MAGENTO

SICHERHEIT IM ECOMMERCE

FABIAN BLECHSCHMIDT

- PHP seit 2008
- Magento seit 2011
- IT-Sicherheit als Passion

WER SEID IHR?

- Backend-Entwickler
- Frontend-Entwickler
- Projektleiter
- Shopbetreiber, Anwender
- wer hat sich nicht gemeldet?

OWASP

OPEN WEB APPLICATION SECURITY PROJECT

- weltweit
- gemeinnützig
- Organisation fokusiert auf Sicherheit in Software

OWASP TOP 10

TOP 10 *Sicherheitsprobleme* in der Informationstechnologie

1. UNVALIDATED INPUT

- 4. Cross Site Scripting (XSS)
- 5. Buffer Overflow
- 6. Injection Flaws

4. CROSS SITE SCRIPTING (XSS)

```
echo '<input type="text" name="search" value="' . $_GET['search'] . '"/>';
```

Lösung: `htmlstriptags()`, htmlpurifier.com

"Gästebücher", Foren, Bewertungen
die den Inhalt nicht prüfen sind dauerhaft!

5. BUFFER OVERFLOW

Problem von PHP, nicht "unseres"

-> Updaten!

PHP: 5.6.25 (bis Dez. 2018), 7.0.10

PHP 5.5, 5.4 out of maintenance

6. INJECTION FLAWS

- SQL-Injection
- Mail Injection
- System Call Injection
- LDAP Injection
- Redis?
- CouchDB?
- Mongo?
- API x?

2. BROKEN ACCESS CONTROL

- Passwort/Berechtigung/UserID im Cookie speichern
  - Link ist ausgeblendet, aber nutzbar

z.B. Liste aller Bestellungen eines Benutzers,
KEINE Prüfung, beim Öffnen einer bestimmten Bestellung.

3. BROKEN AUTHENTICATION AND SESSION MANAGEMENT

- Passwortstärke (Mindestlänge, Zahlen, Umlaute...)
- Einlogversuche minimieren, danach verzögern
- Passwort ändern benötigt altes Passwort
- Session ID ist erratbar oder lesbar (HTTPS!)
- Authentifizierung immer POST - GET wird gecacht

7. IMPROPER ERROR HANDLING

- Stack Traces
- Datenbank dumps/Fehler (PASSWÖRTER!)
- Pfade zu Konfigurationsdateien
- Informationen welche System im Hintergrund laufen
- Niemand liest Logdateien

8. INSECURE STORAGE

BENUTZERPASSWÖRTER

- ~~md5~~
- ~~SHA1~~
- ~~DES~~
- ~~RC4 (WEP)~~
- PBKDF2
- bcrypt

8. INSECURE STORAGE

ZUGANGSDATEN

- Zertifikate (HTTPS)
- Schlüssel (HTTPS)
- Passwörter (Datenbank, API, ...)

10. INSECURE CONFIGURATION MANAGEMENT

- WENN .git im htdocs, dann NICHT LESBAR!
  - Datenbank von außen erreichbar

10. INSECURE CONFIGURATION MANAGEMENT

- falsche Verzeichnisrechte
- Ungepatchte Software
- unnötige Services (RPC, FTP, SMTP, telnet, ...)
- falsche und/oder Standard- und Beispielkonfigurationen
- Standard-Accounts mit STANDARD Passwörtern!
- selbst signierte oder Standard-SSL-Zertifikate (Public Key Pinning)

LINKS

- Magento Security Best Practices
- https://www.owasp.org/index.php/A12004Unvalidated_Input
- https://www.owasp.org/index.php/A22004BrokenAccessControl
- https://www.owasp.org/index.php/A32004BrokenAuthenticationandSessionManagement
- https://www.owasp.org/index.php/A42004CrossSiteScripting
- https://www.owasp.org/index.php/A52004Buffer_Overflow
- https://www.owasp.org/index.php/A62004Injection_Flaws
- https://www.owasp.org/index.php/A72004ImproperErrorHandling
- https://www.owasp.org/index.php/A82004Insecure_Storage
- https://www.owasp.org/index.php/A92004ApplicationDenialof_Service
- https://www.owasp.org/index.php/A102004InsecureConfigurationManagement
- https://www.youtube.com/watch?v=nN-uBiWoufg (Mage Titans Italia 2016 - Andreas von Studnitz - Magento Worst Practice))
- http://security.stackexchange.com/
- http://docs.magento.com/m1/ce/user_guide/magento/magento-security-best-practices.html
- http://de.slideshare.net/avoelkl/secure-input-and-output-handling-57946042
- https://blog.limesoda.com/2015/07/sicherheit-von-magento-online-shops-ein-status-quo/
- https://blog.limesoda.com/2014/05/sicherheit-fuer-web-anwendungen/
- https://github.com/ikonoshirt/pbkdf2

Magento - Sicherheit im eCommerce, mainIT16, Fabian Blechschmidt