Útoky na webové aplikace

Radek Megyesi, MEG0007

Obsah

- Co je útok na webovou aplikaci
- Typy útoků
- Jak se bránit
- Praktická ukázka

Co je to útok na webovou aplikaci?

- Co je webová aplikace
- Kontext prohlížeče
- Možné cíle:
  - Přesměrování
  - Manipulace s obsahem
  - Zneužití uživatelského oprávnění
  - Krádež relace/sezení (tzv. session)
  - Získání údajů/dat

(SQL) injection

- Špatně ošetřené vstupy a sestavení dotazu

```
SELECT * FROM Users WHERE UserName = param;
```

User name : Pepa OR 1=1

```
SELECT * FROM Users WHERE UserName = Pepa OR 1=1;
```

- Subselecty a joiny
- Obrana: escape znaků, nesestavování pomocí spojování řetězců, omezení práv na straně serveru

Spuštění nebo načtení souboru

- Načtení nebo spouštění parametrem

  ```
  readfile($_GET["file"]);
  ```

  index.php?file=/etc/passwd

- Obrana: kontrola parametrů (whitelist), nepřidělování práva načítání/spouštění

Krádež sezení/relace (session)

- Session ID
- Cookies nebo URL parametr
- Přihlášení -> server vygeneruje session ID -> předá ID -> prohlížeč uloží ID -> útočník ukrade ID -> útočník přistoupí na server
- Obrana: Expirace, IP, HttpOnly (cookies)

Cross Site Scripting (XSS)

- Ošetření ukládání/zobrazování vstupů
- Persistent vs Non-Persistent
- Obrana:
  - HTML -> TEXT (entitní vyjádření: **<** za **<**)
  - “Escapování” znaků
  - Oprava kódu (doplnění chybějících značek a odstranění nepovolených)
  - Použití knihoven

Cross Site Request Forgery (CSRF)

- Není totéž jako XSS
- Předem známý cíl (zná/odhadne strukturu) -> přesný požadavek

```
<img
src="http://blog.tld/admin/zmenprava.php?id=666&prava=1
" width="1" height="1" border="0">
```

- Př: nevědomé hlasování v anketách, nákupy v e-shopech
- Obrana: autorizační token

Clickjacking (Click Hijacking)

- Př: email->banka, šíření odkazů facebook/twitter, přihlášený uživatel nakoupí v e-shopu
- Zneužití IFrame - další vrstva

Praktická ukázka

```
This is <script>alert('This is succesfull XSS attack!')</script>comment.

<script>$("#showTitle").text("THIS IS NEW TEXT");$("#showTitle").css({"background-color": "yellow","font-size": "30px"});</script>
```