WEBALKALMAZÁSOK BIZTONSÁGA

Bordás Ákos
MSC I.

„Programming is like sex because one mistake and you have to support it for the rest of your life.”

Bevezetés

- Régen statikus oldalak, ma már dinamikus webalkalmazások
- Komoly, összetett rendszerek Pl.: webshopok, netbankok, közösségi oldalak
- Nagy konkurencia a webes piacon
- Megnőtt az érdeklődés a hibák iránt is

Támadási típusok

A

- Account lockout attack
- Argument Injection or Modification
- Asymmetric resource consumption (amplification)

B

- Binary planting
- Blind SQL Injection
- Blind XPath Injection
- Brute force attack
- Buffer overflow attack

C

- CSRF
- Cache Poisoning
- Code Injection
- Command Injection
- Comment Injection Attack
- Cross Frame Scripting
- Cross Site History Manipulation (XSHM)
- Cross Site Tracing
- Cross-Site Request Forgery (CSRF)
- Cross-User Defacement
- Cross-site Scripting (XSS)
- Cryptanalysis
- Custom Special Character Injection

D

- Denial of Service
- Direct Dynamic Code Evaluation ('Eval Injection')
- Direct Static Code Injection
- Double Encoding

F

- Forced browsing
- Format string attack
- Full Path Disclosure

H

- HTTP Request Smuggling
- HTTP Response Splitting

L

- LDAP injection

M

- Man-in-the-browser attack
- Man-in-the-middle attack
- Mobile code: invoking untrusted mobile code
- Mobile code: non-final public field
- Mobile code: object hijack

N

- Network Eavesdropping

O

- One-Click Attack
- Overflow Binary Resource File

P

- Page Hijacking
- Parameter Delimiter
- Path Manipulation

P cont.

- Path Traversal

R

- Regular expression Denial of Service - ReDoS
- Relative Path Traversal
- Repudiation Attack
- Resource Injection

S

- SQL Injection
- Server-Side Includes (SSI) Injection
- Session Prediction
- Session fixation
- Session hijacking attack
- Setting Manipulation
- Special Element Injection
- Spyware

T

- Traffic flood
- Trojan Horse

U

- Unicode Encoding

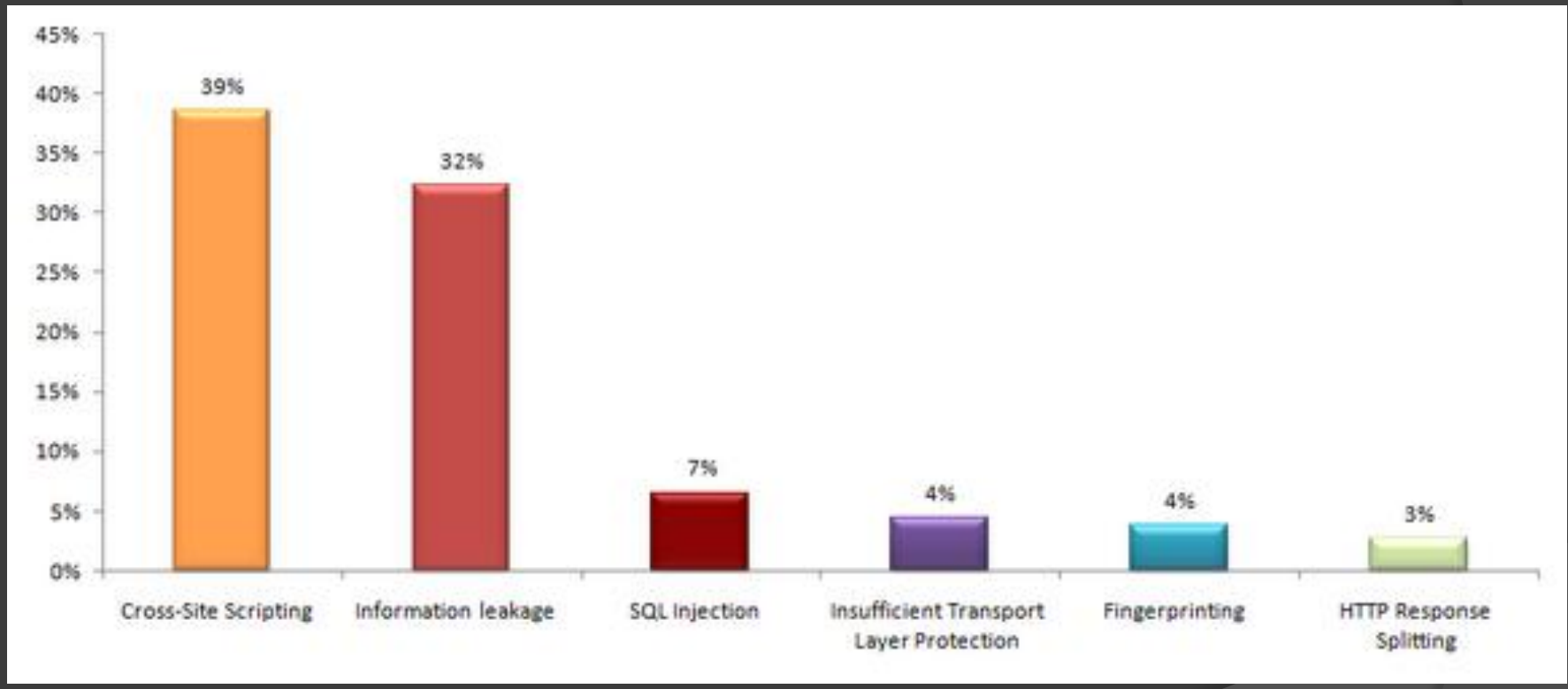
W

- Web Parameter Tampering
- Windows ::DATA alternate data stream

X

- XPATH Injection
- XSRF

Legelterjedtebb támadások



A biztonságról általában

- Teljesen biztonságos rendszer nem létezik
- „Minden rendszer éppen olyan biztonságos mint annak a leggyengébb pontja.”
- Általános elv: „Minden adat, ami a felhasználótól érkezik, veszélyes.”
- Megoldás: „Validálni, validálni validálni!”

SQL injection

- A webalkalmazás mögött lévő adatbázist támadják ezzel a módszerrel
- Alapelve: valamilyen módszerrel olyan kódot injektálnak a rendszerbe, amit a háttérben lévő DBMS lefuttat
- Korábban ez a támadás vezette a legelterjedtebb támadások listáját
- Támadás okai: inputvalidáció hiánya, DBMS hibaüzenetei

SQL injection II.

- Megoldások:
- PHP esetén a mysql_real_escape_string() használata
- JSP esetén a prepared statement megoldja
- ASP.NET esetén reguláris kifejezésekkel vagy SqlParameterCollection()
- Scannerek: SQLiX, SQLMap, SQLninja, SCRAWLR, Acunetix

Cross Site Scripting (XSS)

- Általában injection jellegű támadás
- Nagyon sok típusa létezik
- Két alapvető csoport: perzisztens és non-perzisztens XSS
- Az esetek nagy részében javascript támadások
- DOM-alapú XSS, Karakterkódolásos XSS
- 2007 MySpace Samy virus

XSS védelem

- PHP esetén a strip_tags() vagy a htmlspecialchars() függvények
- JSP esetén vagy saját függvény, vagy JSLT használata esetén <c:out … escapeXml = „true”>
- ASP.NET esetén az AntiXSSLibrary.dll segítségével

Cross Site Request Forgery (CSRF)

- A szerver felé küldött kérés nincs azonosítva
- Böngésző áll a támadás középpontjában
- Könnyen figyelmen kívül hagyható, hiszen a HTTP kérést „nem látjuk”
- Kivédése: rövid session idő, referer ellenőrzőkód, automatikus kilépés

Session és a biztonság

- Session: csoportosítja a beérkező kéréseket, a csoportokat session azonosítóval különíti el
- Két alapvető módszer: session hijacking, session fixation

Header Injection

- Header injection

```
HTTP/1.0 302 Redirect
Location: http://www.pelda.com/index.php?lang=en
Connection: Keep-Alive
Content-Length: 0
```

- A kérést URL-en keresztül manipulálhatjuk

```
index.php?lang=en%0d%0aConnection:%20Keep-Alive%0d%0aContent-Length:
%200%0d%0a%0d%0aHTTP/1.0%20200%20OK%0d%0aContent-Type:%20text/html
%0a%0aContent-Length:%2020%0d%0a%0d%0a
<html>Ide jöhet a támadó kódrész!< /html>
```

Header Injection II.

```
HTTP/1.0 302 Redirect
Location: http://www.pelda.com/index.php?lang=en
Connection: Keep-Alive
Content-Length: 0

HTTP/1.0 200 OK
Content-Type: text/html
Content-Length: 20

<html>Ide jöhet a támadó kód!</html>
Connection: Keep-Alive
Content-Length: 0
```

Egyéb támadási pontok

- Fájlfeltöltés
- Hitelesítés
- Jelszavak, biztonsági kérdések
- Hibakezelés

Köszönöm a figyelmet!