

A walk on the web's wild side

STUDIENARBEIT

des Studiengangs Angewandte Informatik

an der Dualen Hochschule Baden-Württemberg Karlsruhe

von

Samuel Philipp
Daniel Brown
Jan-Eric Gaidusch

Abgabedatum 25. Januar 2017

Bearbeitungszeitraum

6 Monate

Matrikelnummern

9207236, DANIEL, 8296876

Kurs

TINF14B2

Ausbildungsfirma

Fiducia & GAD IT AG

Gutachter der Studienakademie

Dr. Martin Johns

Erklärung

(gemäß §5(3) der „Studien- und Prüfungsordnung DHBW Technik“ vom 29.9.2015)

Wir versichern hiermit, dass wir unsere Studienarbeit mit dem Thema:

„A walk on the web’s wild side“

selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt haben. Wir versichern zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Karlsruhe, den 25. Januar 2017

Ort, Datum

Samuel Philipp

Karlsruhe, den 25. Januar 2017

Ort, Datum

Daniel Brown

Karlsruhe, den 25. Januar 2017

Ort, Datum

Jan-Eric Gaidusch

Inhaltsverzeichnis

Abkürzungsverzeichnis	IV
Abbildungsverzeichnis	V
Tabellenverzeichnis	VI
Listings	VII
1 Einleitung	1
1.1 Einführung	1
1.2 Team	1
1.3 Aufgabenstellung	1
1.4 webifier	2
2 Theorie	3
3 Grundlagen	4
3.1 Frontend Technologien und Frameworks	4
3.2 Backend Technologien und Frameworks	4
3.3 Angriffstypen	4
3.3.1 Malware	4
3.3.2 Request Header Investigation	4
3.3.3 JavaScript Portscanning	4
4 Konzept	5
4.1 Überblick	5
4.1.1 webifier platform	5
4.1.2 webifier scheduler	5
4.1.3 webifier tester	5
4.1.4 webifier tests	5
4.2 Sicherheitstests	5

5	Umsetzung	6
6	Fazit	7
6.1	Zusammenfassung	7
6.2	Bewertung	7
6.3	Ausblick	7

Abkürzungsverzeichnis

WWW World Wide Web

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

1 Einleitung

1.1 Einführung

1.2 Team

1.3 Aufgabenstellung

Anbieter von zwielichtigen Web-Angeboten greifen ihre User mit diversen Client-seitigen Methoden an. Beispiele für solche Angriffe sind Malware Downloads, Phishing, JavaScript Intranet Angriffe, oder Browser Exploits.

Ziel der Arbeit ist eine systematische Untersuchung der Aktivitäten von semi-legalen Webseiten im World Wide Web (WWW). Das erwartete Ergebnis ist ein Prüfportal, auf dem jene Webseiten automatisiert analysiert werden und Ergebnisse präsentiert werden sollen.

Nach dem ersten Schaffen einer Übersicht von interessanten Zielen, wie z.B. One-Click-Hoster oder File-sharing Sites sollen ausgewählte Webseiten manuell untersucht werden. Außerdem sollen verschiedene Angriffsszenarien zur weiteren Prüfung ausgewählt werden. Der Untersuchungsprozess der Webseiten soll im Verlauf dieser Arbeit stückweise automatisiert und in den Rahmen einer Prüfanwendung gebracht werden.

Abschließend sollen eine Vielzahl von Webseiten mit der Anwendung getestet und die Ergebnisse ausgewertet und dokumentiert werden.

1.4 webifier

webifier ist eine Anwendung, um Webseiten auf deren Seriosität und mögliche client-seitige Angriffe auf den Nutzer hin zu untersuchen.

- Konzeption einer Evaluierungsplattform, basierend beispielsweise auf einem automatisch angesteuerten Web Browser in einer virtuellen Maschine.

2 Theorie

3 Grundlagen

3.1 Frontend Technologien und Frameworks

- HTML
- CSS
- JavaScript
- jQuery
- Bootstrap

3.2 Backend Technologien und Frameworks

- Java
- Spring
- Docker

3.3 Angriffstypen

3.3.1 Malware

3.3.2 Request Header Investigation

3.3.3 JavaScript Portscanning

4 Konzept

4.1 Überblick

4.1.1 webifier platform

4.1.2 webifier scheduler

4.1.3 webifier tester

4.1.4 webifier tests

4.2 Sicherheitstests

5 Umsetzung

6 Fazit

6.1 Zusammenfassung

6.2 Bewertung

6.3 Ausblick