

鳥取湖陵高校 2年生
情報セキュリティ講座

外部公開用

サイバー攻撃を疑似体験しながら学ぶ ～攻撃からシステムを守るために必要なことを考える～

2026年7月14日（火）

講師紹介

○若林 遥大（わかばやし はると）

▶ 静岡大学 大学院総合科学技術研究科 情報学専攻 1年

→ 情報セキュリティ教育やプログラミング教育などについて研究

○一昨年より、湖陵高校での情報セキュリティ講座に関与

▶ 今年度もそのご縁で開催します

本日の内容

1. 情報セキュリティの基本

▶情報セキュリティとは？

2. 不正アクセスとその対策

- ①公開された情報から，個人情報抽出してみよう
- ②データベースを不正に操り，情報を盗む
- ③サービスを安定的に提供するために必要なことって何だろう？

3. おわりに

1. 情報セキュリティの基本

○そもそも「情報セキュリティ」って何だろう？

- ▶ ウイルス対策
- ▶ 迷惑メール・架空請求
- ▶ SNSの使い方・闇バイト など

○「情報セキュリティ」= 情報の安全を守る対策

- ▶ 情報の盗難・破壊・サービス提供の妨害からどれだけ守れるか！
→ コンピュータのデータ，個人情報，機密情報など
- ▶ 個人だけでなく，企業や公的機関までもが被害を受ける時代に…
→ 間違いなく他人ごとではないが，どうすればいいのだろうか？

1. 情報セキュリティの基本

○「情報セキュリティ」の定義

▶日本産業規格（JIS : Japanese Industrial Standards）

→情報の機密性・完全性・可用性を維持すること（JIS Q 27000）

	用語の意味	主な対策
機密性	アクセス許可された人だけが、 情報を扱うことができること	暗号化
完全性	情報が最新で正確であり、 欠損がないことが保証されること	電子署名 なりすましや改ざんを防ぐための 電子的な署名
可用性	アクセスを許可された人が、 いつでも情報にアクセスできること	システムの冗長化 障害に備えて、予備の設備など バックアップを運用しておく

1. 情報セキュリティの基本

○「不正アクセス」とは？

- ▶ 正当な権限を持たないものが、ネットワークを通じて情報システムに不正にアクセスすること

○主な不正アクセスの事例

- ▶ なりすまし
→ アカウントの乗っ取り・不正なプログラムの実行 など
- ▶ 改ざん
→ 情報の書き換え・暗号化して利用不可にする など
- ▶ 盗聴
→ 個人情報や機密情報を不当に収集・第三者に公開 など

1. 情報セキュリティの基本

○「不正アクセス」がどのように発生するのか…

①調査（事前調査）

→「脆弱性のある入り口ないかな～、あれここなら突破できるかも」

②発見（権限取得）

→「パスワード解析して、正規のユーザーのふりをするぞ～」

③攻撃（不正実行）

→「アクセスできたから、ファイル盗んだり、削除して邪魔するぞ」

→「このユーザーの友達や仕事仲間にも攻撃を仕掛けるぞ～」

④制御（後処理）

→「また来るときのための通路の準備しとこうかな～」

→「不正アクセスした証拠を隠滅しとこう」

2. 不正アクセスとその対策

①公開された情報から，個人情報抽出してみよう

○サイバー攻撃のための情報収集

- ▶特定の相手を狙う攻撃では，まず情報収集から始まります
 - インターネット上に公開されている情報から抽出する
 - やみくもに攻撃するわけではない（現実の泥棒と同じ）

○ネット上に公開されている情報から，個人情報が特定できる！？

- ▶嘘のような話だけど，本当…
- ▶Googleのストリートビューを利用したゲームも話題だよね…
 - どこにいるかを周囲の電柱やガードレールなどから特定する

2. 不正アクセスとその対策

①公開された情報から，個人情報抽出してみよう

○誰が攻撃をしてくるかはわからない

▶名前を公開していなければ安心なのか？

→フォロワーや共通の友人，プロフィール欄などから集めることも

→身近な人が悪意をもってやってくるケースもある

○「OSINT」とは？

▶Open-Source Intelligence

→誰でも入手可能な膨大な情報の中から，必要な情報を収集・分析

→セキュリティ対策や犯罪捜査などで活用される

→攻撃者だけが利用する技術ではない

2. 不正アクセスとその対策

①公開された情報から、個人情報を抽出してみよう

○教材を開きましょう

コンテンツ一覧

公開中  ①公開された情報から、個人情報を抽出してみよう

何気ない投稿には個人情報がいっぱい！？
SNSの投稿から個人情報を収集して、秘密の質問を突破してみよう。

公開中  ご参加いただきありがとうございます！

本日は、鳥取湖陵高校 2年生 情報セキュリティ講座「サイバー攻撃を疑似
いただきありがとうございます。

Web教材システムとお手元に配布した資料を利用して講座を進めます。

青色の文字をクリックすると
教材が開きます

SNS情報漏洩シミュレータ : <https://visusec.jp/app/SNSLeakSimulator/>

2. 不正アクセスとその対策

①公開された情報から，個人情報抽出してみよう

Mockitter

ターゲットに戻る



佐藤 ユキ

@sato_yuki

大学生！毎日楽しい！無言フォロー歓迎

6  投稿 4  フォロー 1  フォロワー 1  いいね



佐藤 ユキさんがリポスト

懸賞プレゼントBot @gift_bot

🎁 秋の大還元祭 🎁 抽選で100名様にAmazonギフト券1000円分が当たる！この投稿をリポストで応募完了！

👍 124  3  3

2024/10/25 12:00



佐藤 ユキさんがリポスト

Sparkle Girls 公式 @idol_official

🌟 冬の全国ツアー決定！🌟 チケット先行受付は明日からスタートです！

👍 210  2  2

2024/10/20 18:00



佐藤 ユキ @sato_yuki

ついに20歳になりました！お酒解禁 🍷

👍 2  0  1

2024/10/10 00:05

OSINT パスワード突破演習

ターゲットの公開情報（OSINT）を収集し、パスワード再設定画面の「秘密の質問」を突破してください。
※投稿をクリックすると詳細（返信スレッド）が見られます。「❤️いいね」の数からも情報が探せます。

演習シナリオの選択

無防備なプロフィールと投稿

パスワード再設定

ターゲットID

@sato_yuki

質問1: 生年月日は？ (例: 2004/01/01)

回答を入力

質問2: 出身の都道府県は？

回答を入力

再設定を実行

2. 不正アクセスとその対策

①公開された情報から，個人情報を抽出してみよう



パスワード再設定

ターゲットID

@sato_yuki

質問1: 生年月日は? (例: 2004/01/01)

回答を入力

質問2: 出身の都道府県は?

回答を入力

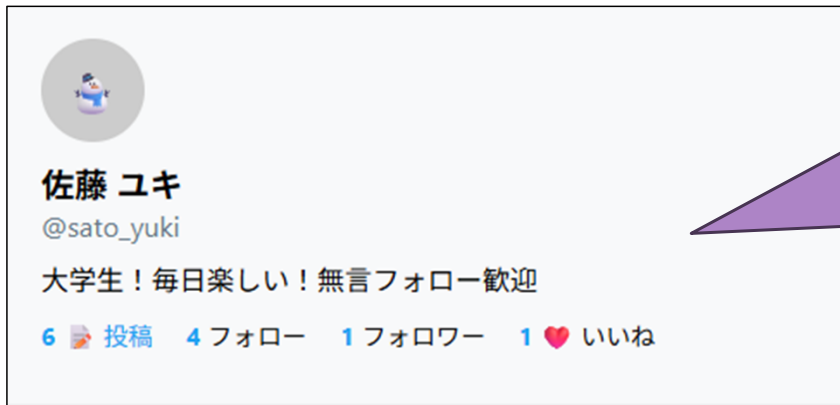
再設定を実行

SNSに投稿された情報から，
パスワードを忘れたときの
合言葉を探して不正な
アクセスを試みます

この2つの回答を
探してみましょう！

2. 不正アクセスとその対策

①公開された情報から，個人情報を抽出してみよう



「佐藤 ユキ」さんという
大学生のようです

まずは，生年月日を
探したいのですがプロフィール
には表示されていません...

2. 不正アクセスとその対策

①公開された情報から，個人情報を抽出してみよう



何気ない日常を
投稿しているようですね

誕生日がわかるきっかけは
ないでしょうか？

2. 不正アクセスとその対策

①公開された情報から，個人情報を抽出してみよう



直接的に生年月日は言っていないが，20歳になったことを投稿していますね

投稿日から逆算できるのでは？
→ 2004/10/10

2. 不正アクセスとその対策

①公開された情報から，個人情報抽出してみよう

演習シナリオの選択

無防備なプロフィールと投稿

無防備なプロフィールと投稿

フォロワー（家族）からの漏洩

横断的な調査（引用リポストと文脈）

画像解析と自然な秘密の質問

芋づる式・連帯責任（返信といいね）

【実践級】複合OSINT調査（タケル編）

他にもいろいろな
シチュエーションがあります
10分間とりますので、
チャレンジしてみてください

必要な情報が見つからないと
きは、「いいね」の一覧から
別のユーザーの投稿を見に行
くといいかも

2. 不正アクセスとその対策

①公開された情報から，個人情報抽出してみよう

○「OSINT」で自宅や職場が特定されることも…

- ▶犯罪につながる可能性（ストーカーや詐欺など）
- ▶アカウントを忘れた時の，秘密の質問の特定につながる可能性も
→秘密の質問に真面目に答えないことも大切！

○ネット上に日常を公開するときは，個人が特定される情報には注意する

- ▶今の時代投稿するべきでないとは，言えない
→リスクがあることは必ず理解すること
- ▶SNSのプロフィール欄に，学校名・クラス・部活など書いてない？
→フォロワーから芋づる式にほかの人に迷惑が及ぶ可能性も

2. 不正アクセスとその対策

①公開された情報から，個人情報抽出してみよう

○システムを設計するうえで考えないといけないこと…

- ▶利用者は覚えやすい情報を認証情報に利用してしまうことがある
→アカウントの乗っ取りに悪用できてしまう
- ▶個人情報を含んだパスワードは覚えやすいのも事実…
→結局どれだけ禁止しても，うまいこと回避されてしまう
- ▶調べたら出てくるものもある・巧妙に聞き出せる場合も
→「そういえば，出身ってどこだっけ？」

2. 不正アクセスとその対策

①公開された情報から，個人情報抽出してみよう

パスワードを忘れた場合

最初のペットの名前は?	▼
答え	
生まれた場所の名前は?	▼
答え	
いちばん年上のいとこの名前は?	▼
答え	

皆さんは，バカ真面目に
答えてないですね？

とあるOSのユーザー作成の時に
毎回求められて正直面倒です

2. 不正アクセスとその対策

①公開された情報から，個人情報抽出してみよう

○これから，パスワードはどうすべきなんだろうか

- ▶本人がきちんと管理できる

- 覚えやすくないと本質的には意味がない

- でも覚えやすいものって，推測しやすくなる可能性が高い

- ▶複数の文字種を組み合わせる・桁数を多くさせる

- システムとしては安全になる

- 利用者は面倒に感じる

2. 不正アクセスとその対策

①公開された情報から，個人情報抽出してみよう

○これから，パスワードはどうすべきなんだろうか

- ▶誰でも使いやすい認証を実現するにはどうすればよいのだろうか
→情報化は避けて通れない（高齢者でもスマホを持つ時代）
- ▶利用者の行動を前提にした設計も必要なのかもしれない
→いい意味でも，悪い意味でも
- ▶実社会でも，パスワードを用いないシステムも増えてきた
→パスキー・生体認証・ワンタイムパスワード
→新技術を面倒くさく感じる層も一定するいるわけだが…

2. 不正アクセスとその対策

①公開された情報から、個人情報抽出してみよう

○少し考えてみよう！（近くの人と相談OK）

- ▶「母親の旧姓は？」「ペットの名前は？」といった『秘密の質問』は、本人確認の方法として安全でないと言われるのはなぜでしょうか？理由を考えてみてください。

コンテンツ一覧

公開中

 ディスカッション①

ディスカッション①の回答フォームです。
周りの人と相談しながら、自身の回答をまとめて教えてください。

確認する

コメント(0)

公開中

 ご参加いただきありがとうございます！

2. 不正アクセスとその対策

② データベースを不正に操り，情報を盗む

○データベースを不正に操り，情報を盗む

- ▶正しいパスワードを入力せずにログインできるシステムってあるの？
 - パスワードを強固にした意味が全くない
 - 個人情報流失したらどうしよう…

○Webアプリケーションにおいて利用者を識別する仕組み

- ▶ID（メールアドレス など）とパスワードを入力するのが一般的

○IDとパスワードをどのように管理して認証しているんだろう

- ▶データベース

2. 不正アクセスとその対策

② データベースを不正に操り，情報を盗む

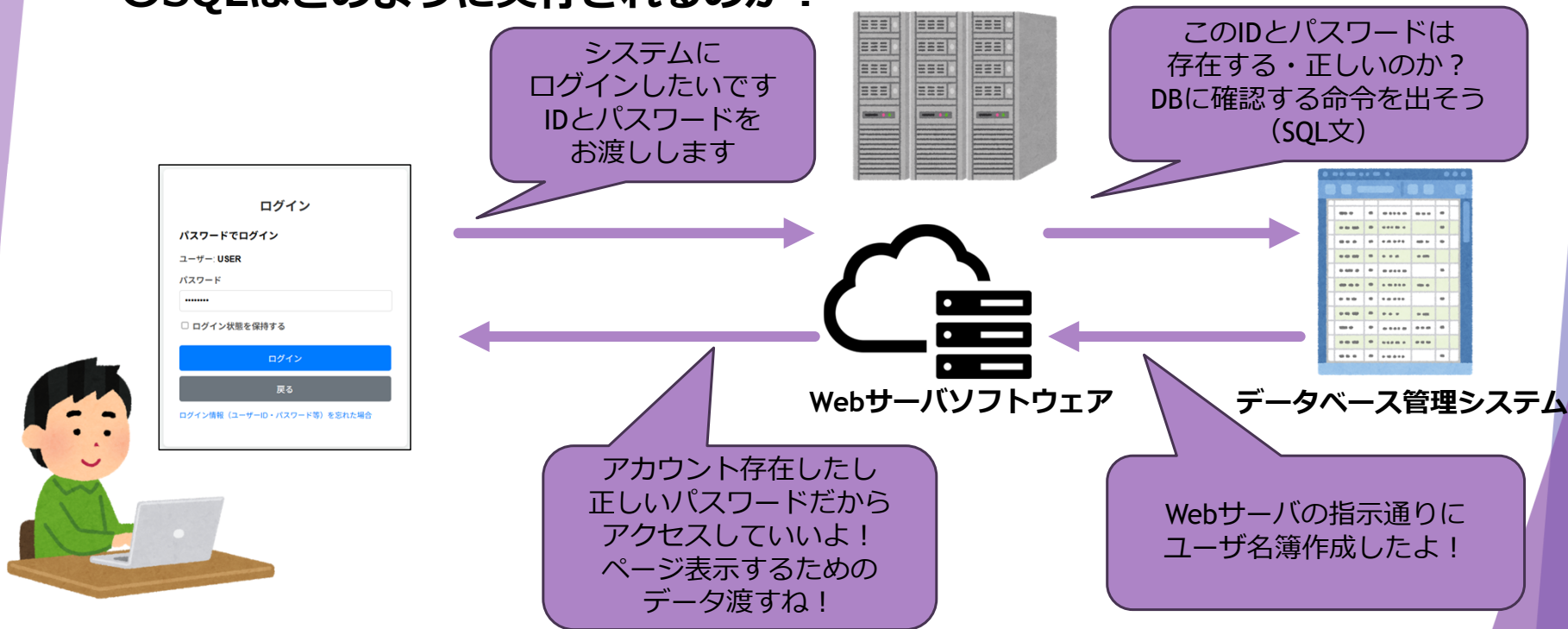
○データベースとは…

- ▶ 検索や管理を容易にできるように整理された情報の集まり
 - ユーザリスト
 - 商品リスト
 - 電子カルテ
- ▶ SQLで操作
 - データベースを管理するための命令語

2. 不正アクセスとその対策

② データベースを不正に操り，情報を盗む

OSQLはどのように実行されるのか？



2. 不正アクセスとその対策

② データベースを不正に操り，情報を盗む

OSQLはどのように実行されるのか？

ログイン

パスワードでログイン

ユーザー USER

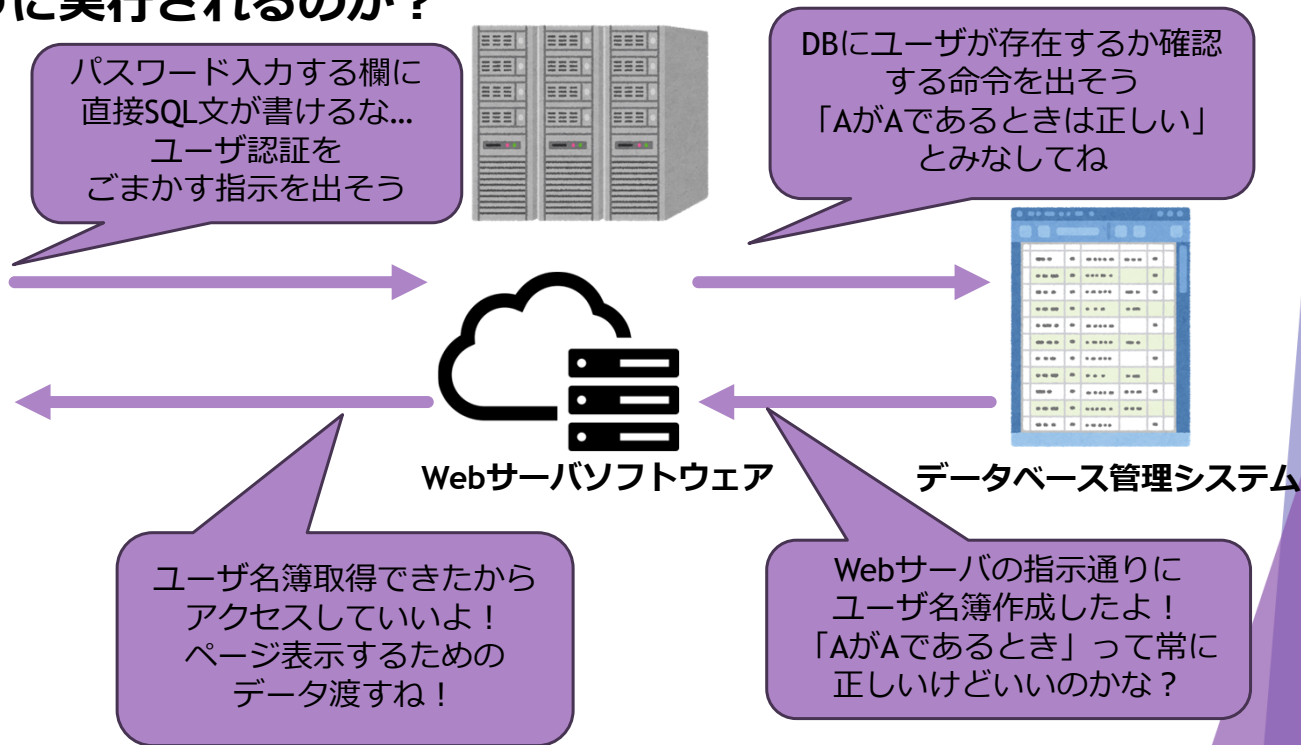
パスワード

☐ ログイン状態を保持する

ログイン

戻る

ログイン情報（ユーザーID・パスワード等）を忘れた場合



2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

OSQLインジェクション攻撃

- ▶ データベースに送信するデータの中にSQL文を混入する
→ サービス提供者の意図しない不正な操作をすること
- ▶ 不正なログインが可能に
→ ユーザ認証をごまかす
- ▶ データベースのデータをすべて削除される
→ 編集や削除の指示をすることによって可能

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

コンテンツ一覧

公開中  ② データベースを不正に操り、情報を盗む

アカウント管理ページに不正ログインして個人情報を盗む攻撃を体験することを通して、適切なセキュリティ管理の重要性を学ぶ

公開中  ご参加いただきありがとうございます！

本日は、鳥取湖陵高校 2年生 情報セキュリティ講座「サイバー攻撃を疑似体験」にご参加いただきありがとうございます。

Web教材システムとお手持に配布した資料を利用して講座を進めます。

青色の文字をクリックすると
教材が開きます

SQLインジェクション攻撃 : <https://visusec.jp/app/SQLInjectionAttack/>

2. 不正アクセスとその対策

② データベースを不正に操り，情報を盗む

○演習の想定

- ▶社内システムのログイン画面に脆弱性があります

○どのような脆弱性があるのか…

- ▶パスワードの入力欄にSQL文を記述することが可能です
→認証するときにそのままSQL文を送信してしまいます
- ▶不正にログインすることで個人情報すべて閲覧できます
- ▶すべてのユーザのパスワードが閲覧できます
→詳しい説明は，後ほどします

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

○お題1：正しいパスワードを入力することなくシステムにログインする

Part.1: 正しいパスワードを入力することなく、システムに不正にログインする

いくら難しいパスワードを設定していても、システムに欠陥があると無意味です。正しいパスワードを入力することなく欠陥を悪用して不正にログインして重要な情報を盗んでみましょう。

[Part.1へ](#)

2. 不正アクセスとその対策

② データベースを不正に操り，情報を盗む

○お題1：正しいパスワードを入力することなくシステムにログインする

▶まずは普通にログインしてみましょう

従業員情報管理ページ
ログイン

メールアドレスまたは従業員ID
admin

パスワード
password

ログイン

IDに「admin」パスワードに「password」と入力してください

初期アカウントとパスワード
あるあるですね...絶対だめですよ！

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

○お題1：正しいパスワードを入力することなくシステムにログインする

▶まずは普通にログインしてみましょう

SQLインジェクションの体験ページ Part.1

正しいパスワードを入力することなく、ログインできてしまいました....
従業員の個人情報もパスワードも流失してしまいました。
パスワードを他のサービスでも流用していたら、被害が拡大してしまいます....

従業員情報 管理ページ

名前	従業員ID	メールアドレス	パスワード	住所	電話番号	誕生日
管理者	admin	admin@toru-tori.co.jp	password	月影県影原市月町13-14-15 株式会社取鳥 4F サーバー管理部門	080-5678-901	2024/04/01

ログアウト

普通にログインできました
なんも不思議な点は
ありません...

まあ、実はこれが
怖いところなんです...

確認出来たら「ログアウト」
しておいてください

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

○お題1：正しいパスワードを入力することなくシステムにログインする

▶では、不正にログインをしてみましょう

○その前に、以下の言葉を聞いてどう思いますか？

▶AがAであるとき正しい

→かなり違和感があるけど、まあそうだよね

▶「 $1=1$ 」という等式は正しい

→これも当たり前だよね

2. 不正アクセスとその対策

② データベースを不正に操り，情報を盗む

○お題1：正しいパスワードを入力することなくシステムにログインする

▶では，不正にログインをしてみましょう

従業員情報管理ページ
ログイン

メールアドレスまたは従業員ID

パスワード

ログイン

IDは入力しなくていいです
パスワードを以下のように
入力してください

' OR 'A' = 'A'

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

○お題1：正しいパスワードを入力することなくシステムにログインする

▶本来は、本人の情報しか取得しない仕組みなのですが…

SQLインジェクションの体験ページ Part.1

正しいパスワードを入力することなく、ログインできてしまいました…。

従業員の個人情報もパスワードも流失してしまいました。

パスワードを他のサービスでも流用していたら、被害が拡大してしまいます…。

従業員情報 管理ページ

名前	従業員ID	メールアドレス	パスワード	住所	電話番号	誕生日
管理者	admin	admin@toru-tori.co.jp	password	月影県影原市月町13-14-15 株式会社取鳥 4F サーバー管理部門	080-5678-901	2024/04/01
井上 花子	hanako	hanako.inoue@tori-mail.com	9jTpMn3b	虹川県夢見市光町10-11-12	090-4567-890	1993/04/18
佐藤 一郎	i-sato	i-sato@tanuki-mail.com	Gf4z2PmA	青影県幻影市虚町1-2-3	090-1234-567	1990/01/15
鈴木 勇	i-suzuki	isamu.suzuki@mail.usagi.com	R6p2Btl.s	星海県夜空市星町7-8-9	070-3456-789	1995/03/12
高橋 恵子	k-taka	k.takahashi@neko-mail.com	b9lp3YxN	霧山県幽谷市霞町4-5-6	080-2345-678	1988/02/20

ログアウト

あれ…
ログインできた…
個人情報丸見え…

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

○お題2：対策済みのログインページでも確認しておこう

Part.2: 正しい対策するとどうなるか確認する

正しいパスワードを入力しないとログインできないことを確認します。万が一不正にログインされたときに被害を最小限にする工夫についても併せて学びましょう。

Part.2へ

2. 不正アクセスとその対策

② データベースを不正に操り，情報を盗む

○お題2：対策済みのログインページでも確認しておこう

▶不正ログインを試しておきましょう

従業員情報管理ページ
ログイン

メールアドレスまたは従業員ID

パスワード

ログイン

IDは入力しなくていいです
パスワードを以下のように
入力してください

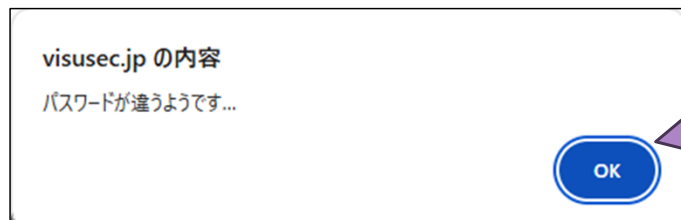
' OR 'A' = 'A'

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

○お題2：対策済みのログインページでも確認しておこう

▶不正ログインを試しておきましょう



当然ログインできないですね

もしできるなら、世の中の
システム不正し放題ですよ(笑)

違いは後ほど説明します

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

○お題：正しいパスワードを入力することなくシステムにログインする

▶なぜログインできたのか

○DBに確認する命令に問題が...

▶SELECT * FROM USERS WHERE id = '\$id' AND pass = '\$pass'

→変数として入力した内容をそのまま検索の命令に利用...

SQL文	役割
SELECT * FROM USERS	USERSテーブルの一覧を取得したいです
WHERE	検索条件を次に示します
id = '\$id' AND pass = '\$pass'	idに関する情報が入力した変数idと一致するとき さらにpassに関する情報が入力した変数passと一致するとき

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

○理解してほしいこと

- ▶ SQL文を利用するときに入力された情報をそのまま利用するのは危険
 - 危険だけど認証するには入力された情報を利用する必要がある…
 - 何らかの形で処理をする？
- ▶ 情報の流失や破壊につながる
 - DBをつかさどる命令を外部からされることは非常に危険
 - 大事なデータなどの資産喪失
 - 顧客からの信頼の喪失・売り上げにおける損失
- ▶ この類のトラブルは、ほとんどが人為的なミスであること

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

○おまけ：なんで人為的なミスが発生するのだろうか

▶ OSやソフトウェアのアップデートをしていないから

→ Windowsの更新とかずさんなところは結構多い

▶ 最新の情報セキュリティの動向を追いかけていないから

→ これは結構大変だけど、アンテナを常に張ることは大切

▶ 楽に実装できるから

→ エスケープ処理のひと手間が面倒に感じる

→ 試作段階で仮実装したものが本番環境に…

→ 納期や開発スケジュールに追われ、十分な確認ができないことも…

2. 不正アクセスとその対策

② データベースを不正に操り、情報を盗む

○少し考えてみよう！（近くの人と相談OK）

▶SQLインジェクションを防ぐには、開発にお金や時間がかかります。

「社内の人間しか使わないシステムなら、対策はお金をかけず適当でも良い」という考え方が危険である理由（なぜ対策が必要なのか）を考えて教えてください。

コンテンツ一覧

公開中

ディスカッション②

ディスカッション②の回答フォームです。
周りの人と相談しながら、自身の回答をまとめて教えてください。

確認する

コメント(0)

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

○サービスの提供を妨害するのも，サイバー攻撃

- ▶情報を盗んだり改ざんするだけが，妨害のやり方ではない
→アクセスできないようにする = 可用性を失わせる

ODoS / DDoS攻撃

- ▶サーバーに対して過剰なアクセスによってサービスを停止させること
→サービス提供を阻害する古典的かつ典型的な手法

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

ODoS攻撃とDDoS攻撃の違い理解していますか？

- ▶ DoS (Denial Of Service) 攻撃

- 攻撃者の端末から標的に過剰な負荷をかける攻撃

- ▶ DDoS (Distributed Denial Of Service) 攻撃

- 攻撃者とは別の人が持つ多数の端末を踏み台にしてDoS攻撃をする

ODoSとDDoS攻撃の違いによって攻撃方法以外に何が変わるのだろう？

- ▶ 理屈よりも体験してみよう

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

○教材を配信します

コンテンツ一覧

公開中  ③サービスを安定的に提供するために必要なことって何だろう？

DoS攻撃とDDoS攻撃の違いを理解できていますか？
それぞれの違いを実際体験しながら確認してみよう。

手動で対策する大変さと、セキュリティ強化と利便性のトレードオフも学ぼう。

公開中  ご参加いただきありがとうございます！

本日は、鳥取湖陵高校 2年生 情報セキュリティ講座「サイバー攻撃を疑似体験」
いただきありがとうございます。

Web教材システムとお手元に配布した資料を利用して講座を進めます。

青色の文字をクリックすると
教材が開きます

DDoS攻撃・防衛体験シミュレータ：<https://visusec.jp/app/DDoSDefenseSimulator/>

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

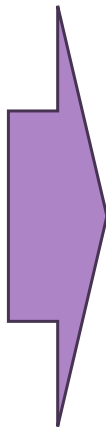


2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

操作方法を説明していきます

シナリオ進行「1: 平和な日常」をクリックしてください



2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

アクセスログを監視して, DoS / DDoS攻撃の前兆を見つけます

アクセス元 IPランキング (クリックで即時遮断)				
	10.0.1.204.220			12 Req/s
	10.0.1.241.146			8 Req/s
	10.0.1.160.200			8 Req/s
	10.0.1.122.244			8 Req/s
	10.0.1.173.127			8 Req/s

リアルタイム通信ログ				
属性	IPアドレス	パス	状態	判定
	10.0.1.78.102	/ticket	200	✓ 通過
	10.0.1.108.103	/ticket	200	✓ 通過
	10.0.1.150.212	/ticket	200	✓ 通過
	10.0.1.243.115	/ticket	200	✓ 通過
	10.0.1.180.159	/ticket	200	✓ 通過
	10.0.1.108.103	/ticket	200	✓ 通過
	10.0.1.94.235	/ticket	200	✓ 通過
	10.0.1.94.235	/ticket	200	✓ 通過

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

怪しい通信は，赤色の文字で示されます

アクセス元 IPランキング (クリックで即時遮断)				
	192.168.142.142.98			350 Req/s
	10.0.1.35.146			8 Req/s
	10.0.1.221.211			8 Req/s
	10.0.1.208.142			8 Req/s
	10.0.1.128.63			8 Req/s
リアルタイム通信ログ				
属性	IPアドレス	パス	状態	判定
	192.168.142.142.98	/login	200	✓ 通過
	192.168.142.142.98	/login	200	✓ 通過
	192.168.142.142.98	/login	200	✓ 通過
	192.168.142.142.98	/login	200	✓ 通過
	192.168.142.142.98	/login	200	✓ 通過
	192.168.142.142.98	/login	200	✓ 通過
	192.168.142.142.98	/login	200	✓ 通過

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

怪しい通信は，赤色の文字で示されます

アクセス元 IPランキング (クリックで即時遮断)

192.168.142.142.98	350 Req/s
10.0.1.35.146	8 Req/s
10.0.1.221.211	8 Req/s
10.0.1.208.142	8 Req/s
10.0.1.128.63	

リアルタイム通信ログ

属性	IPアドレス	リクエスト	レスポンス	ステータス
	192.168.142.142.98			
	192.168.142.142.98			
	192.168.142.142.98			
	192.168.142.142.98	/login	200	通過
	192.168.142.142.98	/login	200	通過
	192.168.142.142.98	/login	200	通過

同じIPアドレスから
攻撃を受けています！
ブロックが必要です

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

怪しい通信を，IP BAN（ブロック）してください！

アクセス元 IP ランキング (クリックで即時遮断)

🇯🇵 192.168.142.142.98	350 Req/s
🇯🇵 10.0.1.35.146	8 Req/s
🇯🇵 10.0.1.221.211	8 Req/s
🇯🇵 10.0.1.208.142	8 Req/s
🇯🇵 10.0.1.128.63	8 Req/s

リアルタイム通信ログ

属性	IP アドレス
🇯🇵	192.168.142.142.98
🇯🇵	192.168.142.142.98
🇯🇵	192.168.142.142.98
🇯🇵	192.168.142.142.98
🇯🇵	192.168.142.142.98
🇯🇵	192.168.142.142.98
🇯🇵	192.168.142.142.98

怪しい通信を見つけました！
1秒間に350リクエストも
しています

クリックすると
IP BAN（ブロック）されます

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

この時サーバー負荷が、100%にならないように気をつけてください
100%になると、サーバーが処理落ちしたことを示します



通常のアクセス時も
当然サーバーには負荷が
かかりますが、攻撃されると
著しく高い負荷がかかります



2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

それでは、DoS攻撃からシナリオを開始してください



2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

ODoS攻撃の特徴

▶ 攻撃の頻度

→500Req/s程度のアクセスがあると止まってしまう

→放置すると当然サーバーは停止してします

▶ 1台で攻撃できる能力には限界がある

→単純に端末の性能

→通信回線の速度など

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

ODoS攻撃の特徴

- ▶ 攻撃元が1つのIPアドレスだけ
→ 1度ブロックしてしまえば比較的容易に対応できる！

アクセス元 IPランキング (クリックで即時遮断)	
 192.168.116.204.198	500 Req/s
 10.0.1.167.8	4 Req/s
 10.0.1.139.249	3 Req/s
 10.0.1.77.147	2 Req/s
 66.249.66.1	1 Req/s

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

それでは、今度はDDoS攻撃のシナリオをやってみてください



2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

ODDoS攻撃の特徴

▶ 攻撃の頻度

→ DoS攻撃よりも1端末当たりのアクセス数は少ない

→ 小さい攻撃が束になって襲ってくるイメージ

▶ スマートカメラなどネットワークに接続された機器を踏み台にする

→ 性能よりも、複数のアクセス元に分散することに意味がある

→ 脆弱性がありながら、ネットワークに接続されている端末を悪用

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

ODDoS攻撃の特徴

- ▶複数のIPアドレスから攻撃が来る（攻撃元が複数となる）
 - ブロックしてもブロックしてもキリがない…
 - 実際は、小さい攻撃で来られると気が付きにくい場合もある

アクセス元 IPランキング (クリックで即時遮断)		
	172.16.10.129.244	25 Req/s
	172.16.10.203.57	25 Req/s
	172.16.10.254.181	25 Req/s
	172.224.98.214	25 Req/s
	172.85.151.40	25 Req/s

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

○手作業でのブロック（IP BAN）には限界がある

- ▶ 攻撃元が次々と変わるDDoS攻撃を人間が監視して防ぐのは不可能

○自動化する：WAF（Web Application Firewall）の活用

- ▶ サーバーへのアクセスを自動で監視・検査するシステム
→ 攻撃先は、Webサーバーだけとは限らない
- ▶ 異常な回数のアクセスや、攻撃特有の通信を自動で遮断する
→ 設定を誤ると健全な通信までも遮断する危険性はある
- ▶ 人の目だけでなく、システムでシステムを守る仕組みが必要

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

○ WAFの設定をチューニングしてみよう！

- ▶ 攻撃を完全に防ごうとして、制限を厳しくすると…
 - 正常なアクセスまで遮断してしまう（誤BANの発生）
- ▶ 逆に、制限を緩くしすぎると…
 - 攻撃をすり抜けさせてしまい、サーバーがダウンする

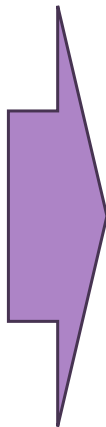
○ セキュリティと利便性の「トレードオフ」

- ▶ どちらかを立てれば、どちらかが立たなくなる関係性
 - シナリオ4で、最適なバランス（WAFの設定）を探してみよう！

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

WAFを操作してみよう！



2. 不正アクセスとその対策

③ サービスを安定的に提供するために必要なことって何だろう？



1秒間で60リクエストした
通信をブロックする設定

緩すぎて通過してしまっている

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？



2. 不正アクセスとその対策

③ サービスを安定的に提供するために必要なことって何だろう？



2. 不正アクセスとその対策

③ サービスを安定的に提供するために必要なことって何だろう？



悪意はないが、更新ボタン (F5) を連打していたユーザーがいた

厳しすぎるとこういったユーザーを誤ってBANするの原因になる (システム側が悪いとも言い難い...)

2. 不正アクセスとその対策

③サービスを安定的に提供するために必要なことって何だろう？

○少し考えてみよう！（近くの人と相談OK）

- ▶DDoS攻撃を防ぐ際、正常な利用者を誤ってブロックしてしまうリスクがあります。システムを運用する立場として、「正常な利用者を巻き込んででも攻撃を完全に防ぐことを優先する」か、「攻撃を少し見逃してでも正常な利用者の利便性を優先する」か、あなたはどちらの考えに近いですか？その理由も教えてください。

コンテンツ一覧

公開中

ディスカッション③

ディスカッション③の回答フォームです。
周りの人と相談しながら、自身の回答をまとめて教えてください。

確認する

コメント(0)

公開中

ご参加いただきありがとうございます！

3. おわりに

〇ここまでお疲れさまでした！

▶情報セキュリティについて少し詳しくなったでしょうか？

〇今回は攻撃者の目線を中心に講座を進めてきました

▶どこが狙われるのか（脆弱性）を客観的に知ることは重要です

→もちろん、実際のサービスに攻撃したら**犯罪です！！！！**

3. おわりに

○今日のまとめ

- ▶ SNSに投稿した内容や画像から住所などが特定される可能性が…
 - 投稿する前に一度立ち止まって、確認すること
 - 秘密の質問って仕組みとして適切なんだろうか…
- ▶ 今回のセキュリティ事例の多くは人為的なミス
 - SQLやOSコマンドといったシステムの核を露出させない
 - 楽に実装できる裏には、脆弱性が潜むことも少なくない

3. おわりに

○今日のまとめ

- ▶ システムの脆弱性や更新情報にアンテナを立てること
 - 人為的なミスに次ぐ原因は、ハードウェア・ソフトウェアの不良
 - OSやソフトウェアのアップデート, コミュニティからの情報収集
- ▶ サイバー攻撃を受けた時の被害を最小にすること
 - バックアップなどシステムの冗長構成を検討する

3. おわりに

〇もっと詳しく学びたいと思ったら

- ▶今回利用したWebアプリは視覚的な理解を重視しています
→実際の挙動と多少異なる点があります（極端な誤りはないです）
- ▶他にも様々な事例があります
→身近なものから、少しディープな世界まで
- ▶VISUSECでも様々な教材を提供中！
→ <https://visusec.jp/app/>

3. おわりに

○もっと詳しく学びたいと思ったら

- ▶ インターネットや文献などをぜひ調べてみてほしいです
 - 公的機関や企業などのサイトが信用性が高いです
- ▶ IPA（独立行政法人 情報処理推進機構）
 - 最新のセキュリティー事情や注意喚起などを提供している
 - <https://www.ipa.go.jp/security/index.html>

3. おわりに

○講座の内容・教材に関するお問い合わせ先

▶ 若林 遥大（ワカバヤシ ハルト）

Mail : wakabayashi.haruto@whr.jp