Mindent a biztonságról

1.

Alapok

Fogalmak, jogi háttér, milyen támadásokra számítsunk

Információbiztonság

1. **Bizalmasság (Confidentiality)** – Csak az arra jogosult személyek férhetnek hozzá az információkhoz.

2. **Sértetlenség (Integrity)** – Az adatok nem módosulhatnak illetéktelen vagy véletlen beavatkozás révén.

3. **Rendelkezésre állás (Availability)** – Az információk és rendszerek mindig elérhetők azok számára, akik jogosultak használni őket.

Információbiztonság

1. Mindenki **hozzáfér** minden adathoz amihez **van jogosultsága**

2. Senki **nem fér hozzá** olyan adathoz, amihez **nincs jogosultsága**

Jogi háttér – büntető jog

1. Információs rendszer felhasználásával elkövetett csalás (Btk 375. §)
   - 0-10 év
   - Károkozás

2. Információs rendszer vagy adat megsértése (BTK 423. §)
   - 0-8 év
   - Akkor is ha nem történik károkozás (jelentős érdeksérelem, közérdekű üzem súlyosbító tényező)

3. Információs rendszer védelmét biztosító technikai intézkedés kijátszása (BTK 424. §)
   - 0-2 év

Jogi háttér - adatvédelem

1. GDPR (2016/679/EU)
2. Adatvédelem (Info tv. 25/I. §)
3. Hatósági eljárás (Info tv. 60. §)

Jogi háttér – a gyakorlat

1. Az incidensek legtöbbször rejtve maradnak
2. Ritka a hatóság bevonása
3. Ritka a hatóság effektív és sikeres eljárása

Ne válj áldozattá, ne legyél jó célpont

Támadások célja

1. Erőforrás, vagy információ megszerzése
2. Károkozás
3. Politikai, vallási, pszichológiai

Támadás megtérülése

- Infrastruktúra
- Humán-erőforrás
- Kockázatok
- Technikai nehézségek
- IDŐ!

- Adatok felhasználhatósága
- Erőforrások felhasználhatóság
- Okozott kár mértéke

Támadások csoportosítása

Tömeges

- Mennyiség
- Károkozás mértéke alacsony
- Könnyen kivédhető
- Könnyen helyreállítható

Célzott

- Konkrét célpont
- Károkozás mértéke magas
- Nehezebben kivédhető
- Sokszor nehezen, esetleg egyáltalán nem állítható helyre

Tömeges támadások

Az tömeges támadások céljai:

- **Spam** (SEO linkek, email, átirányítás, stb.)
- **Malware telepítése** (kártékony kód futtatása)
- **Cryptojacking** (frontend vagy szerver oldalon)
- **Adatlopás** (pl. jelszavak, email-címek)
- **Proxy** további támadásokhoz erőforrás

ALACSONY MEGTÉRÜLÉS < $1/weboldal

Tömeges támadások

Az tömeges támadások módszerei

- **Ismert sebezhetőségek** (sablonok, bővítmények, szerver szoftver, stb)
- **Attack chain** (trójai, phishing, adatszivárgás)
- **Brute force és szótáras támadások** (wp admin, SSH, FTP, stb)

Célzott támadások

A célzott támadásoknak céljai:

- **Adatszerzés** (vásárlók, beszállítók, egyéb érzékeny adatok)
- **Károkozás** (adattörlés, módosítás, működés)
- **Zsarolás** (ransomware, célzott, vagy “puha” zsarolás)
- **Whitehat** (bug bounty)

MAGAS MEGTÉRÜLÉS > $500-$1000/weboldal

Célzott támadások

A célzott támadások módszerei

- Ismert sebezhetőségek
- **Egyedi, vagy 0day sebezhetőségek keresése**
- Attack chain (trójai, phishing, **adatszivárgás, social engineering)**
- Brute force és szótáras támadások (wp admin, SSH, FTP, stb)
- **Rossz szomszéd**
- **DOS/DDOS támadások**

Leggyakoribb támadások

Remote Code Execution (RCE)

A támadó lehetőséget kap arra, hogy távolról kódot futtasson a szerveren, például fájl feltöltéssel, parancssoros hozzáféréssel. Ez akár a szerver kontrolja feletti teljes átvételhez vezethet.

Leggyakoribb támadások

XSS (Cross-Site Scripting)

A támadó kártékony JavaScript kódot juttat be egy weboldalba, amely aztán a látogatók böngészőjében fut le. Célja lehet például sütik ellopása, felhasználók átverése vagy más műveletek végrehajtása a nevükben.

Célpontjai elsősorban a magasabb jogosultsággal rendelkező felhasználók (admin)

Leggyakoribb támadások

XSS (Cross-Site Scripting)

```
<p>Ez itt egy teljesen legitimnek tűnő üzenet</p>
<script>/*injektált JavaScript*/</script>

<img src="image.webp" onload="alert(1)">
```

Leggyakoribb támadások

CSRF (Cross-Site Request Forgery)

A támadó ráveszi az áldozatot, hogy az akarata ellenére műveletet hajtson végre egy bejelentkezett oldalon. Például: véletlen jelszóváltoztatás vagy tranzakció indítása.

```
<img src="delete-post.php?id=32">
```

Célpontjai **CSAK BEJELENTKEZETT FELHASZNÁLÓK!**

Leggyakoribb támadások

SQL Injection (SQLi)

A támadó az adatbázis-lekérdezéseket manipulálja úgy, hogy saját SQL parancsokat fűz a bemeneti mezőkbe. Ennek eredményeként adatokat olvashat ki, módosíthat vagy akár törölhet is az adatbázisból, legrosszabb esetben akár fájlt és létrehozhat.

Leggyakoribb támadások

SQL Injection (SQLi)

```
SELECT * FROM table WHERE id = $_GET["id"] ORDER BY id DESC

SELECT * FROM table WHERE id = %d ORDER BY id $_GET[”sort"]

SELECT "[code]" INTO OUTFILE ("/var/www/html/shell.php")
```

Leggyakoribb támadások

Privilege Escalation (jogosultságkiterjesztés)

A támadó egy alacsony jogosultságú fiókból admin vagy magasabb szintű hozzáférést szerez. Ez történhet hibás jogosultságkezelés, hibás konfiguráció vagy sebezhetőség miatt.

Ez fejlesztői hiba, a mi oldalunkról gyakorlatilag védhetetlen

Leggyakoribb támadások

Directory Traversal

A támadó úgy manipulálja az útvonalakat, hogy a szerveren lévő érzékeny fájlokat érje el (pl. wp-config.php). Ez akkor fordul elő, ha a fájlelérés nincs megfelelően szűrve.

Olvasás és törlés is probléma lehet!

Leggyakoribb támadások

Authentication Bypass

A támadó megkerüli a bejelentkezést, például hibás jelszóellenőrzés, token-kezelés vagy logikai hiba miatt. Ezzel közvetlen hozzáférést szerezhet védett tartalmakhoz.

Ez fejlesztői hiba, a mi oldalunkról gyakorlatilag védhetetlen

Leggyakoribb támadások

File Upload támadás

A támadó veszélyes fájlokat (pl. PHP webshell) tölt fel a szerverre, ha a szerver nem ellenőrzi megfelelően a fájltípust, tartalmat vagy a célmappát.

Ez fejlesztői hiba, a mi oldalunkról csak részben védhető

Leggyakoribb támadások

DOS

A támadó kis erőforrás felhasználásával veszi rá a szervert egy olyan műveletre, ami a támadásnál nagyobb erőforrást használ. Ezzel a támadó egyszerűen felhasználja a szerver összes erőforrását (tipikusan CPU, vagy max connection limit)

Leggyakoribb támadások

DDOS

A támadó rengeteg eszközről egyszerre (disztribútált), kis erőforrás felhasználásával veszi rá a szervert egy műveletre. Ezzel a támadó egyszerűen felhasználja a szerver összes erőforrását (tipikusan bandwidth, CPU, hálózati, vagy max connection limit)

Szürkezónás támadások

1. Jogilag nem, vagy csak nehezen kifogásolhatóak
2. Nem feltétlenül igényel technikai tudást
3. Sokszor “business logic” hibák
4. Információszerzésre, de károkozásra is használhatók
5. **Nagyon nehezen kivédhetőek!**

Szürkezónás támadások

Flood

Olyan legitim kérések küldése a szerver felé, amik nehezen szűrhetőek ki, de valamilyen – akár human – erőforrást elhasználnak

- Legitimnek tűnő hamis rendelések
- Valamilyen hibagenerálás (hibanapló -> tárhely)

Szürkezónás támadások

Adatszivárgás

Olyan lekérések küldése a szerver felé, amiből következtethetünk valamilyen információra

- Ilyen lehet akár egy rendelés leadás
- Regisztráció, bejelentkezés, vagy jelszóemlékeztető
- Webscraping megoldások (pl raktárkészlet)

2.

A gyakorlat

Konkrét példák és marketing bullshitek

XSS to RCE

- Stored vagy reflected
- A támadó lefuttat egy scriptet, ami

1. egy iframe-et hoz létre, ami betölti a wp-admin/user-new.php-t
2. a scripttel kitölti a form-ot
3. létrehoz egy admin usert, erről ugye megy automatikus e-mail
4. automatikusan belép, feltölt egy plugint => RCE

SQLi to RCE

- Általában WordPress alatt nem megy a multi-query
- Ha van file írásjog: file létrehozása
- Ha UPDATE, vagy INSERT: user létrehozása, _site_transient_update_plugins felülírása, options default_role felülírása

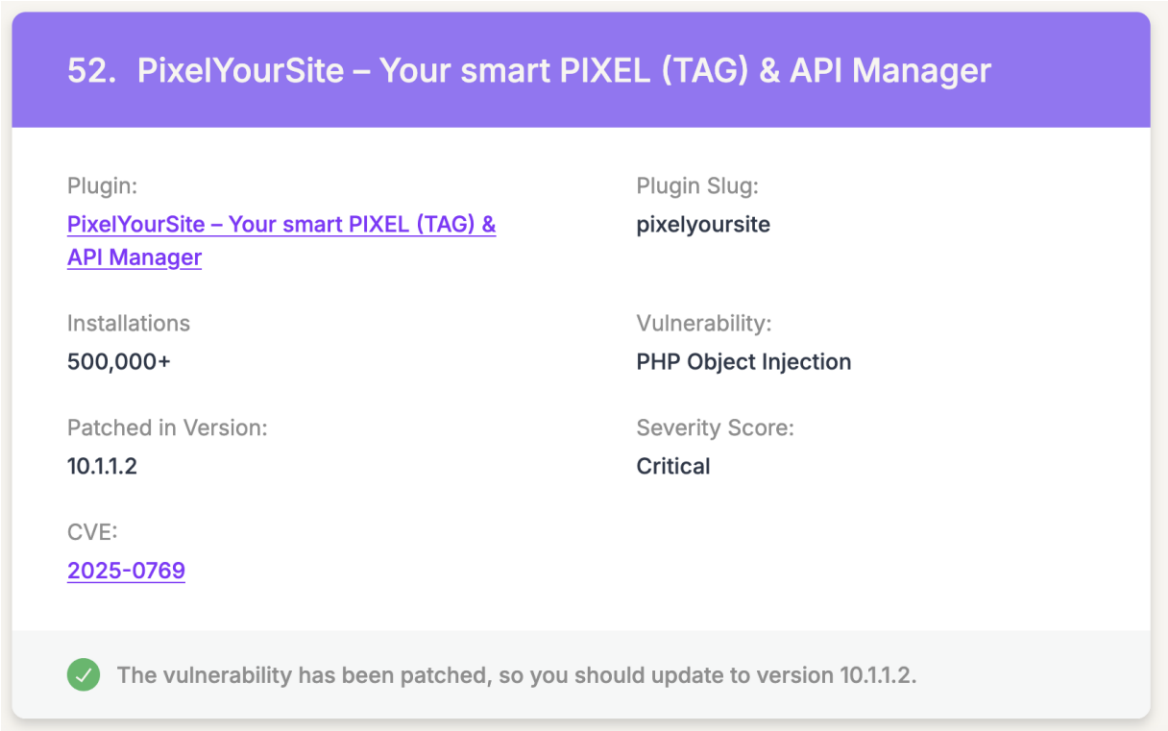
WP sebezhetőségek a gyakorlatban

A legtöbb WP sebezhetőség nem, vagy csak nehezen használható ki a gyakorlatban.

A kihasználható sebezhetőségek viszont hamar tömeges, automatizált támadásokhoz vezetnek.

Célzott támadások esetén a 0day sebezhetőségek jelentik a tényleges kockázatot

Konkrét példa



WP sebezhetőségek a gyakorlatban

PixelYourSite POI

- Kell hozzá a PYS sebezhető verziója
- Valahogy kell nonce-ot szerezni
- Kell egy olyan plugin vagy theme ami tartalmaz injectálható PHP objektumot
- Ekkor mondjuk törölhetjük a wp-config.php-t vagy file-t hozhatunk létre

Konkrét példa

WP sebezhetőségek a gyakorlatban

[/] Shortcode

```
[su_lightbox src='" onmouseover="alert(1);' type="image"]Link[/
su_lightbox]
```

```
<div class="mfp-preloader">
  Failed to load content.
  <a href="" onmouseover="alert(1);" target="_blank"> event
    <u>Open link</u>
  </a>
</div>
```

Hogyan néz ki egy támadás?

Tömeges támadások

- Egy konkrét endpoint-ot próbálnak végig
- Több millió site-on
- Egy site maximum pár másodperc
- Nagyon tipikus pattern-ek
- Könnyű észlelni, WAF megfogja

Hogyan néz ki egy támadás?

Célzott támadások

- Elemzik az oldalt, információ gyűjtés
- Gyenge pontokat keresnek:
  - Pluginek, sablon, szerver szoftver, header
  - Regisztrálnak, belépnek
  - Indexelt oldalak, hibaüzenetek keresése
  - Alkalmazottak elleni phishing, social engeniering

Hogyan néz ki egy támadás?

Célzott támadások

- Megszerzett adatok alapján ismert sebezhetőségek
- 0day sebezhetőség keresése
- Egyedi sebezhetőségek keresése <= ezt észrevehetjük
- Bruteforce és szótáras támadások

Hogyan rejtőzködnek a támadók?

- Távoli országokból indított (proxyzott) támadások
- Anonymous proxy, VPN
- Nyílt hálózatok
- Proxy chain
- TOR
- Feltört szerverek, zombi eszközök

3.
Védekezés

Technikai és logikai megoldások

Az első vonal – Hálózat

- Reverse proxy használata (pl: Cloudflare)
  - **WAF**
  - **Rate limiting**
  - Bot protection (JS challenge, captcha)
  - DDOS védelem
  - TOR, bizonyos IP tartományok kizárása

Ne legyél jó célpont!

Második vonal - Szerver

- Rendszeres frissítések
- Tűzfal (csak a szükséges portok legyenek nyitva), fail2ban
- Cseréld le a default SSH portot (több idő megtalálni)
- Ne küldd el a verzióinformációkat (server_tokens off)
- Szerver szintű rate limiting (ha nincs reverse proxy)
- Megfelelő erőforrások, optimalizálás

Ne legyél jó célpont!

Második vonal - Környezet

- Soha ne írd ki a hibaüzeneteket éles szerveren!
- PHP verzió elküldésének tiltása
- open_basedir, disable_functions (exec, shell_exec, stb)
- Megfelelő fájl jogosultságok
- Directory listing tiltása
- Fileok tiltása (readme.html, license.txt, .git, .zip, stb)
- **Legalább napi (remote) backup!**

Ne legyél jó célpont!

Harmadik vonal - WordPress

- Rendszeres frissítés, nem használt plugin/sablon törlése
- Megfelelő adatbázis beállítások
- Tiltsd le a nem használt REST API endpointokat és az xmlrpc-t
- 2FA hitelesítés és megfelelő jelszavak, IP whitelist
- Tiltsd a fájlszerkesztőt (wp-config.php-ban)
- Opcionálisan biztonsági bővítmények

Ne legyél jó célpont!

Negyedik vonal

- Megfelelő jogosultságok a munkatársaknak
- 403 helyett más hibaüzenet
- Nem inkrementális order id
- Honeypot e-mail cím
- Munkatársak és magunk képzése
- Az ideiglenes dolgok tényleg ideiglenesek legyenek (felhasználók, staging oldalak)

Ne legyél jó célpont!

Tippek vegyesen

- A jó jelszó
  - Egyedi (ne használd máshol)
  - Bonyolult, de megjegyezhető
  - Használj össze nem illő szavakat (Pl: mákoscsikóhal)
  - Használj ékezeteket, szóközt
  - 8+ karakter bőven elég (24 759 631 762 948 096 variáció)

Ne legyél jó célpont!

Tippek vegyesen

- Egy oldal – egy VPS
- E-mail legyen külön szerveren
- Kevesebb plugin kisebb kockázat
- Naplózás, időnként logok vizsgálata
- Ha könnyen felderíthető a támadó, éljünk a jogi lehetőségekkel!

Ne legyél jó célpont!

4.
Összefoglalás

Take home message

Nincs feltörhetetlen oldal, csak
gazdaságosan feltörhetetlen

Ne válj áldozattá, ne legyél jó célpont

Köszönöm a figyelmet!