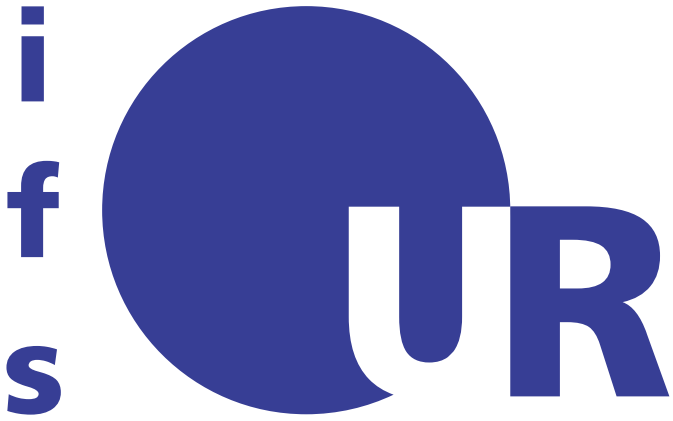
Universität Regensburg
Fakultät für Wirtschaftswissenschaften
Lehrstuhl für Wirtschaftsinformatik I - Informationssysteme

Angriffssimulation und strukturierte Datenerfassung



Praxisseminar

Eingereicht bei: Prof. Dr. Günther Pernul
Betreuung: Marietheres Dietz
Daniel Schlette

Eingereicht am 24. Juli 2020

Eingereicht von:

Johannes Seitz
Matrikelnummer: 2136257

Abstract

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

Abkürzungsverzeichnis

Bsp.	Beispiel
SaaS	Software as a Service

Kapitel 1

Einleitung

Wie sich in den Anfangsmonaten des Jahres bereits gezeigt hat, ist unser Wirtschaftssystem bei Weitem fragiler, als es viele Experten vorhersagen konnten. Innerhalb kürzester Zeit versetzte ein kleiner Virus die komplette Weltwirtschaft in einen ungewollten Ruhemodus. Es zeigte sich zudem, wie vorteilhaft sich der Einsatz von IT-Systemen in den meisten Branchen auszahlt. Heimarbeit wurde von vielen Unternehmen gefördert, Universitäten konnten von zu Hause aus lehren und auch Teamtraining von Profisportlern wurde durch Einsatz von Videotelefonie ermöglicht.
Dass die Verwendung von Informationssystemen und Internettechnologie nicht immer ohne Sicherheitsrisiken einhergeht, ist allerdings nicht zuletzt seit der "Corona-Krise"bekannt. Immer wieder gelingt es Angreifern an hochsensible Daten zu gelangen. Beispielsweise mussten Patienten eines tschechischen Krankenhauses verlegt werden, da die Uniklinik Brno gehackt wurde und somit der Betrieb der Klinik lahmgelegt wurde [Hol20]. Aber auch in der Industrie und bei Behörden kommt es immer öfter zu Angriffsversuchen. Deshalb ist es für die jeweiligen IT-Abteilungen eine ständige Herausforderung die betriebseigenen Systeme sowohl proaktiv, als auch präventiv zu schützen.
Um sich vor potentiellen Risiken zu schützen ist es schwierig das laufende System unter Stresstests zu setzen. Zu groß ist die Gefahr einen Ausfall herbeizuführen und den Betrieb dadurch zu unterbrechen. Als eine hilfreiche Methode hat sich in den letzten Jahren das Simulieren eines sogenannten Digitalen Zwillings herauskristallisiert. Dieser Digital Twin soll es Entwicklern ermöglichen ein reales System in einer geschützten Simulationsumgebung zu spiegeln und dieses unter beliebigen Bedingungen zu testen.
Eine weitere Herausforderung stellt die Präsentation von möglichen Angriffsvektoren dar. Die generierten Daten sind meistens nur schwer zu entziffern und daher nicht für den alltäglichen Umgang mit Bedrohungen im eigenen Netzwerk zu gebrauchen. Um dieses Problem zu lösen bietet es sich an einen Standard zu verwenden, der von vielen Aktoren genutzt wird. Ein derartiger Standard ist STIX (Structured Threat Information eXpression).
Im Rahmen eines Praxisseminars mit dem Titel Ängriffssimulation und strukturierte Datenerfassungßollte ein industrielles Setting abgebildet werden und der Netzwerkver-

kehr eines simulierten Angriffs mitgeschnitten werden. Die erfassten Daten sollten, dann mittels STIX 2.x strukturiert für Cyber Threat Intelligence aufgearbeitet werden.

Kapitel 2

Hauptteil

2.1 Beispiele

Dies ist eine Referenz auf ein Paper. Die Verwaltung der Referenzen erfolgt in der Datei References.bib. Zur Bearbeitung der Referenzen kann beispielsweise das Programm JabRef[1] verwendet werden.

Besonders interessant ist auch die automatische Erstellung des Abkürzungsverzeichnisses. Zuerst wird die Abkürzung definiert um bei erstmaliger Verwendung im Abkürzungsverzeichnis zu erscheinen: Beispiel (Bsp.), Software as a Service (SaaS)

Referenzen auf Grafiken: **??**, **??**, **??**

[1] http://jabref.sourceforge.net/

Querseite, Kopf- und Fußzeile aber korrekt für gebundene Arbeit.

Kapitel 3

Schluss

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Appendices

Anhang A

Erster Anhang

Anhang B

Zweiter Anhang

B.1 Anhang

B.2 Anhang

Literaturverzeichnis

[Hol20] HOLLAND: Wend Coronavirus-Pandemie: Cyberangriff legt tschechischesKrankenhaus lahm. (2020). https://www.heise.de/-4683370

Erklärung an Eides statt

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.
Die elektronische Ausfertigung der Arbeit habe ich bereits beim Prüfer eingereicht.

Regensburg, den 24. Juli 2020

Johannes Seitz
Matrikelnummer 2136257