

Leveraging Magento 2 to defend against

The OWASP Top Ten





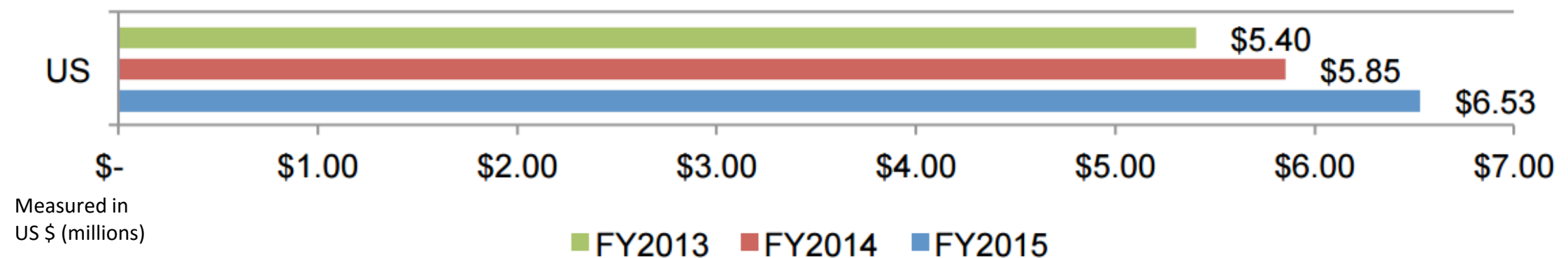
Talesh Seeparsan

Magento Security podcast – magedef.com

<http://tale.sh/croatia-16>



Average total organizational cost of a data breach



*“While the cost of data breach stayed relatively constant for most industries, **the retail sector** experienced a significant increase...in 2015.”*

-2015 Cost of Data Breach Study: Global Analysis
<http://tale.sh/ponemon-2015>



Prevention vs Cure



The OWASP Top Ten

- Flagship publication of the OWASP Foundation
- OWASP are the unsung heroes of web security



Important: This talk does not suggest that OWASP Foundation endorses anything I say or certify compliance of the Magento platform



Our Approach



- What are the top ten?
- Features built into Magento 2 you should be using.





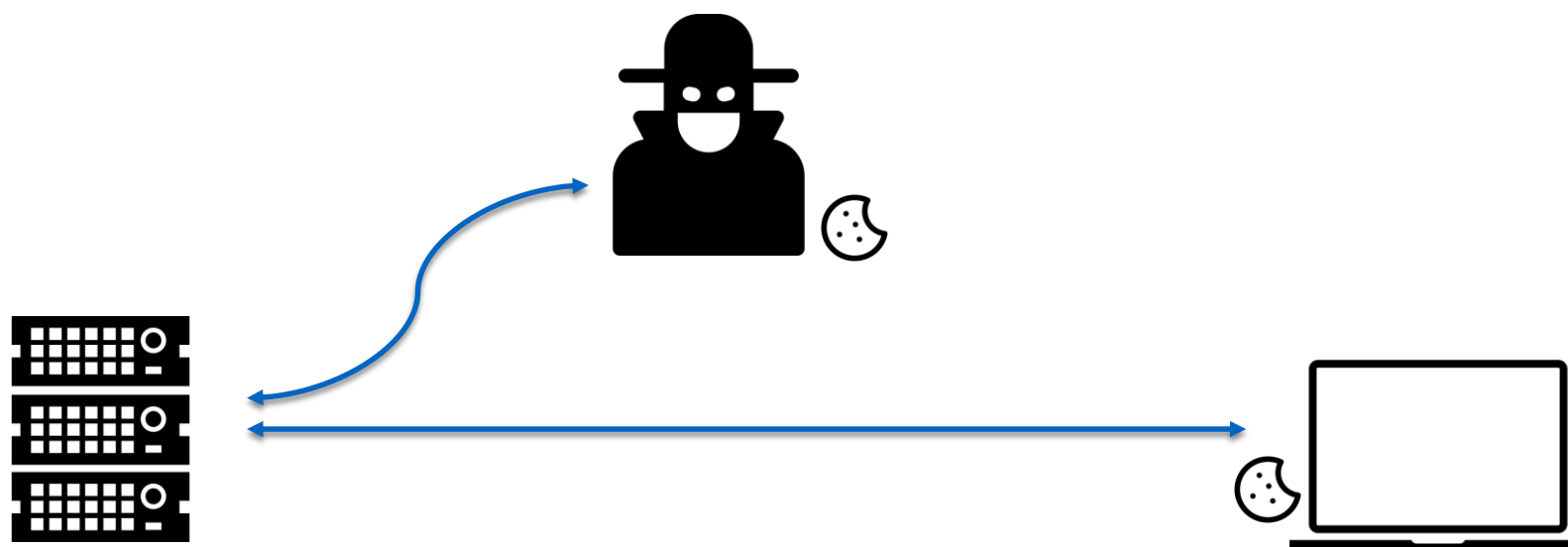
A1 Injection





A2 Broken Authentication & Session Management

- Breaking in through the front door





A3 Cross Site Scripting : XSS

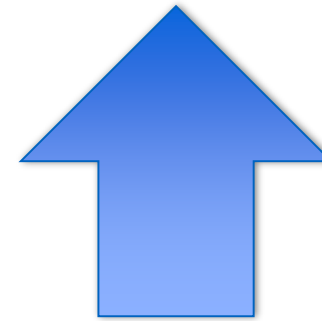
Unauthorized scripts running on your site.





A4 Insecure Direct Object References

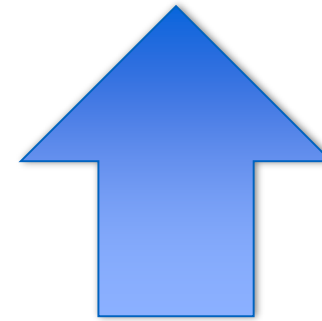
<https://mage2.com/customer/address/edit/id/52/>





A4 Insecure Direct Object References

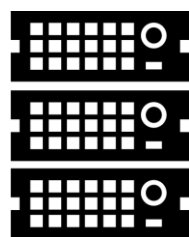
<https://mage2.com/customer/address/edit/id/53/>





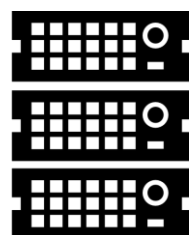
A5 Security Misconfiguration

- Attack to your application stack
- Attack to unnecessary features
- Surface of attack



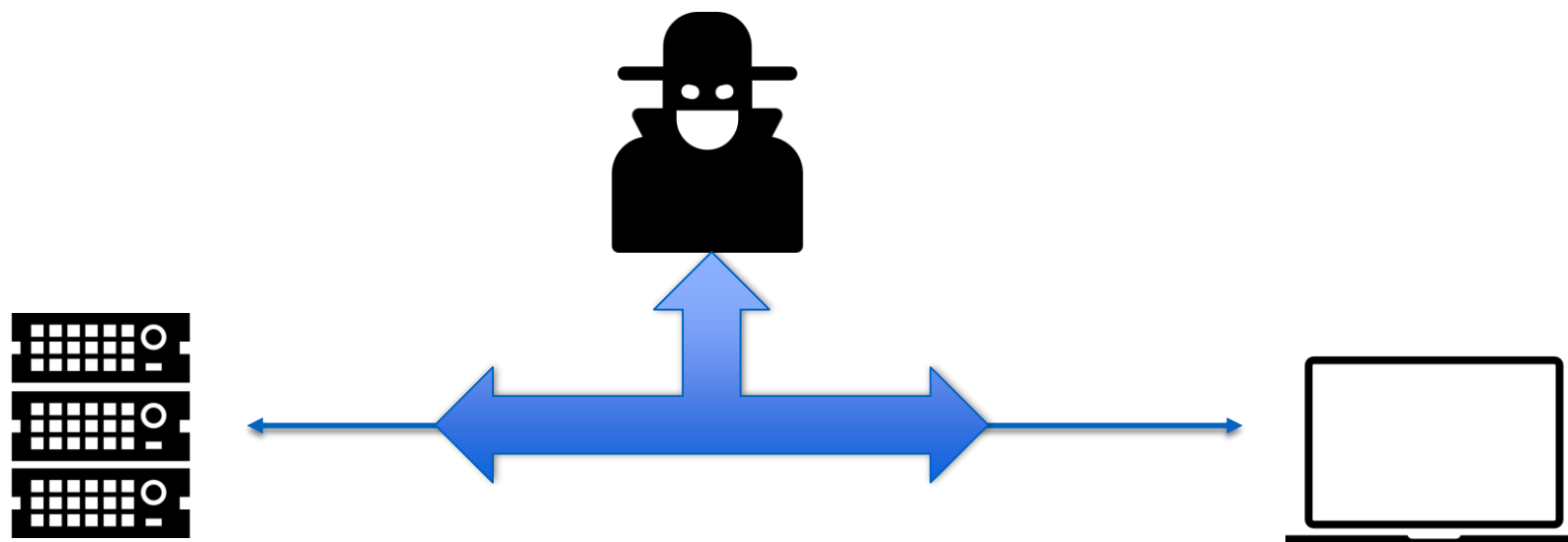


A6 Sensitive Data Exposure





A6 Sensitive Data Exposure



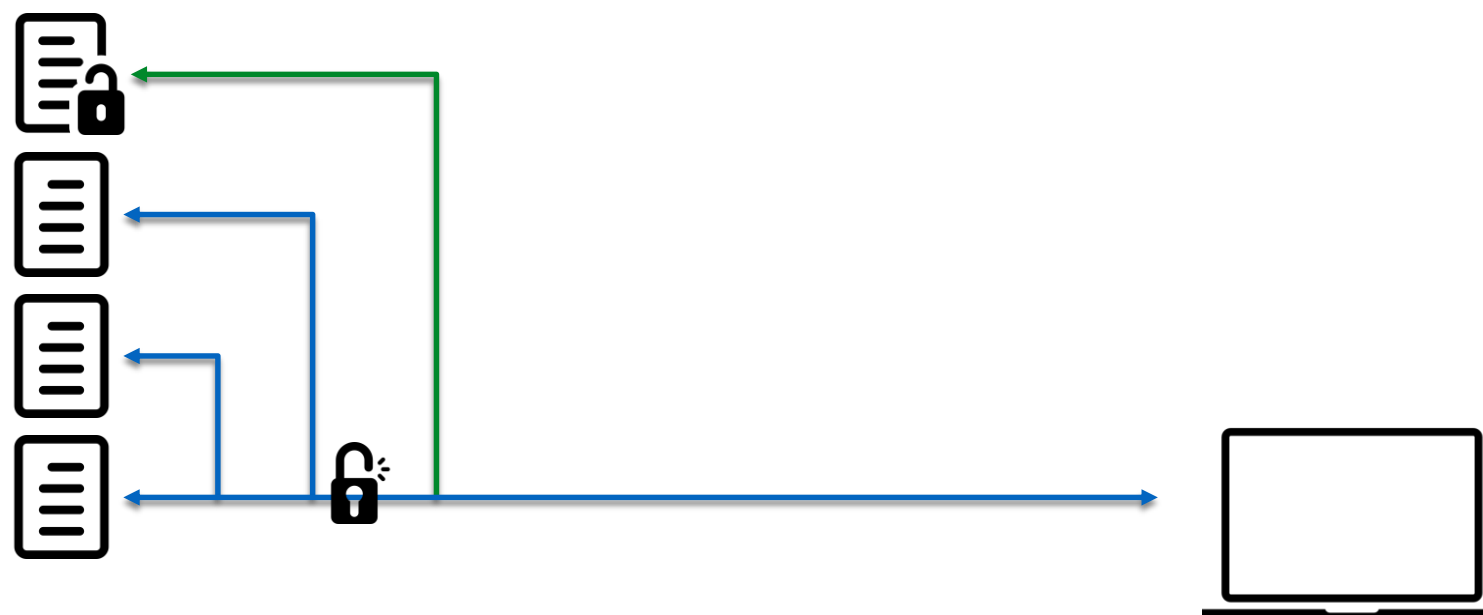


A7 Missing Function-Level Access Control





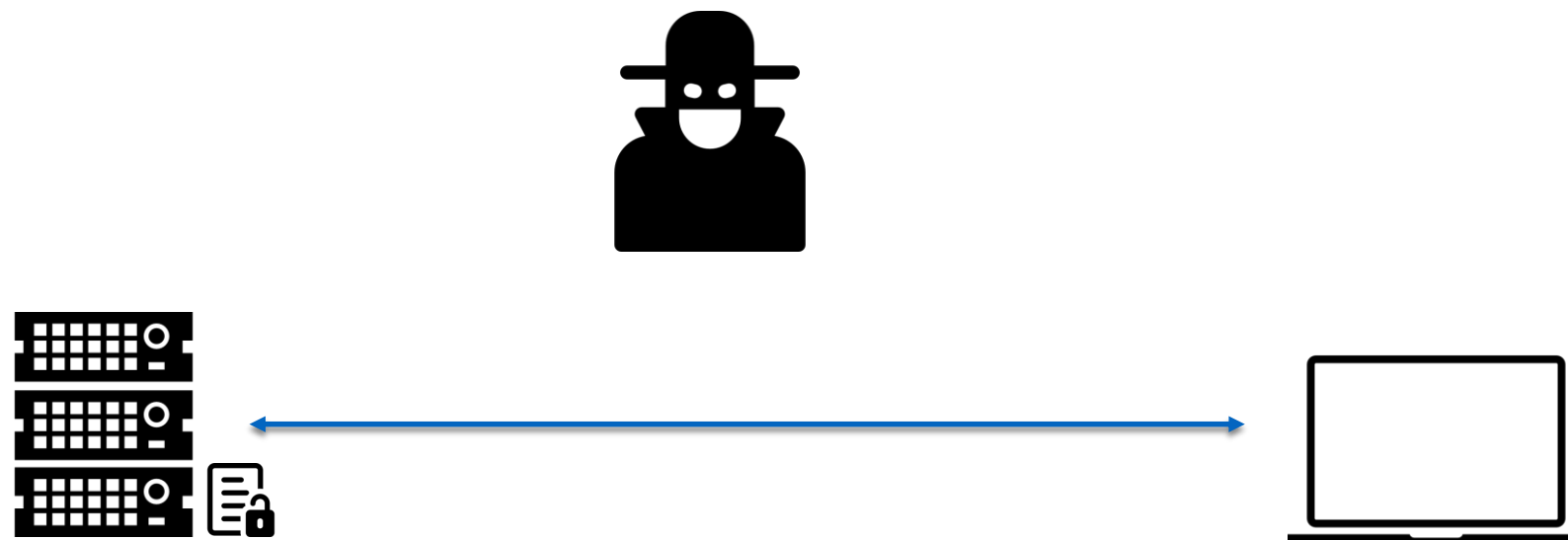
A7 Missing Function-Level Access Control





A8 Cross-Site Request Forgery (CSRF)

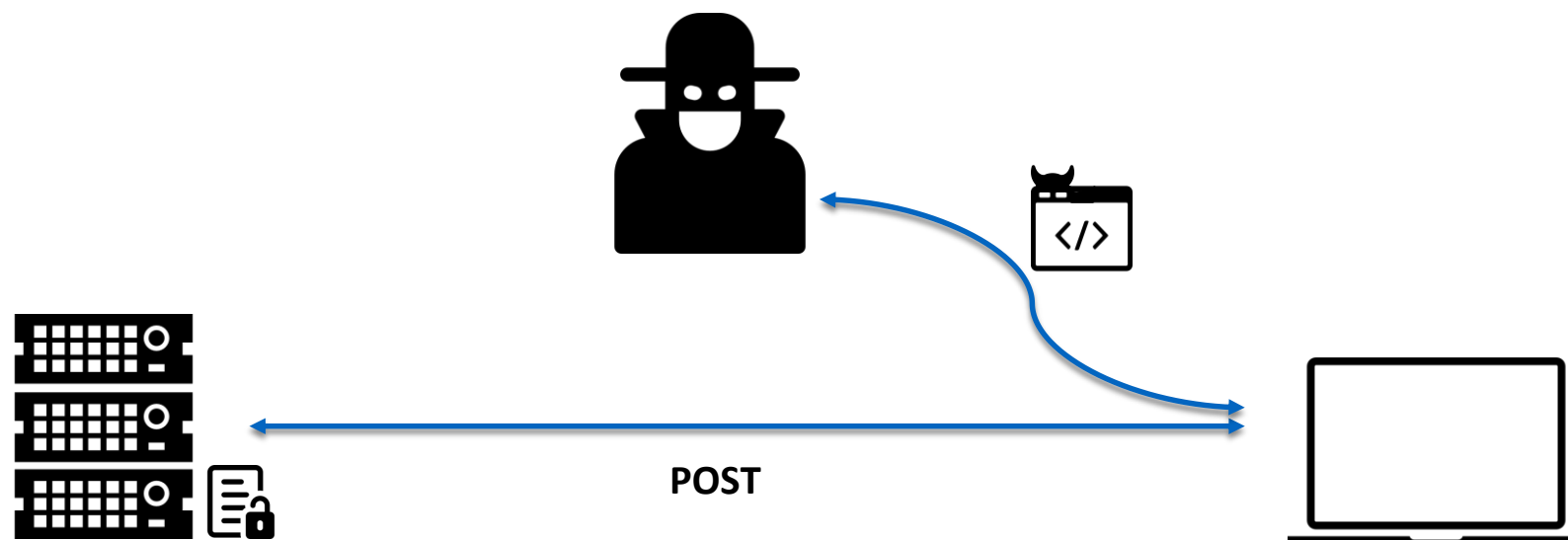
- Trick an authenticated user to POST information on your site





A8 Cross-Site Request Forgery (CSRF)

- Trick an authenticated user to POST information on your site





Using Components with Known Vulnerabilities



Unvalidated Redirects and Forwards





Magento 2 Builtin Defenses



Use the Magento 2 ORM

- ~~Handcoded SQL queries~~
- Robust framework that facilitates Server side input validation



Defends against Injection and XSS

DevelopersParadise

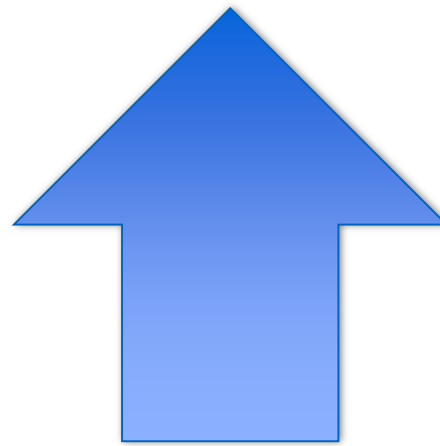
2016 / Opatija / Croatia



The Magento 2 Escaper

Implementation: `/lib/internal/Magento/Framework/Escaper.php`

Usage: `<?php echo $this->escapeHtml(__($this->variable); ?>`



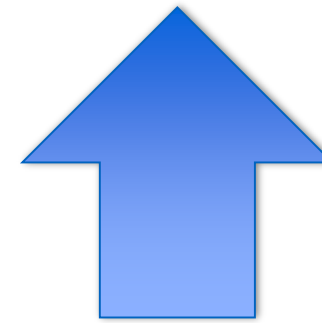
Defends against XSS

DevelopersParadise

2016 / Opatija / Croatia



```
<?php echo $this->getBlockHtml( ' formkey ' )?>
```



Defends against CSRF

DevelopersParadise

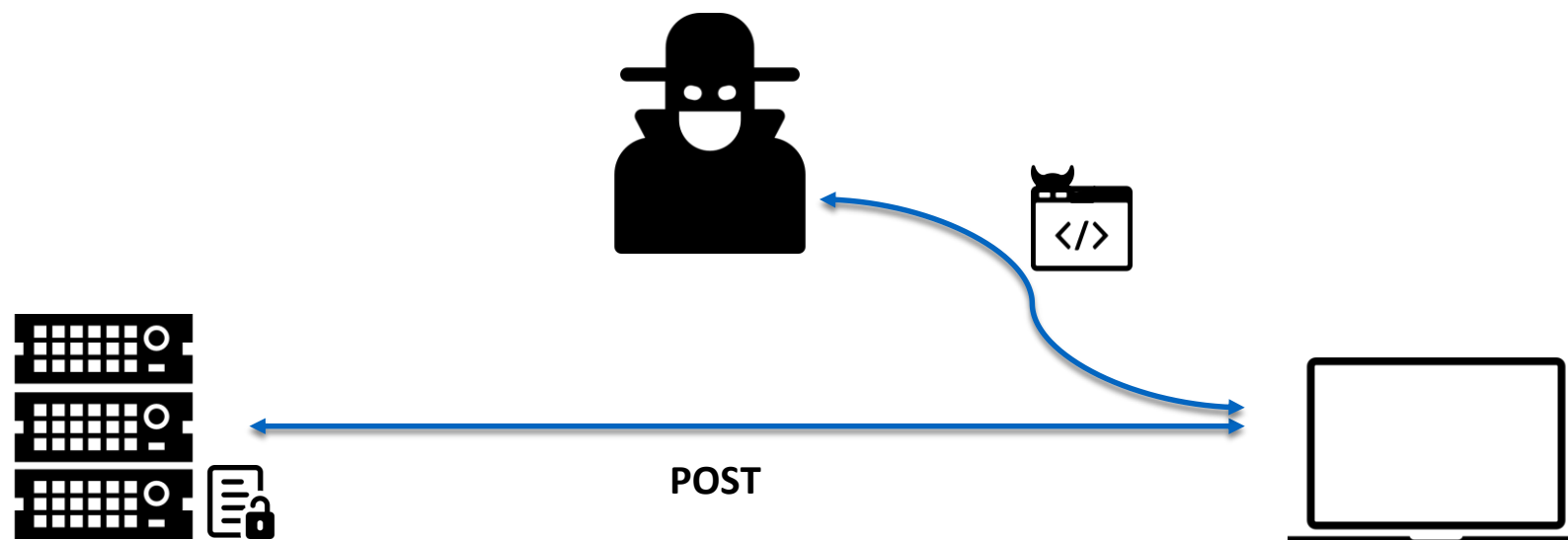
2016 / Opatija / Croatia





A8 Cross-Site Request Forgery (CSRF)

- Trick an authenticated user to POST information on your site



Headers

Post

HTML

Cache

Cookies

Parts

multipart/form-data

form_key

reAu87kvSulVhfwM

config_state[design_theme...

0

groups[theme][fields][the...

groups[theme][fields][ua_...

config_state[design_head]

1

groups[head][fields][shor...

groups[head][fields][defa...

Magento Commerce

groups[head][fields][titl...

groups[head][fields][titl...

groups[head][fields][defa...

Default Description

groups[head][fields][defa...

Magento, Varien, E-commerce

groups[head][fields][incl...

<script src="https://ajax.googleapis.com/ajax/libs/prototype/1.7.3.0/prototype.js"></script>

groups[head][fields][demo...

0

config_state[design_searc...

0

groups[search_engine_robo...

INDEX, FOLLOW

groups[search_engine_robo...

config_state[design_heade...

0

groups[header][fields][lo...

groups[header][fields][lo...

groups[header][fields][lo...

groups[header][fields][lo...

Magento Commerce

groups[header][fields][we...

Default welcome msg!

config_state[design_foote...

0

groups[footer][fields][co...

Copyright © 2015 Magento. All rights reserved.

groups[footer][fields][ab...

 Defends against CSRF

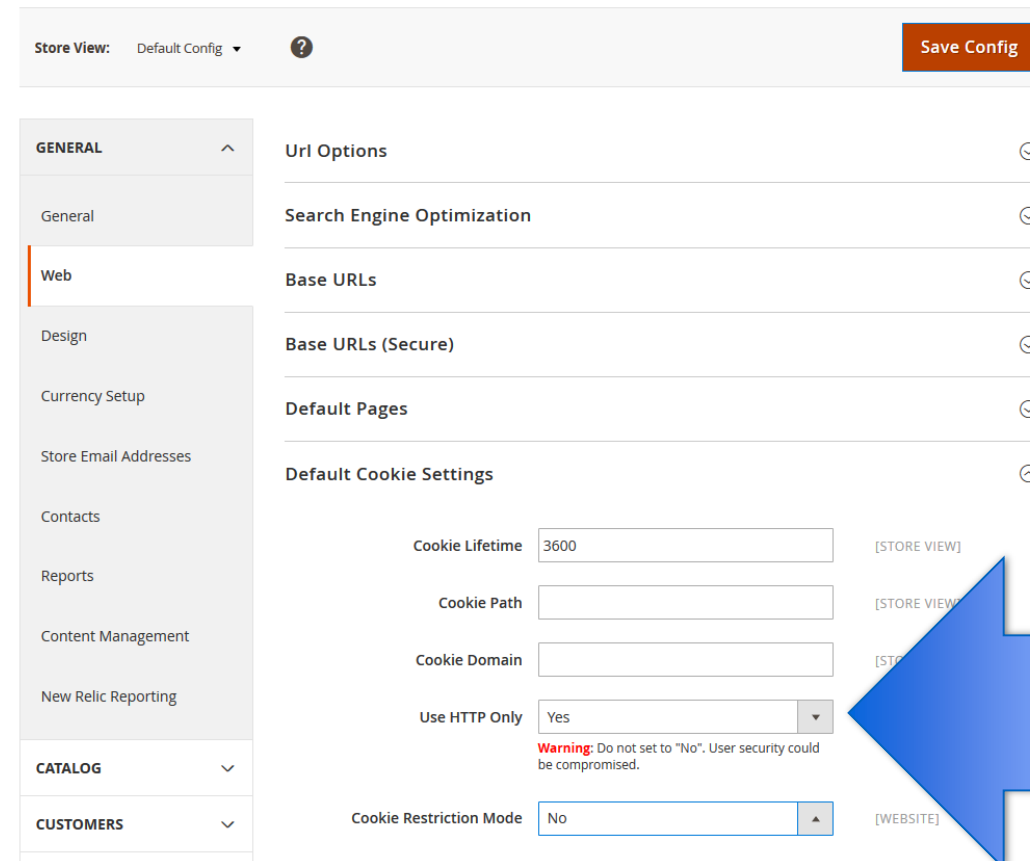
DevelopersParadise

2016 / Opatija / Croatia



Pay attention to cookie permissions

- “**HttpOnly**” flag is set on some important cookies eg:
 - “admin” cookie
 - “PHPSESSID” cookie
 - “X-Magento-Vary” cookie



Store View: Default Config ? Save Config

GENERAL ^

General

Web

Design

Currency Setup

Store Email Addresses

Contacts

Reports

Content Management

New Relic Reporting

CATALOG v

CUSTOMERS v

Url Options

Search Engine Optimization

Base URLs

Base URLs (Secure)

Default Pages

Default Cookie Settings

Cookie Lifetime 3600 [STORE VIEW]

Cookie Path [STORE VIEW]

Cookie Domain [STORE VIEW]

Use HTTP Only Yes [v]
Warning: Do not set to "No". User security could be compromised.

Cookie Restriction Mode No [^] [WEBSITE]

- “**Secure**” flag is set on some important cookies eg:
 - “admin” cookie
 - “X-Magento-Vary” cookie



Defends against Broken Authentication

DevelopersParadise

2016 / Opatija / Croatia



Rely on the CustomerSession Object

```
public function __construct(  
    Context $context,  
    CustomerSession $customerSession  
)  
{  
    parent::__construct($context, $customerSession);  
}
```



Defends against risks:

Insecure Direct object references
Missing function Access control

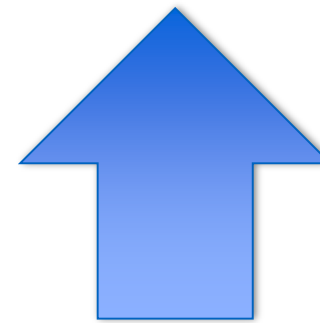
DevelopersParadise

2016 / Opatija / Croatia



Don't roll your own Crypto!

```
<field id="password" translate="label" type="obscure" showInStore="0">  
  <label>Password</label>  
  <backend_model>Magento\Config\Model\Config\Backend\Encrypted</backend_model>  
</field>
```



Defends against risks:

DevelopersParadise

2016 / Opatija / Croatia

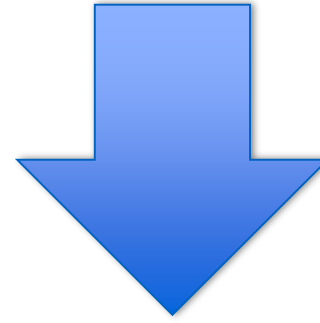
Security Misconfigurations

Sensitive data exposure

Missing function level access control



Don't roll your own Crypto!



```
<field id="password" translate="label" type="obscure" showInStore="0">  
  <label>Password</label>  
  <backend_model>Magento\Config\Model\Config\Backend\Encrypted</backend_model>  
</field>
```



Defends against risks:

DevelopersParadise

2016 / Opatija / Croatia

Security Misconfigurations

Sensitive data exposure

Missing function level access control





 Defends against using vulnerable components

DevelopersParadise

2016 / Opatija / Croatia



DASHBOARD
SALES
PRODUCTS
CUSTOMERS
MARKETING
CONTENT
REPORTS
STORES
SYSTEM
FIND PARTNERS & EXTENSIONS

System Messages: 1

Notifications

Actions

▼

1 records found

20

▼

per page

<

1

of 1

>

<input type="checkbox"/>	Severity	Date Added ↑	Message	Actions
<input type="checkbox"/>	CRITICAL	Jan 28, 2016, 7:08:45 PM	Important: Magento Community Edition 2.0.2 Addresses Upgrade Issues – January 28, 2016 Newly released Magento Community Edition 2.0.2 resolves issues encountered by some users when upgrading Magento Community Edition 2.0.0 and 2.0.1. The issues occur with products that were installed from a compressed archive (.tar.gz, .zip, and .bz2); merchants who used other installation options are not affected. More information is available in the Technical Bulletin at http://devdocs.magento.com/guides/v2.0/release-notes/tech_bull_201-upgrade.html .	Read Details Mark as Read Remove

Copyright© 2016 Magento Commerce Inc. All rights reserved.

Magento ver. 2.0.0
[Report Bugs](#)

 Defends against using vulnerable components



Thank You!



<https://community.magento.com/>



<https://magento.stackexchange.com/>



<https://owasp.org/>



https://twitter.com/_Talesh

Questions?



DevelopersParadise

2016 / Opatija / Croatia