Bezpečnost síťových aplikací

2019/2020

Př 6

WWW servery a aplikace
Čeho se bát ??

- Zneužití
  - Data na serveru
  - Data uživatelů na PC
  - Odesílaná data
- Odmítnutí
  - Kompromitace serveru
  - Odmítnutí služeb

Oblasti k řešení

- Server
  - Prostředí, aplikace, dostupnost ...
- Programátor
  - Zdrojový kod, špatné
- Prostředí
  - SSL, DNSSEC, Viry, ...
- Uživatel
  - Čemu věřit, co zadávat a kam ....

Prostředí serveru

- Sdílené prostředí ? Problém
- Práva všem? NE!
- Chroot ? ANO!
- Nepotřebný SW ? Smazat!
- Monitorovací služby? Zakázat!
- Zálohování ANO ANO ANO

WWW server – sdílené prostředí

- Vkládání cizího obsahu
  - allow_url_include, allow_url_fopen
- Přistup k cizím datům
  - open_basedir, chroot, fastcgi, práva
- Nahrávání dat
  - file_upload, upload_max_filesize
- Nahraný soubor nahradí jiný
  - Může jít spustit, cache, tmp => nonexec

WWW server – bannery + infa

- Server-status, server-info
  - Kdo, kam, kdy a odkud přistupuje
- phpinfo()
  - Nastavení, cesty
- Welcome page
  - Tomcat, Jetty
- Managery
  - /admin /manager /opcache

WWW programátor

- Kontrola vstupních dat
- Problém při práci s databází
- Ladící výpisy
- Nepořádek na serveru i v kódu
- Ukládání citlivých dat
- Bezpečné prostředí

WWW programátor – vstupní data

- Kontrolujte vše!
- Mezní hodnoty

/index.php?=timeout=10000000

```
<?php sleep( $timeout ); ?>
```

- Neoprávněný přístup

index.php?command=edit&id=3

- Validace Javascriptem ? NE!

pěkné, ale pro bezpečnost k ničemu

WWW programátor – databáze

- Escapování všech dat!
  - mysql_real_escape_string()
  - addslashes() / stripslashes()
- Bindovaní proměnných
  - $bind=mysqli->preprare(„insert into user values(?,?)“);
  - $bind->bind_parm(„pepa“,“pepa“);
  - $bind->execute();

WWW programátor – XSS – HTML/Javascript

- Vložení obsahu přes formulář
- Místo pokus vložím <B>**pokus**</B>
- Ale mohu i javascript a mám problém

<script src="http://s.cz/xss2.js"></script>

replace(/</g, '<').replace(/>/g, '>')

htmlspecialchars()

WWW programátor – XSS - CSS

- MS IE

  * *

- Mozilla, Firefox

* x *

- WhiteListy + Filter
  - Programová filtrace
  - Vlastní – není úplně triviální
  - Existující, např HTML Purifier

WWW programátor – XSS - zneužití

- Logování všeho **jen** do souboru
  - soubor nenalezen ?
  - Když něco na obrazovku tak jen pro uživatele
  - A musí to být vidět
    - @mysql_conect(….)MS IE
- Ladící výpisy pod heslem
  - Produkční server **není** na ladění

WWW programátor – Nepořádek v kódu

- V HTML zakomentované části – pryč s nimi
- V kódu – hesla v komentářích
- V souborech
  - neco.bak, neco.php~, zaloha....
  - Zakázat výpis adresářů
  - Neumožnit stahování .htaccess, xx.inc, config.ini

WWW programátor – Nepořádek v datech

- Citlivá data
  - Co nemusím, neukládám
  - Hesla, č. kreditek,op, č. pasu
  - Vždy přes POST, GET se ukládá
- Šifrovat ukládání
  - sha256(náhodnáčísla+sha256(cit.data))
- Šifrovat komunikaci
  - https, kontrolovat a redirectovat

WWW prostředí

- Minimalismus je základ
- Šifrování spojení
  - Dříve nutná vlastní IP, dnes SNI
  - Certifikační autority Symantec, Thawte
- DNSSEC
  - Ověření platnosti záznamu
  - Podepsané kořenové servery
  - Cyklické generování

WWW uživatelé

- Základní proškolení
  - Jak poznat šifrované spojení
  - Jak poznat důvěryhodný certifikát
  - Nastala ZMĚNA ověření, vadí to ?
  - Phishing
    - důvěrné věci nikdy mailem
  - Je to podezřelé ?
    - Okamžitě pryč + upozornit správce