**T.C.**

**SAKARYA ÜNİVERSİTESİ**

**BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ**

BSM 498 BİTİRME ÇALIŞMASI

**WEB SECURİTY PENTEST TOOL**

**UYGULAMASI**

**RAPOR-4**

**B181210030 – VEDAT ARSLAN**

**Fakülte Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ**

**Tez Danışmanı : Prof.(Doç.) Dr. İbrahim Özçelik**

**2023-2024 Bahar Dönemi**

**İÇİNDEKİLER**

|  |  |  |
| --- | --- | --- |
| BÖLÜM 4. WEB UYGULAMA GÜVENLİĞİ |  |  |
| 4.1 Web Uygulama Güvenliği Neden Önemlidir................................................ |  | 2 |
| 4.1.1 Veri İhlalleri ……………………………………………………… |  | 2 |
| 4.1.2.Web Uygulama Zafiyetleri ...…………………………………….. |  | 2 |
| 4.1.3 DDoS Saldırıları………………………………………………….. |  | 2 |
| 4.1.4 Fidye Yazılımı ………………….................................................… |  | 3 |

4.1.5 İnsan Hataları……………………………………………………… 3

4.2 Uygulamanın Avantajları Nelerdir?................................................................. 3

4.3 Uygulama Pazarlama Aşamaları…………………………………………….. 4

4.4 Sonuçlar ve Öneriler………………………………………………………… 5

4.5 Kaynakça…………………………………………………………………….. 6

**BÖLÜM 4. WEB UYGULAMA GÜVENLİĞİ**

Günümüzde web güvenliği büyük bir öneme sahiptir ve yaygın olarak kullanılmaktadır. İnternetin ve dijital teknolojilerin yaygınlaşmasıyla birlikte, web üzerindeki tehditler ve saldırılar da artmıştır. Bu nedenle, web güvenliği önlemleri ve çözümleri büyük bir gereklilik haline gelmiştir.2

**4.1 Web Uygulama Güvenliği Neden Önemlidir?**

Web uygulama güvenliği, hem kullanıcıların hem de işletmelerin güvenliğini sağlamak ve veri ihlallerini önlemek için hayati öneme sahiptir. Uygulamaların güvenliği sağlandığında, kullanıcılar güvenli bir ortamda işlem yapabilir, kişisel verilerini güvende tutabilir ve dolandırıcılık veya veri kaybı gibi risklere maruz kalmazlar. Aynı zamanda şirketler, güvenilirliklerini artırabilir, itibarlarını koruyabilir ve yasal düzenlemelere uyum sağlayarak cezai ve hukuki sorunlarla karşılaşma riskini azaltabilirler. Web güvenliğin neden önemli olduğuna dair bazı nedenler ve istatistikleri paylaşılmıştır.

1.Veri İhlalleri:

2.Web Uygulama Zafiyetleri:

3.DDoS Saldırıları:

4.Fidye Yazılım(Ransomware):

5. İnsan Hataları

6. ….

**4.1.1 Veri İhlalleri**

2020 yılında, Verizon tarafından yapılan bir araştırmaya göre, veri ihlallerinin %80'i hedef organizasyonun zayıf parola kullanımı nedeniyle gerçekleşti. İhlal edilen veri türleri arasında en yaygın olanlar kişisel kimlik bilgileri (%58), tıbbi veriler (%36) ve mali bilgiler (%12) olarak belirtilmiştir. En büyük veri ihlali vakalarından biri 2020'de Marriott otel zinciri tarafından bildirildi. Bu olayda, yaklaşık 5.2 milyon müşterinin kişisel bilgileri ihlal edildi.

**4.1.2 Web Uygulama Zafiyetleri**

2020 yılında yapılan bir OWASP raporuna göre, en yaygın web uygulama zafiyetleri arasında XSS (Cross-Site Scripting), SQL enjeksiyonu, hassas verilerin yanlış yapılandırılması ve kimlik doğrulama sorunları yer alıyor. XSS saldırıları, web uygulamalarında bulunan güvenlik açıklarını kullanarak saldırganların kullanıcılara zararlı kod enjekte etmelerini sağlar. Bu tür saldırıların %65'inden fazlası hala mevcuttur.

**4.1.3 DDoS Saldırıları**

Verisign tarafından yapılan bir araştırmaya göre, 2020'de DDoS saldırıları %154 arttı.İş dünyasında DDoS saldırılarının yıllık maliyeti ortalama olarak 2 milyon dolara ulaştı.IoT (Nesnelerin İnterneti) cihazlarının artması, DDoS saldırıları için yeni birer hedef haline gelmelerini sağladı.

**4.1.4 Fidye Yazılımı**

2020 yılında yapılan bir McAfee raporuna göre, fidye yazılımı saldırıları %165 artarak rekor seviyeye ulaştı. Fidye yazılımı saldırıları, genellikle e-posta yoluyla yayılan kötü niyetli dosyalar veya bağlantılarla gerçekleştirilir.Kulanıcının dosyaya veya sistemine erişimi engeller. Ransomware saldırıları, kuruluşlara büyük mali kayıplar ve itibar zedelenmesi riski taşır.

**4.1.5 İnsan Hataları**

IBM tarafından yapılan bir araştırmaya göre, web tabanlı saldırılara neden olan güvenlik açıkları arasında en yaygın olanlar, kullanıcıların zayıf parolalar kullanması (%85), doğrulama bilgilerini paylaşması (%55) ve kötü niyetli bağlantılara tıklaması (%30) olarak belirlenmiştir.Şirketlerin çalışanlarına yönelik güvenlik farkındalık eğitimleri, bu tür hataların azaltılmasına yardımcı olabilir.

**4.2 Uygulamanın Avantajları Nelerdir?**

* Uygulamayı kullanan kullanıcı brute force atağın nasıl bir şekilde gerçekleştiğini görebildiği için güçlü şifre kullanması gerektiğini anlar.
* Web te oluşan zafiyetleri ve etkilerini uygulamada canlı olarak görüp test edeceği için verilerini tuttuğu server da verilerin şifreli halde kalması gerektiğini anlar bu sayede verinin gizliliği ve bütünlüğü sağlanmış olur. Web uygulaması varsa kullanıcının, client tarafından gelen istekleri filtreleyebilir yada uygulama ve client arasında gelen isteklerin zararlı olup olmadığını anlamak için WAF(Web Application Firewall) kullanabilir.
* Kullanıcı uygulamamızda kendi web sitesinin varsa açık portlarında DoS saldırısı test edebilir. Eğer istekler, site server bandgenişliği aşarsa web server hizmeti sonlanabilir bu da müşteri kaybına sebep olabilir. Kullanıcı bunun için önlemler alabilir.
* Kullanıcı uygulamamızı kullandığında gerçek kullanıcı ile bot arasında farkı anlayabilir ve bunun için önlemler alabilir.Uygulamamızda Usomdan aldığımız zararlı domainlerle kullanıcı oltalama saldırıları hakkında bilgi edinebilir.
* Owasp Top Tenden güncel olarak veri çektiğimiz için kullanıcı en son hangi zaafiyetlerin olduğunu ve zafiyetlerin CVE skorlarını görebilir.
* Uygulamamız kullanıcı için iyi bir eğitim ve farkındalık sağlar.

**4.3 Uygulama Pazarlama Aşamaları**

**1.Hedef Kitleyi Belirlemek**

Etik Hackerlar, Güvenlik Uzmanları, Geliştiriciler, Web Sitesi Sahipleri, Öğrenciler ve Araştırmacılar

**2.Rekabet Analizi:**

Burp Suite, OWASP Zap, Nessus, Acunetix gibi pentest araçları için rekabet sağlayabilirmiyiz ve bizim uygulamamızın diğer araçlardan farkı nedir ve değerini belirleme

**3. Marka Oluşturma**

Uygulamamız için güçlü bir marka oluşturmalıyız. İyi bir logo, renk paleti ve marka kimliğiyle kullanıcıların dikkatini çekebiliriz. Markamızı etkili bir şekilde iletmek için tutarlı bir marka diline ve mesajlaşmaya sahip olmalıyız.

**4.Dijital Pazarlama**

İnternet ve dijital kanalları kullanarak uygulamamızı pazarlamalıyız. Bir web sitesi oluşturmalıyız, sosyal medya platformlarında aktif olmalıyız, blog yazıları ve içerik üretin, e-posta pazarlaması yapmalıyız, SEO (arama motoru optimizasyonu) çalışmaları yapın ve dijital reklamlar kullanmalıyız. Kullanıcıların uygulamamızı bulmalarını ve indirmelerini sağlamak için etkili bir dijital pazarlama stratejisi oluşturmalıyız.

**5.İçerik Pazarlaması**

Kullanıcıları eğitmek, bilgilendirmek ve etkilemek için içerik pazarlaması yapmalıyız. İlgili blog yazıları, video içerikleri, e-kitaplar veya beyaz kağıtlar gibi içerikler üreterek, hedef kitlenizin sorunlarına çözümler sunarak uygulamamızın değerini arttırmalıyız

**6.İşbirlikleri ve Ortaklıklar:**

İlgili sektördeki diğer firmalarla işbirlikleri ve ortaklıklar kurmalıyız. Bu, uygulamamızın daha geniş bir kitleye ulaşmasına ve kullanıcılara sunulmasına yardımcı olur.

**7. Test ve Doğrulama**

Uygulamamızı geliştirme sürecinin son aşamasında kapsamlı bir şekilde test etmeliyiz. Bu, uygulamanın tüm işlevlerini doğru bir şekilde yerine getirdiğini, beklenen sonuçları ürettiğini ve güvenlik açıklarının bulunmadığını doğrulamak için gereklidir.

**8. Canlı Ortama Çıkması**

Gerekli testler ve denetimden başarılı bir gözlem elde edersek uygulamamamız canlı ortama hazır hale gelir.

**9. Yama Güncellemeleri**

Uygulamamızda güvenlik açıklarını düzeltmek veya performansı iyileştirmek için yama güncellemeleri yapmalıyız.

**4.4 Sonuçlar Ve Öneriler**

**Sonuçlar:**

* Yapılan pentest testleri sonucunda uygulamanın güvenlik açıkları ve zafiyetleri tespit edilmiştir.
* Tespit edilen güvenlik açıkları arasında XSS (Cross-Site Scripting), SQL enjeksiyonu ve kimlik doğrulama sorunları gibi yaygın web uygulama zafiyetleri bulunmaktadır.
* Tespit edilen güvenlik açıkları, saldırganların uygulamaya zararlı kod enjekte etmesine, hassas verilerin sızdırılmasına veya yetkisiz erişime olanak sağlayabilir.

**Öneriler:**

* XSS zafiyetlerini önlemek için uygulama içinde giriş verilerinin doğru bir şekilde filtrelenmesi ve kullanıcıdan gelen verilerin güvenli bir şekilde işlenmesi gerekmektedir.
* SQL enjeksiyonu zafiyetlerini önlemek için veritabanı sorgularının parametreleştirilmesi veya doğru bir şekilde kaçış karakterleriyle işlenmesi önemlidir.
* Kimlik doğrulama sorunlarını gidermek için güçlü parola politikaları, iki faktörlü kimlik doğrulama ve oturum süresi yönetimi gibi önlemler alınmalıdır.
* Uygulamada kullanılan kütüphaneler ve bileşenler güncel tutulmalı ve yaygın olarak bilinen güvenlik açıklarına karşı düzenli olarak taranmalıdır.
* WAF (Web Application Firewall) gibi güvenlik önlemleri uygulanarak zararlı isteklerin engellenmesi ve güvenlik filtreleme yapılması sağlanmalıdır.

Bu öneriler, uygulamanın güvenliğini artırmak ve tespit edilen zafiyetleri gidermek için alınabilecek önlemlerdir. Bunların uygulanmasıyla kullanıcılar, uygulamayı daha güvenli bir şekilde kullanabilir ve potansiyel saldırılardan korunabilir.

**4.5 Kaynakça**

<https://docs.python.org>

<https://peps.python.org>

<https://pypi.org>

<https://stackoverflow.com/questions/tagged/python>

<https://www.riverbankcomputing.com/static/Docs/PyQt5/>

<https://www.btkakademi.gov.tr>

[Web-Uygulama-Guevenligi-Bir-Oernek-Calisma-Web-Application-Security-A-Case-Study.pdf (researchgate.net)](https://www.researchgate.net/profile/Fatih-Kilic-5/publication/341266898_Web_Uygulama_Guvenligi_Bir_Ornek_Calisma_Web_Application_Security_A_Case_Study/links/5eb6990a299bf1287f77f64d/Web-Uygulama-Guevenligi-Bir-Oernek-Calisma-Web-Application-Security-A-Case-Study.pdf)

[Karaarslan.pdf (mu.edu.tr)](http://acikerisim.mu.edu.tr/xmlui/bitstream/handle/20.500.12809/10210/Karaarslan.pdf?sequence=3&isAllowed=y)

<https://owasp.org>

<https://www.nist.gov>

[www.sans.org](http://www.sans.org)

<https://enterprise.verizon.com/resources/reports/dbir>

<https://www.symantec.com/security-center/threat-report>

<https://www.mcafee.com/enterprise/en-us/threat-center/threat-reports.html>