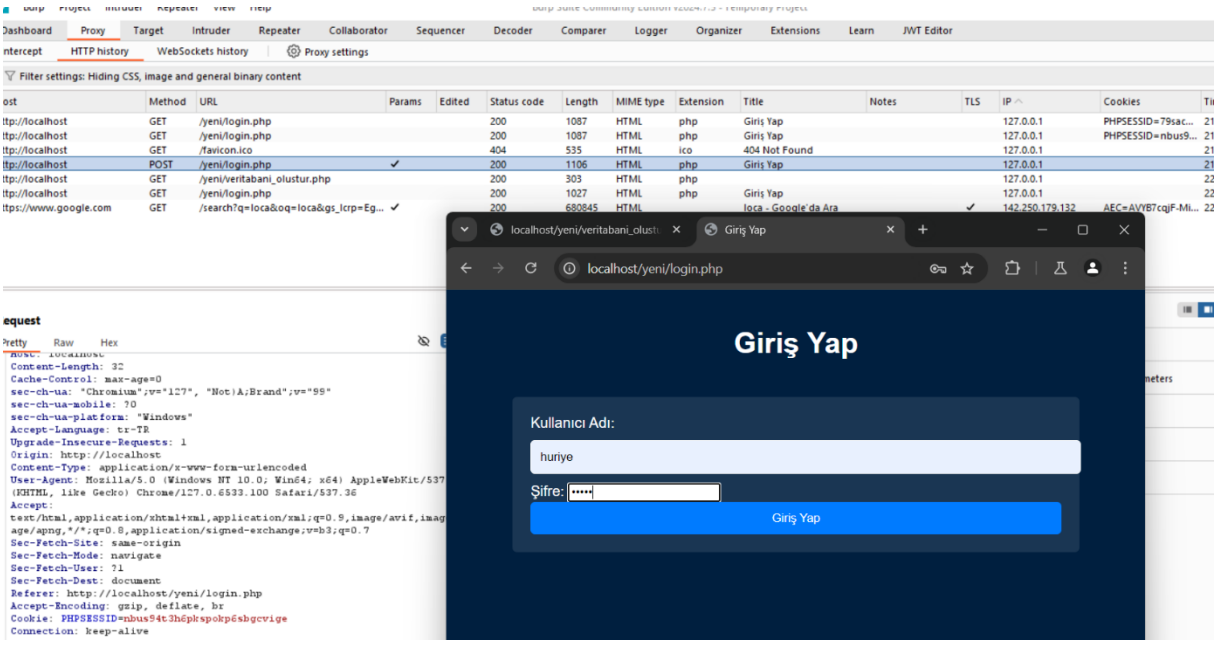
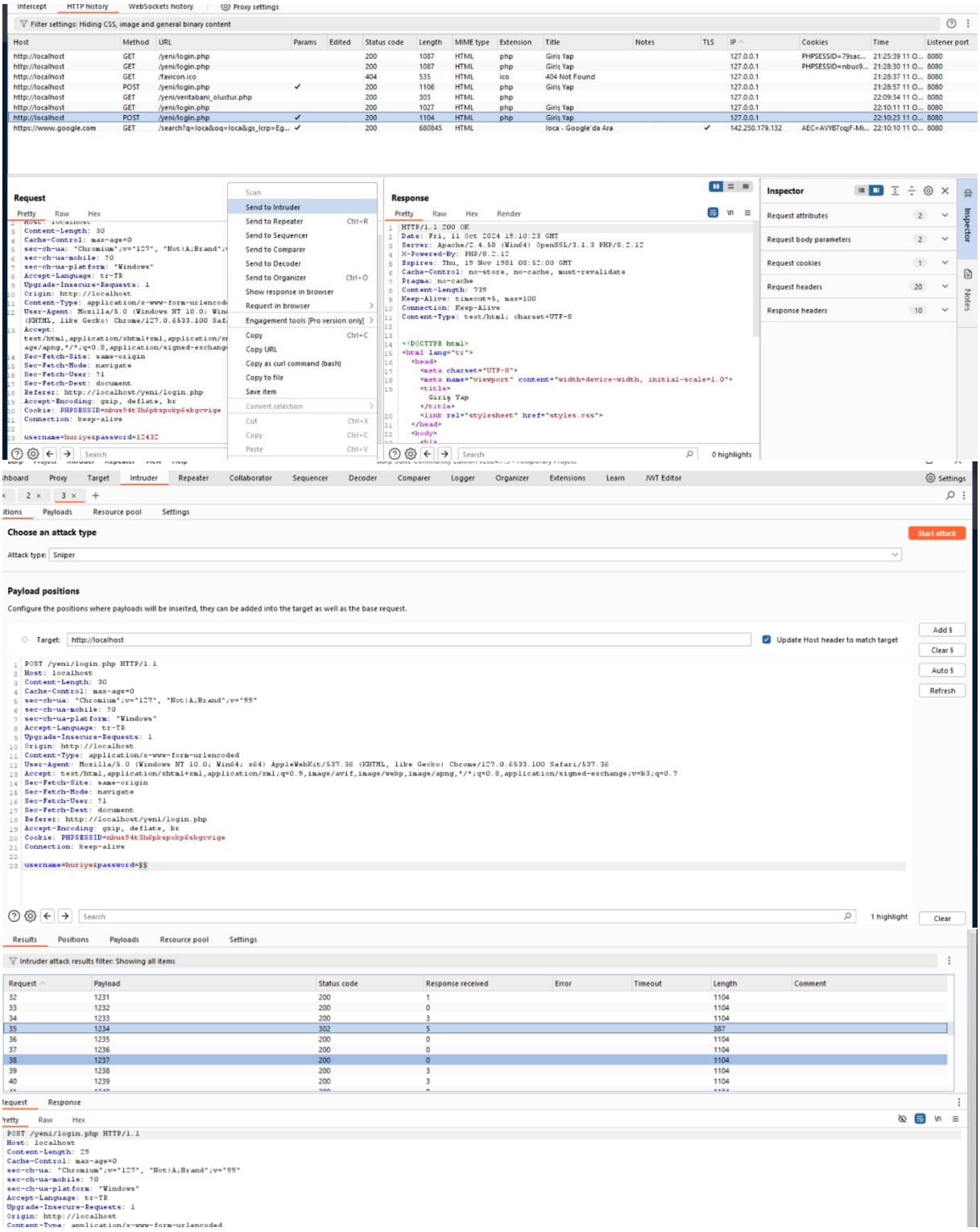
Zayıf Şifreleme

Zafiyet:
Şifreler hash('sha256', $password) fonksiyonu ile şifreleniyor. SHA-256, şifreleme için güvenli bir algoritma değildir ve güçlü bir tuzlama mekanizması ile birleştirilmediğinde zayıf kalır.
Nerde Oluştu: login.php
Neler yapılabilir?
Zayıf şifreleme, özellikle SHA-256 gibi tuzlanmamış veya zayıf bir şekilde hashlenmiş şifrelerin kullanılması durumunda ciddi güvenlik riskleri oluşturabilir. SHA-256 bir kriptografik hash algoritması olsa da, parola hashleme için uygun değildir çünkü saldırganlar rainbow tabloları veya brute-force saldırıları ile zayıf tuzlama olmadan SHA-256 hashlerini kolayca çözebilirler.
Brute Force atarak gösterelim:



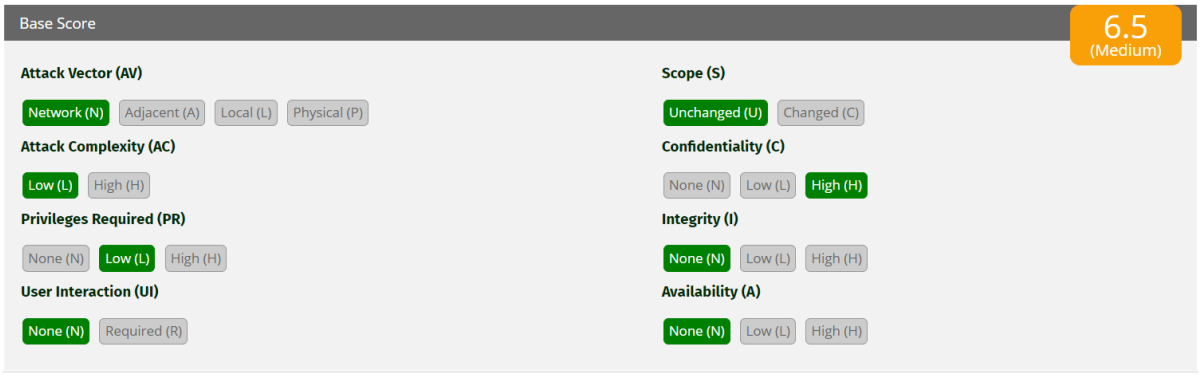


Bu şekilde bulmuş olduk şifreyi.

Öneri:

PHP'de password_hash() fonksiyonunu kullanarak şifreleri daha güvenli bir şekilde hash'leyin. Bu, hem daha güvenli bir algoritma kullanır hem de otomatik olarak tuz ekler.

CVSS:



Cross-Site Scripting (XSS)

Nerede olabilir?

- **Yemek isimleri** ve **kullanıcı girdilerinin** bulunduğu admin.php sayfasında ekranda gösterilen herhangi bir veri XSS saldırısına açık olabilir. O yüzden admin.php sayfasına XSS zafiyeti denedim. En basit bilinin payloads ile.

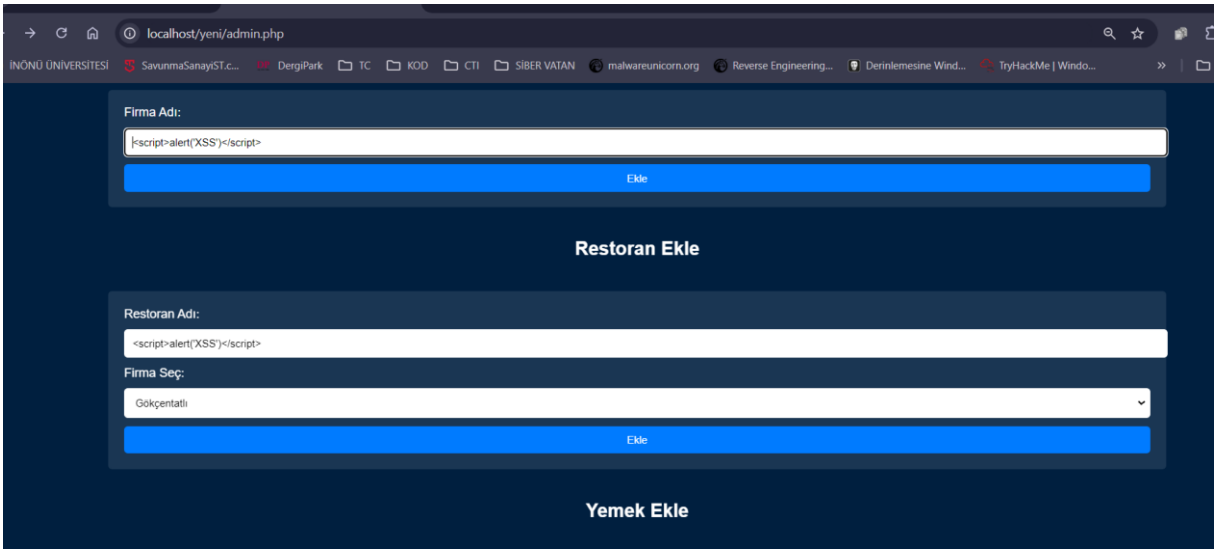
Nelere yol açar?

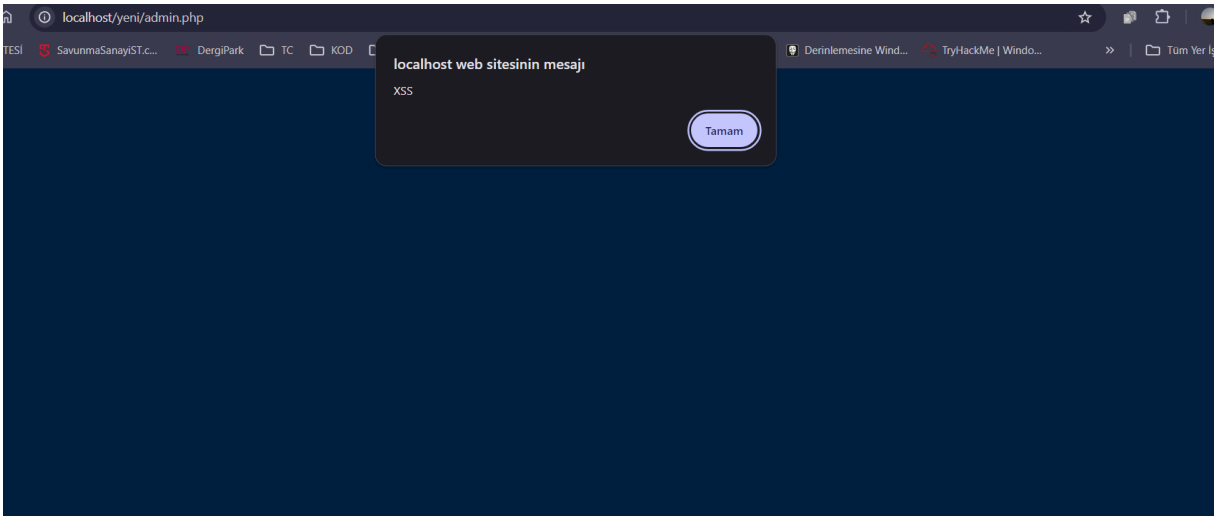
- • **Kullanıcı Arayüzünde Manipülasyon**: Saldırganlar, sayfa içeriklerini değiştirebilir, kullanıcıları yanlış yönlendirici linklere tıklamaya zorlayabilir veya yanıltıcı bilgiler gösterebilirler.
- • **Zararlı Yazılım Bulaştırma**: XSS ile kötü amaçlı yazılımlar (malware) siteye enjekte edilebilir ve bu yazılım siteyi ziyaret eden kullanıcıların cihazlarına bulaştırılabilir.

Nasıl Test Edilir?

- **Kullanıcı giriş formları** veya yemek ekleme alanlarına şu tür JavaScript kodlarını girmeyi deneyin:

  <script>alert('XSS')</script>





Aldığımız yanıta göre XSS saldırısına göre savunmasız.

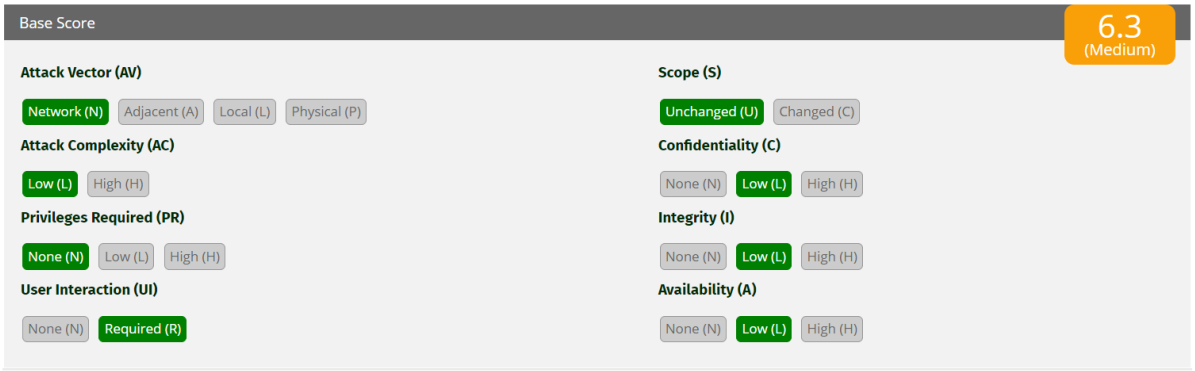
Nasıl Önlenir?

- **HTML özel karakterlerinin kaçarılması**: Kullanıcıdan alınan her türlü veriyi htmlspecialchars() fonksiyonuyla kaçırarak gösterin.

CVSS:

Common Vulnerability Scoring System Version 3.0 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.0).



Hata Yönetimi

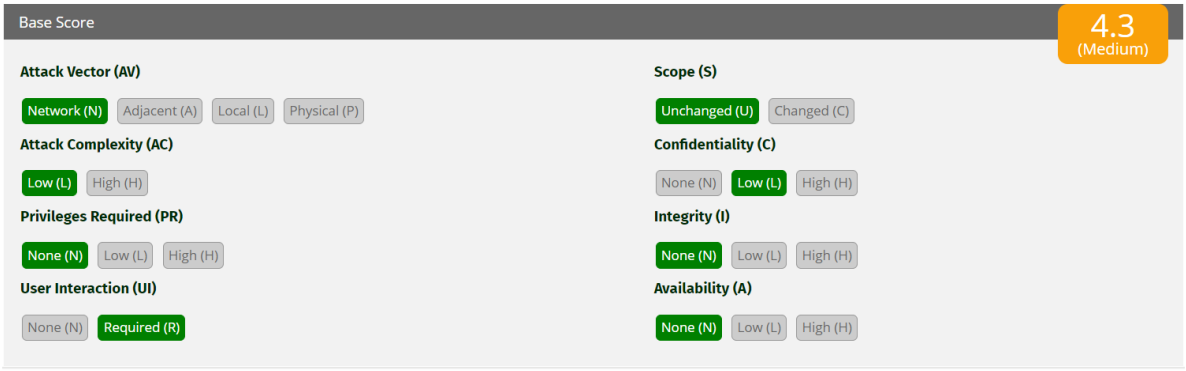
Zafiyet:

- Hata mesajları doğrudan kullanıcıya gösteriliyor. Bu, potansiyel bir saldırgana sistemin yapısını anlamasına yardımcı olabilir.

Nasıl Çözülür:

- Hata mesajlarını gizleyin veya genel bir hata mesajı gösterin. Hata detaylarını yalnızca geliştirici modunda görüntüleyin veya log dosyasına kaydedin.

CVSS:

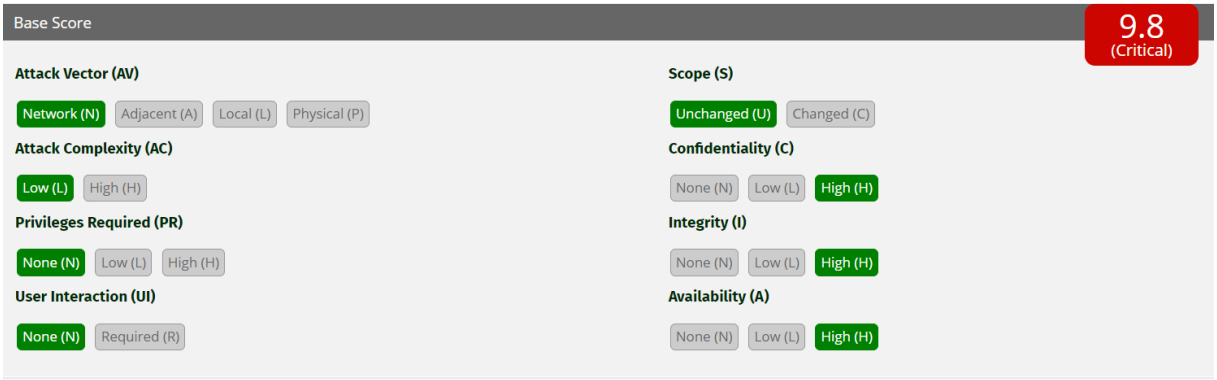


Buffer Overflow

Zafiyet Türü : Buffer Overflow

Zafiyetin Doğurabileceği Sonuçlar : Tampon tasması, uygulamanın veya sunucunun çökmesine neden olabilir, bu da hizmetin sürekliliğini tehdit eder ve kullanıcıların erişimini engeller. Ve Saldırgan, tampon taşmasını kullanarak bellek üzerinde kontrol elde cdebilir ve kötü amaçh kod çalştirabilir. Bu, sunucunun veya uygulamanın cle geçirilmesine yol açabilir. Zafiyetin Kapatılması için Öneriler: Kullanicidan gelen tüm verilerin boyutunu ve formatını kontrol edilmeli. Girdi uzunluğunu sinırlayarak, beklenmedik veri girişleri engellenmeli

CVS: 7.0


Base Score
9.8
(Critical)
Attack Vector (AV)
Network (N)
Adjacent (A)
Local (L)
Physical (P)
Attack Complexity (AC)
Low (L)
High (H)
Privileges Required (PR)
None (N)
Low (L)
High (H)
User Interaction (UI)
None (N)
Required (R)
Scope (S)
Unchanged (U)
Changed (C)
Confidentiality (C)
None (N)
Low (L)
High (H)
Integrity (I)
None (N)
Low (L)
High (H)
Availability (A)
None (N)
Low (L)
High (H)