



4. Exercise

SS 16

Security of Distributed Software

1. Exercise

Dipl.-Inf. Fabian Wiedemann

Technische Universität Chemnitz

Faculty of Computer Science

Distributed and Self-organizing Systems

<https://vsr.informatik.tu-chemnitz.de>



Task 1 - XSS

- What is Cross-Site Scripting (XSS)?

Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites

(The Open Web Application Security project)



Task 1 - XSS

- Which defense methods against XSS do you know?
 - Validate user inputs
 - Encode output
 - Use **HttpOnly** flag for cookies
 - Deactivate JavaScript in the browser
 - Web Application Firewalls



Task 2 - XSS

- What is the difference between *stored*, *reflected* and *DOM-based* XSS attacks?
 - **Stored XSS Attacks:** Malicious code is stored on the server side – forums, guestbooks, etc.
 - **Reflected XSS Attacks:** Malicious code will be delivered to the client without storing on the server side
 - **DOM-based Attacks:** attack payload is executed as a result of modifying the DOM “environment”

