セキュリティ教育方法の議論

展開実例紹介

RICOH
imagine. change.

株式会社リコー
リコーICT研究所 システム研究センター
S&S開発室 AC開発グループ
大平浩貴（おおひら こうき） CISSP-32515

セキュリティ教育方法の議論

RICOH
imagine. change.

- 組織のセキュリティは教育・啓蒙による展開がとても大切
- セキュリティに興味のない人、セキュリティ業務を嫌いな人にも受けれてもらえる教育を作成した
- このセッションの概要
  - その教育を紹介
  - そのような教育が許されるかどうか議論

背景

RICOH
imagine. change.

- おっさんになりました
- ここ最近思うこと
  - 他人の役に立ちたい
  - 会社の役に立ちたい
  - 社会の役に立ちたい
- 誰しもおっさんになると、そういうことを考えるらしい

みんなの「困りごと」を解決しよう！
セキュリティ屋としてみんなの役に立とう！

セキュリティの困りごとを解決する！

RICOH
imagine. change.

- 弊社は実はみんなセキュアであった
  - セキュリティ業務は全員行っている ／ 社内体制も整備されている
- あまり困っていない？
- セキュリティが嫌いな人もいる
  - セキュリティ対策ばかりでは自由な開発業務を妨げてしまう
  - 怖がらせようったって、だまされないぞ
  - まずはお客様に喜んでもらう機能をつくるのが大切、セキュリティは後回しに

世の中で一番怖い物は…

何とかしなきゃ

怖いもの知らず

何が必要？

RICOH
imagine. change.

- セキュリティの行動は充分
- セキュリティのマインドもっと身につけたい！
- マインドがあれば…
  - 現場の対応が高度化する
  - 想定外にも自律的に対応できる

「なぜ？」を知っていると強い

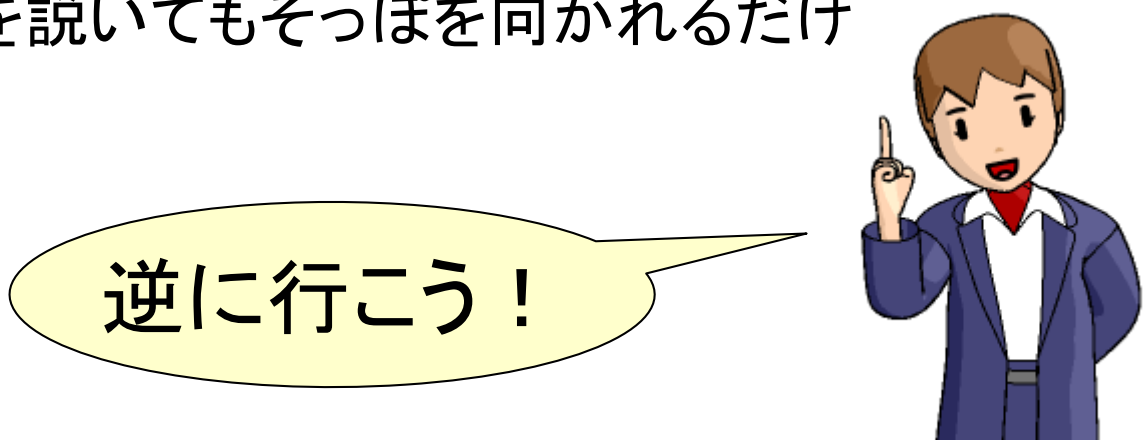
- セキュリティが嫌いな人は、セキュリティのマインドを持てない
  - 嫌いな物を理解するのは難しい

どうする？

発想を転換しよう

RICOH
imagine. change.

- セキュリティが嫌いな人は、痛い目にあったことのない人
  - 危険を説いてもそっぽを向かれるだけ



- **痛みを教えるのではなく、他人に痛みを与えることを教える**
- 簡単に攻撃できることを体感してもらう
  - さすがにみんな大人なので…
    - 自分が簡単に攻撃できることを知れば、誰でも自分を攻撃できることに気づく

攻撃だけ教えてもだめ

- 攻撃だけを教えると
  - 自分が何でもできる気になってしまう人もいる
- 攻撃は防御よりもリスキーな行為であることも教えよう
  - 違法であることもちゃんと教える

社内展開の結果

RICOH
imagine. change.

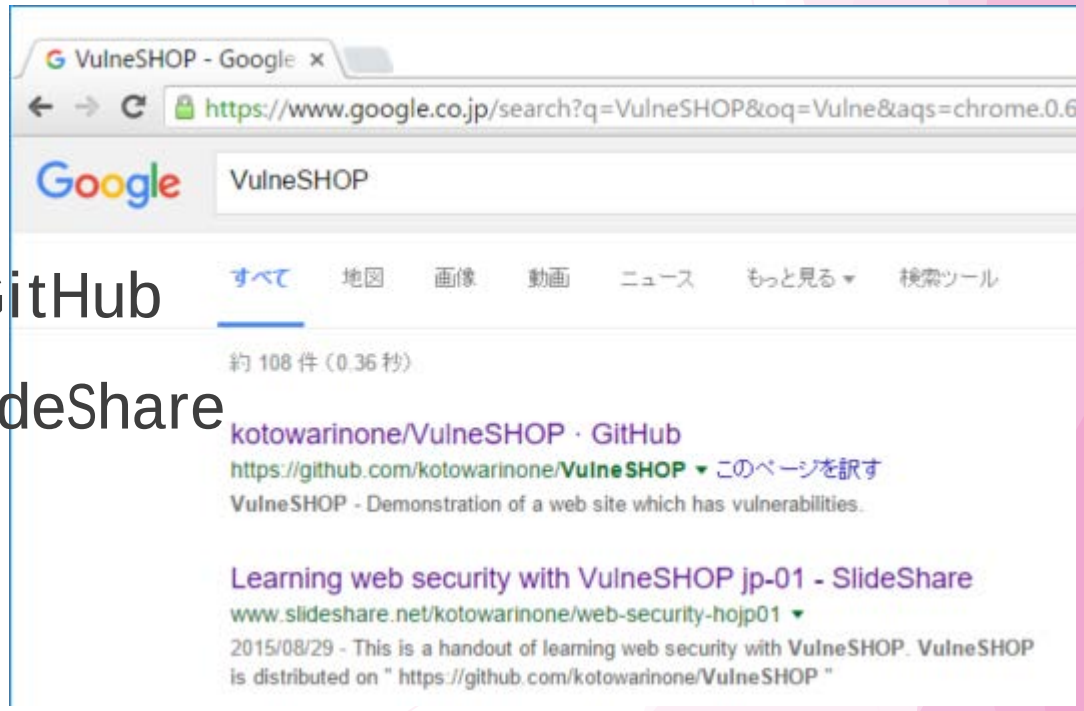
- 部署内展開
  - { 興味深かった:**9割** ， 普通だった:**1割**, 興味なかった:0% }
  - { 新しい知見だった:**4割**, 知っていたが一部新しい:**5割**, 知っていた:**1割**}
  - { 業務に役立つ:**9割**, どちらともいえない:**1割**, 役に立たない:0% }
  - どんな部分で役に立つ？
    - GUIをWebにしているので、気をつける
    - ユーザ登録やログアウトなどの怖さ
    - ネットワークに関わる以上無視できないと思った
    - etc...
  - そのほか
    - ハンズオンであることがよかった

VulneSHOPの紹介と議論

CISSP-322515
大平 浩貴（おおひら こうき）
kotowarinone@gmail.com
https://www.facebook.com/kohki.ohhira

VulneSHOPの概要

- セキュリティを啓蒙する
  - 他者への攻撃を教えることで、
    自分も同じ目にあう危険があることを理解させる
- マテリアルは二つ
  - Webサイト実現OSS@GitHub
  - 解説ハンドアウト@SlideShare
- VulneSHOPで検索を！



VulneSHOPを
とにかく試してみる

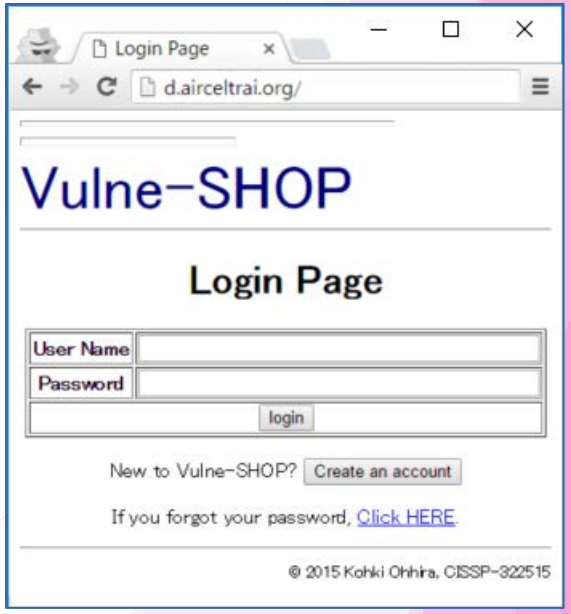
これから操作していただく事柄

以下はJANOG37で実施した
デモンストレーションの解説であり
URLなどはすでに無効となっております

- サイトへ接続
- サイトへログイン
- 攻撃
  - 攻撃例１：範囲外数値による異常な購買
  - 攻撃例２：SQLインジェクションによる不正ログイン

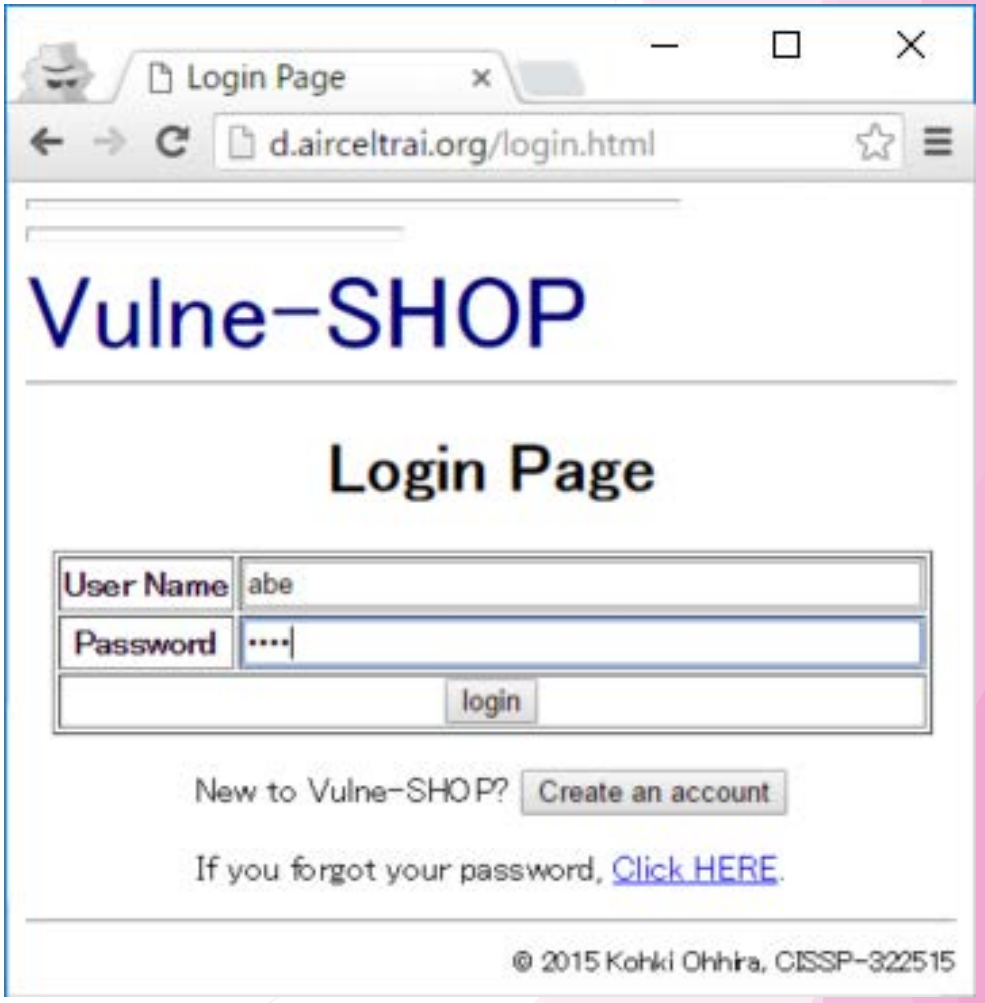
サイトへの接続

- VulneSHOPサーバに接続してください
  - ~~http://d.airceltrai.org/~~
  - ~~m4.xlarge@AWS東京リージョン~~
  - ブラウザは新しいものを推奨
    - 使用しているタグは基本的にHTML2.0レベル
    - パスワードはクライアントサイドでJavaScriptライブラリ（jsSHA）を使って不可視化（SHA256化）している
- 右記の ログインページを表示させてください



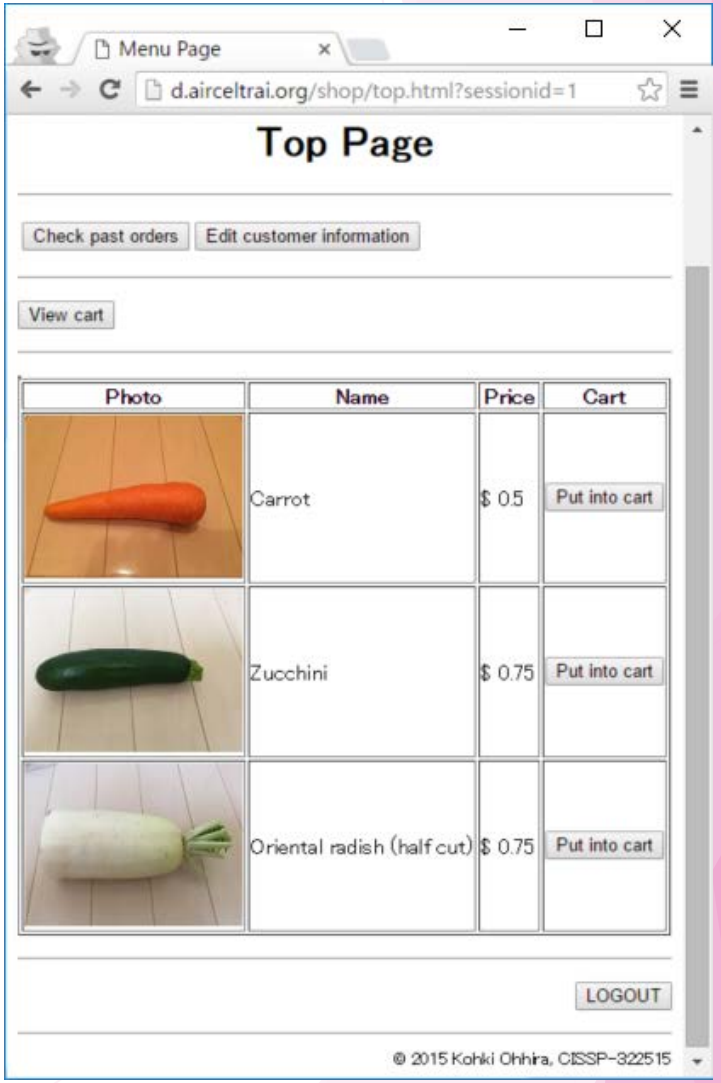
サイトへログイン

- 「Create an account」ボタンを押す
  - ユーザ名やパスワードなどを設定する
- ユーザ名つきでログインページが表示されるので、登録したパスワードを入力してログインする



トップページ

- 人参と、ズッキーニと、大根を売っている
- それぞれの右のボタンでカートに入れることができる
- カートの中を見たり、購入（チェックアウト）したり、購入履歴を見ることができる

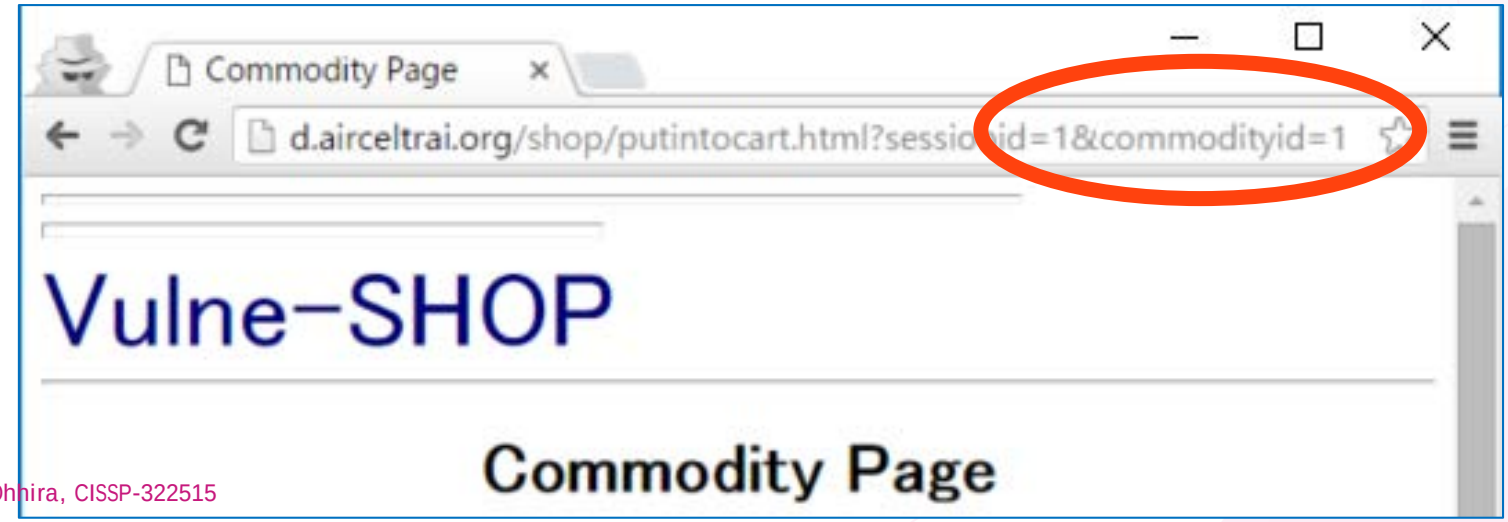


人参をカートに入れる
～ 攻撃のはじまり ～

- トップページでニンジンを「put into cart」する

攻撃のお試し１

- ニンジン・ズッキーニ・大根をカートに入れると…
  - それぞれ、putintocart.htmlに対してcommodityid=1~3が指定されている
  - では、commodityid=4の時は？
  - **URLを直接いじって試してみよう！**



東京スカイツリー

- 価格の $ 521,000,000 は総工費
  - JPYで650億円、レートは2015年8月の夏休み頃
- 何の話か分からない人は、commodityid=4でアクセスしてみよう
- わざわざ地下鉄乗り継いで、人が少ない早朝に撮影しに行ったら曇りだった

範囲外数値指定の危険性

- ユーザが使うことを前提としていないデータが使われる
  - 番兵（データ構造において、終端を示す特殊なデータ）
  - テスト用データ
  - オーバーフロー時に残存するごみデータ
- テストデータ・ごみデータがお客様に見えてしまう事故は多数起きている
  - 損失だけでなく、こじれて裁判にも発展しかねない
    - 価格が異常である
    - 付与ポイントやキャッシュバック額が異常

攻撃のお試し２：SQLインジェクションしてみよう

- ログアウトして、トップページへ
- ユーザ名とパスワードを使わずにログインする
- ユーザ認証時にDBアクセス言語（SQL）を使う
  - それの誤動作を引き起こして、強制的にログインします

ログイン時にSQL文が走行する

- ユーザアカウントはDBに記録されているので、下記のSQL文を実行する
  - unameとpassがユーザの入力

```
'SELECT userid FROM users WHERE username="'+uname+
 '" AND password="'+pass+'" ;'
```

- このクエリで1行発見できれば認証成功、0行なら認証失敗
- ユーザ入力例

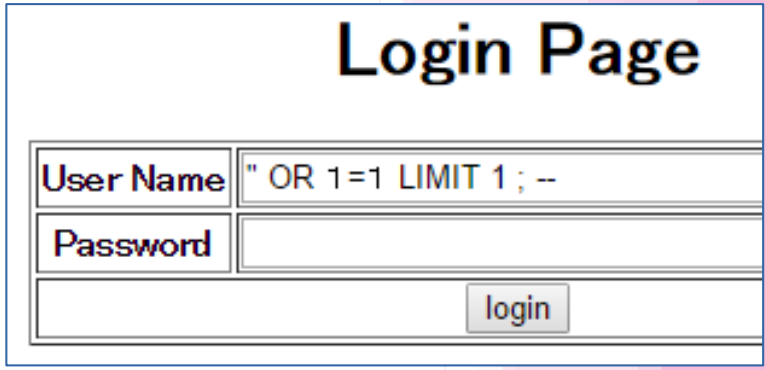
```
uname=abe
pass=abf3123··········ea3
```

```
'SELECT userid FROM users WHERE username=“abe"
   AND password="abf3123··········ea3" ;'
```

SQLインジェクションしてみよう

- では、ユーザの入力がこんな時は？

```
uname=" OR 1=1 LIMIT 1 ; --
pass=
```



-- の後ろに空白があるのを忘れずに

- SQL文はこうなる

```
'SELECT userid FROM users WHERE username="" OR
 1=1 LIMIT 1 ; -- " AND password="" ;'
```

- 常に成立する条件となる
- 成立行は LIMIT修飾子で1行に制限している
- -- 以降はコメント行になる

以上で攻撃教育のデモは
完了です

VulneSHOPは攻撃を教えるOSS

知らなかった or
知識だけで体験したことがなかった
↓
実際にインジェクションした

- 未経験者から、経験者に転換する
  - プログラムを作ったことのないプログラマはだめ
- 危機感や勘所を知り、自発的に対応できる

- 攻撃手段を教えることの危険もある

意見交換と議論のお願い

セキュリティ教育として
攻撃を教えることの良し悪しを
どう見るか

相談１
攻撃を教えることはアリ？ナシ？

- 質問１： セキュリティ啓蒙のために攻撃を教えるのは良いと思うか？
  - A. あらゆる攻撃を**教えるべきではない**
  - B. 攻撃を教えてもよいが、**知識に留めて行為は避ける**べき
  - C. **今回の程度の攻撃なら**教えてもよい
    - 基本的な運用で容易く防護される攻撃
  - D. **何を教えてもよい**、防御を高度化すべきである

挙手・コメントください！

回答A/B
おしえるべきでない / 知識にとどめるべき

- 教育はしない
  - 人材を望む方向に育てないで良い？

- 教育は防衛手段教育にとどめ、経験させない
  - 教えたことにより、正しい行動（手段）はできる
  - 本質の理解は類推に頼らざるを得ない
  - 類推できない人は放置？

コメントください！

回答C
今回の程度の攻撃実用性なら許せる？

- では一体、どの辺に閾値がある？
  a. 今回程度ならOK ？
  b. 応用攻撃もOK？
     - 掲示板や、偽HTMLメール/Webで水飲み場へ誘導するなど
  c. さらに危うい手法も教えてOK？
     - Torとか、Wi-Fi対応Hardware Key Loggerとかは?
  d. 攻撃戦略まで教えてOK？
- ほかに許される基準は？

挙手・コメントください！

回答D
何を教えてもよい、技術はそうして育つ

- 原理主義的
  - 黎明期のインターネットはそうだった
- 今のインターネットは社会インフラになりつつある
  - 一般にインフラは質を担保するために法律で縛られる
  - 誰でも使えるように、悪用できないように
- 黎明期のフロンティアスピリッツは残したい！
  - フロンティアスピリッツはイノベーションの源泉だ！
  - フロンティアスピリッツを残すにはどうしたらよいか？
    - だれもがイノベーションに加担できるように、優しく、気持ちよく、楽しくナレッジ展開したい（私見）

コメントください！

ISOC-JPでの反応

- アンケート結果
  - 今回程度の攻撃ならOK→8割
  - 何を教えてもOK→2割
- 意見（一部）
  - 「教えてよい内容」は「教える理由」によって異なる
    - プログラマに対する教育なら必ずOKだろう
    - では、VulneSHOPのような、組織内の底上げは？
  - この内容を高校生に教えられるか？
    - 自分で生活に直結するお金を稼いでいる人ならOKでは
  - 同時に行う道徳・倫理教育をしっかり
  - 法律も教えよう

本質を知らないとわからないこと

- GIZMODOさんの面白い記事
  - http://gizmodo.com/5498412/sql-injection-license-plate-hopes-to-foil-euro-traffic-cameras
- 一目見てこの面白さがわかる？
  - 今日VulneSHOPを体験した人ならわかる
    - 「あー、DROP DATABASE してるわー」
  - 「入力を関数に通しなさい（サニタイズしなさい)」「ORM使いなさい」とだけ教えられている人はわからない
- 想定外の事態の実例である
  - 想定外に対応できるようになるのがよいのでは？

教える人の選択は重要かも

- 犯罪を犯しても困らない人、積極的に犯す人がいる
  - DQNとかChavとかだけでなく、社会的序列を問わず

- 攻撃を伝えてよいのは誰？
  - **利他的行動**をとれる人に提供する
  - **法律に従わないと受ける損失が大きい**人に提供する
    - ISOC-JPで語られた「自分で働いてお金を稼いでいる人」はその例と考えられる
  - できれば社会的序列にとらわれたくない

参考情報１：法律面 1/3

- 不正アクセス行為の禁止等に関する法律（平成11年128号）
  - 無許可者による権限昇格なども含まれそう（素人の私見）
- 刑法
  - （幇助）
    第六十二条 正犯を幇助した者は、従犯とする
- VulneSHOPは犯罪幇助に該当するか？
  - …こわいよ

参考情報１：法律面 2/3

- 似た活動はある
- IPAさんのAppGoat / SECCONさんの活動など
  - 彼らは法執行機関の支援を得ているよう
  - 法執行機関に相談するときの参考になりそう
- 目的・運用次第？
  - AppGoatも、繰り返し悪用するなと伝えている
- 現在、方針検討中
  - 良い方法や、良いつてがあれば、情報ください！

参考情報１：法律面 3/3

- 自分でもいろいろ調査中
- **ICT jp Law** Wikiを構築中
  - http://wikiwiki.jp/ictjplaw/
  - ICT関連の法律リンク

- ICT jp Lawも弁護士法に抵触しないように注意
  - 一歩間違えると法に触れかねない
  - いずれ有資格者の確認を得たい

参考情報２：倫理・道徳面

- 道徳単体はあまり語られない
  - **利他的行動**をとることなどが含まれる
  - 倫理の一部（個人の社会的な責務）として語られる
  - 現実には**社会的序列に根差す**ことも多い
- 入手できる情報倫理は良いが表層に終始
  - **反社会的行動の禁忌** / 知財保護 / マナー / 利用の節度など
- ICT活動における利他的行動の検討は面白そう
  - 倫理は時代によって変わるので注意

参考情報３：国際化に関わる問題

- 言語的な問題（グローバライズ）
  - 英語化は必須
    - 通訳やってる女房のおかげでどうにか達成
- 各国法規対応（ローカライズ）
  - 個人としての活動なので簡単ではない
  - 各国の団体に相談して、その伝で法執行機関に相談するしかない？
  - 価値を高めれば相談に乗ってくれる国際組織はある？
    - *NIC とか、ISOCとか、…？

まとめ

長時間おつきあいくださり ありがとうございました

- 元の目的
  - セキュリティに興味のない人にセキュリティを伝えたい
  - 痛みを教えるのではなく、痛みを与える方法を教える
    - 痛みを知らない人はこの方が理解しやすい
- 議論
  - 攻撃を教えるのはよいか？
  - 程度は？
  - ガバナンス・法・倫理は？

私見ですが…

- 世の中には
  - 持たない方がいいものもある（銃とかナイフとか）
  - 知らない方がいい情報もある
- 知ったからには、責任が必要
  - 強者こそ自制が求められる
  - 少なくともICTセキュリティ分野にはその理想がある
  - 「諸君、だから私はICTセキュリティが好きだ！」
- まぁ、VulneSHOPはそんなに大上段に構えるようなレベルの攻撃でもないですけどね
  - 今後は大上段に近づきたい

もしよろしければ、使ってみてくださいね

- VulneSHOPの配布場所
  - VulneSHOPでググれば出てきます
    - OSS https://github.com/kotowarinone/VulneSHOP
    - 日本語解説 http://www.slideshare.net/kotowarinone/web-security-hojp01
    - 英語解説 http://www.slideshare.net/kotowarinone/easy-introduction-of-web-security
- 社内教育などで使ってくださったらうれしいです
- 役務になりますが、講演/解説のご要望にも対応できます
  - 英語での講演はフリーランス通訳（うちの女房）も付けられます
- でも、みなさんご自身で活用すればもちろん無料！

謝辞

- IAjapan IPv6 ディプロイメント委員会のみなさん
  - 藤崎 智宏さま、 新 善文さま
- IPv6 普及高度化推進協議会 共存WG アプリv6化SWGのみなさん
  - 波田野 裕一さま、渡辺 露文さま
- 株式会社リコーのみなさん
- ISOC-JPのみなさん
- **JANOG参加のみなさん・Committeeのみなさん**
- うちの女房
  - 大平 有さま

ありがとうございました

- 大平 浩貴（おおひら こうき）
- CISSP-322515
- kotowarinone@gmail.com
- https://www.facebook.com/kohki.ohhira

参考資料
予備資料

相談２：あなたが社内教育チーフだとして攻撃を従業員に教える？

- VulneSHOP程度の攻撃を教えたい？
  - 確実に技術の底上げになる
  - しかし、いたずらをできる人は確実に増加する
- もっと高度な攻撃も教えたい？
  - 軍隊と同様で、メンバーは強い方がよい
- 攻撃を教えるのは避けたい？
  - 社外への攻撃など、従業員の不要な技術が高まりすぎるとアンコントローラブルになる可能性が高い
  - 倫理教育が必要だが、そのメソッドが確立していない

挙手・コメントください！

VulneSHOPの概要

VulneSHOPサイト OSSの機能

- 機能
  - ECサイトの真似事
    - ユーザアカウント登録
    - ログイン
    - 商品三つを販売
    - 商品を複数個カートに投入・保持
    - カートの中身を購入
    - 購入履歴確認
    - ユーザアカウント編集
    - ログアウト
    - パスワード忘れ対応
- 保有脆弱性
  - サニタイズなし
    - 入力のHTML表示
    - 入力のSQL実行
    - 入力のOSコマンド実行
  - 暗号化なし
    - ただしパスワードはブラウザが不可視化する
  - セッションID推測可能
    - 単調増加の整数値
  - 商品はシーケンシャルなIDで指定
  - ブラウザ→サーバ伝送は全てGETを使用
  - エラーメッセージで不要情報提示

VulneSHOP OSS構成

- 配布
  - https://github.com/kotowarinone/VulneSHOP
  - MITライセンス
- 実行環境
  - Node.js （サーバサイドJavaScript実行環境）
    - Express （Node.js用Webサイトフレームワーク）
      - レンダラはEJSを採用
  - jsSHA （Brian Turek 氏によるJSライブラリ）
  - MySQL （データ記憶用RDMBS）
  - Mailコマンド
    - 昔からあるmailコマンド
  - OSはUNIXライクOSを前提

解説ハンドアウトの内容

- コンテンツ
  - 日本語版＆英語版@SlideShare
    - VulneSHOPで検索してください
  - 2015年12月31日現在、Ver. 1.5
- 内容
  - （実習）VulneSHOPサイトの正常な使い方
  - （実習）VulneSHOPサイトへの攻撃方法と防御
    - 非公開情報の参照
    - SQLインジェクション
    - セッションハイジャック
    - OSコマンドインジェクション
  - （解説）そのほかの攻撃
  - （解説）2015年最近のWebセキュリティ解説

先行ソリューション

先行ソリューション

- AppGoat
  - 脆弱性に触れることができる
- IPAさんによるソリューション
- 一人で自習できる
- 多彩な脆弱性に対応
  - XSS / SQL injection / XSRF / OS command injection / Directory traversal / HTTP header injection / その他認証不備 / Session hijack / Error message 放置
- プログラムの脆弱性修正までサンドボックスで教える

VulneSHOPとAppGoatとの違い

- 攻撃させることで理解を促進することは同じ
- 目的が違う
- AppGoat：プログラマに対するセキュリティ教育
  - 大切なことをたくさん教える
  - 独習可能
  - 完成されている
- VulneSHOP：非プログラマも対象で興味を引く
  - セキュリティ嫌いにセキュリティを教える
    - 苦手意識を取り除くことが第一目標
  - 独習よりも教師による教育が基本
    - 道徳教育が必須なので、自動化しないほうがよいと判断
  - 教育の改変・活用は自由自在
    - OSSであり、解析・改変・活用OK