

# Sicherheit im Web

Bachelor – Projekt  
Digitale Medien

Dieter Hutter

Deutsches Forschungszentrum  
für Künstliche Intelligenz  
Cyber-Physical-Systems



# Motivation

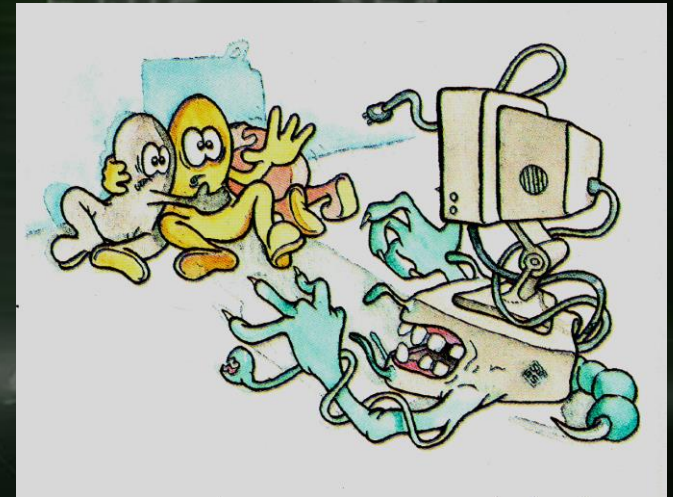
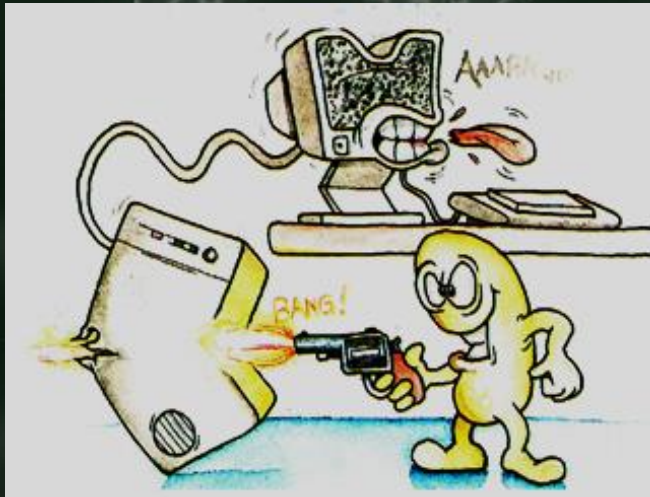


- Webseiten enthalten Programme
  - Javascript, PHP, ...
- Mein Rechner führt unbekannte Programme aus !
  - Was tun diese Programme?
  - Schaden mir die Programme?
- Mein Programm arbeitet mit unbekanntem Daten (json, php,...)
  - Arbeitet mein Programm sicher?
- Fast alle Webseiten benutzen solche Programme
  - Javascript – Sandbox
  - Browserbeschränkungen

The image shows a screenshot of the WetterOnline website for Bremen. The page displays weather information, including a current temperature of -3°C and a forecast for the next few days. A NoScript extension popup is visible in the foreground, listing various domains that are blocked or allowed. The popup includes options to temporarily allow or permanently allow certain domains, as well as a list of blocked sites and a link to the extension's settings.

Icon	Action
🚫	wetteronline.de verbieten
🔒	ligatus.com temporär erlauben
🔒	ligatus.com erlauben
🚫	ioam.de verbieten
🔒	criteo.com temporär erlauben
🔒	criteo.com erlauben
🚫	ivwbox.de verbieten
🔒	googletagservices.com temporär erlauben
🔒	googletagservices.com erlauben
🚫	Nicht vertrauenswürdig (1)
🚫	Kürzlich blockierte Websites
🔒	Temporär alle Beschränkungen für diese Seite aufheben
🔒	Alle Beschränkungen für diese Seite aufheben
🚫	Skripte allgemein erlauben (nicht empfohlen)
	<a href="#">Einstellungen...</a>
	<a href="#">Über NoScript 2.6.8.14rc1...</a>

1. Entwicklung eines Programms, das Javascript-Programme auf Sicherheitslöcher überprüft (statische Programmanalyse)
2. Spiel: jede Gruppe versucht, die Überprüfungsprogramme der anderen zu überlisten/überwinden



- Nützliche Vorkenntnisse
  - JavaScript, Syntaxanalyse (Parsen), Webprogrammierung,..
- Anpassung der Aufgabe an Teilnehmer
  - Einschränkungen der Programmiersprache
    - ▶ Analyse wird einfacher
  - Modifikation der Sandbox
    - ▶ Angriffe werden einfacher
  - Beispiele, die erkannt werden müssen
    - ▶ Alles ablehnen ist keine Lösung!

Prof. Dr. Dieter Hutter

Deutsches Forschungszentrum für Künstliche Intelligenz  
Cyber-Physical Systems

Bibliotheksstr. 1 (MZH 1350)

28359 Bremen

Tel.: (+49) 421-218-59831

Fax: (+49) 421-218-9859831

E-Mail: [hutter@dfki.de](mailto:hutter@dfki.de) / [hutter@uni-bremen.de](mailto:hutter@uni-bremen.de)