agendize

Application Security

OWASP Top Ten Recommendations

From: Georges-Edouard Rambaud

Last Update: 23rd August 2017

Application Security

Agendize is committed to complying with OWASP Top 10 recommendations. Below are technical aspects put in place:

The Injection	• No field filled in the interface sent to the database • No field takes into account the entire SQL queries
Broken Authentication and Session Management	• Creation of an account: validation by captcha • Authentication: an account is blocked following 3 failed logins
Cross-Site Scripting	• Only one field accepts JavaScript. This JS only impacts the customer widget • Other fields block symbols such as <, > or the words "script", "onclick" ...
Insecure Direct Object References	• Control of the id depending on the user' session • Checks each operation (playback, writing, deletion) • Verification is done according to the relevant user's rights
Security Misconfiguration	• New versions of each component are installed upon validation • Default configuration files are deleted
Sensitive Data Exposure	• All exchanges of data between the server and the Internet are done via the secure protocol HTTPS

	• Database not accessible from the outside • No data sent without encryption • Database not linked to the Internet
Missing Function Level Access Control	• No password sent from Agendize servers to the Internet • No payment card required: all payments are made using PayPal
Cross-Site Request Forgery (CSRF)	• Each form submission is verified by the domain name to ensure that it is not an external solution
Using Components with Known Vulnerabilities	• Frequent updates of the components and application of the patches of security
Un-validated Redirects and Forwards	• Blocking in case of redirects (access codes 30x)

For more information on Open Web Application Security Project, refer to: https://fr.wikipedia.org/wiki/Open_Web_Application_Security_Project.