

**T.C.**

**AYDIN ADNAN MENDERES ÜNİVERSİTESİ**

**YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI**

**LİSANS TEZİ**

**TÜRKİYE’DE SANAL GÜVENLİK**

**Ufuk İNCİBAŞ**

**Prof.Dr. Mustafa Çetin**

**MART 2024**

**T.C.**

**AYDIN ADNAN MENDERES ÜNİVERSİTESİ**

**YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI**

**LİSANS TEZİ**

**TÜRKİYE’DE SANAL GÜVENLİK**

**Ufuk İNCİBAŞ**

**Prof.Dr. Mustafa Çetin**

**MART 2024**

**T.C.**

**AYDIN ADNAN MENDERES ÜNİVERSİTESİ**

**SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE**

**AYDIN**

Yönetim Bilişim Sistemleri Ana Bilim Dalı öğrencisi Ufuk İNCİBAŞ tarafından hazırlanan “Türkiye’de Sanal Güvenlik” başlıklı tez, 22/03/2024 tarihinde yapılan savunma sonucunda aşağıda isimleri bulunan jüri üyelerince kabul edilmiştir.

|  |  |  |
| --- | --- | --- |
| **Ünvanı**   **Adı ve Soyadı** | **Kurumu** | **İmzası** |
| Prof.Dr. Mustafa ÇETİN | Aydın Adnan Menderes Üniversitesi |  |

Jüri üyeleri tarafından kabul edilen bu Lisans tezi, Yönetim Bilişim Sistemleri Anabilim Dalında hazırlanmış ve jürimiz tarafından kabul edilmiştir.

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar

bütün safhalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik

ve etik kurallar içinde elde ettiğimi, bu tez çalışması ile elde edilmemiş bütün bilgi ve

yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine

bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir

davranışımın olmadığı beyan ederim.

(24/03/2024)

Öğrencinin Ufuk İNCİBAŞ

İmza

**ÖZET**

Bu tez, Türkiye'deki kurumsal web sitelerindeki kritik güvenlik açıklarını belirleyerek, ülkenin siber güvenlik alanındaki geçmiş sorunlarından ders çıkarmayı ve daha sağlam güvenlik uygulamalarını teşvik etmeyi amaçlamaktadır. Çalışma, özellikle port taraması gibi saldırı tekniklerini ve SQL enjeksiyonu, XSS (Cross-Site Scripting) gibi web hacking tekniklerinin ciddi sonuçlarına odaklanmaktadır.

Türkiye, geçmişte MERNİS veri sızıntısı gibi önemli siber güvenlik olayları yaşamıştır. Bu olaylar, ülkenin siber güvenlik politikalarını ve bilinç düzeyini geliştirmesi gerektiğini göstermiştir. Bu tez, Türkiye'nin bu tür olaylardan ders çıkararak gelecekteki benzer sorunlardan kaçınmasına yardımcı olmayı amaçlamaktadır.

Ayrıca, tez, geliştirici hatalarının (örneğin, güvensiz dosya yükleme, güvenlik duvarının uygun şekilde yapılandırılmamış olması gibi) nasıl kritik güvenlik açıklarına yol açabileceğini açıklamaktadır. Bu tür hataların önlenmesi için daha iyi kodlama standartları ve güvenlik testleri gibi uygulamaların önemine dikkat çekmektedir. Sonuç olarak, tez, kurumsal web sitelerinin güvenliğini artırmak için alınabilecek önlemleri ve daha etkili güvenlik uygulamalarını tartışmaktadır.

**Anahtar Sözcükler:** Kurumsal web siteleri, güvenlik açıkları, Türkiye, siber güvenlik, geliştirici hataları, güvenlik uygulamaları, port taraması, web hacking, SQL enjeksiyonu, XSS, MITM, CSRF, subdomain.

**ABSTRACT**

This thesis aims to identify critical security vulnerabilities in corporate websites in Turkey, learn from the country's past cybersecurity incidents, and promote stronger security practices. The study focuses on attack techniques such as port scanning, SQL injection, and XSS (Cross-Site Scripting), highlighting their serious consequences.

Turkey has experienced significant cybersecurity incidents in the past, such as the MERNIS data breach. These events have underscored the need for the country to enhance its cybersecurity policies and awareness. This thesis seeks to help Turkey avoid future similar problems by learning from these incidents.

Additionally, the thesis explains how developer errors (such as insecure file uploads, improperly configured firewalls, etc.) can lead to critical security vulnerabilities. It emphasizes the importance of better coding standards and security testing to prevent such errors. Ultimately, the thesis discusses measures to improve the security of corporate websites and enhance security practices.

**Keywords:** Corporate websites, security vulnerabilities, Turkey, cybersecurity, developer errors, security practices, port scanning, web hacking, SQL injection, XSS.

**ÖNSÖZ**

Bu tez, Türkiye'de siber güvenlik konusundaki mevcut durumu incelemekte ve ülkemizdeki kurumların web sitelerinde bulunan güvenlik açıklarını belirlemeyi amaçlamaktadır. Günümüzün dijital dünyasında, siber güvenlik sadece bireyler ve kurumlar için değil, ulusal güvenlik açısından da büyük önem taşımaktadır. Siber saldırılar, ekonomik kayıplara ve bilgi sızıntılarına yol açabilmekte, dolayısıyla güvenlik açıklarının tespiti ve giderilmesi hayati bir önem arz etmektedir.

Tez çalışmam boyunca, hem kendi üniversitemin web sitesinde hem de diğer bazı kurumsal web sitelerinde gerçekleştirdiğim sızma testleri ile güvenlik açıklarını tespit ettim. Bu çalışmada, tespit edilen açıklar ve bu açıkların nasıl giderilebileceği konularında önerilerde bulunmaktayım.

Bu çalışmanın gerçekleştirilmesinde bana yol gösteren ve destek olan değerli danışman hocama, akademik süreç boyunca desteğini esirgemeyen aileme ve arkadaşlarıma teşekkür ederim. Ayrıca, çalışmam için gerekli izinleri veren ve destek olan kurumlara da şükranlarımı sunarım.

Son olarak, bu tezin Türkiye'deki siber güvenlik farkındalığını artırmasını ve gelecek araştırmalara katkı sağlamasını temenni ediyorum.

Saygılarımla,

Ufuk İNCİBAŞ

10.06.2024

[1. GİRİŞ 9](#_Toc1517265973)

[2. GENEL BİLGİLER 9](#_Toc847464699)

[2.1 Problem durumu 9](#_Toc226233201)

[Türkiye, dijitalleşme sürecinde hızla ilerlerken, siber güvenlik konusunda yaşanan problemler de artmaktadır. Bu problemlerin temelinde, bilgi sistemlerinin ve altyapıların yeterince güvenli olmaması, bilgi güvenliği politikalarının yetersizliği ve siber saldırılara karşı bilinç düzeyinin düşüklüğü gibi faktörler yer almaktadır. Bu nedenle, Türkiye'nin siber güvenlik konusundaki durumunun detaylı bir şekilde incelenmesi ve çözüm önerilerinin geliştirilmesi gerekmektedir. 9](#_Toc1725025544)

[2.2 Araştırmanın Amacı 9](#_Toc365786449)

[2.3 Araştırmanın Önemi 9](#_Toc662743152)

[2.4 Problem Cümlesi ve Alt Problemler/Hipotezler 9](#_Toc393022398)

[2.5 Varsayımlar 9](#_Toc2130737404)

[2.6 Sınırlılıklar 9](#_Toc1786554294)

[3. LİTERATÜR TARAMASI 9](#_Toc1720274893)

[3.1. Türkiye'deki Siber Güvenlik Durumu 9](#_Toc1331571372)

[3.2. Önemli Siber Güvenlik Olayları: MERNIS Veri İhlali 9](#_Toc459666535)

[3.3. Mevcut Güvenlik Standartları ve Uygulamaları 9](#_Toc310381594)

[4.1. Penetrasyon Testleri için Kullanılan Yöntemler 9](#_Toc1410489643)

[4.1.1 Nessus 9](#_Toc1617532281)

[4.1.2 Nikto: 9](#_Toc117706016)

[4.1.3 DirBuster: 9](#_Toc1261098686)

[4.1.4 Nuclei-Subfinder-HTTPX: 9](#_Toc616023281)

[4.1.5 Nmap: 9](#_Toc639325642)

[4.1.6 Wappalyzer :Web sitesinin kullandığı teknolojileri (örneğin, web sunucusu, içerik yönetim sistemi, analiz araçları) belirlemeye ve listelemeye yarayan bir tarayıcı eklentisidir. 9](#_Toc1451215396)

[4.2. Testlerin Gerçekleştirilmesi 9](#_Toc398708112)

[4.2.1 Bilgi Toplama (Reconnaissance): 9](#_Toc1223131975)

[4.2.2 Zaafiyet Taraması (Vulnerability Scanning): 9](#_Toc804225713)

[4.2.3 Sızma Denemeleri (Exploitation): 9](#_Toc1024968829)

[4.2.4 Raporlama: 9](#_Toc931946863)

[4.3 Web Sitelerinin Seçimi 9](#_Toc543484741)

[4.3.1 Web sitelerinin Çeşitliliği 9](#_Toc2074015363)

[4.3.2 Web Sitelerinin Önemi ve Etkinliği 9](#_Toc1900107458)

[4.3.3 Web Sitelerinin Güvenlik Öncelikleri 9](#_Toc977205201)

[4.3.4 Gizlilik ve Onaylar 9](#_Toc1037241928)

[4.4 Etik İzleme 9](#_Toc1101598292)

[5. BULGULAR 9](#_Toc1847773359)

[5.1 Karşılaşılan Yaygın Güvenlik Açıkları 9](#_Toc1658951122)

[5.1.4 Diğer Güvenlik Açıkları 9](#_Toc1174871149)

[5.2 Test Sonuçlarının Detaylı Analizi 9](#_Toc729787638)

[5.2.1 Wappalyzer 9](#_Toc650661115)

[5.2.1.1 Test Sonuçları: 9](#_Toc32876493)

[5.2.1.2 Eski ve Güvensiz Teknolojiler: 9](#_Toc1914314353)

[5.2.1.3 Potansiyel Etki: 9](#_Toc898465846)

[5.2.1.4 Çözüm: 9](#_Toc933793996)

[5.2.2 Nessus 9](#_Toc7296842)

[5.2.2.1 Test Sonuçları: 9](#_Toc485584352)

[5.2.2.2 (CVE-2020-5344): 9](#_Toc424064726)

[5.2.2.3 Çözüm: 9](#_Toc116422680)

[5.2.2.4 DNS Sunucusu Sahte İstek Yükseltmesi DDoS : 9](#_Toc549813668)

[5.2.2.5 Çözüm: 9](#_Toc1220683515)

[5.2.3 DirBuster 9](#_Toc2146039142)

[5.2.3.1 Test Sonuçları: 9](#_Toc2010870061)

[5.2.3.2 Potansiyel Etki: 9](#_Toc1162777759)

[5.2.4 Nuclei-Subfinder-HTTPX: 9](#_Toc1647693842)

[5.2.4.1 Test Sonuçları: 9](#_Toc1558084915)

[5.2.5 Nmap 9](#_Toc839795971)

[5.2.5.1 Test Sonuçları: 9](#_Toc773363882)

[5.2.5.2 CSRF Açığının Kapatılması 9](#_Toc2135213409)

[5.2.6 Genel Değerlendirme ve Öneriler 9](#_Toc495542420)

[5.2.6 Öneriler 9](#_Toc771273129)

[5.2.6.1 Güvenlik Güncellemeleri: 9](#_Toc1348462037)

[5.2.6.2 Güvenlik Testleri 9](#_Toc329237479)

[5.2.6.3 Kullanıcı Eğitimleri 9](#_Toc2119865031)

[5.2.6.4 Güvenlik Politikaları 9](#_Toc1387799063)

[5.2.6.5 Yedekleme ve Kurtarma Planları 9](#_Toc80958541)

[6.TARTIŞMA 9](#_Toc814244347)

[6.1 Bulguların Özeti 9](#_Toc1883391346)

[6.2 Bulguların Yorumlanması 9](#_Toc1960729529)

[6.3 Karşılaştırmalar 9](#_Toc1938578988)

[6.4 Güçlü ve Zayıf Yönler 9](#_Toc1474030266)

[ÖZGEÇMİŞ 9](#_Toc381274914)

**RESİMLER DİZİNİ**

Resim1. Wappalyzer uzantısı görseli.................................................................................... 20

Resim2. Nessustaramasonucugörseli ................................................................................ 21

Resim3. DirBuster tarama sonucu görseli ............................................................................. 23

Resim4. Nuclei test sonucu.................................................................................................... 24

Resim5. Açığın test edilmiş hali............................................................................................ 24

Resim6. Nmap script sonuçları.............................................................................................. 25

Kısaltmalar ve Simgeler Dizini

**A:** Acknowledgment

**KOBİ**: Küçük ve Orta Büyüklükteki İşletme

**MERNIS**: Merkezi Nüfus İdaresi Sistemi

**Nmap:** Network Mapper

**SQL:** Structured Query Language

**XSS:** Cross-Site Scripting

**CSRF:** Cross-Site Request Forgery

**CVE:** Common Vulnerabilities and Exposures

**DDoS:** Distributed Denial of Service

**HTTP:** Hypertext Transfer Protocol

**MITM:** Man in the Middle

**POST:** Post Office Protocol

**GET:** General Event Template

**CAPTCHA:** Completely Automated Public Turing test to tell Computers and Humans Apart

**HSTS:** HTTP Strict Transport Security

**1. GİRİŞ**

Günümüzde dijital teknolojilerin hızla gelişmesiyle birlikte, siber güvenlik konusu giderek daha fazla önem kazanmaktadır. Siber saldırılar, hem bireylerin hem de kurumların güvenliğini tehdit etmektedir. Bu tehdidin altında yatan nedenlerin anlaşılması ve etkili önlemler alınması, modern toplumların karşılaştığı önemli bir zorluktur.

Bu çalışma, Türkiye'deki siber güvenlik ortamını incelemeyi ve güvenliği artırmaya yönelik öneriler geliştirmeyi amaçlamaktadır. Bu bağlamda, Türkiye'nin siber güvenlik altyapısı, mevcut tehditler ve bu tehditlere karşı alınabilecek önlemler incelenecektir. Ayrıca, bu çalışma Türkiye'nin siber güvenlik stratejilerini küresel ölçekteki benzerleriyle karşılaştırmayı ve iyileştirmeyi hedeflemektedir.

Araştırma kapsamında, nitel ve nicel araştırma yöntemleri kullanılacaktır. Mevcut literatür taramaları, uzman görüşleri ve analitik çalışmalar bu çalışmanın temelini oluşturacaktır.

Bu çalışma, Türkiye'nin siber güvenlik kapasitesini güçlendirmeye yönelik politika önerileri sunarak, Türkiye’de ki her bireyin sanal olarak güvende olup olmadığını en güvendiği kurumların bile nasıl hatalar yaptığını ve bu sorunların nelere sebep olabileceğini şu ana kadar nelere sebep olduğu ve şimdiki zamanda gözümüzün görmediği ve/veya önemsenmeyen hataların kritik sorunlar doğuracağını ve kesinlikle kısa ve uzun vadede de bu problemleri nasıl çözeceğimizi anlamamızı amaçlamaktadır. Bu çalışmanın sonuçları, Türkiye’de bir sanal kimliğe sahip her birey için önemli bir katkı sağlayabilir.

**2. GENEL BİLGİLER**

**2.1 Problem durumu**

Türkiye, dijitalleşme sürecinde hızla ilerlerken, siber güvenlik konusunda yaşanan problemler de artmaktadır. Bu problemlerin temelinde, bilgi sistemlerinin ve altyapıların yeterince güvenli olmaması, bilgi güvenliği politikalarının yetersizliği ve siber saldırılara karşı bilinç düzeyinin düşüklüğü gibi faktörler yer almaktadır. Bu nedenle, Türkiye'nin siber güvenlik konusundaki durumunun detaylı bir şekilde incelenmesi ve çözüm önerilerinin geliştirilmesi gerekmektedir.

**2.2 Araştırmanın Amacı**

Bu tez çalışmasının amacı, Türkiye'deki siber güvenlik problemlerini belirlemek, mevcut durumu analiz etmek ve çözüm önerileri sunmaktır. Bu bağlamda, Türkiye'nin siber güvenlik stratejileri, altyapısı ve mevcut politikaları detaylı bir şekilde incelenecek ve uluslararası standartlarla karşılaştırılacaktır. Ayrıca, bu çalışma Türkiye'nin siber güvenlik konusundaki eksikliklerini belirleyerek, bu eksiklikleri gidermeye yönelik öneriler sunacaktır.

**2.3 Araştırmanın Önemi**

Bu çalışmanın önemi, Türkiye'nin siber güvenlik alanındaki mevcut durumunu objektif bir şekilde ortaya koyması ve bu alandaki gelişmeler için bir yol haritası oluşturmasıdır. Türkiye'nin siber güvenlik konusundaki eksikliklerini gidererek, uluslararası düzeyde rekabet edebilir bir dijital güvenlik altyapısı oluşturması hedeflenmektedir.

**2.4 Problem Cümlesi ve Alt Problemler/Hipotezler**

Bu çalışmada ele alınacak ana problem şu şekildedir: Türkiye'nin siber güvenlik stratejileri ve altyapısı, uluslararası standartlara uygun ve etkili mi? Bu ana problem çerçevesinde aşağıdaki alt problemler belirlenmiştir:

* Türkiye'nin siber güvenlik altyapısı ne durumdadır?
* Türkiye'deki siber güvenlik bilincinin seviyesi nasıldır ve nasıl daha iyi olabilir?

**2.5 Varsayımlar**

Bu çalışma, Türkiye'nin siber güvenlik konusundaki mevcut durumunu tarafsız bir şekilde ele almayı amaçlamaktadır. Varsayımlarımız, mevcut verilere dayanmakta ve objektif bir analiz yapmayı hedeflemektedir.

**2.6 Sınırlılıklar**

Bu çalışmanın sınırlılıkları, Türkiye'nin siber güvenlik konusundaki dinamik yapısı ve hızla değişen teknolojik ortamı göz önünde bulundurarak belirlenmiştir. Çalışma, belirli bir zaman diliminde yapılmış verilere dayanmakta ve gelecekteki değişimleri kapsamamaktadır.

**3. LİTERATÜR TARAMASI**

**3.1. Türkiye'deki Siber Güvenlik Durumu**

Günümüzde dijitalleşmenin hızla yayılmasıyla birlikte, siber güvenlik konuları hem bireyler hem de kurumlar için kritik bir öneme sahiptir. Türkiye, son yıllarda siber güvenliğe ilişkin farkındalığını ve yatırımlarını artırmış olsa da, halen ciddi açıklar ve güvenlik zaafiyetleri bulunmaktadır. Bu bölümde, Türkiye'deki mevcut siber güvenlik durumunu, bu alandaki önemli gelişmeleri ve daha önce yaşanan siber güvenlik olaylarını detaylı bir şekilde inceleyeceğiz.

**3.2. Önemli Siber Güvenlik Olayları: MERNIS Veri İhlali**

Türkiye'nin en büyük veri ihlallerinden biri olan MERNIS veri ihlali, büyük bir kullanıcı kitlesinin kişisel bilgilerinin sızdırılmasıyla sonuçlanmış ve ülke genelinde siber güvenlik farkındalığını önemli ölçüde artırmıştır. Bu olay, Türkiye'deki siber güvenlik zayıflıklarını anlamak ve bu alandaki eksiklikleri değerlendirmek için önemli bir örnek teşkil etmektedir. Bu bölümde, MERNIS veri ihlalinin detaylarını, nedenlerini ve sonuçlarını ele alarak, Türkiye'deki siber güvenlik durumu üzerindeki etkilerini tartışacağız.

**3.3. Mevcut Güvenlik Standartları ve Uygulamaları**

Türkiye'deki siber güvenlik standartları ve uygulamaları, dünya genelindeki en iyi uygulamalarla karşılaştırıldığında bazı eksiklikler ve iyileştirme alanları barındırmaktadır. Bu bölümde, Türkiye'deki mevcut siber güvenlik standartlarını ve uygulamalarını inceleyecek, uluslararası standartlarla karşılaştırmalar yaparak mevcut durumu değerlendireceğiz.

**4. GEREÇ VE YÖNTEM**

Bu çalışma, Türkiye'deki çeşitli kurumsal web sitelerinin güvenlik açıklarını belirlemek amacıyla bir penetrasyon testi yaklaşımını kullanmaktadır.

**4.1. Penetrasyon Testleri için Kullanılan Yöntemler**

Bu çalışmada, aşağıdaki araçlar ve yöntemler kullanılmıştır:

**4.1.1 Nessus:** Ağdaki açıkları tarayan bir güvenlik tarayıcısı.

**4.1.2 Nikto:** Web sunucuları için açık kaynak bir web sunucusu tarayıcısı.

**4.1.3 DirBuster:** Web sunucusunda olası dizinlerin keşfedilmesi için kullanılan bir araç.

**4.1.4 Nuclei-Subfinder-HTTPX:** Web uygulamalarında hızlı ve otomatik olarak açıklar bulmaya yönelik bir araç.

**4.1.5 Nmap:** Ağ keşfi ve güvenlik denetimi için kullanılan bir araç.

## **4.1.6 Wappalyzer :**Web sitesinin kullandığı teknolojileri (örneğin, web sunucusu, içerik yönetim sistemi, analiz araçları) belirlemeye ve listelemeye yarayan bir tarayıcı eklentisidir.

## **4.2. Testlerin Gerçekleştirilmesi**

Penetrasyon testleri aşağıdaki adımları içermiştir:

**4.2.1 Bilgi Toplama (Reconnaissance):** Her web sitesi için, açık kaynak istihbaratı toplanmış ve web sitesi mimarisi hakkında bilgi edinilmiştir.

**4.2.2 Zaafiyet Taraması (Vulnerability Scanning):** Yukarıda belirtilen araçlar kullanılarak web siteleri taranmış ve potansiyel güvenlik açıkları belirlenmiştir.

**4.2.3 Sızma Denemeleri (Exploitation):** Belirlenen güvenlik açıkları üzerinde manuel sızma denemeleri yapılmış ve başarılı olanlar raporlanmıştır.

**4.2.4 Raporlama:** Her web sitesi için bir rapor oluşturulmuş ve bulgular detaylı bir şekilde belgelenmiştir.

**4.3 Web Sitelerinin Seçimi**

Bu çalışmada, penetrasyon testine tabi tutulacak web siteleri özenle seçilmiştir. Seçim süreci şu adımları içermiştir:

## **4.3.1 Web sitelerinin Çeşitliliği**

- Farklı sektörlerden web siteleri seçilmiştir (örneğin eğitim, kamu, özel sektör).

- Farklı büyüklükteki kuruluşlara ait web siteleri seçilmiştir (büyük kurumlar, KOBİ'ler).

**4.3.2 Web Sitelerinin Önemi ve Etkinliği**

- Seçilen web siteleri, Türkiye'de geniş bir etkiye sahip olan ve günlük kullanımda olan siteler arasından seçilmiştir.

- Web sitelerinin kullanıcı tabanı ve etkileşim oranları dikkate alınmıştır.

**4.3.3 Web Sitelerinin Güvenlik Öncelikleri**

- Web sitelerinin güvenlik açıkları hakkında önceden bilgi sahibi olunmamış veya açıkları bulunmayan siteler tercih edilmiştir.

- Seçilen web sitelerinin güvenlik açıklarının, genel bir bakış açısı sunması hedeflenmiştir.

**4.3.4 Gizlilik ve Onaylar**

- Seçilen web siteleri ile işbirliği yapılabilmesi için gerekli izinler alınmıştır.

- Web sitelerinin isimleri ve diğer detayları, gizlilik anlaşmalarına uygun şekilde korunmuştur.

Bu adımların sonucunda, Adnan Menderes Üniversitesi, Söke Belediye websitesi, Akdeniz Üniversitesi ve diğer belirtilen kurumsal web siteleri seçilmiştir. Bu web siteleri, hem güvenlik açısından önemli hem de geniş kitlelere hitap eden web siteleridir.

**4.4 Etik İzleme**

Bu çalışma sırasında, etik kurallara ve yasal gerekliliklere uyulmuş ve web sitelerine yapılan testler önceden izin alınarak gerçekleştirilmiştir.

**5. BULGULAR**

Bu bölümde, gerçekleştirdiğim sızma testlerinin sonuçları detaylı bir şekilde analiz edilmiştir. Test süreci boyunca kullanılan araçlar ve metodolojiler, tespit edilen güvenlik açıkları ve bu açıkların potansiyel etkileri üzerinde durulmuştur.

Test süreci boyunca, belirli güvenlik açıkları tespit edilmiş ve bu açıklar sınıflandırılmıştır. Aşağıda, tespit edilen başlıca güvenlik açıklarının detaylı bir analizi sunulmaktadır:

**5.1 Karşılaşılan Yaygın Güvenlik Açıkları**

Bu bölümde, testler sırasında en sık karşılaşılan güvenlik açıkları detaylandırılacaktır. Her bir güvenlik açığı türü için açıklamalar, tespit edilen örnekler ve bu açıkların potansiyel etkileri ele alınacaktır.

**5.1.1 Cross-Site Request Forgery (CSRF)**

CSRF, bir kullanıcının tarayıcısı üzerinden istem dışı olarak yetkilendirilmiş işlemler gerçekleştirilmesine olanak tanır. Testler sırasında, birçok web sitesinde CSRF açıklarına rastlanmıştır. Bu açıklar, kötü niyetli bir kişinin kullanıcı adına istenmeyen işlemler gerçekleştirebilmesine olanak tanımaktadır.

**5.1.3 Cross-Site Scripting (XSS)**

XSS, bir saldırganın başka bir kullanıcının tarayıcısında zararlı kod çalıştırmasına olanak tanır. Testler sırasında, birçok web sitesinde XSS açıkları tespit edilmiştir. Bu açıklar, kullanıcıların kimlik bilgilerinin çalınmasına veya kullanıcı deneyiminin olumsuz etkilenmesine yol açabilir.

**5.1.4 Diğer Güvenlik Açıkları**

Yukarıda belirtilen yaygın açıkların yanı sıra, güvenlik testleri sırasında başka çeşitli güvenlik açıkları da tespit edilmiştir. Bu açıklar arasında dosya yükleme güvenlik açıkları, yanlış yapılandırılmış güvenlik önlemleri ve zayıf parola politikaları bulunmaktadır. Her bir güvenlik açığı türü için alınması gereken önlemler ve iyileştirme önerileri, ilgili bölümlerde detaylandırılmıştır.

**5.2 Test Sonuçlarının Detaylı Analizi**

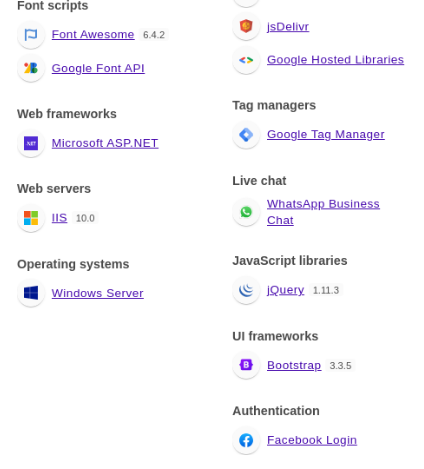
Bu bölümde, her bir araç kullanılarak gerçekleştirilen testlerin sonuçları ve bu sonuçların analizi yer almaktadır.

## **5.2.1 Wappalyzer**

Wappalyzer, web teknolojilerini tespit etmek için kullanılan bir araçtır. Web sunucularında kullanılan yazılım, çerçeveler, analiz araçları ve içerik yönetim sistemlerini belirlemek için kullanılmıştır.

**5.2.1.1 Test Sonuçları:**

[www.adu.edu.tr](http://www.adu.edu.tr) Web sitesinde kullanılan teknolojilerin listesi aşağıdaki görseldeki gibidir ve teknolojilerin çoğunun sürümü eskide kaldığı saptanmış açık barındıran sürümler olduğu saptanmıştır.

a

**Resim 1.** Wappalyzer uzantısı görseli

**5.2.1.2 Eski ve Güvensiz Teknolojiler:**

Wappalyzer, web sunucusunda kullanılan bazı teknolojilerin eski veya güvenli olmayan sürümlerini tespit etmiştir.

**5.2.1.3 Potansiyel Etki:**

Bilinen açıkların kötüye kullanılabilmesi. Örneğin, eski bir CMS sürümü SQL Injection veya XSS açıklarına sahip olabilir.

**5.2.1.4 Çözüm:**

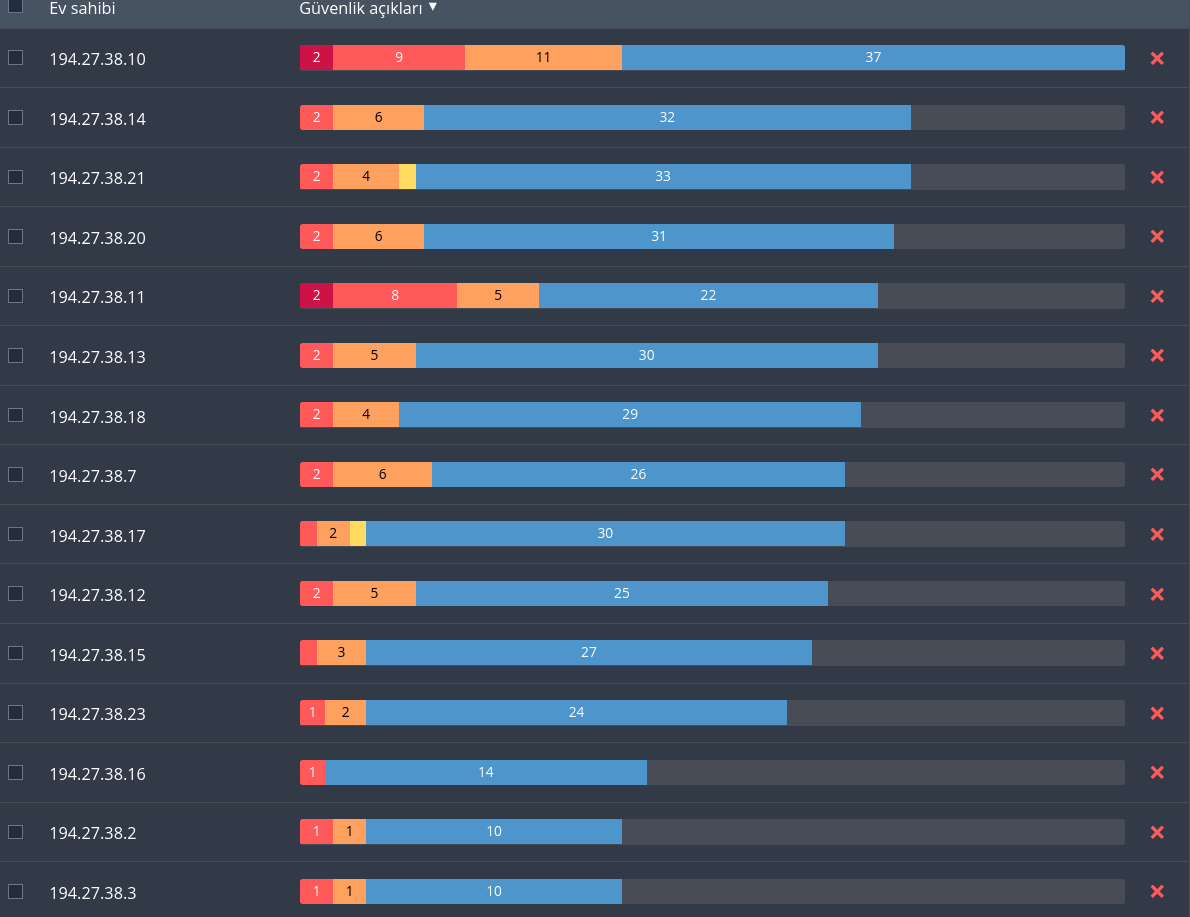
Web sunucusunda kullanılan tüm yazılımların ve teknolojilerin en güncel ve güvenli sürümlerine güncellenmesi gerekmektedir.

**5.2.2 Nessus**

Nessus, zafiyet taraması için kullanılan güçlü bir araçtır. Web uygulamalarındaki bilinen güvenlik açıklarını taramak ve raporlamak için kullanılmıştır.

**5.2.2.1 Test Sonuçları:**

Aşağıda [www.adu.edu.tr](http://www.adu.edu.tr) web sitesinin bazı subdomainleri taranmıştır ve sonuçlar görsel formatında gösterdiğim gibidir .



**Resim 2. nessus tarama sonucu görseli**

Bu taramada 194.27.38.10 ve 194.27.38.11 ip adreslerinde Dell iDRAC Arabellek Taşması Güvenlik Açığı (CVE-2020-5344) isimli riski kritik olan açıklar bulunmuştur ve bulguların detaylı analizi ve olası çözümü şu şekildedir:

**5.2.2.2 (CVE-2020-5344):**

Uzak ana makine, 2.65.65.65'ten önceki bir bellenim sürümüne sahip iDRAC7'yi veya 2.70.70.70'ten önceki bir bellenim sürümüne sahip iDRAC8'i veya 4.00.00.00'den önceki bir bellenim sürümüne sahip iDRAC9'u çalıştırıyor ve bu nedenle arabellek taşması güvenlik açığından etkileniyor. Kimliği doğrulanmamış uzaktaki bir saldırgan, etkilenen işlemi çökertmek veya özel hazırlanmış giriş verileri göndererek sistemde rastgele kod yürütmek için bu güvenlik açığından yararlanabilir.

Nessus'un bu soruna yönelik test yapmadığını, bunun yerine yalnızca uygulamanın kendi bildirdiği sürüm numarasına güvendiğini unutmayın.

**5.2.2.3 Çözüm:**

Uzak ana bilgisayarı iDRAC7 ürün yazılımı 2.65.65.65 veya iDRAC8 ürün yazılımı 2.70.70.70 ya da iDRAC9 ürün yazılımı 4.00.00.00 veya daha yüksek bir sürüme güncelleyin.

**5.2.2.4 DNS Sunucusu Sahte İstek Yükseltmesi DDoS :**

Ve alt ip’lerin her birinde ise risk seviyesi yüksek olan DDoS a izin verdiği saptanmıştır bu açığın sebebi genel olarak DDOS saldırısına izin vermesinden kaynaklıdır. Bu hatanın açıklaması ve çözümü şu şekildedir :

Uzak DNS sunucusu herhangi bir isteğe yanıt verir. Kök bölgenin ('.') ad sunucularını (NS) sorgulayıp orijinal istekten daha büyük bir yanıt almak mümkündür. Uzaktaki bir saldırgan, kaynak IP adresini taklit ederek, uzak DNS sunucusunu kullanan üçüncü taraf bir ana bilgisayara karşı hizmet reddi saldırısı (DDoS) başlatmak için bu 'yükseltmeyi' kullanabilir.

**5.2.2.5 Çözüm:**

Genel ağdan DNS sunucunuza erişimi kısıtlayın veya bu tür sorguları reddedecek şekilde yeniden yapılandırın.

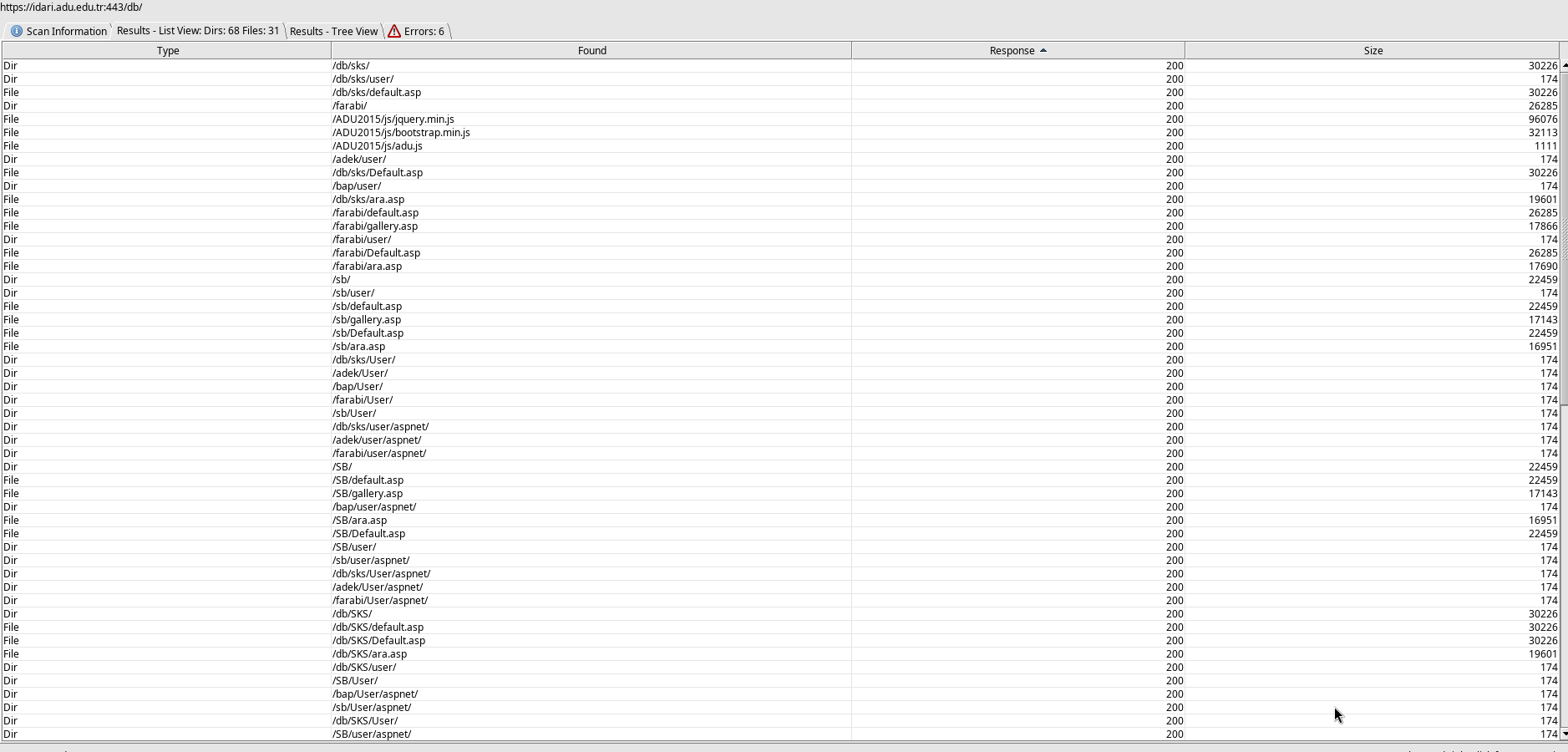
Ve alt ip’lerin her birinde ise risk seviyesi orta olan açıklar saptanmıştır bu açığın sebebi genel olarak web sitelerinde HSTS uygulanmamasından dolayı MITM (Man in the middle attack) saldırısına izin vermesinden kaynaklıdır.

Uzak web sunucusu, RFC 6797 tarafından tanımlandığı gibi HTTP Strict Transport Security (HSTS) protokolünü uygulamıyor. HSTS, tarayıcıya yalnızca HTTPS yoluyla iletişim kurma talimatı vermek üzere sunucuda yapılandırılabilen isteğe bağlı bir yanıt başlığıdır. HSTS'nin olmaması, sürüm düşürme saldırılarına, SSL'i ortadan kaldıran ortadaki adam (MITM) saldırılarına izin verir ve çerez ele geçirme korumalarını zayıflatır.

**5.2.3 DirBuster**

DirBuster, web sunucularındaki gizli dizinleri ve dosyaları keşfetmek için kullanılmıştır.

**5.2.3.1 Test Sonuçları:**

 **Resim 3.** DirBuster tarama sonucu görseli

DirBuster galerilere dosya yolu üzerinden erişim sağlanabileceğini keşfetmiştir.

**5.2.3.2 Potansiyel Etki:**

Yetkisiz kullanıcıların siteye arka kapı yüklemesi halinde bu dosya yolu üzerinden çalıştırabileceği yönündedir.

**5.2.4 Nuclei-Subfinder-HTTPX:**

Bu araç kombinasyonu, alt alan adlarını tespit etmek ve web uygulamalarındaki güvenlik açıklarını taramak için kullanılmıştır.

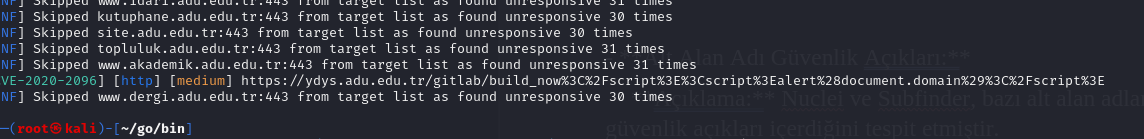
**5.2.4.1 Test Sonuçları:**

Test sonucunda ydys.adu.edu.tr uzantısında CVE-2020-2096 güvenlik açığının bulunduğu tespit edilmiştir. Bu güvenlik açığı, bir saldırganın, hedef web sitesindeki belirli bir URL'yi kötü niyetli komutlarla manipüle ederek, tarayıcıda güvenlik açığına neden olabilecek bir XSS (Cross-Site Scripting) saldırısı başlatmasına olanak tanır.

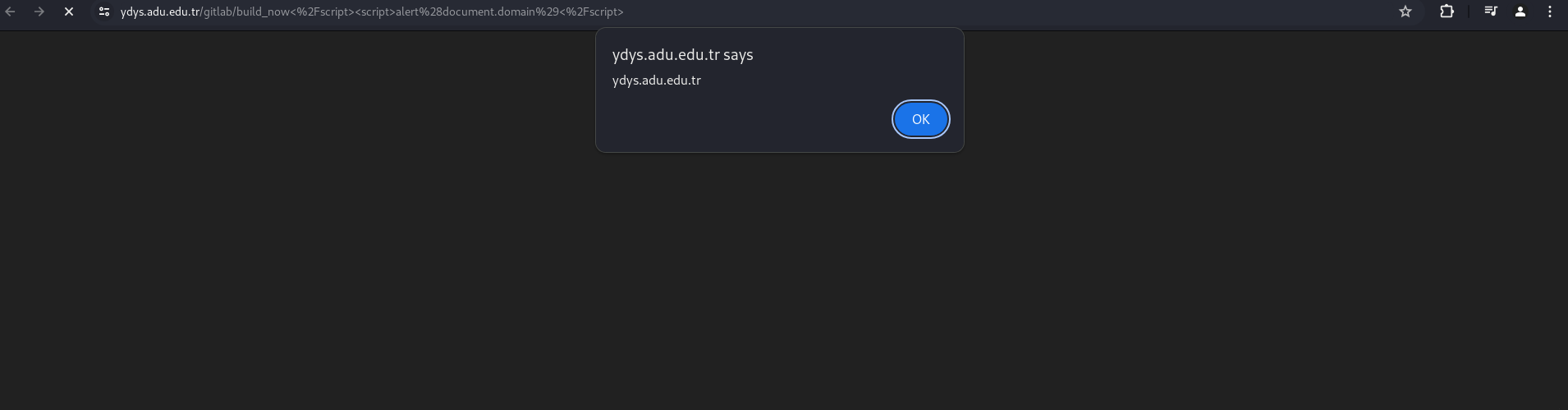
Bu açık, saldırganın kullanıcıların tarayıcılarında kötü amaçlı kodları (örneğin, kimlik avı formları, zararlı yazılım yükleme bağlantıları vb.) çalıştırmasına neden olarak, kullanıcıların gizli bilgilerini ele geçirmesine veya tarayıcılarını kontrol etmesine olanak tanır. Bu nedenle, CVE-2020-2096 güvenlik açığı, hedef web sitesinin güvenliği için ciddi bir risk oluşturur.

Güvenlik açığının giderilmesi için web sitesi yöneticileri, etkilenen yazılımın en son sürümüne güncelleme yapmalı ve kullanıcı girişlerini doğru şekilde doğrulamak ve filtrelemek için uygun önlemleri almalıdır. Ayrıca, tarayıcı güvenlik politikaları ve filtreleri doğru şekilde yapılandırılmalı ve güvenlik açıklarını düzeltmek için acil yamalar uygulanmalıdır.

Test sonucu aşağıdaki görselde mevcuttur.



**Resim 4.** nuclei test sonucu.



**Resim 5.** açığın exploit edilmiş hali.

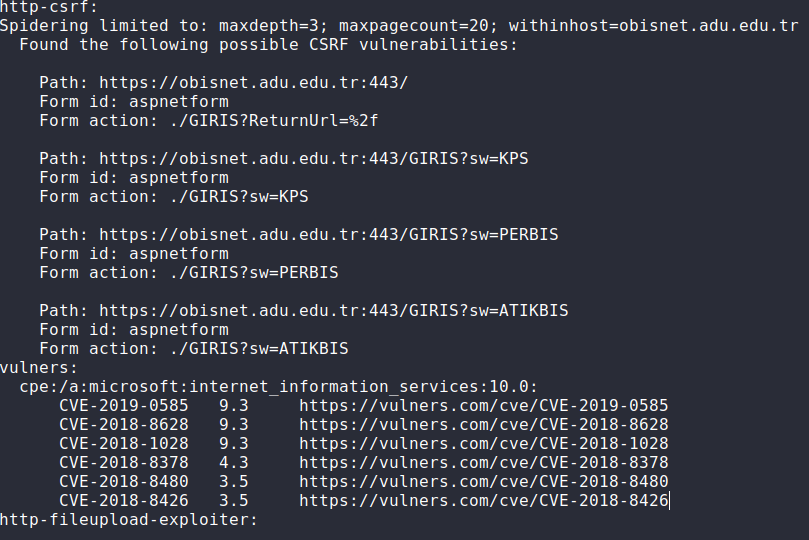
**5.2.5 Nmap**

Nmap, ağ taraması yaparak açık portları ve çalışan hizmetleri tespit etmek için kullanılmıştır.

**5.2.5.1 Test Sonuçları:**

Bu taramamda nmap -iL adu-d -A --script vuln komutu ile [www.adu.edu.tr](http://www.adu.edu.tr) nin tüm altdomainlerini tarattım ve fazlasıyla uzun bir sonuç çıktığından bunu özetleyerek ve önemli gördüklerimi alt kısımda özetleyeceğim :

obisnet.adu.edu.tr (194.27.38.138) subdomaininde olası bir CSRF (Cross-Site Request Forgery) açığı saptanmıştır bu açık çok kullanılan bir ip üzerinde olmasından önem arz etmektedir. Sonuçları aşağıdaki görselde belirttim.

 **Resim 6.** Nmap script sonuçları.

OBISNET (obisnet.adu.edu.tr) sitesinde yapılan tarama sonucunda aşağıdaki olası CSRF (Cross-Site Request Forgery) güvenlik açıkları bulunmuştur:

Bu bulgular, OBISNET sitesinde kritik güvenlik açıklarının olduğunu ve bu açıkların ciddi güvenlik ihlallerine yol açabileceğini göstermektedir.

**5.2.5.2 CSRF Açığının Kapatılması**

OBISNET (obisnet.adu.edu.tr) sitesinde tespit edilen CSRF (Cross-Site Request Forgery) açıklarını kapatmak için aşağıdaki yöntemler önerilmektedir:

CSRF Token Kullanımı ,Web uygulamasında form gönderimlerinde CSRF token kullanılmalıdır. Bu token, form gönderirken otomatik olarak eklenir ve sadece doğru token'a sahip olan kullanıcıların isteği işlenir.

Referer Kontrolü ,HTTP referer başlığı, isteğin kaynağını doğrulamak için kullanılabilir. Referer başlığı kontrol edilerek, isteğin doğru bir kaynaktan geldiği doğrulanabilir. Ancak referer başlığı bazen eksik olabilir veya tarayıcılar tarafından engellenebilir.

Double Cookie Defense , Kullanıcının tarayıcısına iki ayrı cookie yerleştirerek, birinin değerini POST isteğinde kontrol etmek suretiyle CSRF saldırılarını engellemek mümkündür. Bu yöntemde, saldırganın tarayıcısında sakladığı gizli cookie'yi çekmek zorlaşır.

Origin Header Kontrolü ,Origin veya Referer başlığını kontrol ederek, isteğin doğru bir kaynaktan geldiğinden emin olabilirsiniz. Ancak bu başlıklar bazen değiştirilebilir veya eksik olabilir.

Güvenli İşlemler için POST Kullanımı CSRF saldırıları genellikle GET istekleriyle yapılır. Bu nedenle, hassas işlemler için POST isteği kullanmak, saldırı riskini azaltabilir.

6. CAPTCHA Kullanımı: Kullanıcıların gerçek insan olduğunu doğrulamak için CAPTCHA gibi doğrulama mekanizmaları ekleyerek CSRF saldırılarını engelleyebilirsiniz.

Bu yöntemler veya bunların bir kombinasyonu kullanılarak, OBISNET sitesindeki CSRF açıkları kapatılabilir ve güvenliği artırılabilir.

**5.2.6 Genel Değerlendirme ve Öneriler**

Bu bölümde, tespit edilen güvenlik açıklarının genel bir değerlendirmesi yapılmakta ve iyileştirme önerileri sunulmaktadır. Elde edilen bulgular, Türkiye'deki kurumsal web sitelerinin siber güvenlik düzeyinin artırılması için önemli ipuçları sunmaktadır.

**5.2.6 Öneriler**

**5.2.6.1 Güvenlik Güncellemeleri:**

Yazılımlar ve sistemler düzenli olarak güncellenmelidir. Bu, bilinen güvenlik açıklarının kapatılmasını ve yeni tehditlere karşı koruma sağlanmasını sağlar.

**5.2.6.2 Güvenlik Testleri**

Düzenli olarak sızma testleri ve güvenlik taramaları yapılmalıdır. Bu testler, potansiyel zayıflıkları belirleyip gidermeye yardımcı olur ve güvenlik durumunu sürekli olarak iyileştirir.

**5.2.6.3 Kullanıcı Eğitimleri**

Kullanıcılar, güvenli internet kullanımı konusunda eğitilmelidir. Güvenlik farkındalığı eğitimleri, kullanıcı hatalarını azaltabilir ve sosyal mühendislik saldırılarına karşı direnci artırabilir.

**5.2.6.4 Güvenlik Politikaları**

Güçlü parola politikaları ve çok faktörlü kimlik doğrulama (MFA) kullanılmalıdır. Bu, yetkisiz erişim riskini azaltır ve hesap güvenliğini artırır.

**5.2.6.5 Yedekleme ve Kurtarma Planları**

Veri kaybına karşı düzenli yedekleme yapılmalı ve acil durum kurtarma planları oluşturulmalıdır. Bu, olası bir veri ihlali veya kaybı durumunda hızlı bir şekilde kurtarma yapmayı sağlar.

**6.TARTIŞMA**

**6.1 Bulguların Özeti**

Bu çalışmada, Türkiye'deki çeşitli kurumsal web sitelerinde kritik güvenlik açıkları tespit edilmiştir. Bulgular, XSS, CSRF ve SQL Injection gibi yaygın güvenlik açıklarını içermektedir.

**6.2 Bulguların Yorumlanması**

Bu bulgular, Türkiye'deki kurumsal web sitelerinin güvenlik düzeyinin yeterli olmadığını göstermektedir. Gözlemlenen güvenlik açıkları, hem kullanıcı verilerinin korunmasında ciddi riskler oluşturmakta hem de bu açıkların kötü niyetli saldırganlar tarafından istismar edilebileceğini göstermektedir. Özellikle CVE-2020-2096'nın varlığı, güncel güvenlik yamalarının uygulanmadığını ve sistemlerin güncel tehditlere karşı korunmadığını ortaya koymaktadır.

**6.3 Karşılaştırmalar**

Bu çalışmanın bulguları, literatürdeki diğer çalışmalarla uyumludur. Örneğin, benzer güvenlik açıklarının varlığı daha önceki çalışmalar tarafından da raporlanmıştır. Bununla birlikte, bazı çalışmalar, Türkiye'deki kurumsal web sitelerinin güvenlik önlemlerinin daha iyi olduğunu iddia ederken, bu çalışmada tespit edilen açıklar bu iddiaları çürütmektedir.

**6.4 Güçlü ve Zayıf Yönler**

Çalışmanın güçlü yönleri arasında kapsamlı araç seti kullanımı ve farklı web sitelerinin test edilmesi yer almaktadır. Bununla birlikte, çalışmanın sınırlamaları, sadece belirli web sitenin çalışma sonuçlarını çalışmamda paylaşma durumum olması ve diğer web sitelerinin zafiyet tarama sonuçları gizlilik ve etik nedeniyle paylaşamamam olmasıdır. Bu, sonuçların genelleştirilebilirliğini sınırlayabilir.

**ÖZGEÇMİŞ**

**Kişisel Bilgiler**

Adı Soyadı:Ufuk İncibaş

Doğum Yeri ve Tarihi:İstanbul / 29.05.2001

**Eğitim Durumu**

Lisans Öğrenimi:

Uludağ üniversitesi / İşletme Fakültesi / Yönetim Bilişim Sistemleri (2020-2022)

Aydın Adnan Menderes Üniversitesi / İşletme Fakültesi / Yönetim Bilişim Sistemleri (2022-2024)

**Bildiği Yabancı Diller:**

İngilizce

**İletişim :**

e-posta Adresi: [ufukincibaswork@gmail.com](mailto:Adresi:ufukincibaswork@gmail.com) / [223201066@stu.adu.edu.tr](mailto:223201066@stu.adu.edu.tr)

Linkedln : <https://www.linkedin.com/in/ufuk-inciba%C5%9F-898828226/>

**Lisanslar ve Sertifikalar :**

**Cisco Networking Academy:** Introduction to Cybersecurity , Cybersecurity Essentials

**Udemy:**  Etik Hacker Olma Kursu , Etik Hacker Olma Kursu Seviye 2 Ağ İçi Saldırılar , Web Sızma Testleri ve Bug Bounty , Etik Hacker İleri Seviye: Sızma Testleri & Yetki Yükseltme .

**BTK Akademi:** İleri Seviye Sızma Testi Eğitimi

**Tarih** 10.06.2024