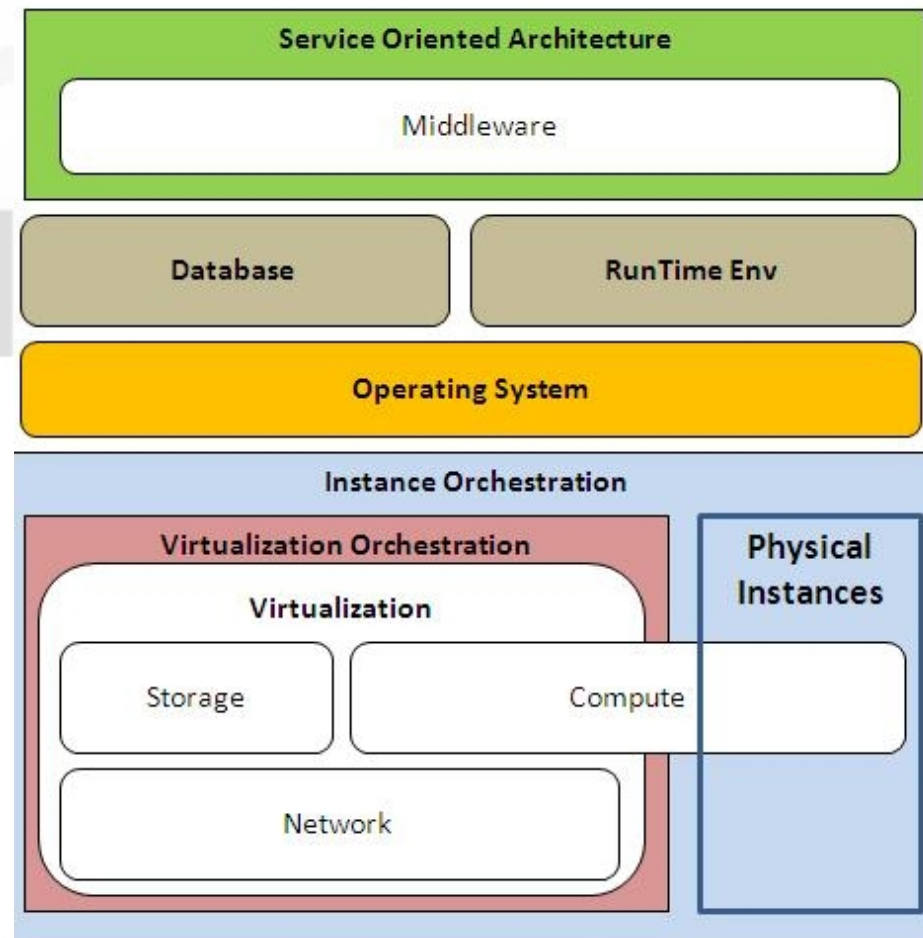


## Aplikacje webowe na celowniku.

Leszek Miś  
IT Security Architect  
RHCA,RHCSS,Sec+  
Linux Polska Sp. z o.o.

# Fakty

- Złożona i rozbudowana architektura:
  - błędy w kodzie
  - błędy w konfiguracji
  - błędy w założeniach
- Zmiana wektora ataków:
  - XSS->Command Execution->dane

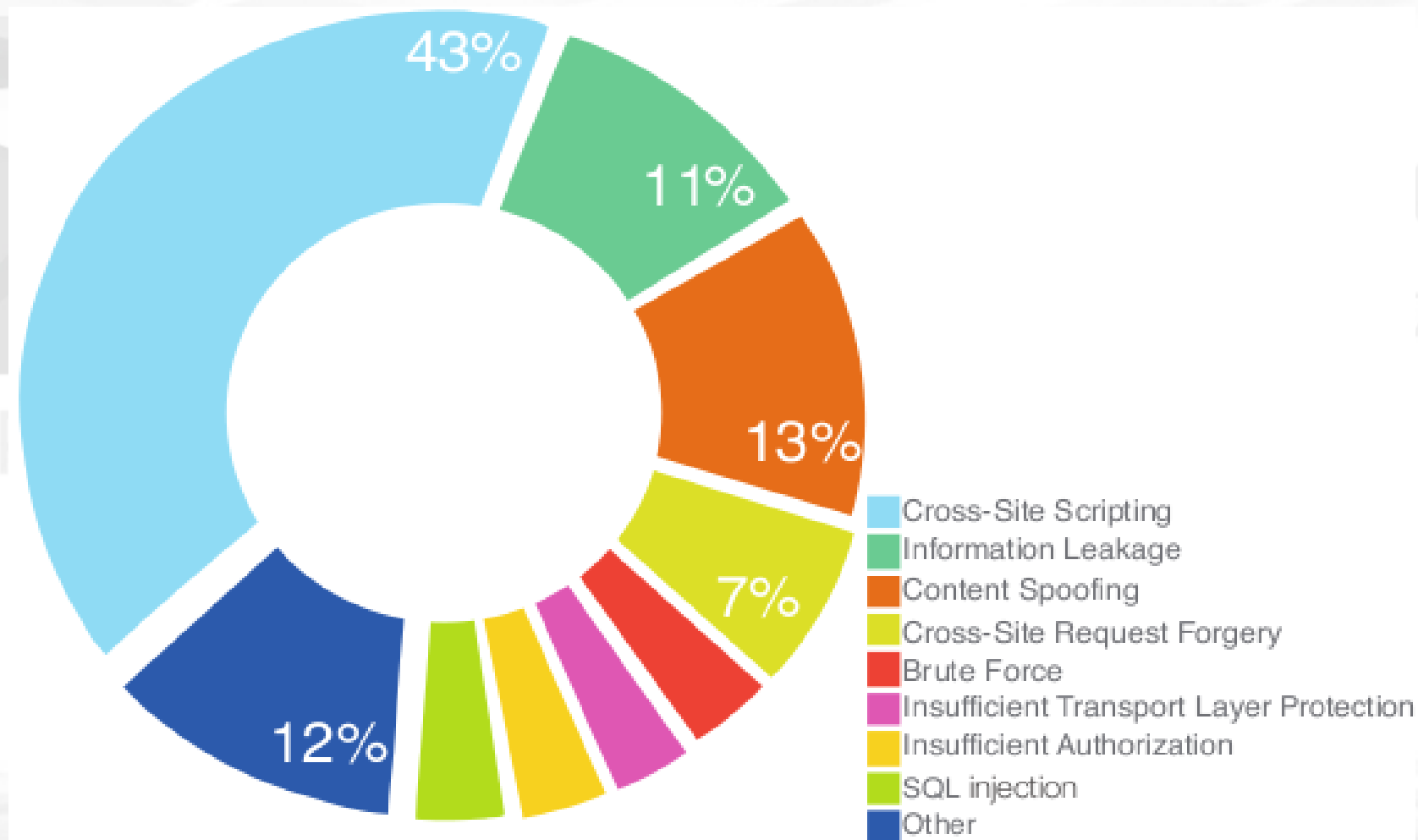


# Fakty

- Ogromna popularność webaplikacji
- W 70% badanych aplikacji znajduje się krytyczny błąd:
  - Oszustwa finansowe
  - Kradzież danych osobowych
  - Kary regulacyjne
  - Utrata reputacji
  - Niedostępność usług
  - Malware
  - Utrata klientów

# Fakty

- Najpopularniejsze podatności w webaplikacjach - 2012



ka  
Z O.O.  
N Y



# Problemy

- Dotychczasowe rozwiązania FW, IPS, AV są nieskuteczne.
- Brak Secure Software Development Life Cycle



- Niedostateczna współpraca na linii “Administratorzy i software” <-> dostawcy przeglądarek -> HTTPS

# Problemy

- Ataki na aplikacje:
  - Błędy w kodzie
  - Niepoprawna konfiguracja
- Ataki na usługi sieciowe:
  - Błędy w kodzie
  - Brak środowisk separujących, np. SELinux
- Ataki na HTTPS:
  - Niepoprawna konfiguracja

-

# Rekomendacja D

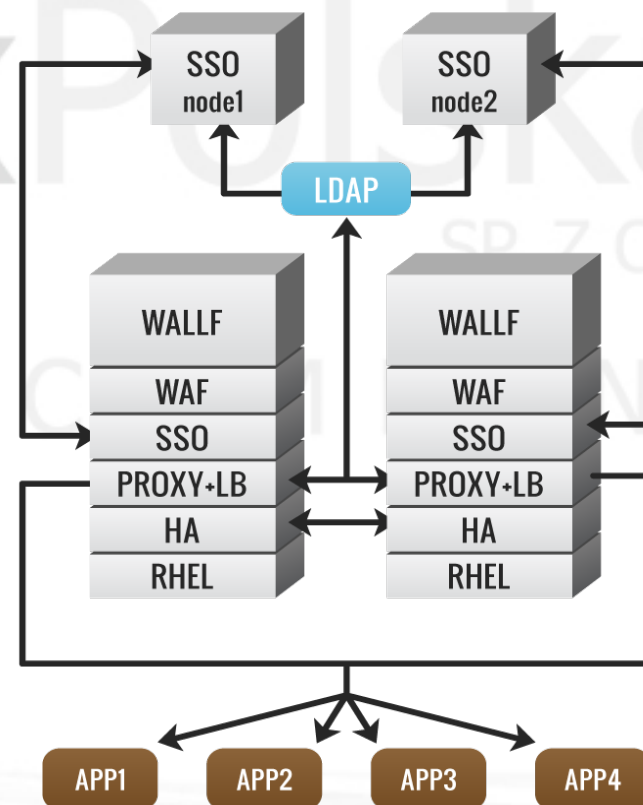


- **9.4:** Styk sieci wewnętrznej banku z sieciami zewnętrznymi (w szczególności Internetem) powinien być zabezpieczony systemem zapór sieciowych.
- **9.15:** Konfiguracja systemu zapór sieciowych powinna zapewniać rejestrowanie niestandardowych aktywności w celu umożliwienia dokonywania ich analizy pod kątem wykrywania ataków zewnętrznych i wewnętrznych.
- **16.4:** Systemy informatyczne wykorzystywane w obszarze tych kanałów powinny być zaprojektowane i skonfigurowane w sposób zapewniający odpowiednio wysoki poziom integralności, poufności i dostępności danych dotyczących transakcji.

# WALLF Web Gateway



- Kompleksowy ekosystem dla infrastruktury aplikacji internetowych
- HA A-A-
- 4 moduły WALLF:
  - Proxy-Auth
  - Load Balancer
  - Web Application Firewall
  - Single Sign On
- Modularne moduły





# WALLF Web Gateway



- Rozwijany i utrzymywany od 2011r. przez zespół architektów Linux Polska
- Referencyjne wdrożenia rozwiązania w środowiskach ponad 20k użytkowników:
  - Aktywnych ~20 aplikacji w integracji SSO
  - Nowe, dodawane regularnie
- Lokalne wsparcie techniczne
- Stawiamy na rozwój

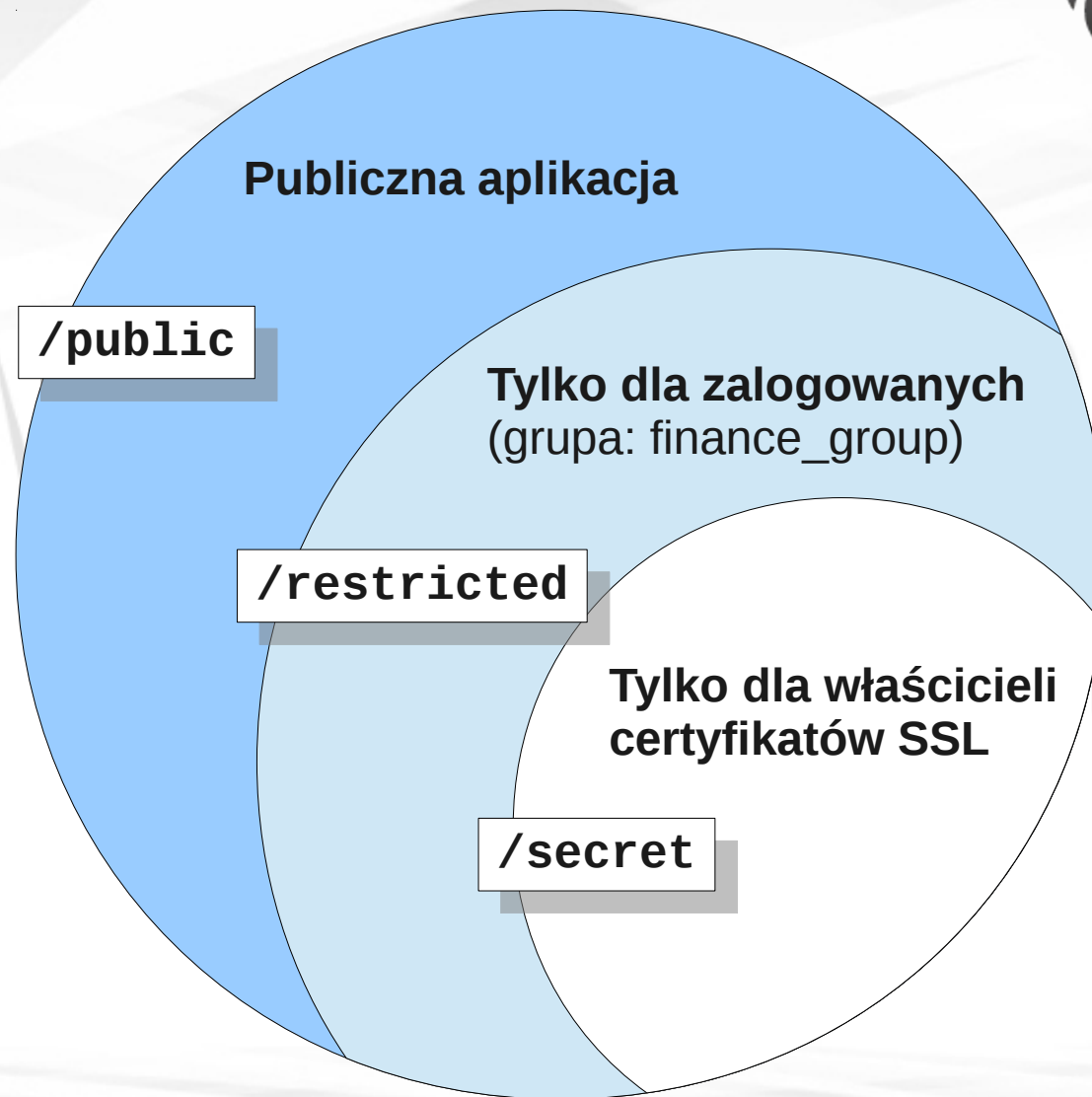


# Podstawowa funkcjonalność



- Architektura Active-Passive / Active-Active:
  - Bonding + keepalived/pacemaker
  - 2x VIP na każdym nodzie
  - Terminacja SSL
  - Uwierzytelnienie LDAP/AD/SSL-certs/2-way
  - Współdzielone tickety SSO poprzez replikowany FS
  - LDAP based auth
  - Definicje klastrów aplikacyjnych (waga, obciążenie, ruch, dostępność)
  - Podłączenie pod frontendowy balancer sprzętowy

# SSL auth



# Podstawowa funkcjonalność



- SPNEGO based SSO – sieci korporacyjne
- Zmiana tożsamości użytkowników w obrębie sesji
- Wsparcie dla LDAP Password Policy Enforcement
- Wirtualne patchowanie aplikacji – ochrona 0-day
- **Web Application Firewall:**
  - Hybryda Blacklist/whitelist
  - **Ofensywne podejście**

**Aby móc się obronić, należy  
wiedzieć jak atakować.**



# Podejście ofensywne - WAF



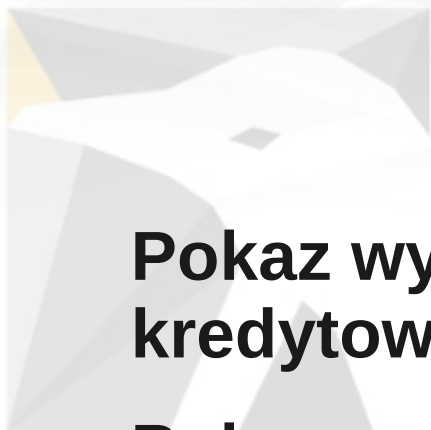
- **Honeytrapy**
- **Data Leakage Protection**
- **Error Handling**
- Wsparcie dla centralnych list RBL
- Wykrywanie modyfikacji treści strony przez malware
- **Profilowanie aplikacji na podstawie sensorów wykrywających anomalie we wczesnej fazie rekonesansu**
- Pełna analiza protokołu HTTP:
  - Możliwość replay'owania sesji
- **Wykrywanie i blokowanie ataków typu brute force**

**Pokaz próby wykorzystania podatności  
przed i po aktywacji mechanizmu WAF.  
Wykradanie sesji z Liferay.  
XSS->session hijacking.**





**WALLF**  
Web Gateway



**LinuxPolska**  
SP. Z O.O.

**Pokaz wykrywania wycieku numerów kart kredytowych.**

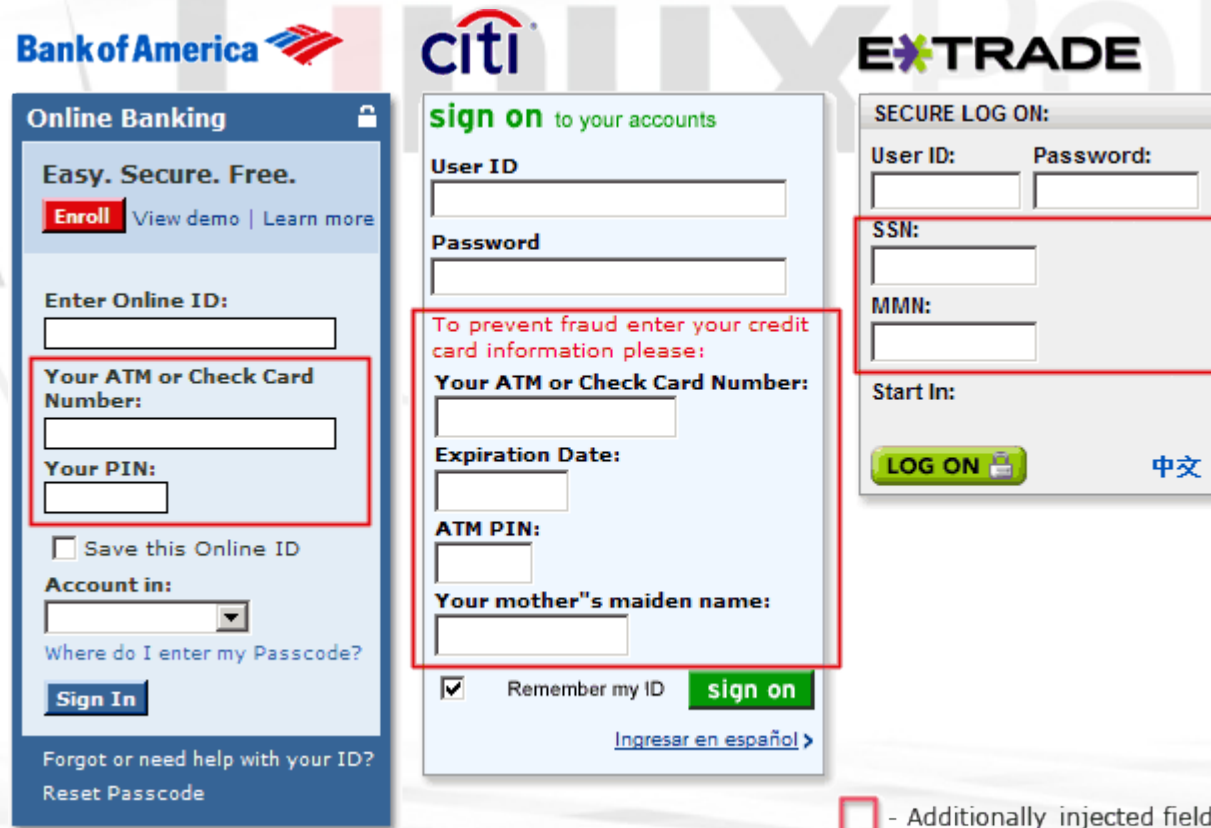
**Pokaz poprawnej obsługi błędów.**

**Pokaz zastosowania podejścia proaktywnego z wykorzystaniem honeytrapów:**

- **Ukryty link do panelu CMS**
- **Ukryte pole typu hidden**

**Wykrywanie anomalii w komunikacji HTTP**

## Omówienie mechanizmu wykrywającego modyfikację strony banku po stronie klienta.



The image displays three screenshots of bank login pages, illustrating the mechanism for detecting modifications to the page from the client side. Red boxes highlight injected fields.

**Bank of America:** The login form includes fields for "Enter Online ID:", "Your ATM or Check Card Number:", and "Your PIN:". A red box highlights the "Your ATM or Check Card Number:" and "Your PIN:" fields, indicating they are injected.

**Citi:** The login form includes fields for "User ID", "Password", "Your ATM or Check Card Number:", "Expiration Date:", "ATM PIN:", and "Your mother's maiden name:". A red box highlights the "Your ATM or Check Card Number:", "Expiration Date:", "ATM PIN:", and "Your mother's maiden name:" fields, indicating they are injected.

**E\*TRADE:** The login form includes fields for "User ID:", "Password:", "SSN:", "MMN:", and "Start In:". A red box highlights the "SSN:" and "MMN:" fields, indicating they are injected.

A legend at the bottom right indicates that the red box represents "Additionally injected fields".



# Trojany bankowe



- Po stronie klienta (desktop):
  - Wykrywają odwiedzane strony banków
  - Wstrzykują szkodliwy kod modyfikując zawartość strony banku prosząc o:
    - Numer karty kredytowej
    - Imię nazwisko
    - Datę wygaśnięcia
    - CVV
    - Secret word
  - Kontrola transakcji danych

# Ciekawostki

- ?



LinuxPolska

SP. Z O.O.

OPEN SOURCE COMPANY

# Podsumowanie



- Elastyczność WALLF:
  - Integracja z podsystemami infrastruktury:
    - LB, SSO, terminacja SSL, inne
  - Brak koncentracji na pudełkowaniu
  - Masz wyjątkowo trudny problem? Jesteś naszym Klientem
  - Open Source jako dobry wybór
  - Tworzenie dedykowanych reguł
- Pomoc w doborze WAF dla Twoich potrzeb
- Dedykowane szkolenie “Modsecurity – skuteczna ochrona aplikacji webowych”

# Linux Polska

[www.LinuxPolska.pl](http://www.LinuxPolska.pl)

**Dziękuję za uwagę.**

**Leszek Miś**  
**IT Security Architect**  
**RHCA,RHCSS,Sec+**  
**Linux Polska Sp. z o.o.**