Keeping your Magento store

Anna Völkl

IN THIS ARTICLE YOU'LL FIND OUT:

- What are the most critical web app security risks
- How Magento deals with security issues
- What are the best practices to keep store safe

E-Commerce websites are a valuable target for hackers and fraud. Customer data – especially payment details like credit card data – make them prone to cyber-attacks. Running and maintaining a Magento e-commerce store requires taking care of the security of a given system, not just at the end of a project but throughout the whole software lifecycle. E-commerce managers, as well as developers, need to be aware of the risks and need to prepare and react to potential threats.

FOLLOW THE MAGENTO SECURITY BEST PRACTICES

Running a secure Magento store requires taking care of the server infrastructure and server environment as well as the Magento installation. Security starts with selecting a reliable Magento agency or Magento developer, a reliable hosting provider and secure software development. Throughout the project, an automated deployment process, limited access to resources, and admin security are essential too.

MORE INFORMATION ABOUT THE MAGENTO SECURITY BEST PRACTICES:

https://docs.magento.com/m2/ce/user_guide/magento/magento-security-best-practices.html

SECURE SOFTWARE DEVELOPMENT

Make sure your developers know and use secure software development techniques to overcome the most common risks to web application security.

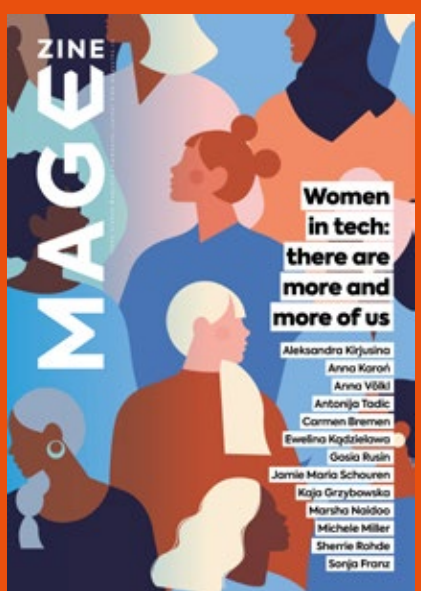
TEN MOST CRITICAL WEB APPLICATION SECURITY RISKS ACCORDING TO THE OWASP TOP 10 (2017) ARE:

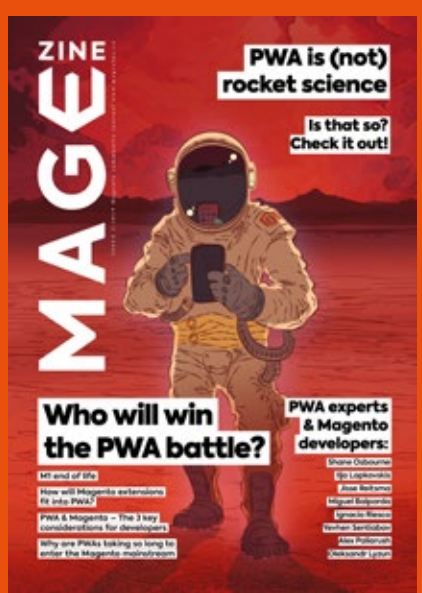
1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient Logging & Monitoring

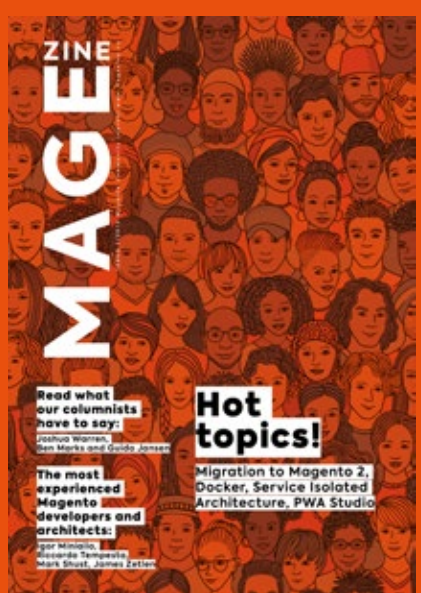
ZINE MAGE

Want more?

Get your free copy of Magazine & enjoy reading!







Download Magezine