GuardPlate
Cyber Security System

Bu test **Zonguldak Bülent Ecevit Üniversitesi Teknopark** bünyesinde gerçekleştirilmiştir.

Sızma Testi

Raporu

Kırıkkale Profesyonel Web Yazılımı

kirikkale.profesyonelwebyazilimi.com

22.02.2021

Guard Plate bir Webanya Ltd. Şti. Markasıdır

İçindekiler

1. Guard Plate Sızma Testi Temellendirme Yöntemleri 4
   1.1. Veri Sağlama 4
   1.2. Ağ Topolojisi Çıkarma 4
   1.3. Zafiyet Araştırma 4
   1.4. Giriş Hakkı Elde Etme 5
   1.5. Yüksek Yetkiye Geçiş 5
   1.6. Kalıcı Olma 5
   1.7. Teknik Rapor 5
2. Çalışma Kapsamı 6
3. Bulgulara Yönelik Önem Dereceleri 7
4. Özet Değerlendirme 8
5. Tespit Edilen Zafiyetler 9
   5.1. SQL Injection – Dil çevirileri ..... Hata! Yer işareti tanımlanmamış.
   5.2. Reflected XSS – Arama 12
   5.3. Stored XSS – Bize Yazın 12
   5.4. Stored XSS – Sayfa Ekle 12
   5.5. Stored XSS – Slider Ekle 12
   5.6. Desteklenmeyen Sürüm 22
   5.7. SQL Injection ile Yetki Yükseltme – tbl_getLog 17
   5.8. SQL Injection ile Yetki Yükseltme – tbl_getProductsTbl 18
   5.9. SQL Injection ile Yetki Yükseltme – tbl_get_desc_and_pagi 20
   5.10. SQL Injection ile Yetki Yükseltme – update_tbl 20
   5.11. SQL Injection ile Yetki Yükseltme – deleteImage 22
   5.12. SQL Injection ile Yetki Yükseltme – tbl_get_desc_and_pagiProperty 24
   5.13. SQL Injection ile Yetki Yükseltme – tbl_get_orders 25
   5.14. SQL Injection ile Yetki Yükseltme – delete_row_orders 27
   5.15. SQL Injection ile Yetki Yükseltme – renderParents 27
   5.16. SQL Injection ile Yetki Yükseltme – delete_row_orders 27
   5.17. SQL Injection ile Yetki Yükseltme – rowStatus Hata! Yer işareti tanımlanmamış.
   5.18. SQL Injection ile Yetki Yükseltme – tbl_get..... Hata! Yer işareti tanımlanmamış.
   5.19. SQL Injection ile Yetki Yükseltme – tbl_get_member 28
   5.20. SQL Injection ile Yetki Yükseltme – tbl_get_full 29
   5.21. Yetki Yükseltme – tbl_get 30
   5.22. Yetki Yükseltme – tbl_get_full 31

5.23. Yapılandırılmamış Form Girdileri Doğrulaması –Alt Slider.....Hata! Yer işareti tanımlanmamış.

5.24. Yapılandırılmamış Form Girdileri Doğrulaması – Slider Masaüstü ..... Hata! Yer işareti tanımlanmamış.

5.25. Yapılandırılmamış Form Girdileri Doğrulaması – Otobüs Firmaları Ekle .....Hata! Yer işareti tanımlanmamış.

5.26. Yapılandırılmamış Form Girdileri Doğrulaması – Havayolu Ekle Hata! Yer işareti tanımlanmamış.

5.27. Yapılandırılmamış Form Girdileri Doğrulaması – Oteller.....Hata! Yer işareti tanımlanmamış.

5.28. Yapılandırılmamış Form Girdileri Doğrulaması – Restaurant Ekle..... Hata! Yer işareti tanımlanmamış.

5.29. Yapılandırılmamış Form Girdileri Doğrulaması – Rota Ekle.....Hata! Yer işareti tanımlanmamış.

5.30. Yapılandırılmamış Form Girdileri Doğrulaması – Mekan Kategorileri Ekle. Hata! Yer işareti tanımlanmamış.

5.31. Yedekleme Dosyasına Yetkisiz Erişim **25**

5.32. Unrestricted File Upload – Dosya Yöneticisi **25**

5.33. Unrestricted File Upload – Slider Masaüstü Ekle **25**

5.34. Captcha Güvenlik Önlemi Eksikliği - Kontrol Paneli **40**

5.35. Hassas Veri Sızıntısı **41**

5.36. Kolay Erişilebilir Kontrol Paneli **42**

1. Guard Plate Sızma Testi Temellendirme Yöntemleri

Guard Plate Sızma Testi temellendirme yöntemleri, şirketimiz bünyesindeki uzman personel tarafından yapılan sızma testleri ile ilgili veri edinme, zafiyet incelemesi, riskler dahil olmak üzere rapor üretimine kadar tüm süreçlerle ilgili detayları içerir. Sızma testi, temel olarak aşağıdaki yöntemlerle oluşturulmaktadır.

1.1. Veri Sağlama

Bu aşamada, değerlendirme adımlarına rehberlik etmek için her türlü veri toplanır. Veri toplama, aktif ve pasif bilgi toplama olarak ikiye ayrılır. Pasif bilgi toplama, sistemlerle doğrudan temas halinde olmaksızın bilgi toplarken, aktif bilgi toplama yönteminde sistemlere doğrudan bağlantı kurulur. İki yöntem de hedef sistem hakkında olabildiğince çok miktarda veri toplamayı amaçlamaktadır. Hedef sistem bir kurum ise bu bilgiler kurum hakkında olabileceği gibi kurum personeli hakkında da olabilir. Bilgi toplamak için aşağıdaki kaynaklar ve otomatik bilgisayar yazılımları kullanılabilir.

Web Sitesi	Shodan	LinkedIn	Kali Linux araçları
Facebook	WebDataExtractor	RIPE	Maltego

1.2. Ağ Topolojisi Çıkarma

Ağ Topolojisi Çıkarma çalışmasındaki ana hedef sistemin ağ yapısını detaylı şekilde tespit etmektir.Ağ üzerindeki aktif portların, servislerin ve servislerin hangi yazılımlara ve yazılımların hangi versiyonlarına ait olduklarına dair bilgilerin, ağ üzerinde güvenlik duvarı, IPS gibi güvenlik cihazlarının cihazların mevcut olup olmadığı ve bu cihazlara ait bilgilerin, içeride bulunan sunucuların sayısı ve üzerindeki işletim sistemlerine dair bilgilerin alınabilmesi ve bu bilgiler doğrultusunda ağ haritasının her yönüyle çıkartılmasıdır.

Bu adımda kullanılan araçlar;

Nessus	Netsparker	Airmon-ng	Nikto
Zenmap	Netcat	RIPE	Fing

1.3. Zafiyet Araştırma

Zafiyet araştırma çalışması, güvenlik açıklarının meydana getirdiği güvenlik risklerini tanımlamak ve yorumlamak için kullanılır. Birçok zafiyet tarama aracı ile sistemler ayrı ayrı araştırılır. Bu çalışmada sisteme herhangi bir müdahalede bulunulmaz. Sistemler üzerinde çalışan yazılımsal ve donanımsal zafiyetler incelenir ve teknik detayları ile raporlanır.

1.4. Giriş Hakkı Elde Etme

Sızma testleri esnasında hedef, sisteme giriş hakkı elde edebilmektir. Sistemde hak elde edilen tüm girdi noktaları tespit edilerek, testin kapsamına bağlı olarak hak yükseltme uygulamaları hedeflenecektir.

1.5. Yüksek Yetkiye Geçiş

Yüksek yetkiye geçiş adımında hedef, ele geçirilen sistemde yüksek yetki haklarına sahip bir kullanıcı grubuna (root, administrator vb) geçiş yapmaktır. Bu adımda parola saldırıları gibi farklı saldırı yöntemleri denenecektir. Bu süreç aynı zamanda sistem içerisinde sadece yüksek yetkili kullanıcıların girebileceği alanlara ulaşım sağladığından sistem hakkında daha kapsamlı testlerin de yapılmasına olanak sağlayacaktır.

1.6. Kalıcı Olma

Kalıcı olma aşamasında, erişim sağlanan sistem üzerinde kalıcı olmanın mümkün olup olmadığı araştırılmaktadır. Sisteme erişim sağlayan istenmeyen bir kullanıcının, izlerini temizlemesi, çalıştırdığı işlemleri saklaması, dışarıdan içeriye veya içeriden dışarıya kurulan bağlantıyı gizlemesi gibi işlemlerin olanak düzeyi tespit edilir.

1.7. Teknik Rapor

Bu aşamada, sistemde veya donanımda tespit edilmiş olan bulgular sistem sahibine teknik rapor halinde sunulmaktadır. Sızma testi sırasında tespit edilen kritik güvenlik zafiyetleri belgelenerek en kısa sürede kuruma bildirilir. Guard Plate Sızma Testi Raporu üst düzey güvenli ortamlarda saklanmakta ve gizlilik sözleşmesi çerçevesinde sadece yetkili kurum yetkilileri ile paylaşılmaktadır.

2. Çalışma Kapsamı

Sızma testlerinin yapılabilmesi ve ilgili teknik raporun oluşturulabilmesi için işlem gerçekleştirilecek erişim noktaları şu şekilde tanımlanmaktadır;

İnternet : Kurum veya kuruluşun internet hatları üzerinden erişilebilen tüm sunucu ve servislerine yönelik sızma testleri gerçekleştirilir.

Anonim Kullanıcı Profili : Web servislerine erişebilen ancak web uygulamalarına giriş yetkisine sahip olmayan kullanıcıları temsil eder. Bu kullanıcıların oluşturabileceği tehditleri tespit etmek ve ortadan kaldırabilmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

Müşteri Profili : İnternet üzerinde web uygulamalarının üyesi olan kullanıcıların sistem içerisinde oluşturabileceği riskleri tespit etmek ve ortadan kaldırmak adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmaktadır.

Çalışan Profili : Çalışan personelin sahip olduğu yetkiler ile sistemde oluşturabileceği riskleri tespit etmek ve ilgili zayıflıkları ortadan kaldırmak adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmaktadır.

Diğer Kullanıcı Profilleri : Sızma testlerinin, daha önce belirtilen dört kullanıcı profilinden farklı olan bir kullanıcı profili ile gerçekleştirilmesi halinde, kullanılan her bir profil için tanımlanan hak ve yetkiler Diğer Kullanıcı Profilleri başlığı altında açıkça ifade edilir.

3. Bulgulara Yönelik Önem Dereceleri

Tespit edilen zafiyet bulguları 5 farklı seviyede belirtilmektedir.

Herhangi bir niteliği, özelliği bulunmayan bir saldırgan tarafından kurum veya kuruluşun dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanabilen saldırılara neden olan açıklardır.

Belirli özellik ve niteliklere sahip bir saldırgan tarafından kurum veya kuruluşun dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanabilen saldırılara neden olan açıklardır.

Kurum veya kuruluş dış ağından gerçekleştirilen ve kısıtlı yetki yükseltilmesi veya hizmet dışı olma gibi bir durumla sonuçlanabilen, bununla birlikte yerel ağ ya da sunucu üzerinden gerçekleştirilen ve yetki yükseltmeyi sağlayan saldırılara neden olan açıklardır.

Kurum veya kuruluşun yerel ağı veya sunucu üzerinden gerçekleştirilen ve hizmet dışı olma ile sonuçlanan saldırılara neden olan açıklardır.

Sonuçlarının net olarak belirlenemediği sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan düşük seviyeli eksikliklerdir.

4. Özet Değerlendirme

Firmamızın yapmış olduğu testler sonucunda **5 Acil**, **1 Kritik**, **19 Yüksek**, **9 Orta** ve **2 Düşük** derecede olmak üzere **36 bulgu** tespit edilmiş ve raporlanmıştır.

Kredi kartı ile ödeme ve şifremi unuttum modülleri aktif olmadığından testlere dahil edilmemiştir.

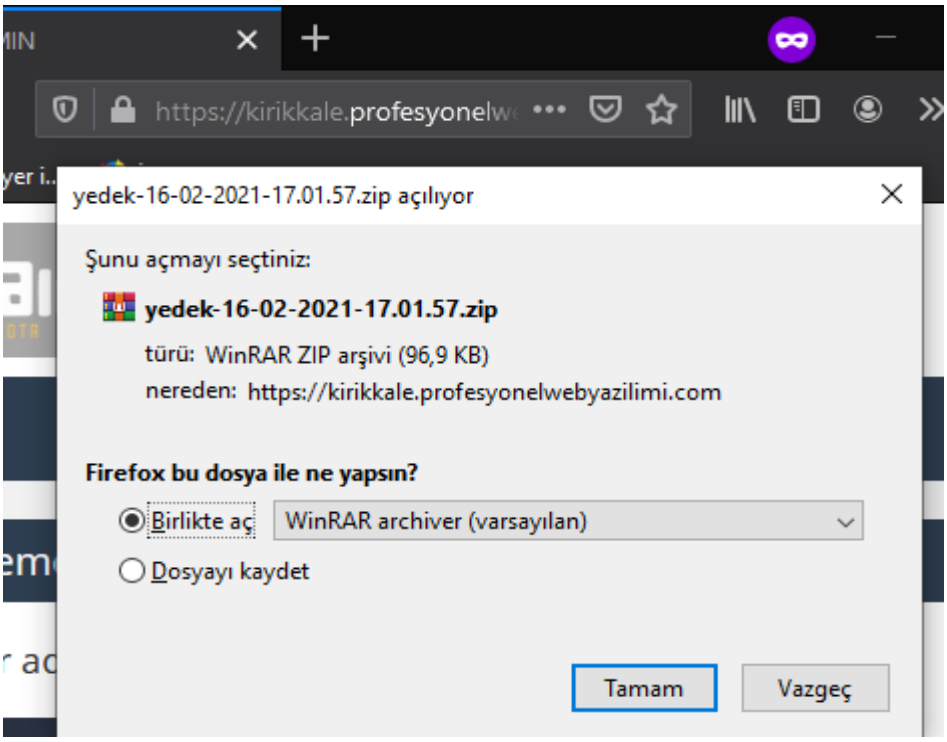
5. Tespit Edilen Zafiyetler

5.1. Yedekleme Dosyasına Yetkisiz Erişim

ACİL	**Bulgu Adı**	**Yedekleme Dosyasına Yetkisiz Erişim**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/yedekleme
	Özet	Yedekleme dosyasına yetkisiz, erişim izni olmayan kullanıcıların erişebildiği keşfedilmiştir.

Bulgu Açıklaması

Yedekleme dosyasına yetkisiz ve erişim izni olmayan tüm kullanıcıların erişebildiği keşfedilmiştir. Yedekleme dosyasında bulunan yönetici ve kullanıcı şifreleri yetki yükseltme ve sisteme sızmak için kullanılabilir.



Çözüm Önerisi

yedekIndir isimli uç noktada yetki kontrolü yapılması tavsiye edilir.

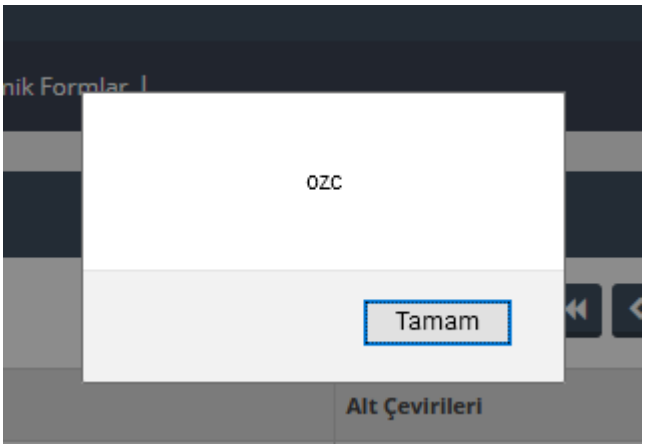
5.2. Reflected XSS – Arama

ACİL	**Bulgu Adı**	**Stored Cross Site Scripting (XSS)**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/arama
	Özet	Arama sayfasında Reflected XSS zafiyeti keşfedilmiştir.

Bulgu Açıklaması

Cross-Site Scripting (XSS), yazılımcının kullanıcıdan aldığı girdileri gerekli HTML ve JavaScript filtrelerinden geçirmediği takdirde oluşan bir zafiyettir. Girdiler gerekli filtrelerden geçmediği taktirde, eğer kullanıcı aynı zamanda bir saldırgan ise; diğer kullanıcılara veya doğrudan sisteme zarar verebilecek zararlı kodları çalıştırabilir. HTML, CSS ve JavaScript tarayıcı tarafından yorumlanan diller olduğundan dolayı, yazılan zararlı kod doğrudan diğer kullanıcıları da etkileyebilmektedir.

Web sayfasında bulunan "Arama" formundan gönderilen HTML kodları, kontrol panelinde üye detaylarının görüntülenmesi durumunda çalışmaktadır. Bu durum kontrol panelinin ele geçirilmesine yol açabilir.



Çözüm Önerisi

Formdan gönderilen veriler sunucu tarafından XSS filtresinden geçirilerek veritabanına kaydedilmelidir. Kontrol panelinin Angular ile kodlanmış olması, XSS filtrelerinde tanımlanmayan bazı zararlı kod yapılarının çalışmasına neden olabilir. Angular tarafında da XSS zafiyetine karşı önlem alınmalıdır.

5.3. Reflected XSS – Arama

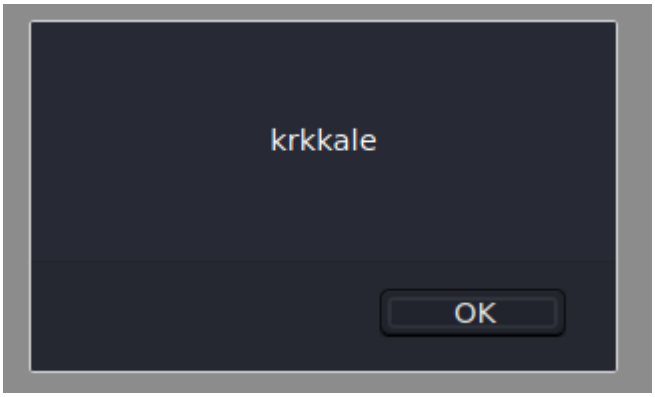
ACİL	**Bulgu Adı**	**Stored Cross Site Scripting (XSS)**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/arama
	Özet	Arama sayfasında Reflected XSS zafiyeti keşfedilmiştir.

Bulgu Açıklaması

Cross-Site Scripting (XSS), yazılımcının kullanıcıdan aldığı girdileri gerekli HTML ve JavaScript filtrelerinden geçirmediği takdirde oluşan bir zafiyettir. Girdiler gerekli filtrelerden geçmediği taktirde, eğer kullanıcı aynı zamanda bir saldırgan ise; diğer kullanıcılara veya doğrudan sisteme zarar verebilecek zararlı kodları çalıştırabilir. HTML, CSS ve JavaScript tarayıcı tarafından yorumlanan diller olduğundan dolayı, yazılan zararlı kod doğrudan diğer kullanıcıları da etkileyebilmektedir.

Web sayfasında bulunan "Arama" formundan gönderilen HTML kodları, kontrol panelinde üye detaylarının görüntülenmesi durumunda çalışmaktadır. Bu durum kontrol panelinin ele geçirilmesine yol açabilir.

```
GET /arama?q=</span><script>alert('krkkale')</script> HTTP/1.1
Host: kirikkale.profesyonelwebyazilimi.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: wbn_session=750a9bf8bee7b714962f446c107a0532f3449a3b; cpsession=%3ansGouRbB4
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



Çözüm Önerisi

Formdan gönderilen veriler sunucu tarafından XSS filtresinden geçirilerek veritabanına kaydedilmelidir. Kontrol panelinin Angular ile kodlanmış olması, XSS filtrelerinde tanımlanmayan bazı zararlı kod yapılarının çalışmasına neden olabilir. Angular tarafında da XSS zafiyetine karşı önlem alınmalıdır.

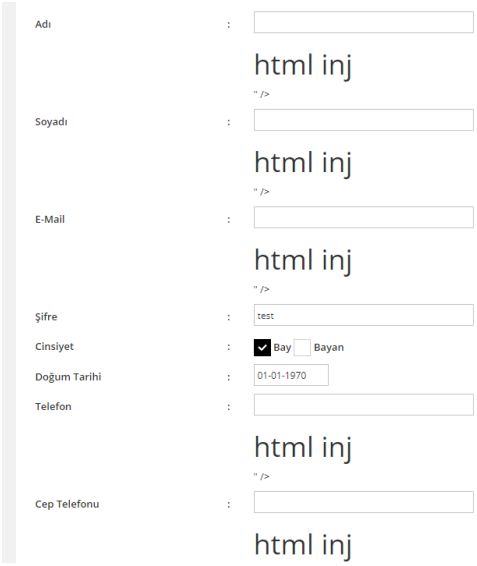
5.4. Stored XSS – Sayfa Ekle

ACİL	**Bulgu Adı**	**Stored Cross Site Scripting (XSS)**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/page_admin/
	Özet	Kullanıcı bilgileri sayfası ve kontrol panelinde Stored XSS zafiyeti keşfedilmiştir.

Bulgu Açıklaması

Cross-Site Scripting (XSS), yazılımcının kullanıcıdan aldığı girdileri gerekli HTML ve JavaScript filtrelerinden geçirmediği takdirde oluşan bir zafiyettir. Girdiler gerekli filtrelerden geçmediği taktirde, eğer kullanıcı aynı zamanda bir saldırgan ise; diğer kullanıcılara veya doğrudan sisteme zarar verebilecek zararlı kodları çalıştırabilir. HTML, CSS ve JavaScript tarayıcı tarafından yorumlanan diller olduğundan dolayı, yazılan zararlı kod doğrudan diğer kullanıcıları da etkileyebilmektedir.

Web sayfasında bulunan "Kullanıcı Bilgileri Düzenleme" formundan gönderilen HTML kodları, kontrol panelinde üye detaylarının görüntülenmesi durumunda çalışmaktadır. Bu durum kontrol panelinin ele geçirilmesine yol açabilir.



Çözüm Önerisi

Formdan gönderilen veriler sunucu tarafından XSS filtresinden geçirilerek veritabanına kaydedilmelidir. Kontrol panelinin Angular ile kodlanmış olması, XSS filtrelerinde tanımlanmayan bazı zararlı kod yapılarının çalışmasına neden olabilir. Angular tarafında da XSS zafiyetine karşı önlem alınmalıdır.

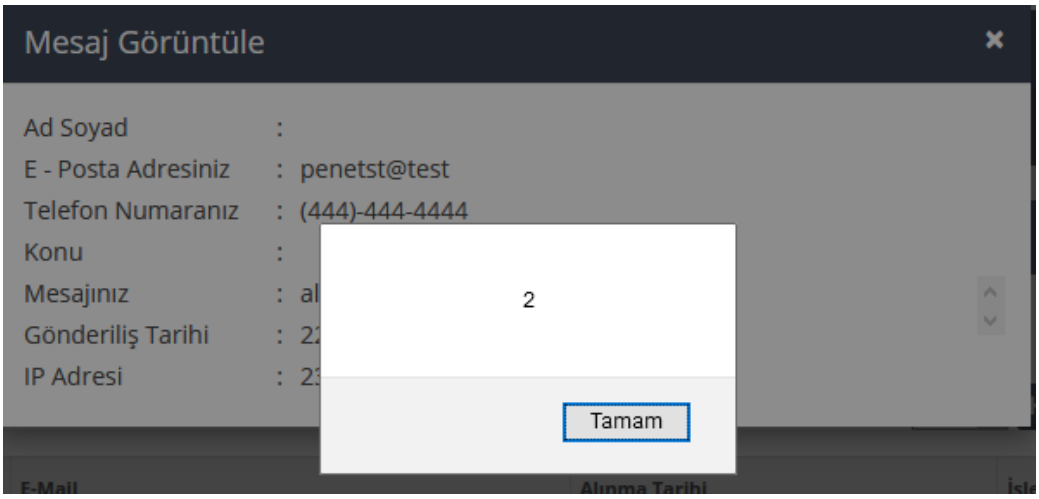
5.5. Stored XSS – Bize Yazın

ACİL	**Bulgu Adı**	**Stored Cross Site Scripting (XSS)**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/iletisim/bize-yazin
	Özet	Bize yazın sayfası ve kontrol panelinde Stored XSS zafiyeti keşfedilmiştir.

Bulgu Açıklaması

Cross-Site Scripting (XSS), yazılımcının kullanıcıdan aldığı girdileri gerekli HTML ve JavaScript filtrelerinden geçirmediği takdirde oluşan bir zafiyettir. Girdiler gerekli filtrelerden geçmediği taktirde, eğer kullanıcı aynı zamanda bir saldırgan ise; diğer kullanıcılara veya doğrudan sisteme zarar verebilecek zararlı kodları çalıştırabilir. HTML, CSS ve JavaScript tarayıcı tarafından yorumlanan diller olduğundan dolayı, yazılan zararlı kod doğrudan diğer kullanıcıları da etkileyebilmektedir.

Web sayfasında bulunan "Bize Yazın" formundan gönderilen HTML kodları, kontrol panelinde üye detaylarının görüntülenmesi durumunda çalışmaktadır. Bu durum kontrol panelinin ele geçirilmesine yol açabilir.



Çözüm Önerisi

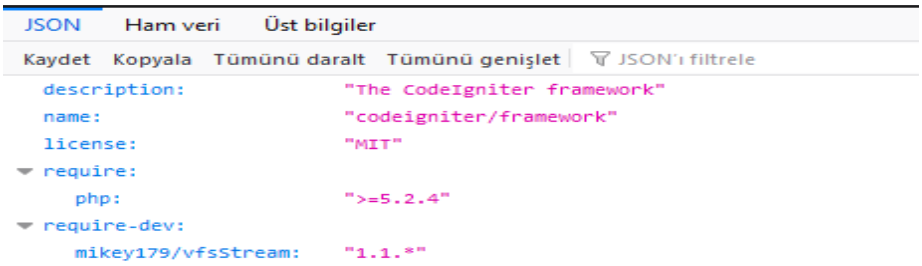
Formdan gönderilen veriler sunucu tarafından XSS filtresinden geçirilerek veritabanına kaydedilmelidir. Kontrol panelinin Angular ile kodlanmış olması, XSS filtrelerinde tanımlanmayan bazı zararlı kod yapılarının çalışmasına neden olabilir. Angular tarafında da XSS zafiyetine karşı önlem alınmalıdır.

5.6. Desteklenmeyen PHP Sürümü

KRİTİK	**Bulgu Adı**	**Desteklenmeyen PHP Sürümü**
	Erişim Noktası	-
	Özet	Sunucuda PHP'nin 5.2.4 sürümünün kullanıldığı gözlemlenmiştir.

Bulgu Açıklaması

Sunucuda PHP'nin desteği kesilmiş, kritik zafiyet barındıran ve güncelleme desteği bulunmayan 5.6.37 sürümünün kullanıldığı gözlemlenmiştir.



Çözüm Önerisi

PHP sürümünün güncellenmesi tavsiye edilir.

5.7. Unrestricted File Upload – Slider Masaüstü Ekle

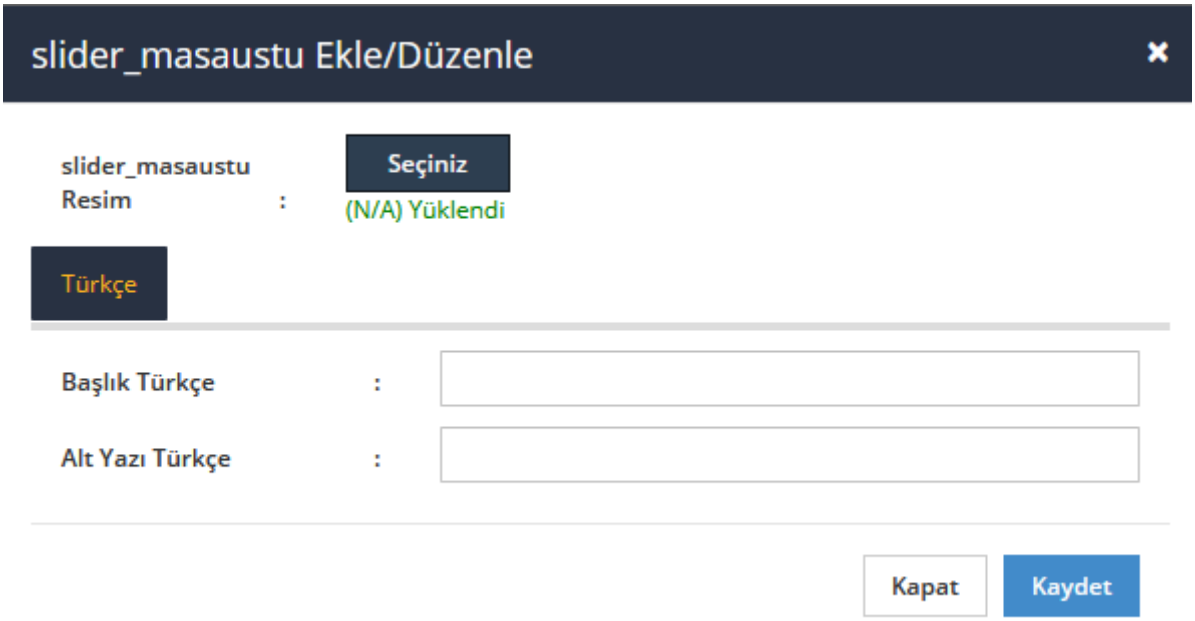
YÜKSEK	**Bulgu Adı**	**Unrestricted File Upload**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/slider_masaustu/
	Özet	Yönetim panelindeki "Slider Ekle"nin slider yükleme bölümünde yüklenen dosyanın içeriğini ve uzantısını kontrol etmediği gözlemlenmiştir.

Bulgu Açıklaması

Yönetim panelindeki "Slider Ekle"nin slider yükleme bölümünde yüklenen dosyanın içeriğini ve uzantısını kontrol etmediği gözlemlenmiştir.

Kullanıcılardan birinin şifresinin çalınması durumunda, saldırganın PHP dosyası yükleyerek sunucuyu ele geçirmesine yol açabilir.

Örneğin, burada yüklenen dosya .php uzantılı bir dosyadır.



Çözüm Önerisi

Dosya yükleme aşamasında, sunucu tarafında dosyanın içeriği ve uzantısı kontrol edilmelidir.

5.8. Unrestricted File Upload – Dosya Yöneticisi

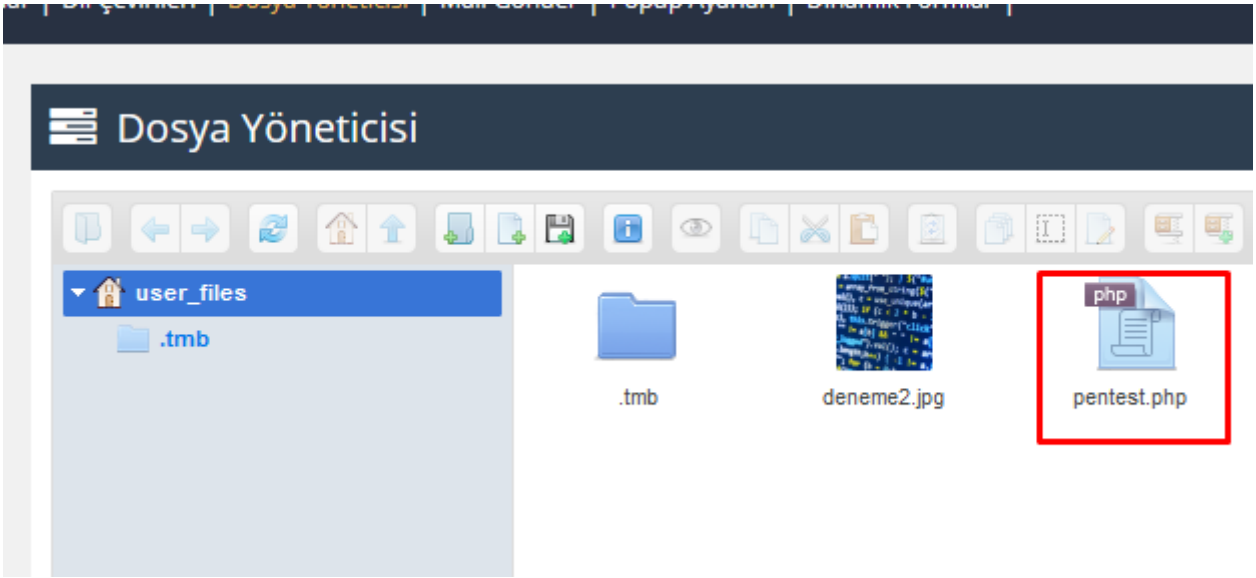
YÜKSEK	**Bulgu Adı**	**Unrestricted File Upload**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/file_manager/#elf_l1_Lw
	Özet	Yönetim panelindeki "Slider Ekle"nin slider yükleme bölümünde yüklenen dosyanın içeriğini ve uzantısını kontrol etmediği gözlemlenmiştir.

Bulgu Açıklaması

Yönetim panelindeki "Slider Ekle"nin slider yükleme bölümünde yüklenen dosyanın içeriğini ve uzantısını kontrol etmediği gözlemlenmiştir.

Kullanıcılardan birinin şifresinin çalınması durumunda, saldırganın PHP dosyası yükleyerek sunucuyu ele geçirmesine yol açabilir.

Örneğin, burada yüklenen dosya .php uzantılı bir dosyadır.



Çözüm Önerisi

Dosya yükleme aşamasında, sunucu tarafında dosyanın içeriği ve uzantısı kontrol edilmelidir.

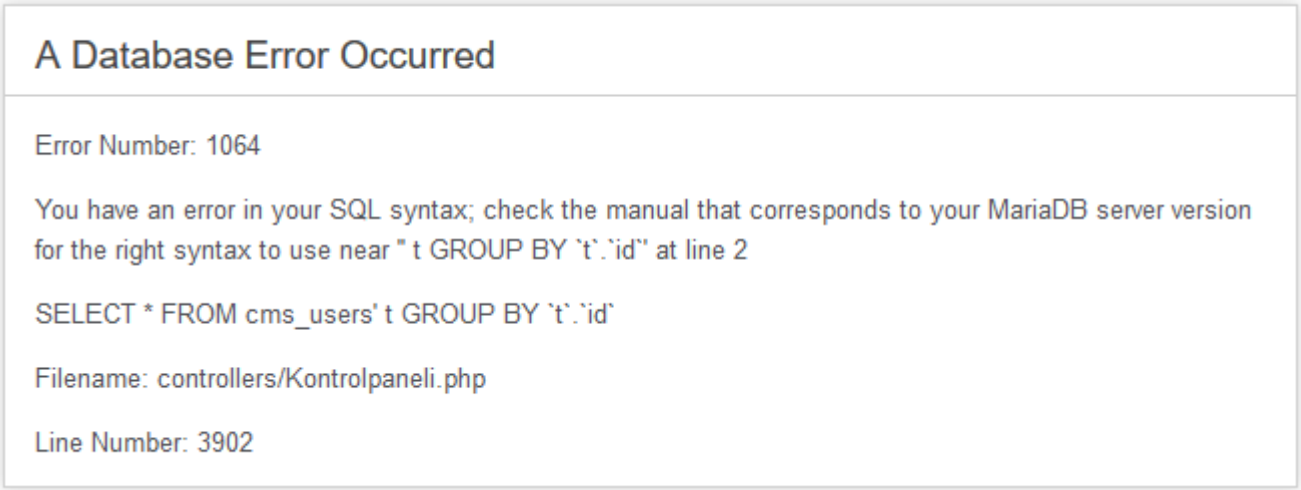
5.9. SQL Injection ile Yetki Yükseltme – tbl_get

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/tbl_get?tbl=%27
	Özet	Kontrol panelinde bulunan "tbl_getLog" isimli uç noktada bir veya birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **tbl_get** isimli uç noktadaki **orderby** parametresinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.


A Database Error Occurred

Error Number: 1064

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' t GROUP BY `t`.`id`' at line 2

SELECT * FROM cms_users' t GROUP BY `t`.`id`

Filename: controllers/Kontrolpaneli.php

Line Number: 3902

Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

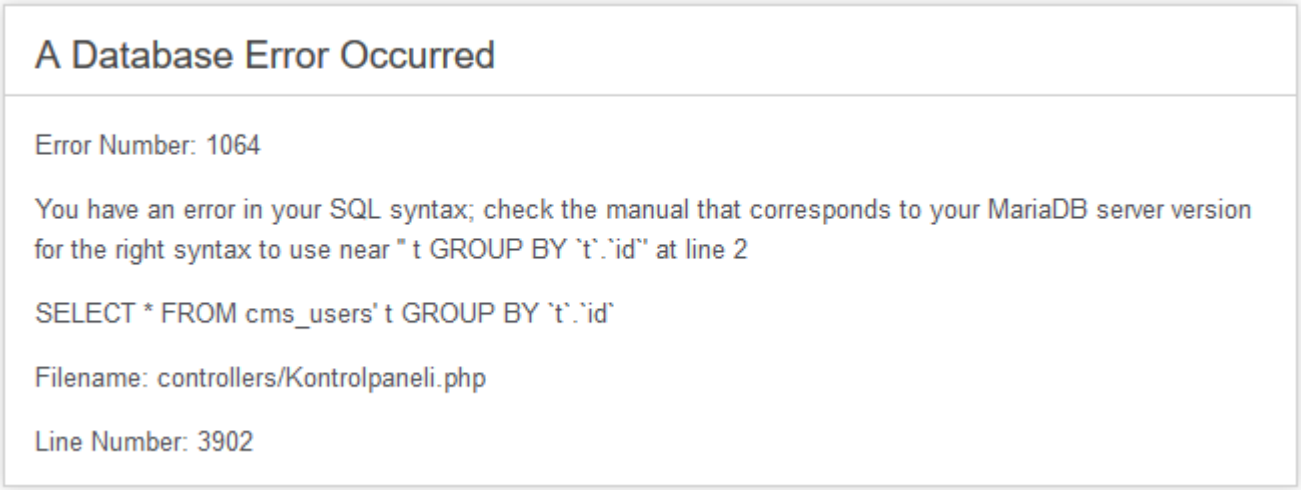
5.10. SQL Injection ile Yetki Yükseltme – tbl_getProductsTbl

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/getProductsTbl?sayfaNo=1&kacar=30&orderby=t.count&orderType=asc&category_id=&id=&marka_id=&title=&code=&barkod_no=&entegrasyon=
	Özet	Kontrol panelinde bulunan "getProductsTbl" isimli uç noktada bir veya birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **tbl_getProductsTbl** isimli uç noktadaki **orderby** parametresinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

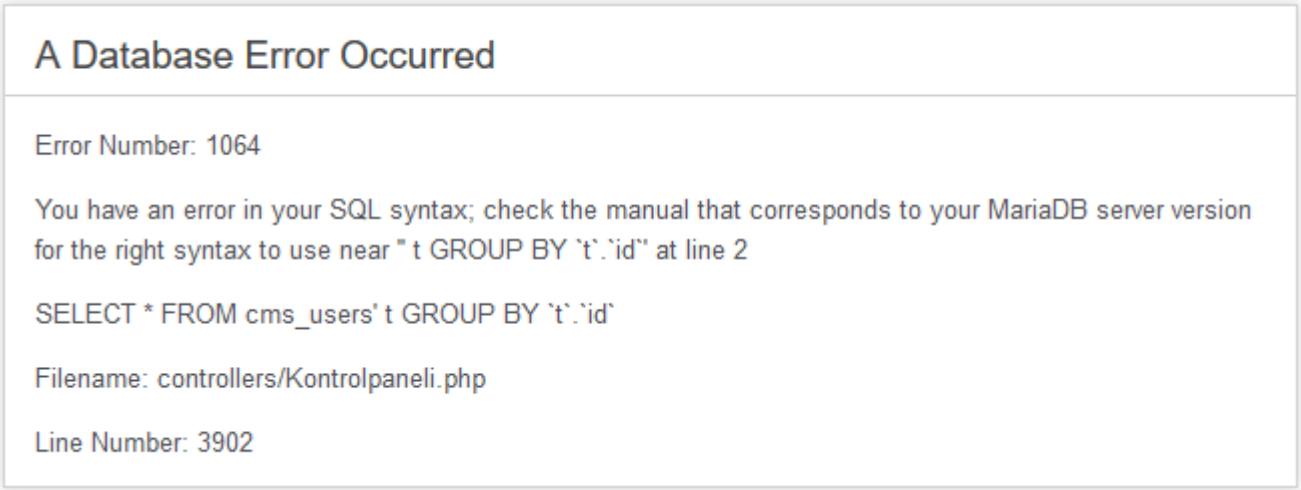
5.11. SQL Injection ile Yetki Yükseltme – rowStatus

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/rowStatus?tbl=product&status=0&id=1
	Özet	Kontrol panelinde bulunan "rowStatusUrun" isimli uç noktada bir veya birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **tbl_rowStatusUrun** isimli uç noktadaki **tbl** parametresinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

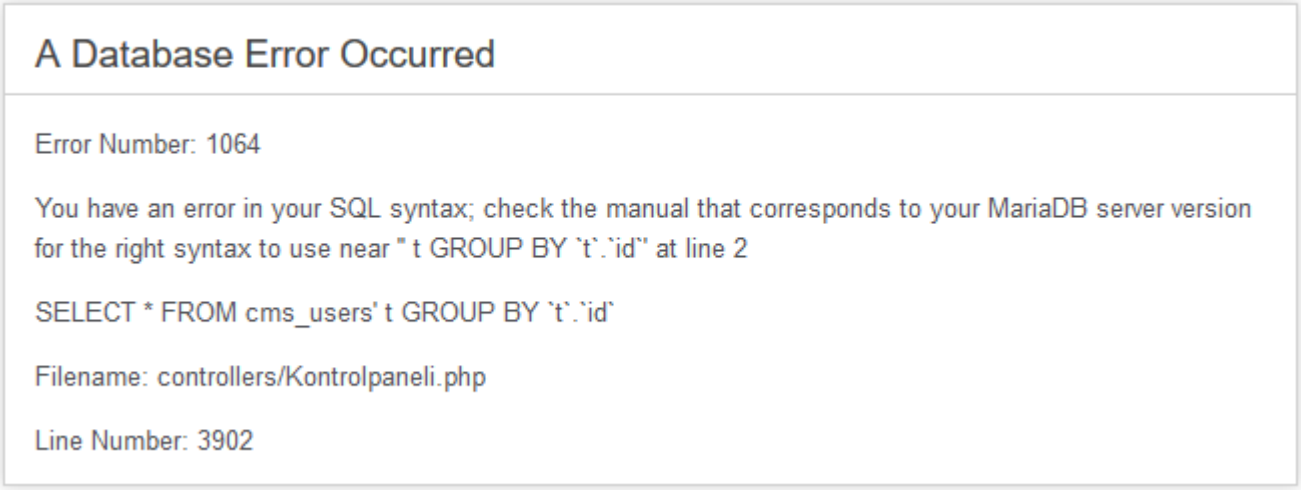
5.12. SQL Injection ile Yetki Yükseltme – tbl_get_desc_and_pagi

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/tbl_get_desc_and_pagi?tbl=product_category&sayfaNo=1&kacar=30&orderby=count&orderType=asc&id=0
	Özet	Kontrol panelinde bulunan "tbl_get_desc_and_pagi" isimli uç noktada birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **tbl_get_desc_and_pagi** uç noktadaki **tbl, where_key** ve **orderby** parametrelerinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

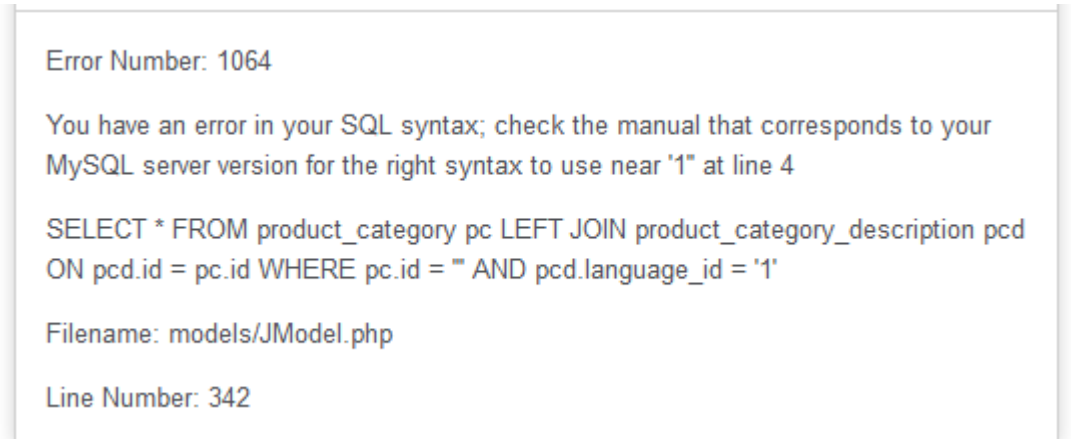
5.13. SQL Injection ile Yetki Yükseltme – renderParents

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/renderParents
	Özet	Kontrol panelinde bulunan "renderParents" isimli uç noktada bir veya birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan, POST methodu ile veri alan **renderParent** isimli uç noktadaki **id** parametresinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

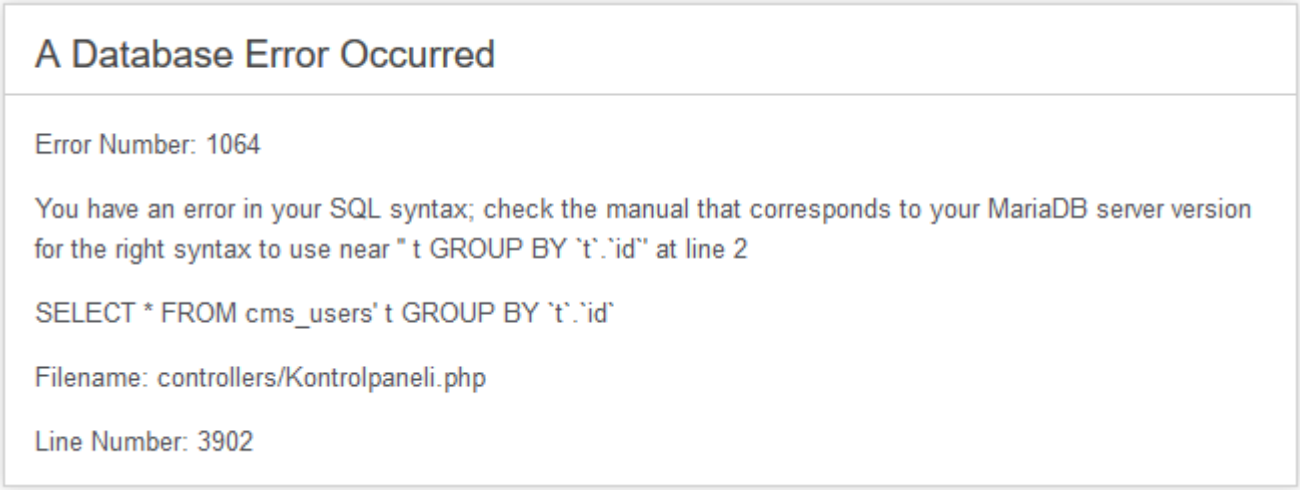
5.14. SQL Injection ile Yetki Yükseltme – deleteImage

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/deleteImage/?tbl=product_category&id=999&dirName=category
	Özet	Kontrol panelinde bulunan "deleteImage" isimli uç noktada bir veya birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **deleteImage** isimli uç noktadaki **tbl** parametresinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

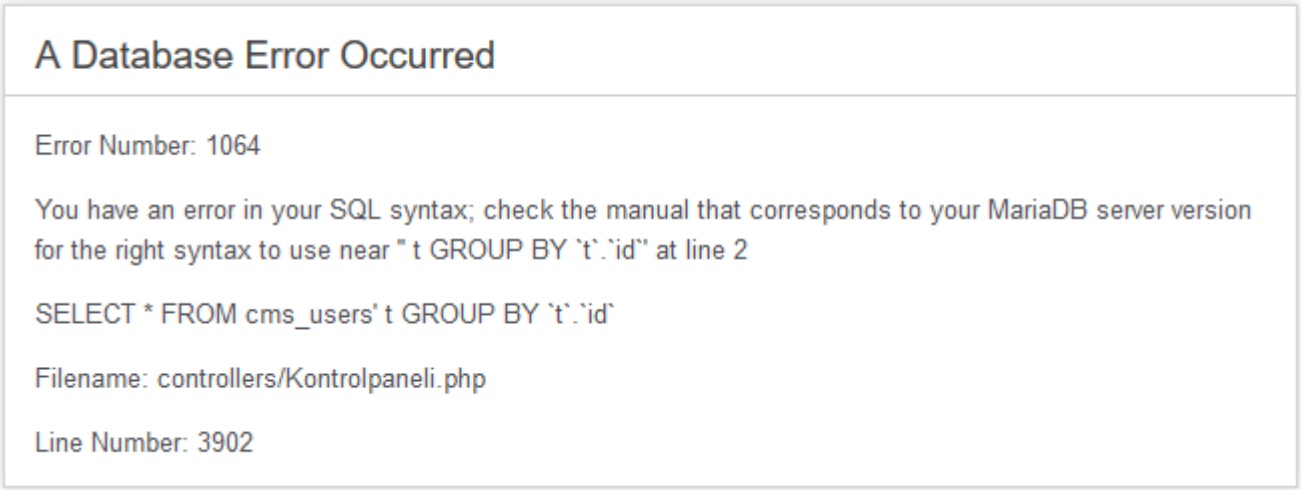
5.15. SQL Injection ile Yetki Yükseltme – delete_row_desc

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/delete_row_desc/?tbl=brand&id=21
	Özet	Kontrol panelinde bulunan "delete_row_desc" isimli uç noktada bir veya birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **delete_row_desc** isimli uç noktadaki **tbl** parametresinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.


A Database Error Occurred

Error Number: 1064

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' t GROUP BY `t`.`id`' at line 2

SELECT * FROM cms_users' t GROUP BY `t`.`id`

Filename: controllers/Kontrolpaneli.php

Line Number: 3902

Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

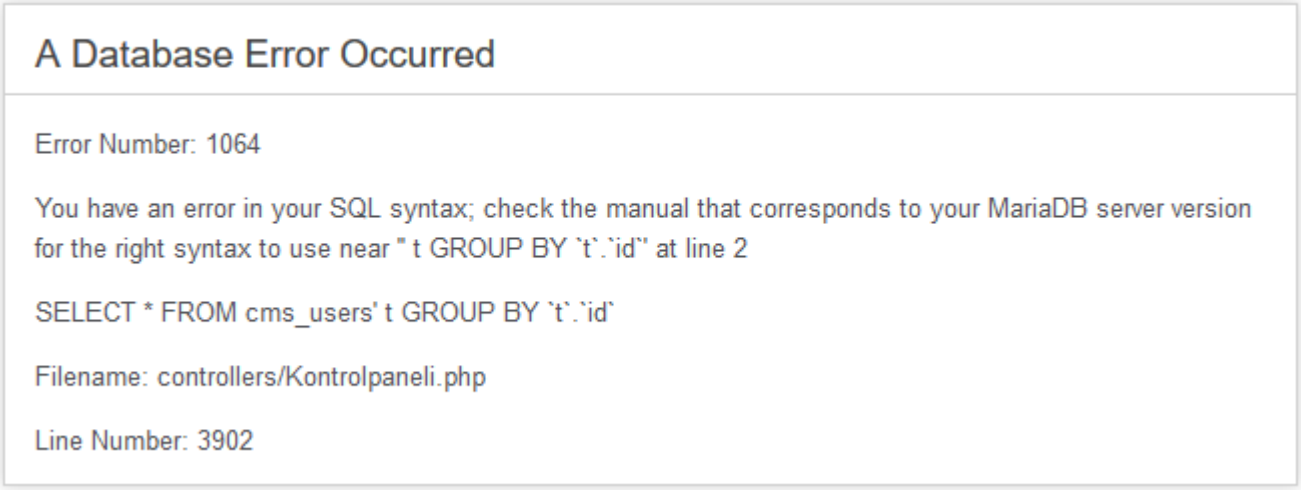
5.16. SQL Injection ile Yetki Yükseltme – tbl_get_desc_and_pagiProperty

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/tbl_get_desc_and_pagiProperty?tbl=product_properties&sayfaNo=1&kacar=30&orderby=count&orderType=asc&id=0&where_key=1%27
	Özet	Kontrol panelinde bulunan "tbl_get_desc_and_pagiProperty" isimli uç noktada bir veya birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **tbl_get_desc_and_pagiProperty** isimli uç noktadaki **tbl, orderby** ve **where_key** parametrelerinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

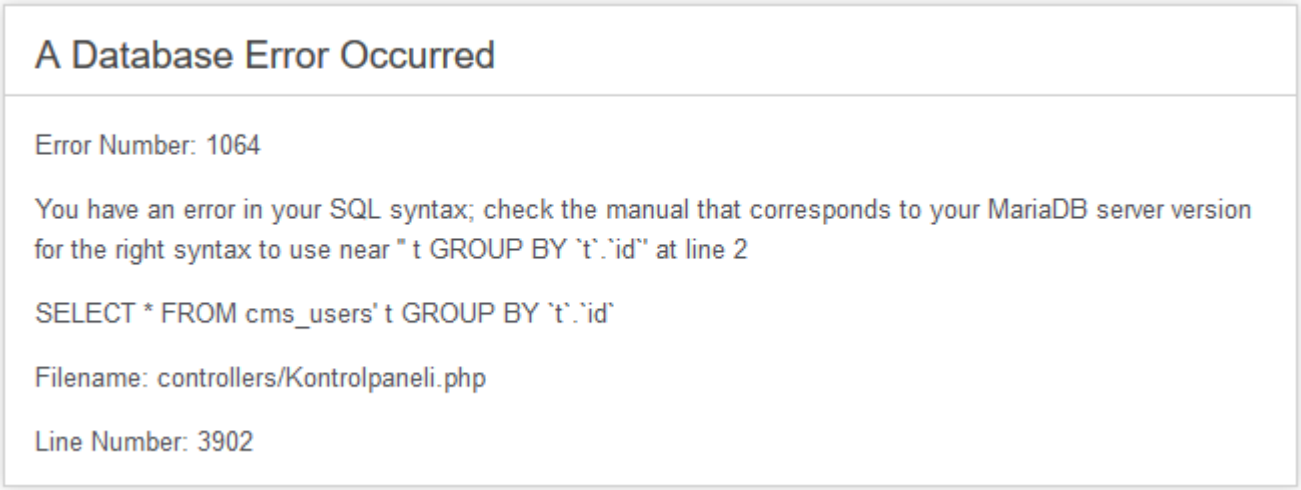
5.17. SQL Injection ile Yetki Yükseltme – tbl_get_orders

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/tbl_get_orders?sayfaNo=1&kacar=30&adi=&tc_kimlik_no=&email=&telefon=&cep_telefonu=&mahalle_id=&orderby=t.id&orderType=desc&filterForm=
	Özet	Kontrol panelinde bulunan "tbl_get_orders" isimli uç noktada bir veya birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **tbl_get_orders** isimli uç noktadaki **orderby** parametresinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

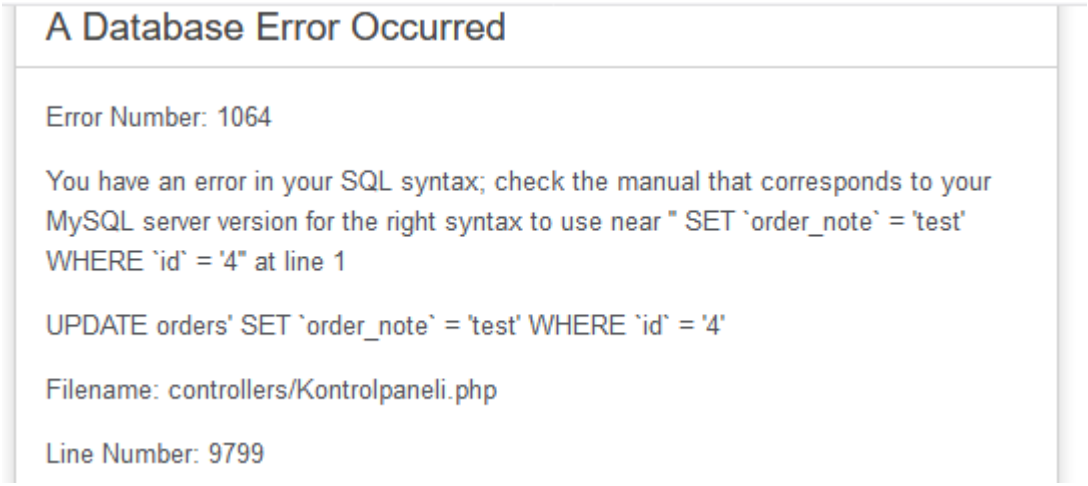
5.18. SQL Injection ile Yetki Yükseltme – update_tbl

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/update_tbl?tbl=orders%27&id=4
	Özet	Kontrol panelinde bulunan "update_tbl" isimli uç noktada bir veya birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan, POST methodu ile veri alan **update_tbl** isimli uç noktadaki **id** parametresinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

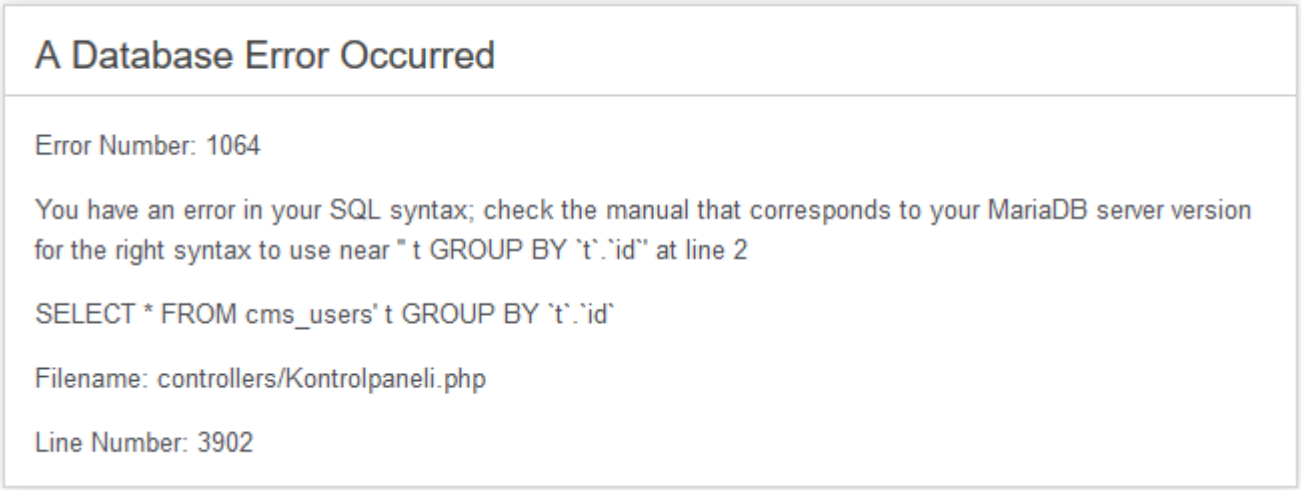
5.19. SQL Injection ile Yetki Yükseltme – delete_row_orders

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/delete_row_orders/?tbl=orders&id=4
	Özet	Kontrol panelinde bulunan "delete_row_orders" isimli uç noktada bir veya birden çok parametrede SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **delete_row_orders** isimli uç noktadaki **tbl** parametresinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

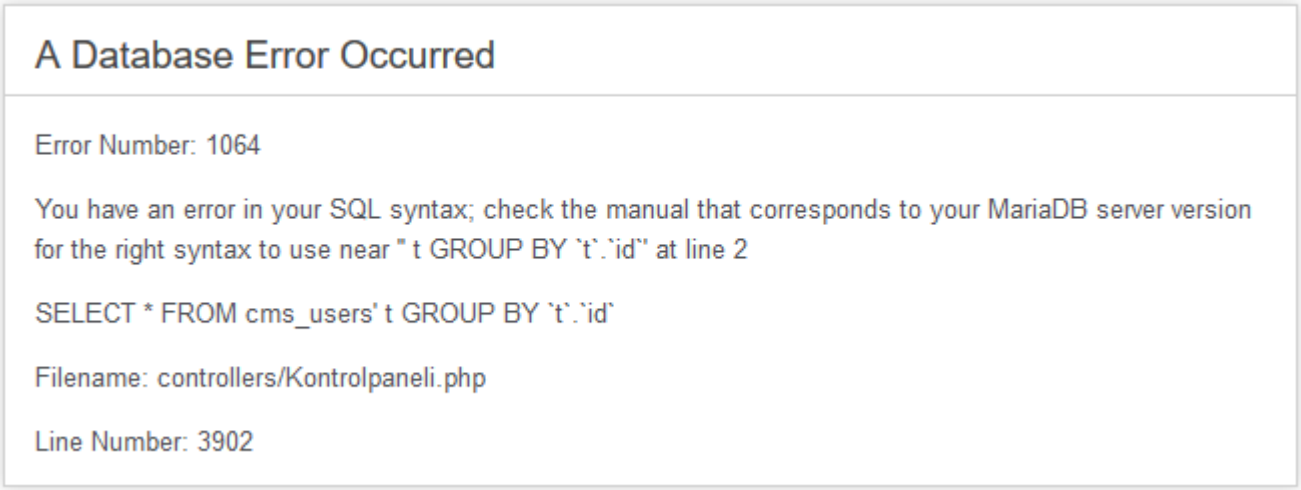
5.20. SQL Injection ile Yetki Yükseltme – tbl_get_member

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme – tbl_get_member**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/tbl_get_member?tbl=member&sayfaNo=1&kacar=30&member_id=&adi=&tc_kimlik_no=&email=&cep_telefonu=&orderby=t.id&orderType=desc&where_key=1
	Özet	Kontrol panelinde bulunan Tbl_get_member isimli bileşende birden çok SQL Injection keşfedilmiştir

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **tbl_get_member** uç noktasındaki **tbl, where_key** ve **orderby** parametrelerinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

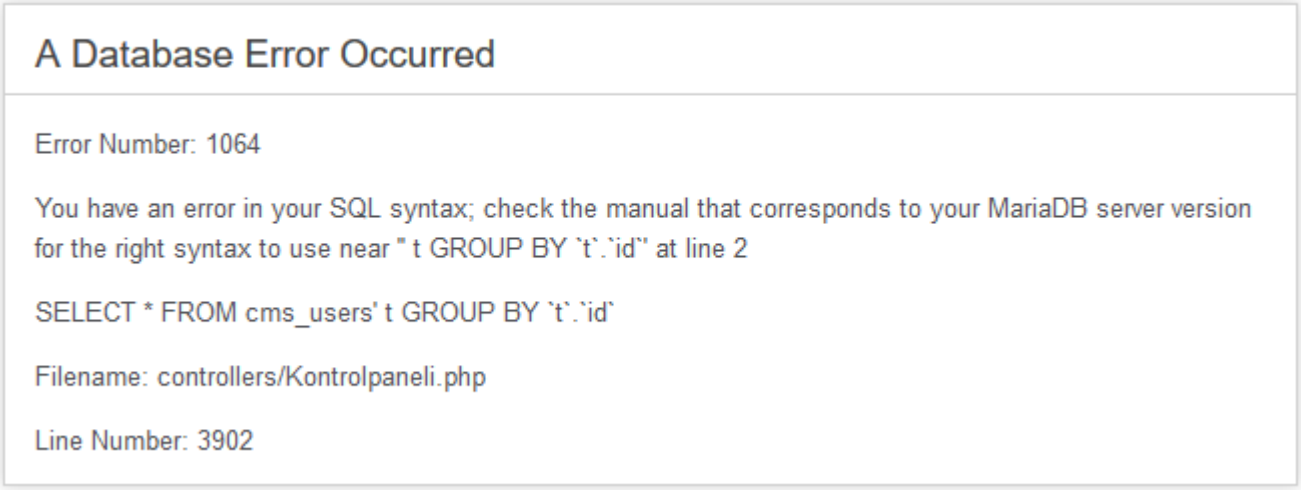
5.21. SQL Injection ile Yetki Yükseltme – tbl_get_full

YÜKSEK	**Bulgu Adı**	**SQL Injection ile Yetki Yükseltme – tbl_get_full**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/tbl_get_full/?tbl=bank_account&join=bank&join_id=bank_id&where=account_type&where_value=banka
	Özet	Kontrol panelinde bulunan Tbl_get_full isimli bileşende bir veya birden çok SQL Injection keşfedilmiştir.

Bulgu Açıklaması

SQL injection, veritabanınızı tahrip edebilecek kötü amaçlı bir kod yerleştirme tekniğidir. SQL injection ile saldırganlar web sitesindeki kullanıcı bilgilerini çalabilir, gizlenmiş bilgilere ulaşabilir, mevcut verilere müdahale edebilir, bazı işlemleri değiştirebilir, yetkisini yükseltebilir, veritabanının tamamını silebilir.

Kontrol panelinde bulunan ve kullanım için yetkiye ihtiyaç duyan **tbl_get_full** uç noktasındaki **tbl, join** ve **where** parametrelerinde SQL Injection keşfedilmiştir. Bileşenin yönetici yetkisi gerektirmesi sebebiyle, bulgu önem derecesi ACİL yerine KRİTİK seçilmiştir. Yetkisi olmayan yöneticilerin yetkisi dışında işlem yapabilmesini sağlamaktadır.



Çözüm Önerisi

İlgili uç noktadaki veritabanı işlemini gerçekleştiren kodda PDO prepare/execute methodları kullanılarak, kullanıcıdan alınan verinin filtrelenmesi tavsiye edilir.

5.22. Yetki Yükseltme – tbl_get

YÜKSEK	**Bulgu Adı**	**Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/tbl_get?tbl=cms_users
	Özet	Yöneticiler tablosunun, yönetici düzenleme ve görme yetkisi olmayan kullanıcılar tarafından okunabildiği keşfedilmiştir.

Bulgu Açıklaması

Yönetim panelinde bazı veri getirme işlemlerini gerçekleştiren **tbl_get** bileşeninin **tbl** isimli parametresinin tablo ismi aldığı görülmüştür. Bu parametre, yönetici bilgilerinin saklandığı tablonun ismi olan **cms_users** olarak düzenlendiğinde, yöneticilerin şifresi dahil olmak üzere tüm bilgilerine Izinsiz olarak erişilebildiği keşfedilmiştir. Bu durum yetkisi düşük yöneticilerin yetkisini yükseltebilmesine ve yüksek yetkili yönetici hesaplarının şifrelerinin ele geçirilmesine yol açmaktadır.

{"kayitSayisi":1,"sayfaSayisi":1,"veriler":[{"id":"32","name":"ugur","surname":null,"email":null,"username":"admin","pass":"[redacted],"yetki":"
[\"Anasayfa\",\"\\u0130\\u015flem Kay\\u0131tlar\\u0131\",\"\\u00dcr\\u00fcnler\",\"\\u00dcr\\u00fcn
Ekle\\/D\\u00fczenle\",\"Kategoriler\",\"Markalar\",\"\\u00dcr\\u00fcn \\u00d6zellikleri\",\"Varyant Sistemi\",\"Sepet
Varyantlar\\u0131\",\"\\u00dcr\\u00fcn Stok G\\u00fcncelleme\",\"Sipari\\u015fler\",\"Kredi Kart\\u0131 Hatal\\u0131
\\u00d6demeler\",\"Sipari\\u015f Rapor\",\"Toplam Sat\\u0131\\u015f\",\"Sayfalar\",\"Statik Sayfalar\",\"Slider Y\\u00f6netimi\",\"2 li
Slider\",\"Orta Kategori G\\u00f6rselleri\",\"Yorum ve \\u00d6neriler\",\"\\u00dcye\\/Bayi Y\\u00f6netimi\",\"Yeni \\u00dcye
Kayd\\u0131\",\"Mahalleler\",\"Genel Ayarlar\",\"Sistem Ayarlar\\u0131\",\"Alt Men\\u00fc Y\\u00f6netimi\",\"Dil Ayarlar\\u0131\",\"Dil
\\u00c7evirileri\",\"Seo\",\"\\u00d6deme
Ayarlar\\u0131\",\"Y\\u00f6neticiler\"]","status":"1","is_admin":null,"webanya_username":null,"date_added":null,"date_modified":null,"count":n

Çözüm Önerisi

Tbl_get bileşenindeki **tbl** parametresinde beyaz liste yaklaşımı uygulanarak, sadece kullanılması gerekli olan tablo isimlerinin girilmesine izin verilmelidir.

5.23. Yetki Yükseltme – tbl_get_full

YÜKSEK	**Bulgu Adı**	**Yetki Yükseltme**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/tbl_get_full?tbl=cms_users
	Özet	Yöneticiler tablosunun, yönetici düzenleme ve görme yetkisi olmayan kullanıcılar tarafından okunabildiği keşfedilmiştir.

Bulgu Açıklaması

Yönetim panelinde bazı veri getirme işlemlerini gerçekleştiren **tbl_get_full** bileşeninin **tbl** isimli parametresinin tablo ismi aldığı görülmüştür. Bu parametre, yönetici bilgilerinin saklandığı tablonun ismi olan **cms_users** olarak düzenlendiğinde, yöneticilerin şifresi dahil olmak üzere tüm bilgilerine Izinsiz olarak erişilebildiği keşfedilmiştir. Bu durum yetkisi düşük yöneticilerin yetkisini yükseltebilmesine ve yüksek yetkili yönetici hesaplarının şifrelerinin ele geçirilmesine yol açmaktadır.

{"kayitSayisi":1,"sayfaSayisi":1,"veriler":[{"id":"32","name":"ugur","surname":null,"email":null,"username":"admin","pass":"[redacted],"yetki":"
[\"Anasayfa\",\"\\u0130\\u015flem Kay\\u0131tlar\\u0131\",\"\\u00dcr\\u00fcnler\",\"\\u00dcr\\u00fcn
Ekle\\/D\\u00fczenle\",\"Kategoriler\",\"Markalar\",\"\\u00dcr\\u00fcn \\u00d6zellikleri\",\"Varyant Sistemi\",\"Sepet
Varyantlar\\u0131\",\"\\u00dcr\\u00fcn Stok G\\u00fcncelleme\",\"Sipari\\u015fler\",\"Kredi Kart\\u0131 Hatal\\u0131
\\u00d6demeler\",\"Sipari\\u015f Rapor\",\"Toplam Sat\\u0131\\u015f\",\"Sayfalar\",\"Statik Sayfalar\",\"Slider Y\\u00f6netimi\",\"2 li
Slider\",\"Orta Kategori G\\u00f6rselleri\",\"Yorum ve \\u00d6neriler\",\"\\u00dcye\\/Bayi Y\\u00f6netimi\",\"Yeni \\u00dcye
Kayd\\u0131\",\"Mahalleler\",\"Genel Ayarlar\",\"Sistem Ayarlar\\u0131\",\"Alt Men\\u00fc Y\\u00f6netimi\",\"Dil Ayarlar\\u0131\",\"Dil
\\u00c7evirileri\",\"Seo\",\"\\u00d6deme
Ayarlar\\u0131\",\"Y\\u00f6neticiler\"]","status":"1","is_admin":null,"webanya_username":null,"date_added":null,"date_modified":null,"count":n

Çözüm Önerisi

Tbl_get bileşenindeki **tbl** parametresinde beyaz liste yaklaşımı uygulanarak, sadece kullanılması gerekli olan tablo isimlerinin girilmesine izin verilmelidir.

5.24. Improper Input Validation – Slider Masaüstü

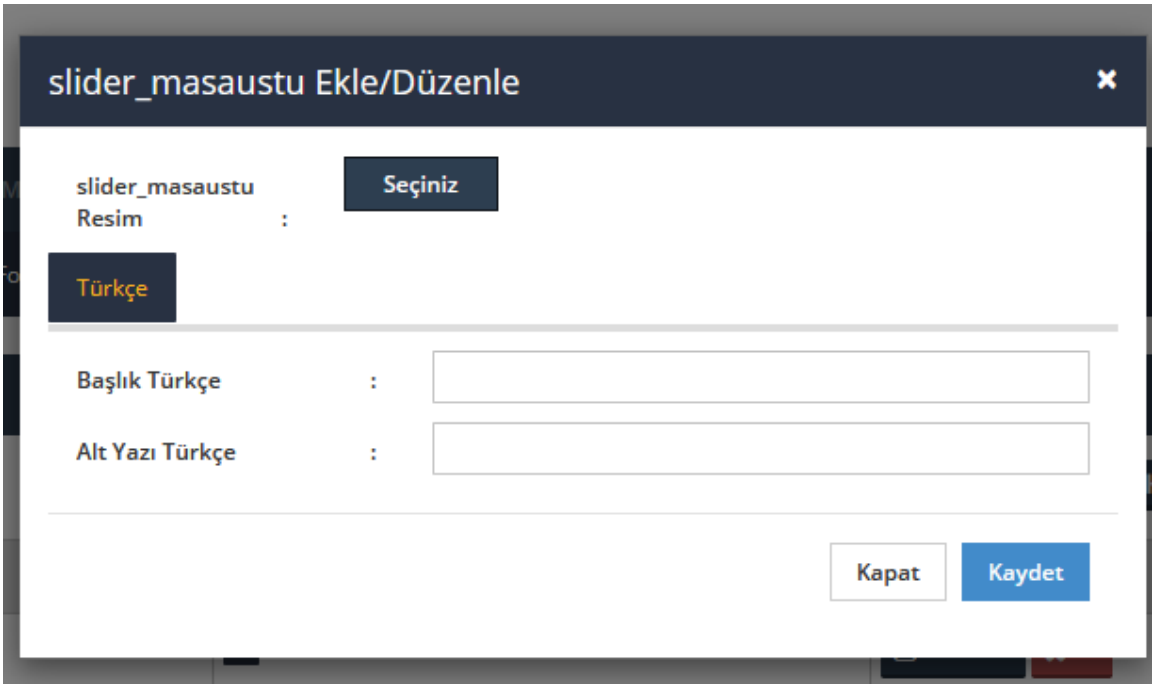
ORTA	**Bulgu Adı**	**Improper Input Validation**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/slider_masaustu
	Özet	Kullanıcıdan alınan birden fazla parametrenin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Bulgu Açıklaması

Girdi doğrulama, girdilerin kod içinde veya diğer bileşenlerle iletişim kurarken güvenli şekilde işlendiğinden emin olmak için potansiyel olarak tehlikeli girdileri kontrol etmek için sık kullanılan bir tekniktir. Yazılım girdiyi düzgün bir şekilde doğrulamadığında, saldırgan girdiyi uygulamanın geri kalanı tarafından beklenmeyen bir biçimde oluşturabilir. Bu, sistemin bazı kısımlarının istenmeyen girdi almasına yol açar ve bu da kontrol akışının değişmesine, bir kaynağın keyfi kontrolüne veya rastgele kod yürütülmesine neden olabilir.

Örneğin, E-Posta adresi yerine gönderilen farklı girdiler SMTP sunucusunda hata meydana getirebilir.

İletişim sayfasında bulunan girdilerin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.



Çözüm Önerisi

Tüm girdilerin kötü amaçlı olduğunu varsayarak sunucu tarafında girdi doğrulama stratejisi kullanılmalı, yani spesifikasyonlara tam olarak uyan girdiler kabul edilebilmeli. Spesifikasyonlara tam olarak uymayan herhangi bir girdi ise reddedilmelidir.
Sunucu tarafında girdilerin RegEx ile kontrol edilmesi tavsiye edilir.

5.25. Improper Input Validation – Alt Slider

Bulgu Adı	**Improper Input Validation**
Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/slider_alt
Özet	Kullanıcıdan alınan birden fazla parametrenin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Bulgu Açıklaması

Girdi doğrulama, girdilerin kod içinde veya diğer bileşenlerle iletişim kurarken güvenli şekilde işlendiğinden emin olmak için potansiyel olarak tehlikeli girdileri kontrol etmek için sık kullanılan bir tekniktir. Yazılım girdiyi düzgün bir şekilde doğrulamadığında, saldırgan girdiyi uygulamanın geri kalanı tarafından beklenmeyen bir biçimde oluşturabilir. Bu, sistemin bazı kısımlarının istenmeyen girdi almasına yol açar ve bu da kontrol akışının değişmesine, bir kaynağın keyfi kontrolüne veya rastgele kod yürütülmesine neden olabilir.

Örneğin, E-Posta adresi yerine gönderilen farklı girdiler SMTP sunucusunda hata meydana getirebilir.

İletişim sayfasında bulunan girdilerin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Çözüm Önerisi

Tüm girdilerin kötü amaçlı olduğunu varsayarak sunucu tarafında girdi doğrulama stratejisi kullanılmalı, yani spesifikasyonlara tam olarak uyan girdiler kabul edilebilmeli. Spesifikasyonlara tam olarak uymayan herhangi bir girdi ise reddedilmelidir.
Sunucu tarafında girdilerin RegEx ile kontrol edilmesi tavsiye edilir.

5.26. Improper Input Validation – Otobüs Firmaları Ekle

Bulgu Adı	**Improper Input Validation**
Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/otobus_firma
Özet	Kullanıcıdan alınan birden fazla parametrenin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Bulgu Açıklaması

Girdi doğrulama, girdilerin kod içinde veya diğer bileşenlerle iletişim kurarken güvenli şekilde işlendiğinden emin olmak için potansiyel olarak tehlikeli girdileri kontrol etmek için sık kullanılan bir tekniktir. Yazılım girdiyi düzgün bir şekilde doğrulamadığında, saldırgan girdiyi uygulamanın geri kalanı tarafından beklenmeyen bir biçimde oluşturabilir. Bu, sistemin bazı kısımlarının istenmeyen girdi almasına yol açar ve bu da kontrol akışının değişmesine, bir kaynağın keyfi kontrolüne veya rastgele kod yürütülmesine neden olabilir.

Örneğin, E-Posta adresi yerine gönderilen farklı girdiler SMTP sunucusunda hata meydana getirebilir.

İletişim sayfasında bulunan girdilerin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Çözüm Önerisi

Tüm girdilerin kötü amaçlı olduğunu varsayarak sunucu tarafında girdi doğrulama stratejisi kullanılmalı, yani spesifikasyonlara tam olarak uyan girdiler kabul edilebilmeli. Spesifikasyonlara tam olarak uymayan herhangi bir girdi ise reddedilmelidir.
Sunucu tarafında girdilerin RegEx ile kontrol edilmesi tavsiye edilir.

5.27. Improper Input Validation – Havayolu Ekle

	**Bulgu Adı**	**Improper Input Validation**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/havayolu/
	Özet	Kullanıcıdan alınan birden fazla parametrenin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Bulgu Açıklaması

Girdi doğrulama, girdilerin kod içinde veya diğer bileşenlerle iletişim kurarken güvenli şekilde işlendiğinden emin olmak için potansiyel olarak tehlikeli girdileri kontrol etmek için sık kullanılan bir tekniktir. Yazılım girdiyi düzgün bir şekilde doğrulamadığında, saldırgan girdiyi uygulamanın geri kalanı tarafından beklenmeyen bir biçimde oluşturabilir. Bu, sistemin bazı kısımlarının istenmeyen girdi almasına yol açar ve bu da kontrol akışının değişmesine, bir kaynağın keyfi kontrolüne veya rastgele kod yürütülmesine neden olabilir.

Örneğin, E-Posta adresi yerine gönderilen farklı girdiler SMTP sunucusunda hata meydana getirebilir.

İletişim sayfasında bulunan girdilerin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Çözüm Önerisi

Tüm girdilerin kötü amaçlı olduğunu varsayarak sunucu tarafında girdi doğrulama stratejisi kullanılmalı, yani spesifikasyonlara tam olarak uyan girdiler kabul edilebilmeli. Spesifikasyonlara tam olarak uymayan herhangi bir girdi ise reddedilmelidir.
Sunucu tarafında girdilerin RegEx ile kontrol edilmesi tavsiye edilir.

5.28. Improper Input Validation – Oteller

	**Bulgu Adı**	**Improper Input Validation**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/otel/
	Özet	Kullanıcıdan alınan birden fazla parametrenin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Bulgu Açıklaması

Girdi doğrulama, girdilerin kod içinde veya diğer bileşenlerle iletişim kurarken güvenli şekilde işlendiğinden emin olmak için potansiyel olarak tehlikeli girdileri kontrol etmek için sık kullanılan bir tekniktir. Yazılım girdiyi düzgün bir şekilde doğrulamadığında, saldırgan girdiyi uygulamanın geri kalanı tarafından beklenmeyen bir biçimde oluşturabilir. Bu, sistemin bazı kısımlarının istenmeyen girdi almasına yol açar ve bu da kontrol akışının değişmesine, bir kaynağın keyfi kontrolüne veya rastgele kod yürütülmesine neden olabilir.

Örneğin, E-Posta adresi yerine gönderilen farklı girdiler SMTP sunucusunda hata meydana getirebilir.

İletişim sayfasında bulunan girdilerin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Çözüm Önerisi

Tüm girdilerin kötü amaçlı olduğunu varsayarak sunucu tarafında girdi doğrulama stratejisi kullanılmalı, yani spesifikasyonlara tam olarak uyan girdiler kabul edilebilmeli. Spesifikasyonlara tam olarak uymayan herhangi bir girdi ise reddedilmelidir.
Sunucu tarafında girdilerin RegEx ile kontrol edilmesi tavsiye edilir.

5.29. Improper Input Validation – Restaurant Ekle

Bulgu Adı	**Improper Input Validation**
Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/restaurant_form/
Özet	Kullanıcıdan alınan birden fazla parametrenin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Bulgu Açıklaması

Girdi doğrulama, girdilerin kod içinde veya diğer bileşenlerle iletişim kurarken güvenli şekilde işlendiğinden emin olmak için potansiyel olarak tehlikeli girdileri kontrol etmek için sık kullanılan bir tekniktir. Yazılım girdiyi düzgün bir şekilde doğrulamadığında, saldırgan girdiyi uygulamanın geri kalanı tarafından beklenmeyen bir biçimde oluşturabilir. Bu, sistemin bazı kısımlarının istenmeyen girdi almasına yol açar ve bu da kontrol akışının değişmesine, bir kaynağın keyfi kontrolüne veya rastgele kod yürütülmesine neden olabilir.

Örneğin, E-Posta adresi yerine gönderilen farklı girdiler SMTP sunucusunda hata meydana getirebilir.

İletişim sayfasında bulunan girdilerin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Çözüm Önerisi

Tüm girdilerin kötü amaçlı olduğunu varsayarak sunucu tarafında girdi doğrulama stratejisi kullanılmalı, yani spesifikasyonlara tam olarak uyan girdiler kabul edilebilmeli. Spesifikasyonlara tam olarak uymayan herhangi bir girdi ise reddedilmelidir.
Sunucu tarafında girdilerin RegEx ile kontrol edilmesi tavsiye edilir.

5.30. Improper Input Validation – Rota Ekle

	**Bulgu Adı**	**Improper Input Validation**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/rotalar/
	Özet	Kullanıcıdan alınan birden fazla parametrenin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Bulgu Açıklaması

Girdi doğrulama, girdilerin kod içinde veya diğer bileşenlerle iletişim kurarken güvenli şekilde işlendiğinden emin olmak için potansiyel olarak tehlikeli girdileri kontrol etmek için sık kullanılan bir tekniktir. Yazılım girdiyi düzgün bir şekilde doğrulamadığında, saldırgan girdiyi uygulamanın geri kalanı tarafından beklenmeyen bir biçimde oluşturabilir. Bu, sistemin bazı kısımlarının istenmeyen girdi almasına yol açar ve bu da kontrol akışının değişmesine, bir kaynağın keyfi kontrolüne veya rastgele kod yürütülmesine neden olabilir.

Örneğin, E-Posta adresi yerine gönderilen farklı girdiler SMTP sunucusunda hata meydana getirebilir.

İletişim sayfasında bulunan girdilerin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Çözüm Önerisi

Tüm girdilerin kötü amaçlı olduğunu varsayarak sunucu tarafında girdi doğrulama stratejisi kullanılmalı, yani spesifikasyonlara tam olarak uyan girdiler kabul edilebilmeli. Spesifikasyonlara tam olarak uymayan herhangi bir girdi ise reddedilmelidir.
Sunucu tarafında girdilerin RegEx ile kontrol edilmesi tavsiye edilir.

5.31. Improper Input Validation – Mekan Kategorileri Ekle

Bulgu Adı	**Improper Input Validation**
Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli/mekan_kategori
Özet	Kullanıcıdan alınan birden fazla parametrenin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Bulgu Açıklaması

Girdi doğrulama, girdilerin kod içinde veya diğer bileşenlerle iletişim kurarken güvenli şekilde işlendiğinden emin olmak için potansiyel olarak tehlikeli girdileri kontrol etmek için sık kullanılan bir tekniktir. Yazılım girdiyi düzgün bir şekilde doğrulamadığında, saldırgan girdiyi uygulamanın geri kalanı tarafından beklenmeyen bir biçimde oluşturabilir. Bu, sistemin bazı kısımlarının istenmeyen girdi almasına yol açar ve bu da kontrol akışının değişmesine, bir kaynağın keyfi kontrolüne veya rastgele kod yürütülmesine neden olabilir.

Örneğin, E-Posta adresi yerine gönderilen farklı girdiler SMTP sunucusunda hata meydana getirebilir.

İletişim sayfasında bulunan girdilerin sunucu tarafında kontrolünün yapılmadığı gözlemlenmiştir.

Çözüm Önerisi

Tüm girdilerin kötü amaçlı olduğunu varsayarak sunucu tarafında girdi doğrulama stratejisi kullanılmalı, yani spesifikasyonlara tam olarak uyan girdiler kabul edilebilmeli. Spesifikasyonlara tam olarak uymayan herhangi bir girdi ise reddedilmelidir.
Sunucu tarafında girdilerin RegEx ile kontrol edilmesi tavsiye edilir.

5.32. Captcha Güvenlik Önlemi Eksikliği – Kontrol Paneli

Bulgu Adı	**Captcha Güvenlik Önlemi Eksikliği**
Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli
Özet	Kontrol Paneline girişte Captcha doğrulama kontrolü eksikliği gözlemlenmiştir.

Bulgu Açıklaması

Yapılan testler esnasında yönetim kullanıcı girişine ait Kontrol Paneli bölümünde Captcha kulanılmadığı belirlenmiştir. Captcha, her oturum açma aşamasında rastgele karakterler veya resimler çıkartılarak kulanıcı tarafından doğrulanması işlemidir. Bu yöntem saldırganların system üzerinde erişim elde edememeleri için uygulanan ek bir güvenlik önlemidir. Captcha kulanılmayan kimlik doğrulama arabirimlerinde, saldırganlar çeşitli otomalize araçlar kullanarak bu web form ve girişlerine sözlük ve kaba kuvvet saldırıları gerçekleştirebilirler. Bu şekilde, kullanıcı hesapları veya yönetim panelindeki yönetici hesabı ele geçirilebilir.

Çözüm Önerisi

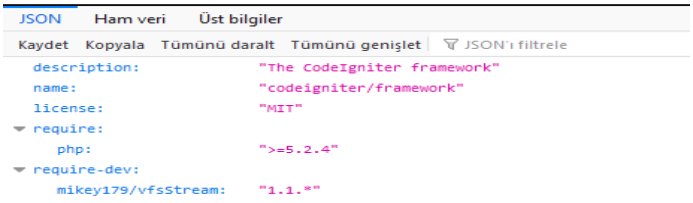
İlgili sayfada CAPTCHA ile kontrol yapılması önerilir.

5.33. Hassas Veri Sızıntısı

DÜŞÜK	**Bulgu Adı**	**Hassas Veri Sızıntısı**
	Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/composer.json
	Özet	Codeigniter ile alakalı bir konfigürasyon dosyasının bazı hassas verileri içerdiği ve bu dosyanın dışa açık olduğu gözlemlenmiştir

Bulgu Açıklaması

Codeigniter ile alakalı bir konfigürasyon dosyasının bazı hassas verileri içerdiği ve bu dosyanın dışa açık olduğu gözlemlenmiştir. Bu dosya içerisindeki versiyon verileri saldırganlara bilgi toplamak için yardımcı olabilir. Dosyadaki uygulamaların birinde zafiyet keşfedilmesi durumunda saldırganın işi kolaylaşacaktır. Bu dosyaların silinmesi veya erişimin engellenmesi tavsiye edilir.



Çözüm Önerisi

.htaccess dosyasına aşağıdaki kodlar yazılarak “package.json” ve “composer.json” isimli dosyalara erişim engellenebilir.

```
<FilesMatch ^((composer|package)\.json)$>
    Deny from all
</FilesMatch>
```

5.34. Kolay Erişilebilir Kontrol Paneli

Bulgu Adı	**Kolay Erişilebilir Kontrol Paneli**
Erişim Noktası	https://kirikkale.profesyonelwebyazilimi.com/kontrolpaneli
Özet	Kontrol paneli yolunun tahmin edilebilir ve dictionary attack yazılımları ile kolay keşfedilebilir olduğu gözlemlenmiştir.

Bulgu Açıklaması

Kontrol paneli yolunun tahmin edilebilir ve dictionary attack yazılımları ile kolay keşfedilebilir olduğu gözlemlenmiştir. Bu durum yönetici kullanıcı adı ve şifrelere yönelik brute-force saldırılarının denenebilmesine yol açabilmektedir.

Çözüm Önerisi

Kontrol paneli yolunun tahmin edilemeyecek ve dictionary attack yazılımları ile kolay keşfedilemeyecek bir dizin ismi ile değiştirilmesi tavsiye edilir.