セキュリティタスクフォースを知らない人のために

セキュリティタスクフォースとは
☞各チームから選出されたセキュリティ担当者のこと

■ミッション
- IPA,WAFの導入サポート
- OWASP ZAPを用いた定期的な脆弱性チェック
- **セキュリティにまつわる定期講習会によるセキュリティ啓蒙活動**

ホワイトハッカーや**セキュリティ監査チーム**とは
別のアプローチを行うチームです。

本編まで、もう少々おまちください。

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

セキュアWEBアプリケーション開発基礎

GMOインターネット
システム本部UXデザイン開発部

発表：谷中 佑貴人

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

☠ 情報漏えい事案の現状

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

情報漏えい事案の現状

情報通信事業例

事業	内容	情報漏えい
ブログサービス	一部が外部から改ざんされたことにより、ブログ閲覧者がマルウェアに感染した	・クレカ情報：件数不明 ・改ざん：被害あり
ウェブコンテンツ配信サービス	オンラインカードゲームサイトへの不正アクセスにより、認証情報とメールアドレスが漏えい	・アカウント情報：約20万件
ポータルサイトサービス	無料コンテンツ共有サービスへの不正アクセスにより、利用者情報が漏えい	・個人情報：最大約400万件
サーバー運営サービス事業	Webサーバーへの不正アクセスにより、応募者の個人情報数千件が閲覧された可能性	・個人情報：数千件
ゲームソフトウェア事業	ポータルサイトへの4百万件弱のパスワードリスト攻撃により、不正ログインが行われ、顧客情報が漏えい	・クレカ情報：約3万件

※株式会社サーバーセキュリティクラウド社調べ

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

情報漏えい事案の現状

リスク総額

JNSAセキュリティ被害調査ワーキンググループによる
個人情報漏えい事件・事故（以降「インシデント」という）の調査分析より算出

名称	データ
漏えい人数	1,510万6,784人
インシデント件数	468件
想定損害賠償総額	2,994億2,782万円
一件あたりの漏えい人数	3万4,024人
一件あたりの平均想定損害賠償額	6億7,439万円
一人あたりの平均想定損害賠償額	3万1,646円

・3万1,646円×人数
・株価への影響

※株式会社サーバーセキュリティクラウド社調べ

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

☠ 情報漏えい事案の現状

GMOインターネットで発生した場合は更に

・グループ全体のブランドイメージ毀損
・社会的信用の失墜
・総務省への対応、業務改善命令
・金融庁への対応、銀行業、銀行代行業の取り消し
・関東財務局への対応
・大口顧客への対応
・グループ各社への対応

など

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

☠ 情報漏えい対策への義務

アクセス管理者による防衛措置（第8条関係）

不正アクセス行為の発生を防止するためには、その禁止・処罰に頼るのみではなく、不正アクセス行為が行われにくい環境を整備することが必要となります。そのためには、個々のアクセス管理者が自ら防御措置を講じることが必要となりますが、その実施状況は必ずしも十分ではないのが現状です。
そこで、アクセス管理者に防御措置の実施を促すため、**アクセス管理者に不正アクセス行為からの防御措置を講ずべき責務があることを法律上明確にしました。**そして、 アクセス制御機能を特定電子計算機に付加したアクセス管理者は、ＩＤ・パスワード といった識別符号等の適正な管理に努めるとともに、常にアクセス制御機能の有効性 を検証し、必要があると認めるときにはアクセス制御機能の高度化その他必要な措置 を講ずるよう努めるものとしています。
アクセス管理者に求められる防御措置の主な内容は次ページに記述する

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

☠ 情報漏えい対策への義務

■利用権者の異動時における識別符号の確実な追加・削除、長期間利用されていない識別符号の
　確実な削除、パスワード・ファイルの暗号化といった識別符号の適正な管理

■アクセス制御機能として用いているシステムのセキュリティに関する情報(セキュティ・ホール情報、バージョン・アップ情報など)の収集といったアクセス制御機能の有効性の検証

■パッチプログラムによるセキュリティ・ホールの解消、アクセス制御プログラムのバージョン・アップ、指紋・虹彩などを利用したアクセス制御システムの導入といったアクセス制御機能の高度化

■ワンタイム・パスワードや指紋、暗号鍵等の他人に窃用されにくい識別符号の採用

■コンピュータ・ネットワークの状態を監視するのに必要なログを取得しその定期的な検査を行う、ログを利用して前回アクセス日時を表示し利用権者にその確認を求めるといったログの有効活用

■ネットワーク・セキュリティ責任者の設置

といったことが挙げられる。

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

セキュアWEBアプリケーション開発基礎

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

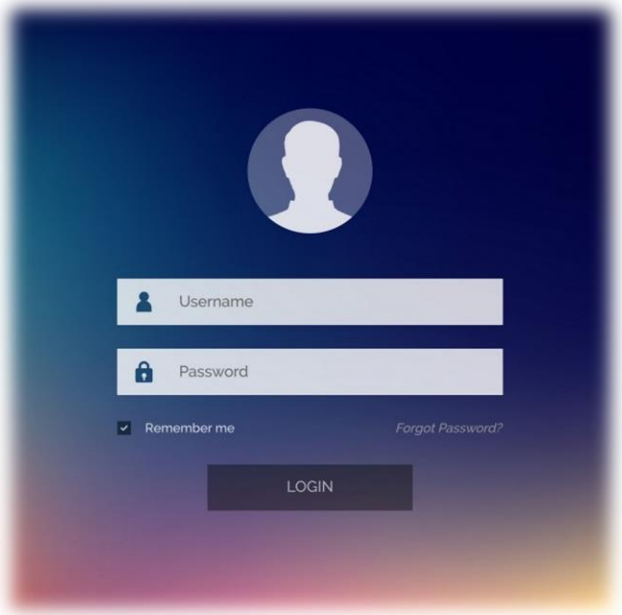
- ログインを狙う攻撃と対策
- ユーザーの意図しない操作・なりすまし攻撃と対策
- セッションを狙う攻撃と対策
- 入力、出力に潜む脆弱性と対策
- その他の脆弱性、注意点

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

ログインを狙う攻撃と対策



webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

ログインを狙う攻撃と対策

WEBアプリケーションにおけるログインの役割

■識別

固有のユーザーアカウント（ID）：システムがユーザーを特定する識別子。
IDが1つの場合、基本的にユニークであるが組織やドメイン、役割（ロール）などの識別子と組み合わせて一意となるシステムもある。シリアル番号、ランダム文字列、ドメイン名、メールアドレス、ユーザー設定文字列などがある。マーケティング目的などでログイン以外でユーザーを個別に識別したい場合は、ユーザーIDとは別のランダムなキーを使用するべきである。

■認証

ユーザーが本人である事を確認する。パスワードによる認証が中心だが証明書認証、ワンタイムパスワード、生体認証（指紋・虹彩・顔）や、認証トークン（ハード、ソフト）などもある。
複数組み合わせる事により強固な認証となる。

■認可

ユーザー毎に提供するリソースと操作できる権限を制限する。システムに役割（ロール）の概念がある場合、更に詳細に制限される。

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

ログインを狙う攻撃と対策

総当たり攻撃（ブルートフォースアタック）

特定のIDに対してパスワードがマッチするまで文字列を総当りに試行する攻撃

辞書攻撃（ディクショナリアタック）

総当り攻撃の時間を短縮する為に、パスワードとして良く使われている文字列や、
英単語のリストを組み合わせて使いログインを試行する攻撃

逆総当たり攻撃（リバースブルートフォースアタック）

良く用いられるパスワードを固定し、IDがマッチするまで文字列を総当りに
試行する攻撃。数字のIDやメールアドレスのIDがターゲットにされやすい。

リスト型攻撃（リストベースアタック）

パスワードを使いまわしているユーザーをターゲットに、他のWebサイトなどから
入手したユーザーIDとパスワードのリストを使ってログインを試行する攻撃。
メールアドレスのIDがターゲットにされやすい。

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

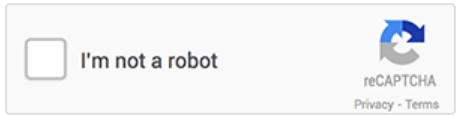
ログインを狙う攻撃と対策

ロックアウト

短時間に規定回認証エラーが続く場合、ロックアウトしログイン試行できないようにする。
ユーザーID、IPアドレス、セッション、フィンガープリント単位で行う。

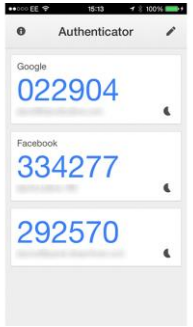
チューリングテスト（ボット避け）

CAPTA、reCAPTA、パズル認証



二段階認証

ログイン後に追加のセキュリティコード（トークン）を
入力させて不正ログインを防止する。



webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

ログインを狙う攻撃と対策

認証エラーメッセージの注意点

攻撃のヒントとなるようなエラーメッセージを出さない。

「IDが見つかりません」
「パスワードエラー」
「パスワードは半角英数文字8～16桁で入力してください」
「使用可能な記号は＃＄％＆です」

「ID、またはパスワードが違います」
「認証できませんでした」

※システムの統合や移行などで、お客様がIDを勘違いしやすい場合、
説明文やエラーメッセージで注意を促す場合はある。

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

ログインを狙う攻撃と対策

パスワードポリシーを設定しよう

パスワードの複雑さはお客様の利便性とのトレードオフです。扱う情報の重要度やサービスの性質に合わせてあらかじめ関係者間でポリシーを設定しておく事が大切です。

■オートコンプリートの有無

ブラウザにパスワード情報を記録させるか。

■文字数範囲

8～1024文字、等

■利用可能な文字種類

アルファベット大文字・小文字、数字、記号（具体的に）、等

■複雑さ

必ず記号を含める、3種類以上の文字種類を混在させる、等

■予測可能なパスワードの禁止

IDの文字列を含むパスワードの禁止、生年月日を含むパスワードの禁止、
よく使われるパスワードTOP50まで禁止、Cracklibでチェックする、など

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

ログインを狙う攻撃と対策

パスワード情報のDB保存方法

万が一DBからパスワードが流出した場合の為に保存方法を工夫する。

不要データの削除

総務省通達の個人情報保護の観点からも、退会済みなどの不要なデータの削除、またはマスキング

ハッシュ化

非可逆関数で変換してから保存する。MD5やSHA-1では不十分（レインボーテーブルが存在する）
SHA-2以降の強度や、処理に一定の時間をかけられる変数を持っているアルゴリズム
（Argon2、 PBKDF2、 scrypt、 bcrypt等）を使用する事も有効。

ソルト

ハッシュ化する前にある程度の長さ（32byte以上推奨）の、ランダムな文字列を付加する。

ストレッチング

ハッシュ値の計算を数千回～数万回繰り返し行う事で攻撃にかかる時間を長くする。
ストレッチ回数を多くすれば強度は上がるがサーバーの負荷も増えるというデメリットがる。

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

- ログインを狙う攻撃と対策
- **ユーザーの意図しない操作・なりすまし攻撃と対策**
- セッションを狙う攻撃と対策
- 入力、出力に潜む脆弱性と対策
- その他の脆弱性、注意点

webカメラ位置

生配信中

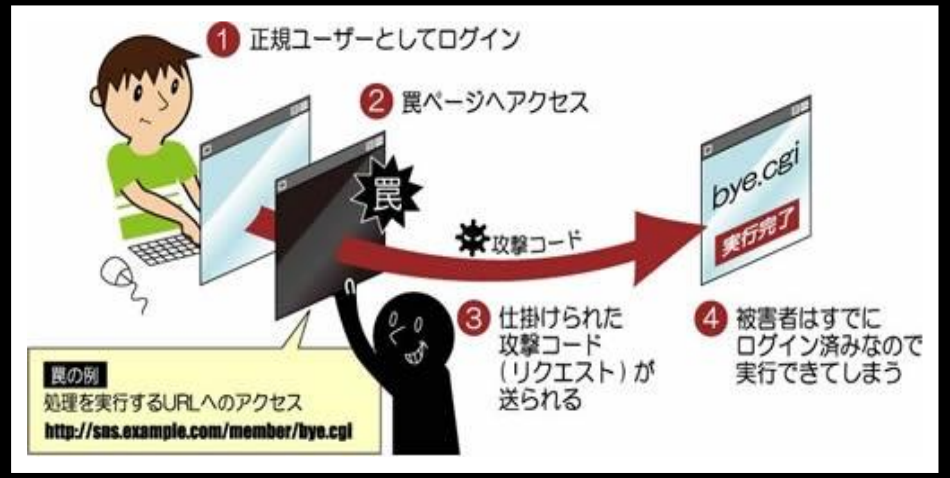
ご要望･ご質問は
チャットワークで受付中です。

☠ ユーザーの意図しない操作、なりすまし攻撃と対策

☠クロスサイト・リクエスト・フォージェリ（CSRF）

他サイトからのリクエストを直接受け取り、処理してしまうこと。攻撃者は一見無害に見える罠ページを準備し、ターゲットサイトにログイン済みのユーザが罠ページにアクセスするよう誘導する。罠ページにはターゲットサイトに不正なリクエストを送るよう設定されているため、ターゲットサイトが他サイトからのリクエストを無条件に受け取ってしまう場合、不正リクエストが処理され攻撃が成立してしまう。

- 掲示板やSNSへの、いたずら書き込み、不正サイトへ誘導リンク、犯罪予告。
- ECサイトやサービス申し込み画面では意図しない注文、解約。



webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

ユーザーの意図しない操作、なりすまし攻撃と対策

フレームワークのCSRF対策機能を使用する

CSRFトークンをhiddenやHTTPヘッダー、Cookie等に組み込みサーバー側で再度有効性をチェックする。
Originヘッダのチェックが非常に有効だが現時点ではブラウザ間の挙動に差異がある。

webカメラ位置

生配信中

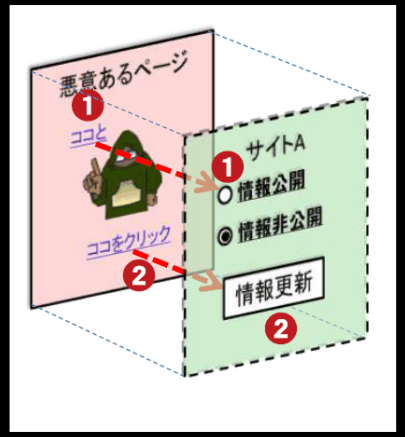
ご要望・ご質問は
チャットワークで受付中です。

☠ ユーザーの意図しない操作、なりすまし攻撃と対策

☠ クリックジャッキング

一見無害に見える罠ページの上にターゲットサイトを透過状態でかぶせる。
「続きを見る」などのクリック操作を誘い、ユーザーがそれをクリックして
しまうと、実際にはその上に透明で存在するターゲットサイトの実行ボタンを
押す事になり、ユーザーの意図しない操作が実行されてしまう。

・サイトA(プログラムが起動するページ)
・悪意あるページ(騙すための表示)



これらのページはiframe等に入れられ、サイトAはCSSにより
透明に設定され利用者には見えない。利用者は悪意ある
ページの①と②をクリックしているつもりでいても、実際に
クリックされるのは、手前側に配置された(見えない)サイトAの
ボタンとなる。結果、利用者は意図しない画面操作をさせられてしまう。

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

ユーザーの意図しない操作、なりすまし攻撃と対策

サイトのiframe内の埋め込みを制御するHTTPヘッダを設定

HTTPヘッダー「X-FRAME-OPTIONS」をDENYに設定することにより、他サイトの中にiframeで埋め込まれないようにする。

・DENY
全てのサイトからフレームで埋め込まれる事を拒否。

・SAMEORIGIN
読み込み元が同じドメイン、同じプロトコル、同じポートの場合にのみ、フレームで埋め込まれる事を許可。

・ALLOW-FROM
指定されたドメイン、またはURIからのみ、フレームで埋め込まれる事を許可。
（ブラウザによって挙動が異なる場合がある為注意）

※DENYに設定しても、そのサイトがフレームを利用する事は可能。

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

- ログインを狙う攻撃と対策
- ユーザーの意図しない操作・なりすまし攻撃と対策
- セッションを狙う攻撃と対策
- 入力、出力に潜む脆弱性と対策
- その他の脆弱性、注意点

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

セッションを狙う攻撃と対策

セッションとは

ステートレスなHTTP(S)プロトコル上のアプリケーションでは、セッションを用いて擬似的にステートフルな振る舞いをさせている。

通常は有効期限を設定したセッションIDをCookieに持たせてセッションの継続を実現する。
古くはセッションIDをHiddenタグやURLのクエリパラメータとして持ち回るアプリケーションも存在したが、セッションID流出の危険性が高く、現在ではアンチパターンとされる。
以降の説明ではCookieにセッションIDを持つアプリケーションを想定する。

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

☠セッションを狙う攻撃と対策

☠セッションハイジャック

ターゲットユーザーのCookie内のセッションIDを不正に入手し、自身のPCのCookieに書き込む事により、ターゲットユーザーになりすまして個人情報を盗む、改ざんする、不正な注文を行うなどののっとりを行う攻撃。

ターゲットユーザーのCookieのセッションIDを取得する方法は
・ターゲットユーザーのPCから直接取得する
・ブラウザのセキュリティホールを利用して取得する（クッキーモンスターバグ）
・マルウェアを感染させて取得する
・通信経路でパケットを盗聴する
・偽の無線APに接続させてhttps→http→443ポートと通信を流しSSLを外して盗聴する
・XSSの脆弱性を利用して別サーバーに送信させる
など

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

セッションを狙う攻撃と対策

サーバー側セッションに有効期限を設定する

一定時間アクセスが無い場合、サーバー側でそのセッションを無効にする。
AjaxやiframeハートビートⅠ等で定期的にポーリングしているアプリケーションの場合は明示的にタイムアウトさせる必要がある。

SSL通信を必須にする（非SSLを拒否、またはSSLにリダイレクトさせる）

通信経路からの盗聴を防ぐ

セッションIDのCookieに適切なオプションを付ける

・Expire(満了日付) またはMax-age(有効期間の秒数)を設定する
・Domainを指定しない（範囲を最小にする）
・Pathを適切に設定する
・HttpOnlyをtrueにする
・SecureOnlyをtrueにする

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

☠セッションを狙う攻撃と対策

☠セッション固定攻撃（セッション・フィクセーション）

既に攻撃者がターゲットサイトで発行済みのセッションIDを、ターゲットユーザーのブラウザのCookieに対し強制的に設定してからターゲットサイトにログインさせる事により、そのセッションIDがターゲットユーザーのセッションにすり替わる為、個人情報を盗む、改ざんする、不正な注文を行うなどののっとりが可能となる攻撃。

ターゲットユーザーにセッションIDを強制的に設定する方法は、セッションハイジャックの手法がほぼ全て利用可能だが、加えてURLのクエリにセッションIDを設定したリンクを踏ませるなど、プログラム言語やフレームワークの機能を悪用して固定できる場合もある。

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

セッションを狙う攻撃と対策

サーバー側セッションに有効期限を設定する

一定時間アクセスが無い場合、サーバー側でそのセッションを無効にする

SSL通信を必須にする（非SSLを拒否、またはSSLにリダイレクトさせる）

通信経路からの盗聴を防ぐ

セッションIDのCookieに適切なオプションを付ける

・Expire(満了日付) またはMax-age(有効期間の秒数)を設定する
・Domainを指定しない（範囲を最小にする）
・Pathを適切に設定する
・HttpOnlyをtrueにする
・SecureOnlyをtrueにする

ログイン時にセッションIDを変更する

ログインが成功した時点で、既存のセッションIDを破棄(無効化)し、新しいセッションIDを払い出す。

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

- ログインを狙う攻撃と対策
- ユーザーの意図しない操作・なりすまし攻撃と対策
- セッションを狙う攻撃と対策
- **入力、出力に潜む脆弱性と対策**
- その他の脆弱性、注意点

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

入力、出力に潜む脆弱性と対策

種類	タグ	通常状態	無効状態
テキスト	<input type="text">	テキスト	テキスト
パスワード	<input type="password">	••••••••	••••••••
ラジオボタン	<input type="radio">	◉選択肢1-1 ○選択肢1-2	◉選択肢2-1 ○選択肢2-2
チェックボックス	<input type="checkbox">	☑選択肢1-1 ☐選択肢1-2	☑選択肢2-1 ☐選択肢2-2
ファイル	<input type="file">	参照... ファイルが選択されていません。	参照... ファイルが選択されていません。
テキストエリア	<textarea>	テキストエリア	テキストエリア
セレクトボックス	<select><option>	選択肢1-1	選択肢2-1
日付	<input type="date">		
時刻	<input type="time">		
レンジ	<input type="range">		
色	<input type="color">		
送信ボタン	<input type="submit">	送信	送信
リセットボタン	<input type="reset">	リセット	リセット
汎用ボタン	<input type="button">	ボタン	ボタン
	<button>	ボタン	ボタン

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

入力、出力に潜む脆弱性と対策

SQLインジェクション

不正なSQLクエリを発行し認証をパススルーしたり、DBデータの不正取得、改ざん、破壊、
ストアドプロシージャを利用してサーバーの乗っ取りを行う攻撃。
ex) シングルクォート(')、コメント化(--) など

OSコマンドインジェクション

シェル機能を悪用し情報漏えい、ファイルの改ざん・削除、不正なシステム操作、
ウィルスなどのマルウェア感染、踏み台にされ他サイトへ攻撃などを行う攻撃。
ex) セミコロン(;)、パイプ(|) など

ディレクトリートラバーサル

パスやファイル名のメタ文字を悪用し、Webサーバーのディレクトリパスをさかのぼったり
横断し、公開されていないディレクトリにアクセスする攻撃。
ex) ドットドットスラッシュ(../)、ドットドットバックスラッシュ(..¥) など

※インクルードファイルや設定ファイル、ログファイルの権限設定が不適切でブラウザなどから
直接参照可能な場合も含まれる。（強制的ブラウジング）

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

入力、出力に潜む脆弱性と対策

メールヘッダーインジェクション

入力値を利用してメールを送るアプリケーションにおいてメールヘッダを改ざんし、件名や送信元、本文の改ざん、迷惑メールの送信に悪用、ウイルス（マルウェア）メールの送信に悪用する攻撃。
改行文字(¥r¥n) など

HTTPヘッダーインジェクション

入力値を利用してLocation等のHTTPヘッダーを設定するアプリケーションにおいて
HTTPヘッダーを改ざんし、意図しないHTMLやJavaScriptなどをレスポンスさせる攻撃。
フィッシングやクロスサイトスクリプティング、セッションハイジャック等あらゆる攻撃に
繋げる事が可能。
改行文字(%0d%0d) など

クロスサイトスクリプティング（XSS）

掲示板やSNS、レビューサイト等、入力値を別のユーザーが閲覧できるアプリケーションにおいて、意図しないHTMLタグやJavaScriptを含ませる攻撃。フィッシングやクロスサイトスクリプティング、セッションハイジャック等あらゆる攻撃に繋げる事が可能。
不等号(<>)、特殊文字(<) など

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

入力、出力に潜む脆弱性と対策

- サニタイズ（無害化）を正しく行う

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

入力、出力に潜む脆弱性と対策

サニタイズの流れ

1．補正（トリム、ノーマライズ）
2．事前検証（プリバリデーション）
} クライアントサイド

3．検証（バリデーション）
4．メタ文字のエスケープ
} サーバーサイド

・入力値の検証はサーバーサイドで実装する（UIに依存しない）
・前工程で実施済みの処理であっても、エスケープ処理はあらためて行う。（バリデーションはエスケープの代用にならない）
・エスケープは必要になる直前で行う
・SQLインジェクションのエスケープはフレームワークの機能を使う（自前で実装しない）
・外部からのパラメータでOSコマンドやファイルを直接指定しない
・インジェクションの手法はブラウザやプログラミング言語、フレームワークのエスケープ処理の脆弱性を利用される事がある（フィルターバイパス）
　HEX、BASE64、URLエンコード、HTML特殊文字（「文字実体参照」「数値文字参照」）
　改行コード、Tabコード、空白コードなど。

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

入力、出力に潜む脆弱性と対策

- **入力値の検証はサーバーサイドで実装する（UIに依存しない）**
- **前工程で実施済みの処理であっても、エスケープ処理はあらためて行う（バリデーションはエスケープの代用にならない）**
- **エスケープは必要になる直前で行う**
- **SQLインジェクションのエスケープはフレームワークの機能を使う（自前で実装しない）**
- **外部からのパラメータでOSコマンドやファイルを直接指定しない**
- **インジェクションの手法はブラウザやプログラミング言語、フレームワークのエスケープ処理の脆弱性を利用される事がある（フィルターバイパス）**
  HEX、BASE64、URLエンコード、HTML特殊文字（「文字実体参照」「数値文字参照」）
  改行コード、Tabコード、空白コードなど。

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

- ログインを狙う攻撃と対策
- ユーザーの意図しない操作・なりすまし攻撃と対策
- セッションを狙う攻撃と対策
- 入力、出力に潜む脆弱性と対策
- その他の脆弱性、注意点

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

その他の脆弱性、注意点

- 個人情報やカード情報をログに残さない
- デバックモード、デバッグオプションの起動はクエリやヘッダー等のスイッチだけに頼らずソースIPも確認する
- HTMLやJavaScriptに攻撃や進入のヒントに繋がるようなコメントを残さない
- エラーメッセージにOSやプログラム言語名、バージョンを表示しない
- デバッグ目的のエラーメッセージを出力しない
  （独自のエラーコードを発行しログで突合させる）

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

webカメラ位置

まとめ

生配信中

ご要望・ご質問は
チャットワークで受付中です。

☠ 死亡フラグまとめ

- ☠ 昔から使ってるシステムだから大丈夫
- ☠ 大した情報がないから大丈夫
- ☠ 使ってる人が少ないから大丈夫
- ☠ 先輩が作った所だから大丈夫
- ☠ 他社のサービスだから大丈夫
- ☠ 他の人が作った所だから良く分からない
- ☠ 古いプログラム言語、フレームワークだから良く分からない

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。

安心して開発者生活をおくるために

- 攻撃手法と対策を正しく、全て身に付ける（正確性、網羅性）
- 脆弱性診断ツールを使う（Owaspzap/WebInspect等）
- プログラム言語やフレームワークの脆弱性情報を常にキャッチし
  即座に対応できるフローを作る
- アプリケーションの一覧表を作る
  （管理チーム名や個人情報の有無、脆弱性の最終診断日、
  プログラム言語、フレームワーク名、バージョンなど）
- セキュリティポリシーを決める
- SQLインジェクションは絶対ダメ！

webカメラ位置

生配信中

ご要望･ご質問は
チャットワークで受付中です。

今日からもう一度はじめよう
セキュアWEBアプリケーション開発

webカメラ位置

生配信中

ご要望・ご質問は
チャットワークで受付中です。