

2023/03/27

A04:安全の確認されない不安な設計

菅田大輔

目次

- A04:安全の確認されない不安な設計とは
- 補足：用語集
- 対策
- 具体的なシナリオ：秘密の質問
- OWASP Juice Shopにおける実践
- Meta Geo Stalking
- 原因
- 対策
- 実際の動き

A04:安全の確認されない不安な設計

安全が確認されない不安な設計とは、様々な脆弱性を表す広範なカテゴリです。

安全でない設計と安全でない実装は異なります。

対応する CWE 数	最大発生率	平均発生率	加重平均 (攻撃の難 易度)	加重平均 (攻撃によ る影響)	最大網羅率	平均網羅率
40	24.19%	3.00%	6.46	6.78	77.25%	42.51%

補足:用語集

- ・CWEs Mapped(カテゴリにあたるCWEの数): Top10チームがカテゴリにマッピングしたCWEの数です。
- ・Incidence Rate(発生率): 発生率とは、当年に機関によってテストされた母集団のうち、カテゴリにマップされたCWEに脆弱なアプリケーションの割合を示します。
- ・(Testing) Coverage(テスト)網羅範囲: カテゴリにマップされたCWEに対して、機関がテストできたアプリケーションの範囲。
- ・Weighted Exploit(重み付けされた悪用性): CVEに割り当てられているCVSSv2およびCVSSv3スコアの悪用性サブスコアを正規化し、10ptのスケールで表示したものです。
- ・Weighted Impact(重み付けされた影響度): CVEに割り当てられているCVSSv2およびCVSSv3スコアの影響サブスコアを正規化し、10ptのスケールで表示したものです。

対策

脅威モデリング:

開発対象のソフトウェアがどのようなセキュリティ脅威にさらされており、攻略される可能性を持ちうるかを洗い出す活動である。潜在するセキュリティ脆弱性を上流工程で見つけ出すことによって、より効果的に脆弱性を排除することを狙う。

- セキュリティおよびプライバシー関連の管理策の評価および設計を支援するために、アプリケーションセキュリティの専門家とともにセキュアな開発ライフサイクルを確立し使用する。
- セキュアなデザインパターンまたは、信頼性が高く安全性も検証されているコンポーネントライブラリを構築し使用する。
- 重要な認証、アクセスコントロール、ビジネスロジック、および暗号鍵の管理フローに脅威モデルを使用する。

具体的なシナリオ:秘密の質問

クレデンシャルの回復フローには「秘密の質問と答え」が含まれることがあります。「秘密の質問と答え」は、**NIST 800-63b**、**OWASP ASVS**、および **OWASP Top 10** で禁止されています。「秘密の質問と答え」は複数の人が答えを知ることができるため、アイデンティティの証拠として信頼できないためです。このようなコードは削除し、より安全な設計に置き換えるべきです。

クレデンシャル：
ネットワークセキュリティの世界で使用された場合には、IDやパスワードをはじめとする、ユーザ等の認証に用いられる情報の総称

ASVS:

OWASP ASVS Projectの活動を通じて開発された、最新のWebアプリケーションとWebサービスの設計、開発、テストに必要な機能的および非機能的なセキュリティコントロールの定義に焦点を当てたセキュリティ要件とコントロールのフレームワーク。

NIST 800-63b:

アメリカ国立標準技術研究所の認証に関するガイドライン

OWASP Juice Shopにおける実践

- Meta Geo Stalking : Determine the answer to John's security question by looking at an upload of him to the Photo Wall and use it to reset his password via the Forgot Password mechanism.
- Visual Geo Stalking : Determine the answer to Emma's security question by looking at an upload of her to the Photo Wall and use it to reset her password via the Forgot Password mechanism.

Meta Geo Stalking

- 概要


OWASP Juice Shopでは、パスワードを忘れた場合の復旧に「秘密の質問」を採用している。Johnの秘密の質問を、サイト内にあるJohnの投稿から推測し、パスワードを変更する。

- 脆弱性

1. パスワードの変更が、秘密の質問に答えるだけで完了してしまうこと。
2. 秘密の質問が、メールアドレスを知っている人間に表示されてしまうこと。

Meta Geo Stalking

1. Johnのメールアドレスを推測する。
Juice Shopで登録されているメールアドレスのドメイン名は @juice-sh.op であることが多かったなので、Johnの名前と合わせて john@juice-sh.opで検索してみる。
2. すると、秘密の質問が「What's your favorite place to go hiking?」であることがわかる。



The screenshot shows a 'パスワード再設定' (Reset Password) form. The 'メールアドレス *' (Email Address) field contains 'john@juice-sh.op'. The 'セキュリティ質問 *' (Security Question) field is highlighted with a red box and contains the text 'What's your favorite place to go hiking?'. A Firefox password manager popup is visible over the security question field, suggesting a password 'wugr5PYNjn9urM' and offering to save it. Below the security question is a '新しいパスワード(確認用) *' (New Password) field. At the bottom, there is a toggle for 'パスワードのアドバイスを表示' (Show password advice) and a '変更' (Change) button.

パスワード再設定

メールアドレス *
john@juice-sh.op

セキュリティ質問 *
What's your favorite place to go hiking?

Use a Securely Generated Password
wugr5PYNjn9urM
Firefox will save this password for this website.
View Saved Logins

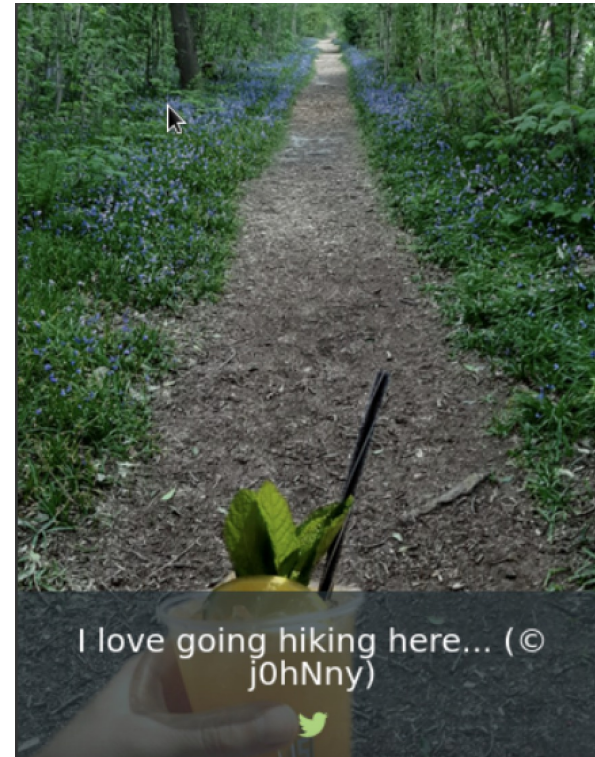
新しいパスワード(確認用) *

パスワードのアドバイスを表示

変更

Meta Geo Stalking

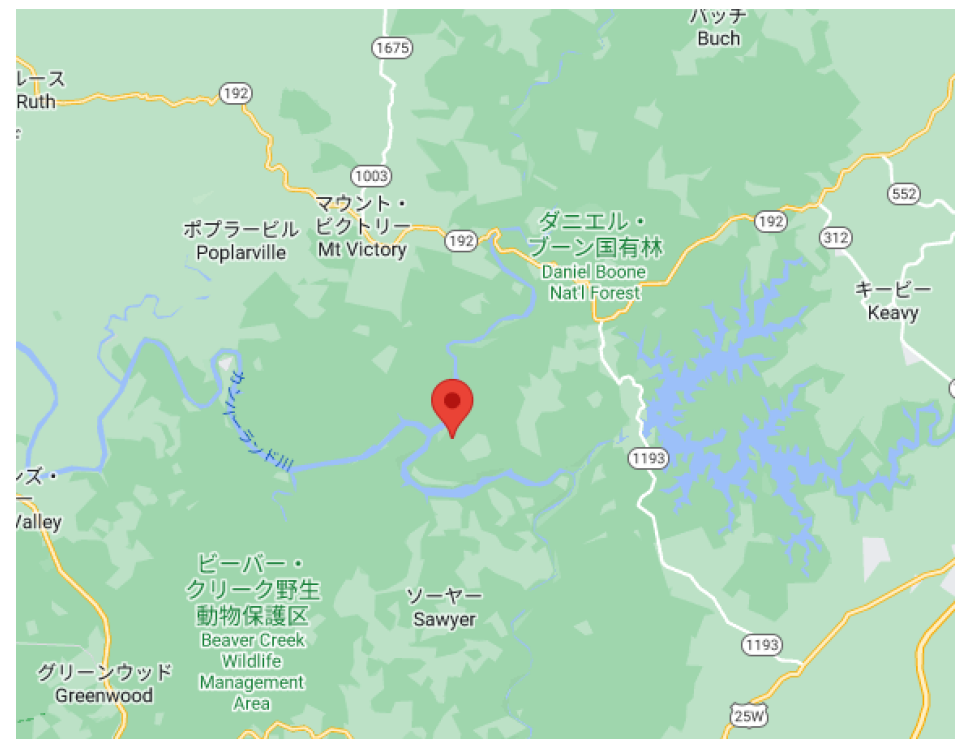
3. サイト内のフォトウォールを見てみると、右のような投稿が見られる。
4. 写真データに位置情報が含まれている場合があるので、サイト内から写真をダウンロードし、<https://image-convert.cman.jp/imgInfo/>を利用してGPS情報を確認する。



Meta Geo Stalking

5. GPS Positionが確認できたので、実際にGoogle Mapを使って場所を特定する。
6. いくつか候補地はあるが、Daniel Boone National Forestを入力してみると、実際にパスワードの再設定ができた。
7. 完了！

exif情報 (日本語 / 英語)	
<div>Exif、メタデータ等を削除</div> <div>Exif内サムネイルを削除</div>	
GPS Position	36 deg 57' 31.38" N, 84 deg 20' 53.58" W
GPSタグバージョン	2.2.0.0



原因

- 設計上の問題：

クレデンシャル回復フローに、秘密の質問のみを採用していること。

- 実装上の問題：

ユーザーが設定した秘密の質問（機密情報）を、メールアドレスを知っているユーザーに公開していること。

- (ユーザー側のリテラシーの問題):

不特定多数が閲覧できるプラットフォームに、個人情報の特定につながるような情報を投稿していること。

対策

- サイトの設計段階で、セキュアなデザインパターンを採用する。
- セキュリティの専門家に相談し、最新のセキュリティシステムに更新する。
- ユーザーの認証に、別のメールアドレスや電話番号を用いた2段階認証を採用する。

実際の動き

- Yahoo!Japan

秘密の質問による本人確認を完全に廃止し、メールアドレスや電話番号による認証にシフトした。(2021/06/16)

- Apple, Google

新規にIDを作成する場合、2段階認証が必須となるので、秘密の質問を設定する必要はなくなった。しかし、過去に作成したアカウントで、2段階認証がオフになっているものは、現在でも秘密の質問による認証が利用されている。(2016年ごろから)