される技術的脅威とその対策（案）」

No.	脅威			発生頻度	影響の大きさ	対策
13	機密性の侵害	故意	盗聴、情報漏洩 不正アクセス なりすまし	少ない	システム全体に影響を及ぼし秘密情報漏洩にもつながる	暗号化 侵入検知 ユーザ認証 アクセス制御
14			ウイルス感染	多い	システム全体に影響を及ぼし秘密情報漏洩にもつながる	ウイルス対策
15		偶発	ー	ー	ー	ー
16	完全性の侵害	故意	情報の改ざん、削除 不正アクセス なりすまし	少ない	システム全体に影響を及ぼす	侵入検知、監査 ウイルス対策 ユーザ認証 アクセス制御 電子署名 原本性保証1
17			ウイルス感染	多い	システム全体に影響を及ぼす	ウイルス対策
18		偶発	ー	ー	ー	ー
19	可用性の侵害	故意	不正アクセス （DDoS 等含む） なりすまし	多い	システム全体に影響を及ぼす	侵入検知 ユーザ認証 アクセス制御
20			ウイルス感染	多い	システム全体に影響を及ぼす	ウイルス対策
21		偶発	トラフィック過負荷	多い	システム全体に影響を及ぼす	負荷分散装置の設置、トラフィックの監視

「多い」:　「半年～1年間に1度発生するかどうか程度」
「少ない」:「ほぼ発生しないと思われるが発生する可能性のある脅威」

経済産業省「モデル契約書」別紙3より引用 http://www.meti.go.jp/policy/it_policy/softseibi/index.html#05

情報資産洗いだしの例

保護すべき資産	保護の必要性	機密性	完全性	可用性	要保護
サービス利用に関するドキュメントデータ(個人情報)	インターネット上においてサービス利用者と本情報システム間で送受信されるサービス利用に関するドキュメントデータ及び本情報システム内に存在するサービス利用に関するドキュメントデータの漏えい、改ざんを防止しなければ、サービス利用者の個人情報を保護できない。	3	2	2	○
Web コンテンツデータ本情報システム内に存在するWebコンテンツデータ	に対する改ざん、削除を防止しなければ、正常なサービスを提供できなくなり、社会的な信用を失墜する。	1	2	2	○
様式データ	本情報システム内に存在する様式データ及びインターネット上においてサービス利用者と本情報システム間で送受信される様式データに対する改ざんを防止しなければ、正常なサービスを提供できない。	1	2	2	○
秘密鍵データ	本情報システム内に存在する秘密鍵データに対する改ざん及び漏えいを防止しなければ、正常なサービスを提供できない。	3	2	2	○
システムの構成情報データ	本情報システム内に存在するシステムの構成情報データに対する改ざんを防止しなければ、正常なサービスを提供できない。	2	2	2	○
証明書データ	本情報システム内に存在する証明書データに対する改ざん、漏えいを防止しなければ、正常なサービスを提供できない。	2	2	2	○
監査証跡	本情報システム内に存在する監査証跡データに対する改ざん、削除、漏えいを防止しなければ、インシデントが発生した場合等の原因追究ができない。	2	2	1	○

完全性と可用性はだいたい「中」くらいになる

機密性の高低くらいを洗い出せば十分

「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」より引用

脅威分析の例

No	脅威分類	脅威タイトル／脅威内容
脅威(公開)-T1	情報資産の漏えい、改ざん、削除	**不許可サービスの悪用による脅威** インターネット上の攻撃者が明示的に利用を許可されていないサービスを使用することにより、情報資産の漏えい、改ざん、削除が発生する。
脅威(公開)-T2	情報資産の漏えい、破壊	**インターネットを流通するデータに対する脅威** インターネット上の攻撃者がサービス利用者と本情報システムとの間で送受信されるサービスの利用に関するWeb 入出力データを含むパケットに対して盗聴、改ざんを行うことにより、サービス利用者の個人情報が漏えい、破壊される。
脅威(公開)-T3	サービスの可用性低下	**情報資産の漏えい、改ざん、削除、不正なプログラムによる脅威** インターネット上の攻撃者により本情報システムに対して意図的に不正なプログラムを侵入させる、又は偶発的に不正なプログラムが混入することにより、サービス えい、改ざん、削除が発生す
脅威(公開)-T4	情報資産の漏	 になりすまして不正な操作を
脅威(公開)-T5	情報資産の漏 ざん、削除	 業務担当者、監査担当者、又 により、情報資産の漏えい、改 ざん、削除が発生する。
脅威(公開)-T6	情報資産の漏えい、改ざん、削除	**サービス利用者の権限を逸脱した不正行為による脅威** インターネット上のサービス利用者が与えられた操作範囲を逸脱して不正な操作を行うことにより、他のサービス利用者の情報資産を漏えいさせる。また、本情報システムの運営にかかわる情報資産に対する不正な操作を行うことにより、Webコンテンツの改ざん、削除が発生する。
脅威(公開)-T7	情報資産の漏えい、改ざん、削除	**運用関係者の権限を逸脱した不正行為による脅威** 本情報システムの運用に携わる者が各々に付与された役割と権限の範囲を逸脱して不正な操作を行うことにより、情報資産の漏えい、改ざん、削除が発生する。

脅威分析は、どのサイトでも同じような結果になる

開発プロジェクトごとに脅威分析をやってもあまり意味はない

「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」より引用

脅威に対する技術的対策の例

No	技術的セキュリティ対策のタイトル／内容
技術対策-1	**ネットワーク通信データ制御** インターネットと公開セグメントの間、公開セグメントと内部セグメントの間では、本情報システムが提供するサービスに**必要となるサービスポートのみのネットワーク通信データを流通させる**。また、特定の送信パターンに該当するネットワーク通信データを制御することにより、不正なネットワーク通信データを遮断し、必要最小限のネットワーク通信データのみを流通させる。加えて、正当なサービス利用者によるサービス要求過多時においても、同時接続数の制限や通信量の制限により、過負荷を抑止制御する。また、本情報システムの動作に不要なサービスプログラムは非活性化する。更に、インターネットと公開セグメントの間は、識別された特定箇所のみでネットワーク接続する。
技術対策-2	**識別と認証** 本情報システムにかか 利用者に対しては、ユー 行う。公開セグメント及び 者、監査担当者及び保
技術対策-3	**アクセス制御** 本情報システムが提供 者、監査担当者、本情報 ステムを利用又は管理 **囲を制御する**。アクセス する。
技術対策-4	**監査証跡の採取と侵害** 本情報システムの利用状 監査証跡を特定の監査証跡属性情報に従って分析を行う。
技術対策-5	**高信頼データ転送** インターネット上のサービス利用者と公開セグメントとの間で送受信されるネットワーク通信データを**SSL により暗号化**を施す。また、IDC と監視センター間で送受信されるネットワーク通信データは、VPN により暗号化を施す。
技術対策-6	**不正プログラムの排除** ウィルスやワーム等の**不正プログラムの侵入を検知し、その削除、非活性化と、運用者にアラートを通知**する。また、不正プログラムを検出するための検出パターンを常に最新状態に維持する。

技術的対策も、毎回同じようなものが「候補」にあがる

脅威分析の結果というより、情報資産の価値と機密性に応じて、対策を選ぶような形になりがち

脅威分析の結果によって技術的対策が左右されることはあまりない･･･と思う

「情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書」より引用

リスク分析は手間の割に効果が少ない

- 一般的なWebアプリの場合、わかりきっていることをなぞる結果になりやすい
  - 重要な情報はなにか?
    - 個人情報、企業情報など
  - 情報の格納場所はどこか
    - データベースに決まっている
  - 情報資産に対する対策方法は?
    - ベストプラクティスが分かっている
- 重要なのは、なにが重要情報か(What)ではなく、それをどう(How)扱うか
- わかりきった資産洗いだしをするよりも、「対策を選ぶ」ようなアプローチの方が効果的

Copyright (C) 2009 HASH Consulting Corp.

リバース・リスク・アセスメントの勧め

ベストプラクティスのセキュリティ対策から選択しあるいはリスクを許容する

対策	採用	不採用時のリスク	代替コントロール
ファイアウオール	○	-	-
WAF	○	-	-
IDS/IPS	×	攻撃予兆の見逃し、脆弱性対策の漏れに対する攻撃	WAFによる防御、 WAF等のログ監視強化、 脆弱性対策強化
認証方式	パスワード認証	パスワード管理の不備を突いた攻撃を受ける	パスワード管理の徹底
回線の選択	SSL	-	-
データベースの暗号化	△（パスワードのハッシュ化のみ）	ストレージ持ちだしによる情報漏洩	入退室管理強化による持ち出し対策
監査証跡	認証、エラー、操作ログ	-	-
ウィルス対策ソフト	×	マルウェアの感染	速やかなパッチ適用、 本番環境と運用環境間のFW

Copyright (C) 2009 HASH Consulting Corp.

脆弱性対策と開発プロセス

- 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)などが「ないこと」という要求は、仕様として盛り込みにくい
- リスク分析の結果で脆弱性対策をするものではない。
  脆弱性対策は常にすべき。
- これらはセキュリティバグであり、バグがないことはわざわざ仕様に明記するものではない
- 脆弱性対策は、開発標準に盛り込むのがよい
  - だから、ベンダーの開発標準が重要
  - 開発標準の閲覧を要求するのも一法
- ただし、契約上の問題は別
  - ベンダーの責任範囲は、発注仕様に書いてある範囲

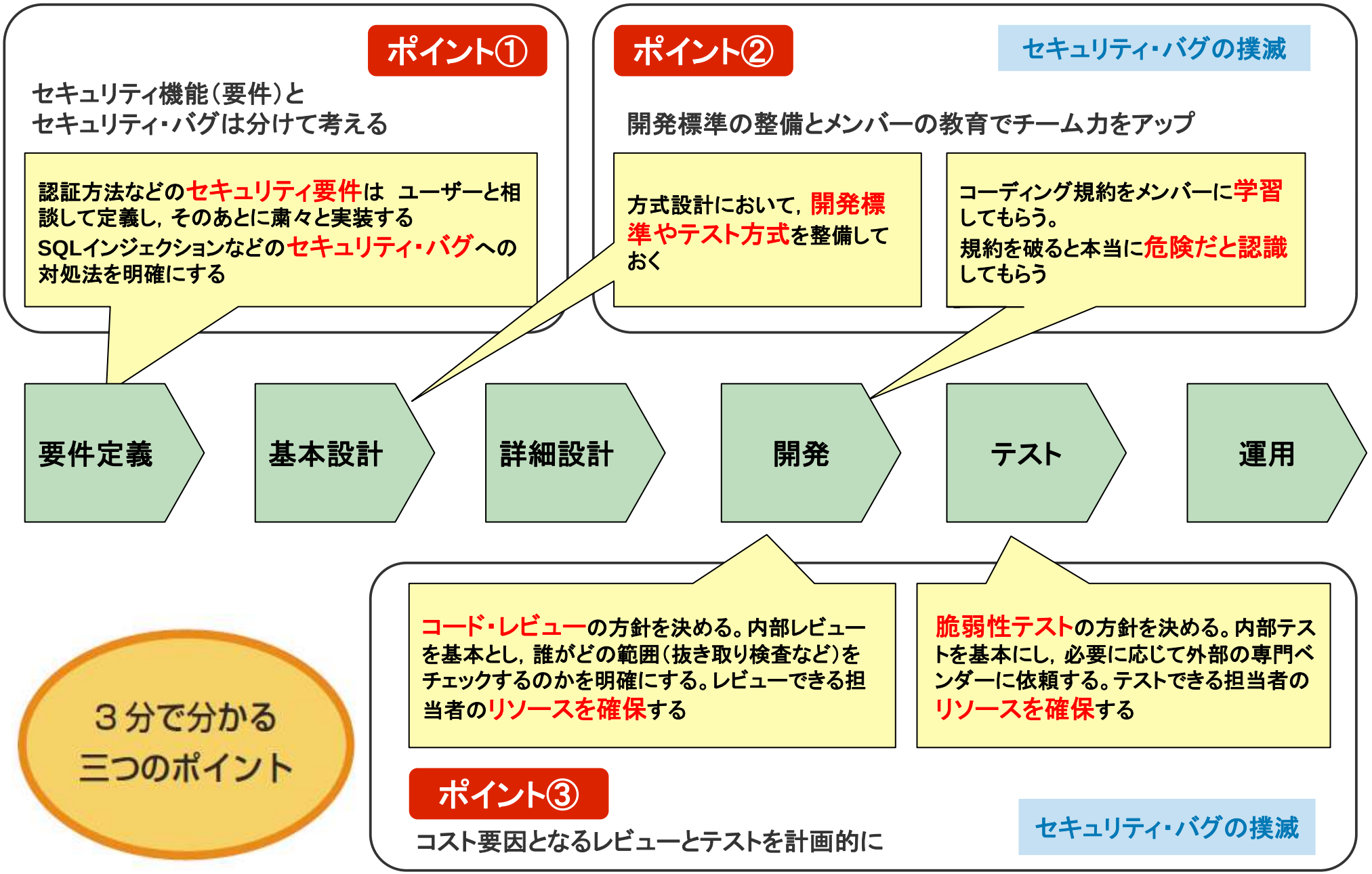
Copyright (C) 2009 HASH Consulting Corp.

提案:3つのポイント

- セキュリティ要件とセキュリティバグ
- 開発標準と教育
- セキュリティテスト

Copyright (C) 2009 HASH Consulting Corp.

3分で分かるセキュアプログラミング



日経SYSTEMS2009年8月号「プロマネの技で守るWebセキュリティ」図1を改変

セキュリティ要件とはなにか

- リバース・リスク・アセスメントのところで出てきたような「積極的な」セキュリティ対策
- セキュリティ仕様の例
  - パスワード仕様、アカウント・ロック…
  - 暗号化（回線、データベース）
  - ログ
  - ウィルス対策ソフトの導入
  - …
- セキュティ仕様の実装は、要件定義からウォーターフォールで粛々と実施(通常機能と同じ)
- 脆弱性対策は開発標準で対応

Copyright (C) 2009 HASH Consulting Corp.

開発標準と教育

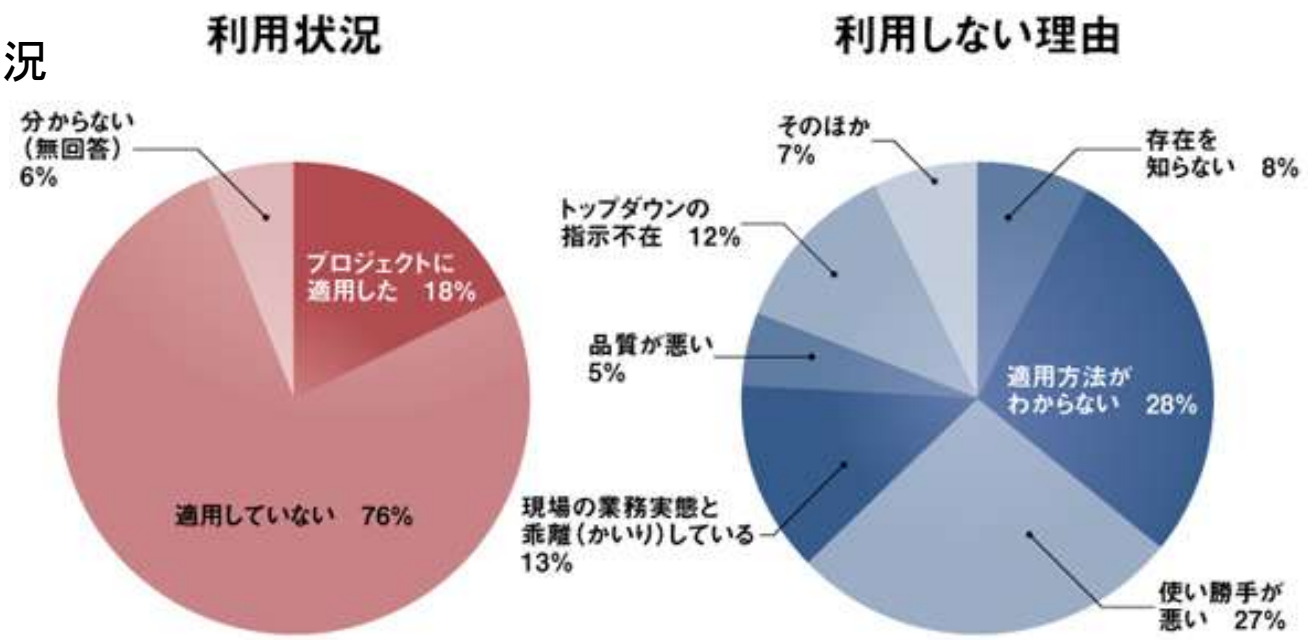
- SQLインジェクション対策やXSS対策などは、実装設計時に個別に設計していたのでは効率が悪いし、対応が統一できないので、開発標準で定義する
- 開発標準は作りっぱなしになることが多く、定着が難しい。教育を実施して、テストで定着度を確認するとよい
- 日経SYSTEMS寄稿時に各社にインタビューした際の印象では、「やられサイト」を作って開発者向けにデモしている企業が意外に多く、効果が期待できる

Copyright (C) 2009 HASH Consulting Corp.

開発標準として利用できるリソース

- 安全なウェブサイトの作り方　改訂第3版
  - http://www.ipa.go.jp/security/vuln/websecurity.html
- 発注者のためのWebシステム／Webアプリケーション セキュリティ要件書
  - http://脆弱性診断.jp/specifications/index.html
- いずれも基本的な内容だが、これくらいからスタートするほうが賢明

【参考】K社の
開発標準利用状況



引用:http://techtarget.itmedia.co.jp/tt/news/0902/10/news01.html

Copyright (C) 2009 HASH Consulting Corp.

方式設計のすすめ

- 開発標準の抽象度が高い場合、基本設計フェーズの「方式設計」として、具体的なコードレベルに落としておくとよい

XSS対策のため特殊文字をエスケープする

HTML表示の際に「<」、「>」、「&」、「”」は文字参照によりエスケープする

HTML表示の際にhtmlspecialchars()関数によりエスケープ

HTML表示の際にライブラリ e()関数を用いる
【実装】

```
function e($p) {
  echo htmlspecialchars($p, ENT_QUOTES, 'UTF-8');
}
```

Bad

Good

- 開発言語、アーキテクチャ、ライブラリ、チームの習慣等を考慮し、コピペ可能なレベルまで具体化しておく
- 方式設計の際には、テスト方法も検討しておくとよい

Copyright (C) 2009 HASH Consulting Corp.

コスト要素はどこか

- 「セキュリティ要件」については、機能が増えることになるので、直接コスト増となる
  - 発注者と要件詰めをしっかり行う必要がある
- セキュリティバグについては以下がコスト要因となる
  - 開発標準作成、開発者の教育
  - セキュリティテスト
- 「発注者のための…セキュリティ要件書」でコスト増になるのは・・・
  - アカウントロック機能の作りこみ
  - SSLの証明書代　　…たいしたことはない
- 開発標準や教育はプロジェクトをまたがって有効なので間接費用と考えられる。一度しっかりしつものを作れば使い回しがきく
- セキュリティテストはプロジェクトごとに必要であり、費用も大きいので、**セキュリティテストのコスト削減**が、セキュア開発の課題

Copyright (C) 2009 HASH Consulting Corp.

セキュリティテスト

- セキュリティ要件にせよ、セキュリティバグにせよ、最終的にはテストで品質を保証することになる
- 開発工程
  - ソースコードレビュー、ソースコードチェッカー
  - 単体テスト工程での「ウェブ健康診断仕様」利用もあり
- テスト工程
  - ツールでのテスト・・・ツールが高価、全項目テストできない
  - ウェブ健康診断仕様の活用
  - 専門家にアウトソース
- 受け入れテスト（検収）
  - ウェブ健康診断仕様の活用
  - 専門家にアウトソース

Copyright (C) 2009 HASH Consulting Corp.

ウェブ健康診断とは

診断方式： 遠隔地からインターネット経由による手動若しくは自動診断ツールを利用
診断実施数：約300団体
診断対象： 地方公共団体が保有若しくは利用している、現在インターネットで稼動中のWebサーバ1サイト分（1ドメインネーム）

http://www.lasdec.nippon-net.ne.jp/cms/12,1284.html より引用

ウェブ健康診断仕様(1)

- 12項目の診断項目により危険度の高い脆弱性項目を網羅している
  - 実被害に至る可能性の高いものに限定
  - 「安全なウェブサイトの作りかた 改定第3版」で解説されている9種類の脆弱性を包含
- 診断仕様、判定基準、抜き取り基準が明確に定義・公開されている
- 公開された無償ツールのみで診断できる
- 本番稼働サイトの診断を前提とした安全性の高い診断仕様である

Copyright (C) 2009 HASH Consulting Corp.

ウェブ健康診断仕様(2)

記号	診断項目（脆弱性名）	危険度	能動的攻撃/受動的攻撃	想定被害		
				情報漏洩	改ざん	妨害
(A)	SQL インジェクション	高	能動的	○	○	○
(B)	クロスサイト・スクリプティング(XSS)	中	受動的	○	△	
(C)	クロスサイト・リクエスト・フォージェリ(CSRF)	中	受動的	△	○	○
(D)	OS コマンドインジェクション	高	能動的	○	○	○
(E)	ディレクトリ・リスティング	低～高	能動的	○		
(F)	メールヘッダインジェクション	中	能動的			○
(G)	パストラバーサル	高	能動的	○	△	
(H)	意図しないリダイレクト	中	受動的	○		
(I)	HTTP ヘッダインジェクション	中	受動的	○	△	
(J)	認証	低～中	能動的	○	○	
(K)	セッション管理の不備	低～高	能動的／受動的	○	○	
(L)	アクセス制御の不備、欠落	高	能動的	○	○	

http://www.lasdec.nippon-net.ne.jp/cms/12,1284.html より引用

ウェブ健康診断仕様(3)

診断対象画面（機能）名称	診断対象画面(機能)の定義	最低限実施する診断項目
ログイン	ユーザ ID とパスワードを入力する等して認証を行う画面。パスワードの代わりに「暗証番号」等の表記になっている場合もある。認証機能のある Web サイトの場合は、かならずどこかにログイン画面がある(はず)。	(H) 意図しないﾘﾀﾞｲﾚｸﾄ (J) 認証 (K) ｾｯｼｮﾝ管理不備
ログアウト	認証状態を廃棄するための機能。認証機能があれば、ログイン機能は必ずあるが、ログアウト機能を有しているとは限らない。ログアウトボタン等が見当たらない場合は、よく探すか、サイト管理者に問い合わせる等で調べる。	(K) ｾｯｼｮﾝ管理不備
DB アクセス	検索機能やデータ登録・参照機能等、SQL を利用していると想定される画面のこと。実際に SQL を使っているか、他の手段(ファイル、オブジェクト DB 等)を利用しているかは分からないので、通常 SQL を利用していると想定されるものを列挙すればよい。	(A) SQL ｲﾝｼﾞｪｸｼｮﾝ
入力内容確認	ユーザが入力した値を次の画面で表示し、確認できるようになっている画面。一般的に、データ入力の画面は、「入力」→「確認」→「登録」の 3 画面構成になっていることが多く、その場合の 2 番目の画面を指す。Web サイトによっては「入力」→「登録」という構成の場合もある(この場合は確認画面がない)ので、その場合は別の画面を探す。	(B) ｸﾛｽｻｲﾄ･ｽｸﾘﾌﾟﾃｨﾝｸﾞ

http://www.lasdec.nippon-net.ne.jp/cms/12,1284.html より引用

ウェブ健康診断仕様(4)

画面チェックシート

チェックシート生成

			認証		SQL	XSS			ヘッダ		特定副作用			
	タイトル	URL	ログイン	ログアウト	DBアクセス	入力確認	エラー	ファイル名	Cookie	リダイレクト	パスワード変更	DB更新	メール送信	アクセス制御有
1	ログイン	http://xxxxxxxxxlg.jp/begin.jsp	レ		レ				レ	レ				
2	ログアウト	http://xxxxxxxxxlg.jp/logout.jsp		レ										
3	個人情報入力	http://xxxxxxxxxlg.jp/entryPersonalInfo.jsp												
4	個人情報入力確認	http://xxxxxxxxxlg.jp/confirmPersonalInfo.jsp				レ								
5	個人情報登録	http://xxxxxxxxxlg.jp/registPersonalInfo.jsp										レ		
6	パスワード変更	http://xxxxxxxxxlg.jp/changePassword.jsp									レ	レ	レ	

			1	2	3	4	5	6	7	8	9	10	11	12
	タイトル	URL	SQLインジェクション	パストラバーサル	XSS	HTTPヘッダインジェクション	メールヘッダインジェクション	OSコマンドインジェクション	CSRF	意図しないリダイレクト	ディレクトリリスティング	認証	セッション管理不備	アクセス制御不備
1	ログイン	http://xxxxxxxxxlg.jp/begin.jsp												
2	ログアウト	http://xxxxxxxxxlg.jp/logout.jsp												
3	個人情報入力	http://xxxxxxxxxlg.jp/entryPersonalInfo.jsp												
4	個人情報入力確認	http://xxxxxxxxxlg.jp/confirmPersonalInfo.jsp												
5	個人情報登録	http://xxxxxxxxxlg.jp/registPersonalInfo.jsp												
6	パスワード変更	http://xxxxxxxxxlg.jp/changePassword.jsp												

Copyright (C) 2009 HASH Consulting Corp.

ウェブ健康診断仕様(5)

2.4 診断時に利用する診断項目毎の検出パターン（目安）、脆弱性有無の判定基準について

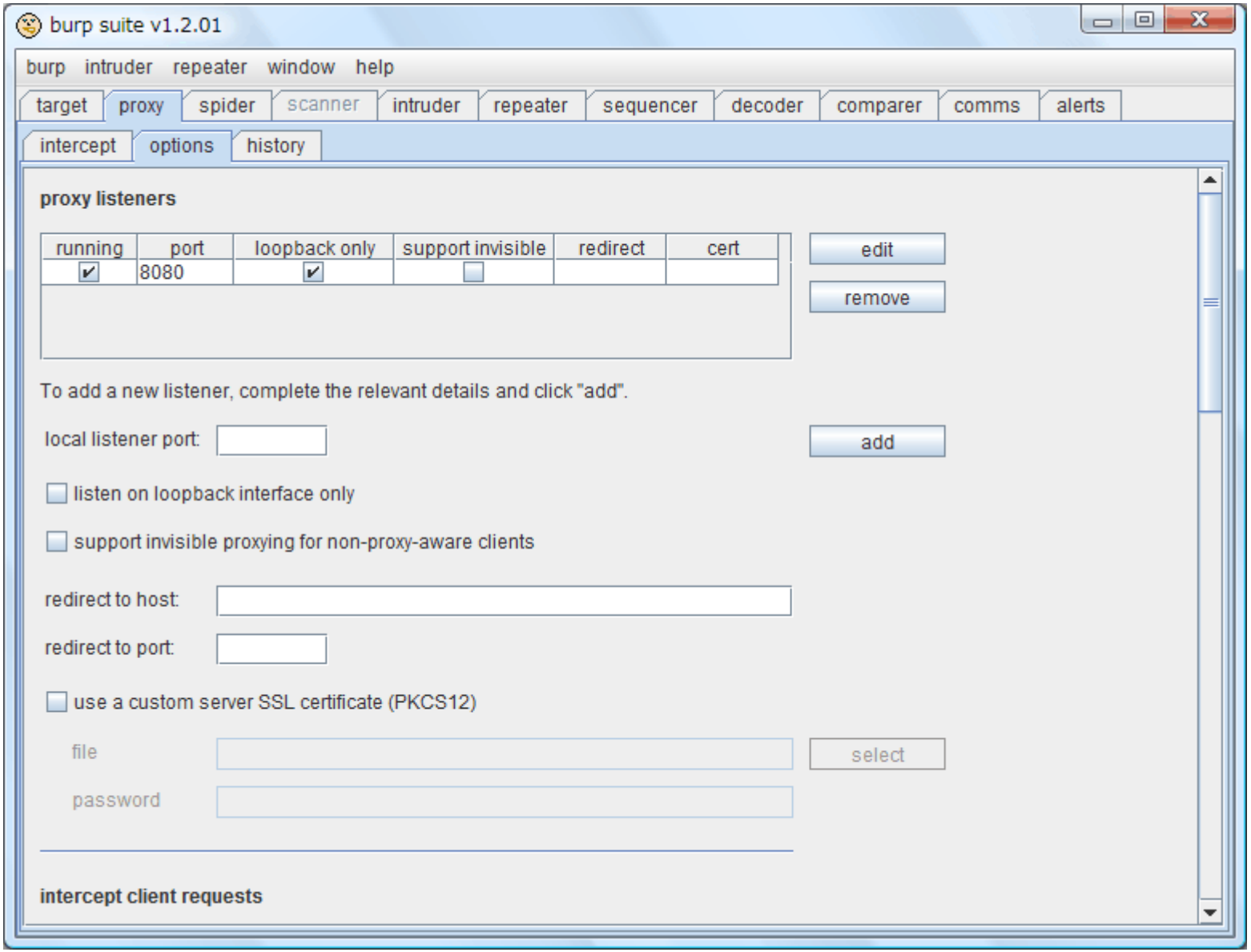
各診断項目における検出パターン及び脆弱性有無の判定基準は以下のとおり。なお、厳密な意味で言えば、本基準で判定される挙動は、「当該脆弱性がある可能性が高い」ということになる（必ず当該脆弱性があることを 100%保障はしない）。

（A） SQL インジェクション			
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）
1	「'」（シングルクォート）1 個	エラーになる	レスポンスに DBMS 等が出力するエラーメッセージ（例：SQLException、Query failed 等）が表示された場合にエラーが発生したと判定します。
2	「*検索キー*」と「*検索キー*'and'a'='a」の比較	*検索キー*のみと同じ結果になる	HTTP ステータスコードが一致し、かつレスポンスの diff（差分）が全体の 6%未満の場合、同一の結果と判定します。検査対象が検索機能の場合は、検索結果件数が同一の場合にも、同一の結果と判定します。
3	「*検索キー(数値)*」と「*検索キー* and 1=1」の比較	*検索キー*のみと同じ結果になる	同上

（B） クロスサイト・スクリプティング（XSS）			
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）
1	「'>"><hr>」	エスケープ等されずに出力される	レスポンスボディーに検査文字列の文字列がエスケープ等されずに出力されると脆弱と判定します。
2	「'>"><script>alert(document.cookie)</script>」	エスケープ等されずに出力される	同上
3	URL 中のファイル名として <script>alert(document.cookie)</script>	エスケープ等されずに出力される	同上。http://www.xxxx.jp/service/index.html という URL であった場合、「index.html」の部分に検査文字列をエンコードせずに挿入します。
4	javascript:alert(document.cookie);	href 属性等に出力される	レスポンスボディーの特定の URI 属性（src, action, background, href, content）や、JavaScript コード（location.href, location.replace）等に検査文字列が出力される場合、脆弱と判定します。

Copyright (C) 2009 HASH Consulting Corp.

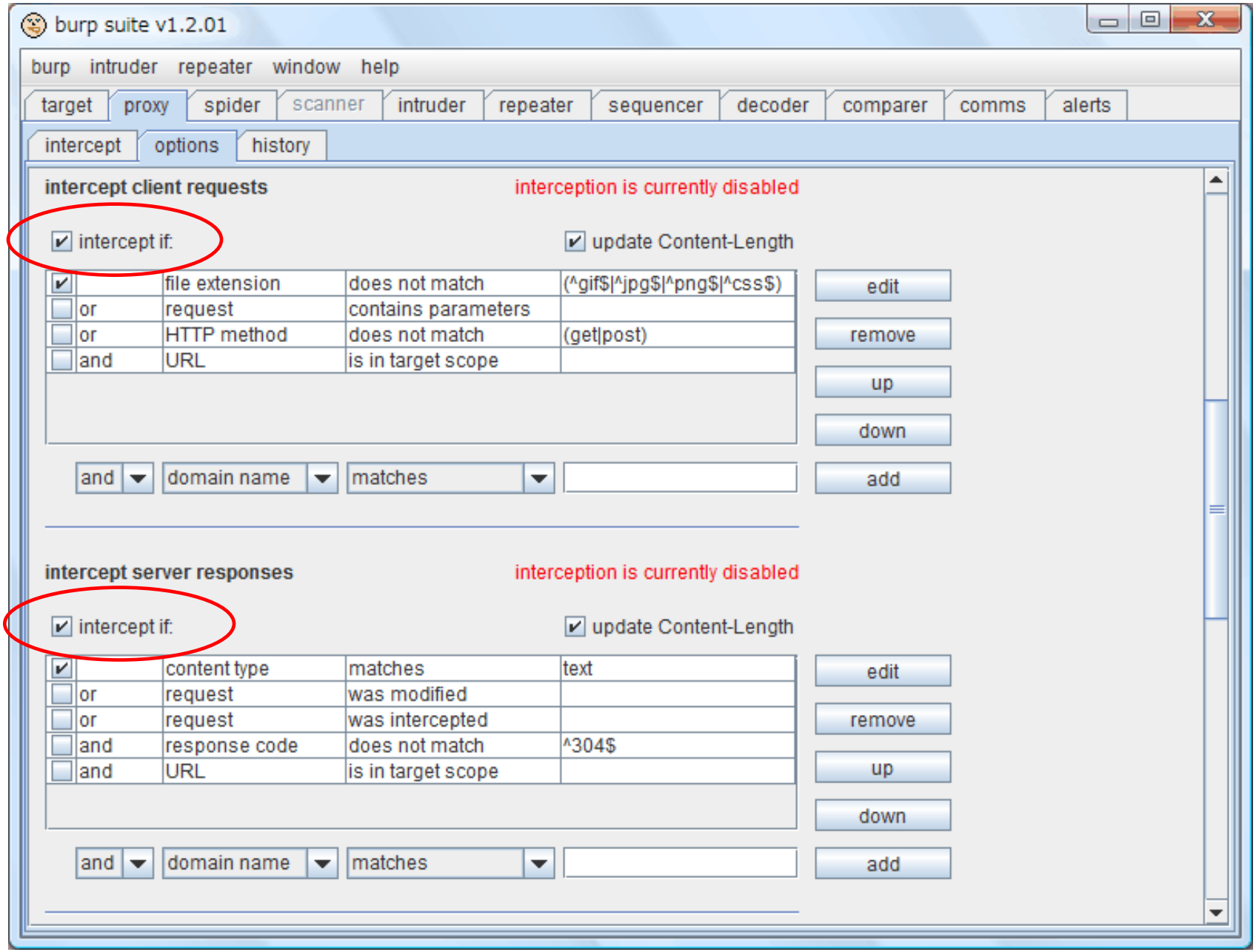
検査に必要なツールの例(burp suite)



http://www.portswigger.net/suite/

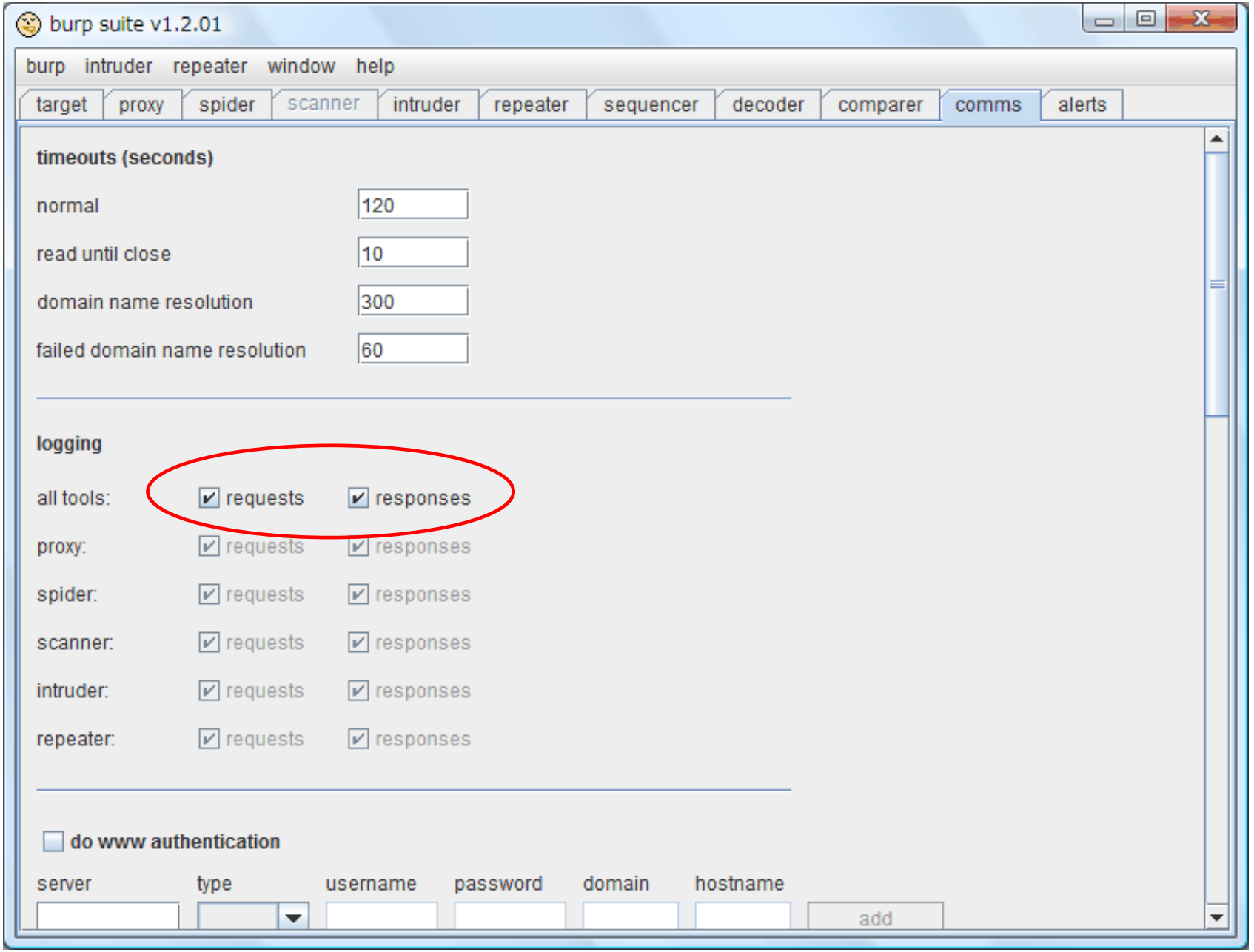
Copyright (C) 2009 HASH Consulting Corp.

burp suiteの設定(Intercept)



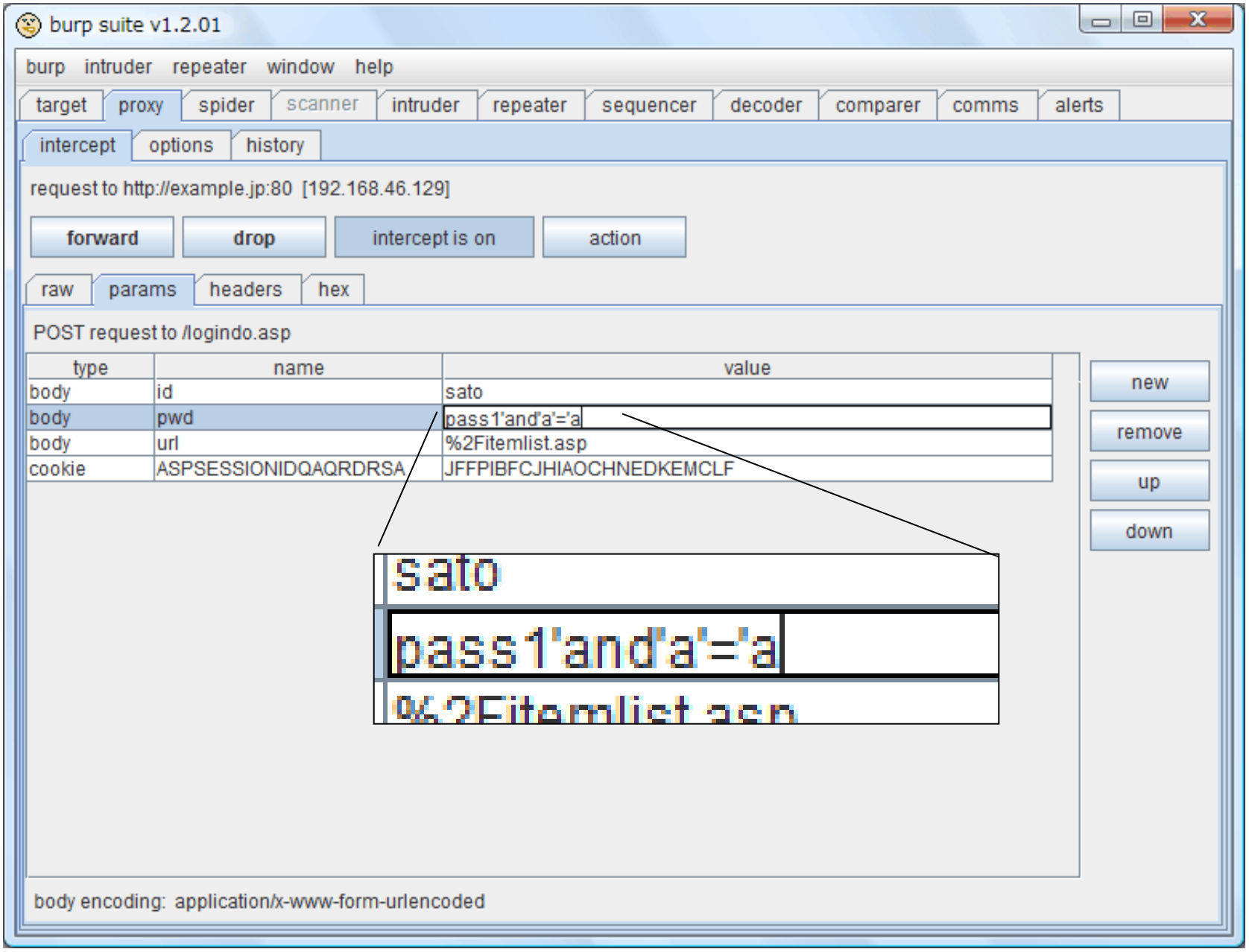
Copyright (C) 2009 HASH Consulting Corp.

burp Suite の設定（ログ取得）



Copyright (C) 2009 HASH Consulting Corp.

Intercept と検査パターンの入力



Copyright (C) 2009 HASH Consulting Corp.

デモ

テスト工程のコスト削減方法

- 専門家に全部頼むと高いので、できる部分は**自分でやる**
- 必ずしも全項目をテストする必要はない
- 明らかにテスト不要なもの
  - 外部コマンドを利用しない・・・OSコマンドインジェクションは不要
  - メール送信しない・・・メールヘッダインジェクションは不要
- ソースコード検査の方が効率がよいもの
  - OSコマンドインジェクション
  - パストラバーサル
  - SQLインジェクション(ソースコード検査しやすいように開発標準を定めておくと良い)
- セルフテスト工数を削減して浮いた費用で、専門家にも検査してもらうとなお可

Copyright (C) 2009 HASH Consulting Corp.

まとめ

- セキュアな発注方法論は発展途上であり、まだ業界標準といえる方法がない
- 要件について
  - セキュリティ要件とセキュリティバグに分けて考える
  - 資産洗い出し、脅威分析は定石だが、Webアプリの場合、うんと簡略化してよい
- セキュリティバグ対応は、開発標準整備とチームの教育が鍵
- テスト、検収について
  - おもなコスト要素はセキュリティテスト
  - セキュリティテストツールとしての「ウェブ健康診断仕様」
- 契約にも注意

Copyright (C) 2009 HASH Consulting Corp.

ご清聴ありがとうございました