

<b>Projekttitel</b>	
WebSecBot – Web Security Bot	
<b>Projektleiter (Name, E-Mail)</b>	<b>Coach (Name, E-Mail)</b>
Rijha Ehtsham, rijhaehtsham1@gmail.com	Jörg Häderli, joerg.headerli@zli.ch
<b>Projektstart</b>	<b>Projektende</b>
07.06.2023	30.06.2023
<b>Idee / Kurzbeschreibung</b> (Um was geht es bei diesem Projekt?)	
<p>In meinem Projekt geht es darum, die Sicherheit von Webapplikationen zu verstehen und zu testen, indem ich ein Bot entwickle, welcher verschiedene Sicherheitsmechanismen umgehen kann. Daraus kann ich lernen, wie (un)sicher das Web ist und wie man die Sicherheit verstärken kann.</p> <p>Der Schwerpunkt des Projekts liegt auf das Umgehen von Website-Einschränkungen mit der Codierung eines Bypass-Scripts, dem Eingeben vorinstallierter Daten und der Bewältigung von Captcha-Systemen mit einem Bot.</p> <p>Zusätzlich werden optionale Ziele wie die Verwendung verschiedener Proxys und das Überwachen des Backends der Website verfolgt.</p>	
<b>Ausgangslage</b> (Was ist los? Warum wird der Projektauftrag gestellt?)	
<p>Da ich mich seit längerem mit dem Thema befasst habe und ich dieses Projekt schon immer mal machen wollte, möchte ich die Chance nutzen und die Idee bei meinem Abschlussprojekt umsetzen.</p> <p>Generell interessiert mich der IT-Security Bereich in meinem Beruf am meisten, weshalb ich mir mit meinem Projekt neues Wissen in diesem Bereich erlernen möchte.</p>	
<b>Projektziele</b> (Erwartete Resultate. Forderungen und Wünsche)	<b>Prior.<sup>1</sup></b>
Website-Einschränkungen wie zum Beispiel queueit also Warteschleifen bei Loadingpages mit der Codierung eines Bypass Scripts umgehen können.	A
Vorinstallierte Daten eingeben können (z. B. Name, Adresse, Kartendetails usw.).	A
Der Bot sollte mit Captcha-Systemen wie Capmonster kompatibel sein, um das Captcha zu lösen	A
Verwendung verschiedener Proxys, um als „neue Benutzer“ zu erscheinen.	B
Überwachen des Backends der Website anhand des SKU-Codes.	B
<b>Vorgehensziele</b> (Forderungen und Rahmenbedingungen)	<b>Prior.<sup>1</sup></b>
Wissen in der Programmiersprache JavaScript vertiefen.	A
Grundwissen in HTML und CSS vertiefen/wiederholen.	A
Verständnis für die Struktur und Funktionsweise von Webanwendungen vertiefen.	A

Die Grundlagen der Webanwendungssicherheit, einschliesslich der gängigen Sicherheitslücken und Angriffstechniken wie Cross-Site Scripting (XSS), SQL-Injection, Cross-Site Request Forgery (CSRF) usw. erlernen	A
Verschiedene Techniken und Ansätze zur Umgehung von Website-Einschränkungen kennenlernen.	A
Verschiedene Web-Frameworks und deren Verwendung, um Webanwendungen zu entwickeln kennenlernen.	A
Mit dem erlernten Wissen Bypass Script entwickeln.	A
Das entwickelte Bypass Script auf seine Funktionalität überprüfen, indem ich es auf der betreffenden Website testen.	A
<b>(Erstes Ziel erreicht)</b>	
Verschiedene HTML-Tags und -Elemente erkunden, um das Formular für die Dateneingabe zu verstehen.	A
Die Struktur von HTML-Formularen studieren und wie sie Informationen erfassen.	A
Lernen, wie HTTP-Anfragen funktionieren und wie Daten zwischen einem Client (Bot) und einem Server ausgetauscht werden.	A
Die Unterschiede zwischen GET- und POST-Anfragen kennenlernen und wie Daten in Anfragen übertragen werden.	A
Automatisierungswerkzeuge und -frameworks erforschen, welche ermöglichen, Interaktionen mit Webseiten zu automatisieren.	A
Wissen über Web Scraping vertiefen, um Daten von Webseiten zu extrahieren.	A
Programmierkenntnisse anwenden, um eine Logik zu entwickeln, mit der der Bot vorinstallierte Daten in die entsprechenden Formularfelder eingeben kann.	A
Bot auf verschiedenen Webseiten testen, um sicherzustellen, dass er die vorinstallierten Daten korrekt eingibt.	A
Mögliche Fehler oder Probleme analysieren und diese beheben, um die Funktionalität des Bots zu verbessern.	A
<b>(Zweites Ziel erreicht)</b>	
Lernen, wie Captcha-Systeme funktionieren und warum sie eingesetzt werden, um automatisierte Bots zu erkennen.	A
Verschiedene Captcha-Techniken wie Textbasierte Captchas untersuchen.	A
Über die Capmonster-API und deren Funktionsweise informieren.	A
Lernen, wie ich HTTP-Anfragen an die Capmonster-API senden kann, um Captchas zu lösen.	A
Bot so zu erweitern, dass er das Captcha automatisch über die Capmonster-API lösen kann.	A

Bot auf verschiedenen Webseiten testen, die Captchas verwenden, um sicherzustellen, dass er das Captcha korrekt lösen kann.	A
Mögliche Fehler oder Probleme analysieren und diese beheben, um die Funktionalität des Bots zu verbessern.	A
<b>(Drittes Ziel erreicht)</b>	
Grundlagen von IP-Adressen, Ports, TCP/IP-Protokollen und Netzwerkverbindungen vertiefen/wiederholen.	B
Proxy-Server erforschen und wie sie verwendet werden, um den Datenverkehr zwischen einem Client und einem Server umzuleiten.	B
Verschiedenen Arten von Proxys kennenlernen.	B
Vertrauenswürdigen Proxyservice-Anbietern suchen, die eine Liste von Proxys zur Verfügung stellen.	B
Über die unterschiedlichen Funktionen und Eigenschaften der Proxyservices informieren, wie z. B. die Möglichkeit, Proxys nach Standort, Geschwindigkeit und Protokoll auszuwählen.	B
Den Bot so zu erweitern, dass er Proxys verwenden kann, um als "neue Benutzer" zu erscheinen.	B
Lernen, wie ich HTTP-Anfragen über einen Proxy-Server senden und die Proxy-Adresse in Ihre Anfragen integrieren können.	B
Lernen, wie ich in meinem Bot die Fähigkeit implementieren kann, zwischen verschiedenen Proxys zu wechseln, um Ihre Identität zu ändern.	B
Bot testen	B
<b>(Erstes Optionales Ziel erreicht)</b>	
Lernen, was ein SKU-Code ist und wie er verwendet wird, um ein Produkt oder einen Artikel zu identifizieren.	B
Lernen, wie der SKU-Code in der Datenbank oder im Backend der Website verwendet wird.	B
Monitoring-Tools suchen, die helfen, das Backend einer Website zu überwachen.	B
Die Möglichkeiten erforschen, um Daten aus dem Backend einer Website abzurufen, wie APIs, Datenbankabfragen oder Protokolldateien.	B
Lernen, wie ich die gewünschten Informationen über den SKU-Code aus den Monitoring-Schnittstellen extrahieren kann.	B
Programmierkenntnisse verwenden, um einen Mechanismus zu erstellen, um die relevanten Daten aus dem Backend der Website anhand des SKU-Codes zu extrahieren.	B
Lernen, wie ich HTTP-Anfragen oder Datenbankabfragen verwenden kann, um die gewünschten Informationen abzurufen.	B
Lernen, wie ich die erhaltenen Daten aus dem Backend analysieren und relevante Informationen extrahieren können.	B

Implementierung testen.	B
<b>Lernziele</b> (Welche Kompetenzen werden angestrebt?)	<b>Prior.<sup>1</sup></b>
Website Frameworks kennenlernen.	A
Gefährdete Bereiche analysieren können.	A
Verständnis der IT-Sicherheit im Web lernen.	A
Lernen, wie die Sicherheit auf Websites erhöht werden kann.	A
Lernen wie Dinge gefiltert werden.	A
<b>Ressourcen</b> (Personal, Sachmittel, Material?)	<b>Menge</b>
Leistungsstarker Computer für die Entwicklung und Ausführung des Bots sowie für die Analyse der Webanwendungen.	1
Zugang zu Websites und Webanwendungen, welche ich mit Einverständnis des Eigentümers mein Bot einsetzen kann.	1-2
Handbücher und Anleitungen im Internet	-
<b>Projektentscheidung</b> (Freigabeunterschrift)	<b>Datum</b>
Freigabe durch:	

1) A = Must have

B = Starkes Wunschziel, wenn irgendwie möglich

C = "Nice to have"