**SE 356 WEB APPLICATION DEVELOPMENT**

**MIDTERM PROJECT**

**Phishing Testing Platform**

**Instructor**

**Asst. Prof. Emre Atlıer Olca**

**Project Members**

**Tolga Emre Koraş 200706042**

**Emin Mert Demirci 180706023**

***The aim of the project***

*With this project, learn how phishing attacks are carried out in real life. By building our own phishing testing platform, we will discover how to protect ourselves from such attacks and how to recognize them.*

***What is Phishing?***

*Phishing attacks are fraudulent emails, text messages, phone calls or web sites designed to trick users into downloading malware, sharing sensitive information or personal data (e.g., Social Security and credit card numbers, bank account numbers, login credentials), or taking other actions that expose themselves or their organizations to cybercrime. By masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them, similarly to how a fisherman uses bait to catch a fish. Successful phishing attacks often lead to identity theft, credit card fraud, ransomware attacks, data breaches, and huge financial losses for individuals and corporations.*

*Phishing is the most common type of social engineering, the practice of deceiving, pressuring, or manipulating people into sending information or assets to the wrong people. (Figure 1.0)*

A diagram of a computer virus

Description automatically generated

(Figure 1.0)

**Types of phishing attacks**

* ***Spear phishing*** *is a phishing attack that targets a specific individual—usually a person who has privileged access to sensitive data or network resources, or special authority that the scammer can exploit for fraudulent or nefarious purposes.*
* ***Bulk email phishing*** *is the most common type of phishing attack. A scammer creates an email message that appears to come from a large, well-known legitimate business or organization—a national or global bank, a large online retailer, the makers of a popular software application or app—and sends the message to millions of recipients.*
* ***Business email compromise (BEC)*** *BEC is a class of spear phishing attack that attempts to steal large sums of money or extremely valuable information—e.g. trade secrets, customer data, financial information—from corporations or institutions.*
* ***SMS phishing****, or smishing, is phishing using mobile or smartphone text messages.*
* ***Voice phishing, or vishing****, is phishing via phone call.*
* ***Social media phishing*** *employs various capabilities of a social media platform to phish for members' sensitive information.*
* ***Application or in-app messaging****.*
* ***Website forgery fraud.***
* ***Clone phishing*** *involves mimicking a previously delivered legitimate email and modifying its links or attached files in order to trick the victim into opening a malicious website or file.*
* ***Whaling*** *for attacks that are directed specifically at senior executives or other privileged users within businesses, the term whaling is commonly used. These types of attacks are typically targeted with content likely to require the attention of the victim such as legal subpoenas or other executive issues.*

**How To Recognize Phishing**

**Common Features of Phishing Emails**

* ***Too Good to Be True****: Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people’s attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just do not click on any suspicious emails. Remember that if it seems too good to be true, it probably is!*
* ***Sense of Urgency****: A favourite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it is best to just ignore them. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account, and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.*
* ***Hyperlinks****: A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different, or it could be a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully.*
* ***Attachments****: If you see an attachment in an email, you were not expecting or that does not make sense, do not open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.*
* ***Unusual Sender****: Whether it looks like it is from someone you do not know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general do not click on it!*

**Characteristic features of phishing emails:**

* *Requests for sensitive or personal information, or to update profile or payment information.*
* *Requests to send or move money.*
* *File attachment(s) the recipient did not request or expect.*
* *A sense of urgency, whether blatant ('Your account will be closed today...') or subtle (e.g., a request from a colleague to pay an invoice immediately) threats of jail time or other unrealistic consequences.*
* *Threats of jail time or other unrealistic consequences.*
* *Poor spelling or grammar.*
* *Inconsistent or spoofed sender address.*
* *Links shortened using Bit.Ly or some other link-shortening service.*
* *Images of text used in place of text (in messages, or on web pages linked to in messages).*
* *Say they have noticed some suspicious activity or log-in attempts — they have not*
* *Claim there is a problem with your account or your payment information — there is not*
* *Say you need to confirm some personal or financial information — you do not*
* *Include an invoice you do not recognize — it is fake*
* *Want you to click on a link to make a payment — but the link has malware*
* *Say you are eligible to register for a government refund — it is a fraud*
* *Offer a coupon for free stuff — it is not real*

A computer screen with text and symbols

Description automatically generated

(Figure 1.1)

**Real-world example of a phishing email:**

A screenshot of a phone

Description automatically generated

Figure (1.2)

**How To Protect Yourself from Phishing Attacks**

1. *Spam filters and email security software use data on existing phishing frauds and machine learning algorithms to identify suspected phishing emails (and other spam), then move them to a separate folder and disable any links they contain.*
2. *Antivirus and anti-malware software detects and neutralizes malicious files or code in phishing emails.*
3. *Multi-factor authentication requires at least one login credential in addition to a username and a password—for example, a one-time code sent to the users' mobile phone. By providing and additional last line of defence against phishing frauds or other attacks that successfully compromise passwords, multi-factor authentication can undermine spear phishing attacks and prevent BEC.*
4. *Web filters prevent users from visiting known malicious web sites ('blacklisted' sites) and display alerts whenever users visit suspected malicious or fake web sites.*
5. *Organizations should provide security awareness training to employees to recognize the risks.*

**Chosen Phishing Type for the Project:**  ***Bulk e-mail phishing***

We chose to focus on phishing emails for our project due to their increasing prevalence and impact in our digital-first world. Phishing scams, which trick individuals into giving sensitive information, represent a significant threat to personal and organisational security. Through this project, we aim to dive into the methods used by phishers to craft convincing emails, exploring how they exploit human vulnerabilities and technological loopholes. This phishing type will not only enhance our understanding of cybersecurity but also raising awareness about this common form of digital deception.

**Database Design**

**Database Choice: Microsoft SQL Server**

**1. Administration Panel**

**PhishingEmailTemplates Table:**

**TemplateID (PK): A unique identifier for each template.**

**TemplateName: Name of the template.**

**TemplateContent: HTML content of the email template.**

**CreationDate: Date when the template was created or modified.**

**TargetEmailAddresses Table:**

**EmailAddressID (PK): A unique identifier for each email address.**

**EmailAddress: The fake email addresses used for testing.**

**OwnerName: (Optional) Name associated with the email address for testing scenarios.**

**SentEmails Table:**

**EmailID (PK): A unique identifier for each sent email.**

**TemplateID (FK): Links to the PhishingEmailTemplates table.**

**EmailAddressID (FK): Links to the TargetEmailAddresses table.**

**SendDate: Date and time the email was sent.**

**Clicked: Boolean indicating if the email was clicked.**

**ClickDate: Date and time of the click (if any).**

**2. Phishing Email Template Creation Page**

**This functionality can be supported by the PhishingEmailTemplates table.**

**3. Reporting Page**

**UserResponses Table:**

**ResponseID (PK): A unique identifier for each response.**

**EmailID (FK): Links to the SentEmails table.**

**EnteredData: Information entered by the user (for testing purposes only).**

**ResponseDate: Date and time when the response was recorded.**

**AccessLogs Table:**

**LogID (PK): A unique identifier for each log.**

**EmailID (FK): Links to the SentEmails table.**

**IPAddress: IP address of the user who interacted with the email.**

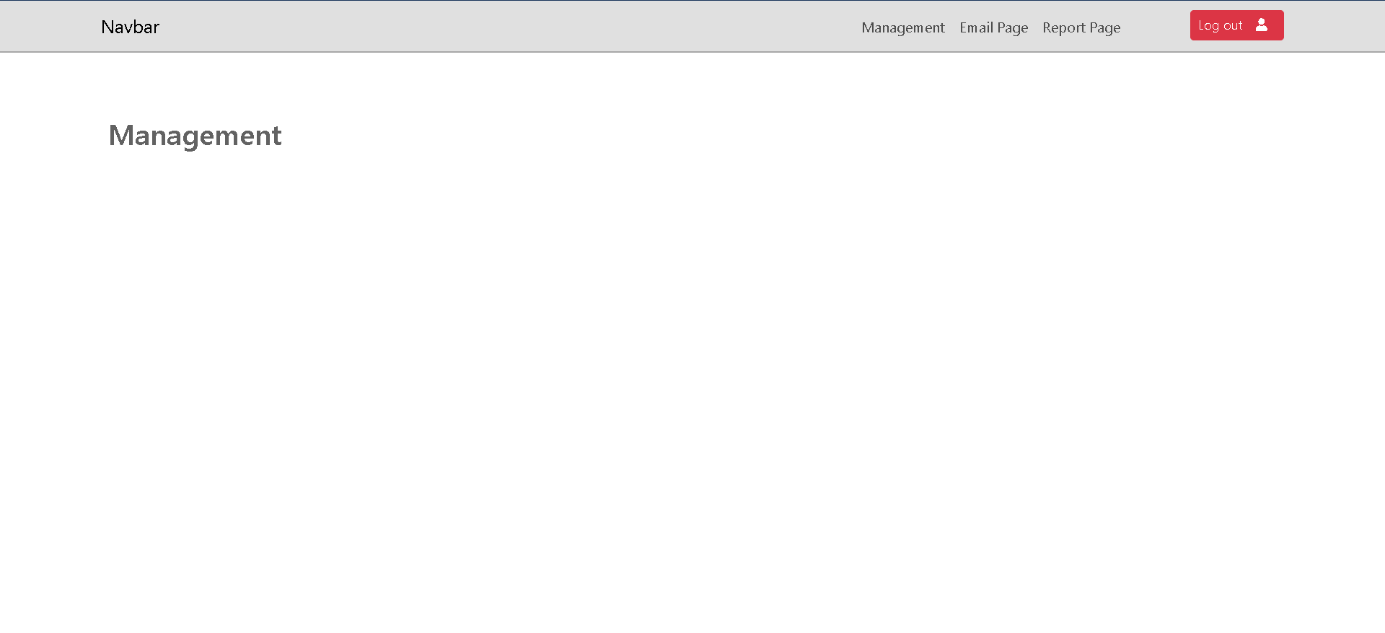
**AccessDate: Date and time of access.**

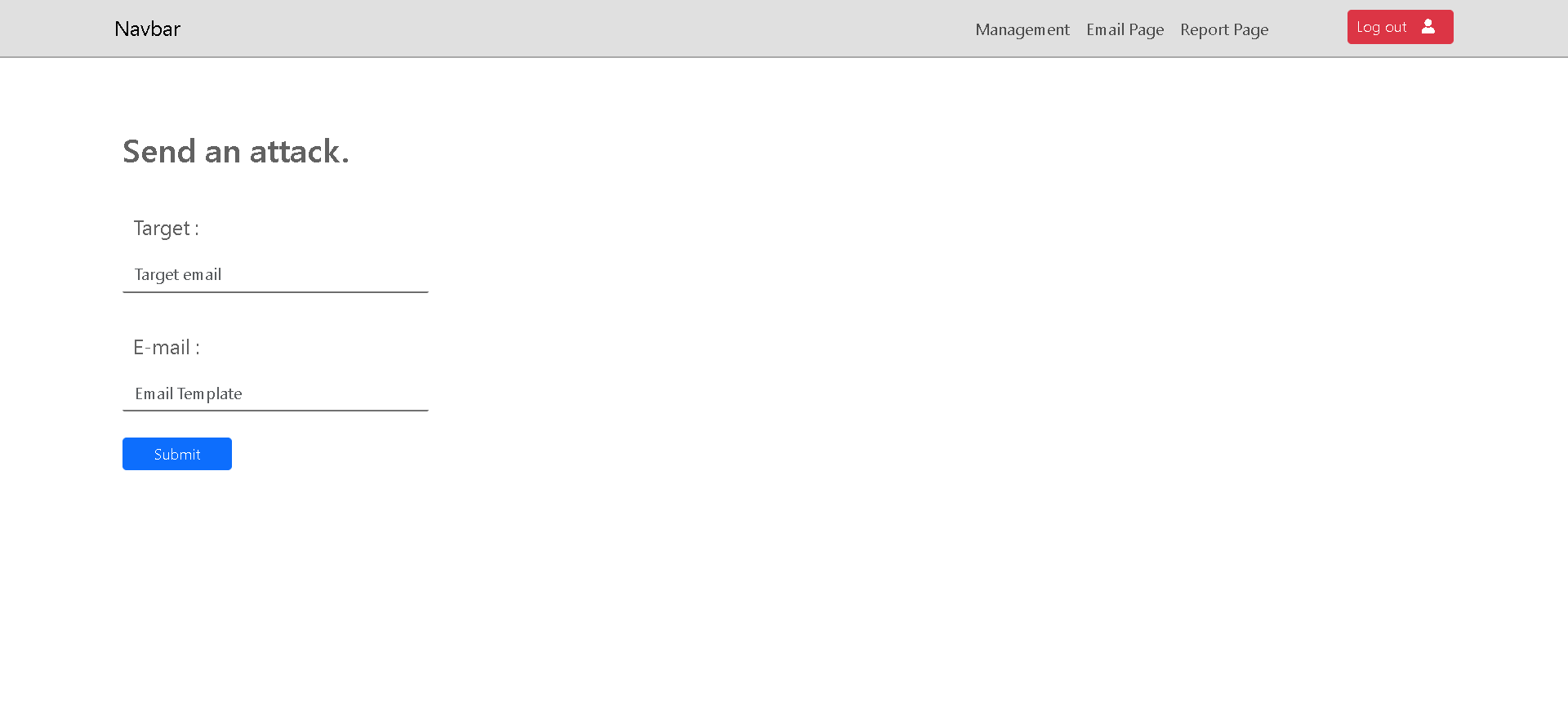
A diagram of a software application

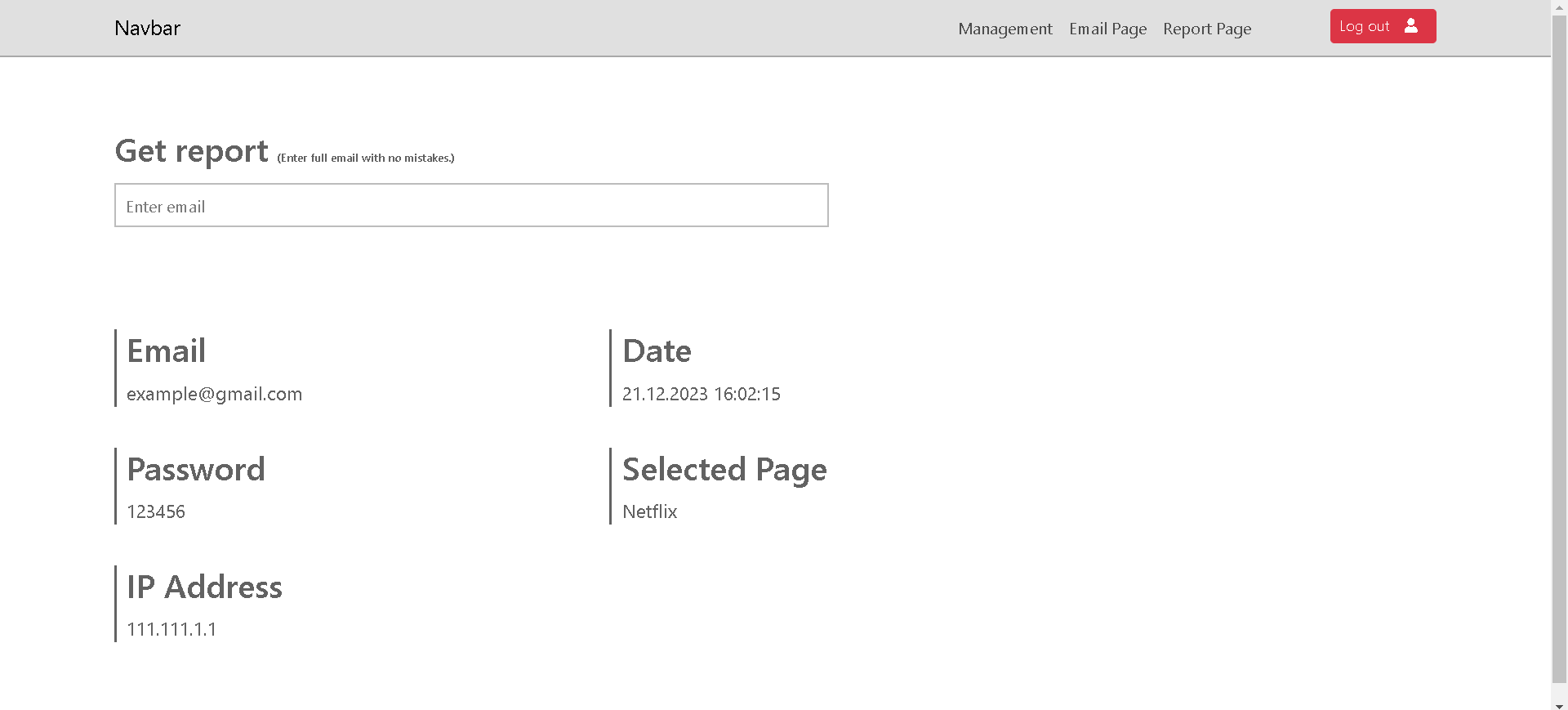
Description automatically generated with medium confidence

**User Interface & Email Design**

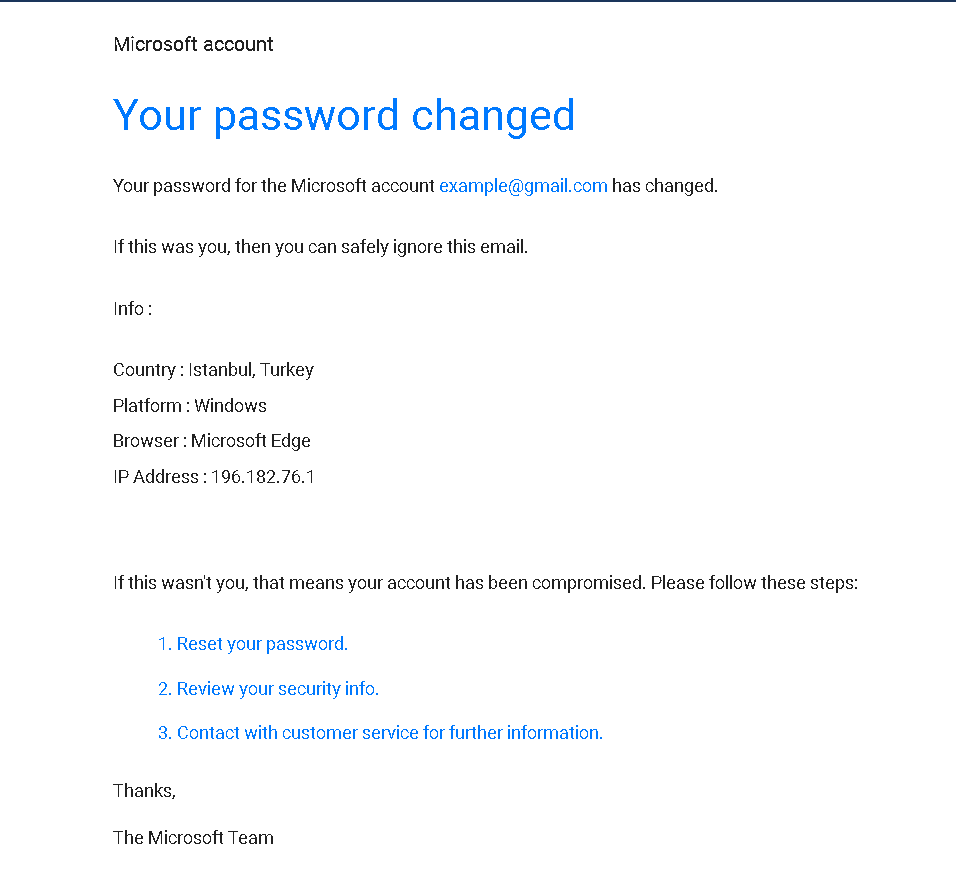
**1.Management Page**

****

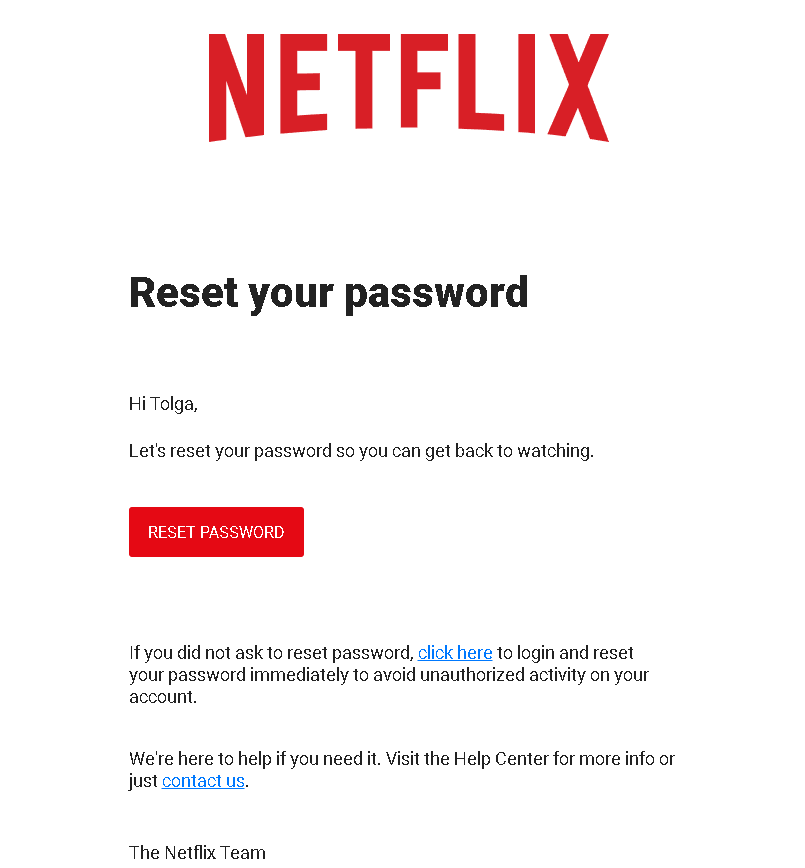
**2.Email Page**

**3.Report Page**

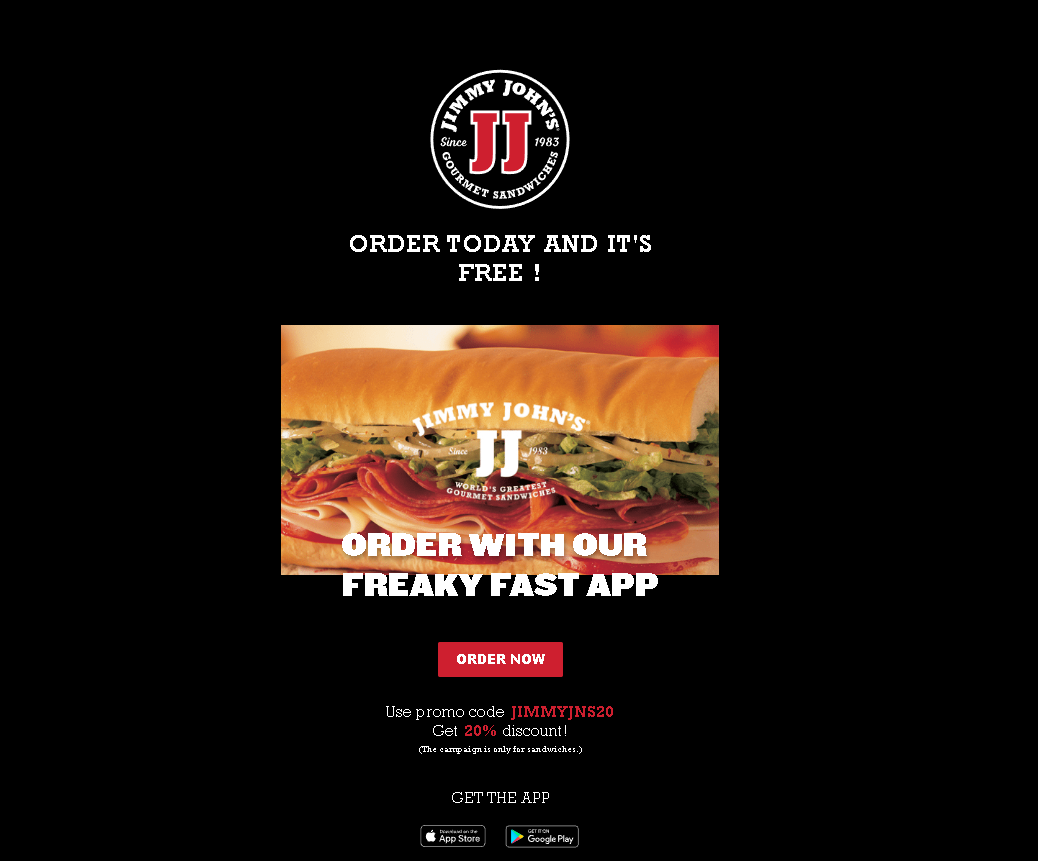
**4.Microsoft Fake Email**

****

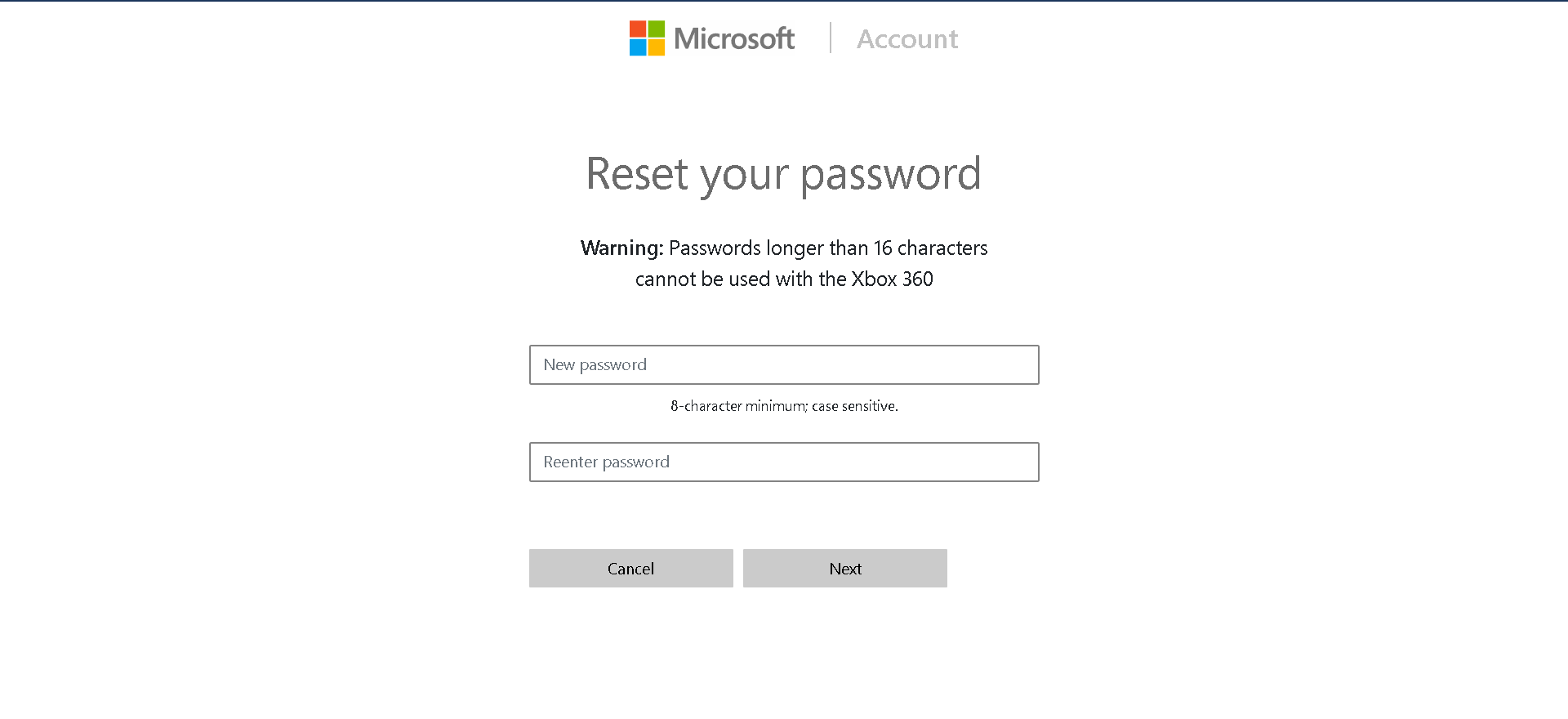
**5.Netflix Fake Email**



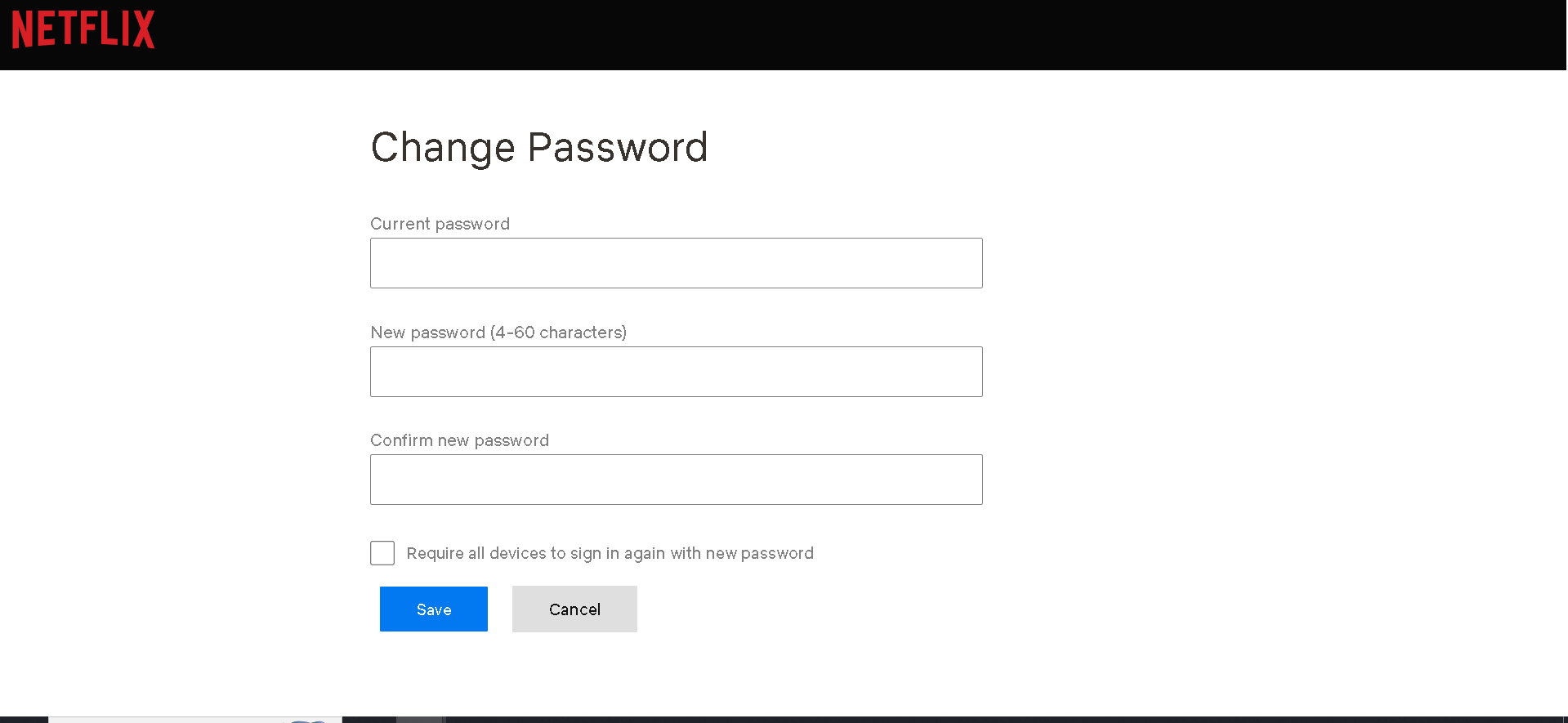
**6.Jimmy Jones Fake Email**



**7.Microsoft Fake Page**



**9.Netflix Fake Page**



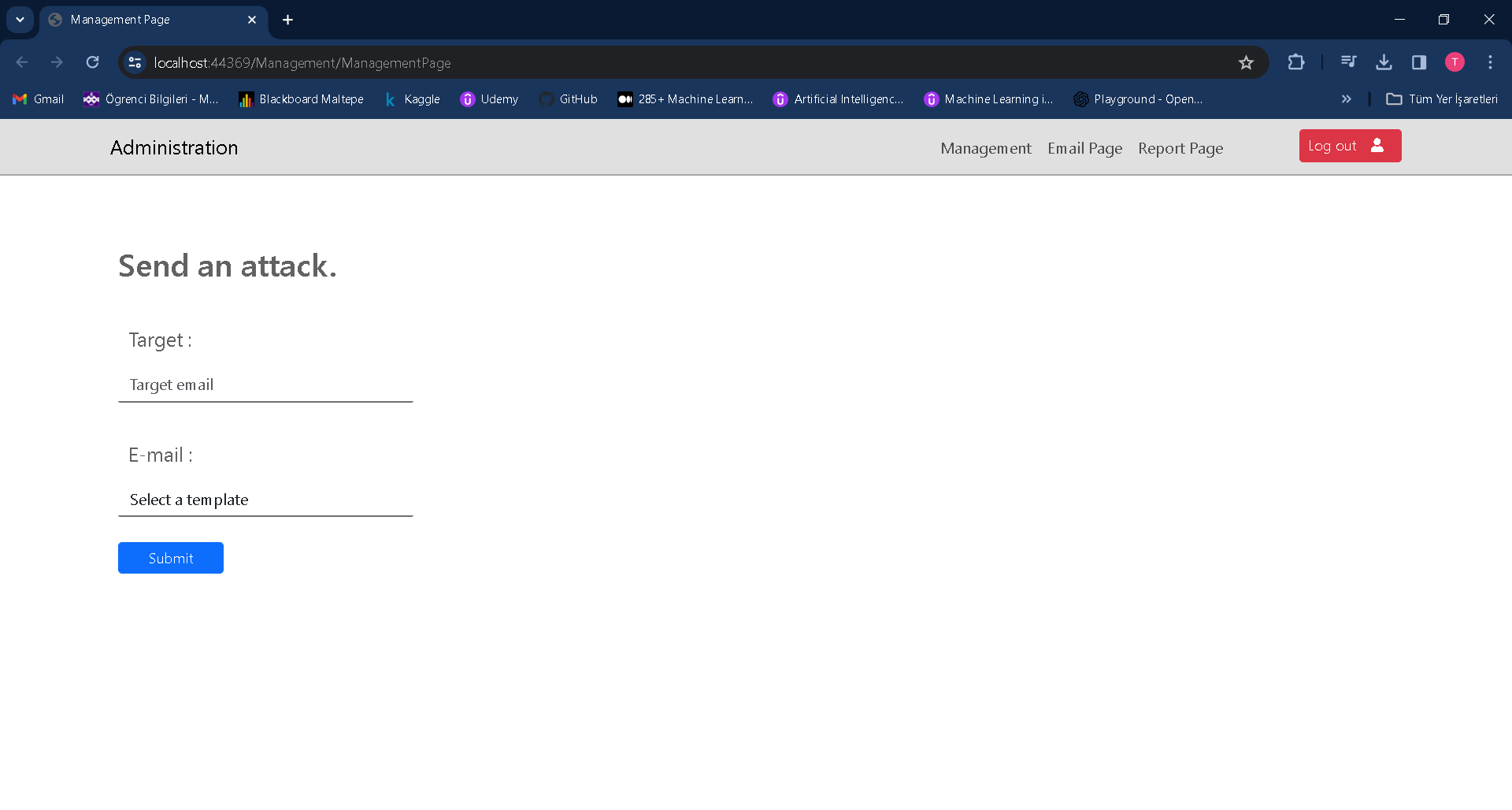
**Final Changes and Latest Situation**

1. **Database Design**

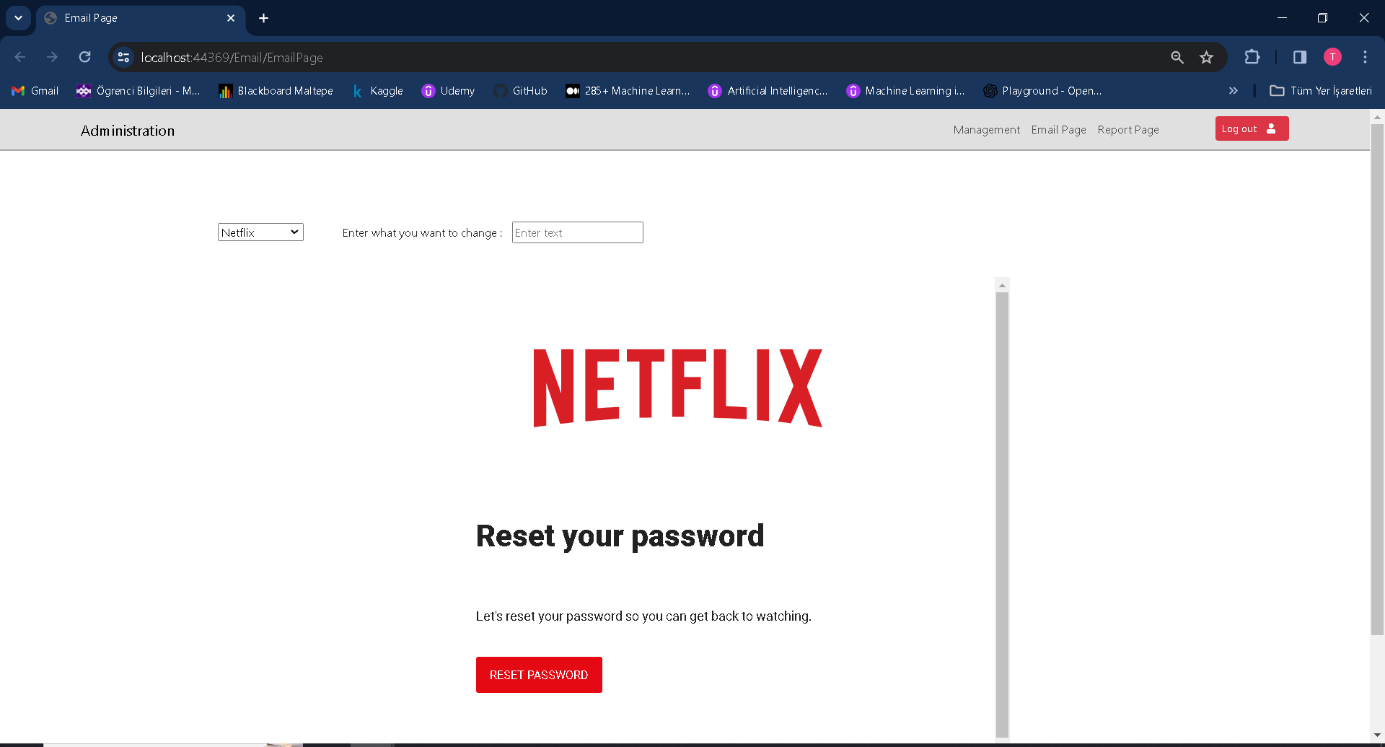
A diagram of a computer

Description automatically generated

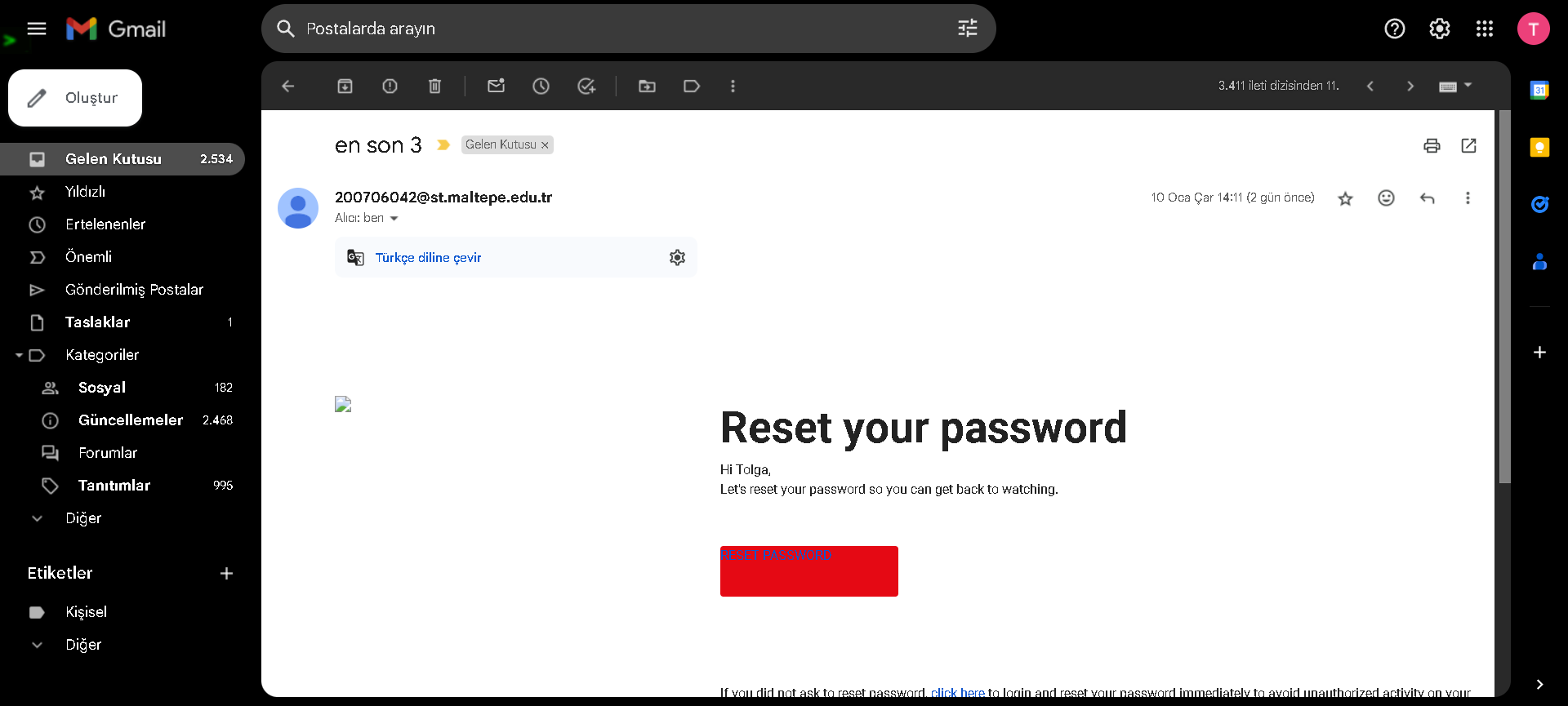
1. **Management Page**

****

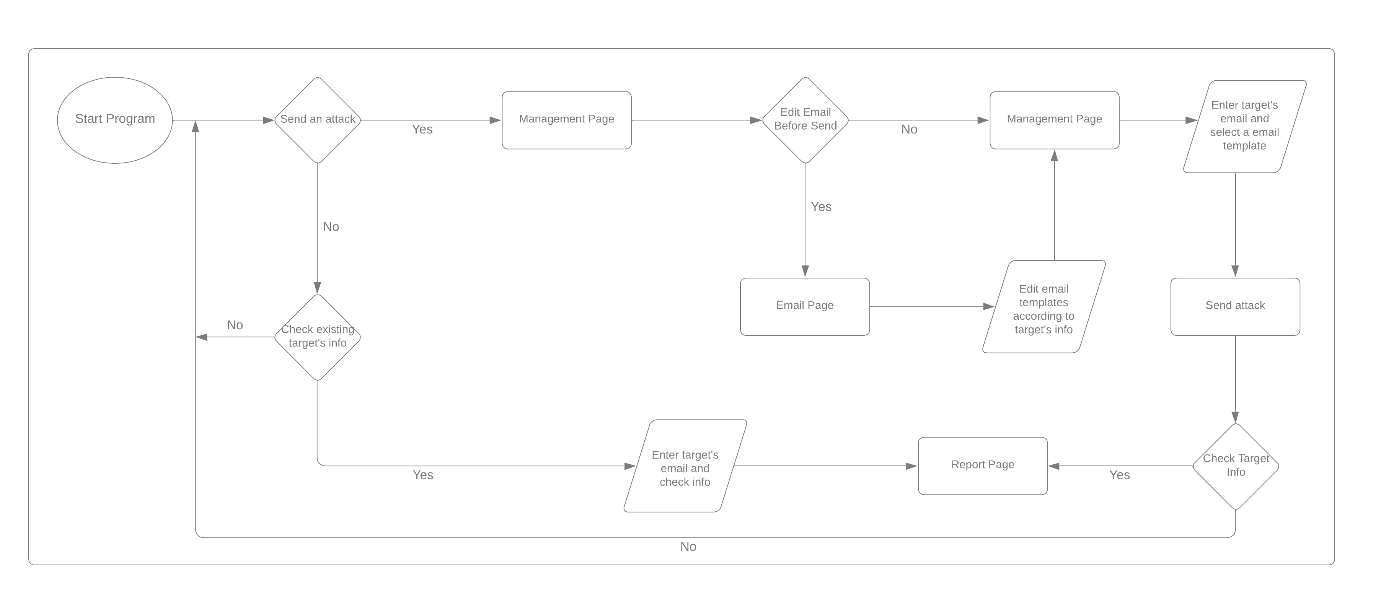
1. **Email Page**

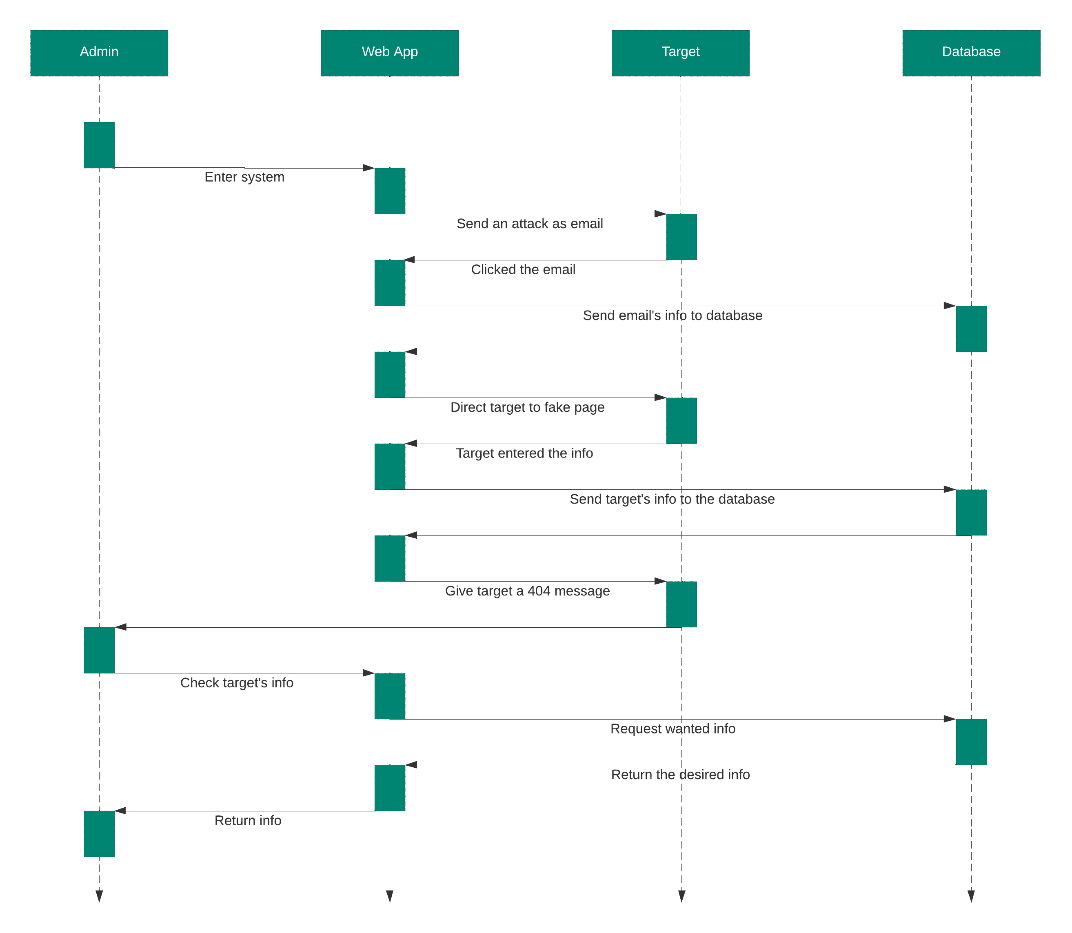


1. **An Example of Received Email**

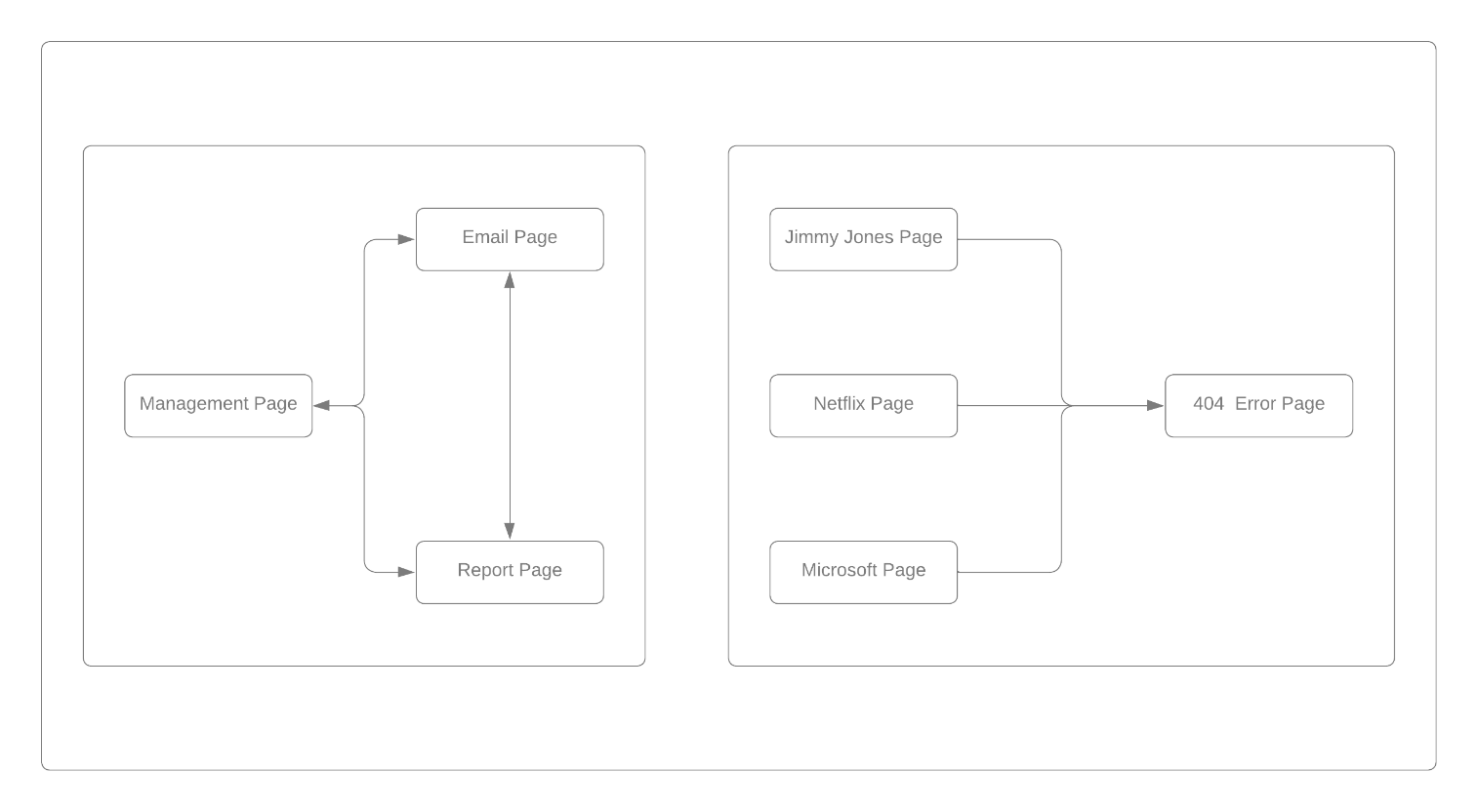
****

**UML Diagrams and Flow Chart**

1. **Activitiy Diagram**
2. **Sequence Diagram**



1. **Flow Chart**

****