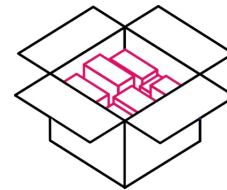


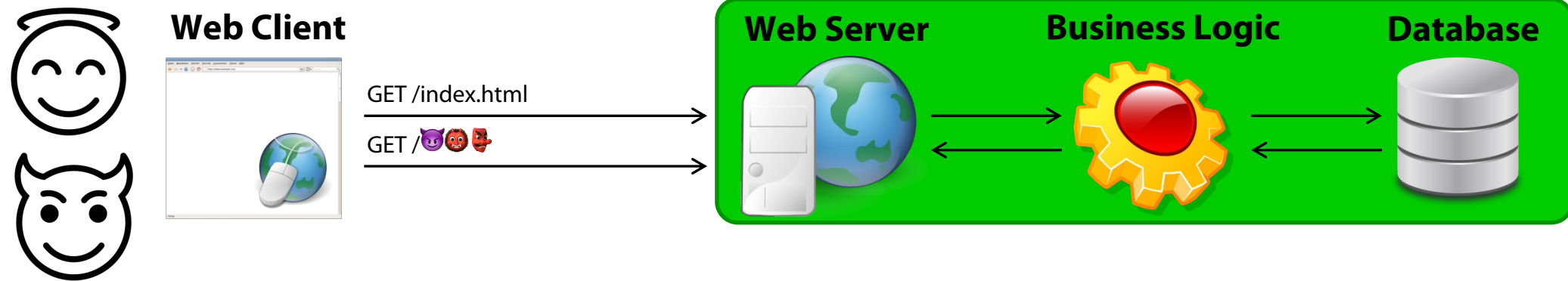
Eingabevalidierung

Hoai Viet Nguyen – TH Köln

Technology
Arts Sciences
TH Köln



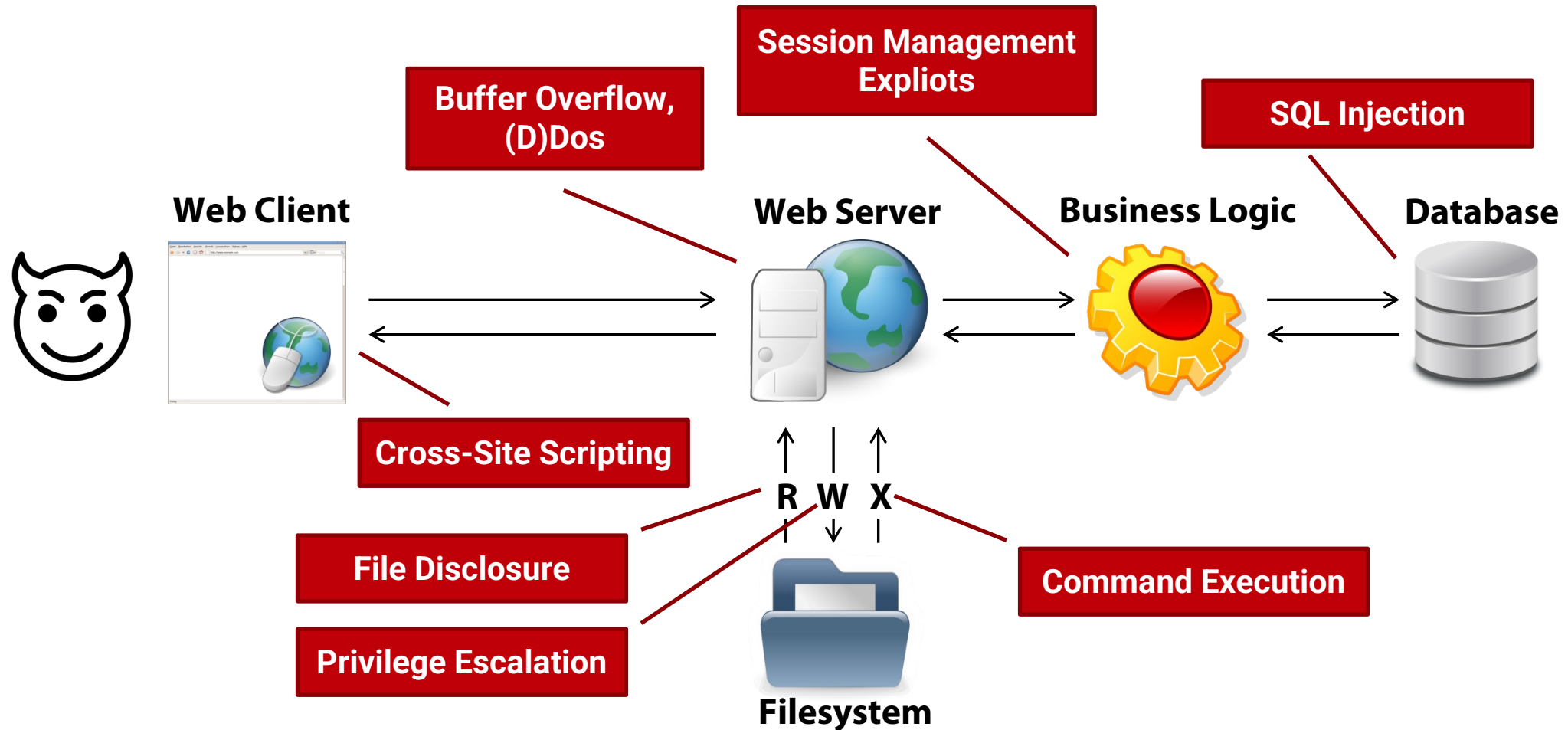
Trust Boundary



Client/Webbrowser nicht vertrauenswürdig

- Webanwendungen sind i.d.R. öffentlich zugänglich
- Betreiber von Webanwendung hat keine Kontrolle über Client
- Angreifer können beliebige Clients verwenden und beliebige HTTP-Anfragen konstruieren und absetzen

Angriffsziele in Webanwendungen (Auszug)



Eingabevalidierung

- Prüft Eingaben nach Plausibilität
- Invalide Eingaben werden nicht weiter verarbeitet
- Eingabevalidierung kann schon viele bekannte als auch unbekannte Angriffe vereitelt werden
- Arten von Eingabevalidierung
 - Whitelisting: Zulassung von bestimmten Zeichen und Muster
 - Blacklisting: Bestimmte Muster oder Zeichen verbieten
 - Längen- und Formatprüfung
 - Eingabe muss eine bestimmte Mindestlänge bzw. Maximallänge haben
 - Eingabe muss ein bestimmtes Format entsprechen z.B. E-Mail oder URL
 - Formatprüfung mit RegEx: Eingabevalidierung durch reguläre Ausdrücke

Regular Expression (Reguläre Ausdrücke)

- Wird zur Textsuche, -validierung und -manipulation genutzt
- Besteht aus Zeichen und Metazeichen, die Muster definieren
- Fast alle Programmiersprachen unterstützen RegEx
- Beispiele
 - Ein Zeichen aus der Menge a, b oder c: [abc]
 - Eine Ziffer von 0 bis 9: [0-9]
 - Gültige E-Mail: `^((?!\.)[\w\-_\.]*[^\.])(@\w+)(\.\w+(\.\w+)?)?[^\.W]$`

Eingabevalidierung mit RegEx

- Hier ist Vorsicht geboten, bei selbst definierten RegEx
- Selbst definierte RegEx können zu ReDoS führen
 - ReDoS: Regular expression Denial of Service
- Wenn möglich, vordefinierte RegEx verwenden
- RegEx immer mit einem ReDoS-Checker prüfen
 - <https://devina.io/redos-checker>

Registrierung

The image shows a browser window with the URL `https://example.org/registerform`. The page has a navigation bar with "Login" and "Registrierung" (highlighted). The main heading is "Registrierung". The form contains the following fields from top to bottom: "Vorname", "Nachname", "E-Mail", "Geburtstag", "Männlich" (a dropdown menu), "Passwort", and "Passwort wiederholen". A blue "Registrieren" button is at the bottom. Handwritten annotations with arrows point to the fields: "Längenprüfung: Maximal und minimal Länge" points to "Vorname" and "Nachname"; "Formatprüfung z.B. mit RegEx" points to "E-Mail" and "Geburtstag"; "Whitelisting" points to "Männlich"; and "Blacklisting" points to "Passwort".

Lernzielkontrolle

- **Warum sollte man den Client nicht vertrauen?**
- **Was ist Eingabevalidierung/Inputvalidierung?**
- **Welche Arten von Eingabevalidierung gibt es?**
- **Was sollte bei der Verwendung von RegEx für Eingabevalidierung beachtet werden?**

Zusammenfassung

- Clients sind als nicht vertrauenswürdig zu betrachten, weil wir keine Kontrolle darüber haben
- Eingabevalidierung prüft Eingaben nach Plausibilität
- Arten von Eingabevalidierung
 - Whitelisting/Blacklisting
 - Längenprüfung und Formatprüfung
 - Formatprüfung kann z.B. RegEx durchgeführt werden
- RegEx sollte auf ReDoS-Anfälligkeit geprüft werden