Conclusion

Christian Wenz

@chwenz

OWASP Top Ten (1-5)

#1

Injection

#2

Broken Authentication & Session Management

#3

Cross-Site Scripting (XSS)

#4

Insecure Direct Object References

#5

Security Misconfiguration

OWASP Top Ten (6-10)

#6

Sensitive Data Exposure

#7

Missing Function Level Access Control

#8

Cross-Site Request Forgery (CSRF)

#9

Using Known Vulnerable Components

#10

Unvalidated Redirects and Forwards

Summary

Validate input, escape output

Better paranoid than offline