

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 Oluştur: 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:

The image shows a screenshot of Burp Suite and a web browser. The Burp Suite interface displays a list of intercepted HTTP requests. The selected request is a POST to /yeni/login.php with a status code of 200. The browser window shows a login page titled 'Giriş Yap' (Login) with fields for 'Kullanıcı Adı:' (Username) and 'Şifre:' (Password). The username field contains 'huriye' and the password field contains '*****'. A blue 'Giriş Yap' button is visible.

Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
http://localhost	GET	/yeni/login.php			200	1087	HTML	php	Giriş Yap			127.0.0.1	PHPSESSID=79sac...	21
http://localhost	GET	/yeni/login.php			200	1087	HTML	php	Giriş Yap			127.0.0.1	PHPSESSID=mbus9...	21
http://localhost	GET	/favicon.ico			404	535	HTML	ico	404 Not Found			127.0.0.1		21
http://localhost	POST	/yeni/login.php		✓	200	1106	HTML	php	Giriş Yap			127.0.0.1		21
http://localhost	GET	/yeni/veritabani_olustur.php			200	303	HTML	php				127.0.0.1		22
http://localhost	GET	/yeni/login.php			200	1027	HTML	php	Giriş Yap			127.0.0.1		22
https://www.google.com	GET	/search?q=loca&oeq=loca&gs_lcrp=Eg...		✓	200	680845	HTML		loca - Google'da Ara		✓	142.250.179.132	AEC=AVVB7cqJF.ML...	22

```
request
Netty Raw Hex
HTTP/1.1 200 OK
Content-Length: 32
Cache-Control: max-age=0
sec-ch-ua: "Chromium",v="127", "Not)A;Brand",v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: tr-TR
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/yeni/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=mbus9463h6p6p6s6bgcveig
Connection: keep-alive
```

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
http://localhost	GET	/yeni/login.php			200	1087	HTML	php	Giriş Yap			127.0.0.1	PHPSESSID=79sac...	21:25:39 11 O...	8080
http://localhost	GET	/yeni/login.php			200	1087	HTML	php	Giriş Yap			127.0.0.1	PHPSESSID=nbu5...	21:28:30 11 O...	8080
http://localhost	GET	/favicon.ico			404	535	HTML	ico	404 Not Found			127.0.0.1		21:28:37 11 O...	8080
http://localhost	POST	/yeni/login.php		✓	200	1106	HTML	php	Giriş Yap			127.0.0.1		21:28:57 11 O...	8080
http://localhost	GET	/yeni/venetana.olustur.php			200	303	HTML	php				127.0.0.1		22:09:34 11 O...	8080
http://localhost	GET	/yeni/login.php			200	1027	HTML	php	Giriş Yap			127.0.0.1		22:10:11 11 O...	8080
http://localhost	POST	/yeni/login.php		✓	200	1104	HTML	php	Giriş Yap			127.0.0.1		22:10:23 11 O...	8080
https://www.google.com	GET	/search?q=loca&oq=loca&ig=loca		✓	200	600645	HTML		loca - Google'da Ara		✓	142.250.179.132	AEC=AV1BTcqF-ML...	22:10:10 11 O...	8080

Request

Raw

```
POST /yeni/login.php HTTP/1.1
Host: localhost
Content-Length: 30
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="127", "Not(A;Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: tr-TR
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/yeni/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=nbu54t3h6p6sp6p6sb6q6vige
Connection: keep-alive
username=buruyy&password=12432
```

Response

Raw

```
HTTP/1.1 200 OK
Date: Fri, 11 Oct 2024 19:10:23 GMT
Server: Apache/2.4.58 (Ubuntu) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 739
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>
Giriş Yap
</title>
<link rel="stylesheet" href="styles.css">
</head>
<body>
<div>
```

Inspector

Request attributes

Request parameters

Request cookies

Request headers

Response headers

Choose an attack type

Attack type: Sniper

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost

Update Host header to match target

Add

Clear

Auto

Refresh

```
1 POST /yeni/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 30
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="127", "Not(A;Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Accept-Language: tr-TR
9 Upgrade-Insecure-Requests: 1
10 Origin: http://localhost
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/yeni/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=nbu54t3h6p6sp6p6sb6q6vige
21 Connection: keep-alive
22
23 username=buruyy&password=$$
```

Results

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
32	1231	200	1			1104	
33	1232	200	0			1104	
34	1233	200	3			1104	
35	1234	302	5			367	
36	1235	200	0			1104	
37	1236	200	0			1104	
38	1237	200	0			1104	
39	1238	200	3			1104	
40	1239	200	3			1104	
41	1240	200	0			1104	

Request

Raw

```
POST /yeni/login.php HTTP/1.1
Host: localhost
Content-Length: 29
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="127", "Not(A;Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: tr-TR
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
```

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:

Base Score		6.5 (Medium)
Attack Vector (AV)		Scope (S)
<input checked="" type="radio"/> Network (N) <input type="radio"/> Adjacent (A) <input type="radio"/> Local (L) <input type="radio"/> Physical (P)		<input checked="" type="radio"/> Unchanged (U) <input type="radio"/> Changed (C)
Attack Complexity (AC)		Confidentiality (C)
<input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)		<input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)
Privileges Required (PR)		Integrity (I)
<input type="radio"/> None (N) <input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)		<input checked="" type="radio"/> None (N) <input type="radio"/> Low (L) <input type="radio"/> High (H)
User Interaction (UI)		Availability (A)
<input checked="" type="radio"/> None (N) <input type="radio"/> Required (R)		<input checked="" type="radio"/> None (N) <input type="radio"/> Low (L) <input type="radio"/> High (H)

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 bilinen 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>`

localhost/yeni/admin.php

Firma Adi:

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

Ekle

Restoran Ekle

Restoran Adı:

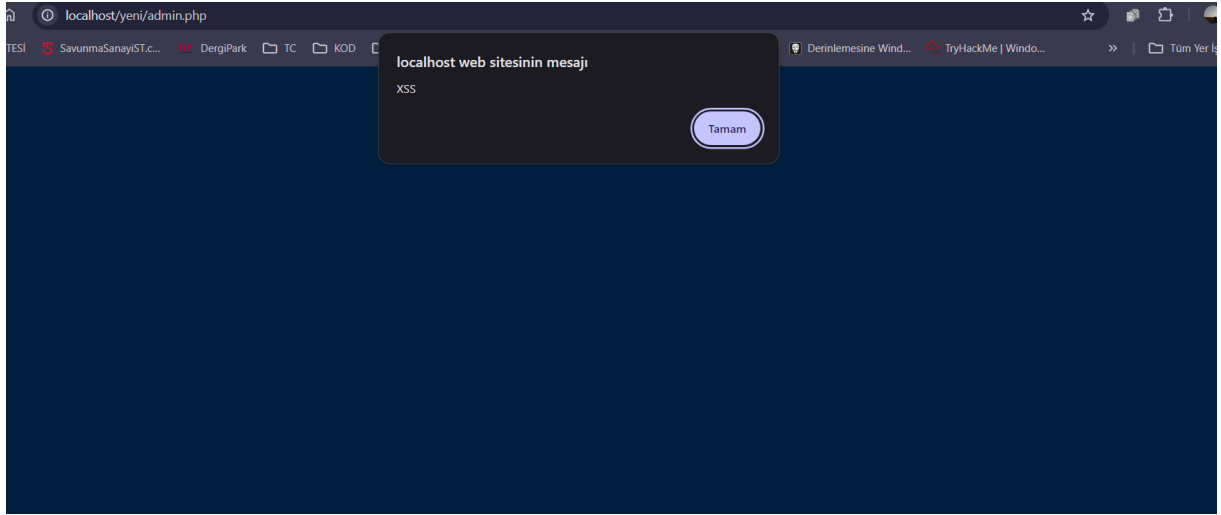
<script>alert('XSS')</script>

Firma Seç:

Gökçentatlı

Ekle

Yemek Ekle



Aldığımız yanıtla göre XSS saldırısına göre savunmasız.

Nasıl Önlenir?

- **HTML özel karakterlerinin kaçırılması:** 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).

Base Score

6.3
(Medium)

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)

Hata Yönetimi

Zafiyet:

- Hata mesajları doğrudan kullanıcıya gösteriliyor. Bu, potansiyel bir saldırıya 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:

Base Score

4.3
(Medium)

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)

Buffer Overflow

Zafiyet Türü : Buffer Overflow

Zafiyetin Doğurabileceği Sonuçlar : Tampon taşması, 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 edebilir ve kötü amaçlı kod çalıştırabilir. Bu, sunucunun veya uygulamanın cle geçirilmesine yol açabilir. Zafiyetin Kapatılması için Öneriler: Kullanıcıdan gelen tüm verilerin boyutunu ve formatını kontrol edilmeli. Girdi uzunluğunu sınırlayarak, beklenmedik veri girişleri engellenmeli

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)