Silent Signal Kft.

Webáruházak biztonsági vizsgálatainak lehetőségei és tapasztalatai

Szabó Péter

Veres-Szentkirályi András

2010.02.26.

Témáink

- Bevezető
- Vizsgálati módszerek, megközelítések
- Egy sérülékenységi vizsgálat lépései
- Tipikus biztonsági hibák és következményeik webáruházaknál
- Konkrét esetek, példák

Bevezető

- Mennyire biztonságos az Ön webáruháza?
  - Miből tudja ezt?
- Lehet vizsgálni a webáruház biztonságát?
- Érdemes a biztonsággal foglalkozni?
  - Amíg nincs baj, addig még nem, ha pedig már baj van, akkor már nem?! – Nagy kockázat!
- Ki támadná az én webáruházamat?
- Nagyon nagy munka egy sikeres támadás végrehajtása, ritkán fordul elő ilyen. Ez tényleg így van?
- Melyek a tipikus hibák, és mit lehet velük elérni?

Kik vagyunk

Információtechnológia

↓

Informatikai biztonság

↓

Etikus hackelés

IT biztonsági tanácsadás

IT biztonsági oktatás

Etikus hackelés

- Legális autófeltörés - hacker technikák alkalmazása legális keretek között
- Teljes mértékben a megbízó adja a szabályokat
- Többfajta megközelítés, szerepkör
  - Hatókör
  - Információ bázis
  - Agresszivitás
- Nem kihasználjuk, hanem feltárjuk a biztonsági réseket!

Vizsgálati megközelítések

- **Black-box vizsgálat**
  - Információ nélkül, egy külső támadó lehetőségei a webáruház infrastruktúráján
- **Tulajdonságok:**
  - Feltárja a legtöbb kívülről kihasználható sérülékenységet
  - Rövidebb idő alatt elvégezhető
  - „Sötétben” kell a vizsgálatot végezni, így fontos az intuíció
  - Teljességre törekszik, de nem lehet teljeskörű
  - Működő rendszernél használható

Vizsgálati megközelítések

- **Grey-box vizsgálat**
  - Egy regisztrált felhasználó támadási lehetőségei a webáruház infrastruktúráján
  - Egy volt rendszergazda, fejlesztő támadási lehetőségei a webáruház infrastruktúráján
- **Tulajdonságok:**
  - A kezdő lépések megoldottak, így „mást” lehet vizsgálni
  - Vizsgálható, hogy egy valós felhasználó mit láthat a többi felhasználó adataiból
  - A kezdeti lépések után itt is „sötétben” kell a vizsgálatot végezni, így fontos az intuíció
  - Teljességre törekszik, de nem lehet teljeskörű
  - Működő rendszernél használható

Vizsgálati megközelítések

- **White-box vizsgálat**
  - Üzemeltetői, fejlesztői oldalról történő vizsgálat, a teljes rendszer ismeretében

- **Tulajdonságok:**
  - Minden ismert a vizsgáló fél részéről. (kód, beállítások, infrastruktúra, stb…)
  - Legidőigényesebb, de a legalaposabb
  - Fontos az intuíció, de itt lépésről-lépésre kell vizsgálni
  - Rendszerfejlesztés, bevezetés előtt a leghatékonyabb

Igénytől a jelentésig

- Pontos igénydefiniálás az ügyféllel
- Nincs két ugyanolyan projekt
- Az ajánlat tartalmazza, hogy pontosan milyen lépésekből áll a vizsgálat
- Részletes szerződés (mit, mikor, kapcsolattartás, titoktartás, stb.)
- Projekt közben folyamatos kapcsolattartás – A megrendelő minden lépésről tud
- Vizsgálati jelentés (Vizsgált területek, feltárt hibák, a hibák osztályozása, a hibák javításának módja)
- … (hibajavítás, oktatás, visszamérés)

Vizsgálat lépései

- Felderítés
  - Nyilvános forrásból megszerezhető információk (weboldalak, domain reg., keresők, stb…)
- Scannelés, letapogatás
  - Információszerzés a rendszer beállításairól, konfigurációjáról, szolgáltatásairól
- Hiba kihasználás
  - A megszerzett információk alapján hozzáférést szerezni a rendszerhez. Csak a szerződésben meghatározott módon!

Mit nyújt egy vizsgálat

- Pontosan lehet látni, hogy mekkora a baj
- Képet ad egy felkészült támadó lehetőségeiről
- A feltárt hibák kijavításával jelentősen javul a webáruház biztonsági szintje
- Utat mutat egy későbbi továbbfejlesztéshez
- Visszacsatolást ad a fejlesztőcsapat munkájáról
- Kiderülhet, mi a leggyengébb láncszem a rendszerben
- Hogyan reagál a rendszer egy támadásra
- Éles indulás előtt kivédhetők a biztonsági problémák

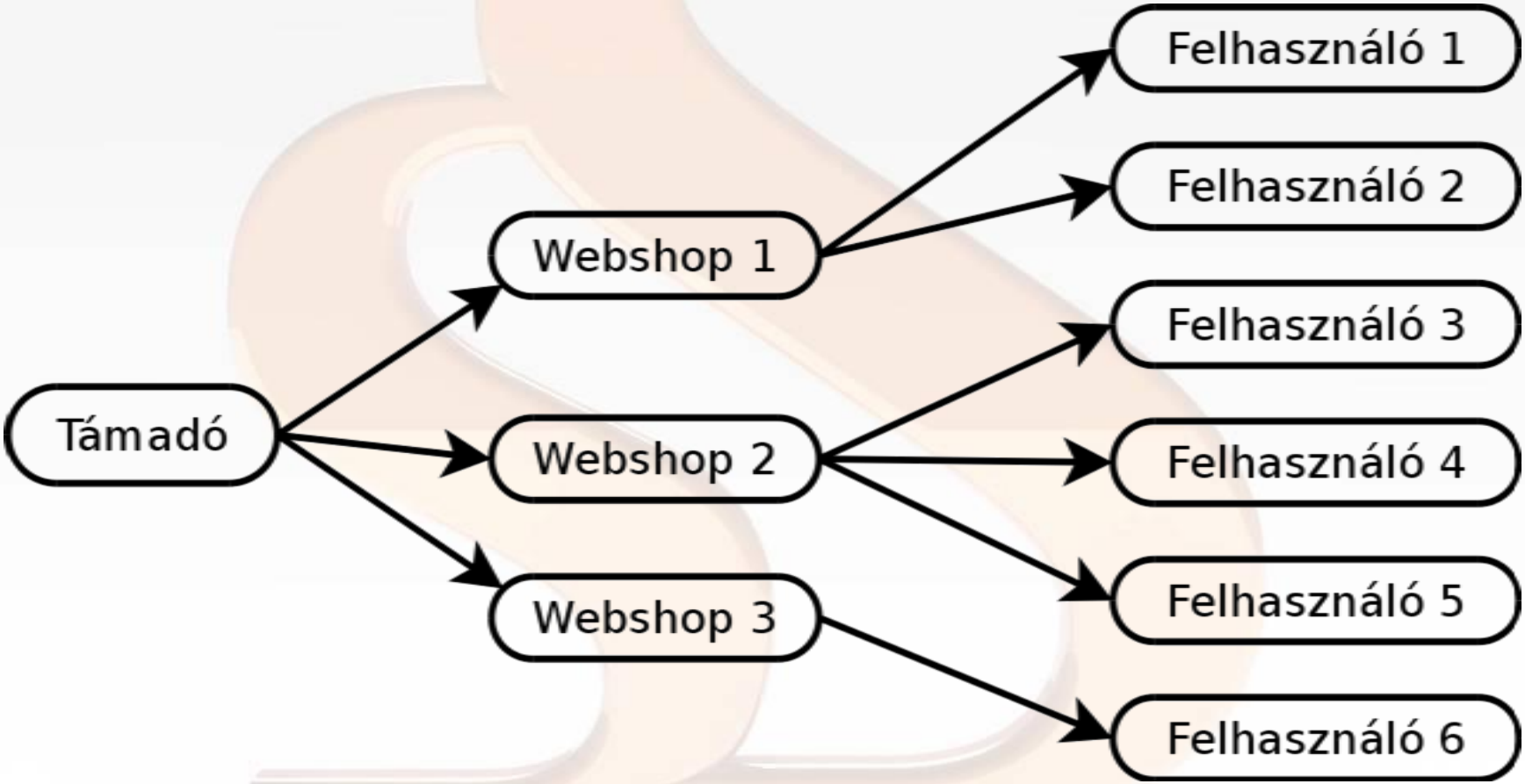
A technika ördögei

- **Webshop = Komplex IT rendszer**
  - Hibamentes rendszer létrehozása szinte lehetetlen
- **Minden felhasználó potenciális támadó lehet**
  - Nem tudjuk megkülönböztetni a valós vásárlót egy szervezett támadótól
- **Minden felhasználói kezelőelem fegyverré válhat egy támadó kezében**
- **Egy webalkalmazás jó bejutási pont lehet a háttérinfrastruktúrához**
  - Belső adatbázisok, fájlszerverek, munkaállomások

A támadások céljai

- **Adatlopás, adathalászat**
  - Személyes adatok
  - Pénzügyi információk
- **Közvetlen és közvetett pénzügyi kár okozása szolgáltatásmegtagadásos (DoS) támadással**
- **Deface**
  - Politikai, társadalmi aktivizmus
  - Hitelrontás
  - Szórakozás, önkifejezés...
- **Másodlagos cél (lásd következő dia)**

Másodlagos célok



SILENT SIGNAL

A titkosításról

- **Felhasználói adatok, elsősorban jelszavak**
  - Az ügyfél jelszavához az üzemeltetőnek semmi köze!
  - Titkosítás nélkül a komplex jelszavak sem érnek semmit
  - Az egyedi fejlesztésű eljárások soha sem megbízhatóak
- **Hálózati forgalom**
  - SSL

Tapasztalataink 1.

- **Szabadon elérhető, ingyenes rendszerek használata**
  - Ez még önmagában nem lenne baj!
- **Triviálisan adódik a felhasználók magas száma**
  - Ami ingyen van, és minőségi, azt többen használják
- **Amit sokan használnak, abban jobban megéri hibát keresni**
  - Amiben hibát keresnek, abban találnak is
- **Emiatt szükség lenne a frissítések nyomon követésére és telepítésére**
  - Ideális esetben ez magától értetődne, tapasztalataink éppen az ellenkezőjét mutatják

Tapasztalataink 2.

- **„Ha egyedi webshopom van, a támadónak nincs meg a forráskód, így nem tud mit kezdeni vele” – tévedés**
- **A „security through obscurity” sosem működött**
- **A fejlesztők is emberek, és nagyon hasonló hibákat követnek el.**
- **Lásd hibák TOP25 listája (következő dia)**
- **Nem az egyedi webshop a probléma, hanem az általa keltett hamis biztonságérzet.**
  - Megoldás: rendszeres ellenőrzés és hibajavítás

Néhány a TOP25 hibából

No.	Hiba megnevezése	Lehetséges következmények
1.	Failure to Preserve Web Page Structure (XSS)	Weboldal tartalmának akár maradandó változtatása, üzenetek elhelyezése
2.	Failure to Preserve SQL Query Structure (SQL injection)	Adatbázis (ügyfelek, partnerek, üzleti információk) tartalmának megszerzése, szerkesztése, törlése – akár észrevétlenül
4.	Cross-Site Request Forgery	Ügyfelek ill. adminisztrátor nevében tranzakciók indítása (rendelés, jelszó, …)
5.	Improper Access Control	Egyszerű ügyfél regisztrációval magasabb jogosultság megszerzése, ugródeszka
6.	Reliance on Untrusted Inputs in a Security Decision	Kedvezmények manipulálása, árak megváltoztatása
17.	Information Exposure Through an Error Message	Rendszerinformációk megszerzése, ezen keresztül további támadások véghezvitele

SILENT SIGNAL

Összefoglalás

- **A biztonság NEM felesleges költség**
- **Alacsony biztonsági szint = magas üzleti kockázat**
- **Bárki támadási célponttá válhat**
- **A szoftver és biztonsága nem termék, hanem folyamat**
- **Nem egyszer kell jó rendszert alkotni, hanem folyamatosan – FRISSÍTÉSEK**
- **Titkosítás kiemelten fontos**

Köszönjük megtisztelő figyelmüket!

SILENT SIGNAL

VÉSZJELZÉS HELYETT...

Szabó Péter

szabo.peter@silentsignal.hu

Veres-Szentkirályi András

vsza@silentsignal.hu

www.silentsignal.hu

info@silentsignal.hu