

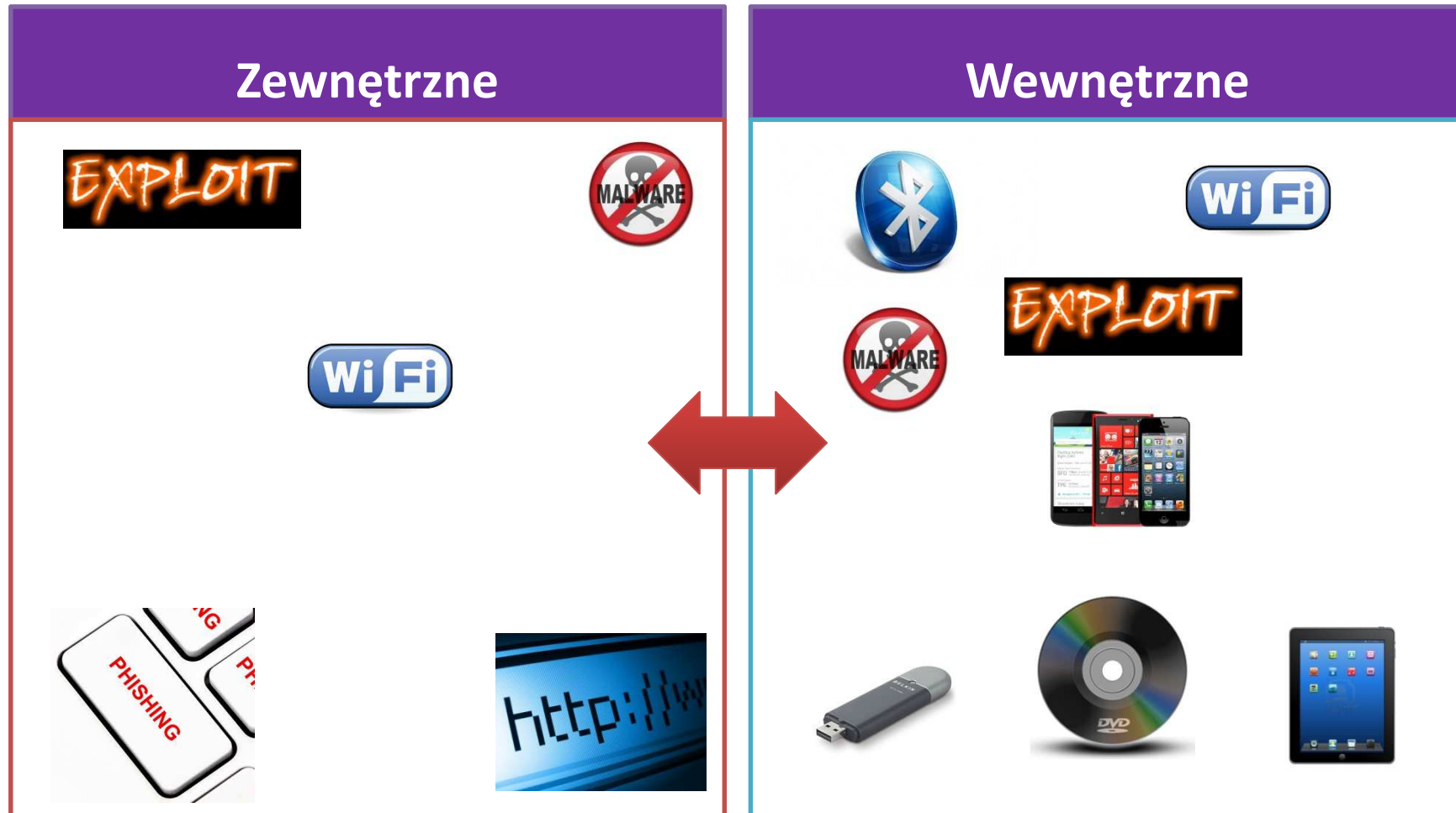
Studium przypadku łamania zabezpieczeń w systemach bankowych

Aleksander P. Czarnowski

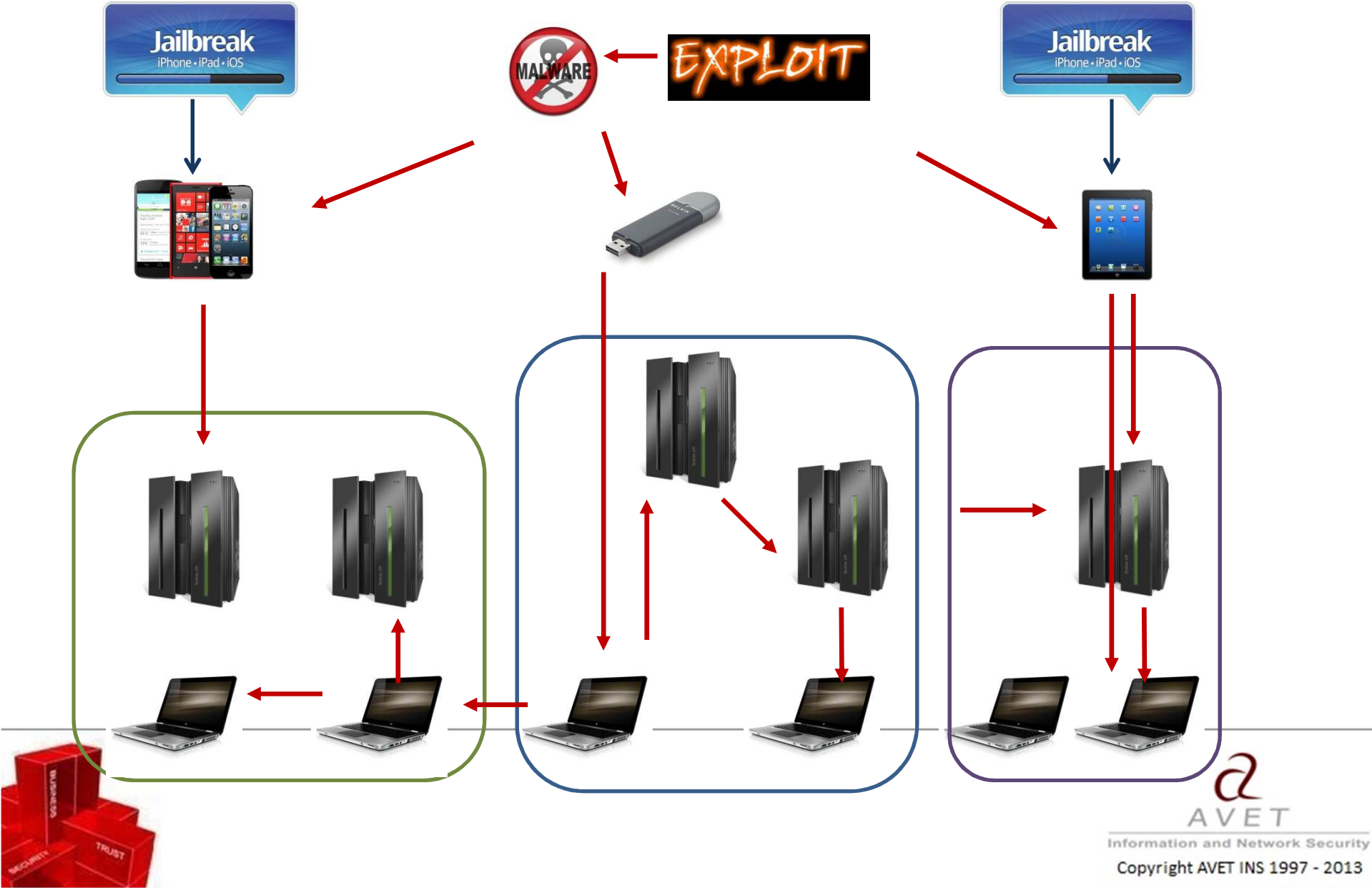
AVET Information and Network Security Sp. z o.o.



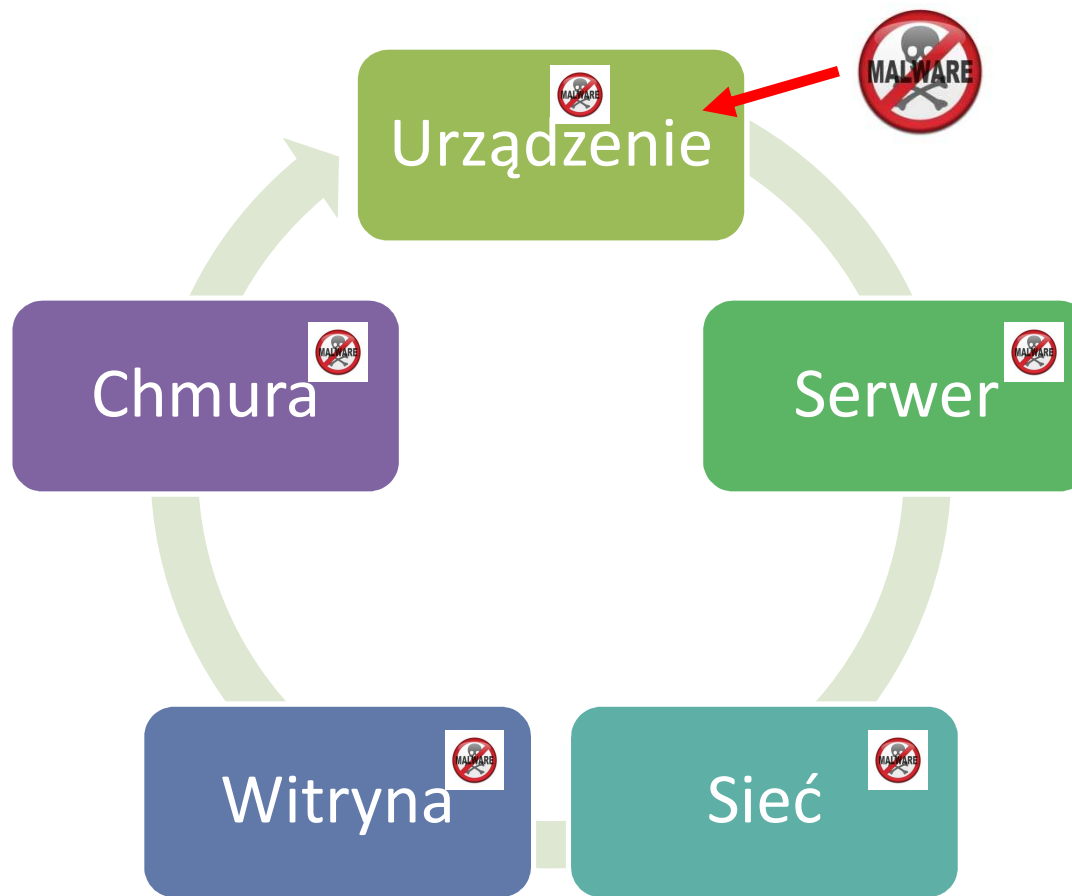
Podział na zagrożenia



BYOD



BYOD

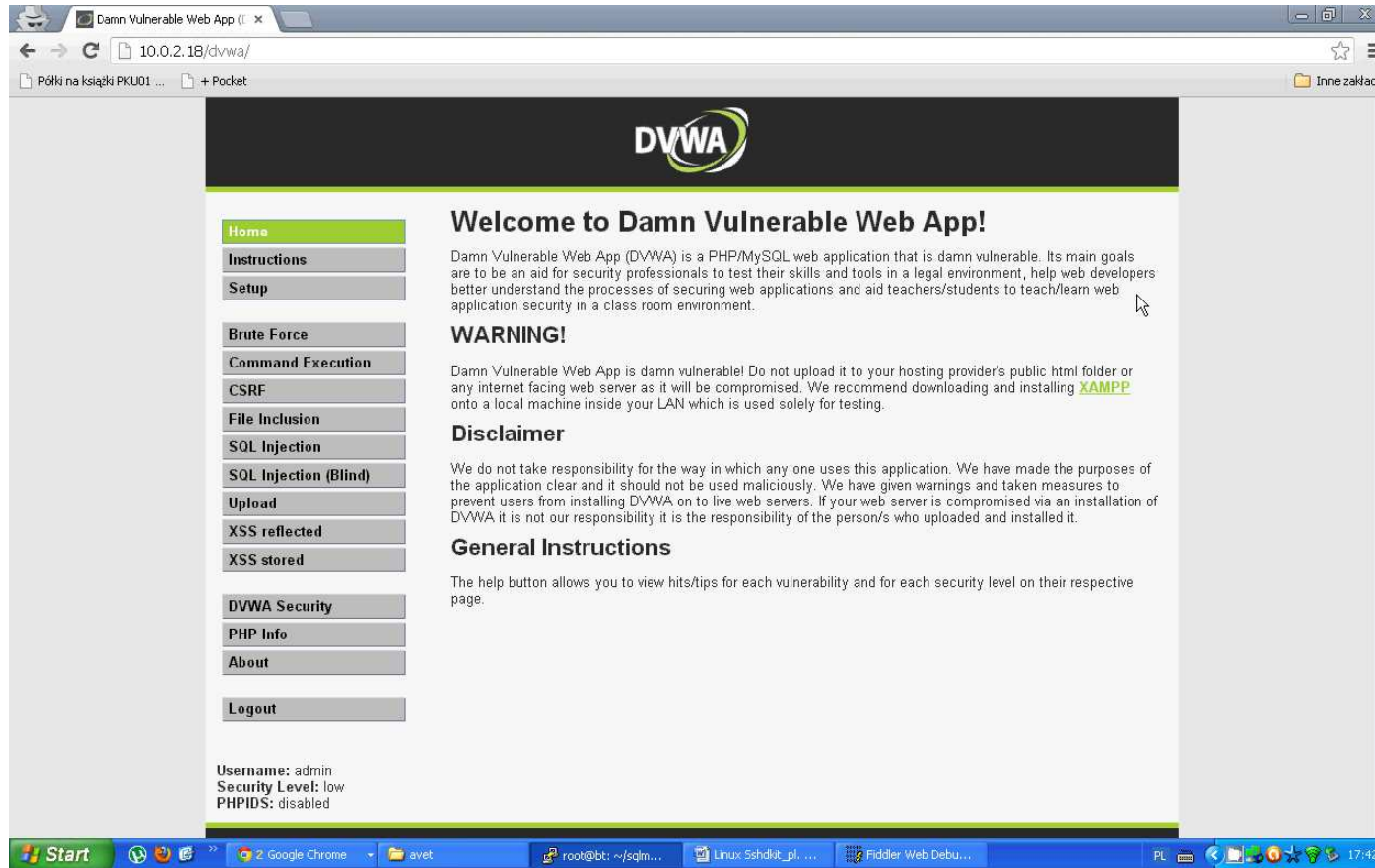


3 przypadki poważnych podatności

- 1) Dlaczego testowe systemy nie zawsze ujawniają poważne błędy które występują w środowiskach produkcyjnych
- 2) Dlaczego generowanie dokumentów dla klienta może przerodzić się w wyciek informacji
- 3) Jak pobrać fragmenty księgi głównej przez moduł logowania do systemu e-bankingu



Demonstracja



The screenshot shows a web browser window displaying the homepage of the Damn Vulnerable Web App (DVWA). The browser's address bar shows the URL `10.0.2.18/dvwa/`. The page features a navigation menu on the left with options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area includes a welcome message, a warning about not uploading the app to a public web server, a disclaimer, and general instructions. The system tray at the bottom shows the time as 17:42.

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Username: admin
Security Level: low
PHPIDS: disabled



Dziękuję za uwagę

Podsumowanie

- Zagrożenia zmieniają się w dynamiczny sposób
- Standardy i regulacje prawne nie nadążają za technologią
- Aplikacje i systemy należy testować pod kątem bezpieczeństwa
- Aby odpowiednio zaadresować ryzyko najpierw trzeba dobrze rozumieć zagrożenie
- Krótsze czasy realizacji transakcji sprzyjają fraudom

Kontakt

- aleksander.czarnowski@avet.com.pl

