Behatolás-tesztelés esettanulmányok

A helyzet reménytelen?

Veres-Szentkirályi András

Varga-Perke Bálint

Ingyenes email szolgáltató

- Külső blackbox vizsgálat
- Session problémák
- Nem megfelelően véletlen értékek a munkamenet azonosítókban
- Perzisztens XSS (tárgy mező, csatolmány)
  - Mennyire súlyos a probléma?

Email szolgáltató

- Külső blackbox vizsgálat
- Kezdőknek gyakorló rendszer
- Kritikus problémák
- Szinte mindenhol hiba van!
  - Beléptető felület
  - Aláírás
  - Csatolmány kezelés
  - Email tárgy, törzs,stb...mezőben XSS

SILENT SIGNAL

Blogszolgáltató

- Külső blackbox vizsgálat
- Feltöltési probléma
  - Apache konfiguráció
  - Command shell feltöltési lehetőség
- XSS session hijack

Hálózati vizsgálatok

- **Belső vizsgálat**
- **Csak hálózat sérülékenységvizsgálata**
- **ARP poisoning – port security**
- **SNMP (default, gyenge jelszavak)**
- **Elfelejtett routing protokollok**
- **Kapcsolat eltérítés**
- **VIDEO**

Online dokumentum-kezelő rendszer

- Külső blackbox vizsgálat
- Feltöltési probléma
- Bármilyen fájl feltölthető
- Dokumentum rendező felület hibája
  - Hidden mező fontossága?

SILENT SIGNAL

Állami nagyvállalat

- Külső blackbox vizsgálat, kizárólag web
- Hibás és felesleges funkció
- Fájl olvasási lehetőség
- Parancs végrehajtás
- Local kernel null pointer dereference

SILENT SIGNAL

Hírportál

- Külső blackbox vizsgálat
- Régi, ott felejtett CGI program
- Fájl olvasás, parancs végrehajtás (szóköz)
- Paraméterezett parancsokat kell végrehajtani!
- Cukorka biztonság (jogosultsági problémák, régi kernel)

Szolgáltató cég

- Külső vizsgálat
- Rengeteg rendszer (10+)
- Upload, SQL injection (MS)
- Közös domain
- Tűzfal problémák
- Dual homed szerver
- ARP poisoning

Pénzintézet

- Belső vizsgálat
- Néhány szerver, hálózati teszt nincs
- Rengeteg felesleges szolgáltatás
- Backup rendszeren keresztül file olvasás
- Jelszó fájlból SSH hozzáférés
- .login kikerülése
- Jogosultsági problémák miatt root jogosultság

Kliens oldal

- Számlázási osztályra küldött email
- PDF exploit mellékletben
  - Mindenhol van
  - Nem frissítik
- AV-kat könnyű átverni
- Connect back shell
- VIDEO

Összefoglalás...

- **Automatizált eszközökkel ilyen hibák felderítése lehetetlen**
- **Körültekintő fejlesztéssel, üzemeltetéssel a hibák nagy százaléka kiküszöbölhető lenne**
- **Oktatás hiánya látható minden területen**
- **Jól szabályzott belső folyamatok és vezetői szinten elkötelezettség**
- **Folyamatos felülvizsgálat – biztonság NEM termék, hanem folyamat!**

Köszönjük megtisztelő figyelmüket!

SILENT SIGNAL

VÉSZJELZÉS HELYETT...

Veres-Szentkirályi András
Varga-Perke Bálint
info@silentsignal.hu
www.silentsignal.hu