Web- und Magento-Security

Fabian Blechschmidt
& Bastian Ike

Meet Magento

Sicherheit

Meet Magento

Wer wir sind

Bastian Ike

2006: Security

2011: Zertifizierung

2012: Vorträge auf der Imagine, Meet-Magento, Developers Paradise

Fabian Blechschmidt

2011: Zertifizierung

2010: Security-Extensions

2013: Vortrag Imagine

Sicherheit? Schon wieder?

- Unsichere Community-Module
- Angreifbare Payment-Gateways
  - PayPal
  - GoogleCheckout
  - Moneybookers

Sicherheit? Ja klar!

- Software planen
- von Anfang an Gedanken machen
- erst denken, dann coden

Konzeptionelle Probleme

- unsichere Objektreferenzen
- blindes Vertrauen in Drittherstellercode
- Open Redirect

Probleme in PHP

Meet Magento

Probleme in PHP

```
strcmp(”foo”, ”bar”) !== 0
strcmp(Array(), ”something“) === NULL

md5(”240610708”) == ”0e462097431906509019562988736854”
md5(”240610708”) == ”0”

=== statt ==
```

Meet Magento

Magento

Meet Magento

Magento Lücken

- 3x XSS (1x persistent)
- 2x File Disclosure (get.php, Zend_XmlRpc)
- 3x Angriffe auf die API
- Magento 2 alpha: Dateien schreiben

unserialize() in Magento 2

- unserialize() ruft auf:

```
__wakeup()
__destruct()

unserialize($_COOKIE[”some_cookie”])

Mage_Core_Model_Design_Fallback_CachingProxy::
    __destruct():

$this->_filesystem->
    write($filePath, serialize($section['data']));
```

Auswirkungen

Meet Magento

Auswirkungen

- Backdoors
- Datendiebstahl
- Proxy/Spamversand

Schutzmaßnahmen

Schutzmaßnahmen

- Prävention statt Patchen
  ... oder merkt ihr schnell genug einen Angriff?
- denken wie ein Angreifer
- fremden Code prüfen
  – selbst ein kleiner Blick schadet nicht
- nachdenken bevor man programmiert

Frameworks gegen Fehler

- Template Engine (Twig) statt XSS
- PDO statt MySQL Injection
- TLS (HSTS) zur Prävention von MITM

... leider kein 100%iger Schutz :-(

SSL

- SSL im Backend
- HSTS Header senden
- kein FTP (SCP ist sicher)
- ordentliche Zertifikate für den Kunden
- wenn self-signed Zertifikate, eigene CA

Zusammenfassung

Danke

Bastian Ike @b_ike

Fabian Blechschmidt @Fabian_ikono

Meet Magento