

# **Bezpieczeństwo aplikacji internetowych**

**Wykład VII - VIII**

**dr inż. Sabina Szymoniak**

Katedra Informatyki  
Politechnika Częstochowska

Rok akademicki 2023/2024



Wydział Inżynierii  
Mechanicznej i Informatyki



# Ataki na aplikacje internetowe



1. Ataki Cross-Site Scripting

2. Ataki Cross-Site  
Request Forgery



3. Ataki z rodziny  
Denial of Service

4. Literatura

# Plan wykładu

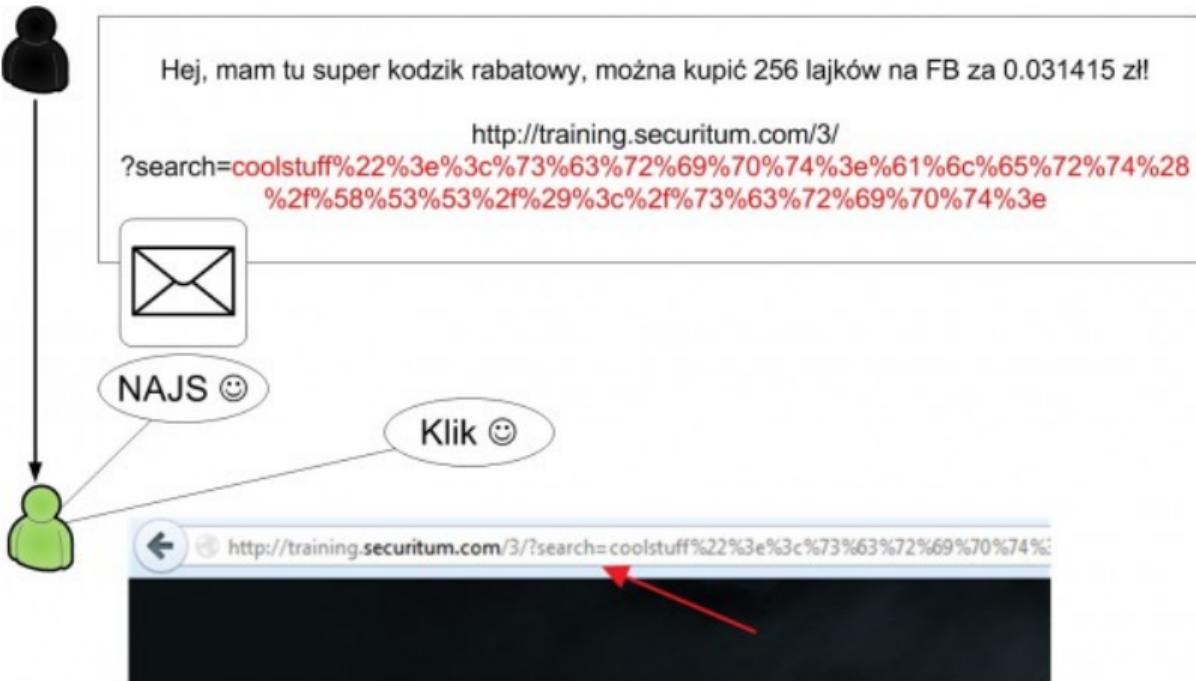
# Ataki Cross-Site Scripting I

[KI]>

- rodzaj wstrzykiwania,
- złośliwe skrypty są wstrzykiwane do innych łagodnych i zaufanych witryn internetowych,
- atakujący używa aplikacji internetowej do wysłania złośliwego kodu (zazwyczaj w postaci skryptu po stronie przeglądarki), do innego użytkownika końcowego,
- kategorie ataków:
  - Stored (kod jest zapisany w bazie danych przed wykonaniem),
  - Reflected (kod nie jest zapisany w bazie danych, ale jest zwracany przez serwer),
  - DOM-based (kod jest przechowywany i wykonywany w przeglądarce).

# Ataki Cross-Site Scripting II

[KI]



# Ataki Cross-Site Scripting III

[KI]



# Ataki Cross-Site Scripting IV

[KI]>

- uruchamiają w przeglądarce skrypt, który nie został napisany przez właściciela aplikacji,
- mogą działać za kulisami bez żadnych oznak wizualnych i są uruchamiane bez udziału użytkownika,
- mogą przechwycić dowolnego typu dane obecne w bieżącej aplikacji internetowej,
- mogą swobodnie przyjmować dane ze złośliwego serwera WWW i je tam wysyłać,
- są wynikiem wbudowania w kod interfejsu użytkownika niepoprawnie oczyszczonych danych wejściowych od użytkownika,

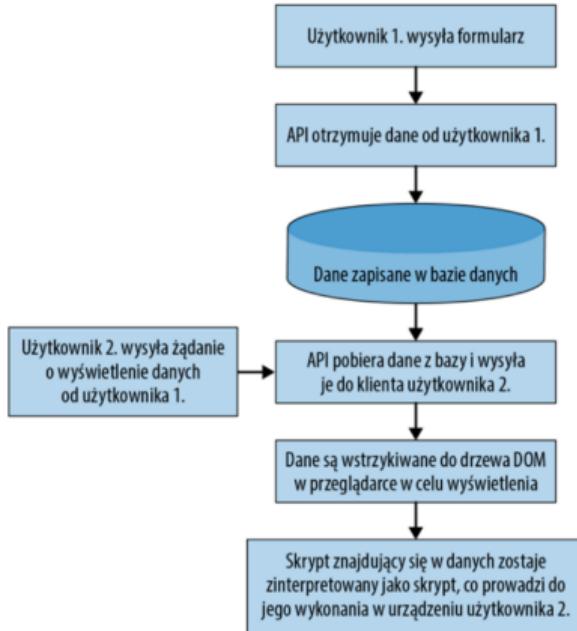
# Ataki Cross-Site Scripting V

[KI]>

- za ich pomocą można wykradać tokeny sesji, co może doprowadzić do przejęcia konta,
- za ich pomocą można wyświetlać obiekty DOM nad istniejącym interfejsem użytkownika, co może doprowadzić do perfekcyjnych ataków phishingowych, których nietechniczny użytkownik nie rozpozna,
- metody ochrony przed atakami XSS.

# Zapisane ataki XSS

[KI]



Źródło: Hoffman A.: Bezpieczeństwo nowoczesnych aplikacji internetowych. Przewodnik po zabezpieczeniach, Helion

# Odbite ataki XSS

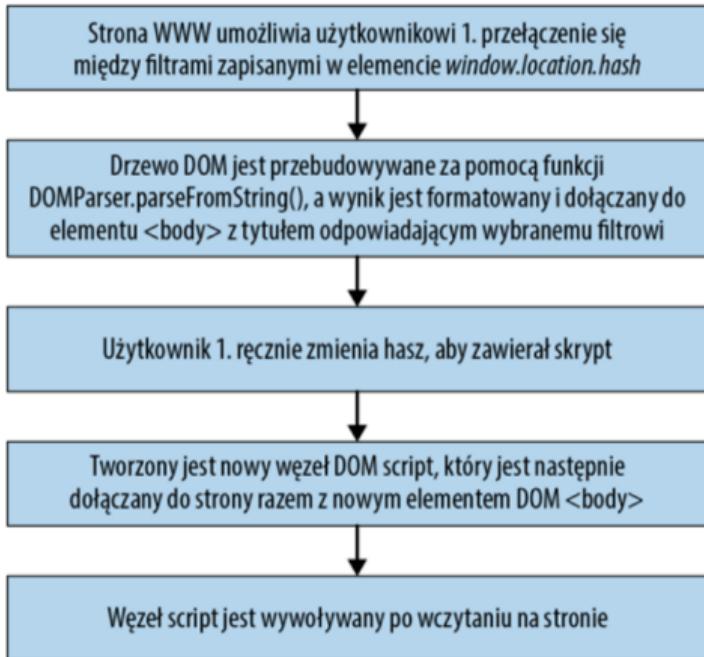
[KI]



Źródło: Hoffman A.: Bezpieczeństwo nowoczesnych aplikacji internetowych. Przewodnik po zabezpieczeniach, Helion

# Ataki XSS oparte na drzewie DOM

[KI]



# Ataki XSS - przykłady na świecie

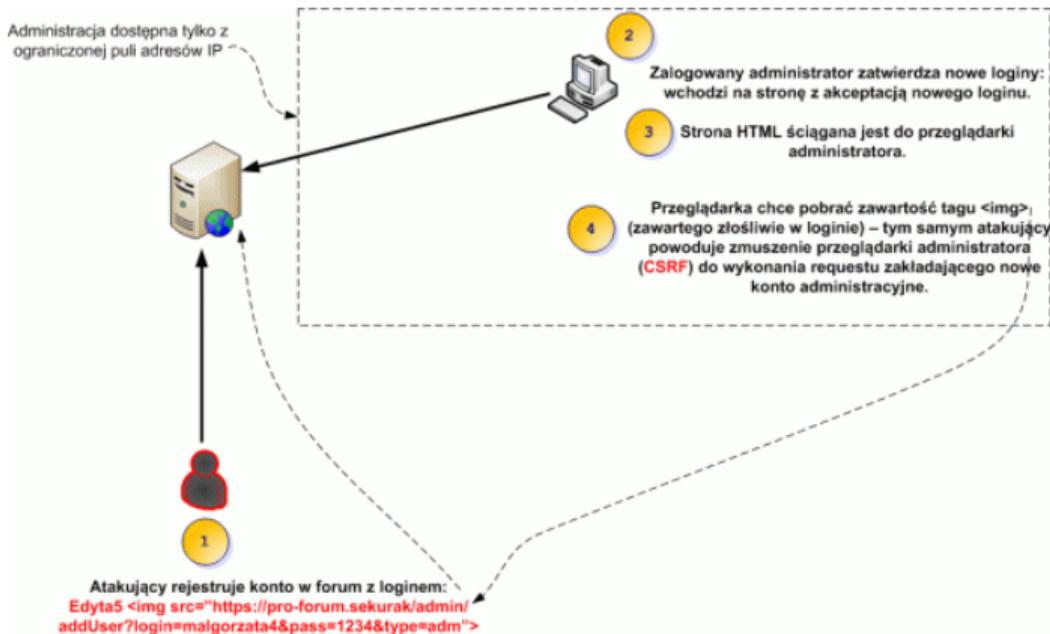
[KI]>

# Cross-Site Request Forgery I

- wykorzystują sposób działania przeglądarek i relację zaufania między witryną a przeglądarką,
- znajdując wywołania API można przygotować linki i formularze, które sprawią, że użytkownik wykona żądanie w imieniu agresora bez świadomości użytkownika generującego żądanie,
- to nie to samo co XSS, ale jeżeli w aplikacji występuje XSS, to CSRF również jest możliwy.

# Cross-Site Request Forgery II

Przykład 1:



# Cross-Site Request Forgery III

[KI]

Przykład 2:

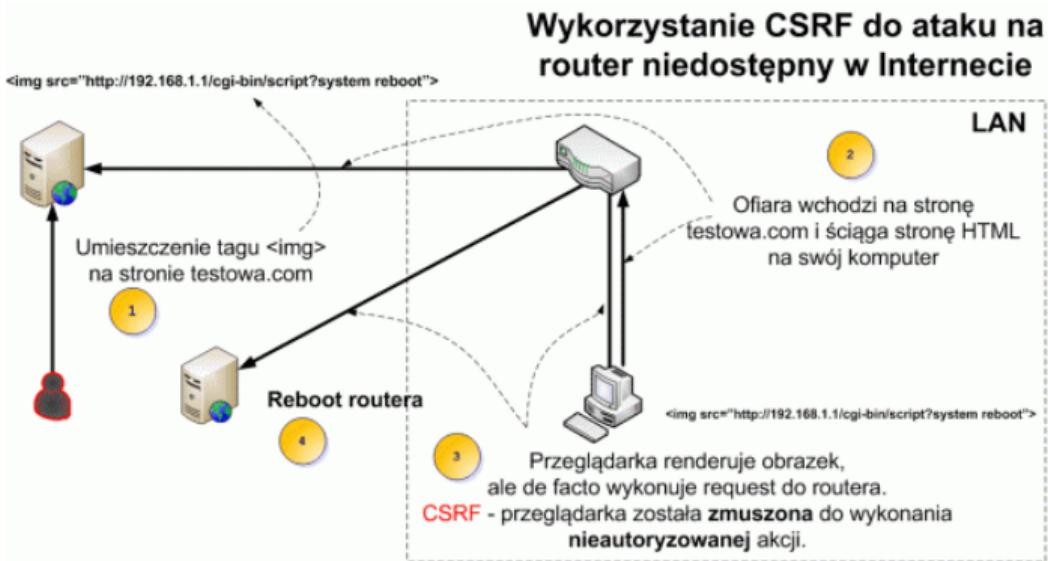
```
192.168.1.1/cgi-bin/script?system ps aux
```

PID	Uid	VmSize	Stat	Command
1	root	1304	S	init
2	root		S	{keventd}
3	root		S	[ksoftirqd_CPU0]
4	root		S	[kswapd]
5	root		S	[bdflush]
6	root		S	[kupdated]
7	root		S	[mtdblockd]
34	root	2780	S	/usr/bin/cm_pc
36	root	1304	S	init
37	root	1192	S	/usr/sbin/tthttpd -d /usr/www -u root -p 80 -c /cgi-b
38	root	3616	S	/usr/bin/cm_logic -m /dev/ticfg -c /etc/config.xml
60	root	608	S	/usr/bin/cm_klogd /dev/klog
64	root	1668	S	/usr/sbin/snmpd
164	root	684	S	/usr/sbin/udhcpd /var/tmp/udhcpd.conf
169	root	640	S	/sbin/dproxy -c /etc/dproxy.conf -d
237	root	1320	S	/bin/sh script system ps aux
238	root	1192	S	/usr/sbin/tthttpd -d /usr/www -u root -p 80 -c /cgi-b
250	root	1304	R	/bin/ps aux

# Cross-Site Request Forgery IV

[KI]

Przykład 2:

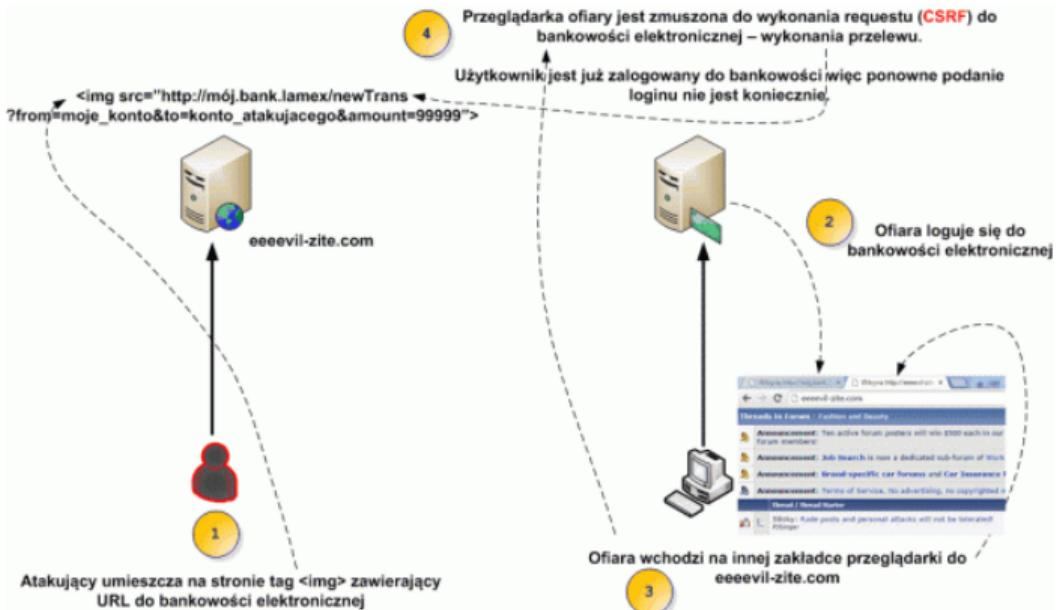


Źródło: sekurak.pl

# Cross-Site Request Forgery V

[KI]

Przykład 3:



# Metody ochrony przed CSRF

- losowe tokeny,
- Double Submit Cookies,
- użycie gotowych bibliotek.

# Ataki CSRF - przykłady na świecie

[KI]>

# Ataki z rodziny Denial of Service

[KI]

- wielka sieć urządzeń zalewa serwer żądaniami, spowalniając jego działanie lub uniemożliwiając jego użycie przez zwykłych użytkowników,
- przybierają różne formy,
- mają różne skutki,
- bardzo trudne do przetestowania.

# Rodzaje ataków DoS

- ataki DoS wykorzystujące wyrażenia regularne (ReDoS),
- logiczne ataki DoS,
- rozproszone ataki DoS.

# Ataki (D)DoS - przykłady na świecie

[KI]

# Literatura

[KI]

Wykorzystano następujące materiały:

- Hoffman A.: Bezpieczeństwo nowoczesnych aplikacji internetowych. Przewodnik po zabezpieczeniach, Helion
- Bentkowski M. i inni: Bezpieczeństwo aplikacji webowych, Securitum.

# Dziękuję za uwagę! Pytania?

Spostrzeżenia i sugestie

sabina.szymoniak@icis.pcz.pl

