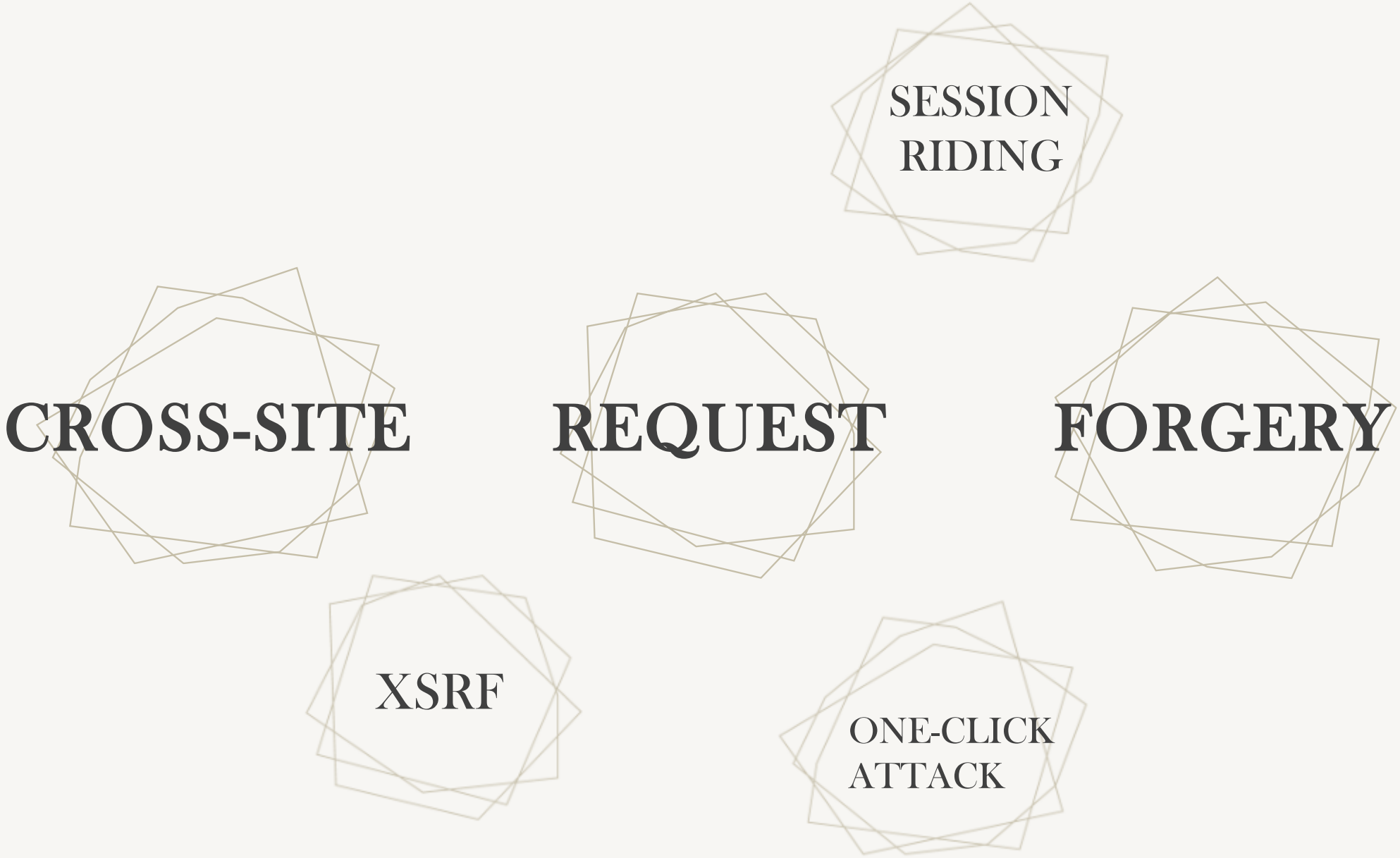
ATAK CSRF

Wiktoria Gajos Karina Zawada Paweł Pasternak

PLAN PREZENTACJI

1. Czym jest CSRF?
2. Mechanizmy HTTP, sesja i ciasteczka
3. Metody ataku
4. Porównanie CSRF vs XSS
5. Głośne ataki z przeszłości
6. Quiz i bibliografia

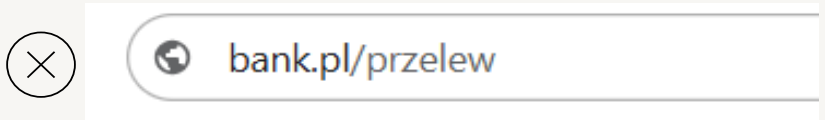

CROSS-SITE
REQUEST
FORGERY


SESSION
RIDING
CROSS-SITE
REQUEST
FORGERY
XSRF
ONE-CLICK
ATTACK

> **Aplikacja nie sprawdza, czy wysłane do niej prawidłowe żądanie HTTP zostało świadomie wykonane przez użytkownika**

HTTP jest bezstanowy

Każde zapytanie dla serwera jest nowym wydarzeniem



Rozwiązanie → ciasteczko sesyjne

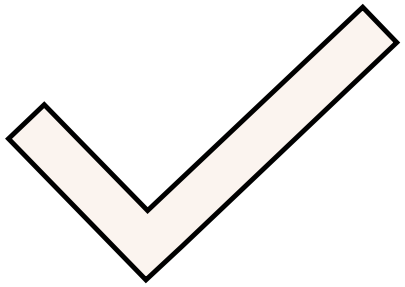
Po zalogowaniu otrzymujemy indentyfikator potwierdzający naszą tożsamość

Haczyk?

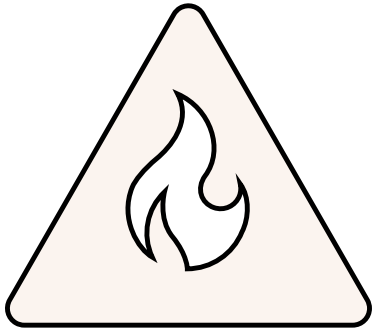
Przeglądarka sprawdza **gdzie** leci żądanie ale nie sprawdza **skąd** przyszło

METODY ATAKU

RODZAJE ZAPYTAŃ



Simple



Non-simple

GET

```
<img src="https://forum.czerwony.kapturek.com/admin/delete_account">
```

Atakujący umieszcza w źródle HTML strony tag i nakłania zalogowanego administratora do wejścia na swoją stronę

POST

1

```
<form action="bank.cz.kapturek.com" method="post">
 ...
</form>
```

Domena atakujícego

POST

1

```
<form action="bank.cz.kapturek.com" method="post">
 ...
</form>
```

Domena atakujícího

2

Logowanie do bankowości

POST

1

```
<form action="bank.cz.kapturek.com" method="post">
 ...
</form>
```

Domena atakującego

3

Atakujący zachęca do odwiedzenia jego strony

2

Logowanie do bankowości

POST

1

```
<form action="bank.cz.kapturek.com" method="post">
 ...
</form>
```

Domena atakującego

3

Atakujący zachęca do odwiedzenia jego strony

```
... transfer.do" method="POST">
<input type="hidden" name="dstacct" value="WILK"/>
<input type="hidden" name="srcacct" value="BABCIA"/>
<input type="hidden" name="amount" value="10000'/>
<input type="submit" value="test"/>
...
```

CSRF, żadanie HTTP, przelew na konto atakującego

4

2

Logowanie do bankowości

PORÓWNANIE CSRF VS XSS

- **XSS (Cross-Site Scripting):** Atakujący wstrzykuje złośliwy skrypt na stronę.
  Cel: kradzież danych (np. ciasteczek), przejęcie sesji, zmiana wyglądu strony.
  Skrypt wykonuje się w kontekście Twojej przeglądarki na zaufanej stronie.

- **CSRF (Cross-Site Request Forgery):** Atakujący wykorzystuje Twoją aktywną sesję, by wykonać akcję w Twoim imieniu na innej stronie.
  Cel: wykonanie konkretnej operacji (przelew, zmiana hasła). Atakujący nie musi widzieć Twoich danych, by atak się udał.

Głośne ataki z przeszłości

1. YOUTUBE (2008) – MASOWE AKCJE

Problem: Brak tokenów CSRF przy kluczowych akcjach.

Skutek: Atakujący mogli zmusić zalogowanego użytkownika do:

- Dodania filmu do ulubionych.
- Wysłania wiadomości do znajomych.
- Subskrybowania kanału.

ING DIRECT (2008) – KRADZIEŻ PIENIĘDZY

Problem: Podatność na CSRF w panelu bankowości online.

Skutek: Atakujący mógł stworzyć formularz, który po załadowaniu przez ofiarę:

- Wykonywał przelew na zdefiniowane konto.
- Zmieniał dane kontaktowe użytkownika.

TIKTOK (2020) – CSRF + XSS

Problem: Wykryto lukę, która w połączeniu z XSS pozwalała na przejęcie konta.

Skutek: Atakujący mógł:

- Wysyłać wiadomości w imieniu użytkownika.
- Publikować i usuwać filmy.
- Zmieniać ustawienia prywatności konta na „publiczne”.

JAK SIĘ BRONIĆ?

Dowiecie się za tydzień! 

BIBLIOGRAFIA

- **OWASP Foundation** – *CSRF Prevention Cheat Sheet* (Standardy bezpieczeństwa)
- **PortSwigger Web Security Academy** – *Cross-Site Request Forgery (CSRF)*
- **Sekurak.pl** – *Czym jest podatność CSRF?*
- **B. Zeller, E. Felten (Princeton, 2008)** – Analiza podatności YouTube i ING Direct na ataki CSRF.
- **HackerOne, Raport #968082 (2020)** – Techniczny opis przejęcia konta na TikToku (One-click Account Takeover).
- **Bezpieczeństwo aplikacji webowych** - Gynvael Coldwind, Michał Sajdak, Michał Bentkowski, Artur Czyż, Rafał Janicki, Jarosław Kamiński, Adrian Michalczyk, Mateusz Niezabitowski, Marcin Piosek, Grzegorz Trawiński, Bohdan Widła

QUIZ

DZIĘKUJEMY ZA UWAGĘ!