



T.C.
MANİSA CELAL BAYAR
ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ
BÖLÜMÜ



AllScan

Graduation Project I

HAZIRLAYANLAR

190315041-Ergül Ferik

190315080-Ceyhun BİNAL

DANIŞMAN

Doç. Dr. Bora CANBULA

MANİSA 2023

T.C.
MANİSA CELAL BAYAR ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

Graduation Project I

KABUL VE ONAY BELGESİ

-----'ın
“-----”
isimli lisans projesi çalışması, aşağıda oluşturulan jüri tarafından değerlendirilmiş ve kabul edilmiştir.

Danışman :

Üye :

Üye :

Projenin Savunulduğu Tarih :

Bilgisayar Mühendisliği Bölüm Başkanı

TABLE OF CONTENTS

	Page
1. ABBREVIATION LIST	6
2. FIGURE LIST	7
3. TABLE LIST	8
4. ABSTRACT	9
4.1 Keywords	9
5. INTRODUCTION	10
5.1 Context and Purpose	10
5.2 Workflow	10
5.3 Integration with Kaspersky Threat Intelligence Portal	10
5.4 User Notification	11
5.5 Objective and Impact	11
6. REALISTIC CONSTRAINS AND CONDITIONS	12
6.1 Sustainable Development Goal	12
6.2 Effects on Health, Environment, and the Problems of the Age Reflected in the Field of Engineering	12
6.3 Legal Consequences	13
7. ANALYZING LITERATURE	14
7.1 An Overview of Online Security	14
7.2 State-of-the-Art in Internet Security	15
7.2.1 Artificial Intelligence and Machine Learning	15
7.2.2 Zero Trust Security Model	15
7.2.3 End-to-End Encryption	15
7.2.4 Biometric Security	16
7.2.5 Blockchain Technology	16
7.2.6 Advanced Threat Monitoring and Analysis	16
7.2.7 IoT Security	16
7.2.8 Social Engineering and Awareness	16
7.3 Comparable Technologies and Applications	17
7.4 AllScan Technology	17
7.5 Final Thoughts	18
7.6 References	18
8. STANDARDS	19
8.1 JavaScript Frontend Standards	19
8.2 Python Flask Backend Standards	19
8.3 Data Transfer and Security Controls	19

8.4	Code Security and Performance	20
9.	APPROACHES, TECHNIQUES, AND TECHNOLOGIES	21
9.1	APPROACHES	21
9.1.1	Data Transfer and Analysis Methods:	21
9.1.2	Malicious Link Detection Method.....	21
9.1.2.1	Using Kaspersky's "Threat Intelligence Portal" API.....	21
9.1.2.2	Using Kaspersky API with Asynchronous Thread Technology.....	21
9.2	TECHNIQUES	22
9.2.1	JavaScript Frontend	22
9.2.2	Python Flask Backend	22
9.3	TECHNOLOGIES	23
9.3.1	JavaScript.....	23
9.3.2	Python Flask	24
9.3.3	Kaspersky Threat Intelligence Portal.....	24
9.3.4	RESTful API.....	24
10.	RISK MANAGEMENT	25
11.	PROJECT SCHEDULE AND TASK SHARING.....	26
12.	SYSTEM REQUIREMENTS ANALYSIS	27
12.1	Use Case Model.....	27
12.2	Object Model	29
13.	SYSTEM DESIGN.....	30
13.1	System Architectural Diagram	30
13.1.1	Sequence Diagram	31
13.1.2	State Diagram	34
14.	SYSTEM TEST DESIGN	37
14.1	REQ 01: Reset Database.....	38
14.1.1	TC01: Invalid Operation Selection.....	39
14.1.2	TC02: Incorrect Username Input	40
14.1.3	TC03: Incorrect Password Input	41
14.1.4	TC04: Correct Operation Selection, Valid Username, and Password Input.....	42
14.2	REQ 02: Update Database	43
14.2.1	TC01: Invalid Operation Selection	44
14.2.2	TC02: Incorrect Username Input	45
14.2.3	TC03: Incorrect Password Input	46
14.2.4	TC05: Correct Operation Selection, Valid Username, and Password Input.....	47
14.3	REQ 03: Notifying the User of Security Status of Connections	48
14.3.1	TC06-TC10: Presence on a Page Containing Links with Different Security Fields	50
14.4	REQ 04: Warning of Harmful Connection Inputs	55
14.4.1	TC11: Warning on Malicious Link Click.....	56
14.4.2	TC12: User Redirected if They Choose to Proceed.....	57
14.4.3	TC13: User Stays on the Current Page if They Choose Not to Proceed	58
14.5	REQ 05: Page Scans Should Be Fast in Performance	59

14.5.1	TC14: Perform Operations on More Than One at the Same Time.....	60
14.5.2	TC15: Another Page Must Be Opened Before a Page Loads.....	61
14.5.3	TC16: Access to an Unscanned Page Before the Page Is Loaded.....	62
15.	DISCUSSION OF THE RESULTS.....	63
16.	REFERENCES	65
17.	INTERDISCIPLINARY DOMAIN	66
18.	SUSTAINABLE DEVELOPMENT GOAL	67
19.	SIMILARITY REPORT.....	68

1. ABBREVIATION LIST

AI : Artificial Intelligence.....	13
AJAX : Asynchronous JavaScript and XML.....	20
API : Application Programming Interface.....	8
DOM : Document Object Model.....	20
e.g. : for example.....	21
ECMAScript : European Computer Manufacturers Association.....	17
etc : et cetera.....	20, 21
HTML : Hypertext Markup Language.....	19
IoT : Internet of Things.....	ii, 14
JSON : JavaScript Object Notation.....	20
ML : Machine Learning.....	13
PEP : Python Enhancement Proposal.....	17, 31
RESTful API : Representational State Transfer Application Programming Interface.....	19, 22
UI/UX : User interface / User Experience.....	17
URL : Uniform Resource Locator.....	7
VAPT : Vulnerability Assessment and Penetration Testing.....	13

2. FIGURE LIST

Figure 1- Use Case Diagram 28

Figure 2- Object Model 29

Figure 3- System Architectural Diagram 30

Figure 4- Sequence Diagram 31

Figure 5- State Diagram 34

3. TABLE LIST

Table 1- Risk Management.....	25
Table 2- Project Schedule and Task Sharing.....	26
Table 3- Requirement Traceability Matrix.....	37
Table 4- REQ-01 Detailed Traceability Matrix.....	38
Table 5- Test Case 01	39
Table 6- Test Case 02	40
Table 7- Test Case 03	41
Table 8- Test Case 04	42
Table 9 - REQ-02 Detailed Traceability Matrix.....	43
Table 10 - Test Case 01	44
Table 11 - Test Case 02	45
Table 12 - Test Case 03	46
Table 13 - Test Case 05	47
Table 14 - REQ-03 Detailed Traceability Matrix.....	49
Table 15 - Test Case 06.....	50
Table 16 - Test Case 07	51
Table 17 - Test Case 08	52
Table 18 - Test Case 09	53
Table 19 - Test Case 10	54
Table 20 - REQ-04 Detailed Traceability Matrix.....	55
Table 21 - Test Case 11	56
Table 22 - Test Case 12.....	57
Table 23 - Test Case 13	58
Table 24 - REQ-05 Detailed Traceability Matrix.....	59
Table 25 - Test Case 14	60
Table 26 - Test Case 15	61
Table 27 - Test Case 16	62

4. ABSTRACT

Malicious individuals are using fraudulent links to get users' personal information. Among other things, these data are utilized for account takeovers, financial fraud, identity theft, corporate invasions, and the spread of harmful software.

Because of these advancements, internet security is becoming more and more crucial every day. The aim of the recently developed AllScan technology is to provide users with a safe and secure internet experience. This program is designed to systematically discover and inspect each link on a webpage while doing security checks, thanks to integrated antivirus software. Users may browse the internet with confidence since every connection's security is updated in real time.

Using algorithms, AllScan meticulously checks URLs taken from websites for security flaws. As soon as connections are discovered, the application begins scanning in tandem with leading antivirus applications. The results are then displayed to the user, indicating which connections are safe and which may be hazardous.

AllScan's ability to increase security while integrating seamlessly with the user's browser is one of its main advantages. With the application running in the background, users may make informed decisions about what they do online. AllScan's user-friendly interface and real-time network inspection make accessing the internet safer.

In summary, AllScan integrates link analysis and antiviral characteristics during user interactions to provide protection against cyber threats.

4.1 Keywords

Online Security, Real-Time Threat Detection, Safe Browsing Solution, Risk-Aware Web Surfing, Digital Safety Assurance

5. INTRODUCTION

Cybersecurity has emerged as a critical issue in a time when digital interactions and online activities predominate. Users are continuously exposed to possible hazards hiding in the form of malicious websites and URLs as they browse the wide expanse of the internet. Proactively addressing the issue, the AllScan project seeks to improve user security and safety when they browse the internet.

5.1 Context and Purpose

AllScan is designed to function as a Google Chrome plugin that blends in well with users' surfing routines. The project's basic design creates a dynamic and reliable system by combining a Python Flask backend with a JavaScript frontend. Together, these parts work to extract the material from the webpage that the user is now viewing and send it to the Python backend for additional processing.

5.2 Workflow

AllScan's primary use case is its capacity to locate and evaluate any security risks in the webpage content that is being viewed. Using front-end JavaScript, the project captures the essence of the user's browsing experience. The Python backend then takes over and begins carefully going through the material to look for embedded links. The domain and URL scanning API of the Kaspersky Threat Intelligence Portal is then used to examine these links.

5.3 Integration with Kaspersky Threat Intelligence Portal

The key component of AllScan's risk assessment process is the interaction with Kaspersky's Threat Intelligence Portal. Requests on the integrity and safety of the discovered links are sent by the backend to the portal. For AllScan to assess and categorize the links as safe or possibly hazardous, the API answers are a vital source of information.

5.4 User Notification

Providing consumers with up-to-date information about the security of the websites they visit is one of AllScan's main goals. To convey to the user, the findings of the backend study, the frontend is essential.

5.5 Objective and Impact

AllScan is essentially a proactive protection system against online dangers, aimed at strengthening users' digital perimeters. The initiative aims to increase user awareness of potential threats linked with visited links by utilizing Kaspersky's Threat Intelligence Portal's advanced capabilities. By doing this, AllScan promotes a safer and more secure online environment and adds to the larger field of online security.

We will examine the frontend and backend implementations in depth as we dig into the technical details of AllScan in the next sections of this study.

6. REALISTIC CONSTRAINS AND CONDITIONS

6.1 Sustainable Development Goal

Our initiative is a vital contribution to Sustainable Development Goal 10: Reducing Inequalities, and it is in the multidisciplinary realm of the internet. Even though it's a useful tool for connecting people and getting information, the internet has the potential to make social and economic inequality worse. By improving internet security, our initiative directly tackles this problem and makes sure that everyone, regardless of socioeconomic status, may take use of the advantages of online connectivity.

Creating a safe and welcoming online environment is essential to reducing inequality in the digital sphere. Cyber dangers and data breaches frequently disproportionately impact members of underprivileged or disadvantaged populations. We contribute to a more egalitarian digital landscape by creating cutting-edge solutions like AllScan, which offers a comprehensive defence against dangerous links and cyberattacks.

Our approach tackles the larger problem of digital exclusion in addition to reducing the immediate hazards brought on by cyberthreats. We can lessen disparities in the use of digital resources and promote a more just global society by making online places safer and easier to access.

6.2 Effects on Health, Environment, and the Problems of the Age Reflected in the Field of Engineering

The AllScan project, which sits at the nexus of lowering inequality and the internet, has a significant impact on safety, the environment, and public health from both a universal and social standpoint.

The internet has ingrained itself into daily life, bringing with it the possibility of cyberthreats that might seriously harm one's health. Malicious connections can put people's mental and financial security at risk by facilitating identity theft, financial fraud, and the spread of dangerous malware. By offering a strong defence against such attacks, AllScan directly targets these health hazards and promotes a safer online environment.

Environmental factors are also very important. We tangentially lessen the amount of electrical trash produced by hacked devices by thwarting cyber-attacks. Sustainable engineering techniques are aligned with AllScan's efficient scanning algorithms, which optimize energy usage.

The project also tackles modern technical problems, mostly related to cybersecurity. As technology advances, so are the strategies used by bad actors. AllScan reflects the dynamic problems engineers encounter in the quickly changing digital ecosystem by embodying flexibility and continual development.

Our approach tackles digital exclusion, a significant problem that fuels inequality, in the social sphere. Cyber-attacks can pose a greater risk to vulnerable groups. We contribute to a more equitable digital environment by offering a comprehensive and inclusive internet security solution, which promotes social inclusion and lessens inequalities in access to online resources.

6.3 Legal Consequences

Being an open-source project, the AllScan project stands out for its dedication to openness and user-centric values. The project is based on an open and honest philosophy and adheres to a highly transparent working style that puts the delivery of consistent results from Kaspersky's service—a widely acknowledged leader in security and dependability across a range of domains—first. Building user trust and maintaining ethical procedures in the field of cybersecurity depend heavily on this all-encompassing transparency-oriented strategy.

AllScan's steadfast dedication to user privacy is fundamental to how it operates. The architecture of the project makes sure that user data is never saved in any databases or altered in any way while interacting with the Flask backend written in Python. Users' data is only extracted with the specific intention of maximizing outcomes, adhering to the data minimization principle. This shows a diligent attempt to respect and preserve user privacy because just the information required to get a better optimal result is extracted.

7. ANALYZING LITERATURE

The dynamic field of internet security is always changing due to ongoing technical developments that try to reduce cyberthreats and improve user safety. We explore the cutting edge of internet security in this investigation, concentrating on our project, AllScan technology. This thorough analysis looks at current research, methods used, and related applications in order to give a thorough understanding of the most recent advancements and difficulties in the subject.

The swift advancement of technology has made it imperative to take a proactive stance in comprehending the modern complexities of internet security. Threats change, and so should our understanding of the subject, with a special focus on utilizing cutting-edge technology. In this regard, our examination of the situation of internet security today is accompanied by a special focus on the advancements and contributions made by AllScan.

We also investigate similar applications in the domain. By comparing similar technology, we may learn more about the various strategies used by other projects.

This literature review is essentially an academic investigation into the complex field of internet security, offering a thorough look at the most recent developments, research approaches, and related applications.

7.1 An Overview of Online Security

*With the exponentially increase in usage of cyberspace, cybercriminal actives are also increase exponentially. The basic reasons are that with the inception of world wide web, the web applications were also getting popularity for data storing and data sharing, irrespective of the user. With the passage of time web applications were getting more complex with rapid increase in their design faults, creating the surfing of internet totally unsafe. More than 90 percent web applications have some kind of design or development fault which can be easily exploited by the cyber criminals. These faults in web application can help criminals in getting the illegal access to trade secrets of any business. Sometime the web application may not be posing threat, but the technology used in these applications become the root cause and put the application to the risk of illegal access. Presently the social networks, Internet connected mobile devices,

individual privacy, and the online connectivity of entities such as banks are the most enticing targets for cyber criminals.

******In last twenty years, use of internet applications, web hacking activities have exaggerated speedily. Organizations facing very significant challenges in securing their web applications from rising cyber threats, as compromise with the protection issues don't seem to be reasonable. Vulnerability Assessment and Penetration Testing (VAPT) techniques help them to go looking out security loopholes. These security loopholes could also be utilized by attackers to launch attacks on technical assets. Thus, it is necessary ascertain these vulnerabilities and install security patches.

7.2 State-of-the-Art in Internet Security

7.2.1 Artificial Intelligence and Machine Learning

- Artificial Intelligence (AI) and Machine Learning (ML) stand out in cybersecurity for their ability to rapidly analyse and identify threats.
- AI and ML can be utilized for anomaly detection, identifying deviations from the norm, and thus pre-emptively detecting potential threats.
- Learning algorithms are employed to comprehend the evolution of threats over time and develop more effective defence strategies.

7.2.2 Zero Trust Security Model

- Zero Trust offers a beyond-the-traditional approach, assuming that every user, device, and network segment is untrustworthy.
- Users and devices are continually monitored through authentication, authorization, and access controls, ensuring that security policies are never relaxed at any stage.

7.2.3 End-to-End Encryption

- End-to-end encryption ensures complete security during the transmission and storage of data.
- This not only provides resistance against malicious interventions but also minimizes information leakage in the event of data breaches.

7.2.4 Biometric Security

- Biometric security measures such as fingerprint, facial recognition, and retina scanners offer a more secure and user-friendly means of authentication compared to traditional password-based systems.
- However, caution must be exercised regarding the security and privacy of biometric data.

7.2.5 Blockchain Technology

- Blockchain, with its distributed ledger technology, securely and transparently stores data in an immutable manner.
- Blockchain-based solutions are being developed to enhance the security of encryption keys and provide reliable identity verification.

7.2.6 Advanced Threat Monitoring and Analysis

- Advanced threat monitoring and analysis tools are continually updated to combat the rapidly evolving nature of cyber-attacks.
- Security experts analyse threat intelligence to anticipate future attacks.

7.2.7 IoT Security

- Specialized security solutions for Internet of Things (IoT) devices are being developed, focusing on securing inter-device communication and addressing vulnerabilities.
- Up-to-date software and hardware security are crucial for enhancing the overall security of IoT devices.

7.2.8 Social Engineering and Awareness

- Security awareness training and campaigns are becoming widespread to educate users about social engineering tactics.
- Informed users can better recognize and take countermeasures against fraudulent attempts.

7.3 Comparable Technologies and Applications

The AllScan project has aims in common with several Internet security apps and technologies. Notable among these is VirusTotal, an online tool that uses many antivirus engines to scan files and URLs for possible dangers (VirusTotal, 2022). The goals of the AllScan project are in line with several current Internet security tools and applications, the most notable of which being VirusTotal. As of 2022, VirusTotal is an internet application that uses a variety of antivirus engines to thoroughly scan files and URLs to provide a thorough evaluation of potential risks (VirusTotal, 2022). By utilizing a variety of engines, this cooperative method to threat detection improves the effectiveness of antivirus software and guarantees a more complete and sophisticated examination of possible threats in digital material.

Comparable to AllScan, PhishTank is an endeavour that stands out for being a cooperative community approach that actively monitors and detects bogus websites. AllScan and PhishTank have the common objective of reducing the dangers associated with malicious connections, which emphasizes the value of teamwork in the field of cybersecurity. PhishTank is a prime example of a community-driven strategy that is dedicated to protecting consumers from the ubiquitous risks that come with dishonest online behaviour. In addition to enhancing our common knowledge of new risks, this coordinated vigilance helps build a strong defence against harmful activity in the digital sphere.

AllScan's similarities to VirusTotal and PhishTank essentially highlight the value of teamwork approaches in the creation and use of successful cybersecurity solutions. The mutual dedication to utilizing a range of resources and community-driven projects is indicative of a wider trend in the cybersecurity space, highlighting the necessity of all-encompassing and collaborative methods to tackle the ever-changing obstacles of the digital age.

7.4 AllScan Technology

With the AllScan project, every link on a webpage is automatically found and examined in real time, presenting a approach to internet security. AllScan functions in the background without interruption, in contrast to conventional antivirus programs, enabling users to make well-informed choices regarding their online activity.

7.5 Final Thoughts

As a result of the literature study, the field of internet security is dynamic and changing quickly. Within this framework, the AllScan project presents itself as a response to the current problems related to cyberattacks. Using current research findings and an awareness of comparable application capabilities, AllScan hopes to make a substantial contribution to the continuous endeavours to establish a safe and welcoming digital environment.

7.6 References

- *Abdul Razzaq, Ali Hur, H. Farooq Ahmad, Muddassar Masood, "2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)", March 2013
- **Prashant S. Shinde, Shrikant B. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing", February 2016
- VirusTotal. (2022). About. <https://www.virustotal.com/gui/about-us>
- PhisTank. What is FishTank? <https://phishtank.org/faq.php>

8. STANDARTS

The project includes a JavaScript-based frontend and a Python Flask-based backend. Here are the details about the standards to be used in the project:

8.1 JavaScript Frontend Standards

- **ES6+ Usage:** JavaScript code follows ECMAScript 6 and above standards. This ensures the use of modern JavaScript features.
- **Asynchronous Programming:** Data communication and API requests are performed asynchronously.
- **Development Tool Support:** Browser development tools, such as Chrome Developer Tools, are used for debugging code and performance optimisation.
- **UI/UX Standards:** The user interface and user experience conform to standards that will ensure that the browser plugin is common and understandable among users.

8.2 Python Flask Backend Standards

- **PEP 8 Compliance:** Python code conforms to PEP 8 standards. This ensures readability and consistency.

8.3 Data Transfer and Security Controls

- **Secure Data Transfer:** Page content collected with JavaScript is securely transmitted to the Python backend.
- **Malicious Link Scanning:** The Python backend identifies malicious links by scanning the links in the page content using APIs provided by Kaspersky's Threat Intelligence Portal.
- **User Notifications:** The frontend notifies the user of security assessments from the Python backend in a clear and understandable way.

8.4 Code Security and Performance

- **Performance Optimisation:** Both frontend and backend include regular evaluations for performance optimisations.
- **Error Tracking and Logging:** The application uses appropriate methods to track and log errors.

These standards will provide a basic framework to ensure that the AllScan project operates in a secure, consistent, and effective manner.

9. APPROACHES, TECHNIQUES, AND TECHNOLOGIES

9.1 APPROACHES

9.1.1 Data Transfer and Analysis Methods:

- Using RESTful API for data communication between JavaScript Frontend and Python Flask Backend.
- Transferring and analysing the page content to Python backend.

9.1.2 Malicious Link Detection Method

9.1.2.1 Using Kaspersky's "Threat Intelligence Portal" API

- Domain and URL scanning API is used to analyse the links in the page content.
- By scanning the HTML link tags, the links shown through these tags are examined.
- This scanning process is matched with the security information in the database provided by the Kaspersky API.

9.1.2.2 Using Kaspersky API with Asynchronous Thread Technology

- Asynchronous thread technology is used by the Kaspersky API for scanning links in page content.
- This technology allows requests to be made synchronously, resulting in fast responses.
- The Kaspersky API uses asynchronous thread technology to quickly test links in page content and perform security analysis.

It enables the links in the page content to be tested and security analysis to be performed faster through Kaspersky's API. These methods help to detect potentially malicious links more effectively on the pages users browse.

9.2 TECHNIQUES

9.2.1 JavaScript Frontend

Retrieval of page content and transmission to the server with JavaScript running on the browser:

- JavaScript, as a language running in the browser, retrieves content from the web pages that the user navigates through the DOM (Document Object Model) structure.
- This content is transferred to the Python Flask backend to be transmitted to the server by triggering certain events with the user's interactions (for example, page load, button click, etc.). This is done with AJAX (Asynchronous JavaScript and XML) techniques.

Initiating requests by listening to user interactions:

- JavaScript listens to user interactions on the page (mouse clicks, form submissions, page load events, etc.) and triggers requests based on these interactions.
- For example, when the user clicks on a specific link or performs a specific action, JavaScript detects this event and prepares the data to make the corresponding request to the backend.

9.2.2 Python Flask Backend

Analysing incoming page content and parsing links:

- The Flask backend receives the page content transmitted by JavaScript and processes it to analyse it.
- In this stage, the page content is parse, the necessary data operations are performed, and the links in it are parsed and made processable.

Making requests to Kaspersky's API and processing the received responses to perform security assessment:

- Python Flask makes requests to Kaspersky's API to test specified connections.
- Incoming responses are in JSON format and received by the Flask backend.
- The received responses are analysed, the security status of the connections is determined, and this information is passed to the JavaScript side. The results of this analysis are displayed in the user's browser and information about the security status is provided.

These steps ensure communication by listening to user interactions and retrieving page content on the JavaScript side, while the Python Flask side analyses the data it receives, makes a request to the Kaspersky API and performs security assessment by processing the incoming responses. In this way, security analysis is presented to the user by providing data flow between frontend and backend.

9.3 TECHNOLOGIES

9.3.1 JavaScript

JavaScript is a scripting language that plays a fundamental role in the development of browser-based applications.

- **It is used for browser-based data collection and communication:** Because JavaScript runs in the browser, it is used to collect data from the web pages that users browse and communicate that data to the Python Flask backend. This is done via a Chrome plugin running in the user's browser.
- **It is used for tracking user interactions and triggering requests:** JavaScript listens to user interactions and reacts to actions taken by the user (e.g., page visit, link click, etc.) to generate the necessary requests and communicate with the backend.

9.3.2 Python Flask

Python Flask is a lightweight web framework that runs on the server side.

- **A server-side Python framework:** Flask runs on the server side and processes and analyses incoming data and performs the operations required to make requests to the Kaspersky Threat Intelligence Portal.
- **Processing and analysing page content:** Flask receives the page content delivered by JavaScript, analyses it and extracts links from it.
- **It is used to make requests to the Kaspersky API:** Flask is used to make requests to the API provided by Kaspersky and transmit data required for security analysis.

9.3.3 Kaspersky Threat Intelligence Portal

Kaspersky Threat Intelligence Portal is a service for the detection and analysis of malicious connections.

- **Service for malicious link scanning:** This portal analyses links in page content and assesses their security status through the API it provides.
- **It is used for security analysis of links in page content:** Kaspersky Threat Intelligence Portal scans incoming links and determines their security status.

9.3.4 RESTful API

The RESTful API is used for data communication between JavaScript and Python.

- **It is used for data communication between JavaScript and Python:** JavaScript receives data from the browser and transmits this data to the Python Flask backend via the RESTful API, enabling data sharing.
- **It serves as the basic communication protocol for transferring and analysing page content:** The RESTful API transmits the page content collected by JavaScript to the Python Flask backend, enabling the data transfer necessary for analysis.

These technologies are integrated to evaluate the security of the pages the user navigates by enabling communication, data transfer and processing between the different components within the project.

10. RISK MANAGEMENT

WP No	Risks	Risk Management (Plan B)
1	Lack of Developer Accessible	Ensure that team members are cross utilised to ensure that they understand each other's work and can back each other up. This ensures that in the unlikely event that one developer is absent, another can complete important work.
2	Unbalanced Workload	Routine observation of the allocation of tasks. If an imbalance is found, the duties should be readjusted to lighten the load.
3	Reliance On Own Abilities	Coordinating collaborative workshops to exchange information and skills and to increase sharing to lessen reliance on specialized knowledge.
4	API Usage Limitations	Review API usage policies and use the API in accordance with these policies. Regularly check API limitations.
5	API Accessibility	Use backup API, regularly check API accessibility.
6	Performance	Manage requests asynchronously

Table 1- Risk Management

11. PROJECT SCHEDULE AND TASK SHARING

WP No	Work Package Name	Assigned Project Staff	Time Period (... - ... Week)	Success Criteria
1	Research and Data Collection About the Project	Ergül Ferik Ceyhun Binal	1 st Week	Success
2	Analysis and Planning	Ergül Ferik Ceyhun Binal	2 nd Week	Success
3	Find Links Embedded in a Web Page	Ergül Ferik Ceyhun Binal	3 rd Week	Success
4	Available API Binding and a Link Query	Ergül Ferik Ceyhun Binal	4 th Week	Success
5	List the Statistics of a Link in the Console	Ergül Ferik Ceyhun Binal	5 th Week	Success
6	Test All Links and List Statistics	Ergül Ferik Ceyhun Binal	6 th Week	Success
7	Interface Preparation and Making Google Chrome Extension	Ergül Ferik Ceyhun Binal	7 th Week	Success
8	End Tests and Presentation	Ergül Ferik Ceyhun Binal	8 th Week	Success

Table 2- Project Schedule and Task Sharing

12. SYSTEM REQUIREMENTS ANALYSIS

12.1 Use Case Model

The goal is to ensure a safe browsing experience by detecting dangerous links, confirming the security of the webpages the user visits, and alerting the user when something is wrong.

Priority: High

Actors:

- **User:** An individual utilizing a web browser with the AllScan extension to browse the internet.

Required conditions:

- The AllScan extension for the Google Chrome browser has been installed and enabled by the user.
- The content of the webpage the user visited can now be received and analyzed by the backend.
- The access keys for the Kaspersky Threat Intelligence Portal API are set up correctly and are available.

Basic Flow:

- The user visits a web page using the AllScan extension in Google Chrome browser.
- The extension uses JavaScript to send a request to the backend to transmit the content of the visited page.
- The Python Flask backend analyses the received page content and identifies all the links within it.
- Identified links are sent to the Kaspersky Threat Intelligence Portal API for querying.
- The API examines the incoming links to detect malicious ones.
- The backend performs an analysis based on the responses received from the API regarding the security status of the page.
- The user interface informs the user about the security status of the scanned page based on information received from the backend.

- If malicious links are found, the user is provided with warnings and necessary actions to take.
- The user experiences a secure browsing session by avoiding unsafe links.

Alternative Flow:

- If there is an issue accessing the Kaspersky Threat Intelligence Portal API, the backend cannot send requests to the API, and a security analysis cannot be provided to the user. In this case, the user can be notified about the problem regarding API access.

Outcome:

- Through the AllScan extension, users can verify the security of the web pages they visit and safeguard themselves from malicious links, thus ensuring a safer internet experience. This promotes informed and secure internet usage while taking preventive measures against harmful content.

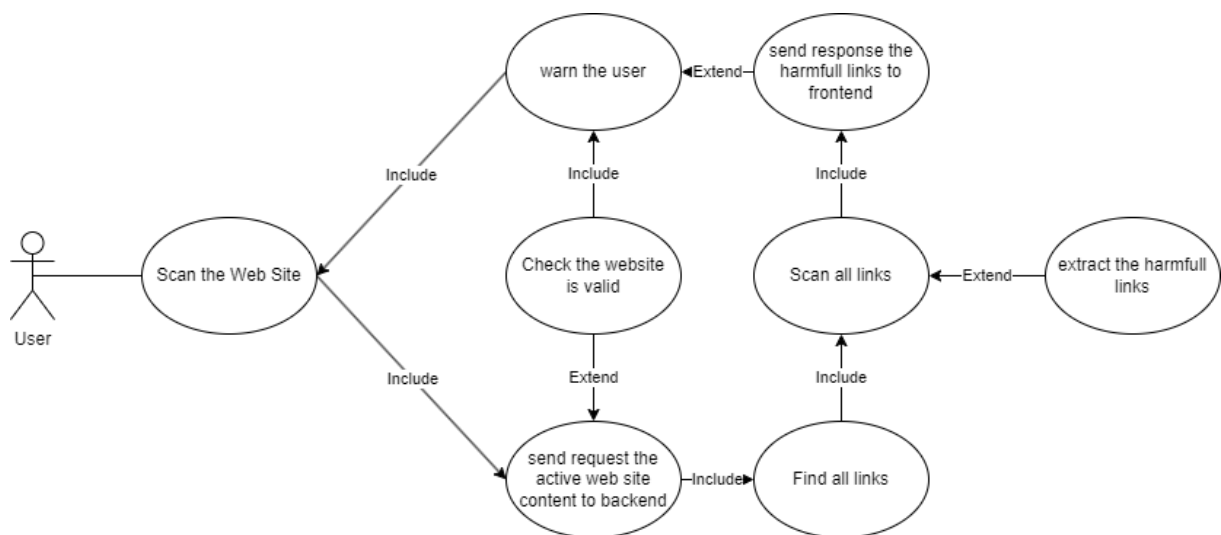


Figure 1- Use Case Diagram

12.2 Object Model

Page	Controller	UrlScanner
<ul style="list-style-type: none"> - LINK: String - MAINPAGE: String - response: Object - soup: Object - PROTOCOL: String - Connections: String[] - Domains: String[] 	<ul style="list-style-type: none"> - harmfulLinks: String[] 	<ul style="list-style-type: none"> - url : String - KASPERSKYURL: String - HarmfullLinks: String[]
<ul style="list-style-type: none"> -isLink(String): Boolean -urlFormatter(String): String -getDomainFromUrl(String): String +setConnections(): Void +getConnections(): String[] +getDomains(): String[] +getLink(): String[] +getProtocol(): String[] 	<ul style="list-style-type: none"> -warnUser(): Void -runMainRoitine(): void -setHarmFullLinks() : Void 	<ul style="list-style-type: none"> +getUrl(): String +setUrl(String):Void +scanByKaspersky():Void +getHarmfullLinks(): String[]

Figure 2- Object Model

13. SYSTEM DESIGN

13.1 System Architectural Diagram

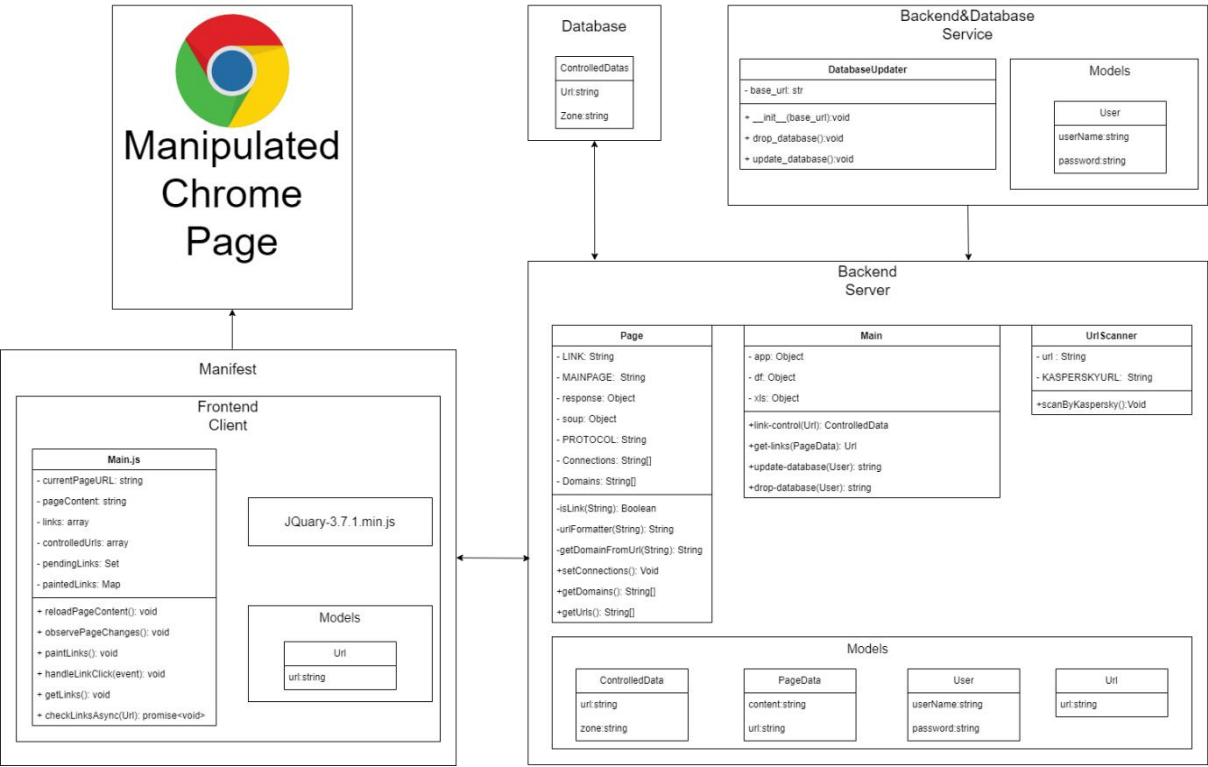


Figure 3- System Architectural Diagram

13.1.1 Sequence Diagram

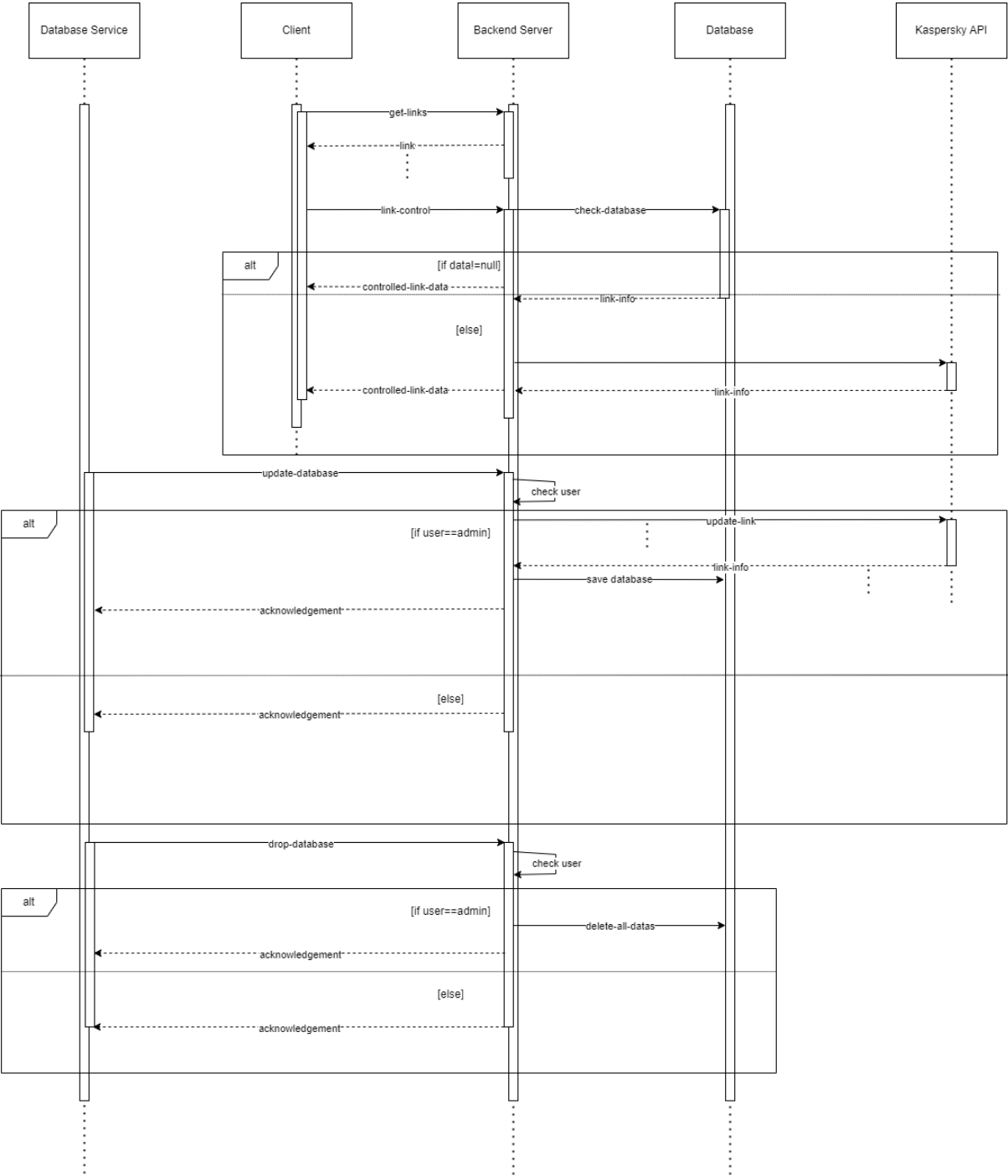


Figure 4- Sequence Diagram

Participants:

The client, which could be a person or another system interacting with the backend server, is one of the participants in this system. As the main system, the backend server handles queries, communicates with the database, and makes use of the Kaspersky API. User data and link data are stored in the database, and link data may be easily scanned for viruses using the Kaspersky API.

Messages:

Several messages are exchanged during communication between the client and the backend server:

- 'get-links': Requested a list of links from the backend server by the client.
- "link-control": A request made to the Kaspersky API by the backend server to scan a particular link for possible malware.
- "check-database": This command is sent by the backend server to confirm that link data is present.
- [if data == null]: If there are no data in the database, the following actions are taken:
 - "Controlled link-data" refers to link data that is obtained from the client by the backend server.
 - "update-database": The database is used to store the link data that has been retrieved.
- [else]: If there is data in the database, the steps are as follows:
 - "check user": The backend server verifies the user's access level.
 - [if user==admin]: The following steps take place if the user is an administrator:
 - "update-link": The addition of fresh client-provided data to the already-existing link data.
 - "save database": Keeps updated link data in the database intact.
 - "acknowledgement": The backend server sends the client an acknowledgment message.
- [else]: If you do not have administrator access, the following actions need to be taken:
 - "Acknowledgment": The backend server sending the client a

"Acknowledgement" message, which could indicate a suspect link.

- "drop-database": Removes any links that are currently in the database.
- [if used]: Depending on the user's access level, the following steps are taken if the link has been used:
 - "check user": The backend server reassesses the user's level of access.
 - [if user==admin]: If the user has administrator privileges, the following actions include:
 - "delete-all-data": The database's link data is completely removed.
 - "acknowledgement": The backend server sends the client an acknowledgment message.
 - [else]: The steps are as follows if the user does not have administrator privileges:
 - "Acknowledgement": When the backend server sends a "Acknowledgement" message to the client, it may signal a link risk.
- "link-info": The backend server sends the link data and any information it has obtained from the Kaspersky API back to the client.

Conditions and Loops:

Conditional branching is used in the diagram to handle different circumstances according to the user's access level and whether link data is present in the database.

Alternative Flows:

Depending on the administrator position of the user, two different flows are visible. Moreover, there are more branching in the "check user" phase depending on whether the link has been used.

Key Interactions:

The exchange of link data between the client and the backend server is the main point of interaction. In order to save and retrieve link data, the backend server also communicates with the database. Links are scanned using the Kaspersky API for possible malware.

13.1.2 State Diagram

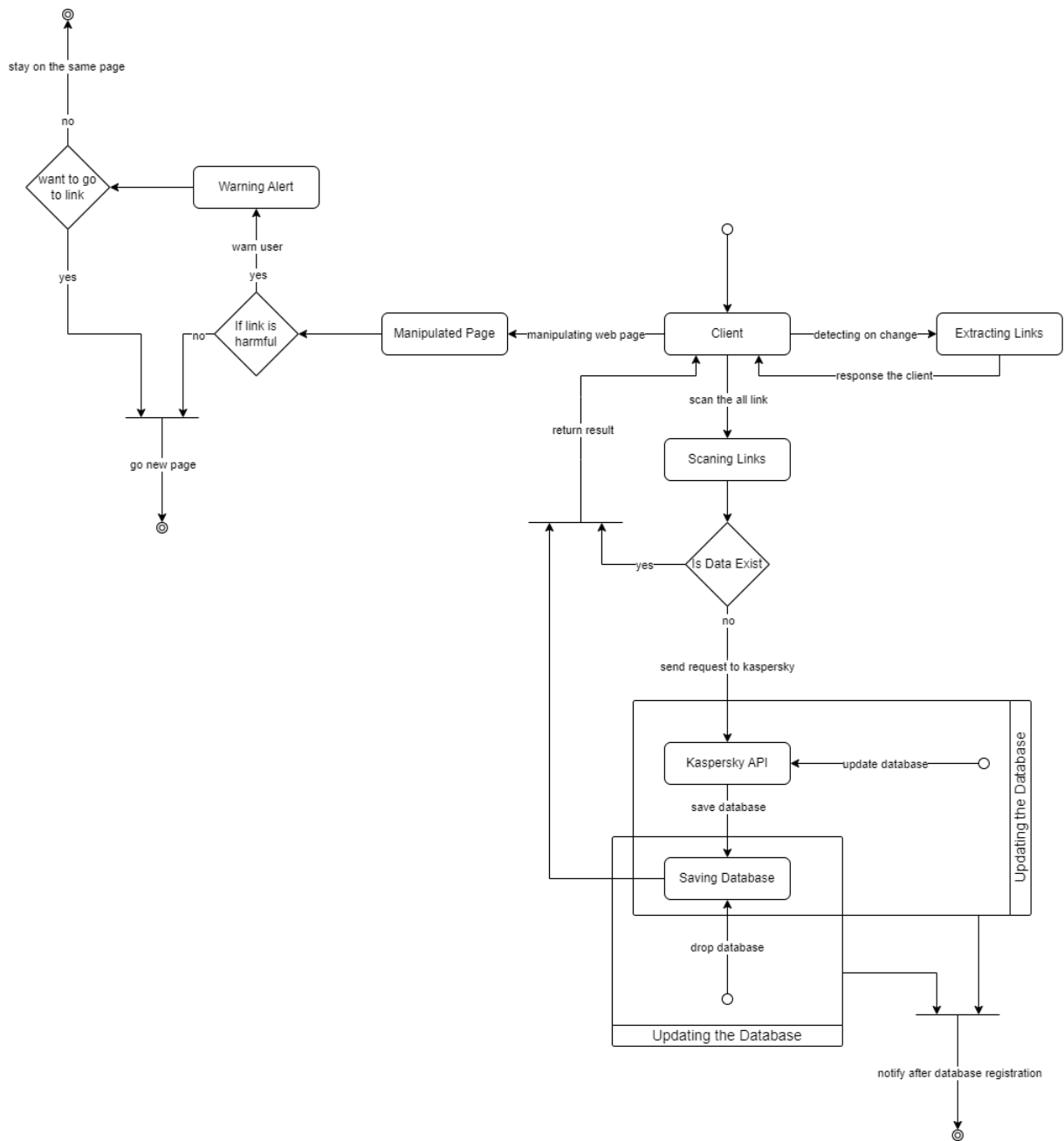


Figure 5- State Diagram

Start Events:

- **Idle:** The system is waiting for the user to perform a search.
- **Update Database:** An event that occurs when a request is received to update the database.
- **Drop Database:** An event that occurs when a request is received to delete the database.

End Events:

- **Go New Page:** An event that occurs when the user navigates to a new page.
- **Stay On Same Page:** An event that occurs when the user remains on the same page.
- **Notify After Database Registration:** An event that occurs to notify the user of the results of database operations.

States:

- **Client:** The system is in an idle state.
- **Extracting Links:** The stage of extracting links.
- **Scanning Links:** The state of scanning links.
- **Kaspersky API:** The state of querying using Kaspersky.
- **Saving Database:** The state of saving database operations.
- **Manipulated Page:** The state of manipulating the page the user is on.
- **Warning Alert:** The state of the user encountering a warning.

Conditions:

- **Is Data Exist:** The condition that the data already exists in the database.
- **If Link is Harmful:** The condition that the page the user wants to go to is harmful.
- **Want to Go to Link:** The condition that the user wants to go to a harmful page.

Events:

- **detecting on change:** When a change is detected in the **Client (Idle)** state, it sends it to the **Extracting Links** state.
- **response the client:** When the data is ready in the **Extracting Links** stage, it redirects to the **Client(Idle)** state.
- **scan the all links:** It allows it to be redirected from the **Client(Idle)** state to the **Scanning Links** state for scanning the data.
- **send requests to kaspersky:** It redirects from the **Scanning Links** state to the **Kaspersky API** state for scanning the data.
- **save database:** It redirects to the **Saving Database** state to save the data coming from the **Kaspersky API** state.
- **return result:** It redirects to the **Client(Idle)** state to return the results.
- **manipulating web page:** It redirects to the **Manipulated Page** state to process the manipulated data from the **Client(Idle)** state.
- **warn user:** It redirects to the **Warning Alert** state to warn the user.

14. SYSTEM TEST DESIGN

Req No	Req Desc	Testcase ID	Status
1	Reset Database	TC01, TC02, TC03, TC04	TC01 - Pass TC02 - Pass TC03 - Pass TC04 - Pass
2	Update Database	TC01, TC02, TC03, TC05	TC01 - Pass TC02 - Pass TC03 - Pass TC05 - Pass
3	Notifying the user of the security status of connections	TC06, TC07, TC08, TC09, TC10	TC06 - Pass TC07 - Pass TC08 - Pass TC09 - Pass TC10 - Pass
4	Warning of harmful connection inputs	TC11, TC12, TC13	TC11 - Pass TC12 - Pass TC13 - Pass
5	Page scans should be fast in performance	TC14, TC15, TC16	TC14 - Pass TC15 - Fail TC16 - Pass

Table 3- Requirement Traceability Matrix

14.1 REQ 01: Reset Database

Req ID	Req Description	Test Case ID	Test Case Description	Test Steps	Test Data	Expected Results	Pass/Fail
REQ 01	Reset Database	TC01	Invalid Operation selection	1.Select an invalid operation	userName:admin password:admin	The operation is invalid and a new operation selection menu appears	Pass
		TC02	Incorrect username input	1.Select operation		Asking for a password after entering the username.	Pass
				2. Enter the wrong username			
		TC03	Incorrect password input	1.Select operation		Indicates that the information entered is incorrect, and a new operation selection menu appears	Pass
				2. Enter the correct username			
				3. Enter wrong password			
		TC04	Correct operation selection, valid username and password input	1.Select deletion		Notification that "reset database" operation was successful	Pass
				2. Enter the correct username			
				3. Enter correct password			

Table 4- REQ-01 Detailed Traceability Matrix

14.1.1 TC01: Invalid Operation Selection

Description: The test checks for the system's response when an invalid operation is selected.

Test Steps: Select an invalid operation.

Test Data: "userName:admin, password:admin".

Expected Results: The operation is invalid, and a new operation selection menu appears.

Pass/Fail: Pass

Test Case ID	TC01	Test Case Description	Invalid Operation selection		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend&database service
2	Starting the backend server
3	
4	

S #	Test Data
1	userName = admin
2	password = admin
3	
4	

Test Scenario	The user who is authorized to access the service select invalid operation
---------------	---

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Select invalid operation which is not in list	The operation is invalid and a new operation selection menu appears	As Expected	Pass

Table 5- Test Case 01

14.1.2 TC02: Incorrect Username Input

Description: This test verifies the system's behavior when an incorrect username is entered.

Test Steps: Select an operation, enter the wrong username.

Expected Results: The system prompts for a password after entering the username.

Pass/Fail: Pass

Test Case ID	TC02	Test Case Description	Invalid username input		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend&database service
2	Starting the backend server
3	
4	

S #	Test Data
1	userName = admin
2	password = admin
3	
4	

Test Scenario	The user who is authorized to access the service input invalid username
---------------	---

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Select operation (Delete or Update)	User prompt when delete or update is selected as one of the two options given on the Consol screen	As Expected	Pass
2	Invalid username input	Asking for a password after entering the username.	As Expected	Pass

Table 6- Test Case 02

14.1.3 TC03: Incorrect Password Input

Description: This test ensures the system handles incorrect password input appropriately.

Test Steps: Select an operation, enter the correct username, enter the wrong password.

Expected Results: The system indicates that the entered information is incorrect, and a new operation selection menu appears.

Pass/Fail: Pass

Test Case ID	TC03	Test Case Description	Invalid password input		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend&database service
2	Starting the backend server
3	
4	

S #	Test Data
1	userName = admin
2	password = admin
3	
4	

Test Scenario	The user who is authorized to access the service input invalid password
---------------	---

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Select operation (delete or Update)	User prompt when delete or update is selected as one of the two options given on the Consol screen	As Expected	Pass
2	Valid username input	Asking for a password after entering the username.	As Expected	Pass
3	Invalid password input	Indicates that the information entered is incorrect, and a new operation selection menu appears	As Expected	Pass

Table 7- Test Case 03

14.1.4 TC04: Correct Operation Selection, Valid Username, and Password Input

Description: Verify the system's response when a correct operation, valid username, and password are provided.

Test Steps: Select deletion, enter the correct username, enter correct password.

Expected Results: Notification that the "reset database" operation was successful.

Pass/Fail: Pass

Test Case ID	TC04	Test Case Description	Correct operation selection, valid username and password input		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend&database service
2	Starting the backend server
3	
4	

S #	Test Data
1	userName = admin
2	password = admin
3	
4	

Test Scenario	The user who is authorized to access the service should be able to reset the database with username and password information.
---------------	---

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Select operation (Delete)	User prompt when deletion is selected as one of the two options given on the Consol screen	As Expected	Pass
2	Valid username input	Asking for a password after entering the username.	As Expected	Pass
3	Valid password input	Performing the deletion process after entering the password and giving an information message that it is finished	As Expected	Pass

Table 8- Test Case 04

14.2 REQ 02: Update Database

Req ID	Req Description	Test Case ID	Test Case Description	Test Steps	Test Data	Expected Results	Pass/Fail
REQ 02	Update database	TC01	Invalid Operation selection	1.Select an invalid operation	userName:admin password:admin	The operation is invalid and a new operation selection menu appears	Pass
		TC02	Incorrect username input	1.Select operation		Proceeding to the password phase	Pass
				2. Enter the wrong username			
		TC03	Incorrect password input	1.Select operation		Indicates that the information entered is incorrect, and a new operation selection menu appears	Pass
				2. Enter the correct username			
				3. Enter wrong password			
		TC05	Correct operation selection, valid username and password input	1.Select deletion		Notification that "update database" operation was successful	Pass
				2. Enter the correct username			
				3. Enter correct password			

Table 9 - REQ-02 Detailed Traceability Matrix

14.2.1 TC01: Invalid Operation Selection

Description: Similar to REQ 01, this test checks the response to an invalid operation selection.

Test Steps: Select an invalid operation.

Test Data: "userName:admin, password:admin".

Expected Results: The operation is invalid, and a new operation selection menu appears.

Pass/Fail: Pass

Test Case ID	TC01	Test Case Description	Invalid Operation selection		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend&database service
2	Starting the backend server
3	
4	

S #	Test Data
1	userName = admin
2	password = admin
3	
4	

Test Scenario	The user who is authorized to access the service select invalid operation
---------------	---

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Select invalid operation which is not in list	The operation is invalid and a new operation selection menu appears	As Expected	Pass

Table 10 - Test Case 01

14.2.2 TC02: Incorrect Username Input

Description: Similar to REQ 01, this test verifies the system's response to an incorrect username.

Test Steps: Select an operation, enter the wrong username.

Expected Results: Proceeding to the password phase.

Pass/Fail: Pass

Test Case ID	TC02	Test Case Description	Invalid username input		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend&database service
2	Starting the backend server
3	
4	

S #	Test Data
1	userName = admin
2	password = admin
3	
4	

Test Scenario	The user who is authorized to access the service input invalid username
---------------	---

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Select operation (Delete or Update)	User prompt when delete or update is selected as one of the two options given on the Consol screen	As Expected	Pass
2	Invalid username input	Asking for a password after entering the username.	As Expected	Pass

Table 11 - Test Case 02

14.2.3 TC03: Incorrect Password Input

Description: Similar to REQ 01, this test checks the system's handling of incorrect password input.

Test Steps: Select an operation, enter the correct username, enter the wrong password.

Expected Results: The system indicates that the entered information is incorrect, and a new operation selection menu appears.

Pass/Fail: Pass

Test Case ID	TC03	Test Case Description	Invalid password input		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend&database service
2	Starting the backend server
3	
4	

S #	Test Data
1	userName = admin
2	password = admin
3	
4	

Test Scenario	The user who is authorized to access the service input invalid password
---------------	---

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Select operation (delete or Update)	User prompt when delete or update is selected as one of the two options given on the Consol screen	As Expected	Pass
2	Valid username input	Asking for a password after entering the username.	As Expected	Pass
3	Invalid password input	Indicates that the information entered is incorrect, and a new operation selection menu appears	As Expected	Pass

Table 12 - Test Case 03

14.2.4 TC05: Correct Operation Selection, Valid Username, and Password Input

Description: Similar to REQ 01, this test verifies the system's response to correct operation, valid username, and password input.

Test Steps: Select deletion, enter the correct username, enter correct password.

Expected Results: Notification that the "update database" operation was successful.

Pass/Fail: Pass

Test Case ID	TC05	Test Case Description	Correct operation selection, valid username and password input		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend&database service
2	Starting the backend server
3	
4	



S #	Test Data
1	userName = admin
2	password = admin
3	
4	

Test Scenario	The user who is authorized to access the service should be able to update the database with username and password information.
---------------	--

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Select operation (Update)	User prompt when update is selected as one of the two options given on the Consol screen	As Expected	Pass
2	Valid username input	Asking for a password after entering the username.	As Expected	Pass
3	Valid password input	Performing the updating process after entering the password and giving an information message that it is finished	As Expected	Pass

Table 13 - Test Case 05

14.3 REQ 03: Notifying the User of Security Status of Connections

Req ID	Req Description	Test Case ID	Test Case Description	Test Steps	Test Data	Expected Results	Pass/Fail
REQ 03	Notifying the user of the security status of connections	TC06	Presence on a page containing a link with the Green field	Find on the page containing a link that has the Green field	www.google.com	Providing page security information to the user 	Pass
		TC07	Presence on a page containing a link with the Red field	Find on the page containing a link that has the Red field	www.codexpgames.com	Providing page security information to the user 	Pass
		TC08	Presence on a page containing a link with the Yellow field	Find on the page containing a link that has the Yellow field	www.gamestatus.info	Providing page security information to the user 	Pass
		TC09	Presence on a page containing a link with the Grey field	Find on the page containing a link that has the Grey field	www.crack-list.co.uk	Providing page security information to the user 	Pass


		TC10	Presence on a page containing a link with the Orange field	Find on the page containing a link that has the Orange field	www.agbedagbi nglobalworld.co m	Providing page security information to the user 	Pass
--	--	------	--	--	---------------------------------------	--	------

Table 14 - REQ-03 Detailed Traceability Matrix

14.3.1 TC06-TC10: Presence on a Page Containing Links with Different Security Fields

Description: These tests check the system's ability to identify and notify the user of the security status of links on a page.

Test Steps: Find a link with the specified security field on the page.

Expected Results: Providing page security information to the user.

Pass/Fail: All Pass

Test Case ID	TC06	Test Case Description	Presence on a page containing a link with the Green field		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	www.google.com
2	
3	
4	

Test Scenario	Notifying the user of the security status of connections
---------------	--


Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Find on the page containing a link that has the Green field	Providing page security information to the user with green icon. 	As Expected	Pass

Table 15 - Test Case 06

Test Case ID	TC07	Test Case Description	Presence on a page containing a link with the Red field		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
------------------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
----------------------	--------------	--------------------	-----------------	---	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	www.codexpcgames.com
2	
3	
4	

Test Scenario	Notifying the user of the security status of connections
----------------------	--


Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Find on the page containing a link that has the Red field	Providing page security information to the user with red icon. 	As Expected	Pass

Table 16 - Test Case 07

Test Case ID	TC08	Test Case Description	Presence on a page containing a link with the Yellow field		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
------------------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
----------------------	--------------	--------------------	-----------------	---	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	www.gamestatus.info
2	
3	
4	

Test Scenario	Notifying the user of the security status of connections
----------------------	--


Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Find on the page containing a link that has the Yellow field	Providing page security information to user with yellow icon. 	As Expected	Pass

Table 17 - Test Case 08

Test Case ID	TC09	Test Case Description	Presence on a page containing a link with the Grey field		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
------------------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
----------------------	--------------	--------------------	-----------------	---	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	www.crack-list.co.uk
2	
3	
4	

Test Scenario	Notifying the user of the security status of connections
----------------------	--

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Find on the page containing a link that has the Grey field	Providing page security information to user with grey icon. ?	As Expected	Pass

Table 18 - Test Case 09

Test Case ID	TC10	Test Case Description	Presence on a page containing a link with the Orange field		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
------------------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
----------------------	--------------	--------------------	-----------------	---	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	www.agbedagbinglobalworld.com
2	
3	
4	

Test Scenario	Notifying the user of the security status of connections
----------------------	--


Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Find on the page containing a link that has the Orange field	Providing page security information to user with orange icon. 	As Expected	Pass

Table 19 - Test Case 10

14.4 REQ 04: Warning of Harmful Connection Inputs

Req ID	Req Description	Test Case ID	Test Case Description	Test Steps	Test Data	Expected Results	Pass/Fail
REQ 04	Warning of harmful connection inputs	TC11	When a user clicks on a malicious link, they should be warned before being redirected to the link	A page with a harmful link is displayed	codexpcgames.com	The user should receive a warning message	Pass
				The harmful link is clicked			
		TC12	If the user still wants to go to the link as a result of the warning, they should be redirected	The harmful link is clicked		User goes to connection	Pass
				Prefers to go to the link			
		TC13	If the user does not want to go to the link as a result of the warning, it should remain on the current page	The harmful link is clicked		User remains on the page	Pass
				Prefers not to go to the link			

Table 20 - REQ-04 Detailed Traceability Matrix

14.4.1 TC11: Warning on Malicious Link Click

Description: This test ensures the system warns the user when clicking on a malicious link.

Test Steps: A page with a harmful link is displayed, the harmful link is clicked.

Expected Results: The user should receive a warning message.

Pass/Fail: Pass

Test Case ID	TC11	Test Case Description	When a user clicks on a malicious link, they should be warned before being redirected to the link		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	codexpcgames.com
2	
3	
4	

Test Scenario	Warning of harmful connection inputs
---------------	--------------------------------------

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	A page with a harmful link is displayed	Providing page security information to user with red icon.	As Expected	Pass
2	The harmful link is clicked	The user should receive a warning message	As Expected	Pass

Table 21 - Test Case 11

14.4.2 TC12: User Redirected if They Choose to Proceed

Description: This test checks if the user is redirected if they choose to proceed after the warning.

Test Steps: The harmful link is clicked, the user chooses to go to the link.

Expected Results: User is redirected to the harmful link.

Pass/Fail: Pass

Test Case ID	TC12	Test Case Description	If the user still wants to go to the link as a result of the warning, they should be redirected		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	codexpcgames.com
2	
3	
4	

Test Scenario	Warning of harmful connection inputs
---------------	--------------------------------------

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	The harmful link is clicked	The user should receive a warning message	As Expected	Pass
2	Prefers to go to the link	User goes to connection	As Expected	Pass

Table 22 - Test Case 12

14.4.3 TC13: User Stays on the Current Page if They Choose Not to Proceed

Description: This test checks if the user remains on the current page if they choose not to proceed after the warning.

Test Steps: The harmful link is clicked, the user chooses not to go to the link.

Expected Results: User stays on the current page.

Pass/Fail: Pass

Test Case ID	TC13	Test Case Description	If the user does not want to go to the link as a result of the warning, it should remain on the current page		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	codexpcgames.com
2	
3	
4	

Test Scenario	Warning of harmful connection inputs
---------------	--------------------------------------

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	The harmful link is clicked	The user should receive a warning message	As Expected	Pass
2	Prefers not to go to the link	User remains on the page	As Expected	Pass

Table 23 - Test Case 13

14.5 REQ 05: Page Scans Should Be Fast in Performance

Req ID	Req Description	Test Case ID	Test Case Description	Test Steps	Test Data	Expected Results	Pass/Fail
REQ 05	Page scans should be fast in performance	TC14	Perform operations on more than one at the same time	Open multiple tabs in the browser		Links within the pages should come quickly	Pass
				Display different pages in each tab			
		TC15	Another page must be opened before a page loads	Load a page		Scanning should be done quickly on the new page that opens	Fail
				Switch to another page before the page loads			
		TC16	Access to an unscanned page before the page is loaded	Load a page		User enters the page	Pass
				Click on the link before the scan takes place			

Table 24 - REQ-05 Detailed Traceability Matrix

14.5.1 TC14: Perform Operations on More Than One at the Same Time

Description: Verify the system's performance when multiple operations are performed simultaneously.

Test Steps: Open multiple tabs in the browser, display different pages in each tab.

Expected Results: Links within the pages should load quickly.

Pass/Fail: Pass

Test Case ID	TC14	Test Case Description	Perform operations on more than one at the same time		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Page scans should be fast in performance
---------------	--

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Open multiple tabs in the browser	Links within the pages should come quickly	As Expected	Pass
2	Display different pages in each tab	Links within the pages should come quickly	As Expected	Pass

Table 25 - Test Case 14

14.5.2 TC15: Another Page Must Be Opened Before a Page Loads

Description: Check if another page can be opened before the current page loads.

Test Steps: Load a page, switch to another page before it loads.

Expected Results: Scanning should be done quickly on the new page that opens.

Pass/Fail: Fail (not meeting the scanning speed requirement).

Test Case ID	TC15	Test Case Description	Another page must be opened before a page loads		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Page scans should be fast in performance
---------------	--

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Load a page	Links within the pages should come quickly	As Expected	Pass
2	Switch to another page before the page loads	Scanning should be done quickly on the new page that opens	Unexpected	Fail

Table 26 - Test Case 15

14.5.3 TC16: Access to an Unscanned Page Before the Page Is Loaded

Description: Verify if the system allows access to an unscanned page before it loads.

Test Steps: Load a page, user enters the page, clicks on the link before the scan takes place.

Expected Results: User can access the unscanned page before the scan completes.

Pass/Fail: Pass

Test Case ID	TC16	Test Case Description	Access to an unscanned page before the page is loaded		
Created By	Ceyhun Binal	Reviewed By	Ergül Ferik	Version	1.0

QA Tester's Log	No have QA tester
-----------------	-------------------

Tester's Name	Ceyhun Binal	Date Tested	Aralık 26, 2023	Test Case (Pass/Fail/Not Executed)	Pass
---------------	--------------	-------------	-----------------	------------------------------------	------

S #	Prerequisites:
1	Starting the backend server
2	Using Google Chrome for web surfing
3	AllScan Chrome Extension is working
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Page scans should be fast in performance
---------------	--

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Load a page	Links within the pages should come quickly	As Expected	Pass
2	Click on the link before the scan takes place	User enters the page	As Expected	Pass

Table 27 - Test Case 16

15. DISCUSSION OF THE RESULTS

The proliferation of cyber threats, particularly through fraudulent links, poses a significant risk to users' personal information and online security. Malicious individuals exploit these links to perpetrate various forms of cybercrime, including account takeovers, financial fraud, identity theft, corporate breaches, and the dissemination of harmful software. As a response to this escalating issue, the AllScan technology has been developed to offer users a safer and more secure internet experience.

AllScan represents a pivotal advancement in internet security, leveraging a comprehensive approach to systematically examine and scrutinize every link present on webpages. Its core functionality lies in conducting rigorous security checks through integrated antivirus software, ensuring that users can browse the internet with confidence, knowing that each connection's security status is constantly updated in real time.

The technology's efficacy is rooted in its sophisticated algorithms that meticulously assess URLs sourced from websites for potential security vulnerabilities. Upon detecting connections, the application seamlessly initiates scanning procedures in tandem with leading antivirus applications. Subsequently, the results are promptly presented to users, clearly indicating the safety of connections or flagging potentially hazardous ones.

One of AllScan's standout features is its seamless integration into users' web browsers, augmenting security without disrupting the browsing experience. Operating discreetly in the background, the application empowers users to make informed decisions while navigating the online landscape. Its user-friendly interface, coupled with real-time network inspection, significantly bolsters internet safety, providing users with peace of mind as they engage with various online platforms.

In essence, AllScan represents a harmonious fusion of link analysis and antivirus capabilities, offering a robust defense mechanism against diverse cyber threats. By actively fortifying user interactions through continuous monitoring and assessment of online connections, it stands as a reliable safeguard in an increasingly perilous digital environment. The technology's ability to seamlessly integrate security measures into the browsing experience underscores its significance in mitigating the risks posed by malicious links and fortifying internet security for users worldwide.

16. REFERENCES

- *Abdul Razzaq, Ali Hur, H. Farooq Ahmad, Muddassar Masood, "2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)", March 2013
- **Prashant S. Shinde, Shrikant B. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing", February 2016
- VirusTotal. (2022). About. <https://www.virustotal.com/gui/about-us>
- PhisTank. What is FishTank? <https://phishtank.org/faq.php>
- Python PEP 8 Documentation. <https://peps.python.org/pep-0008/>
- FastAPI Library <https://fastapi.tiangolo.com/>
- Kaspersky Open Tip https://opentip.kaspersky.com/Help/Doc_data/About.htm
- Kaspersky Threat Intelligence Portal <https://opentip.kaspersky.com/>
- Chrome Extensions <https://developer.chrome.com/docs/extensions>

17. INTERDISCIPLINARY DOMAIN

Interdisciplinary domains, including computer science, information security, software engineering, and security technologies, are all involved in the AllScan project.

Software Engineering and Computer Science: The AllScan project integrates software engineering and computer science concepts. One such project may be an internet connection analysis and web browser integration program.

Information Security: AllScan addresses concerns related to information security and internet security. This might cover subjects like user privacy, data security, and identifying dangerous connections.

Security Technologies: AllScan uses the discipline of security technologies to be able to do security checks by scanning connections. This can involve vulnerability assessments, malware detection, and virus scanning.

The goal of this multidisciplinary approach is to offer an all-encompassing and well-rounded answer to issues related to Internet security.

18. SUSTAINABLE DEVELOPMENT GOAL

Sustainable Development Goal 10 is called Reducing Inequalities. This objective is to improve the social inclusion principle and lessen disparities based on factors including income, gender, race, ethnicity, and handicap status.

Sustainable Development Goal 10 seeks to lessen marginalization and discrimination against underprivileged groups, with an emphasis on social and economic inequality. Reducing income distribution disparities, ensuring opportunity equality, boosting social inclusion, and advancing justice globally are all part of this objective.

Since reaching this objective is a crucial first step toward a more equitable and inclusive society, reducing inequality is seen as a crucial component of sustainable development. According to this paradigm, Sustainable Development Goal 10 attempts to help everyone reach their full potential and improve social fairness globally.

19. SIMILARITY REPORT

190315041 & 190315080

ORJİNALLİK RAPORU

% 14	% 11	% 3	% 12
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	Submitted to University of Greenwich Öğrenci Ödevi	% 4
2	www.coursehero.com İnternet Kaynağı	% 2
3	Submitted to University of Wisconsin, Platteville Öğrenci Ödevi	% 1
4	Submitted to National Tertiary Education Consortium Öğrenci Ödevi	% 1
5	Submitted to Universiti Teknologi Malaysia Öğrenci Ödevi	% 1
6	www.scilit.net İnternet Kaynağı	% 1
7	Submitted to Higher Education Commission Pakistan Öğrenci Ödevi	% 1
8	Submitted to King's Own Institute Öğrenci Ödevi	<% 1

9	open.uct.ac.za İnternet Kaynağı	<% 1
10	pure.tue.nl İnternet Kaynağı	<% 1
11	Submitted to Southern New Hampshire University - Continuing Education Öğrenci Ödevi	<% 1
12	Submitted to University of Pittsburgh Öğrenci Ödevi	<% 1
13	www.aalavai.com İnternet Kaynağı	<% 1
14	fastercapital.com İnternet Kaynağı	<% 1
15	Submitted to College of the North Atlantic-Qatar Öğrenci Ödevi	<% 1
16	www.franksmith.org İnternet Kaynağı	<% 1
17	Submitted to October University for Modern Sciences and Arts (MSA) Öğrenci Ödevi	<% 1
18	Submitted to University of Wolverhampton Öğrenci Ödevi	<% 1
19	livrepository.liverpool.ac.uk İnternet Kaynağı	<% 1

20	www.digitaljournal.com İnternet Kaynağı	<% 1
21	support.kaspersky.com İnternet Kaynağı	<% 1
22	webthesis.biblio.polito.it İnternet Kaynağı	<% 1
23	"Model-Driven Architecture in Practice", Springer Science and Business Media LLC, 2007 Yayın	<% 1
24	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Öğrenci Ödevi	<% 1
25	docs.google.com İnternet Kaynağı	<% 1
26	www.virtenio.com İnternet Kaynağı	<% 1
27	www.slideshare.net İnternet Kaynağı	<% 1

Alıntıları çıkart Kapat
Bibliyografyayı Çıkart üzerinde

Exclude assignment üzerinde
template Eşleşmeleri çıkar Kapat