AEC
DATA SECURITY

Aktuální stav bezpečnosti finančních aplikací

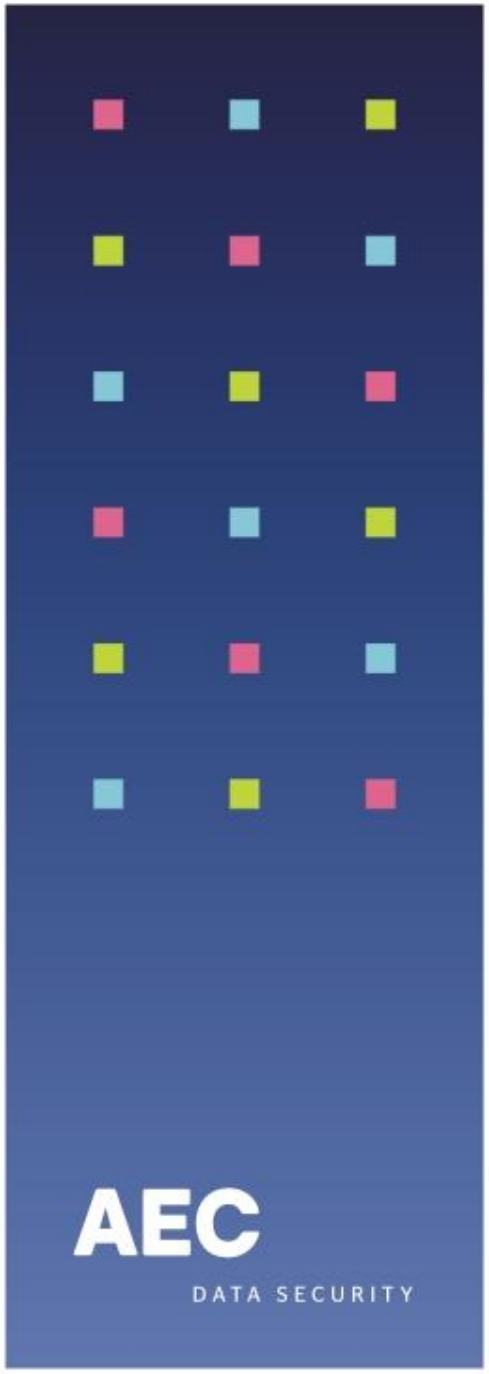
Michal Drozd
Security 2010
17. 2. 2010

Obsah

1. Seznámení s problematikou
   - Sledované aplikace
   - Kategorie rizik
   - Kategorizace zranitelností dle OWASP
2. Výsledné hodnocení
   - Detailní výsledky statistiky
   - Poměry nejčastějších zranitelností
3. Představení nejčastějších zranitelnosti

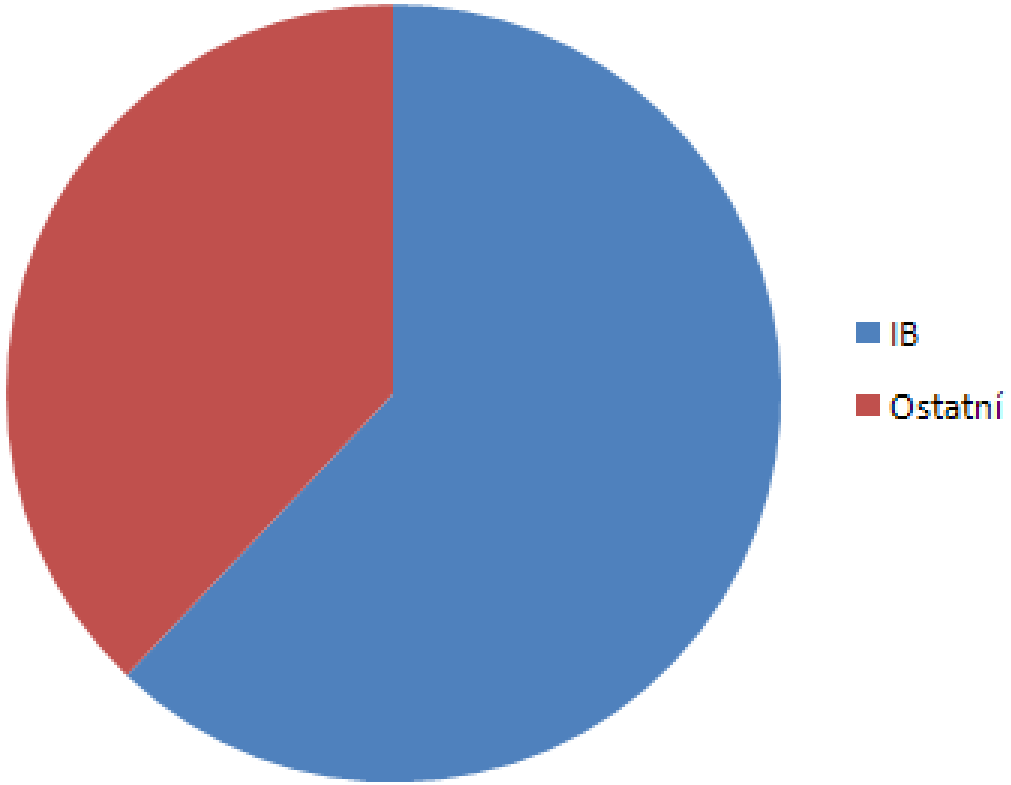
Cil:

Vytvoření vlastního názoru



Zastoupení aplikací

Celkem 29 aplikací …



OBSAHUJE

Internetové bankovnictví

62%

Ostatní aplikace

- finanční management
- pojistné aplikace
- …

38%

NEOBSAHUJE

- e-shopy
- Státní zprávy
- Běžné www portály
- …

Hodnocení rizika nálezu

- kriticky závažná chyba (KRITICKÁ) – CRITICAL

Jako kritické chyby jsou označeny nedostatky, které byly při testech zneužity a vedly (případn
mohou vést) k přímé kompromitaci testovaného systému.

- závažné chyby (VYSOKÁ) – HIGH

Jako závažné klasifikujeme chyby, které bezprostředně umožňují kompromitaci systému, či jeho nedostupnost. U těchto chyb existuje velmi vysoká pravděpodobnost zneužití. Jejich okamžitá náprava je nutná.

- středně závažné chyby (STŘEDNÍ) – MEDIUM

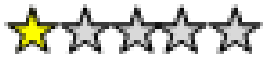
Do této kategorie spadají chyby, jejichž využití k potenciálnímu útoku na IS je technologicky náročnější na realizaci, nebo které umožňují průnik do systému pouze v případě splnění několika určitých navzájem souvisejících podmínek. Jejich závažnost nelze podceňovat s ohledem na potenciálně hrozící zneužití.

- méně závažné chyby (NÍZKÁ) – LOW

Tato kategorie zahrnuje méně závažné chyby, které napomáhají napadení systému. Např. poskytují potenciálnímu útočníkovi informace, jež lze uplatnit v rámci útoku na IS - organizace o svém IS prozrazuje více, než je nezbytně nutné. Ve většině případů se jedná pouze o konfigurační opomenutí apod.

- (INFORMATIVNÍ) – INFO

Informativní kategorie označuje vše, co lze zjistit o systémech a sítích, aniž by bylo možné jakýmkoliv způsobem zabránit úniku těchto informací. Tyto údaje nejsou většinou příliš důležité pro vedení vlastního útoku, ale mnohdy mohou napomoci útočníkovi při dokreslení č doplnění celkového obrazu o cíli potenciálního napadení.

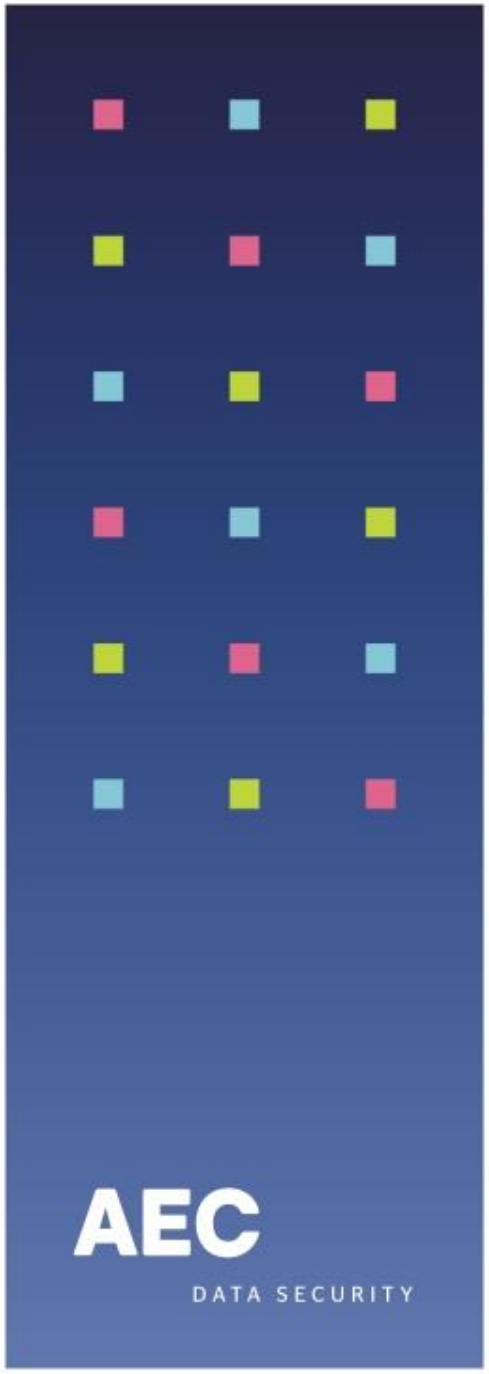


AEC
DATA SECURITY

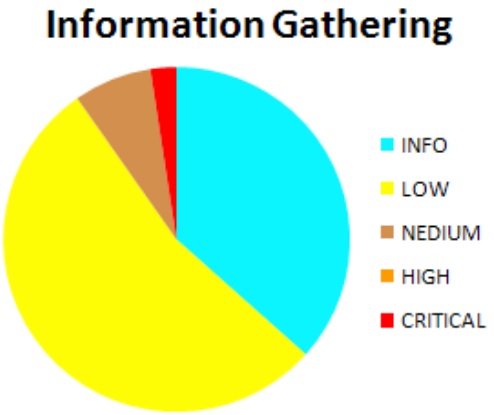
OWASP Testing Guide v3

Metodologie pro penetrační testování

1. Information Gathering
2. Configuration Management Testing
3. Authentication Testing
4. Session Management Testing
5. Authorization testing
6. Business logic testing
7. Data Validation Testing
8. Denial of Servis (DoS) Testing
9. Web Services Testing
10. AJAX Testing

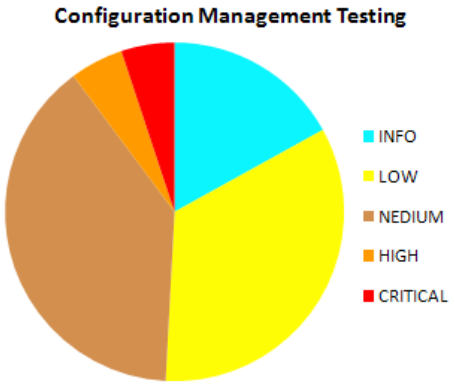


Information Gathering 1/10
OWASP-IG-001 - Spiders, Robots and Crawlers
OWASP-IG-002 - Search Engine Discovery/Reconnaissance
OWASP-IG-003 - Identify application entry points.
OWASP-IG-004 - Testing for Web Application Fingerprint
OWASP-IG-005 - Application Discovery
OWASP-IG-006 - Analysis of Error Codes - Information Disclosure



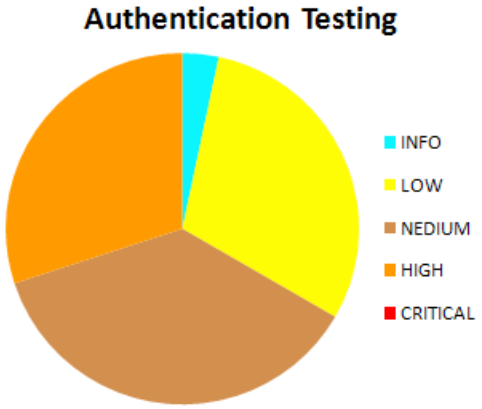
- Únik informací z HTTP hlaviček
- Únik informací z vystavených dokumentů
- Přítomnost zapomenutých aplikací
- Kritická zranitelnost aplikačního serveru
- Email addresses readable for bots
- Information leakage about used technologies

Configuration Management Testing 2/10
OWASP-CM-001 - SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) - SSL Weakness
OWASP-CM-002 - DB Listener Testing - DB Listener weak
OWASP-CM-003 - Infrastructure Configuration Management Testing
OWASP-CM-004 - Application Configuration Management Testing
OWASP-CM-005 - Testing for File Extensions Handling
OWASP-CM-006 - Old, backup and unreferenced files
OWASP-CM-007 - Infrastructure and Application Admin Interfaces - Access to Admin interfaces
OWASP-CM-008 - Testing for HTTP Methods and XST - HTTP Methods enabled, XST permitted, HTTP Verb



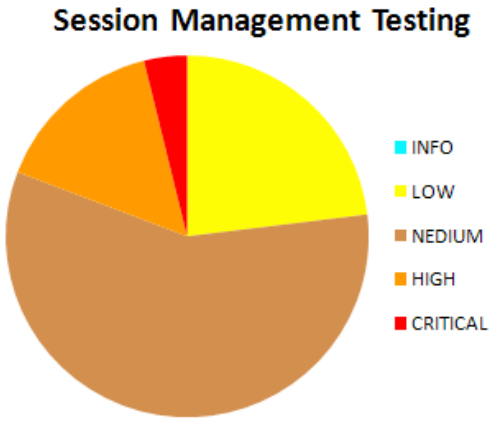
- Akceptace slabých šifer SSL
- Prozrazení interních IP adres
- Nekorektní chování aplikace
- Kontrola nahrávaných souborů
- Únik informací – podporovaná metoda OPTIONS

Authentication Testing 3/10
OWASP-AT-001 - Credentials transport over an encrypted channel
OWASP-AT-002 - Testing for user enumeration - User enumeration
OWASP-AT-003 - Testing for Guessable (Dictionary) User Account
OWASP-AT-004 - Brute Force Testing - Credentials Brute forcing
OWASP-AT-005 - Testing for bypassing authentication schema
OWASP-AT-006 - Testing for vulnerable remember password and pwd reset
OWASP-AT-007 - Testing for Logout and Browser Cache Management
OWASP-AT-008 - Testing for CAPTCHA - Weak Captcha implementation
OWASP-AT-009 - Testing Multiple Factors Authentication - Weak Multiple Factors Authentication
OWASP-AT-010 - Testing for Race Conditions



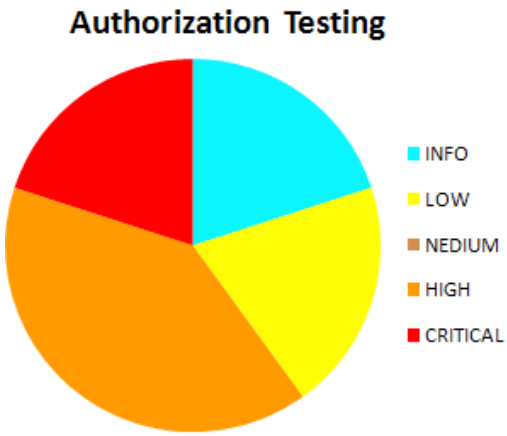
- Přístupná NTLM autentizace k serveru v doméně
- Možnost automatizované enumerace uživatelů
- Replay Attack
- Chyba v autorizaci – veřejně dostupná data uživatele
- Povolená vlastnost AUTOCOMPLETE

Session Management 4/10
OWASP-SM-001 - Testing for Session Management Schema - Bypassing Session Management Schema, Weak Session Token
OWASP-SM-002 - Testing for Cookies attributes - Cookies are set not ‘HTTP Only’, ‘Secure’, and no time validity
OWASP-SM-003 - Testing for Session Fixation
OWASP-SM-004 - Testing for Exposed Session Variables
OWASP-SM-005 - Testing for CSRF – CSRF



- Session Stealing
- Session Fixation
- Slabé session ID - možnost uneseni relace
- Session ID součástí URL
- Slabé Session ID
- CSRF vulnerability

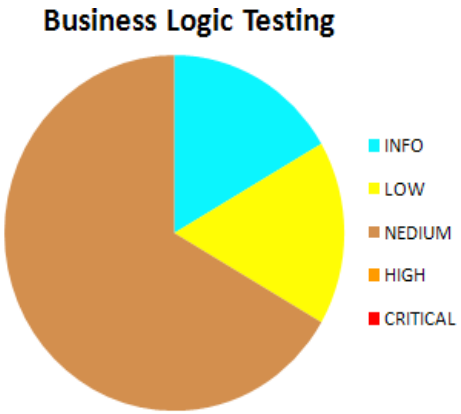
Authorization Testing 5/10
OWASP-AZ-001 - Testing for Path Traversal
OWASP-AZ-002 - Testing for bypassing authorization schema
OWASP-AZ-003 - Testing for Privilege Escalation



- Možnost podvržení klíčového páru
- Obejití druhé fáze autentizace
- Obejití autorizace
- Viditelné soubory ostatních uživatelů

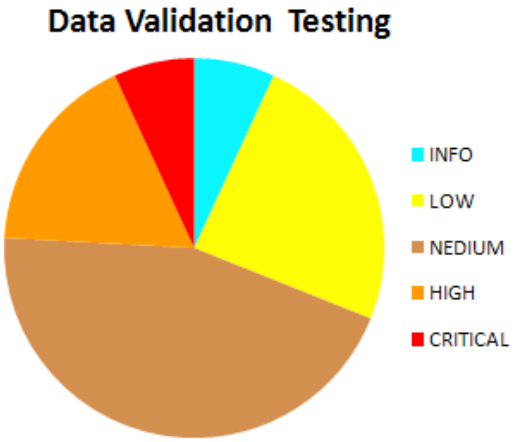
Business logic testing 6/10

OWASP-BL-001 - Testing for Business Logic - Bypassable business logic



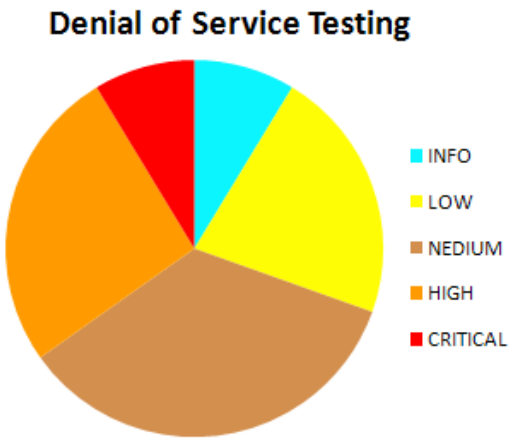
- User can modify foreign cID
- No limits for SMS messages
- Missing countdown timer
- Možnost deaktivace paralelního kanálu ověřování plateb

Data Validation Testing 7/10
Improper Input/Output Validation
OWASP-DV-001 - Testing for Reflected Cross Site Scripting - Reflected XSS
OWASP-DV-002 - Testing for Stored Cross Site Scripting - Stored XSS
OWASP-DV-003 - Testing for DOM based Cross Site Scripting - DOM XSS
OWASP-DV-004 - Testing for Cross Site Flashing - Cross Site Flashing
OWASP-DV-005 - SQL Injection
OWASP-DV-006 - LDAP Injection
OWASP-DV-007 - ORM Injection
OWASP-DV-008 - XML Injection
OWASP-DV-009 - SSI Injection
OWASP-DV-010 - XPath Injection
OWASP-DV-011 - IMAP/SMTP Injection
OWASP-DV-012 - Code Injection
OWASP-DV-013 - OS Commanding
OWASP-DV-014 - Buffer overflow
OWASP-DV-015 - Incubated vulnerability
OWASP-DV-016 - Testing for HTTP Splitting/Smuggling - HTTP Splitting, Smuggling



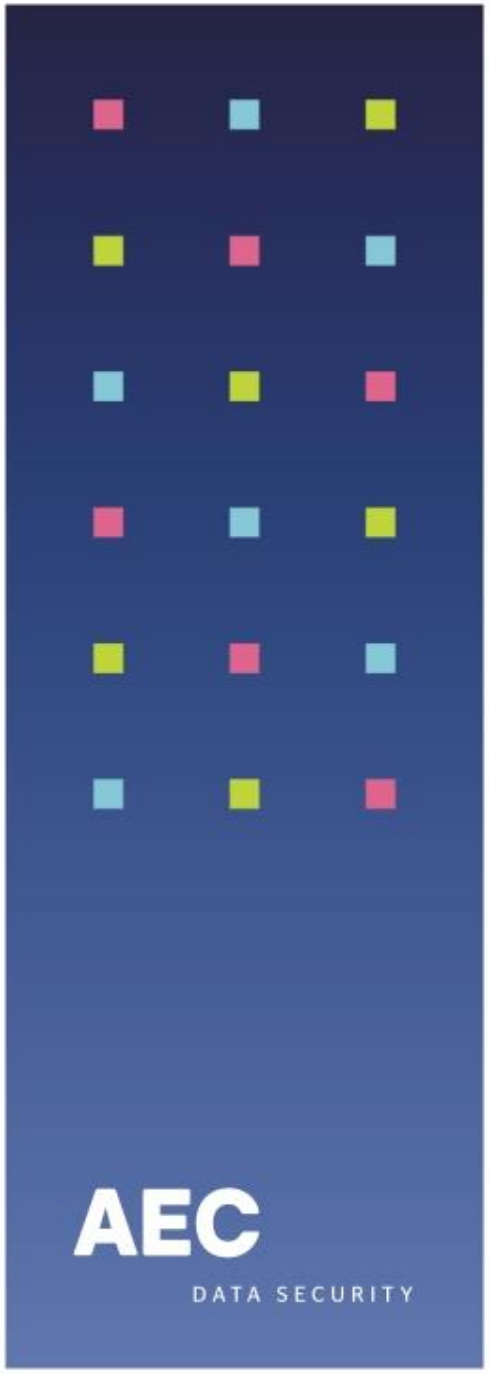
- Nekorektní validace parametrů
- Podvržení modifikovaných dat
- Obejití kontroly vkládaných dat při modifikaci uživatele
- XSS non-persistant
- XSF
- SQL Injection

Denial of Service Testing 8/10
Instable application
OWASP-DS-001 - Testing for SQL Wildcard Attacks
OWASP-DS-002 - Locking Customer Accounts
OWASP-DS-003 - Testing for DoS Buffer Overflows
OWASP-DS-004 - User Specified Object Allocation
OWASP-DS-005 - User Input as a Loop Counter
OWASP-DS-006 - Writing User Provided Data to Disk
OWASP-DS-007 - Failure to Release Resources
OWASP-DS-008 - Storing too Much Data in Session

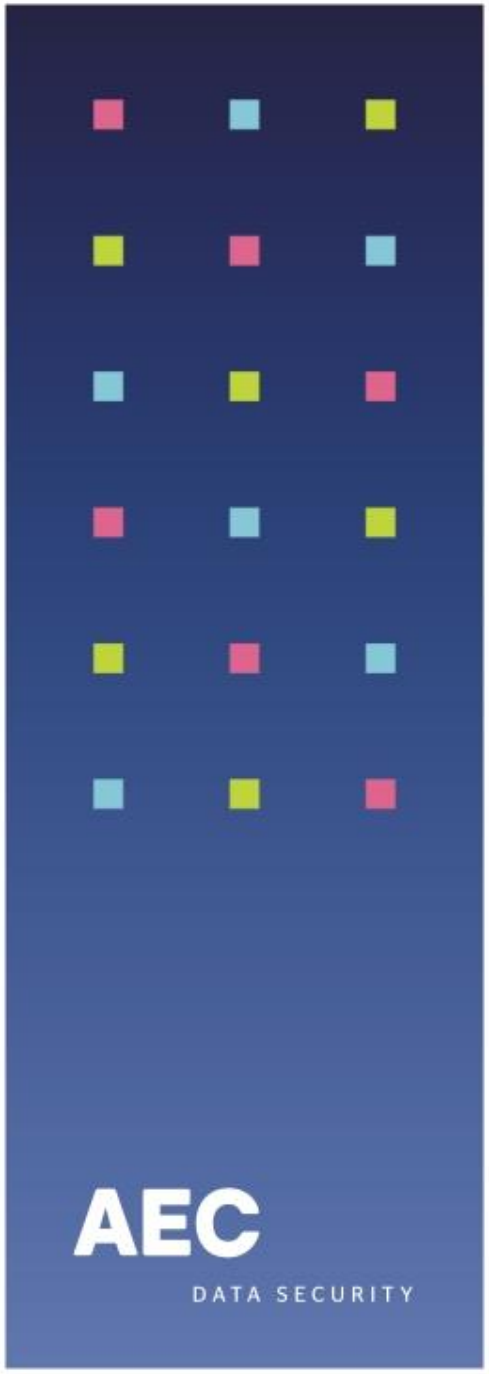


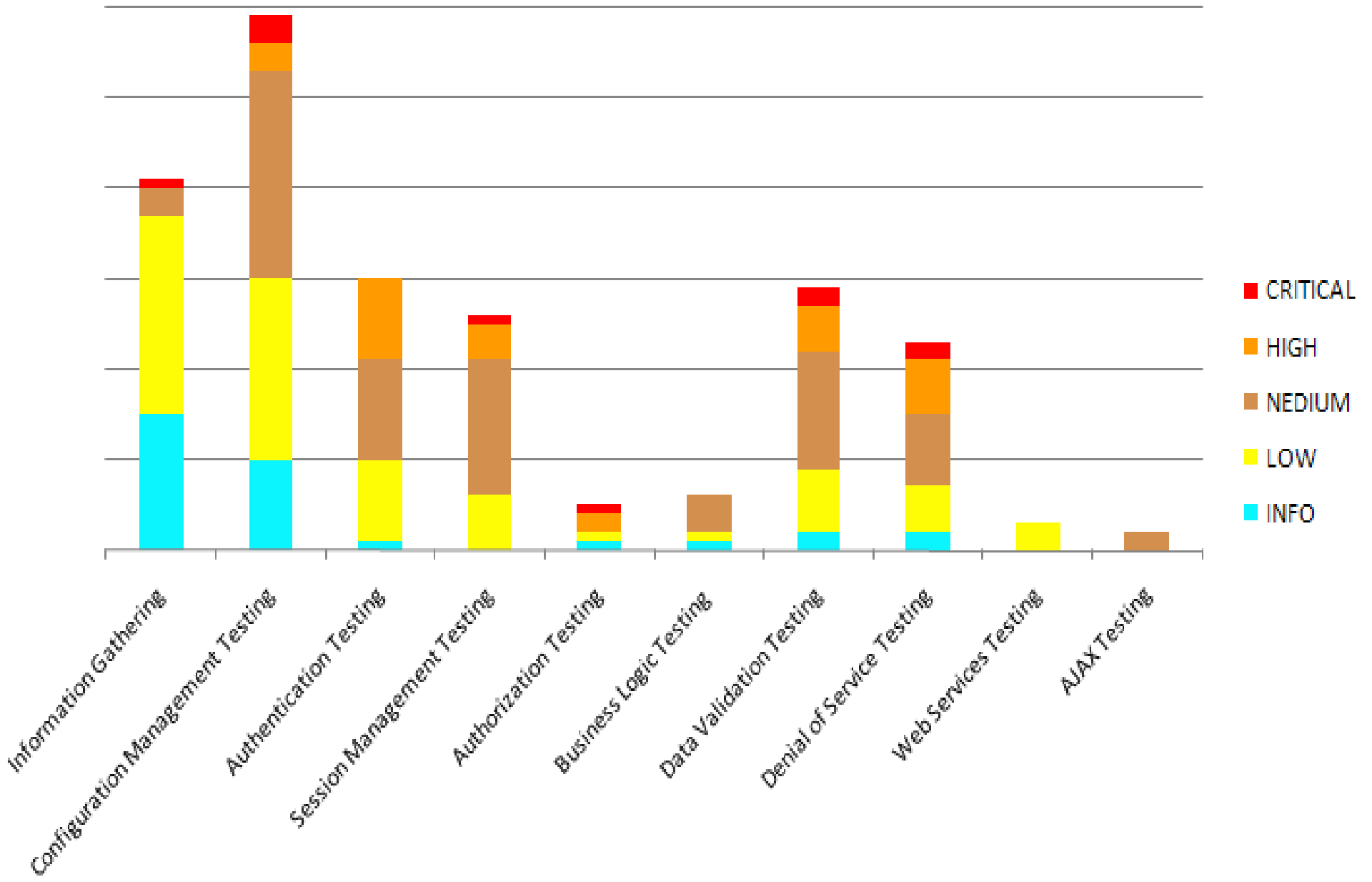
- DoS – automatizované zablokování uživatelských účtů
- Instability of the application
- Looping the application
- The possibility of DoS attack

Web Services Testing 9/10
OWASP-WS-001 - WS Information Gathering
OWASP-WS-002 - Testing WSDL
OWASP-WS-003 - XML Structural Testing
OWASP-WS-004 - XML Content-level Testing
OWASP-WS-005 - HTTP GET parameters/REST Testing
OWASP-WS-006 - Naughty SOAP attachments
OWASP-WS-007 - Replay Testing



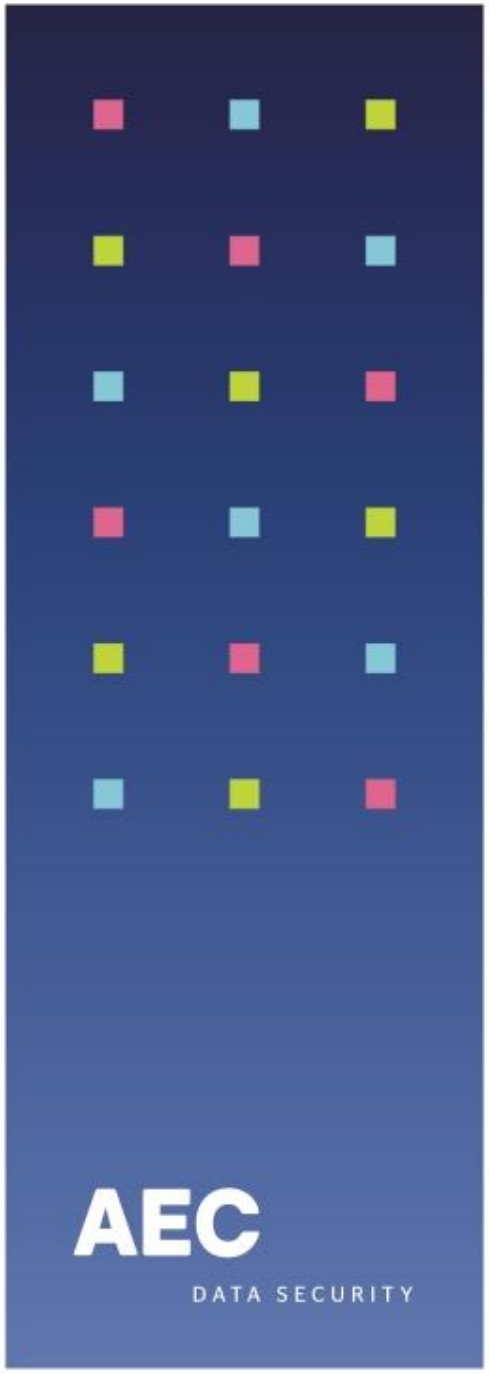
Ajax Testing 10/10
OWASP-AJ-001 – AJAX Vulnerabilities
OWASP-AJ-002 – Testing for AJAX



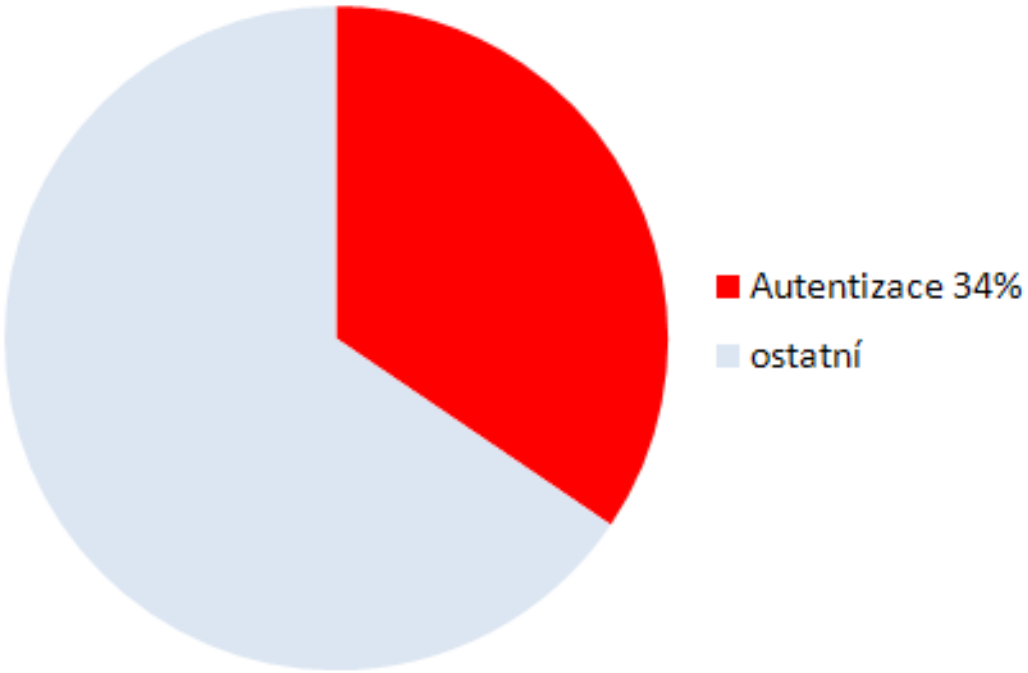

CRITICAL
HIGH
NEDIUM
LOW
INFO
Information Gathering
Configuration Management Testing
Authentication Testing
Session Management Testing
Authorization Testing
Business Logic Testing
Data Validation Testing
Denial of Service Testing
Web Services Testing
AJAX Testing

Nejčastější identifikované vážné nedostatky

1. Autentizace
2. DoS
3. XSS
4. Session management
5. SQL Injection



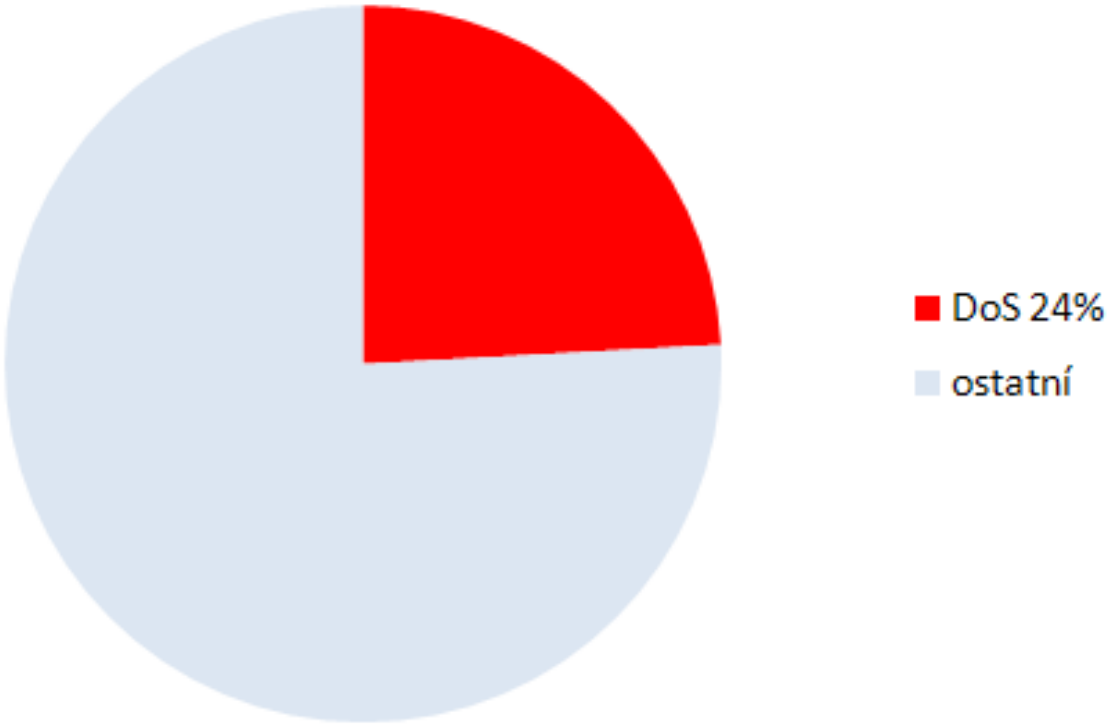
Autentizace – 34%



Autentizace operace vs. autentizace uživatele
Spojeno se session mng. a configuration mng.

- Obejití fáze autentizace
- Slabá autentizace
- Nedostatečné zabezpečení účtů
- Možnost enumerace účtu
- Prostředí přístupné bez autentizace
- Opomenutá konfigurace (formulář + NTLM)

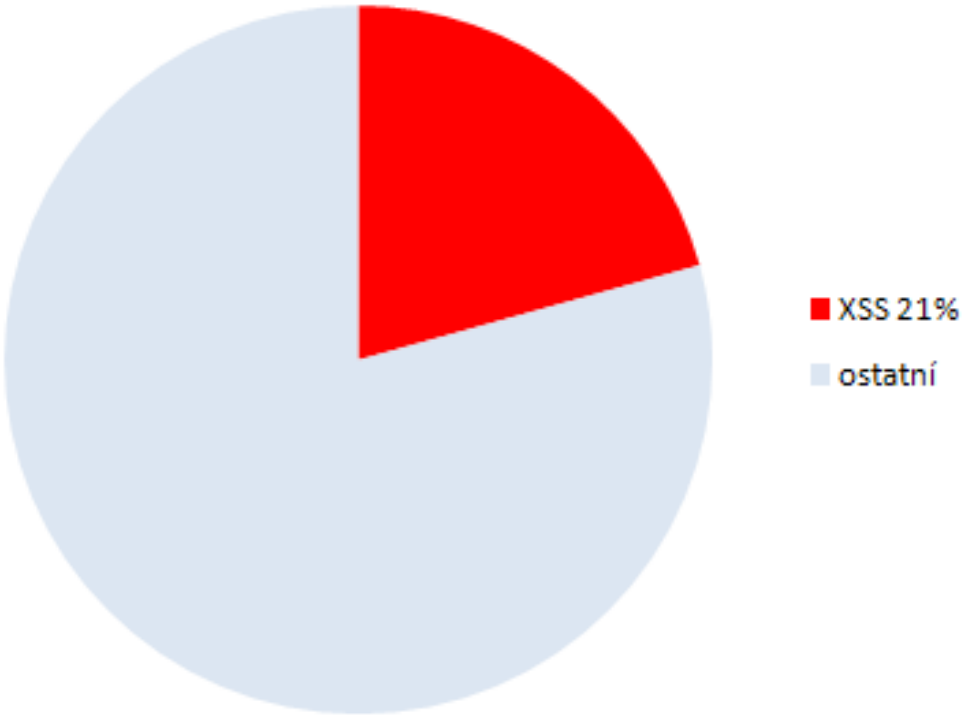
DoS - Denial of service – 24%



Vyčerpání paměti
Úzké hrdlo mezi app a db
Zamykání účtů

AEC
DATA SECURITY

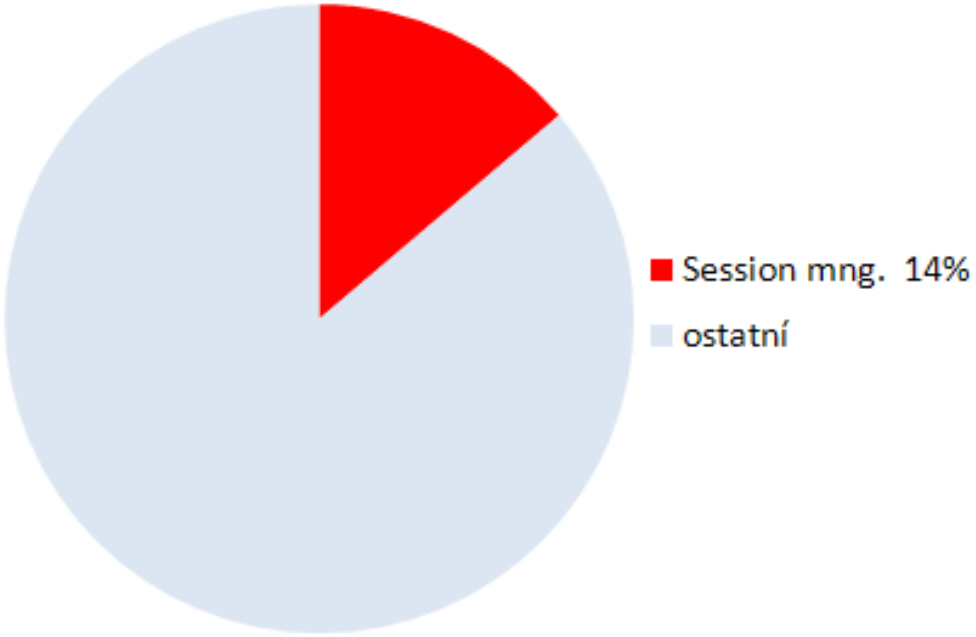
XSS – Cross Site Scripting – 21%



Non-Persistent (reflected)
Persisten (stored)
DOM Based

AEC
DATA SECURITY

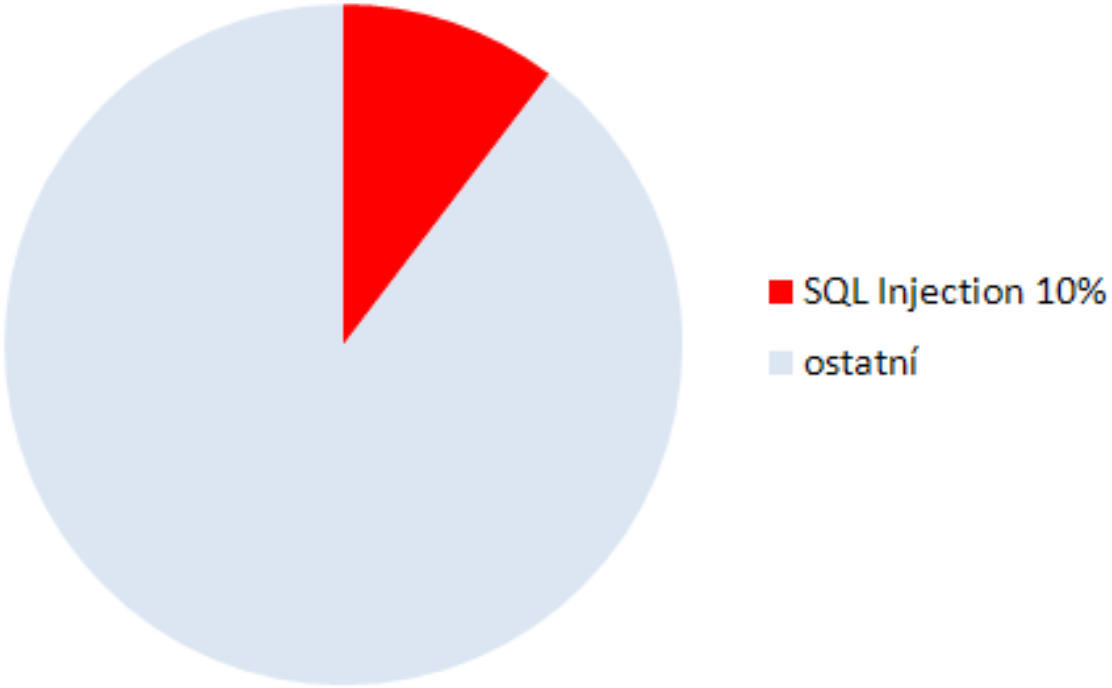
Session management – 14%



Session ID není vázáno na uživatele
Jednoduché SID (v URL)
Paralelní relace

AEC
DATA SECURITY

SQL Injection – 10%



Blind — Obtížné

Nejobtížnější detekce, následuje outband

Out-band — Těžší

Výstup je generován prostřednictvím síťové funkce

In-band — Lehké

Generuje přímé chybové hlášení - nejtriviálnější zneužití

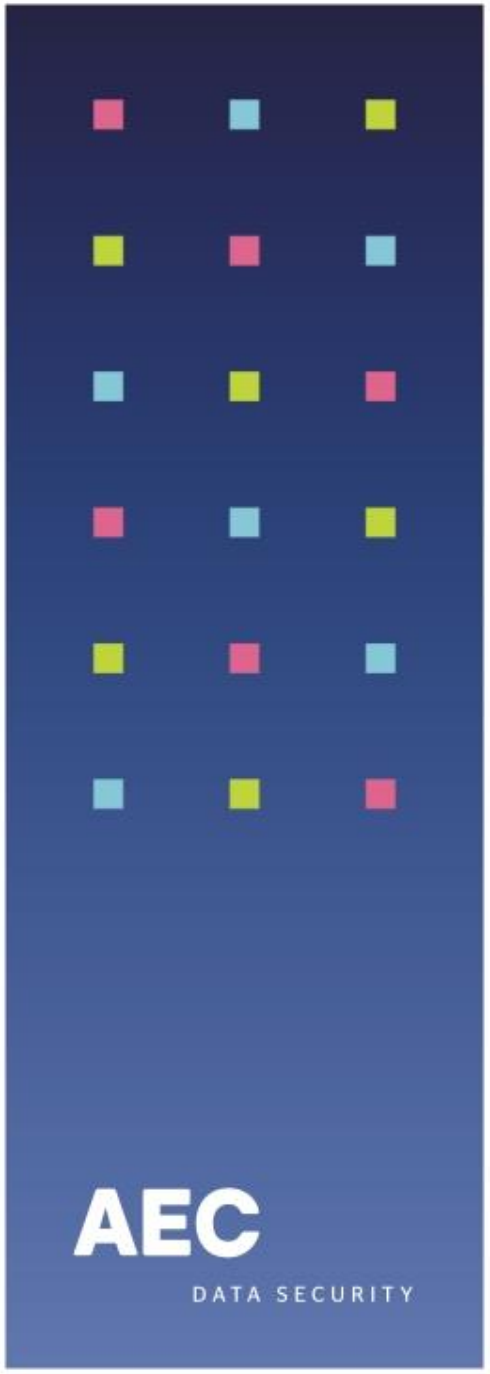
AEC
DATA SECURITY

Závěrem

- Výsledky penetračních testů 29 finančních aplikací auditovaných společností AEC
- Nejčastější zranitelností v oblasti configuration managementu
- Nejvážnější zranitelnosti v oblasti autentizace a validace dat

Cil:

Vytvoření vlastního názoru



AEC
DATA SECURITY

Děkuji za pozornost!

- prostor pro otázky -

AEC

DATA SECURITY

Děkuji za pozornost!

- prostor pro otázky -

Michal Drozd
michal.drozd@aec.cz

AEC, spol. s r.o. · Spielberk Office Centre
Holandská 878/2 · 639 00 Brno · Czech Republic
Phone: +420 541 235 466 · Fax: +420 541 235 038

AEC, spol. s r.o. · European Business Center
Dukelských hrdinů 34 · 170 00 Praha 7 · Czech Republic
Phone: +420 267 311 402 · Fax: +420 266 177 155

www.aec.cz

AEC

DATA SECURITY

Michal Drozd
micha.drozd@aec.cz

AEC, spol. s r.o. · Spielberk Office Centre
Holandská 878/2 · 639 00 Brno · Czech Republic
Phone: +420 541 235 466 · Fax: +420 541 235 038

AEC, spol. s r.o. · European Business Center
Dukelských hrdinů 34 · 170 00 Praha 7 · Czech Republic
Phone: +420 267 311 402 · Fax: +420 266 177 155

www.aec.cz