

# Chaosseminar

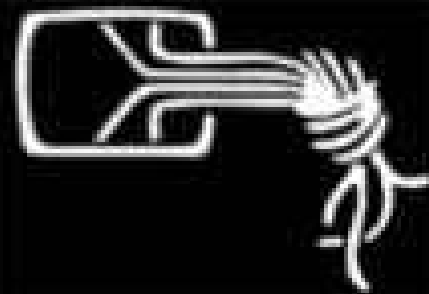


Gefahren für den Internet Client



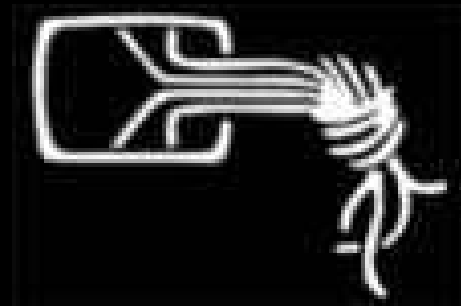
# Angriffsszenario

- DSL / LAN @home
  - Mit oder ohne WLAN AP?
- Öffentlicher Hotspot
  - Bahnhof / Flughafen / Cafe
- Universitätsnetzwerk
  - Mit dem Prof an der Leitung



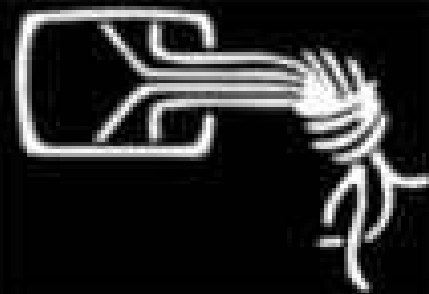
# Worüber wir nicht reden wollen

- Viren
- Würmer
- (Bundes-)Trojaner
- Lücken im OS / Anwendungssoftware
  - > Schalte nicht benötigte Dienste ab!
  - <http://www.dingens.org/win32sec-en.exe>
- Eifersüchtiger Freund / Freundin
- Mom Attack



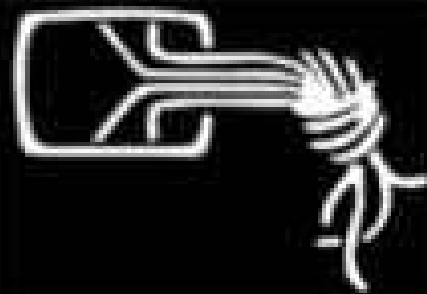
# Stattdessen geht's um...

- Warum sollte ich verschlüsseln?
- Angriffe auf
  - Web Traffic / Browser
  - E-Mail Verkehr
  - Chat Programme
  - Wireless LAN Security
- Was kann sonst noch passieren?



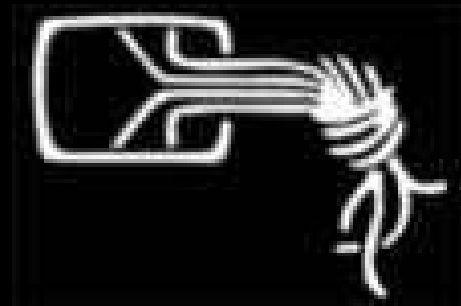
# Warum verschlüsseln?

- Bei unverschlüsseltem Traffic können Angreifer...
  - Passwörter lesen
  - Inhalte lesen / speichern
  - Inhalte manipulieren
- Für ein unverschlüsseltes WLAN trägst Du die volle Verantwortung
- Staatlicher Überwachungswahn
  - TKÜV
  - Vorratsdatenspeicherung?



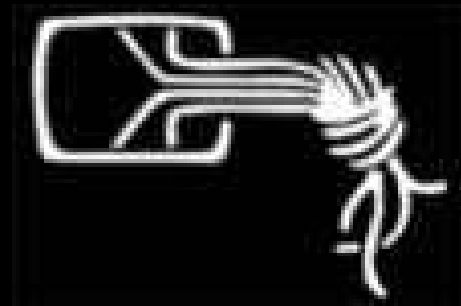
# Angriffe auf den Webtraffic

- Live Demo
  - Mitsniffen des Traffics
  - Mitsurfen
  - Umleiten des Traffics



# Angriffe auf den Browser

- Schadhafter Script Code
  - XSS (Cross Site Scripting)
  - Ajax Exploits
- Ungewollte URL-Aufrufe
  - CSRF (Cross Site Request Forgey)
  - HTTP Request Smuggling



# Cross Site Scripting

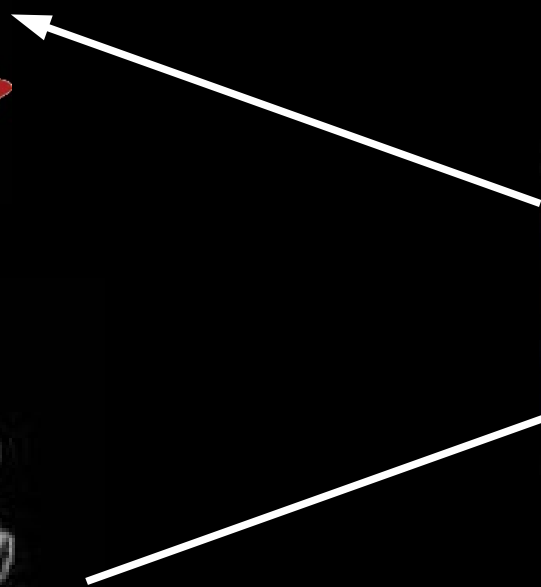
Happy User



Bad Boy

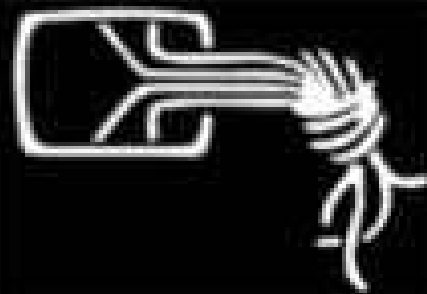


Big Web Server



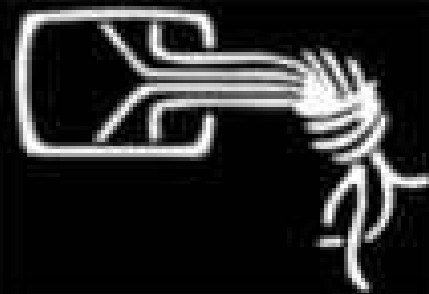
# Cross Site Scripting

- Code kann eingebettet sein in...
  - HTML Seite (Bsp. MySpace)
  - Web Forum
  - Blog Kommentare
  - Komische URLs
  - Fotografier-Links in Zeitungen
  - ...



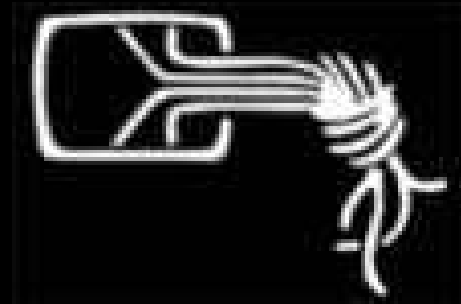
# Was kann XSS ausrichten?

- Kekse klauen
  - Passwortdaten
  - Session Hijacking
- Formulardaten klauen
- Keylogger
- Browser „Rootkit“ (XSSProxy)
- Interne Server angreifen
  - AP umkonfigurieren
  - Drucken



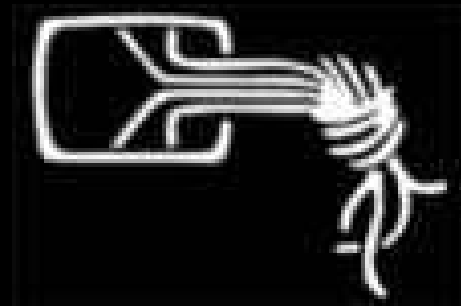
# Wie sieht XSS aus?

- `http://www.trustedside.net/search?q=<script>alert('Buh!');</script>`
- `http://www.trustedside.net/search?q=%3c%73%63%72%69%70%74%3e%61%6c%65%72%74%28%42%75%68%29%3b%3c%2f%73%63%72%69%70%74%3e`
- ``



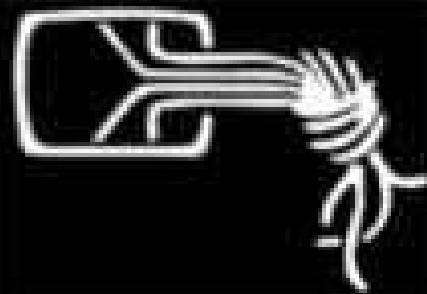
# Ungewollte URL Aufrufe

- CSRF
  - `<iframe width="0px" src="http://www.boehse-url.net/script?bla">`
- HTTP Request Smuggling
  - `http://www.trusted-side.net/script?q=suchmich\r\nhttp://www.boehseurl.net`



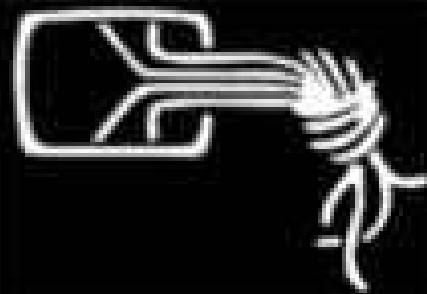
# Wie schütze ich mich?

- Javascript abschalten
- Kein Flash installieren
- Active X ausschalten
- Firefox mit noscript Plugin
- Nicht auf komische URLs klicken
  - Use /dev/brain!
- SSL / TLS verwenden
- Privoxy



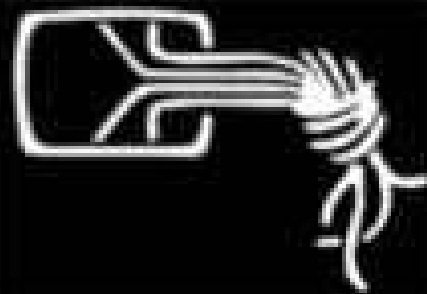
# Playing with E-Mails

- Livedemo
  - Passwort mitlesen
  - E-Mail mitlesen
  - E-Mail fälschen



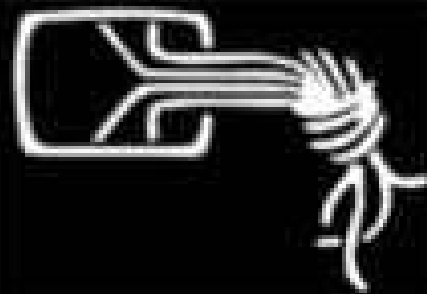
# Chatting around

- Livedemo IRC
  - Nachrichten lesen



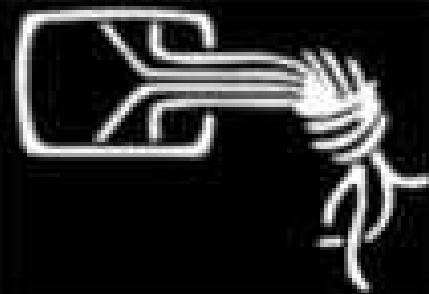
# Wie schütze ich mich?

- SSL / TLS
- PGP / GnuPG
- Für Instant Messaging Jabber mit digest Passwort verwenden
- SILC



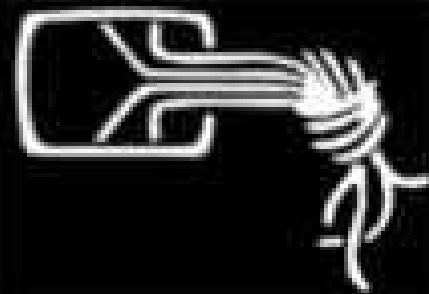
# Wireless Security

- Dont use WEP (Cracked in 60s)
- Use WPA2 / VPN
- MAC-Filter helfen nicht wenn ein Client online ist
- Closed SSID sinnlos
- Web-Interface des AP nur für's LAN
- Keine Default-Passwörter
- Upnp / SNMP abschalten



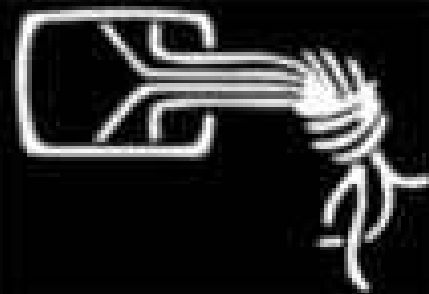
# Was kann sonst noch passieren?

- MiM (Man in the middle) Attacken
  - ARP Poisoning
  - ICMP Redirect
  - Airpwn
- DNS Rebind Attack
- Wireless AP Spoofing



# Tolle Links

- [www.ccc.de](http://www.ccc.de)
  - Für Datenschutz, Privatsphäre, Wahlbeobachtung und IT Security Fragen
- [www.ccc-fr.de](http://www.ccc-fr.de)
  - Der lokale CCC Treff. Einfach mal auf der Mailingliste vorbei schauen.
- [blog.kairaven.de](http://blog.kairaven.de)
  - Tutorials gegen Überwachungsmaßnahmen
- [sf.net/projects/anonym-os](http://sf.net/projects/anonym-os)
  - Die Everything-over-TOR-Cd
- [www.cryptocd.org](http://www.cryptocd.org)
  - Verschlüsselungsprogramme / Howtos





[www.datenterrorist.de](http://www.datenterrorist.de)