Webサービスのセキュリティ維持向上について

啓蒙の案とその議論

CISSP-322515
株式会社リコー
大平浩貴（おおひら こうき）

本日のお題：セキュリティ啓蒙の方策と議論

- セキュリティの向上は大切
  - セキュリティでは特に教育・啓蒙による展開がとても大切
- どのようにセキュリティを向上しようか？

- 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提案したい
  - 最近はセキュリティも流行っていますが、以前はそりゃぁひどいもので
    - 飲み屋の親父モード

- 本日のプレゼン
  - その教育を紹介…VulneSHOPというものを作ってみました
  - そのような教育が許されるかどうか議論
  - セキュリティの教育がどうあるべきか議論

セキュリティ体感型ハンズオンOSS

VulneSHOPのご紹介

RICOH
imagine. change.

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
CISSP-322515

概要

RICOH
imagine. change.

- プライベートでOSSを作りました
- セキュリティが嫌いな人にセキュリティを教えるシステムです
- 自分の会社内に展開しました
  - うまくいった感じです
- もしよければみんなも使ってください

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る
  - 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
  - セキュリティ対策は自由な開発業務の妨げだと思う
  - 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
  - 緊急時に対応できる

「なぜ？」を知っていると強い

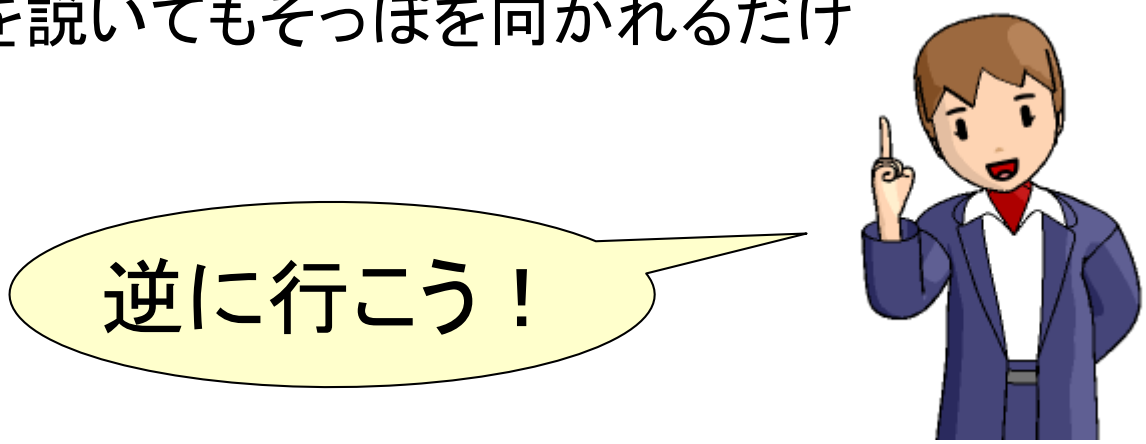
- セキュリティが嫌いな人は、セキュリティのマインドを持てない
  - 嫌いな物を理解するのは難しい
  - ピーマン嫌いにピーマンのおいしさを理解させたい

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:約1割，興味なかった:なし }
  - { 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:なし}
  - どんな部分で役に立つ？
    - GUIをWebにしているので、これから気をつける
    - 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
- これから教育範囲を広げていきます！
  - FacebookにOSSを載せたら、自社の知り合いから引き合いが…(w

触っていただけたら、とても幸いです

RICOH
imagine. change.

- OSSソース
  - https://github.com/kotowarinone/VulneSHOP
- ハンドアウト
  - 日本語：http://www.slideshare.net/kotowarinone/web-security-hojp01
  - 英語：　鋭意作成中
- ご興味のある方はどうぞ
  - ご利用いただけますとすごく嬉しいです

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
  - ユーザに攻撃してもらうための脆弱Webサイト
- 解説ハンドアウト
  - 日本語版：公開中
  - 英語版：鋭意作成中

VulneSHOPサイト 実現OSS

- 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
    - 単調増加のスカラー値
  - 商品はシーケンシャルなIDで指定
  - formメソッドは全てGETを使用

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

- （実験）VulneSHOPサイトの正常な使い方
- （実験）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

解説ハンドアウトの配布

- 配布元
  - 日本語
    - http://www.slideshare.net/kotowarinone/web-security-hojp01
  - 英語
    - 鋭意作成中
- ページ数とプレゼン所要時間
  - 実験・ハンズオン：45分～1時間
    - 40ページほど
  - 解説：（端折って30分）～50分
    - 30ページほど

類似ソリューション

- IPAのAppGoatと類似
  - AppGoatはとても高度
- 当該VulneSHOPと比べた AppGoatの特徴
  - 一人で自習できる
    - 脆弱性Webサイトを運用する担当者が不要
  - 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できる
- VulneSHOPとの違いは後で言及

VulneSHOPにおける攻撃教育の実際

紹介の準備

- Wi-Fiに接続
  - SSID: Vulne52G（5.2GHz） / Vulne24G （2.4GHz）
  - パスワード：password
  - IPアドレス等はDHCPにより配布
- VulneSHOPサイトに接続
  - http://192.168.2.2/
  - 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
    - ただし、ユーザが誤って実運用しているパスワードを入力してしまう事故に対応するため、JavaScriptライブラリ（jsSHA）を使って不可視化（SHA256化）している
    - →新しいブラウザを推奨

操作する事柄

- ユーザに依頼する具体的な操作
  - formのinputコントロールへ入力する
  - URL部のGETメソッドの値を書き換える
- スマートフォン・タブレットでも攻撃可能
  - iPhoneなどはGETの文字の書き換えが若干面倒
    - ただし、GETの入力文字数は数文字なので、あまり手間をかけさせない

紹介体験 1/4：サイトを普通に使う

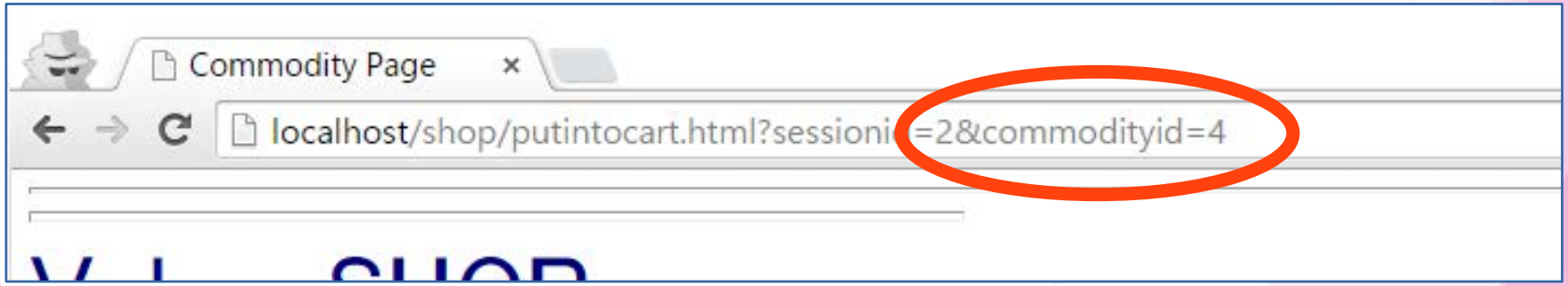
VulneSHOPの利用

1. ログインページの参照
2. 自分のアカウントの作成
3. 自分のアカウントでログイン
4. 購買を試す
   - 商品をカートに入れる / チェックアウトする / 履歴を見る
5. 自分のアカウント変更を確認する
6. ログアウトする
7. パスワードをリセットする

紹介体験 2/4 ：
非公開情報を参照する

商品のIDを確認しよう

- URLに注意しつつ、ニンジン・ズッキーニ・大根をカートに入れてみよう
  - それぞれ、putintocart.htmlに対してcommodityid=1~3が指定されている
- じゃぁ、commodityid=4の時は？
- 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
  - 何？この謎写真

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 / 付与ポイント / キャッシュバック額が異常
  - 最近はテストデータを本番環境で扱うことも流行している
    - 評価設計しっかり
- その他、IDの推測不可能化なども提案

紹介体験 3/4 ： SQLインジェクションでログインする

ログイン時にSQL文が走行する

- ログインでは、ユーザアカウントを確認する
- ユーザアカウントはDBに記録されており、その参照には下記のSQL文が実行される
  - 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
- 動作例

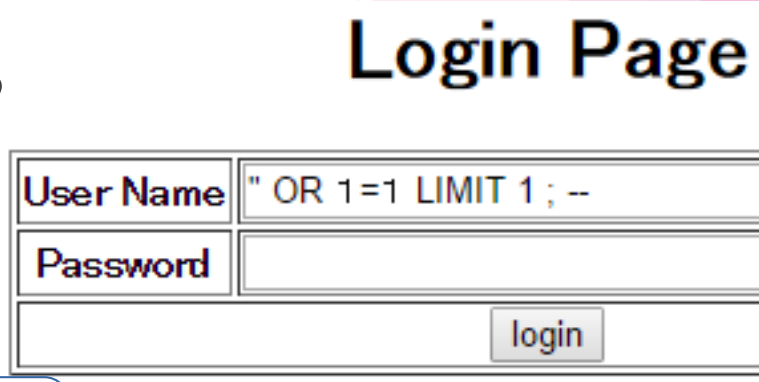
```
uname=user
pass=abf3123··········ea3
```

```
'SELECT userid FROM users WHERE username="user"
   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 ; --
hashedpass=
```



-- 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="01ba747…" ;'
```

- 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

SQLインジェクション対策の解説

- 最良の対策として、O/R Mapper（ORMとも）を提案
  - 言語で参照する「O:オブジェクト」と「R:リレーショナルデータベース」とをルールに従って自動的に連結する
  - オブジェクト～DBのデータの交換を自動化するので変なDB操作は混入しない
  - 計算機資源の消費と交換に検索操作を自動化する
- サニタイズについても言及
  - 適切なサニタイズを、適切なタイミングで
  - いつサニタイズするかも言及

紹介体験 4/4 ： ハンズオンのまとめ

Web攻撃ハンズオンの犯罪活用

- ご理解のとおり、現実の攻撃はこんなに簡単じゃない
  - TLSで暗号化されている
  - GETメソッドを使用しない
  - 操作がログに残っている可能性が高い
    - 特にGETメソッドでSQLインジェクションを行った場合、初期状態で、URLがそのままサーバログに残る
- 法執行機関の対策も素晴らしい
  - 法律で刑事罰を与えることがしっかりと明記されている
    - 「不正アクセス行為の禁止等に関する法律」
  - 攻撃者は自分のIPアドレスを残せない
    - 警察はログに残ったIPアドレスと時刻から回線を特定できる
  - 容疑があれば、警察は当然仕事をする
    - 当然被疑者のPCは押収されてフォレンジックへ
    - 余罪が出てくることも

攻めるよりも守ることが安全である

- 攻撃を補助するものが世に蔓延している
  - ボットネット・脆弱性放置のホスト/ルータ/AP/その他
- しかし、このハンズオンで攻撃の難しさも理解して頂けたと思う
  - 攻撃者が痕跡を残さずに深く長く攻撃するのは薄氷をふむような行為
  - 攻撃者が嫌がるようなサイト・サービスにしよう
  - 攻撃者が嫌がるようなログを取ろう
- 法治国家において、攻撃はものすごくリスクが高い行為
  - ちょっとしたミスで、攻撃者は犯罪捜査の対象となる
  - くだらないイタズラで人生を失いたくない人は攻撃すべきでない

自分がターゲットにならないために

- 今googleでloginという文字を検索したら、3,470,000,000件引っかかった
  - 今回説明した攻撃に対して脆弱なサイトは必ずあるだろう
  - 攻撃できるものを攻撃するというポリシーの攻撃者も多い
- 自分のサイトが攻撃対象にならないように
- ミスや手抜きの組み合わせで、リスクは指数関数的に増大する
  - 手間を惜しむと簡単にセキュリティホールができてしまう
- また、そういう脆弱サイトに無為に触れないように
  - 攻撃なんてもってのほか
  - ハニーポットや攻撃研究家、脅迫に使われることも

他のソリューションとの違い

先行ソリューション

- AppGoat

- 天下のIPAさま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 1/2

- 攻撃させることで理解を促進することは同じ
- 基本方針が違う
- 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
  - セキュリティ嫌いにセキュリティを教える
    - 興味を引くことが第一目標
  - 独習よりも教師による教育が基本
  - 教育の改変・活用は自由自在
    - OSSであり、解析・改変・活用OK

VulneSHOPとAppGoatとの違い 2/2

- AppGoatは、多少きびしく教育
- 例：SQLインジェクションの教育
  1. あれれ、SQLの比較文いじっているのにうまくできない…
  2. 実はそのサイトはパスワード欄が空っぽだとエラーを出す仕様でした
  - な…なんか実践的？

- VulneSHOPの基本的方針とは異なる
  - AppGoatはちゃんと答えさせる
  - VulneSHOPは答えを教えて、興味を引くのが主たる流れ

紹介体験のまとめ

攻撃を教えること

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

- この差はものすごく大きい
  - 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に仕事はできない
  - 経験によって危機感が増す
- しかし、攻撃を教えることの是非もある
  - 攻撃はリスキー、防御は安全であることも教える

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

これまでのまとめ

- VulneSHOPという OSSとハンドアウトを作った
- Webサイトの簡単な攻撃を教えるもの
  - セキュリティに興味を持たせる
  - セキュリティ上のリスクを~~教える~~知覚させる
  - セキュリティの実体験を積ませる
    - プログラミング実体験のないプログラマに何ができるのか？
    - セキュリティ対策プログラミングも同様ではないか？

ご参加の皆さんにお願い

- このOSS/ハンドアウトに対する心象を教えて頂きたいです
  - そして議論したいです

- 攻撃を教えてよいのか？
  - 悪意のある人が / 今は悪意がなくても将来攻撃したくなった人が活用するのではないか？
  - 「この程度の技術なら教えても良い？」
    - だとしたら、どの程度から先が危うい？

質問１の基本
Webサイトへの攻撃を教える理由

- 教えたい理由
  - セキュリティに興味を持たないのは痛みを知らないから
    - まともに言っても理解してもらえない
    - 他人に痛みを与えることを教えて、自分の危機を知ってもらう
  - 具体的な行為を経験することで、応用が効くから
    - プログラミングしたことのないプログラマはダメ
    - 敵に何をされるのか、なぜサニタイズするのかを理解してほしい
- 教えるべきでない理由
  - 悪用できる
  - 悪事のための技術習得のきっかけになる

質問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. **今回の程度の実攻撃活用可能性なら**教えてもよい
    - 暗号化、ログ改竄防御を回避できない程度
  - D. **何を教えてもよい**、防御を高度化すべきである
  - E. その他

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

- 教育は防衛手段にとどめ、経験させない
  - 教えたことにより、正しい行動はとれる
- 「どのように攻撃されるか」の理解は類推に頼る
  - 類推できる人とできない人が生じる
  - 類推できない人は事態に対応できない
    - 自分で類推できない人は切り捨てるべき？
    - 自分で類推できない人こそ教育すべき？
  - 組織力を向上するために教育する？ / 切り捨てる？
    - セキュリティ嫌いでもモノづくりや組織運営がうまかったりする
    - セキュリティは直接儲けにつながらない会社が多くて立場が逆だったりする…

コメントください！

例：本当に教えなくてよいのか？

- GIZMODOさんの面白い記事
  - http://gizmodo.com/5498412/sql-injection-license-plate-hopes-to-foil-euro-traffic-cameras
- この面白さがわかる？
  - 今日VulneSHOPを体験した人ならわかる
    - 「あ、DROP DATABASE してる」
  - 「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
- この記事は想定外の事態の実例ではないか？
  - ルールの想定外の事象にも対処できた方がよいのでは？

コメントください！

余談
公平性に欠けるが教える人の選択は有効かも

- 攻撃＝犯罪
  - 犯罪を犯して困らない人と困る人がいる
- 弁護士になりたい人は犯罪を犯さない
  - 罰金刑になると資格喪失
- 医師も、会計士も、一流企業勤務も、貴重な職を失いたくない

- 犯罪を犯さない、合理的理由がある人だけに教えるというのは一つの手段
  - 会社の教育でも、管理職に教えることの一部は一般職には秘密にしている
  - いささか選民的で残念だが

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？

- 攻撃実用性がさほど高くない
  - サニタイズなし、暗号化なし
  - ECサイト運営にあたって、これらへの対応はDue Careだろう
- では一体、どの辺に閾値がある？
  a. 今回程度ならOK ？
  b. 今回攻撃の応用もOK？
     - メールや偽Webを応用した水飲み場への誘導
  c. 具体的に活用可能な脆弱性・攻撃インフラも教えてOK？
     - TorやHKLが普通になるのは苦しそう
  d. 攻撃戦略と手順まで教えて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・モヒカン主義的
  - 黎明期のインターネットはそうして育った
- しかし、今のインターネットは社会インフラに成長した
  - 黎明期の常識は適用しにくい
  - インフラは質を担保するために法律で縛られることになる
    - 例：放送/電話/電波/電気/水など
  - 今の総務省のインターネット扱いはナイスバランスだと思う
- でも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？
    - 絶妙な加減の自由と規制 / 自主自立主義 / 標準化は個人に付託？ / ヘテロジニアスな環境
    - 水道で新ビジネスは出にくい…違いは？

コメントください！

質問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！

参考情報１：法律面 1/2

- 不正アクセス行為の禁止等に関する法律
  - 不許可者による権限昇格など、今回の説明が含まれている
    - インジェクションでコマンド実行とか、あきらかに抵触
- 刑法(2015年10月現在)
  - （幇助）
    第六十二条 正犯を幇助した者は、従犯とする
  - VulneSHOPは幇助に該当するか？
- …こわいよ

参考情報１：法律面 2/2

- IPAさんのAppGoat / SECCONさんの活動など
  - 先人を参考にする？
    - 彼らは法執行機関のパトロネージを得ているよう
    - 法執行機関に相談するときの参考になりそう
  - 結局運用次第なのか
    - AppGoatも、頑張って丁寧に悪用するなと伝えている
  - 現在、相談する法執行機関の選定と、そのための情報収集をしている状況
    - 良いつてがあれば、情報ください！

参考情報２：倫理面

- 情報倫理の今ある資料は一般ユーザ向けに終始
  - 知財保護 / コミュニケーションマナー / 法規遵守 / 自主保護 など
  - いい資料はありませんか？
- 社会倫理・技術倫理の拡張は有効かも
  - 例：強者が弱者を蹂躙してはならない理由
  - 全体最適ではない
    - 社会が維持できない
  - 多様性が失われる
    - 強者で社会を形成するのは特定資産だけで資産形成するようなもの
  - 強弱の指標がない
    - 自動車に乗った人がか弱い子供を殺してよいわけではない

参考情報３：国際化に関わる問題

- 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ISOCは相談に乗ってくれる？
- 言語的な問題（グローバライズ）
  - 英語化は必須
  - EN/JP→各国は有志が居るかも…居たらうれしいなぁ…

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

- 振り返り
- 元々のお題
  - 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）
  - …だから、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
  - 日本の法律は素晴らしく、うまくフォローしてくれている
  - 強者こそ遵守が求められる倫理
    - ホワイトハッカー…などという言葉が出てくるようになった
- 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

日本は最近どう？

- 日本のICT分野はブラック企業のイメージがひどい
  - 大学などの高等教育では情報科が不人気という話もある
- 子供が触れるICTであるゲームも、ソフトウェア販売からコンテンツ販売へ移行
  - ICT技術の裾野が広がりにくい
- セキュリティは最近話題だが、特定領域に終始
  - 各種情報漏えい事件
  - マイナンバー対応など
- あるべき姿は？
  - 法・倫理を守る（他人を食い物にしない）、技術を大切にする、技術の価値を守る
  - **なんだ、セキュリティって、メインストリームじゃないか！**

謝辞

- IAjapan IPv6 ディプロイメント委員会の皆様
  - 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の皆様
  - 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
  - 東 義一さま、田村 博さま
- **ISOC-JPのみなさん**
  - **橘 俊男さま、本日ご協力・ご参加くださったみなさん**
- うちの女房
  - 大平 有さま

もしよろしければ、使ってみてくださいね

- VulneSHOPの配布場所
  - 解説 http://www.slideshare.net/kotowarinone/web-security-hojp01
  - OSS https://github.com/kotowarinone/VulneSHOP
- 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、高品質フリーランス通訳（うちの女房）も付けられます
- でも、ご自身で活用すればもちろん無料

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