Web Cache Deception Attackについて解説する

kuzushiki

発表内容

Black Hat[1] USA 2017 にてOmer Gil氏が発表した **Web Cache Deception Attack** を解説する

なぜ今なのか？

- 先月 **ChatGPT** で報告されていた
- 直近1ヶ月でHackerOneにて2件のバグレポートが公開された

[1]世界最大級のサイバーセキュリティカンファレンスの一つ

Web Cache Deception Attackとは？

一言で表すと、
「機密情報を含むページをキャッシュさせる攻撃」

Top 10 Web Hacking Technique[1] of 2017にて **2** 位！

※ Top 10 Web Hacking Techniqueについて

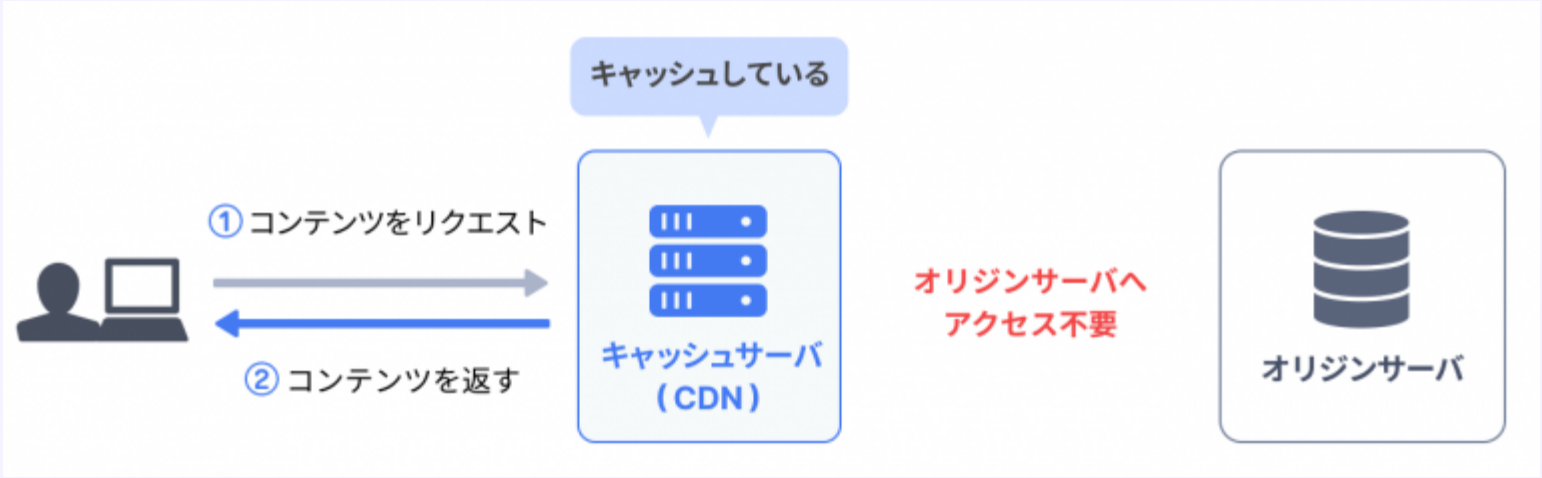
PortSwigger社が毎年公表している脆弱性のランキング
OWASP Top 10 とは異なり、革新的な脆弱性を研究者目線で順位付けしているのが特徴

[1]ちなみに2022年度の1位は「Account hijacking using dirty dancing in sign-in OAuth-flows」

前提知識 - Webにおけるキャッシュとは？

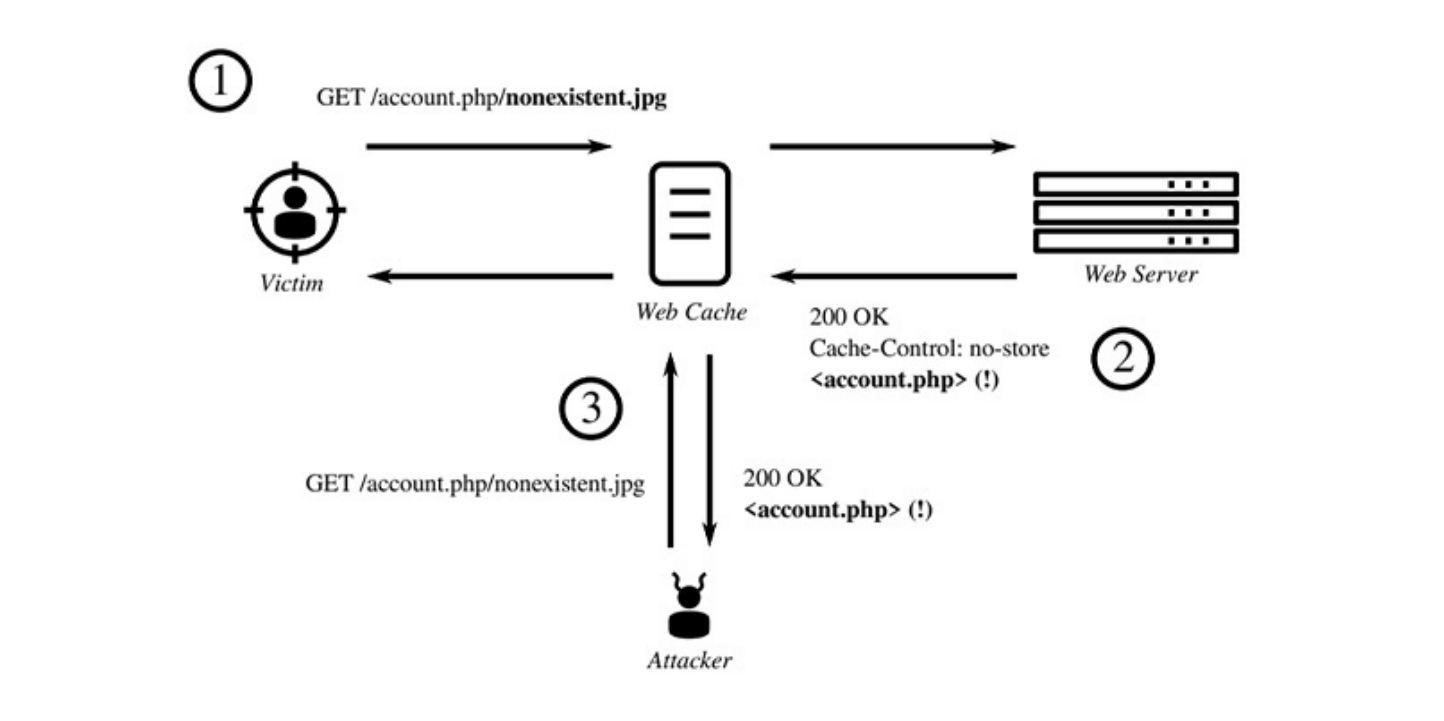
`.css`や`.js`などの静的コンテンツは毎回読み込む必要がない

-> レスポンスを再利用することでより高速にページを表示できる



https://knowledge.sakura.ad.jp/33411/ より引用

攻撃の仕組み



https://portswigger.net/daily-swig/path-confusion-web-cache-deception-threatens-user-information-online より引用

デモ

`Docker Compose`形式で配布しているので、ぜひ触ってみてください

https://github.com/kuzushiki/cache-deception-demo

事例紹介

ChatGPT

- Nagli氏が2023/3/25に報告 -> 2時間以内に修正

`chat.openai[.]com/api/auth/session/test.css`のようなリンクを踏ませることで
被害者の下記情報がキャッシュされ、攻撃者に窃取される可能性があった

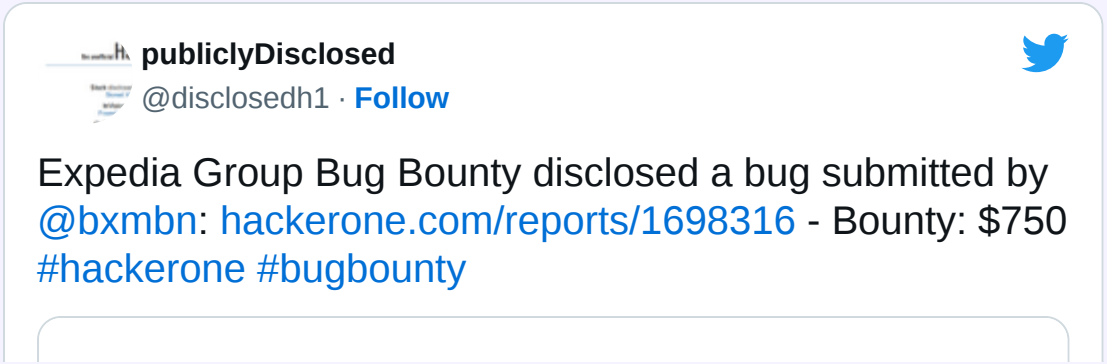
- メールアドレス
- 登録名
- アバター画像
- **アクセストークン**

事例紹介

Expedia

- bombon氏が2022/9/13に報告 -> 2023/4/2に脆弱性レポートが公開

1. 下記URLのレスポンスにセッショントークンが含まれていた
   `www.abritel.fr/search/keywords:soissons-france-(xss)/minNightlyPrice/{anything}`
2. `.jpeg`を末尾に付与してキャッシュさせることができた
   `www.abritel.fr/search/keywords:soissons-france-(xss)/minNightlyPrice/cached.jpeg`



攻撃が成立する条件とその対策[1]

1. http://www.example.com/account.php/nonexistent.css のようなページにアクセスするとaccount.php のコンテンツを返す（素のPHPやDjangoで起こりうる）

-> 正規表現パターンを厳密に設定する

```
× url(r'^inbox/', views.index, name='index')
○ url(r'^inbox/$', views.index, name='index')
```

2. キャッシュ機能がキャッシュヘッダを無視し、拡張子のみでファイルをキャッシュするように設定されている

-> 拡張子のみで判断せず、Content-TypeやCache-Controlヘッダ等をチェックする

3. 被害者が悪意のあるURLにアクセスする際に認証が必要

-> そもそも認証が必要なコンテンツはキャッシュさせない

[1]Gil, Omer. "Web cache deception attack." Black Hat USA 2017 (2017).

おわりに

Web Cache Deception Attack について、デモを交えながら攻撃手法と事例について説明した

ChatGPT や **Expedia** のような有名なサービスでも報告されており、かつ確認手順も簡単なため、診断やバグバウンティで確認する価値はありそう