

Safe Cookies

~ Mateusz Świder & Szymon Bobrowski

Czym jest HTTP Cookie?

- fragment tekstu
- zastosowania
- dostępność





Zastosowania ciasteczek

- sesja
- dane

me:Opens a website
2 seconds later:

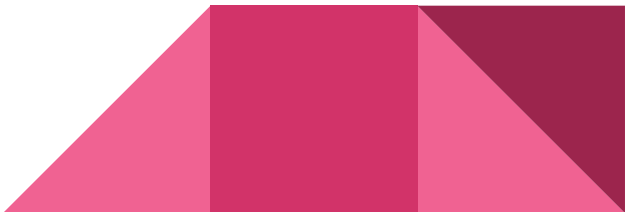


Sposób działania *ciasteczek*

- jak przesyłamy pliki cookie
- metoda Set-Cookie
- pola obowiązkowe i opcjonalne



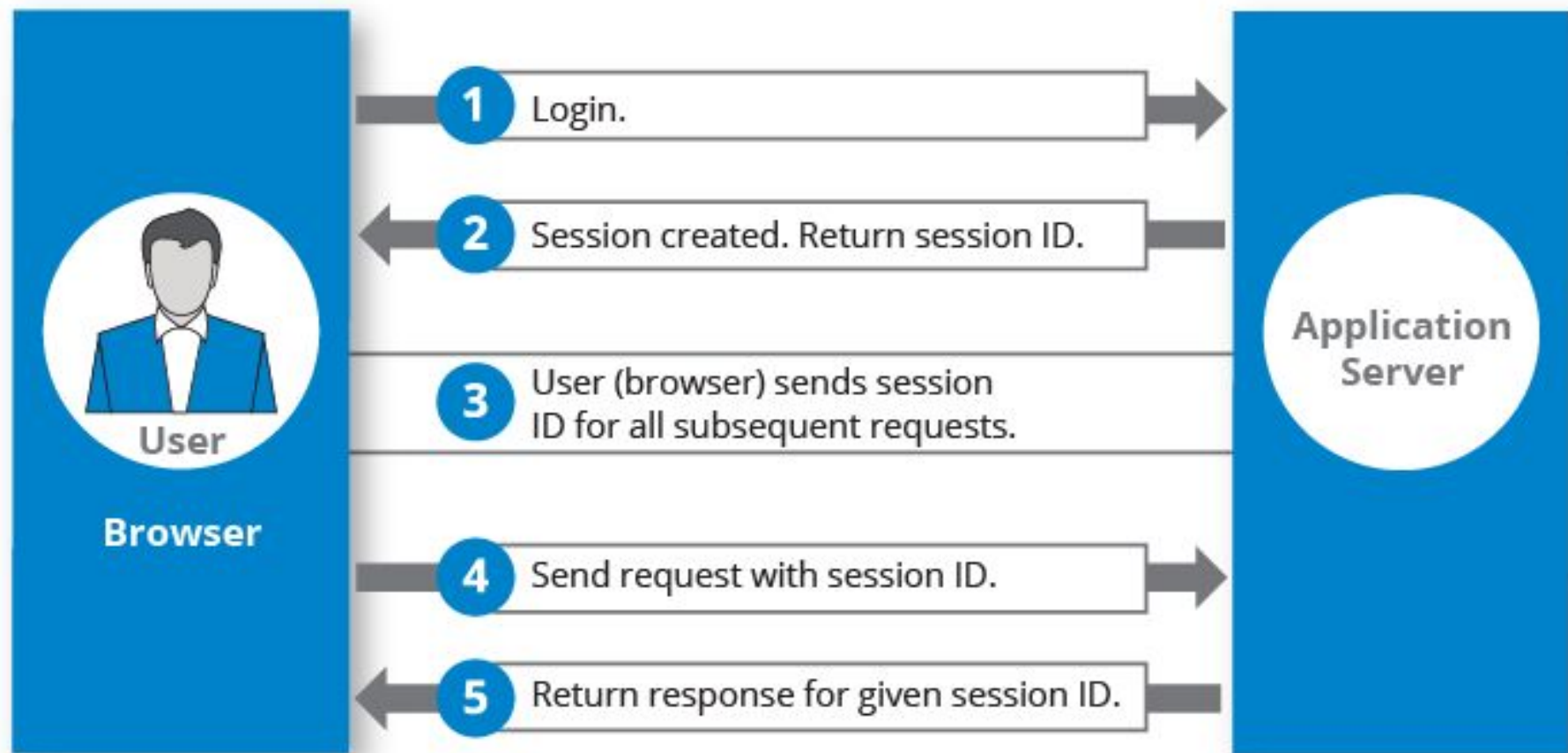
Wybrane pola w metodzie Set-Cookie

- `<cookie-name>=<cookie-value>`
 - `Expires=<date>`
 - `Domain=<domain-value>`
 - `Secure`
- 

Mechanizm Sesji

- informacje o połączeniu
- warunki zakończenia sesji
- sposób przekazywania informacji





Przesyłanie Session ID

1. Wysyłanie session id tekstem jawnym w URL
2. Wysyłanie shashowanego id sesji w URL
3. Wysyłanie id sesji jako ukrytej wartości w formularzu HTML
4. Umieszczenie identyfikatora sesji w pliku cookie





The diagram illustrates a session fixation attack. At the top left, a 'VICTIM' (woman at a laptop) sends 'Login Credentials: admin, p@sSw0rd.!' to a 'Server' (represented by a blue circle with server icons). The 'Server' responds with a 'SessionID: H7456789KLbmDGH'. Below this, an 'ATTACKER' (person in a hoodie at a laptop) is shown. A red dashed arrow points from the SessionID box to the attacker. Another red dashed arrow points from the SessionID box to a red box containing the text 'Session Fixation: Same SessionID: H7456789KLbmDGH'. The attacker's laptop has a skull icon on it.

Login Credentials: admin,
p@sSw0rd.!

SessionID:
H7456789KLbmDGH

VICTIM

Server

Session Fixation: Same
SessionID:
H7456789KLbmDGH

ATTACKER

Session Hijacking



Sposoby przechwytywania sesji

1. **Session fixation**
2. **Session sniffing**
3. **Cross-site scripting XSS**
4. **Brute force**
5. **Złośliwe oprogramowanie**



Session Fixation

```
<a href="http://www.TrustedSite.com/login.php?sessionid=iknowyourkey">Click here to log in now</a>
```



Public Wi-Fi Session Sniffing Attack



Wi-Fi Router

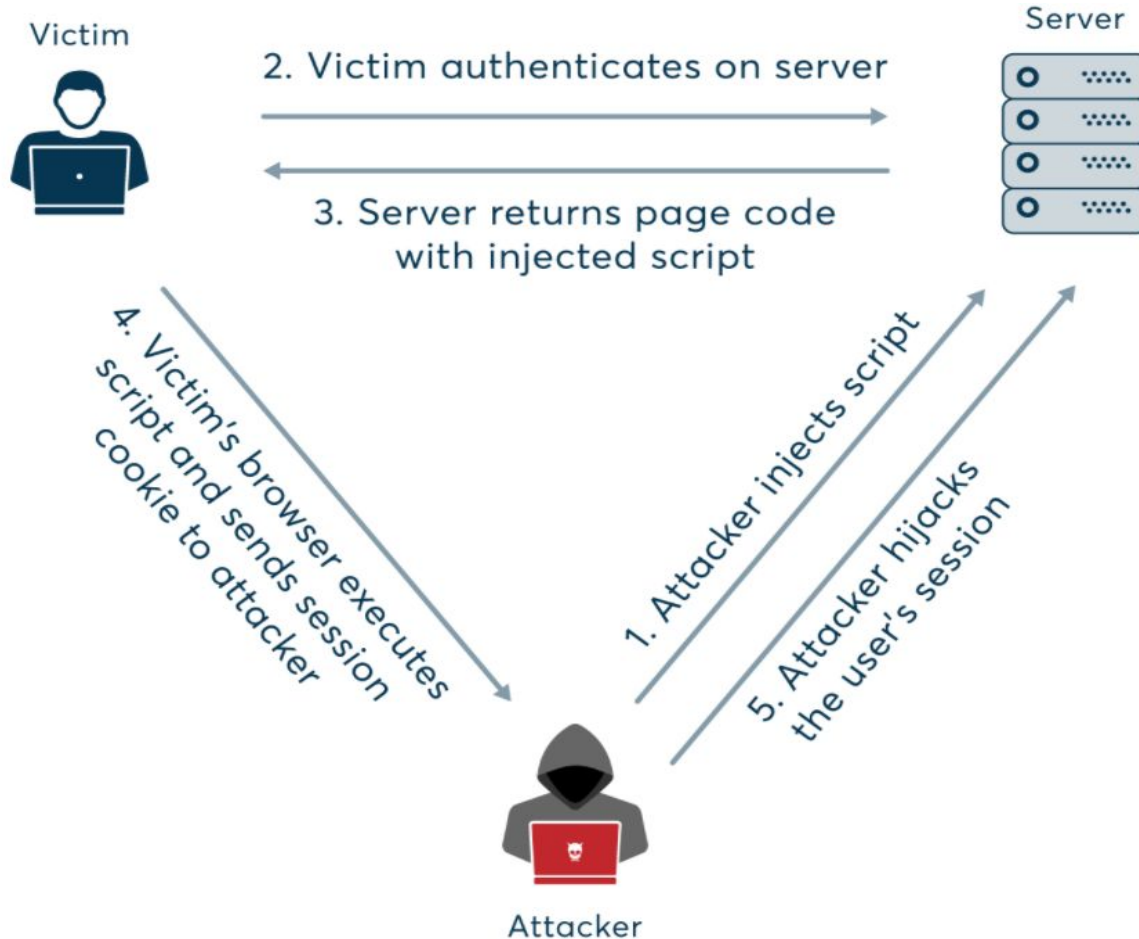


Sniffer Monitors
Traffic for Cookies



Your PC

Cross-site scripting



Brute-force



Malware



Jak zabezpieczyć się przed session hijacking?

- HTTPS
- Długie i losowe klucze
- Frameworki
- Ponowna generacja klucza po zalogowaniu
- Dodatkowe środki weryfikacji



Przykładowe ataki

- Zoom-bombing
- Mozilla Firefox “Firesheep” extension
- Slack
- GitLab

<https://www.keyfactor.com/blog/what-is-session-hijacking-and-how-does-it-work/>



Koniec, dziękujemy za uwagę!

