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	9 Wochen
Matrikelnummer	8296876
Kurs	TINF14B2
Ausbildungsfirma	Fiducia & GAD IT AG
Gutachter der Studienakademie	Dr. Martin Johns

Erklärung

Gemäß §5 (2) der „Studien- und Prüfungsordnung DHBW Technik“ vom 18. Mai 2009.

Hiermit erklären wir,

1. dass wir die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet haben.
2. dass die Übernahme von Zitaten und Gedankengut anderer Autoren gekennzeichnet wurde.
3. dass die eingereichte elektronische Fassung exakt mit der schriftlichen übereinstimmt.
4. dass wir die Projektarbeit keiner externen Prüfung vorgelegt haben.

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

Sperrvermerk

Die vorliegende Projektarbeit T2_2000 mit dem Titel
„A walk on the web's wild side“
ist mit einem Sperrvermerk versehen und wird ausschließlich zu Prüfungszwecken am Studiengang Angewandte Informatik der Dualen Hochschule Baden-Württemberg Karlsruhe vorgelegt. Jede Einsichtnahme und Veröffentlichung - auch von Teilen der Arbeit - bedarf der vorherigen Zustimmung durch die Fiducia & GAD IT AG.

Inhaltsverzeichnis

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 Untersuchungsprozes 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 clientseitige Angriffe auf den Nutzer hin zu untersuchen.

- Konzeption einer Evaluierungsplatform, 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