Pánem World Wide Webu!

aneb povídání o chybě hloupé tak, až to bolí

- **Roman Kümmel**
- r.kummel@hacker-consulting.cz

WFT?#!$...

Session management

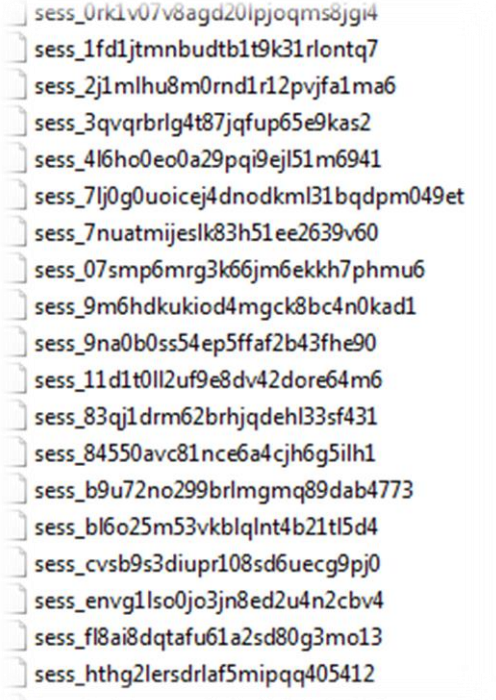
- HTTP je bezstavový protokol
  - Server si nepamatuje předchozí kroky uživatele
- Programovací jazyky zavádí relace (sessions)
  - Identifikace uživatele na základě předávaného session ID
- Vývojář má k dispozici session proměnné
  - Jejich hodnota je perzistentní mezi jednotlivými requesty
- Server ukládá sessions různých webových aplikací v oddělených částech paměti. S výjimkou PHP …

Session storage v PHP

- PHP ukládá relace do souborů na file systému
- Defaultně nastaveno na adresář /tmp
- Storage defaultně sdílí všechny aplikace na serveru
- Po vytvoření relace vznikne soubor defaultně pojmenovaný SESS_gfrnffptlb9s66kfqur4ib4ld5
- Session ID (gfrnffptlb9s66kfqur4ib4ld5) je předáno uživateli jako hodnota cookie (defaultně PHPSESSID)
- Pokud si aplikace ukládá data do session proměnných, ty se ukládají právě do session souboru

Krádeže relací ze serveru

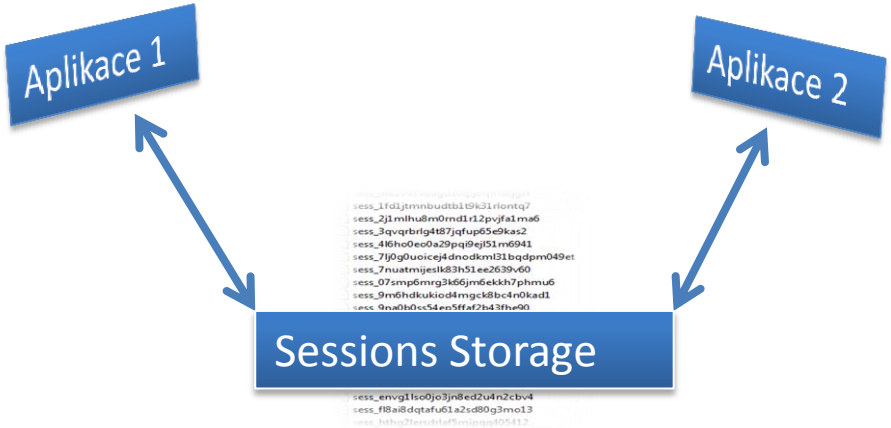
- Útočníci se vždy pokoušeli získat seznam aktivních SID (souborů) ze sdíleného úložiště



- Jako obrana bylo doporučováno
  - Odebrat práva na filesystému pro získání obsahu adresáře

Sdílené sessions

- Existuje zde ale jiný velice závažný problém
- Sdílení jedné relace více aplikacemi
- PHP totiž neví, které aplikaci konkrétní relace patří!



Kdo může být postižen

- Poskytovatelé cloudových služeb (www, eshopy)
- Klienti sdíleného webhostingu
- Každý, komu na serveru běží více než jedna webová aplikace

Poskytovatelé cloudových služeb

- Webové stránky snadno a rychle!
- Prodávejte ve svém novém e-shopu již za 5 minut!
- Spravujte svůj bussines v našem on-line IS!
- …
- Je to pěkné, ale má to jeden háček…

Poskytovatelé cloudových služeb

- Předpoklady pro úspěšný útok
  - Každá ze služeb běží na jiné (sub)doméně/cestě
    - http://automobily.skvelyeshop.cz
    - http://motorky.skvelyeshop.cz
  - Přístup do administrace je na této subdoméně
    - http://automobily.skvelyeshop.cz/admin
  - I přes centralizovanou administraci, nemusí být vyhráno
    - http://www.skvelyeshop.cz/administrace?eshop=motorky
    - (detaily později)

Poskytovatelé cloudových služeb

- Průběh útoku
  - Útočník si založí vlastní e-shop, nebo použije demo účet
    - http://utocnik.skvelyeshop.cz
  - Útočník se přihlásí do administrace svého e-shopu
  - Útočník změní platnost cookie tak, aby platilo i pro cílovou subdoménu, nebo pro všechny subdomény
    - utocnik.skvelyeshop.cz -> (automobily).skvelyeshop.cz
  - Útočník přistoupí do administrace cílového e-shopu

(1 demo > 1000 slov)

Sdílený webhosting

- Levná možnost získání vlastních webových stránek
- Bez nutnosti vlastní administrace serveru
- Jednoduché (upload skrz FTP, webové FTP, apd.)

- I zde je ale jedno ale…

Sdílený webhosting

- Předpoklady pro úspěšný útok
  - Webové stránky klientů jsou uloženy na společném serveru
  - Interpret PHP běží jako modul
  - Webové aplikace spolu sdílí úložiště pro session soubory

Sdílený webhosting

- Průběh útoku
  - Útočník přistoupí k cílové webové aplikaci
    - http://www.mujbussiness.cz
    - Na serveru vznikne relace
  - Útočník získá prostor na stejném webhostingu (serveru)
    - http://www.utocnik.cz
  - Útočník změní platnost cookie
    - www.mujbussiness.cz -> www.utocnik.cz
  - Na svém webu útočník přečte a změní obsah session proměnných
    - isAdmin = False -> isAdmin = True

(1 demo > 1000 slov)

Vlastní server (VPS)

- Server s nikým nesdílím
- Mohu si jej nakonfigurovat dle libosti
- Mohu si na něm vystavovat kolik chci aplikací

- I zde ale může číhat problém

Vlastní server (VPS)

- Předpoklady pro úspěšný útok
  - Na serveru běží více aplikací
    - http://www.nakupujuskreditem.cz
    - http://www.mojeknihovnicka.cz
  - Interpret PHP běží jako modul
  - Webové aplikace spolu sdílí úložiště pro session soubory
  - Vývojář má stále stejné návyky psaní kódu session managementu: if ($_SESSION[“iduser“]) …

Vlastní server (VPS)

- Průběh útoku
  - Útočník se zaregistruje a přihlásí do jedné z aplikací
    - http://www.mojeknihovnicka.cz
    - Na serveru vznikne session soubor
  - Útočník změní platnost cookie
    - www.mojeknihovnicka.cz -> www.nakupujuskreditem.cz
  - Útočník navštíví cílovou webovou aplikaci
    - www.nakupujuskreditem.cz

(1 demo > 1000 slov)

Jiné technologie (.NET, ASP, JAVA)

- I zde může být problém…

- *Cloudové služby*
  - *Všechy služby mohou být jedinou službou zobrazující pouze rozdílná data a vzhled dle konkrétního uživatele*
  - *Subdoména je brána jen jako parametr pro určení, která data se mají načíst*

Obrana

- Do session proměnných ukládat také údaj, které aplikaci relace patří a tento při přístupu kontrolovat
    - $_SESSION[“domain“] = “muj-eshop“
- Každé aplikaci nastavit vlastní úložiště pro session soubory a vhodně nastavit práva přístupu k tomuto úložišti
    - Open_basedir
- Spustit interpret PHP jako CGI (FastCGI)
    - Práva na filesystému jsou -rwx------, jiný účet tedy nemá právo číst ani měnit obsah cizího session souboru

Zkušenosti s oznamováním zranitelnosti

- Nemožnost najít kontakt na zodpovědné osoby
- Jediný dostupný kontakt je často pouze na nekompetentní podporu
- Reagovali pouze cca 2% oslovených
- Oznamující nesmí ve své zprávě nic nabízet (ani pomoc či radu, jak chybu odstranit) = SPAM

Dobrý den,
obdrželi jsme v rámci zákaznického centra od Vás níže uvedenou zprávu. Prosím o vyřazení našeho emailu z databáze kontaktů. Podobnými zprávami se zahlcuje zákaznická podpora a může se stát, že se z tohoto důvodu nebudeme věnovat jinému Vašemu požadavku souvisejícímu s projekty u naší společnosti.

CZ.NIC a jejich CSIRT

- Bezproblémové přijetí a vyslechnutí
- Hledání nejlepšího možného postupu pro oznámení
- Výsledek:
  - Oznámeno na neveřejné schůzce CSIRT týmů
  - Osloveny hostingové společnosti
  - Nabídnuta možnost otestování hostingu na danou zranitelnost
  - Zranitelných 20% z testovaných hostingů