

Do/Don't with HTTPS

- Always use HTTPS exclusively (in production)
- Always have a valid and signed certificate (no self-signed cert)
- Always avoid using absolute URL (mixed-content)
- Always use **secure** cookie flag with authentication cookie

Beyond HTTPS - Attacking the Web Application

Attacking the **Frontend**
(Man-in-the-Browser)

- **Cross-Site Scripting**
- **Cross-site Request Forgery**

Attacking the **Backend**
(Man-on-the-Server)

- **Broken Access Control**
(a.k.a incomplete mediation)
- **SQL Injection**