VULNWEB
DEMO CORP
SIZMA TESTİ RAPORU

Tarih: 05/12/2024

Proje: VW-DC-01

İçindekiler

1. RAPOR HAKKINDA

Bu rapor **Metehan Mehmet Bilen** tarafından var olmayan **VULNWEB DEMO CORP** şirketi üzerine gerçekleştirilen sızma testi sonucunda hazırlanan ve raporlama becerisi hakkında örnek teşkil edilmesi için hazırlanmıştır.

Raporda Acunetix tarafından yayınlanan **testphp.vulnweb.com** web sitesi üzerinden sızma testi gerçekleştirilmiş ve raporlanmıştır.

1.1. Kapsam

Bir sızma testi, belirli bir zaman dilimindeki durumun anlık bir değerlendirmesidir. Bu nedenle, raporda yer alan bulgular ve öneriler yalnızca değerlendirme sırasında elde edilen bilgileri yansıtmakta olup, bu dönem dışında yapılan değişiklik veya güncellemeleri kapsamamaktadır.

Sınırlı süreli çalışmalar, tüm güvenlik kontrollerinin tam bir değerlendirmesini mümkün kılmamaktadır. Bu bağlamda, test sırasında öncelik, saldırganların istismar edebileceği en zayıf güvenlik kontrollerini belirlemeye verilmiştir.

Güvenlik kontrollerinin sürekliliğini sağlamak adına, benzer değerlendirmelerin yıllık olarak iç veya üçüncü taraf denetçiler tarafından gerçekleştirilmesi önerilmektedir.

Test edilen alan adları ve ip adresleri aşağıda listelenmiştir.

Alan Adı	**IP Adresi**
testphp.vulnweb.com	44.228.249.3

1.2. Kapsam Dışı

Müşteri talebi doğrultusunda aşağıdaki saldırıları test sırasında gerçekleştirmemiştir:

- Hizmet Engelleme (DoS) Saldırıları
- Yerel Ağ Sızma Testi
- Phishing/Sosyal Mühendislik

1.3. İletişim Bilgileri

Adı Soyadı	**Unvanı**	**İletişim Bilgisi**
VULNWEB DEMO CORP		
Deneme Testoğlu	Bilgi Güvenliği Müdürü	d.testoglu@vulnwebdemocorp.com
SIZMA TESTİ EKİBİ		
Metehan Mehmet Bilen	Sızma Testi Asistanı	metehan.m.bilen@hotmail.com

1.4. Değerlendirme Genel Bakışı

VULNWEB Demo Corp, 01 Aralık 2024 - 5 Aralık 2024 tarihleri arasında, güvenlik altyapı durumun değerlendirilmesi adına Metehan Mehmet Bilen tarafından test gerçekleştirilmiştir.

Bu çalışmada dahili ağ sızma testi dahil edilmemiştir. Tüm testler OWASP Testing Guide (v4) ve özelleştirilmiş test çerçevesinde gerçekleştirilmiştir.

Sızma testi faaliyetleri şu aşamaları kapsamaktadır:

- Planlama: Müşteri hedefleri toplanmış ve etkileşim kuralları belirlenmiştir.
- Keşif: Tarama ve bilgi toplama süreçleri gerçekleştirilerek potansiyel güvenlik açıkları, zayıf noktalar ve istismar edilebilecek alanlar tespit edilmiştir.
- Saldırı: Potansiyel güvenlik açıkları istismar edilerek doğrulanmış ve yeni erişimler elde edildikçe ek keşifler gerçekleştirilmiştir.
- Raporlama: Bulunan tüm güvenlik açıkları ve istismarlar, başarısız girişimler ile şirketin güçlü ve zayıf yönlerini belgelemek üzere raporlanmıştır.

1.5. Bulguların Derecelendirilmesi

Aşağıdaki tablo, bu belge boyunca güvenlik açıklarının ve risk etkilerinin değerlendirilmesinde kullanılan ciddiyet düzeylerini ve ilgili **CVSS v3 (Ortak Güvenlik Açığı Puanlama Sistemi)** puan aralıklarını tanımlar:

Risk Seviyesi	CVSS Aralığı	Tanım
Kritik	9.0-10.0	İstismar son derece kolaydır ve genellikle sistem düzeyinde ele geçirmeyle sonuçlanır. Hemen bir eylem planı oluşturulması ve yamalanması önerilir.
Yüksek	7.0-8.9	İstismar daha zordur ancak yükseltilmiş ayrıcalıklar, veri kaybı veya kesinti gibi etkiler yaratabilir. En kısa sürede bir eylem planı oluşturulması ve yamalanması önerilir.
Orta	4.0-6.9	Güvenlik açıkları mevcuttur ancak istismar edilebilmesi için sosyal mühendislik gibi ek adımlar gerektirir. Öncelikli sorunlar çözüldükten sonra bir eylem planı oluşturulması ve yamalanması önerilir.
Düşük	0.1-3.9	Güvenlik açıkları istismar edilemez ancak organizasyonun saldırı yüzeyini azaltabilir. Bir sonraki bakım döneminde bir eylem planı oluşturulması ve yamalanması önerilir.
Bilgilendirme		Güvenlik açığı bulunmamaktadır. Test sırasında fark edilen güçlü kontroller, gözlemler veya ek bilgiler sağlanmıştır.

2. GÜVENLİK AÇIĞI ÖZETİ VE RAPOR KARTI

Aşağıdaki tablolar, bulunan güvenlik açıklarını etki seviyelerine göre ve önerilen iyileştirmeleri göstermektedir:

3	2	1	1	1
Kritik	Yüksek	Orta	Düşük	Bilgilendirme

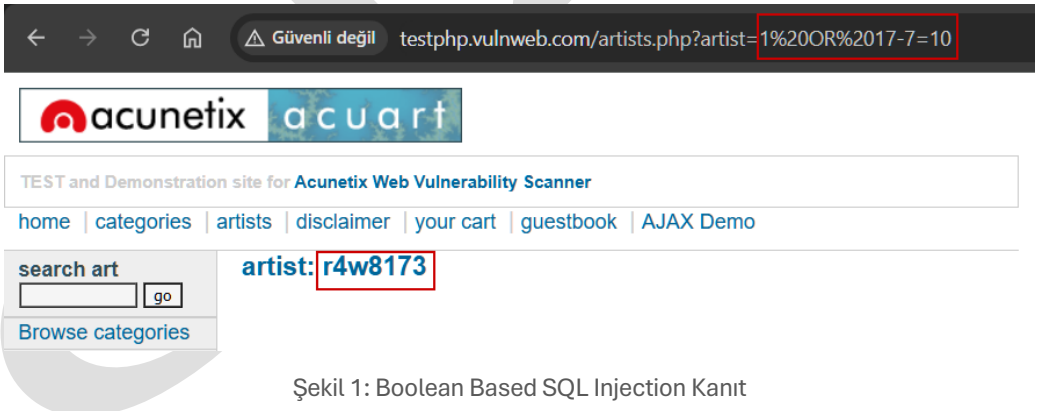
No	Bulgular	Risk Seviyesi	Öneri
1	Boolean Based SQL Injection	Kritik	Kullanıcı girdileri doğrulanmalı ve sadece gerekli yetkiler verilmelidir. WAF kullanılmalıdır.
2	Eski Versiyon PHP Kullanımı	Kritik	PHP kurulumunuzu en son kararlı sürüme yükseltilmelidir.
3	Zaman Tabanlı SQL Injection	Kritik	Kullanıcı girdileri doğrulanmalı ve sadece gerekli yetkiler verilmelidir. WAF kullanılmalıdır.
4	Yerel Dosya Ekleme | LFI	Yüksek	Dosya yollarını sabit kodlanmalıdır veya kullanıcıların yalnızca sınırlı, önceden belirlenmiş bir yol listesi arasından seçim yapmasına izin verilmelidir.
5	HTTP Üzerinden Şifre Aktarılması	Yüksek	Tüm hassas veriler, HTTP yerine HTTPS üzerinden iletilmelidir.
6	Open Policy Crossdomain.xml Tespiti	Orta	Crossdomain.xml dosyanızı, domaininize her yerden erişimi engelleyecek şekilde yapılandırılmalıdır.
7	Veri Tabanı Hata Mesajı İfşası	Düşük	Ayrıntılı hata mesajlarının sadece geliştirici ve sistem yöneticilerine özel log dosyalarına kaydedilmelidir.
8	MySQL Veri Tabanı Tespiti	Bilgilendirme	Ayrıntılı hata mesajlarının sadece geliştirici ve sistem yöneticilerine özel log dosyalarına kaydedilmelidir.

3. BULGULAR

3.1. Boolean Based SQL Injection (Kritik)

Tanım	VULNWEB Demo Corp web uygulamasında, giriş noktalarında Boolean tabanlı SQL enjeksiyonu tespit edilmiştir. Bu açık, saldırganın veri tabanıyla etkileşime geçmesini ve mantıksal ifadeler üzerinden doğru ya da yanlış sonuçlar alarak sistem hakkında bilgi toplamasını sağlar. Bu yöntem, sistemin veri yapısına ve hassas bilgilerine yetkisiz erişim elde etmek için kullanılabilir.
Bulgu No	1
Risk Seviyesi	Kritik
Sistem	testphp.vulnweb.com
Kullanılan Araç	Netsparker
Referans	

3.1.1. Boolean Based SQL Injection Kanıt



Şekil 1: Boolean Based SQL Injection Kanıt

3.1.2. Boolean Based SQL Injenction Zafiyeti İyileştirme Önerisi

Boolean tabanlı SQL enjeksiyonunu önlemek için parametreli sorgular kullanılmalı, kullanıcı girdileri doğrulanmalı ve sadece gerekli yetkiler verilmelidir. Ayrıca, Web Uygulama Güvenlik Duvarı (WAF) kullanımı ile SQL enjeksiyonları engellenebilir.

3.2. Eski Versiyon PHP Kullanımı (Kritik)

Tanım	VULNWEB Demo Corp web uygulamasında, 5.6.40 versiyonlu PHP kullanımı tespit edilmiştir.
Bulgu No	2
Risk Seviyesi	Kritik
Sistem	testphp.vulnweb.com
Kullanılan Araç	Netsparker
Referans	

3.2.1. Eski Versiyon PHP Kullanımı Zafiyet İyileştirme Önerisi

PHP kurulumunuzu en son kararlı sürüme yükseltilmelidir.

3.3. Zaman Tabanlı SQL Injection (Kritik)

Tanım	VULNWEB Demo Corp web uygulamasında, giriş noktalarında zaman tabanlı SQL enjeksiyonu tespit edilmiştir. “Sleep(16000/1000)” fonksiyonunu kullanarak sorguya gecikme ekler. Bu yöntem, veri tabanı sorgusunun başarılı olup olmadığını zaman gecikmesi üzerinden anlamaya çalışır. Yanıt süresi, saldırının başarılı olma ihtimalini gösterir.
Bulgu No	3
Risk Seviyesi	Kritik
Sistem	testphp.vulnweb.com
Kullanılan Araç	Arachni
Referans	

3.3.1. Zaman Tabanlı SQL Injection Kanıtı

HTTP data

Request

```
GET /AJAX/infocateg.php?id=%20sleep%2816000%2F1000%29%3B HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
User-Agent: Arachni/v1.5.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.8,he;q=0.6
X-Arachni-Scan-Seed: 1dbfba83feb0ba639dcff1d1fa14dd1c
Cookie: mycookie=3
```

Şekil 2: Zaman Tabanlı SQL Injection Kanıt

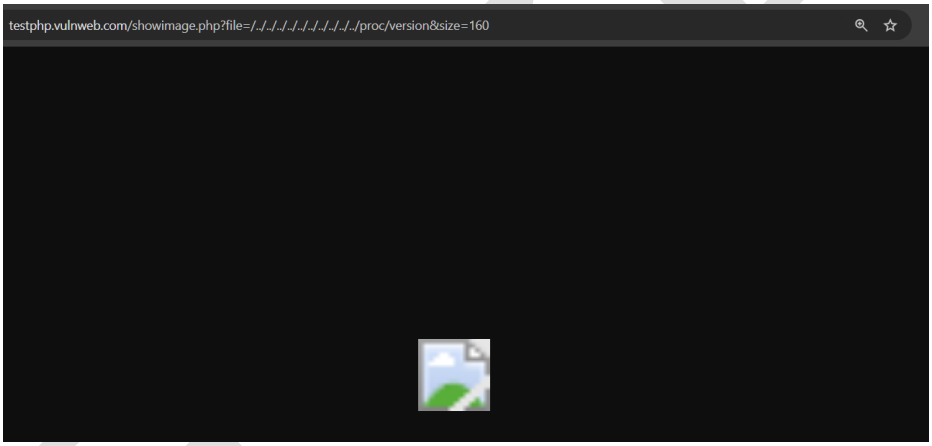
3.3.2. Zaman Tabanlı SQL Injection İyileştirme Önerisi

Zaman tabanlı SQL enjeksiyonunu önlemek için parametreli sorgular kullanılmalı, kullanıcı girdileri doğrulanmalı ve sadece gerekli yetkiler verilmelidir. Ayrıca, Web Uygulama Güvenlik Duvarı (WAF) kullanımı ile SQL enjeksiyonları engellenebilir.

3.4. Yerel Dosya Ekleme | LFI (Yüksek)

Tanım	Saldırganın web sunucusundaki yerel dosyalara yetkisiz erişim sağlamasına ve bu dosyaları okumasına olanak tanır.
Bulgu No	4
Risk Seviyesi	Yüksek
Sistem	testphp.vulnweb.com
Kullanılan Araç	Netsparker
Referans	

3.4.1. Yerel Dosya Ekleme | LFI Kanıtı



Şekil 3: LFI Kanıt

3.4.2. Yerel Dosya Ekleme | LFI İyileştirme Önerisi

LFI zafiyetini azaltmak için, dosya yollarını doğrudan eklemekten kaçınılmalıdır. Bunun yerine, dosya yollarını sabit kodlanmalıdır veya kullanıcıların yalnızca sınırlı, önceden belirlenmiş bir yol listesi arasından seçim yapmasına izin verilmelidir.

Belirli bir dizinden ve alt dizinlerinden dosya eklemeye izin verecek şekilde yapılandırıldığından emin olunulmalıdır.

3.5. HTTP Üzerinden Şifre Aktarılması (Yüksek)

Tanım	Şifre verileri HTTP üzerinden iletiliyor. Bu, güvenli olmayan bir iletişim protokolü kullanılarak şifrelerin şifrelenmeden, açık bir şekilde aktarılması anlamına gelir. HTTP, şifreleme sağlamaz, bu nedenle saldırganlar şifre verilerini ağda izleyerek elde edebilir.
Bulgu No	5
Risk Seviyesi	Yüksek
Sistem	testphp.vulnweb.com
Kullanılan Araç	Netsparker
Referans	

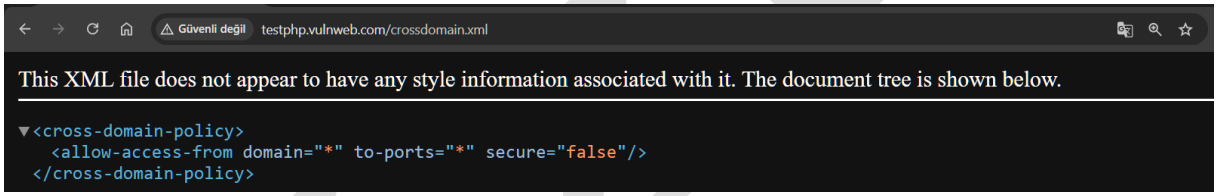
3.5.1. HTTP Üzerinden Şifre Aktarılması İyileştirme Önerisi

Tüm hassas veriler, HTTP yerine HTTPS üzerinden iletilmelidir. Formlar da HTTPS üzerinden sunulmalıdır. Kullanıcı girişi gibi kullanıcı girdisi kabul eden uygulamanın tüm bölümleri, yalnızca HTTPS üzerinden sunulmalıdır.

3.6. Open Policy Crossdomain.xml Tespit Edildi (Orta)

Tanım	Open Policy Crossdomain.xml dosyası tespit edildi. Saldırganların başka bir alan adı üzerinden sunucudaki hassas verilere erişmesine olanak tanır.
Bulgu No	6
Risk Seviyesi	Orta
Sistem	testphp.vulnweb.com
Kullanılan Araç	Netsparker
Referans	

3.6.1. Open Policy Crossdomain.xml Tespit Kanıtı



Şekil 4: Open Policy Crossdomain.xml Tespiti Kanıt

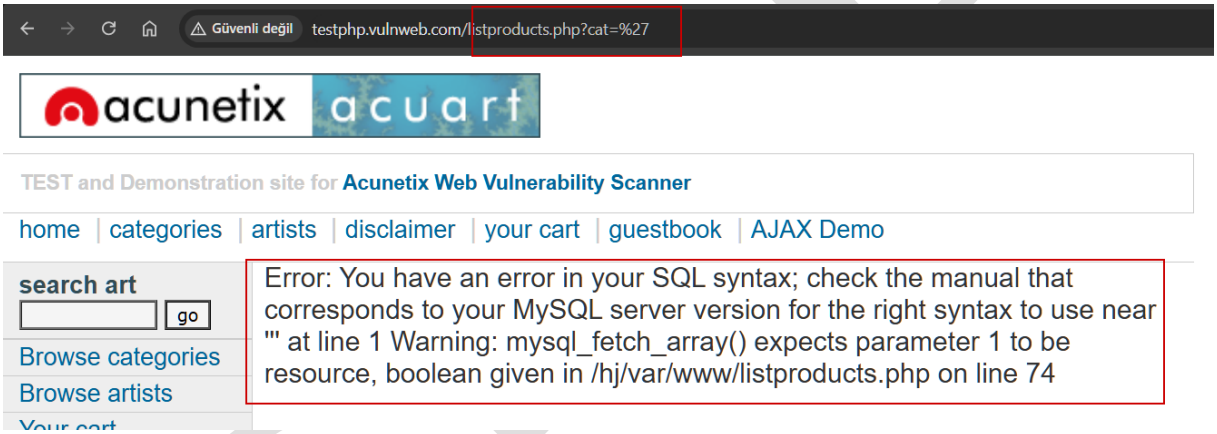
3.6.2. Open Policy Crossdomain.xml Tespit İyileştirme Önerisi

Crossdomain.xml dosyanızı, domaininize her yerden erişimi engelleyecek şekilde yapılandırılmalıdır.

3.7. Veri Tabanı Hata Mesajı İfşası (Düşük)

Tanım	Veri tabanı hata mesajı tespit edildi.
Bulgu No	7
Risk Seviyesi	Düşük
Sistem	testphp.vulnweb.com
Kullanılan Araç	Netsparker
Referans	

3.7.1. Veri Tabanı Hata Mesajı İfşası Kanıt



Şekil 5: Veri Tabanı Hata Mesajı İfşası Kanıt

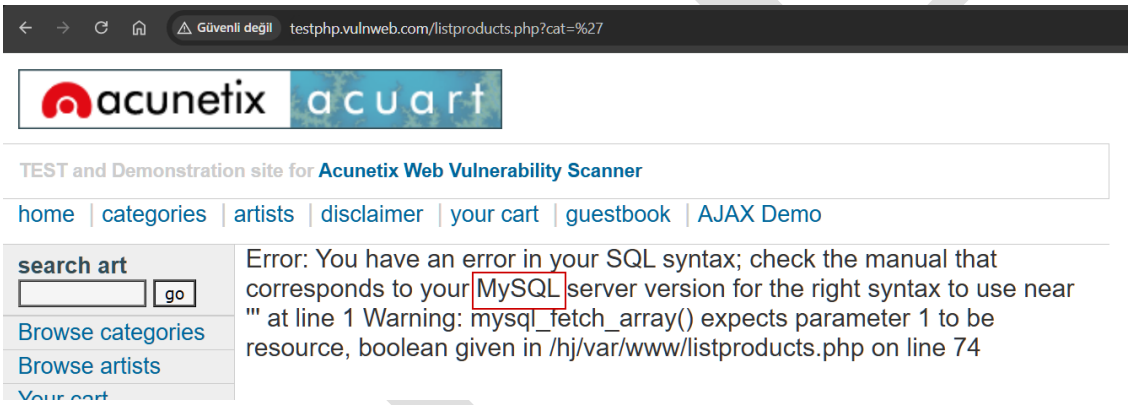
3.7.2. Veri Tabanı Hata Mesajı İfşası Zafiyeti İyileştirme Önerisi

Ayrıntılı hata mesajlarının sadece geliştirici ve sistem yöneticilerine özel log dosyalarına kaydedilmesi gerekmektedir. Kullanıcılara gösterilecek mesajlar, yalnızca genel ve anlaşılır olmalıdır.

3.8. MySQL Veri Tabanı Tespit Edildi (Bilgilendirme)

Tanım	VULNWEB Demo Corp web uygulamasında MySQL veri tabanı kullanıldığı tespit edildi.
Bulgu No	8
Risk Seviyesi	Bilgilendirme
Sistem	testphp.vulnweb.com
Kullanılan Araç	Netsparker
Referans	

3.8.1. MySQL Veri Tabanı Tespit Edildi Kanıt



Şekil 6: MySQL Tespiti Kanıt

VULNWEB
DEMO CORP
SIZMA TESTİ RAPORU
SON SAYFA

Raporu Hazırlayan:

Metehan Mehmet Bilen

metehan.m.bilen@hotmail.com