Silent Signal Kft.

Webáruházak informatikai biztonsága

Veres-Szentkirályi András

2011.03.04.

Témáink

- Bevezető
- Webáruház, mint IT rendszer biztonsága
- OWASP TOP10 webes hiba
- Tévhitek webáruházak biztonságával kapcsolatban
- Konkrét esetek, példák
- DEMO

SILENT SIGNAL

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?

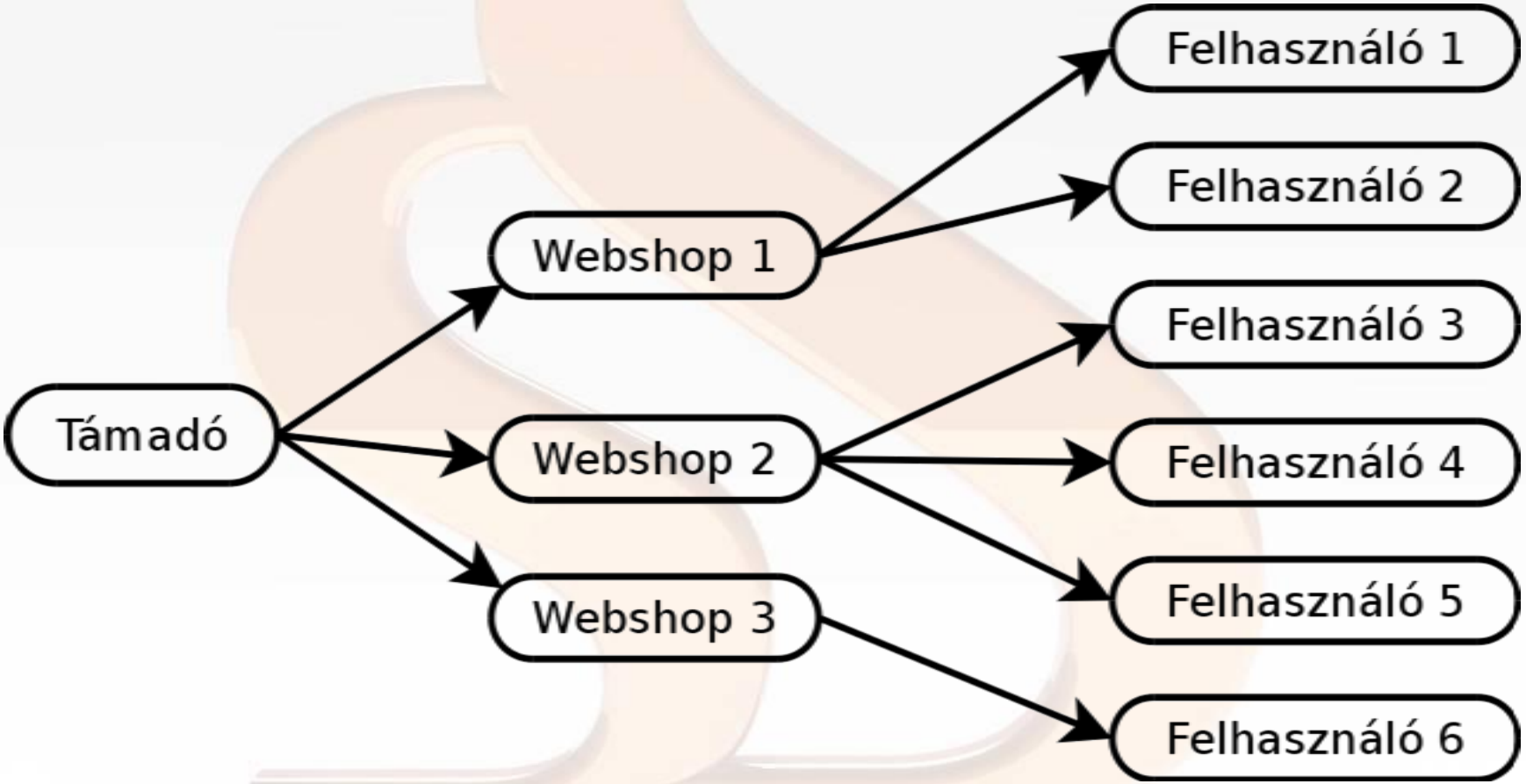
A technika ördögei

- **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



Néhány a TOP10 hibából

No.	Hiba megnevezése	Lehetséges következmények
1.	Injection (**SQL**, OS, LDAP)	Adatbázis (ügyfelek, partnerek, üzleti információk) tartalmának megszerzése, szerkesztése, törlése – akár észrevétlenül
2.	Cross-Site Scripting (XSS)	Weboldal tartalmának akár maradandó változtatása, üzenetek elhelyezése, malware terjesztés, lejáratás, ugródeszka
4.	Insecure Direct Object References	Kedvezmények manipulálása, árak megváltoztatása
5.	Cross-Site Request Forgery (XSRF)	Ügyfelek ill. adminisztrátor nevében tranzakciók indítása (rendelés, jelszó, …)
6.	Security Misconfiguration	Rendszerinformációk megszerzése, ezen keresztül további támadások véghezvitele
8.	Failure to Restrict URL Access	Ügyfél regisztrációval magasabb jogosultság megszerzése, ugródeszka + hírlevél

Biztonságos a webáruházam!

- Mert open-source alapokra épül
- Mert saját fejlesztésű
- Mert a fizetés SSL titkosítással megy
- Mert üzemeltetőnél fut, én csak bérlem
- …
- „vasvilla-biztonság” © Mr. Kocsis

„mert open source”

- **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 megéri hibát keresni**
  - Amiben hibát keresnek, abban találnak is
- **Frissítések nyomon követése és telepítése fontos**
  - Nem csak biztonság miatt, mégis rossz tapasztalatok
- **„Toldozgatás” lehet a leggyengébb láncszem**
  - Állatorvosi ló: Hacktivity 2009 Hack The Vendor

„mert saját fejlesztésű”

- **„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 OWASP webes hibák TOP10 listája**
- **Nem az egyedi webshop a probléma, hanem az általa keltett hamis biztonságérzet.**
  - Megoldás: rendszeres ellenőrzés és hibajavítás

„mert SSL a fizetés”

- **Felhasználói adatok, elsősorban jelszavak**
  - Az ügyfél jelszavához az üzemeltetőnek semmi köze!
  - Titkosítás nélkül a komplex jelszavak sem érnek semmit (OWASP TOP10 7. eleme!)
  - Az egyedi fejlesztésű eljárások soha sem megbízhatóak
- **Hálózati forgalom (OWASP TOP10 9. eleme!)**
  - SSL-t ad minden magyar kártyaelfogadó rendszer
  - Mi a helyzet a regisztrációval, bejelentkezéssel, böngészéssel, rendeléssel?

SILENT SIGNAL

Összefoglalás

- A biztonság NEM felesleges költség (lásd Casco)
- Alacsony biztonsági szint = magas üzleti kockázat
- Akihez az ügyfelek eljutnak, ahhoz a támadók is
- A szoftver és biztonsága nem termék, hanem folyamat, azaz nem egyszer kell minőségit alkotni, hanem folyamatosan tartani kell a szintet
  - Módszer: Frissítések és auditok
  - Alany: platform, (keret)rendszer, konfiguráció
- Adatbiztonság kiemelten fontos (titkosítás!)

Köszönjük megtisztelő figyelmüket!

SILENT SIGNAL

VÉSZJELZÉS HELYETT...

Veres-Szentkirályi András

vsza@silentsignal.hu

www.silentsignal.hu

info@silentsignal.hu