セコム IS研究所
Intelligent Systems Laboratory

XSS + CSRF解説編

JPNIC・JPCERT/CC
セキュリティセミナー2005
「Webのセキュリティ」

2005年10月6日

セコム IS研究所 新井 幹也

Webアプリケーション脆弱性 多発する事件報道

セコムIS研究所 Intelligent Systems Laboratory

SQLインジェクション？

2005/1～2005/6にかけて、某人材派遣会社、人材派遣登録の個人情報61,876件が不正アクセスにより流出の可能性。氏名、住所、電話番号、生年月日、メールアドレスなど。

2005/05/25ごろ、女性向けWebサイトにて不正アクセス。Webページの改ざんを受ける。これによりサイトを閲覧したユーザがウィルスに感染される。なお、顧客情報の漏洩はなかった。

2005/03ごろ、某旅行会社のWebサイトにて不正アクセス。最大約9万300名の会員ID、パスワード、氏名、住所、電話番号、携帯番号、FAX番号などの情報が流出した可能性。

CSRF

ソーシャルネットワークサイト「mixi」にてURLをクリックすると、勝手に「ぼくはまちちゃん！」というタイトルのコンテンツがアップロードされる現象が発生。

XSS？

2004/11ごろ、Yahooを騙ったフィッシングメールがYahooユーザに届く。メール中のリンクをクリックして表示されたページはアドレスバーはYahooであるが、表示されているコンテンツは他ドメインのものであった。どうやらXSSの脆弱性をついたものらしい。

Webアプリケーション脆弱性 国内の状況

セコムIS研究所 Intelligent Systems Laboratory

脆弱性情報届出機関IPA

ソフトウエア製品脆弱性関連情報

例 :OS, ブラウザ、Webサーバなど

Webアプリケーション脆弱性関連情報

サイト固有のサービス

→ **四半期ごとに統計情報を公開**

Webアプリケーションでは…

XSSがトップ

- 46%(全265件)
- 意外と見つけやすい？
- で、もう一度おさらい

CSRFって？

- 最近報告があった
- 事件も発生で話題
- さて、どんなもの？

参考　IPA(独立行政法人 情報処理推進機構)
脆弱性関連情報の取り扱い :http://www.ipa.go.jp/security/vuln/index.html

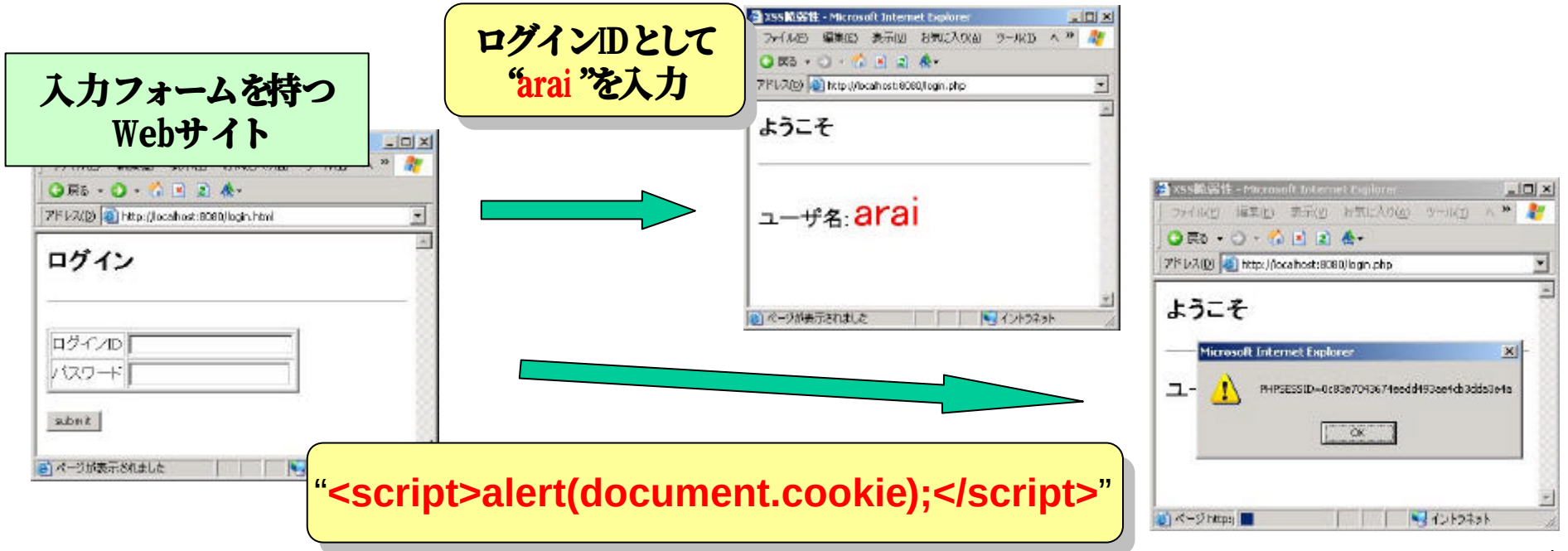
Webアプリケーション脆弱性 XSS :基礎

セコムIS研究所 Intelligent Systems Laboratory

クロスサイトスクリプティング（XSS）とは

動的にWebページを生成するシステムのセキュリティ上の不備を意図的に利用し、サイト間を横断して悪意のあるスクリプトを実行することである。これによりクレジットカード番号やパスワードなどの個人情報が第三者に流出する可能性がある。」

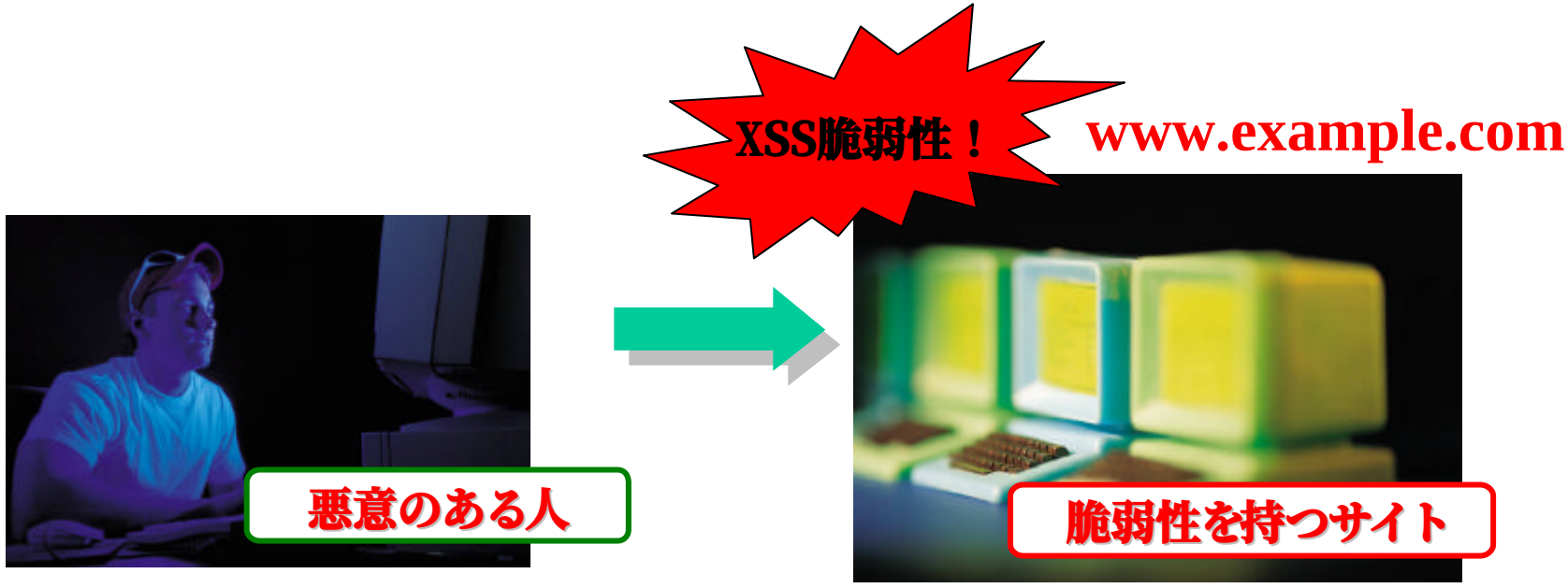
Wikipediaより



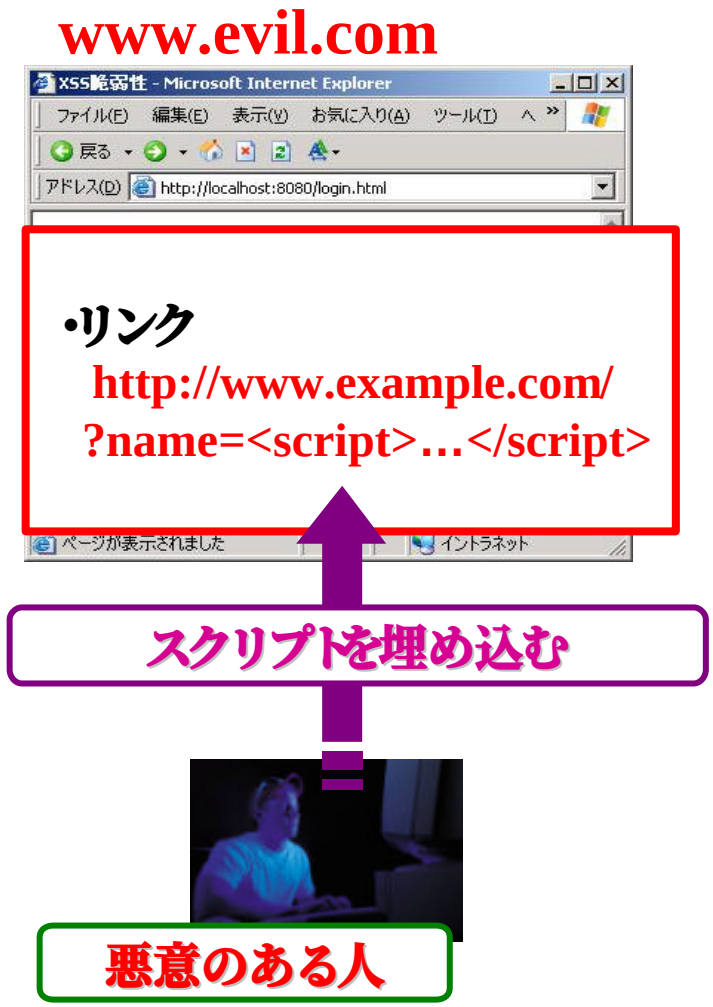
Webアプリケーション脆弱性 XSS :仕組み (1)

セコムIS研究所 Intelligent Systems Laboratory

- 悪意のある人、クロスサイトスクリプティング（XSS）脆弱性を持つサイトを発見



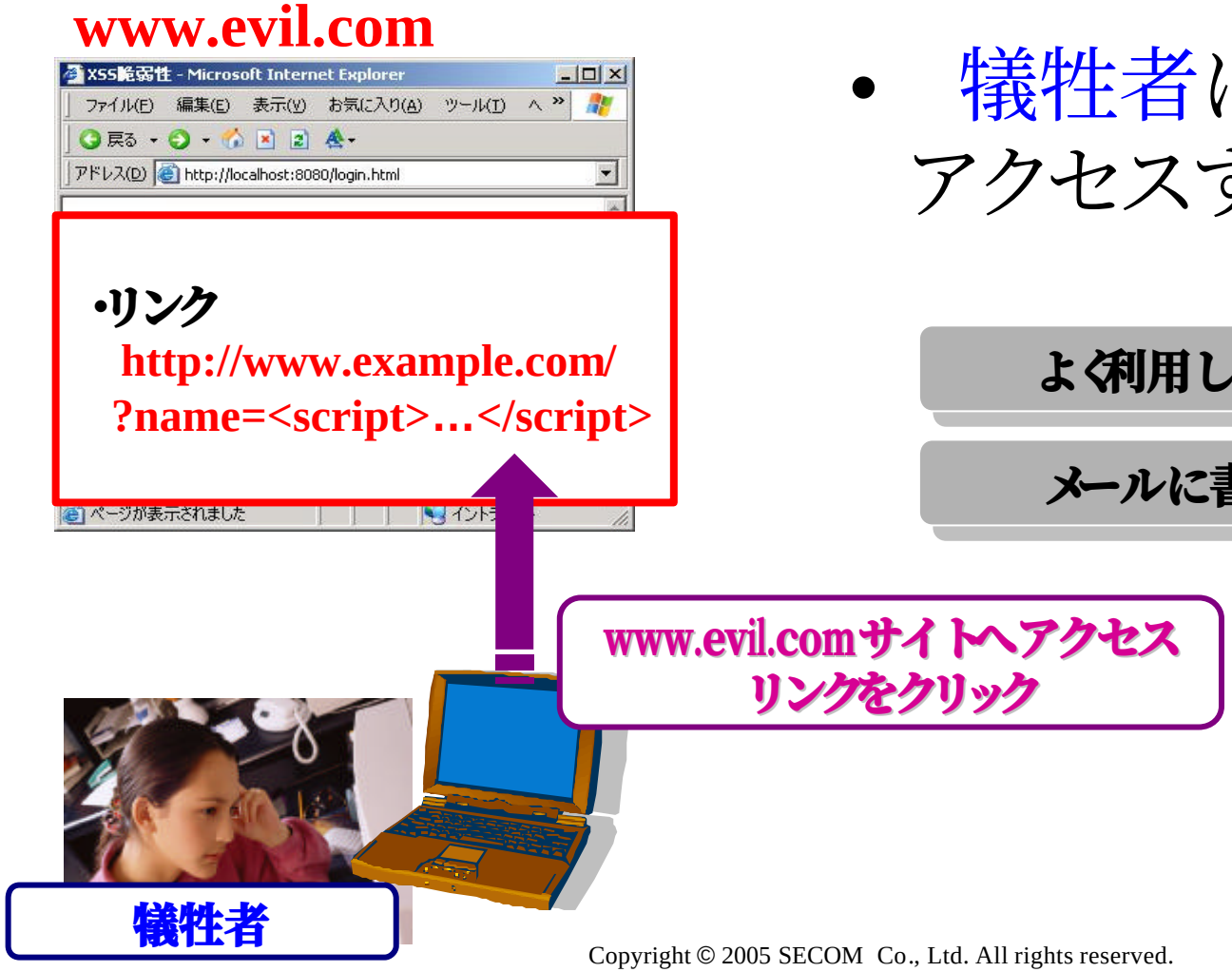
Webアプリケーション脆弱性 XSS :仕組み ⑵



- 悪意のある人、脆弱サイトへのスクリプトを埋め込んだURLを用意
  - 悪意のある人がWebサイトに記述
    - 自前サイト
    - 公開掲示板
  - メールにURLを貼り、配布

Webアプリケーション脆弱性 XSS :仕組み (3)

セコムIS研究所 Intelligent Systems Laboratory



- 犠牲者は、知らずにアクセスする。

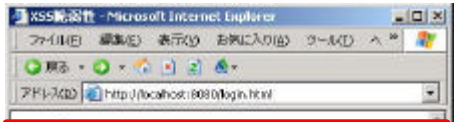
よく利用している公開掲示板

メールに書かれていたURL

Webアプリケーション脆弱性 XSS :仕組み ⑷

セコムIS研究所 Intelligent Systems Laboratory

www.evil.com



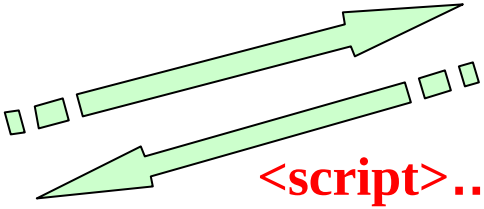
・リンク
http://www.example.com/
?name=<script>…</script>

XSS脆弱性！

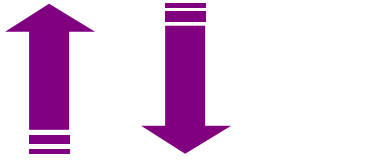
www.example.com

脆弱性を持つサイト

http://www.example.com/
?name=<script>…</script>



<script>…</script>を
含んだコンテンツ



被害者

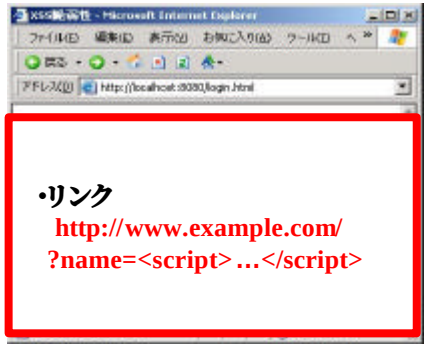
- 犠牲者が気付かない内に、脆弱サイトのスクリプトが、犠牲者PC上で実行される

これがクロスサイトスクリプティング

Webアプリケーション脆弱性
XSS :リスク

セコムIS研究所
Intelligent Systems Laboratory

www.evil.com



・リンク
http://www.example.com/
?name=<script>…</script>

XSS脆弱性！

www.example.com

Webサイト書き換え

Webサイト書き換えにより、
犠牲者の混乱・金銭被害、
脆弱サイト運営側のブランドイメージ侵害
などが発生

Cookie漏えい

犠牲者が、脆弱サイトの利用者であった場合など、脆弱サイトにおける犠牲者のクッキーが悪意のある人に漏えいする

ID、パスワード、セッション番号・・・

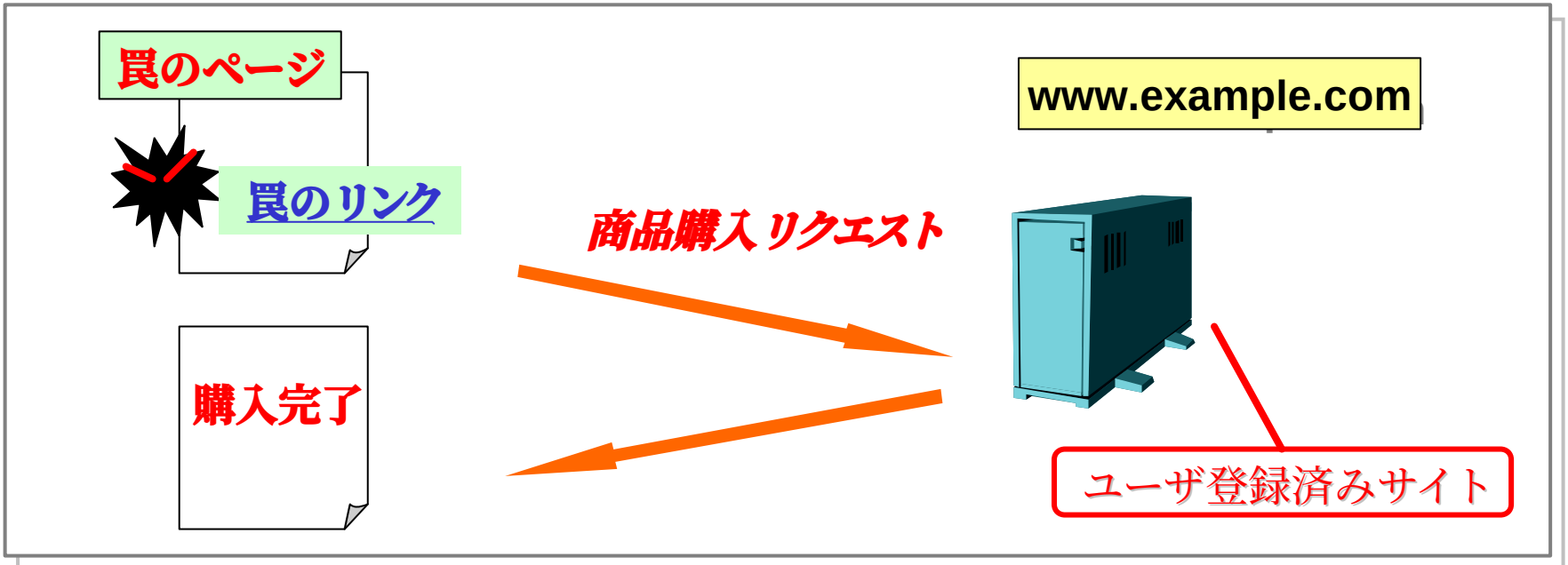
Webアプリケーション脆弱性 CSRF

セコムIS研究所 Intelligent Systems Laboratory

クロスサイトリクエストフォージェリ（CSRF）とは

「ユーザを罠のページに誘導することで、そのユーザが登録済みのサイトにひそかにアクセスさせ、登録情報の変更や商品の購入をさせることができる」

IPAより



Webアプリケーション脆弱性 CSRF :仕組み

セコムIS研究所 Intelligent Systems Laboratory

前提条件

- セッションの管理方法、リクエストの組み立て方法が予測可能
  - 対象アプリケーションを利用できるのならばこれは難しくない
- ログイン認証にCookieやBasic認証
  - 認証後は自動送信される

Webアプリケーション脆弱性 CSRF :攻撃例

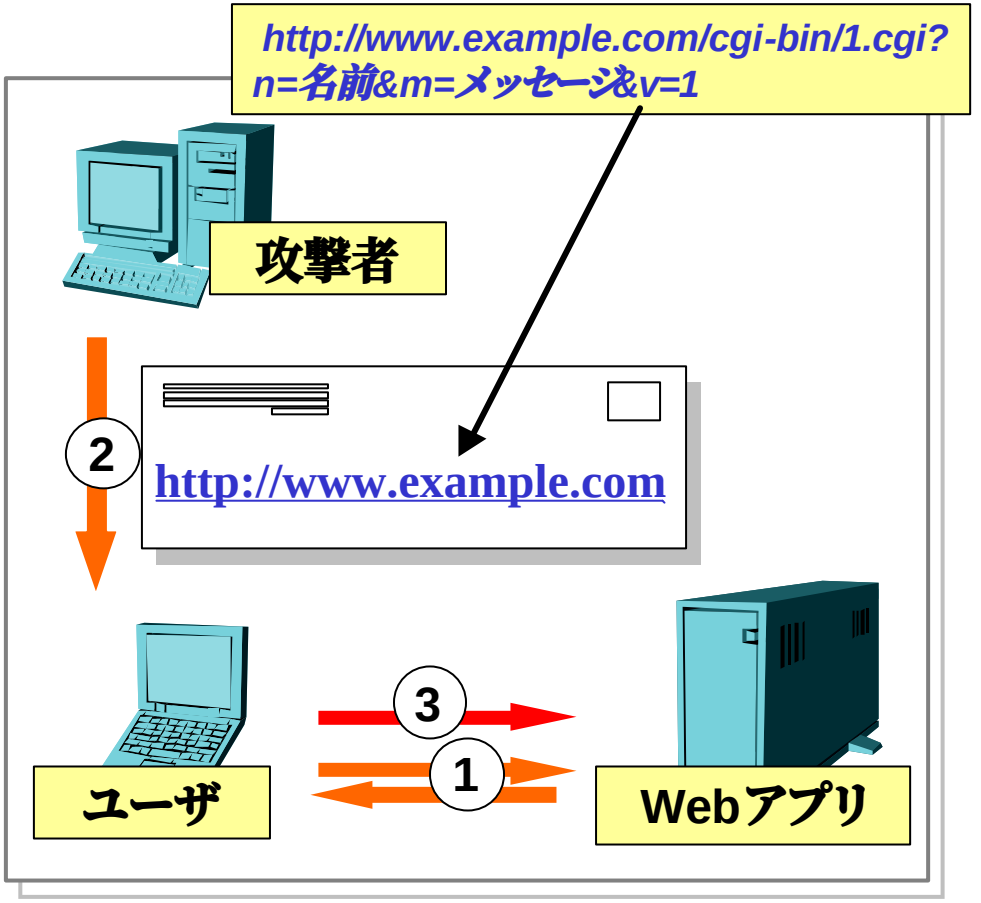
セコムIS研究所 Intelligent Systems Laboratory

条件

- セッション管理が予測可能である
- リクエストの組み立て方法が予測可能である
- ログインのあるWebアプリケーションにおいて、ユーザが既にログインしている

手順

1. 既にユーザはWebアプリにログインしている
2. 悪意のあるURLにより、望まない処理を強制的に発生
3. 悪意のあるURLにより、望まない処理を強制的に発生



Webアプリケーション脆弱性 CSRF :攻撃例(巧妙なわな)

セコムIS研究所 Intelligent Systems Laboratory

IMGタグ

- HTMLコンテンツを開くと同時にリクエスト送信
  - •<IMG SRC="***http://www.example.com/cgi-bin/1.cgi?n=名前&m=メッセージ&v=1***">
- 必ずしも画像ファイルをSRCに指定する必要はない
- Cookieも同時に送信される

JavaScriptの悪用

- ページを表示した瞬間にリクエストを発信
  - •<body onLoad="…;" >

ターゲットサイトへリンクを仕込む

- 悪意のあるリンクをターゲットとなるサイトへ仕込む
  - •Webメール、掲示板への投稿など

Webアプリケーション脆弱性 CSRF :リスク

セコムIS研究所 Intelligent Systems Laboratory

機能がそのまま悪用

- 設定の変更
  - パスワードなど
- メール送信
  - Webメールサイトがスパムメール送信の踏み台とされる？
- ショッピングサイト
  - カートの中に買うつもりのないものが…

Webサーバのログの観点からは…

リクエストはあくまで正規のユーザから発している
リクエスト自体も正常なものと変わらない

正規のユーザの正規なリクエストとしてログが残る
送信元IPアドレスも正規ユーザのPC
ログに残される値に不正な文字はない
(XSSやSQLインジェクションなどと違う)

Webアプリケーション脆弱性 CSRF :事例(1)

セコムIS研究所 Intelligent Systems Laboratory

mixi はまちちゃん

代表的なソーシャルネットワーキングサイトmixiにおいて、URLをクリックすると勝手に「ぼくはまちちゃん！」というタイトルでユーザの日記がアップされてしまう。

いくつかのバージョン

Ver.4にも存在？
（http://simon.tmn.net/wiki/index.php?mixi%2F%A4%DC%A4%AF%A4%CF%A4%DE%A4%C1%A4%C1%A4%E3%A4%F3%A1%AA）

○ Ver.2
　－URLに日記のアップを行わせる記述が直接記載。5時間たらずで400人に被害との情報も。
○ Ver.3
　－専用の攻撃ページを用意、攻撃ページではJavaScriptを用いて自動的にフォームを送信
　－Googleのリダイレクト機能を利用し、Googleの検索結果に見せかけて外部のURLを踏ませる

その他多くのサービス

＊一例です

tDiary

http://slashdot.jp/article.pl?sid=05/07/21/0115221&topic=91

はてなダイアリー

http://d.hatena.ne.jp/hatenadiary/20050715/1121427904

Movable Type

http://bakera.jp/hatomaru.aspx/ebi/topic/2038

Webアプリケーション脆弱性 CSRF :事例(2)

セコムIS研究所 Intelligent Systems Laboratory

Serendipity

○PHPで作成されたBlogサイト構築用のソフトウェア
http://www.s9y.org/

バージョン0.8.4以前にCSRF脆弱性

○2005/09/29にFull-Disclosure、Bugtraqにて公開
[Full-disclosure] Serendipity: Account Hijacking / CSRFVulnerability

○Ver 0.8.5 にて修正
情報公開は修正された後に行われたようだ

問題点

○罠のページを開くことで、ログインしているユーザのユーザ名とパスワードが変更されてしまう

○結果として成りすましが可能となる