**VulnMyWebsite Sızma Testi Raporu**

**Rapor Tarihi:** 13.04.2024

**Hazırlayan:** Melike TEPELİ

**1.Bulgu Adı: NoSQL Injection**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Kritik | <http://10.10.11.18:5000> | Müşteri, Satıcı | /login | Burp Suite |

**Zafiyetin Etkisi**

* Saldırgan, NoSQL veritabanına zararlı sorgular enjekte ederek yetkisiz veri okuma/değiştirme yapabilir.
* Kimlik doğrulama atlatma veya kritik bilgilere erişim mümkün olabilir.

**Zafiyetin Açıklaması**

1. Parametre doğrulama yetersizliği nedeniyle uygulama, kullanıcıdan gelen verileri doğrudan NoSQL sorgularında kullanıyor.
2. Gelen parametrelerde özel karakterler veya dizi formatları kullanılarak veritabanında istenmeyen sorgu sonuçları elde edilebilir.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Çözüm Önerisi**

**1. Input Doğrulama:** Kullanıcı girdilerini mutlaka filtreleyin veya tip denetimi (örneğin yalnızca beklenen formatta JSON vb.) uygulayın.

**2. Parametrik Sorgular:** ORM veya benzeri bir katman kullanarak parametreli sorgular oluşturun.

**Referanslar**

<https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05.6-Testing_for_NoSQL_Injection>

**2.Bulgu Adı: Sensitive Information Disclosure**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Kritik | <http://10.10.11.18:5000> | Müşteri, Satıcı | / | Burp Suite |

**Zafiyetin Etkisi**

* .env gibi dosyalar okunarak veritabanı bilgileri dâhil hassas bilgilere ulaşılabilir.
* Saldırgan, uygulamanın çalıştığı sunucuda kritik yapılandırma dosyalarını okuyup daha büyük ölçekli saldırılar gerçekleştirebilir.

**Zafiyetin Açıklaması**

* Giriş yapmış herhangi bir kullanıcının, sunucunun dosya sistemindeki belirli dosyalara erişebilmesine izin verilmektedir.
* .env dosyasını okuyabildik.
* Bu sayede veritabanı bilgilerine erişilebilir ve bu veritabanında değişiklik yapılabilir.

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

**Çözüm Önerisi**

1. **Parametre Temizleme:** Dosya yollarına ilişkin parametreler mutlaka temizlenmeli veya sabit, izinli bir dizinle sınırlanmalı.
2. **İlkeler ve İzinler:** Uygulamanın okuma/yazma yetkileri kısıtlanarak sistem dosyalarına erişim engellenmeli.

**Referanslar**

<https://owasp.org/Top10/A05_2021-Security_Misconfiguration/>

<https://owasp.org/Top10/A01_2021-Broken_Access_Control/>

**3.Bulgu Adı: Cryptographic Failures**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Kritik | <http://10.10.11.18:5000> | Müşteri, Satıcı | /login | Burp Suite |

**Zafiyetin Etkisi**

* Parolaların depolanırken düzgün bir şekilde şifrelenmemesi veya zayıf kriptografik algoritmaların kullanılması nedeniyle oluşur. Bu tür hatalar, şifrelerin, kişisel bilgilerin veya diğer hassas verilerin ele geçirilmesine, manipüle edilmesine veya çalınmasına yol açabilir.

**Zafiyetin Açıklaması**

Parolalar, şifrelenmeden (plaintext) veritabanında saklanıyor.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer code

AI-generated content may be incorrect.

Veriler, HTTP üzerinden iletilmiş. Bu, şifrelerin ağ üzerinde şifrelenmeden gönderildiği ve dinlenebileceği anlamına gelir.

**Çözüm Önerisi**

1. **Hashleme:** Parolalar bcrypt,argon gibi algoritmalarla hashlenmelidir. Veritabanına erişimi sınırlamak ve sadece yetkilendirilmiş kullanıcıların verilere erişmesine izin vermek gerekir.
2. **HTTTPS:** Sunucu ile istemci arasındaki iletişim trafiği HTTPS üzerinden sağlanmalıdır.

**Referanslar**

<https://owasp.org/Top10/A02_2021-Cryptographic_Failures/>

**4.Bulgu Adı: Weak Password Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Kritik | <http://10.10.11.18:5000> | Müşteri, Satıcı | /login | Burp Suite |

**Zafiyetin Etkisi**

* Zayıf parola politikaları, kötü niyetli kişiler tarafından hızlıca tahmin edilebilir. Bu tür şifreler, özellikle brute-force saldırılarına karşı savunmasızdır. Bu tür parolalar kullanıcının hesabını, güvenlik ve gizlilik açısından ciddi şekilde tehlikeye atar.

**Zafiyetin Açıklaması**

* Kötü niyetli kullanıcıların sistemin zayıf şifre politikasından yararlanarak, otomatik araçlarla binlerce şifreyi hızla deneyerek başarıya ulaşmalarına olanak sağlar.
* Burp isteğine baktığımızda, kullanıcı "eliftepeli" için "123" gibi basit bir şifre kullanılarak giriş yapılmaktadır. Tek haneli (ya da çok kısa) şifrelerin kabul edilmesi, doğru bir şifre politikası olmadığına işaret eder. Bu durumun temel sorunu, şifrenin güçsüz olması ve kötü niyetli birinin kolayca bu şifreyi tahmin etme veya brute-force saldırıları ile hesabı ele geçirme riskini taşımaktadır.

A screenshot of a computer

AI-generated content may be incorrect.

**Çözüm Önerisi**

**1. Minimum uzunluk:** Minimum parola uzunluğu 8 karakter olarak belirlenmelidir.

**2. Karmaşıklık Gereksinimleri:** Büyük harf, küçük harf, rakam ve özel karakter kontrolü olmalıdır. Parolaların basit olmasını engeller ve brute-force saldırılarının etkinliği azaltır.

**3. Çok Faktörlü Kimlik Doğrulama (MFA):** Şifreye ek olarak MFA (Multi-Factor Authentication) uygulanması, sadece şifrenin yeterli olmadığı ve ek bir güvenlik katmanının eklenmesi gereken durumları sağlar.

**Referanslar**

<https://owasp.org/Top10/A02_2021-Cryptographic_Failures/>

**5.Bulgu Adı: Business Logic Flaw**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Kritik | <http://10.10.11.18:5000> | Müşteri, Satıcı | /add-to-cart,/carts, /my-orders | Burp Suite |

**Zafiyetin Etkisi**

* Kullanıcı, sepetinde veya sipariş detayında “total amount” gibi değerleri manipüle ederek ödemeyi değiştirebilir.
* Bu değişiklik satıcının “orders” sayfasına da yansıyarak finansal zarara yol açabilir.

**Zafiyetin Açıklaması**

* Uygulama, kritik iş süreçlerinde (ör. sepet hesaplaması) sunucu yerine istemciden gelen parametrelere güveniyor.
* Burp Suite ile parametreler değiştirildiğinde uygulama bu değerleri sorgusuz kabul edip işliyor.

Kullanıcı sepetine bu şekilde ürün ekledi :

A screenshot of a computer

AI-generated content may be incorrect.

Burp ile bu verinin total amount u degistirilebildi.

A screenshot of a computer

AI-generated content may be incorrect.

Burada olan degısıklık urunun sahıbı olan kullanıcının urunler ve orders sayfasına da yansıdı:

A screenshot of a computer

AI-generated content may be incorrect.

Satıcının orders sayfasına da yansıyor :

A screenshot of a computer

AI-generated content may be incorrect.

**Çözüm Önerisi**

1. **Sunucu Taraflı Doğrulama:** Fiyat, miktar, toplam tutar gibi değerler mutlaka sunucu tarafında yeniden hesaplanmalı veya doğrulanmalı.
2. **İş Kuralları Kontrolleri:** İş mantığıyla ilgili bütün kritik adımlarda yetki ve tutarlılık denetimi yapılmalı.

**Referanslar**

<https://owasp.org/www-community/vulnerabilities/Business_logic_vulnerability>

**6.Bulgu Adı: Stored XSS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Kritik | <http://10.10.11.18:5000> | Müşteri, Satıcı | /add-products | Burp Suite |

**Zafiyetin Etkisi**

* Kullanıcının girdiği zararlı JavaScript kodları veritabanında saklanıp, diğer kullanıcılara görüntülendiğinde tarayıcıda otomatik çalıştırılabilir.
* Çerez çalma, oturum kaçırma veya kullanıcı eylemleri taklit etme gibi saldırılara yol açabilir.

**Zafiyetin Açıklaması**

* Web uygulaması, kullanıcı tarafından gönderilen verileri (ör. mesaj vb.) doğrudan A screenshot of a computer

  AI-generated content may be incorrect.saklıyor.
* Sunum aşamasında (sayfa görüntülenirken) veri filtrelenmeden yazıldığı için zararlı kodlar çalıştırılabiliyor.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Çözüm Önerisi**

1. **Input Validation & Output Encoding:** Girilen verileri saklamadan önce kontrol edin ve gösterirken HTML özel karakterlerini uygun biçimde encode edilebilir.
2. **HTML Sanitizer:** Kullanıcı girdilerine izin verilen etiketler sınırlanmalı (ör. <b>, <i> haricinde HTML etiketlerine izin verilmemeli).

**Referanslar**

<https://owasp.org/www-community/attacks/xss/>

**7.Bulgu Adı: Cookie Stealing (Unrestricted File Upload + Stored XSS)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Kritik | <http://10.10.11.18:5000> | Müşteri, Satıcı | /my-addresses | Burp Suite |

**Zafiyetin Etkisi**

* Zararlı HTML (xss.html) dosyası yüklenerek, oturum çerezleri (cookies) çalınabilir.
* Saldırgan, diğer kullanıcıların session bilgilerini ele geçirerek yetkisiz hesap erişimi sağlayabilir.

**Zafiyetin Açıklaması**

* Uygulamada MIME Type kontrolü bulunmaması nedeniyle .html uzantılı dosyalar yüklenebilmektedir.
* Yüklenen dosya içerisinde bulunan zararlı JavaScript kodları, uygulamaya giriş yapan kullanıcıların oturum cookie bilgilerini saldırganın belirttiği (örneğin http://16.171.42.24) sunucuya gönderir.

A screenshot of a computer

AI-generated content may be incorrect.

* Farklı kullanıcı olarak giriş yapıldığında bile, çalınan cookie veya parametreler (username, userID gibi değerler) manipüle edilerek başkasının hesabına ait bilgiler görüntülenebilmektedir.

A screenshot of a computer

AI-generated content may be incorrect.

**Çözüm Önerisi**

1. **Dosya Yükleme Kısıtlamaları:** Sunucu tarafında MIME Type ve dosya uzantısı kontrolleri uygulanmalı, zararlı içerik yüklenmesi engellenmeli.
2. **Oturum Yönetimi:** Oturum çerezlerinin çalınması riskine karşı HttpOnly, Secure ve SameSite flagleri etkinleştirilmeli.

**Referanslar**

<https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload>

<https://owasp.org/www-community/attacks/xss/>

**8.Bulgu Adı: IDOR (Insecure Direct Object References)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Kritik | <http://10.10.11.18:5000> | Müşteri, Satıcı | /cards, /carts | Burp Suite |

**Zafiyetin Etkisi**

* Kullanıcı, URL’deki parametreleri (ör. ?id=19) değiştirerek farklı kullanıcılara ait verilere erişebiliyor.
* Farklı hesapların hassas bilgileri (örneğin siparişler, kart bilgileri vb.) görüntülenebiliyor.

**Zafiyetin Açıklaması**

* Uygulama, kullanıcının eriştiği kaynağın (ör. id=19) gerçekten o kullanıcıya ait olup olmadığını kontrol etmiyor.
* Intruder kullanılarak farklı ID değerleri denendiğinde, 200 OK yanıt veren sayfalarda başkalarının verileri görülebiliyor.

A screenshot of a computer

AI-generated content may be incorrect.

**Çözüm Önerisi**

1. **Yetkilendirme Kontrolü:** Her istekte, talep edilen kaynağın o kullanıcıya ait olup olmadığını sunucu tarafında doğrulayın.

**Referanslar**

[https://owasp.org/www-project-web-security-testing-guide/v42/4 Web\_Application\_Security\_Testing/05-Authorization\_Testing/04 Testing\_for\_Insecure\_Direct\_Object\_References](https://owasp.org/www-project-web-security-testing-guide/v42/4%20Web_Application_Security_Testing/05-Authorization_Testing/04%20Testing_for_Insecure_Direct_Object_References)

**9.Bulgu Adı: Rate Limiting Eksikliği**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Orta | <http://10.10.11.18:5000> | Müşteri, Satıcı | /login, /register | Burp Suite |

**Zafiyetin Etkisi**

* Aynı IP veya kullanıcı üzerinden /login ve /register gibi endpoint’lere sınırsız istek yapılabilir.
* Brute Force veya DoS (Hizmet aksatma) saldırıları mümkündür.

**Zafiyetin Açıklaması**

* Uygulamada, belirli süre içerisinde yapılabilecek istek sayısını sınırlandıran bir mekanizma bulunmamaktadır.
* Saldırgan, hızlı bir şekilde parolaları deneyebilir veya kaynak tüketimi yaparak uygulamayı çökertmeye çalışabilir.
* Uygulamanın kaynak kodlarına baktıgımızda aynı IP veya kullanıcıdan gelen istekler için limit yok. /login ve /register endpointlerine sınırsız istek yapılabiliyor, Rate limiting kısıtlaması yok. Bu durumda kaynak kullanan /uploads endpointi gibi bir endpointe sınırsız istek yapılarak uygulama çökertilebilir.

A screenshot of a computer

AI-generated content may be incorrect.

* Aynı IP tarafından çok fazla istek yapıldı ancak hiçbir şekilde 429 yani Too Many Request dönmedi.

**Çözüm Önerisi**

1. **Hata Yanıtları ve Gecikme:** Çok fazla hatalı girişte geçici hesap kilitleme veya gecikme eklenmeli.
2. **IP Tabanlı Kısıtlama:** Aynı IP’den 30 saniyede 5 istekten fazla geldiğinde engellenmeli.

**Referanslar**

<https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/>

**10.Bulgu Adı: Information Disclosure (robots.txt)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Düşük | <http://10.10.11.18:5000> | Müşteri, Satıcı | /robots.txt | Burp Suite |

**Zafiyetin Etkisi**

* Kimliği doğrulanmamış bir kullanıcı bile robots.txt dosyasını görüntüleyip, indekslenmemesi gereken önemli URL veya endpoint bilgilerine erişebilir.
* Bu bilgiler saldırganın keşif aşamasında yardımcı olur ve başka zafiyetlerle birleştirilebilir.

**Zafiyetin Açıklaması**

* robots.txt dosyasında duyurulan dizinler/kısıtlamalar, saldırgana uygulamanın dizin yapısı veya hassas sayfalarına dair ipuçları verir.
* Bu sayfalar üzerinde ayrıca zafiyet arayarak sisteme yetkisiz erişim sağlanabilir.

A screenshot of a computer

AI-generated content may be incorrect.

**Çözüm Önerisi**

1. **Hassas URL’lerin robots.txt’de yer almaması:** Hassas yönetim panelleri veya özel yollar, mümkünse ifşa edilmemeli.

**Referanslar**

<https://owasp.org/Top10/A05_2021-Security_Misconfiguration/>

**11. Bulgu Adı: Username Enumeration**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Düşük | <http://10.10.11.18:5000> | Müşteri, Satıcı | /register | Burp Suite |

**Zafiyetin Etkisi**

* /register aşamasında “Username already exists” şeklinde hata mesajı alınarak geçerli kullanıcı adları tespit edilebiliyor.
* Bulunan bu kullanıcı adı, brute force saldırıları için kullanılabilir.

**Zafiyetin Açıklaması**

* /register endpointinde eğer veritabanında kayıtlı bir kullanıcı adı girildiyse uygulama bize : **Username already exists** hata mesajı veriyor. Bu da sistem güvenliğini zayıflatan bir durum. Öğrenilen bu username bilgisiyle brute force kullanılarak parola tespit edilebilir.

A screenshot of a computer

AI-generated content may be incorrect.

* Artık login sayfasına geçip bilinen username i kullanarak web uygulamasına giriş yapmaya çalışıyoruz. Bunun için login sayfasında username i yazıp password ve email kısmı için Intruder’ı kullanmak.

A screenshot of a computer

AI-generated content may be incorrect.

**Çözüm Önerisi**

1. **Genel Hata Mesajları:** “Geçersiz kullanıcı adı veya şifre” gibi birleştirilmiş bir mesaj kullanılmalı, spesifik açıklamalar verilmemeli.

**Referanslar**

<https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/>

**12. Bulgu Adı: Local RCE (Komut Çalıştırma)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Önem Derecesi** | **Erişim Noktası:** | **Kullanıcı Profili** | **Tespit Edilen Bileşenler:** | **Kullanılan Araç:** |
| Düşük | <http://10.10.11.18:5000> | Müşteri, Satıcı | /uploads | Burp Suite |

**Zafiyetin Etkisi**

* Saldırgan, uygulamanın çalıştığı sunucu üzerinde komut çalıştırarak tam yetki elde edebilir.
* Dosyaları okuyabilir, değiştirebilir veya sistemi kalıcı olarak ele geçirebilir.

**Zafiyetin Açıklaması**

* uploads fonksiyonunda komut çalıştırmaya izin verildiği belirtilmiş. Bu sayede saldırgan, HTTP isteği içeriğini manipüle ederek sistem komutlarını tetikleyebiliyor.
* Örneğin hosts dosyasını okuyabildiği gibi, “farklı uygulamaları çalıştırma” imkanı da buluyor.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Çözüm Önerisi**

1. **Komut Çalıştırma Engeli:** Uygulamanın kullanıcı girdileriyle doğrudan komut satırı işlemi yapması kesinlikle engellenmeli (ör. exec, os/exec gibi fonksiyonlara doğrudan erişim kısıtlanmalı).

**Referanslar**

<https://owasp.org/Top10/A03_2021-Injection/>