Universität Osnabrück
Institut für Informatik
Arbeitsgruppe Software Engineering
Prof. Dr.-Ing. Elke Pulvermüller

EXPOSE

ZUM THEMA “ENTWICKLUNG EINER PYTHON BIBLIOTHEK ZUR ABSICHERUNG VON WEBAPPLIKATIONEN”

Vorgelegt von Benjamin Müller am 28.02.2020
Matrikelnummer 962010

Im Bachelorstudiengang Informatik

INHALT

Inhalt

Motivation und Ausgangssituation

Das Feld der IT Sicherheit gewinnt seit Jahren zunehmend an Bedeutung für Organisationen weltweit. Mit dem rasanten technischen Fortschritt und der Digitalisierung werden mehr und mehr Prozesse auf Computern in alles Größen und Umgebungen ausgeführt. Ein Beispiel hierfür ist das Internet of Things, womit immer mehr industrielle und private Endgeräte an das Internet angeschlossen werden. Smart Homes, Smart Facturies und Smart Cities sind schon heute komplexe Vernetzungen einer Vielzahl von Rechnern. Ein anderes Beispiel ist die Digitalisierung von Geschäftsprozessen, die Prozesse und Daten, die für den Unternehmenserfolg kritisch sind, in Rechnernetze verlagert, die prinzipiell alle angreifbar sind.

Die Ausgangssituation meiner Bachelor Arbeit ist eine CRUD (Create, Read, Update, Delete) Web Anwendung mit User-bezogener Datenspeicherung. Die Anwendung wird mit dem Python Framework Django entwickelt. Die Software dient dem Zweck, im Rahmen des universitären Betriebs Dozenten, Studenten und Mitarbeitern des Sekretariats Termine in einen Kalender eintragen zu lassen.

Der Login wird mithilfe des Verzeichnisdienstes LDAP an das Rechenzentrum (RZ) der Universität Osnabrück angebunden, sodass die User sich mit ihren RZ Daten einloggen können. Ein Termin besteht aus Datum und Uhrzeit und einem freien Kommentar. Ein Termin kann öffentlich für alle sichtbar oder privat nur für den User sichtbar sein. Die Benutzeroberfläche besteht aus einem Eingabeformular für neue Termine und einem Kalender zur Ansicht bestehender Termine. Sämtliche Änderungen werden geloggt mit Zeitstempel, eingegebenen Daten und eingebender User.

ZIELSETZUNG

Zielsetzung

Die App wird ohne besondere Rücksicht auf Sicherheit programmiert. Daraus werden einige Schwachstellen resultieren. Das Ziel dieser Arbeit ist die Entwicklung einer Bibliothek, mit dem die bestehenden Sicherheitslücken auf einfache Art und Weise geschlossen werden können. Die Bibliothek kann weitere Abhängigkeiten haben. Insbesondere wird sie die Funktionalitäten von Django ausnutzen, und so eine zusätzliche Hülle bilden, die den Zugriff auf Djangos Sicherheitsfeatures vereinfacht.

Zur theoretischen Vorbereitung für diese Aufgabe werden im ersten Hauptteilkapitel die häufigsten Schwachstellen von Web Applikationen zusammengestellt. Diese werden den Fokus bei der Schwachstellenanalyse der App und der Konzipierung der Bibliothek bilden. Das primäre Kriterium zur Auswahl einer Schwachstelle wird deren Risiko für die Sicherheit der App sein. Als Quelle hierfür eignet sich z. B. das OWASP Top Ten Projekt[1], in dem die 10 kritischsten Schwachstellen von Web Applikationen aufgeführt werden.

Anschließend wird eine Kosten-Nutzen Analyse aufgestellt, in der die Performance Einbußen durch den Einsatz der Bibliothek mit dem Nutzen für die Software Sicherheit verglichen werden. Ersteres wird durch experimentelle Laufzeitmessung festgestellt. Letzteres wird anhand einer oder mehrerer Metriken zur Messung der Sicherheit einer Software ermittelt.

[1] https://owasp.org/www-project-top-ten/

Gliederung

Mein Vorschlag der Gliederung sieht folgendermaßen aus:

1. Abstract
2. Einleitung
3. Häufige Sicherheitslücken in Web Applikationen
4. Beschreibung der CRUD App (Ist-Zustand)
   4.1. Schwachstellenanalyse
5. Sicherheitsbenefits der Bibliothek
6. Kosten-Nutzen Analyse
7. Fazit
8. Quellen










QUELLEN

Quellen

- *OWASP Top Ten (https://owasp.org/www-project-top-ten/)*
- *National Vulnerability Database (https://nvd.nist.gov/)*
- S. M. Srinivasan and R. S. Sangwan, "Web App Security: A Comparison and Categorization of Testing Frameworks," in *IEEE Software*, vol. 34, no. 1, pp. 99-102, Jan.-Feb. 2017, doi: 10.1109/MS.2017.21.
- H. Huang, Z. Zhang, H. Cheng and S. W. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls," in *Computer*, vol. 50, no. 6, pp. 81-85, 2017, doi: 10.1109/MC.2017.183
- Scott, Sharp: „Abstracting application-level web security" in: *WWW '02: Proceedings of the 11th international conference on World Wide Web*, May 2002, Pages 396–407
- A. Alzahrani, A. Alqazzaz, Y. Zhu, H. Fu and N. Almashfi, "Web Application Security Tools Analysis," *2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids)*, Beijing, 2017, pp. 237-242, doi: 10.1109/BigDataSecurity.2017.47.
- S. Kumar, R. Mahajan, N. Kumar and S. K. Khatri, "A study on web application security and detecting security vulnerabilities," *2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),* Noida, 2017, pp. 451-455, doi: 10.1109/ICRITO.2017.8342469.
- L. Giannopoulos, E. Degkleri, P. Tsanakas, and D. Mitropoulos. 2019. Pythia: Identifying Dangerous Data-flows in Django-based Applications. In *Proceedings of the 12th European Workshop on Systems Security* (*EuroSec '19*). Association for Computing Machinery, New York, NY, USA, Article 5, 1–6. DOI:https://doi.org/10.1145/3301417.3312497
- J. Jayakody, A. Perera and G. Perera, "Web-application Security Evaluation as a Service with Cloud Native Environment Support," *2019 International Conference on Advancements in Computing (ICAC),* Malabe, Sri Lanka, 2019, pp. 357-362, doi: 10.1109/ICAC49085.2019.9103414.

QUELLEN

- G. Erdogan, “Security Testing of Web Based Applications,” master’s thesis, Dept. Computer and Information Science, Norwegian Univ. of Science and Technology, 2009;