Web- and Magento-Security

Fabian Blechschmidt
& Bastian Ike

Meet Magento

Security

Meet Magento

Who we are

Bastian Ike

2006: Security

2011: Certification

2012: Talks at Imagine, Meet-Magento, Developers Paradise

Fabian Blechschmidt

2011: Certification

2010: Security-Extensions

2013: Talk at Imagine

Meet Magento

Security? Again!?

- Insecure community modules
- attackable payment gateways
  - PayPal
  - GoogleCheckout
  - Moneybookers

Security? Sure!

- Plan your software
- Think about it from the beginning
- Think first, code afterwards

Meet Magento

Conceptionall problems

- insecure object references
- blind trust in third party extensions
- open redirect

Problems in PHP

Problems in PHP

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

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

=== instead of ==
```

Magento

Magento security issues

- 3x XSS (1x persistent)
- 2x File Disclosure (get.php, Zend_XmlRpc)
- 3x Attacking the API
- Magento 2 alpha: write files

unserialize() in Magento 2

- unserialize() calls:

```
__wakeup()
__destruct()

unserialize($_COOKIE[”some_cookie”])

 Mage_Core_Model_Design_Fallback_CachingProxy::
     __destruct():

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

Meet Magento

Impact

Meet Magento

Impact

- backdoors
- data theft
- proxy/sending spam

precautious measures

Schutzmaßnahmen

- prevention instead of patching
  ... ordo you detect fast enough an attack?
- think like an attacker
- check third party code
  - have an eye on it! It doesn‘t hurt.
- think before you code

Frameworks against mistakes

- template engine (Twig) instead of XSS
- PDO instead of MySQL injection
- TLS (HSTS) to prevent MITM

... but still no 100% protection :-(

SSL

- SSL in the backend
- send HSTS header
- NO FTP! (use SCP instead, it is secure)
- correct SSL certificates for customers
- IF self-signed certificates, implement your own CA

Conclusion

Meet Magento

Thanks

Bastian Ike
@b_ike

Fabian Blechschmidt
@Fabian_ikono

Meet Magento