JPNIC・JPCERT/CCセキュリティセミナー2004

Webの脆弱性

2004年10月4日

中央大学 研究開発機構 専任研究員

塩月誠人<shio@st.rim.or.jp>

はじめに

- 本セッションは、Webシステムにまつわる脆弱性とはどういったものなのか、どういう危険性があるのか、またどのような対策が必要とされるのかについて、Webサービスおよび Webアプリケーションレイヤにターゲットを絞り、網羅的に解説するものである。
- そもそも脆弱性を考える上で重要なのは、脆弱性の要因となる「脅威」（あるいは「攻撃手法」）を理解することである。そのため、ここではWASC（Web Application Security Consortium）が今年の7月に発行した「Web Security Threat Classification」という技術文書をベースに、認証、承認、クライアントサイド・アタック、コマンド実行、情報取得、ロジカル・アタックという大分類に沿ってWebシステムに関する一般的脅威を体系的に述べ、同時にそれぞれの脅威がどのような場合に脆弱性へとつながるかを説明する。
- 今回は時間の関係で、各々のトピックについて深くは掘り下げず、極力全体を網羅する方向でまとめているため、詳細については参考URLの各文献を参照していただきたい。

脆弱である」とは…?

- ドアに鍵がかかっていない家は、はたして脆弱か?

  → It depends!
  - 脅威（ドロボー）」が存在しなければ脆弱でない
- ピッキング対策を施した鍵は、はたして脆弱か?

  → It depends!
  - 「ピッキング」という脅威に対しては脆弱でない
  - しかし、他の脅威に対しては?
  - 「カム送り」は?
  - 「サムターン回し」は?
- 脆弱であるかどうか」を知るためには 脅威（攻撃者、攻撃の手口）」を知ることが重要

脅威、脆弱性、リスク、対策

- 脆弱な鍵は即座に取り替えるべきか?

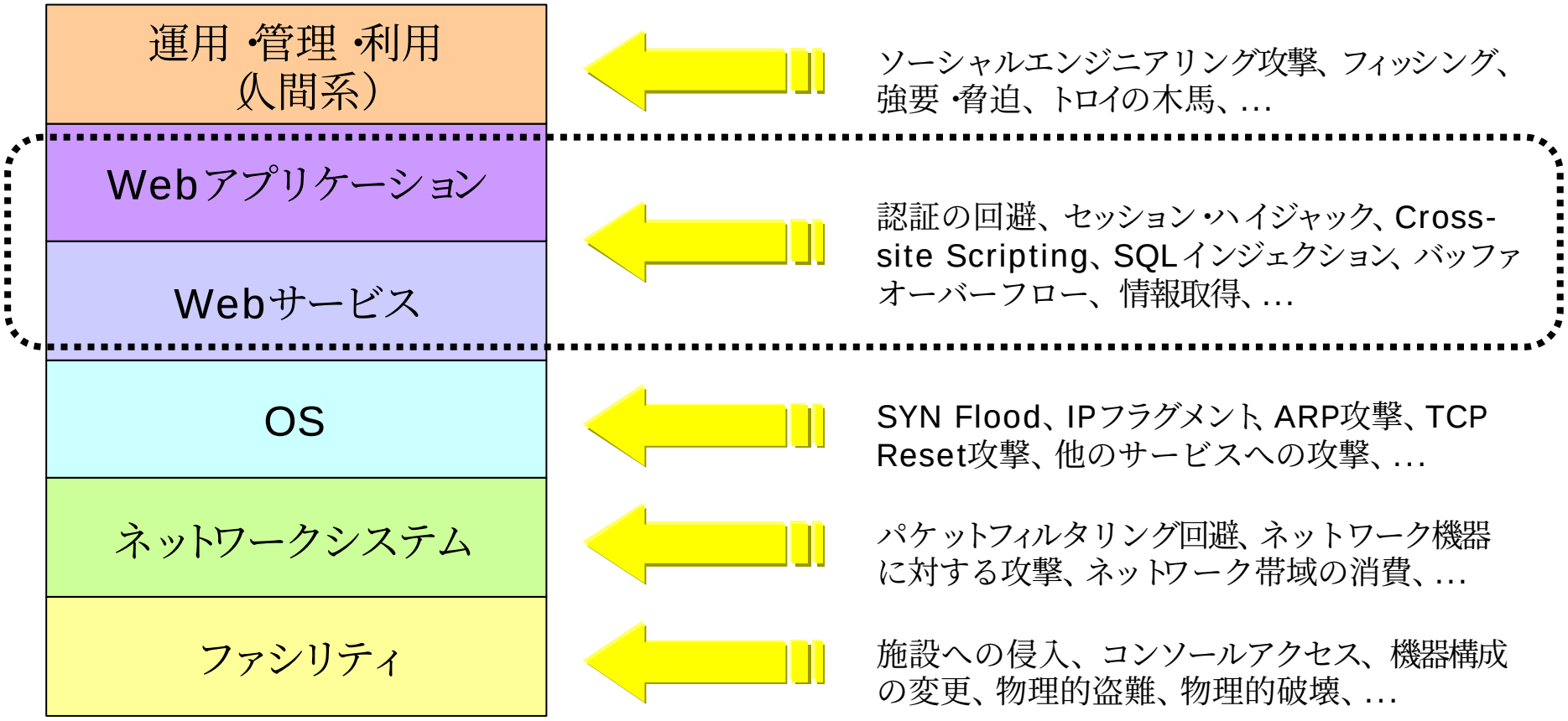
  → It depends!

  - 脅威の実現可能性（解錠の難易度）
  - 脅威の流行状況（手口の普及度、同様手口の犯行傾向）
  - 脅威による被害の大きさ（物理的損失、精神的ダメージ）
  - 他の対策状況（二重ロック、監視カメラ、警報装置、「猛犬注意」のシール、…）

- リスク（どれだけ「ヤバイ」か）を検討して対策を判断

  - 脅威（攻撃者、攻撃の手口）を知る
  - 世の中の状況を知る
  - 自己の状況を知る
  - 鍵を交換する事が必ずしも最適な解決策とは限らない

Webシステムのレイヤ構造と脅威



Webにおける脅威の分類

- 認証
  - ブルートフォース
  - 認証設定の不備
  - パスワードリカバリの不備
- 承認
  - セッションIDの推測
  - アクセス制御の不備
  - セッション終了処理の不備
  - セッション・フィクセイション
- クライアントサイド・アタック
  - コンテンツ・スプーフィング
  - クロスサイト・スクリプティング
- コマンド実行
  - バッファオーバーフロー
  - フォーマットストリング・アタック
  - LDAPインジェクション
  - OSコマンド実行
  - SQLインジェクション
  - SSIインジェクション
  - XPathインジェクション
- 情報取得
  - ディレクトリ内容表示
  - 情報漏洩
  - パス・トラバーサル
  - リソース位置の推測
- ロジカル・アタック
  - 機能の悪用
  - サービス妨害
  - 自動アクセス防止の不備
  - プロセスフロー管理の不備
- その他
  - HTTPレスポンス・スプリッティング
  - Webフィンガープリンティング

（「WASC Web Security Threat Classification」より）

認証（Authentication）

- 認証 … ユーザがそのユーザであることを確認する行為

- ユーザ認証の機能を回避することにより…
  - 認証機能を回避して不正にサービスを利用
  - 正規ユーザになりすましてサービスを利用

- 「認証」に関する脅威
  - ブルートフォース（Brute Force）
  - 認証設定の不備（Insufficient Authentication）
  - パスワードリカバリの不備（Weak Password Recovery Validation）

ブルートフォース

- ユーザIDやパスワードを推測し、認証を通過するまで試行
  - 固定パスワードを用いたWebシステムで、パスワードが容易に推測される場合に発生
  - あるユーザIDに対し、複数のパスワードを試す
  - あるパスワードを用い、複数のユーザIDを試す
  - 辞書の単語、辞書の単語＋数字、英数字記号の組み合わせ
  - いわゆる「オンライン・パスワードクラック」

- 対策：
  - 安易なパスワードの設定を拒否する
  - 連続した認証要求を拒否する（ディレイを入れる）
  - アカウントのロックアウト（正規ユーザが使えなくなる恐れあり）

認証設定の不備

- 認証を通過しなくてもアクセスできるページや機能を探す
  - 認証の設定忘れ、漏れ、あるいは意図的に認証を設定していない（特定の人のみにURL通知等）場合に発生
  - 秘密のURL、隠しURL、テスト用、サンプル、…
  - Webベースの管理機能（/admin/等）
  - Security Through Obscurity … 「不知」によるセキュリティ

- 対策：
  - 必要に応じてページや機能に認証を設定する
  - 不要なテストコンテンツ、サンプルコンテンツ等を削除する

パスワードリカバリの不備

- Webシステムが用意しているパスワードリカバリ機能を利用し、ユーザのパスワードを取得・変更する
  - ユーザのためにパスワードリカバリ機能を提供しているようなWebシステムで発生
  - パスワードリカバリにおける認証は、一般的にパスワードよりも推測しやすい
  - 単純な情報の要求（電子メールアドレス、住所、電話番号、…）
  - 秘密の質問（母親の旧姓、高校の名前、…）
  - ユーザが設定するヒント
- 対策：
  - 単純な情報による認証は避ける
  - 連続した認証要求を拒否する（ディレイを入れる）
  - パスワードをWebページに表示せず、電子メール等でユーザに通知する

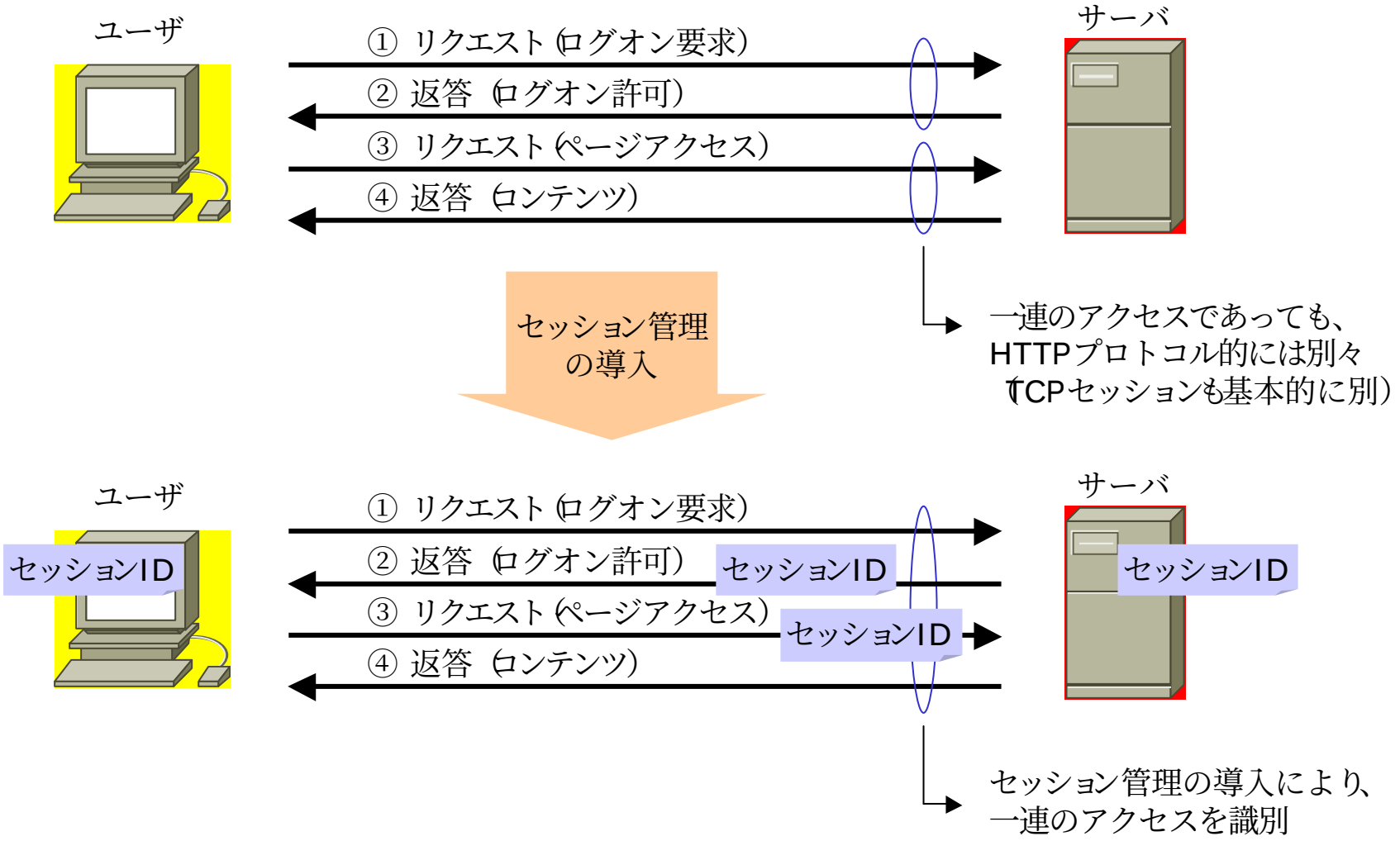
承認（Authorization）

- 承認 … ユーザに適切なアクセス許可を与える行為

- アクセス制御機能を回避することにより…
  - 本来アクセスできないページや機能にアクセス
  - 他のユーザの権限でコンテンツにアクセス

- 「承認」に関する脅威
  - セッションIDの推測（Credential/Session Prediction）
  - アクセス制御の不備（Insufficient Authorization）
  - セッション終了処理の不備（Insufficient Session Expiration）
  - セッション・フィクセイション（Session Fixation）

補足：Webのセッション管理とは

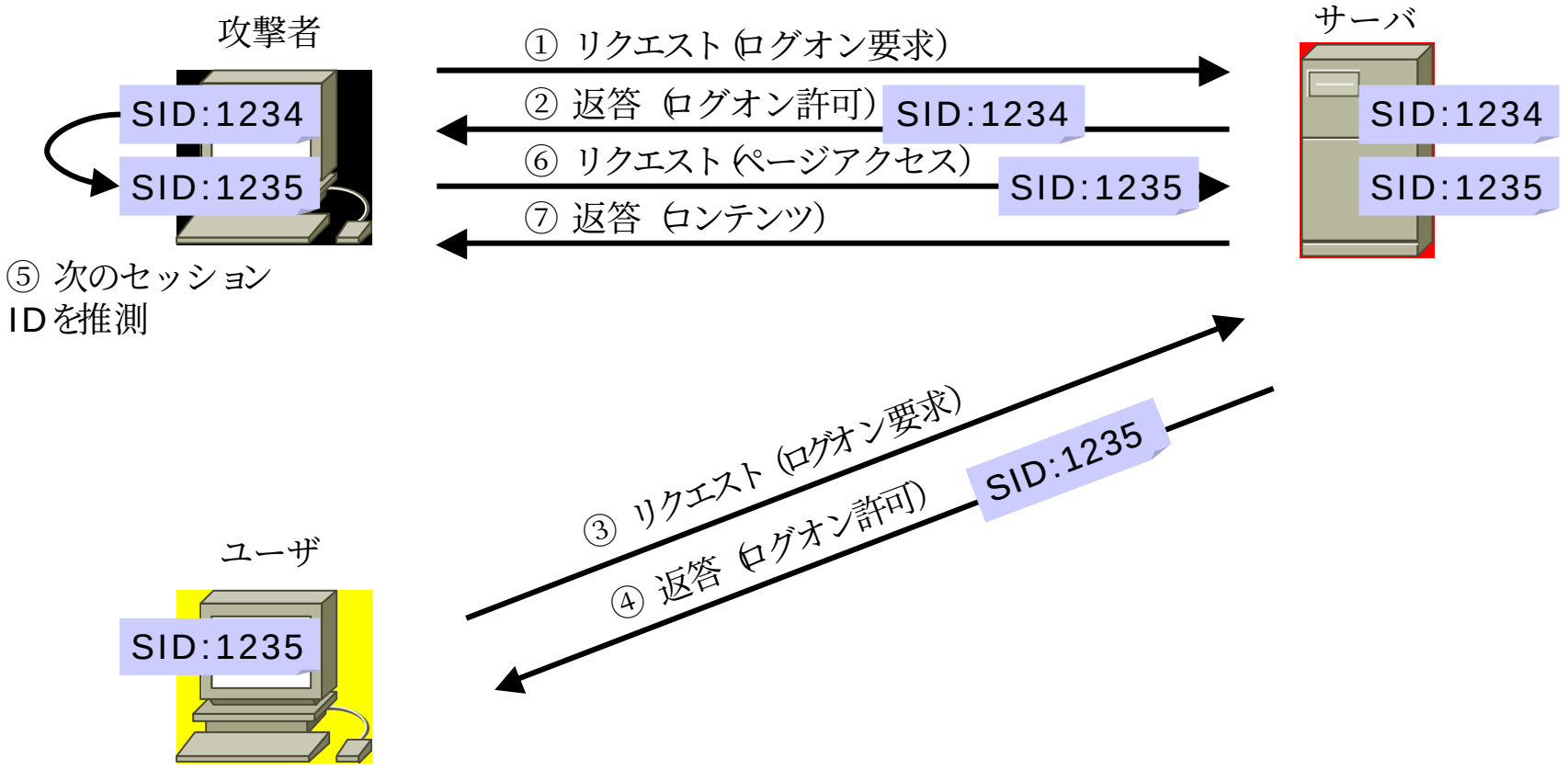


セッションIDの推測

- 他のユーザのセッション管理情報（セッションID）を推測する
  - 他ユーザのセッションIDが容易に推測できるような場合に発生
  - そのユーザの権限でコンテンツや機能に不正にアクセス
  - セッションID生成のアルゴリズムの不備 → 他のセッションIDを推測
    - 連番によるセッションID
    - 桁数の少ないセッションID
    - ユーザ情報を単純にハッシュしたセッションID

- 対策：
  - 十分に複雑なセッションIDを用いる
  - 十分に長いセッションIDを用いる
  - セッションの有効期間を適切に設定する

補足 :セッションIDの推測



アクセス制御の不備

- 本来アクセスが許可されていないリソースにアクセスを試みる
  - アクセス制御の設定忘れ、漏れ、あるいは意図的に設定していない（特定の人のみにURL通知等）場合に発生
  - 管理者のみがアクセス可能なページ、機能
  - 他のユーザからはアクセスできないページ、機能
  - 秘密のURL、隠しURL、テスト用、サンプル、…
  - Security Through Obscurity … 「不知」によるセキュリティ

- 対策：
  - 必要に応じてページや機能にアクセス制御を設定する
  - 不要なテストコンテンツ、サンプルコンテンツを削除する

セッション終了処理の不備

- 他ユーザのセッションIDを入手してWebサイトにアクセス
  - セッションのログアウト処理が適切に行われない、あるいはセッションのタイムアウト処理が適切に行われない場合に発生
  - そのユーザの権限でコンテンツや機能に不正にアクセス
  - セッションIDの盗用 … スニッフィング、XSS、ブラウザのback操作等

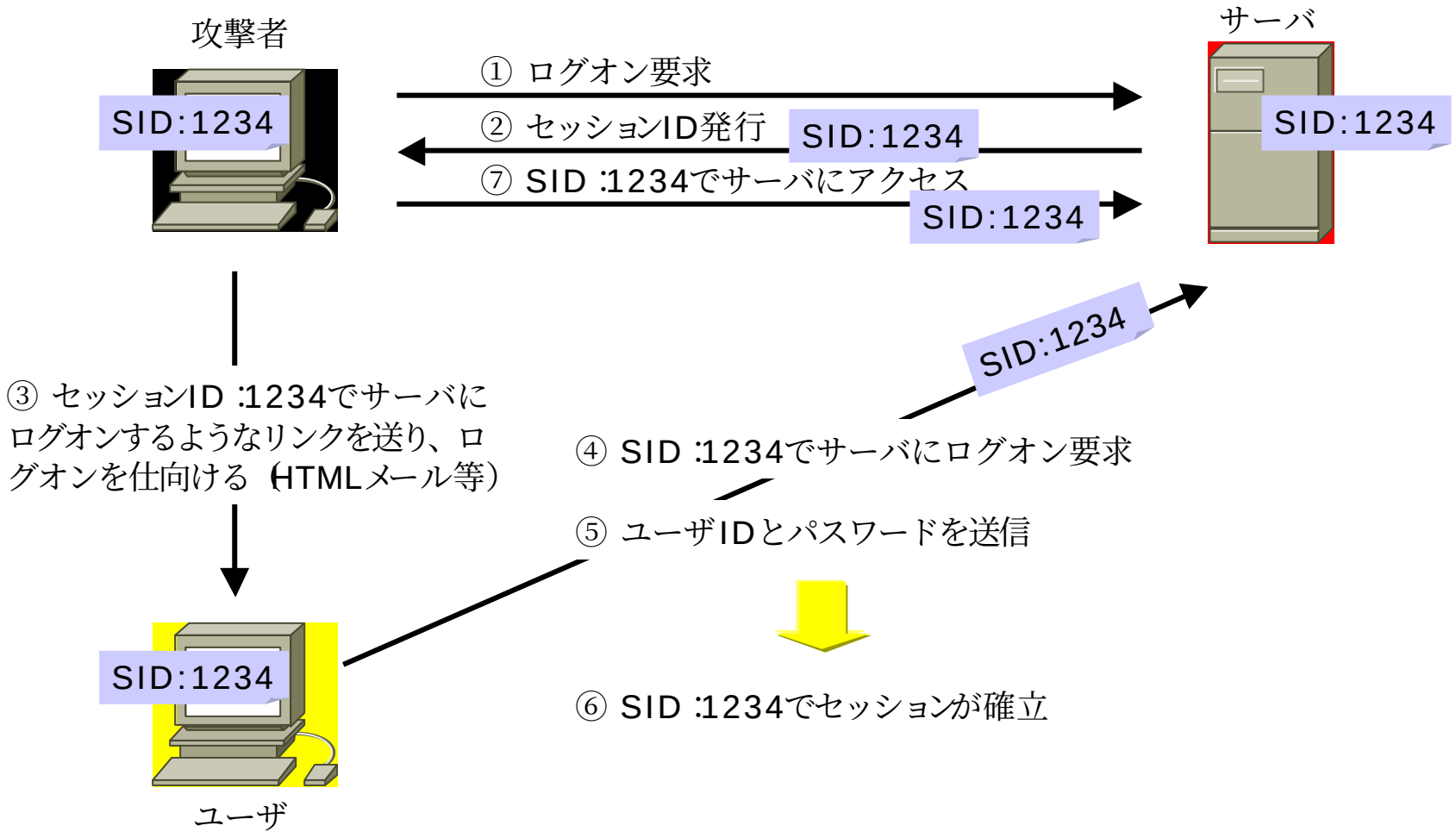
- 対策：
  - ユーザのログアウトによるセッション終了処理を実施する
  - セッションの有効期間を適切に設定する
  - 通信経路を暗号化する（SSL等）

セッション・フィクセイション

- ユーザのセッションIDを既知のもので「fix」させる攻撃
  - Webシステムがユーザ指定のセッションIDを受け入れる場合、あるいはユーザ認証前にセッションIDを発行する場合に発生
  - ユーザのブラウザに既知のセッションIDを送り込む（HTMLメール等）
    - URLのクエリストリングに設定
    - XSS（Cross-site Scripting）によりCookieに設定
  - ユーザがWebサイトにアクセスする際、そのセッションIDが使用される
  - ユーザ認証後、攻撃者はそのセッションIDでWebサイトへアクセス

- 対策：
  - Webシステム自身が発行するセッションID以外は受け入れない
  - ユーザ認証後にセッションIDを発行する
  - セッションIDとブラウザのIPアドレス等を関連付けて管理する

補足 :セッション・フィクセイション攻撃



クライアントサイド・アタック（Client-side Attacks）

- Webサイトにアクセスするユーザ側を攻撃対象
- ユーザのWebサイトに対する「信頼」を利用
  - ユーザ（あるいはブラウザ）はそのサイトが信頼できると期待
  - 心理的信頼
  - 技術的信頼
- 「クライアントサイド・アタック」に関する脅威
  - コンテンツ・スプーフィング（Content Spoofing）
  - クロスサイト・スクリプティング（Cross-site Scripting）

コンテンツ・スプーフィング

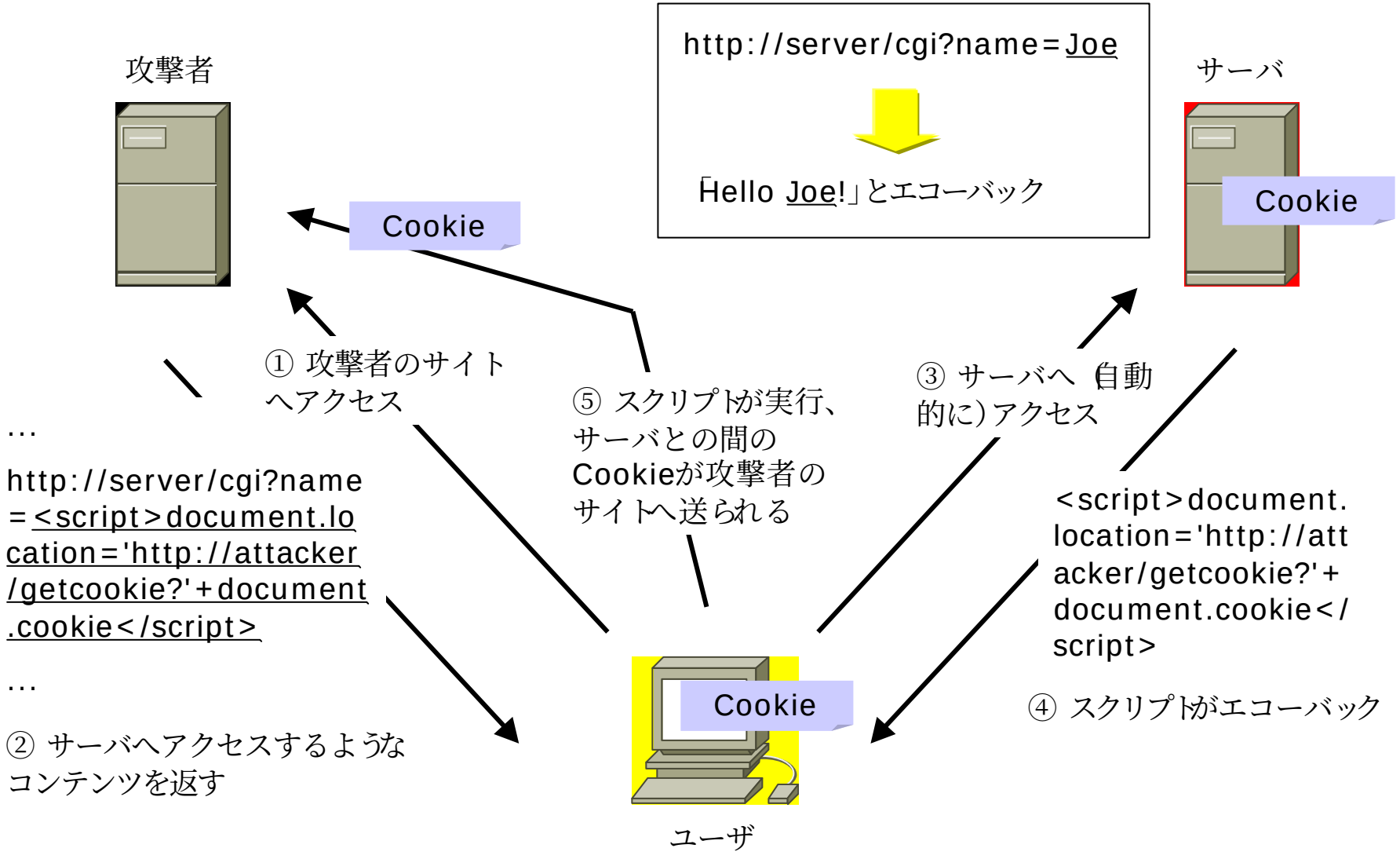
- 正規のWebサイトのコンテンツであるように見せかける攻撃
  - URL内にフレームソースのURLが記述している場合などに発生
    - http://foo.example/page?frame_src=http://foo.example/file.html
      ↓
    - http://foo.example/page?frame_src=http://attacker.example/spoof.html
  - このURLにアクセスしたユーザは、正規のWebサイトのコンテンツだと思い込む（心理的信頼）
  - ユーザ情報の取得（フィッシング詐欺）、偽のプレスリリース、…

- 対策：
  - フレーム内表示コンテンツのURLを、クエリストリング等ブラウザ側で変更できる位置に入れない
  - 不正なフレームソースURLを受け付けない

クロスサイト・スクリプティング（XSS）

- 攻撃者が記述したスクリプトをWebサイトからエコーバックさせ、ユーザのブラウザ上で実行させる攻撃
  - ブラウザからの入力をそのままエコーバックするような場合に発生
  - JavaScript/VBscript等、ブラウザがサポートするスクリプトの実行
  - ブラウザとWebサイトの技術的信頼関係を利用
    - そのWebサイトにおいて実行可能なスクリプトが実行（Eのセキュリティゾーン）
    - そのWebサイトとの間で交信されるCookieを取得 → セッションIDの盗用につながる
- 対策：
  - 入力データとして不適切な文字種を受け付けない
  - 入力データのエコーバックの際には特殊文字を無害化（サニタイズ）
  - Webサービスのバグの場合は、パッチを適用

補足 :クロスサイト・スクリプティング



コマンド実行（Command Execution）

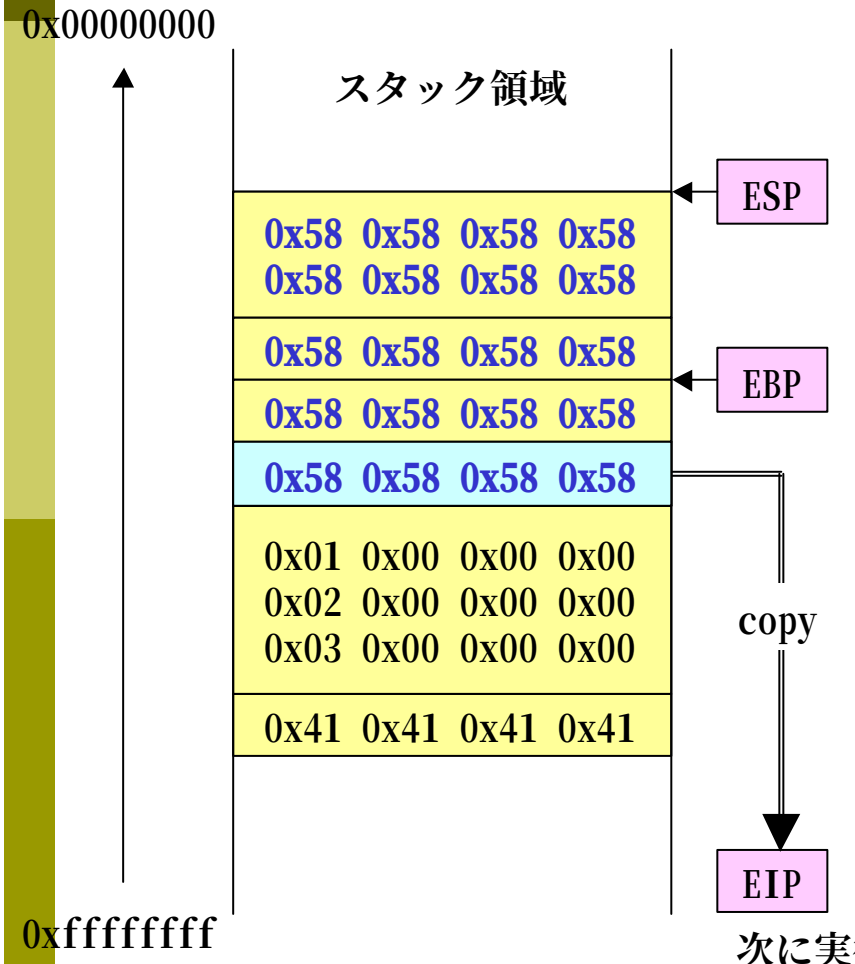
- 開発者が意図しない処理を、リモートからWebサイト上で実行させるような攻撃
- 不正なコマンド実行により…
  - 処理の異常終了、機密データの取得、変更
  - ユーザ認証の回避、不正なプログラムコードの実行、…
- 「コマンド実行」に関する脅威
  - バッファオーバーフロー（Buffer Overflow）
  - フォーマットストリング・アタック（Format String Attack）
  - LDAPインジェクション（LDAP Injection）
  - OSコマンド実行（OS Commanding）
  - SQLインジェクション（SQL Injection）
  - SSIインジェクション（SSI Injection）
  - XPathインジェクション（XPath Injection）

バッファオーバーフロー

- プログラムが確保したメモリ領域を、ユーザ入力によりオーバーフローさせる攻撃
  - バッファへのデータコピーの際の、長さチェックに不備がある場合に発生
  - C/C++で書かれたCGIや、動的に呼び出されるCプログラム等
  - スタック領域におけるバッファオーバーフロー
  - ヒープ領域におけるバッファオーバーフロー
  - 異常終了、パラメータ変更、プログラムコードの実行など

- 対策：
  - バッファコピー時の長さチェック、長さの値の正負チェック
  - 入力データとして不適切な文字種を受け付けない
  - Webサービスのバグの場合は、パッチを適用

補足 :スタック領域におけるBOF




```
void sub(i, j, k)
int i, j, k;
{
    unsigned char a[] = { 0x00, 0x01, 0x02, 0x03 };
    unsigned char b[] = { 0x10, 0x11, 0x12, 0x13,
                          0x14, 0x15, 0x16, 0x17 };
    ..........
    strcpy(b, user-input);
}

void main()
{
    unsigned char A[] = { 0x41, 0x41, 0x41, 0x41 };

    sub(1, 2, 3);

    ..........
}
```

XXXXXXXXXXXXXXXXXXXX

次に実行するプログラムコードのアドレス

フォーマットストリング・アタック

- フォーマットストリング … printf()等における「書式指定文字列」のこと（%s, %d, %x, …）
- ユーザ入力をフォーマットストリングとして処理させる攻撃
  - プログラム上でフォーマットストリングを指定していない場合に発生
    - 例）printf(buf); ← bufにユーザ入力が入るケース
  - C/C++で書かれたCGIや、動的に呼び出されるCプログラム等
  - %xを指定してスタックのデータを表示
  - %nを指定してメモリ中の任意の4バイトを書き換え → 異常終了、不正コードの実行
- 対策：
  - フォーマットストリングをプログラム上で指定する
  - 入力データとして不適切な文字種を受け付けない
  - Webサービスのバグの場合は、パッチを適用

補足 :フォーマットストリング ・アタック

- フォーマットストリング ・アタックによる、スタック上のデータの読み取り

printf("%x", 1);

↓

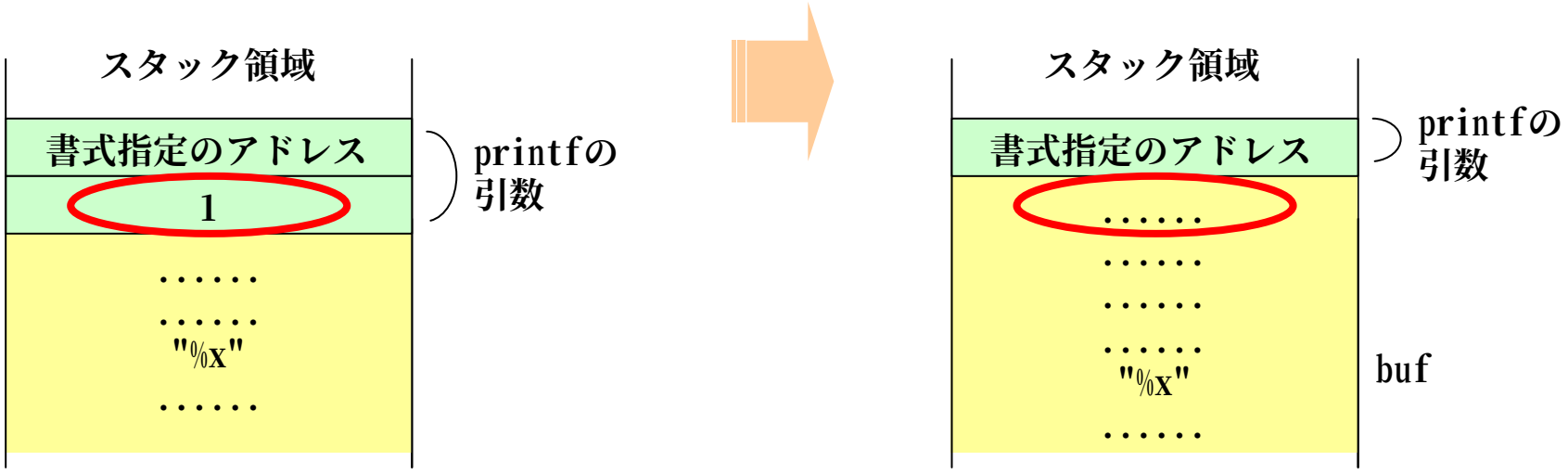
書式指定に従い、「1」を16進数で出力

printf(buf);

buf ← ユーザ入力「"%x"」

↓

書式指定に従い、スタックの次の位置を16進数で出力



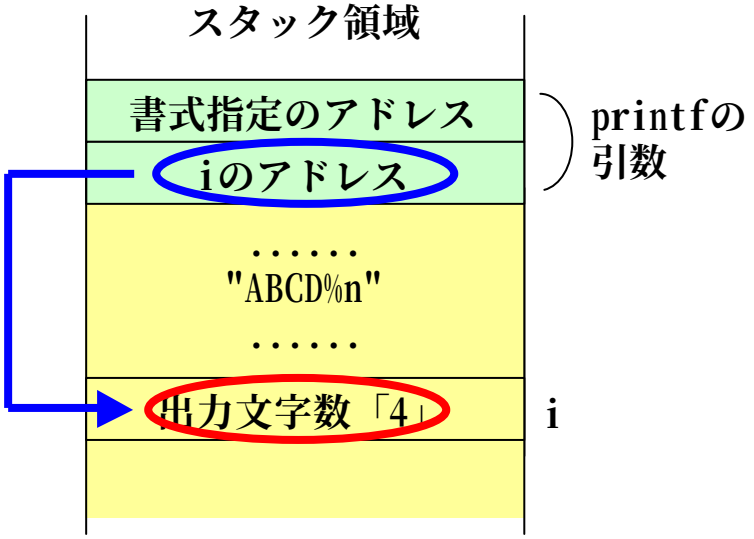
補足 :フォーマットストリング ・アタック

- フォーマットストリング ・アタックによる、スタック上のデータの上書き

```
int i;
printf("ABCD%n", &i);
```

↓

書式指定に従い、「i」に出力文字数「4」が書かれる

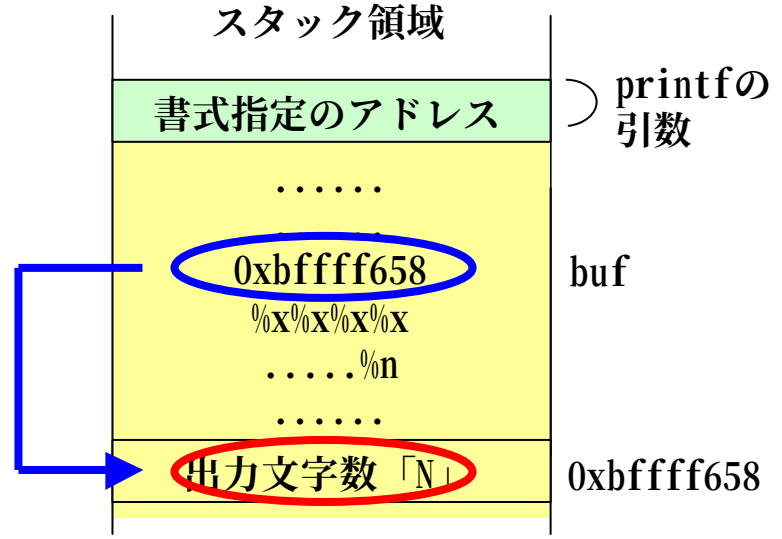



```
printf(buf);
```

buf ← ユーザ入力
「0xbffff658%x%x%x%x...%n」

↓

書式指定に従い、アドレス0xbffff658の位置に出力文字数「N」が書かれる



LDAPインジェクション

- 不正な入力により、不正なLDAPクエリーを発行させる攻撃
  - ユーザの入力に基づき、LDAPサーバに対してクエリーを発行するようなWebシステムで発生
  - 不正な情報取得
    - http://foo.example/ldapsearch?user=*
      ↓
    - (uid=*)でLDAP検索を実行

- 対策：
  - 入力データとして不適切な文字種を受け付けない
  - 必要に応じて文字のエスケープ処理を実施

OSコマンド実行

- 不正な入力により、任意のOSコマンドを実行させる攻撃
  - ユーザ入力に基づいて、ファイルオープンやコマンド実行を行うようなWebシステムで発生
  - Perl、C、PHP、…
    - open(FILE, $fname); ← $fnameに"/bin/ls |"
    - system("ls -la $fname"); ← $fnameに"; cat /etc/passwd"
    - …
  - ユーザ入力を格納するデータベースのデータ等、後でアプリケーションが参照する場合も危険

- 対策：
  - 入力データとして不適切な文字種を受け付けない
  - 必要に応じて文字のエスケープ処理を実施

SQLインジェクション

- 不正な入力により、不正なSQLクエリーを発行させる攻撃
  - ユーザの入力に基づき、データベースサーバに対してクエリーを発行するようなWebシステムで発生
  - ユーザ認証の回避
    - "SELECT Username FROM Users WHERE Username = '$uname' AND Password = '$pass'"
      ↓
    - "SELECT Username FROM Users WHERE Username = '' OR ''='' AND Password = '' OR ''=''"
  - 「Union」句によるデータ取得、ストアドプロシジャを利用したコマンド実行、…
- 対策：
  - 入力データとして不適切な文字種を受け付けない
  - 必要に応じて文字のエスケープ処理を実施

SSIインジェクション

- 不正なSSI記述のHTML文をWebサーバ上に送り込む攻撃
  - ユーザの入力に基づき、HTMLページを生成するようなWebシステムで発生
    - 掲示板サイト、ゲストブック、…
  - 不正なSSI記述を受け付けた場合、そのページを表示する際にSSIが実行
  - OSコマンドの実行
    - `<!--#exec cmd="/bin/ls /" -->`
  - ファイルの表示
    - `<!--#include file="/etc/passwd" -->`
- 対策：
  - 入力データとして不適切な文字種を受け付けない
  - 必要に応じて文字のエスケープ処理を実施
  - 不要な場合はSSIの機能を停止

XPathインジェクション

- XPath … XMLドキュメントを参照するための言語
- 不正な入力により、不正なXPathクエリーを発行させる攻撃
  - ユーザの入力に基づき、XMLドキュメントに対してクエリーを発行するようなWebシステムで発生
  - ユーザ認証の回避
    - `string(//user[name/text()='$uname' and password/text()='$pass']/account/text())`

      ↓

    - `string(//user[name/text()='' or 1=1 or ''='' and password/text()='foobar']/account/text())`
  - 不正なドキュメント内容表示
- 対策：
  - 入力データとして不適切な文字種を受け付けない
  - 必要に応じて文字のエスケープ処理を実施

情報取得（Information Disclosure）

- Webサイトに関するさまざまな情報を取得する攻撃

- 情報取得により…
  - ターゲットサーバのソフトウェアバージョン、パッチレベル、存在するファイル、エラーに関する情報等を入手
  - より攻撃が行いやすくなる、より高度な攻撃に結びつく

- 「情報取得」に関する脅威
  - ディレクトリ内容表示（Directory Indexing）
  - 情報漏洩（Information Leakage）
  - パス・トラバーサル（Path Traversal）
  - リソース位置の推測（Predictable Resource Location）

ディレクトリ内容表示

- ディレクトリ内のファイル一覧を取得する攻撃
  - ディレクトリインデックス機能が有効になっている場合
    - URLにディレクトリを指定してアクセス
  - Webサービスにバグがある場合
    - 例）Apache 1.3; GET //////////..... HTTP/1.0
  - Google等サーチエンジンのキャッシュを調査
    - 過去にファイル一覧を表示させていたケース
  - ファイル一覧を見ることで、データファイル、バックアップファイル、設定ファイル等、隠されたファイルの存在を知ることができる

- 対策：
  - 不要なディレクトリインデックス機能を無効にする
  - Webサービスのバグの場合は、パッチを適用

情報漏洩

- Webシステムに関連する各種情報を取得する攻撃
  - HTMLファイル内のコメント、親切な（？）エラーメッセージ、…
  - 認証やアクセス制御の不備による各種情報漏洩
  - 通信系路上での盗聴
  - Webサービスのバグによるファイル、スクリプト内容表示
  - 物理パスの漏洩
  - バージョン情報の漏洩
  - プライベートIPアドレスの漏洩
- 対策：
  - 不必要なコメントは避け、エラーメッセージは最低限とする
  - 認証、アクセス制御を確実に行い、通信経路を暗号化する
  - Webサービスのバグの場合は、パッチを適用

パス・トラバーサル

- Traversal … 横断する、横切る
- 開発者の意図に反して、他のディレクトリパスやファイルにアクセスする攻撃
  - パラメータに絶対パスや相対パスで別ディレクトリファイルを指定
    - http://example/foo.cgi?file=../../../etc/passwd
  - Unicode形式、UTF-8形式、ダブルエンコード、NULL文字の追加（%00）等で防御を回避
    - http://example/foo.cgi?file=..%255c..%255c..%255cetc/passwd
  - 機密ファイルやスクリプトファイルの表示、OSコマンドの実行
- 対策：
  - 入力データとして不適切な文字種を受け付けない
  - 必要に応じて文字のエスケープ処理を実施
  - Webサービスのバグの場合は、パッチを適用

リソース位置の推測

- 公開していない隠れたファイルや機能に対し、リソース名を推測してアクセスする攻撃
  - 一時ファイル、バックアップファイル、設定ファイル、管理機能、サンプル、…
  - バックアップファイル（.bak、.old、.org、.orig、…）
  - コンフィグファイル（.conf、.cfg、.config、…）
  - データファイル（.dat、.data、…）
  - /admin/、/backup/、/logs/、…

- 対策：
  - 必要に応じてページや機能に認証・アクセス制御を設定する
  - 不要なテストコンテンツ、サンプルコンテンツ等を削除する

補足：NiktoによるWebスキャン

- Nikto（http://www.cirt.net/code/nikto.shtml）

```
$ perl nikto.pl -nolookup -host 192.168.183.12
---------------------------------------------------------------------------
- Nikto 1.34/1.29     -     www.cirt.net
+ Target IP:       192.168.183.12
+ Target Hostname: 192.168.183.12
+ Target Port:     80
+ Start Time:      Thu Sep 30 07:27:42 2004
---------------------------------------------------------------------------
......
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH,
LOCK,UNLOCK
+ /<script>alert('Vulnerable')</script>.shtml - Server is vulnerable to Cross Site
Scripting (XSS). CA-2000-02. (GET)
......
+ /blahb.ida - Reveals physical path. ......
......
+ /xxxxx.htw - Server may be vulnerable to a Webhits.dll arbitrary file retrieval. ...
+ /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir - IIS is vulnerable to a
double-decode bug, which allows ......
......
+ /_vti_bin/fpcount.exe - Frontpage counter CGI has been found. ......
......
......
+ 2648 items checked - 20 item(s) found on remote host(s)
+ End Time:       Thu Sep 30 07:28:28 2004 (46 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

ロジカル・アタック（Logical Attacks）

- Webシステムのロジックをだます、あるいは悪用する攻撃

- ロジカル・アタックにより…
  - 開発者が期待する結果とは異なる方向へWebシステムの機能を導く
  - 正常な処理を誤らせる、処理を異常終了させる
  - 他者への攻撃の踏み台にする

- 「ロジカル・アタック」に関する脅威
  - 機能の悪用（Abuse of Functionality）
  - サービス妨害（Denial of Service）
  - 自動アクセス防止の不備（Insufficient Anti-automation）
  - プロセスフロー管理の不備（Insufficient Process Validation）

機能の悪用

- Webシステムの機能を不正に使用する攻撃
  - Webページのサーチ機能 → Webディレクトリ以外を検索
  - ファイル表示機能 → スクリプト内容表示
  - コメント投稿のメール送信機能 → スパム発信
  - ファイルアップロード機能 → Webページや設定ファイルの書き換え
  - hidden項目の価格データ → 価格を書き換えて送信
  - Webサービスのデフォルト機能
    - Frontpage Server Extensions（IS）
    - WebDAV（IS）
- 対策：
  - そのパラメータが機能にとって適切かどうかをチェックする
  - 不必要なパラメータをhidden項目等でブラウザに渡さない
  - 不要なデフォルト機能は削除する

サービス妨害

- Webサイトに対する正常なアクセスができないような状態に陥らせる攻撃
  - リソースを大量に消費させる … 膨大な量のデータベースアクセス
  - 特定のユーザのログオン失敗を繰り返す … アカウントロックアウト
  - SQLインジェクションでデータテーブルを書き換える
  - バッファオーバーフローでWebサーバを異常終了させる

- 対策：
  - そのパラメータが機能にとって適切かどうかをチェックする
  - Webサービスのバグの場合は、パッチを適用

自動アクセス防止の不備

- Webサイトに対するアクセスを自動化して各種攻撃を実行
  - アクセスの自動化により、さまざまな攻撃がより容易に行われる
  - ユーザログオンのブルートフォース
  - 大量のスパム発信
  - 掲示板への繰り返し投稿
  - 大量アクセスによるサービス妨害

- 対策：
  - 手動アクセスを想定している機能は、機械的なアクセスを阻止する
  - ディレイの設定
  - 一定時間内の処理数の限定

プロセスフロー管理の不備

- 開発者の意図したロジック・フローを回避する攻撃
  - ユーザ操作のステート（状態）管理が適切でない場合に発生
  - ユーザのステート（どこまで処理したか）をブラウザ側で変更
    - hidden項目、Cookie等
  - 必要な処理をバイパスして不正に機能を実行
  - 不正な送金、パスワード変更、商品購入、…

- 対策：
  - ユーザ操作のステート情報をサーバ側で管理

その他

- HTTPレスポンス・スプリッティング（HTTP Response Splitting）
  - サーバに不正なリクエストを送り、サーバのレスポンスを二つに分割させることで、プロキシやブラウザのキャッシュ上でコンテンツ・スプーフィングを実現する攻撃
  - ブラウザからの入力に基づいてリダイレクトのLocationヘッダを構築するようなWebシステムで発生

- Webフィンガープリンティング（Web Server/Application Fingerprinting）
  - アプリケーションレイヤにおけるフィンガープリンティング攻撃
  - レスポンスヘッダ、Cookie、エラーページ、ファイル拡張子等の情報に基づいて、WebサービスやWebアプリケーションを特定する

再び、「脆弱である」とは…?

- 「脆弱である」とは、脅威すなわち攻撃手法に対抗できない状態をあらわす
  - ブルートフォース攻撃に対抗できるか?
  - パスワードリカバリ攻撃に対抗できるか?
  - セッションIDの推測に対抗できるか?
  - セッション・フィクセイション攻撃に対抗できるか?
  - クロスサイト・スクリプティング攻撃に対抗できるか?
  - SQLインジェクションに対抗できるか?
  - ……
- Webサービスの脆弱性 → 広く調査され、一般に公開
- Webアプリケーションの脆弱性 → (基本的に)誰も(タダでは)調べてくれないし、教えてもくれない

まとめ

- 脆弱であるかどうか」を知るためには 脅威」を知ることが重要
- Webにおけるさまざまな脅威
  - 認証
  - 承認
  - クライアントサイド・アタック
  - コマンド実行
  - 情報取得
  - ロジカル・アタック
- 適切なリスク判断なしに、適切な対策はできない
  - その脅威がどれほど実現可能か
  - どれほど流行しているか
  - どの程度の影響があるか
  - 他の対策状況はどうか、…
  - 物事には優先順位がある!!

参考

- WASC Web Security Threat Classification
  http://www.webappsec.org/threat.html
- OWASP Top Ten
  http://www.owasp.org/documentation/topten.html
- OWASP A Guide to Building Secure Web Applications
  http://www.owasp.org/documentation/guide/guide_about.html
- @IT Webアプリケーションに潜むセキュリティホール
  http://www.atmarkit.co.jp/fsecurity/rensai/webhole01/webhole01.html
- @IT クロスサイトスクリプティング対策の基本
  http://www.atmarkit.co.jp/fsecurity/special/30xss/xss01.html
- HTTP Response Splitting
  http://www.sanctuminc.com/pdf/whitepaper_httpresponse.pdf
- The Google Hackers Guide
  http://johnny.ihackstuff.com/security/premium/The_Google_Hackers_Guide_v1.0.pdf