securiTeam

Web Security

Tőke – tokesisr@gmail.com

securiTeam

Miért foglalkozunk web securityvel?

- 2013-as adatok szerint IT rendszerek elleni támadások 80% webs, vagy tartalmaz webes elemeket
- Tesztelt oldalak 86% tartalmaz KOMOLY sérülékenységet
- Userek által gyakran használt, megbízhatónak vélt felületek is lehetnek veszélyesek
- Pénz, pénz, pénz!!

securiteam

Támadás fajták

- Server side attack
  - **Sql injection** (7-50%)
  - File inclusion
  - Server side request forgery
  - ….
- Client side attack
  - **XSS** (>50%)
  - **Clickjacking**
  - Cross site request forgery
  - …

securiTeam

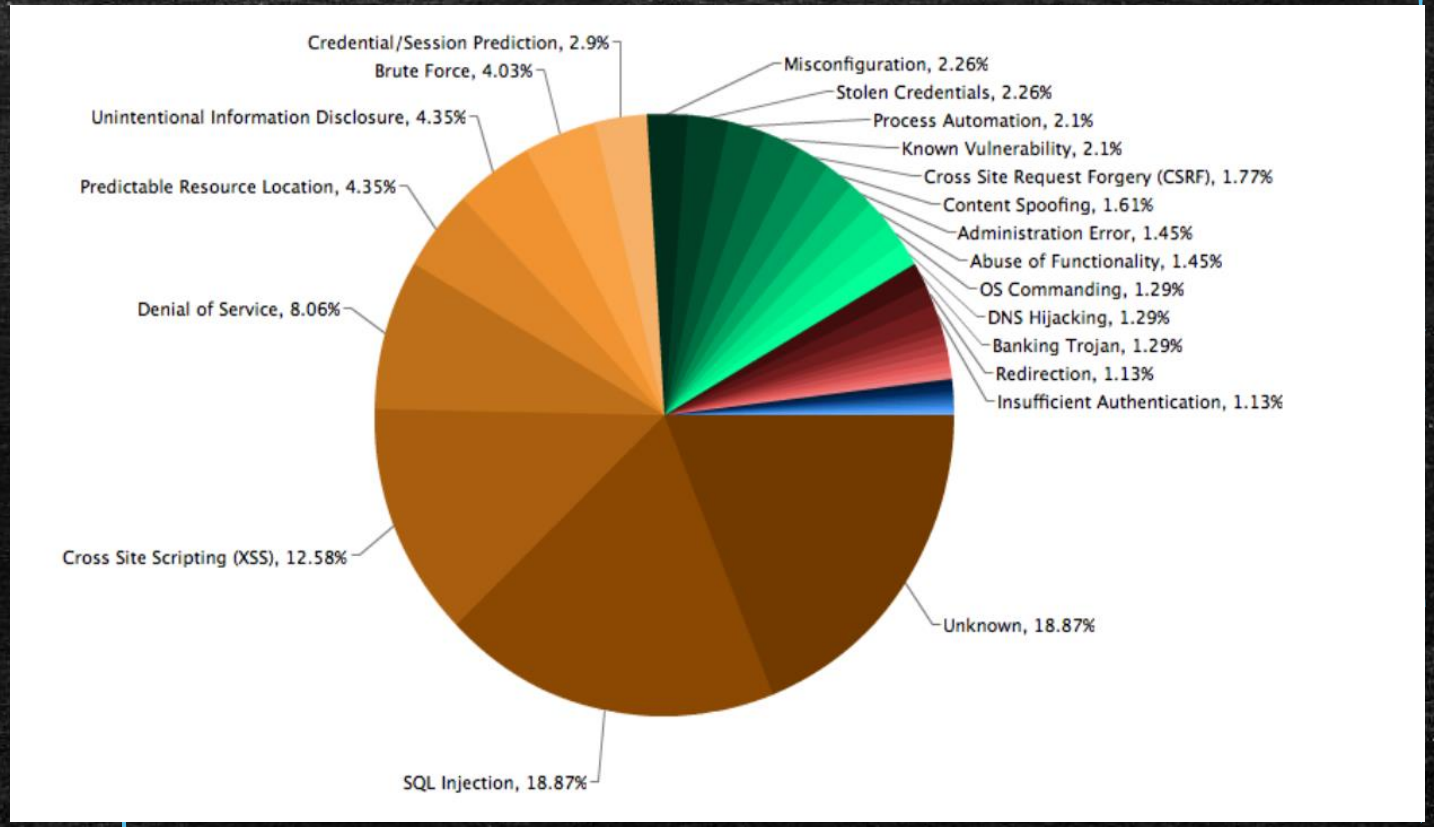
2011-es dia a támadásokról

SQLi: 18.87%

XSS:12.58%

DoS: 8.06/%

UNKNOWN: 18.87%



securiTeam

SQL alapok

- Adatbázisokkal való kommunikációhoz
- SELECT, INSERT, UPDATE, DELETE, DROP, CREATE
- Pl: SELECT * FROM tablename WHERE attr1 > 0 AND attr2 LIKE '%s'
- Attack vectors: 1' or '1' = '1; UNION; --

securiteam

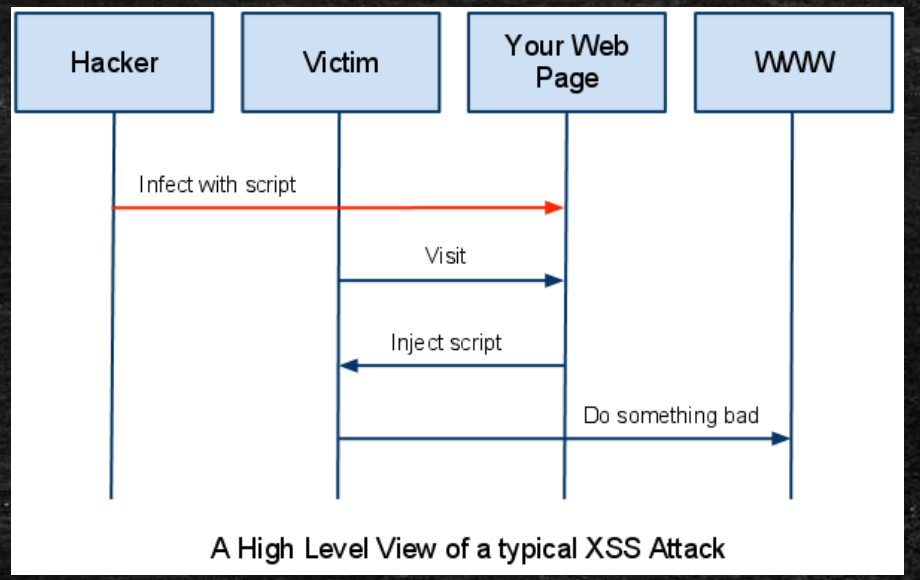
SQL injection

- Egy technika, amellyel a támadó SQL paranccsot ágyazhat egy lekérdezésbe weboldal input mezőjén keresztül
- SELECT * FROM Users WHERE UserId = 105 or 1=1
- Blind SQLi
- Nem validált user inputokból ered
- Védekezés, whitelist/blacklist

securiTeam

XSS – Cross Site Scripting

Leggyakrabban használt webes támadás



A High Level View of a typical XSS Attack

Attack vectors:

- <script>
- <body onload=alert("XSS") >
- <body background="javascipt:alert('XSS')">

securiteam

XSS fajták

- Persistent
  - A szerver tárolja az xss kódot, ami letöltéskor a kliensnél meghívódik
  - Pl: comment, üzenet, felhasználói adat
  - Tárolt adatbázis ad vissza veszélyes adatot
- Reflected:
  - Nincs a szerveren tárolva, post/get paraméterként utazik
  - Szerver szkript válaszol veszélyes adattal
- DOM based (nem foglalkozunk most vele)

securiTeam

Clickjacking

- Felhasználót rávenni, hogy olyan helyre kattintson, ahova a támadó szeretné
- Like gyűjtés, ajánlás gyűjtés (Facebook, twitter, ebay)
- Bank oldalánál nem kért átutalás, …
- Egér alatt lévő terület mozgatása
- Láthatatlan frame
- //nem csak JS, lehet FLASH, Silverlight, JAVA

Köszönöm