INF FAKULTÄT FÜR INFORMATIK

Der Webauftritt durchleuchtet:

das privatere, datensparsamere, nachhaltigere und IT-sicherere Web

SITSEC: DR1
17.05.2023

Jonas Morawietz
Bernhard Birnbaum
Meryem Lasri

Inhalt

1. Motivation & Aufgabenverständnis
2. Aufgabenverteilung
3. Ansätze & Fortschritte
   a. Allgemein
   b. EDPS
   c. Methodik
4. Tabellarische Zusammenfassung
   a. Tools
   b. Referenzen
5. bisherige Untersuchungsergebnisse
6. Nächste Schritte

1. Motivation & Aufgabenverständnis

Motivation:

- Webauftritte im Bereich Soziales/Gesundheit oftmals alles andere als datensparsam
- datenschutzrelevante Nutzerdaten werden an Drittparteien übermittelt und für Werbung und Profiling genutzt
- IT-sicherheitsrelevante Schwachstellen gefährden Nutzer zusätzlich

Aufgabenverständnis:

- Webauftritte mit OpenSource-Werkzeugen überprüfen, mit Bezug auf
  - Datensparsamkeit
  - Datenschutz
  - Nachhaltigkeit im Sinne des Ressourcenverbrauchs
  - IT-Sicherheit
- Möglichkeiten zu Selbstschutz/Selbstverteidigung erforschen
- Vergleich: Ressourcen vor und nach Blockierung von Trackern

2. Aufgabenverteilung

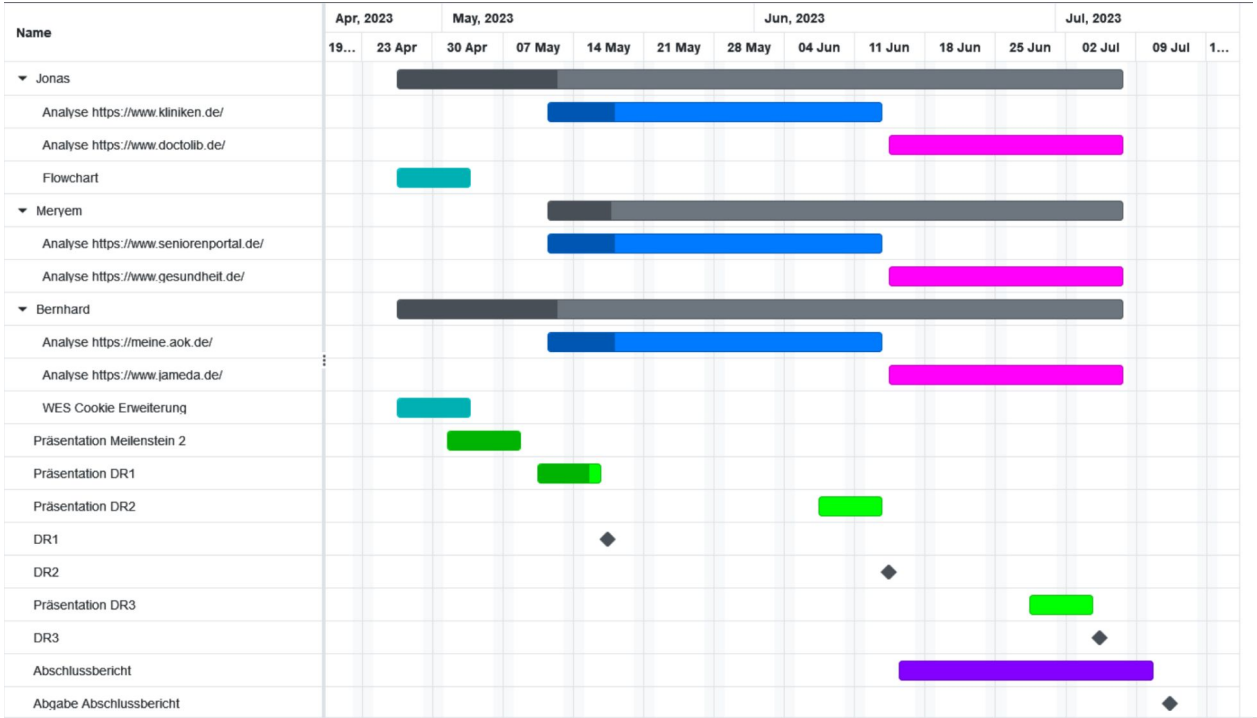
Ausgewählte Websites:

Website	Kurzbeschreibung	Warum gewählt?	Bearbeitung
https://meine.aok.de/	Website der Allgemeinen Ortskrankenkasse	sehr bekannte Krankenkasse, hohe Relevanz	Bernhard
https://www.kliniken.de/	Informationen zu Krankenhäusern, Rehakliniken, Pflege- und Altenheimen	Arbeit mit sensiblen, ortsspezifischen Krankheitsdaten	Jonas
https://www.seniorenportal.de/	Anlaufstelle für Senioren und ihre Angehörigen; bietet nützliche Informationen und Tipps	Informationsportal für ältere Menschen, welche meistens keine Affinität zu IT haben	Meryem
https://www.jameda.de/	Arzt finden und Termin online buchen	Website arbeitet direkt mit sehr sensiblen Informationen, die direkt mit dem Patienten in Verbindung stehen	Bernhard
https://www.doctolib.de/	Arzt finden und Termin online buchen	Website arbeitet direkt mit sehr sensiblen Informationen, die direkt mit dem Patienten in Verbindung stehen	Jonas
https://www.gesundheit.de/	Informationsseite zu Gesundheit, Krankheiten, Medizin, Ernährung		Meryem

2. Aufgabenverteilung

Aufgabenverteilung:

- **Alle**: Untersuchung von 2 Websites
- Jonas: Konzeptionierung der Tests
- Bernhard: EDPS-Cookie-Banner
- Meryem: ?



3. Ansätze & Fortschritte

- Arbeitsumgebung aufgesetzt
- Methodik für Untersuchung erarbeitet
- mit Ausarbeitung der Methodik für Auswertung begonnen

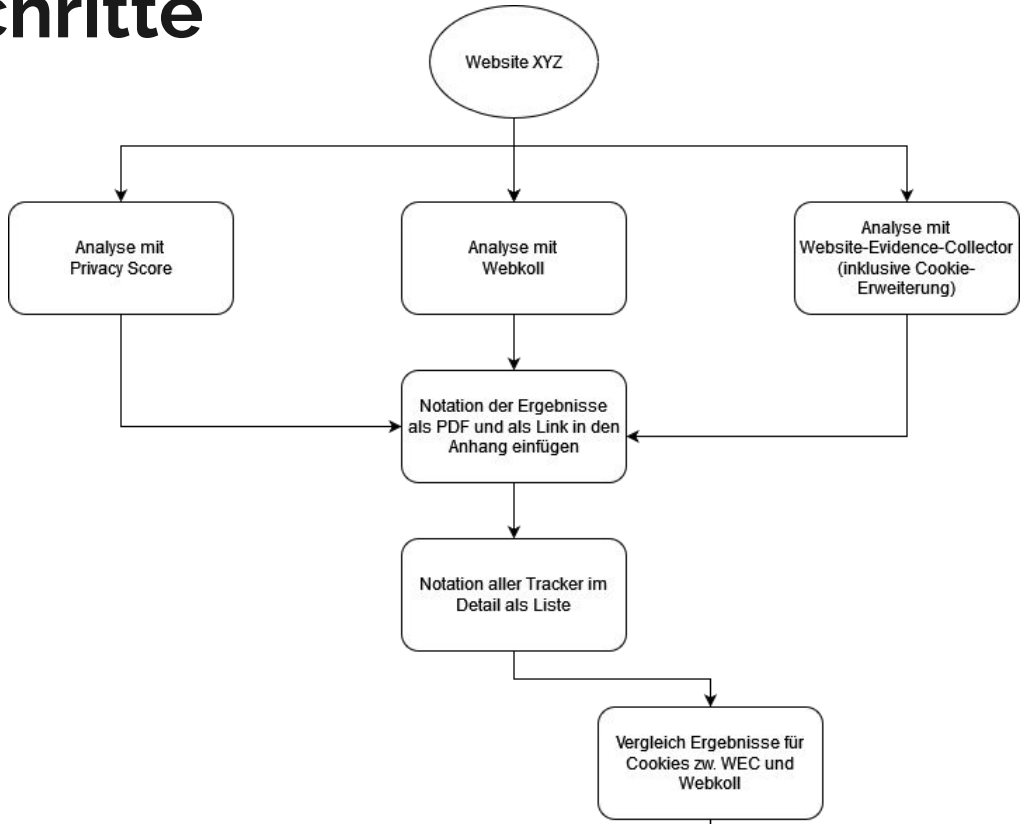
EDPS-Script-Erweiterung für pre-set-Cookies:

- Cookies werden vor Untersuchung mit dem EDPS manuell von der Website ausgelesen
- für das Banner relevante Cookies werden extrahiert und an EDPS übergeben
- bei der Website entsteht der Eindruck, der Nutzer hätte den Banner bereits bei einem früheren Besuch akzeptiert
- Umsetzung: Erweiterung des EDPS-Launch-Scripts des Testersticks
  → Nutzer wird vom Script aufgefordert Cookies einzugeben

3. Ansätze & Fortschritte

Methodik der Untersuchung:

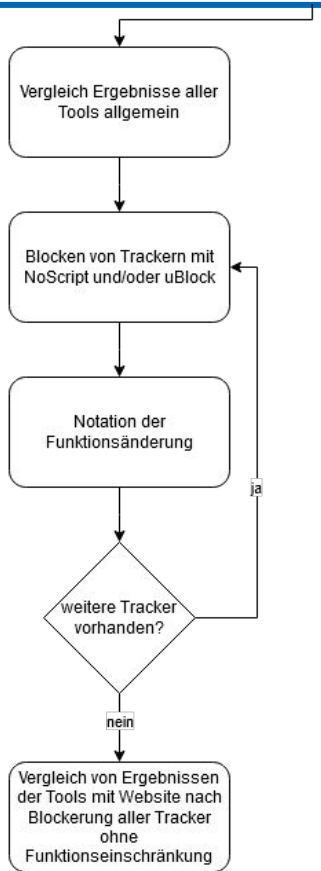
- Flowchart zum Vorgehen



3. Ansätze & Fortschritte

Methodik der Untersuchung:

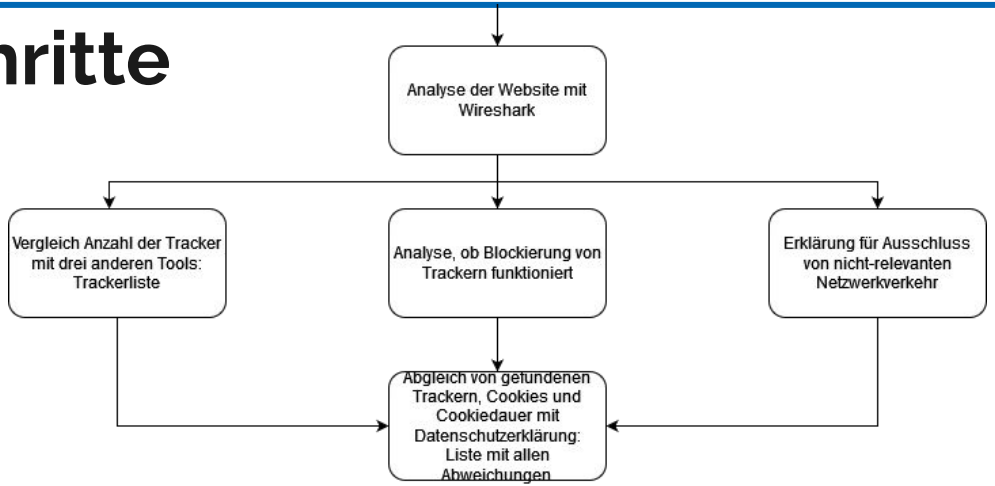
- Flowchart zum Vorgehen



3. Ansätze & Fortschritte

Methodik der Untersuchung:

- Flowchart zum Vorgehen



4. Tabellarische Zusammenfassung: Tools

Ausgewählte Werkzeuge:

Titel	Link	Beschreibung
Testerstick	intern	rauscharme Untersuchungsumgebung
Website-Evidence-Collector (EDPS)	https://github.com/EU-EDPS/website-evidence-collector	automatisierte Analyse von Speicherung und Transfer von persönlichen Daten
PrivacyScore	https://privacyscore.org/	bewertet Websites hinsichtlich einer Reihe von Sicherheits- und Datenschutzfunktionen
webbkoll	https://webbkoll.dataskydd.net/	prüft, welche Datenschutzmaßnahmen eine Website ergriffen hat
Firefox ESR	https://www.mozilla.org/de/firefox/all/#product-desktop-esr	Webbrowser mit Netzwerkanalyse
NoScript	https://noscript.net/	Blockierung bzw. kontrollierte Freigabe von JavaScript
uBlockOrigin	https://ublockorigin.com/de	Open-Source-Werbeblocker mit Zusatzfunktionen
Wireshark	https://www.wireshark.org/	Netzwerkprotokoll-Analyse und Entschlüsselung von Traffic (SSLKEYLOGFILE)

4. Tabellarische Zusammenfassung: Referenzen

Wissensbasis:

Titel	Quelle
[AKL+20] Introduction to Being a Privacy Detective: Investigating and Comparing Potential Privacy Violations in Mobile Apps Using Forensic Methods	ISBN 978-1-61208-821-1, pp 60-68, 2020
[Rie23] GitHub - EU-EDPS/website-evidence-collector: The tool Website Evidence Collector (WEC) automates the website evidence collection of storage and transfer of personal data.	https://edps.europa.eu/edps-inspection-software_en

5. Bisherige Untersuchungsergebnisse

Website	PrivacyScore	Webbkoll	Website Evidence Collector
https://www.jameda.de/	- HSTS preloading-Angriff evtl. möglich - SWEET32-Angriff evtl. möglich	- HSTS nicht für Subdomains - CSP fehlerhaft implementiert - Referrer-Policy nicht vorhanden - externe Ressourcen werden über HTTP oder mit relativen URLs geladen: integrity mit Prüfsumme bzw. crossorigin anonymous fehlt - ein Cookie bietet pot. Möglichkeit von XSS-Angriff bzw. MITM-Angriff (HttpOnly & Secure) - 80 Anfragen an 17 einzigartige Hosts	- HTTPS mit Redirect - keine Social-Media-Verknüpfungen - 1 First-party host, 17 einzigartige Third-party hosts - First-Party-Cookies: 2 - Third-Party-Cookies: 2 - über https://track.hubspot.com/__ptq.gif (1px GIF) werden m.H. von HTTP GET Tracking-Informationen übertragen
https://www.kliniken.de/	- HSTS preloading-Angriff evtl. möglich - kein CSP-Header - keine Referrer-Policy	- HSTS nicht für Subdomains - keine CSP implementiert - Referrer-Policy nicht vorhanden - alle Ressourcen laden vom gleichen Ursprungsort - keine Drittanbieteranfragen	- HTTPS mit Redirect - Twitter, Facebook, Linkedin - 1 First-party host host - 3 einzigartige Third-party hosts - First-Party-Cookies: 3 - Third-Party-Cookies: 2 - Beacons: Google Analytics und GoogleTagmanager

6. Nächste Schritte

- Methodik für Auswertung im Detail ausarbeiten
- Untersuchung(en) durchführen: mit allen gewählten Tools

Danke für Ihre Aufmerksamkeit!