VAPT - IA1

Keyur Patel - 16010421073

Krishiv Patel - 16010421074

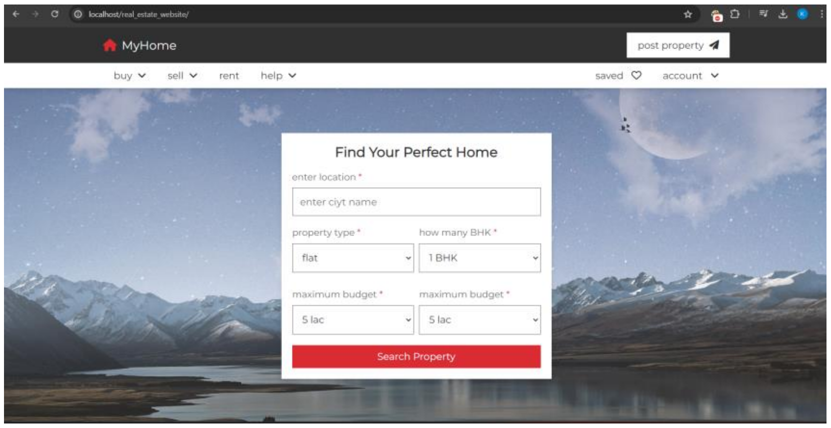
Batch : A2

Aim : Explain and fix an Insecure Direct Object Reference (IDOR) vulnerability in a Real Estate Listing Platform, specifying the relevant CWE: Insecure Direct Object Reference (CWE-639) and (CWE-353) Missing Support for Integrity Check.

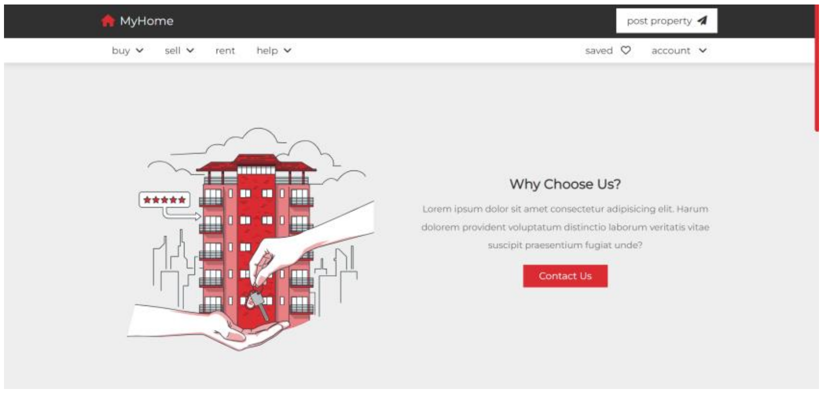
Resources needed: Real Estate website , Burpsuite , Xampp

Real Estate Listing Platform

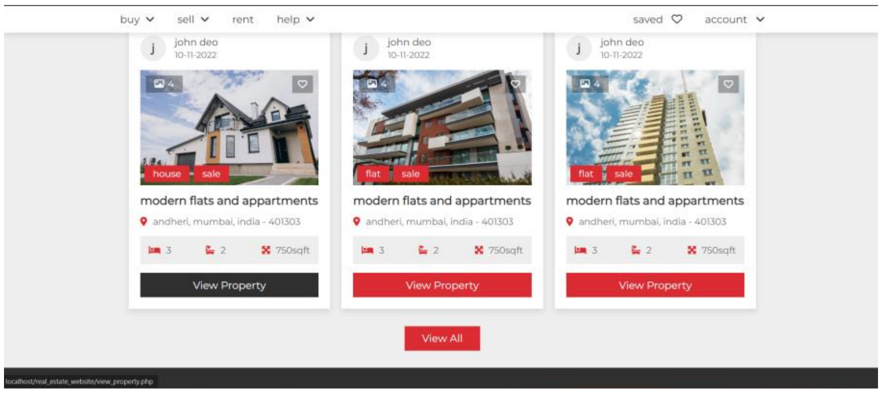
Home Page of website



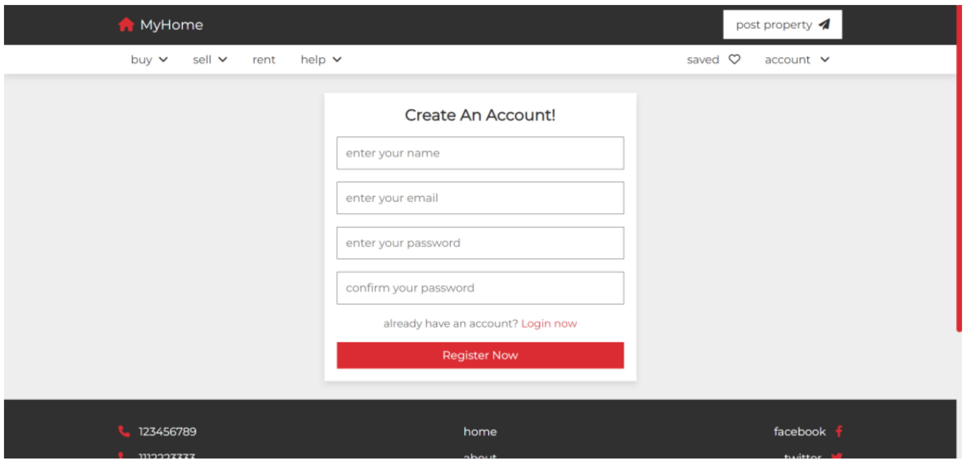
About us


MyHome
post property
buy
sell
rent
help
saved
account
Why Choose Us?
Lorem ipsum dolor sit amet consectetur adipisicing elit. Harum dolorem provident voluptatum distinctio laborum veritatis vitae suscipit praesentium fugiat unde?
Contact Us

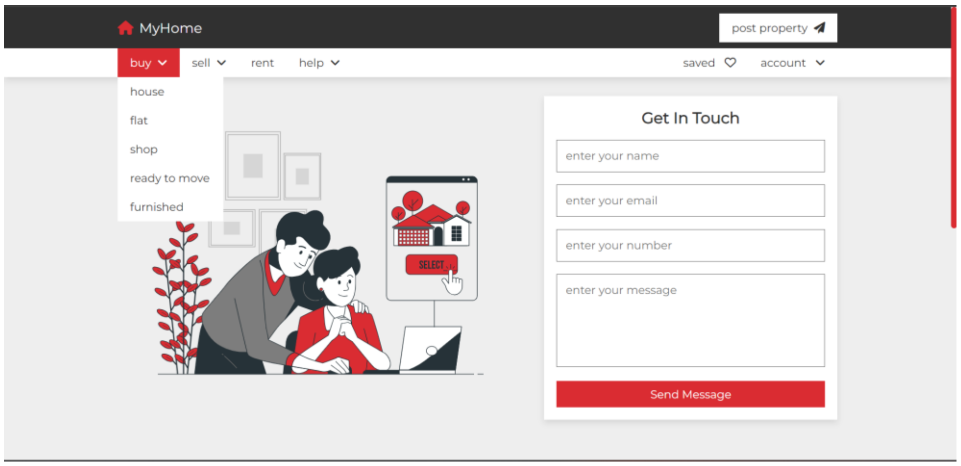
View Property of website


buy
sell
rent
help
saved
account
john deo
10-11-2022
house
sale
flat
modern flats and appartments
andheri, mumbai, india - 401303
3
2
750sqft
View Property
View All
localhost/real_estate_website/view_property.php

Create Account



Contact Us



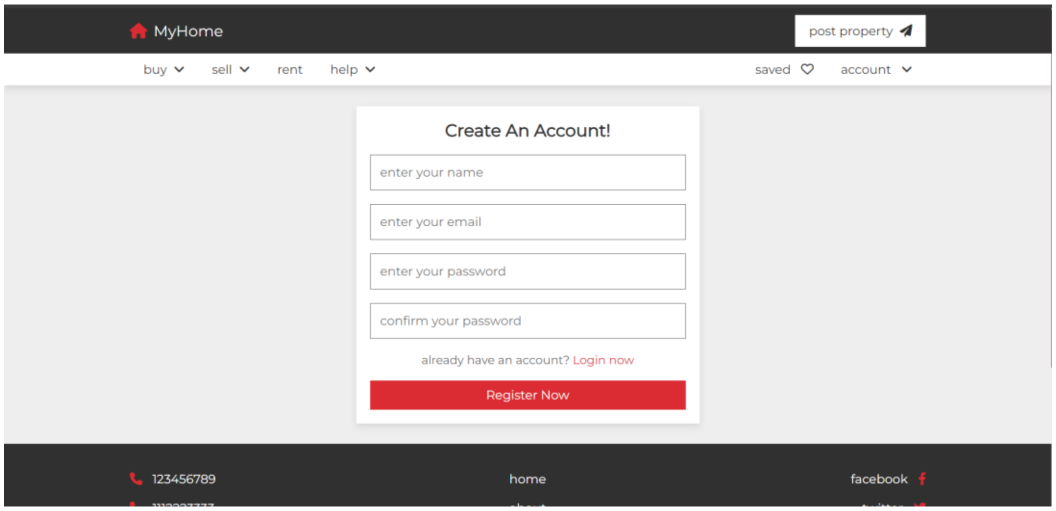
Vulnerability - 1 (CWE – 639 Insecure Direct Object Reference)

Insecure Direct Object Reference:-

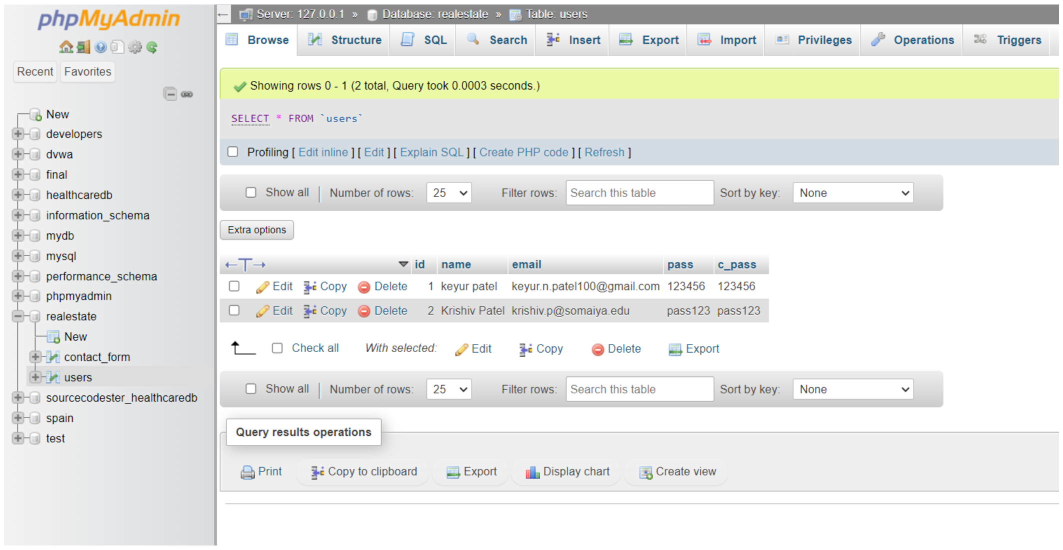
Insecure Direct Object Reference refers to a vulnerability that occurs when a web application exposes a reference to an internal implementation object, such as a file, directory, database record, or key, in a way that allows unauthorized access to that object.

Procedure to Expose Vulnerability:

Step-1) This is the Create Account page where we are going to exposing the modification of user credential using burpsuite.



Step-2) Data stored for user in phpMyAdmin having database as ‘realestate’.

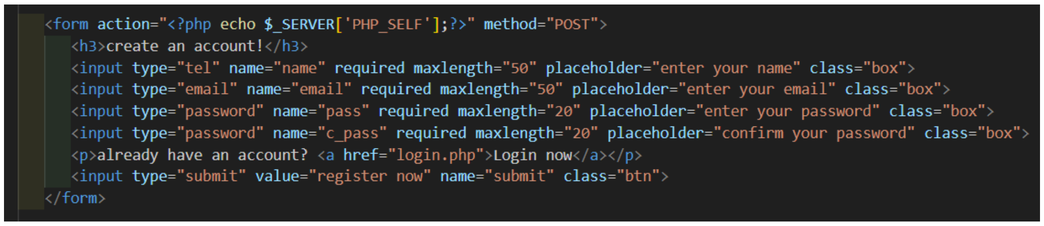


Showing rows 0 - 1 (2 total, Query took 0.0003 seconds.)

```
SELECT * FROM `users`
```

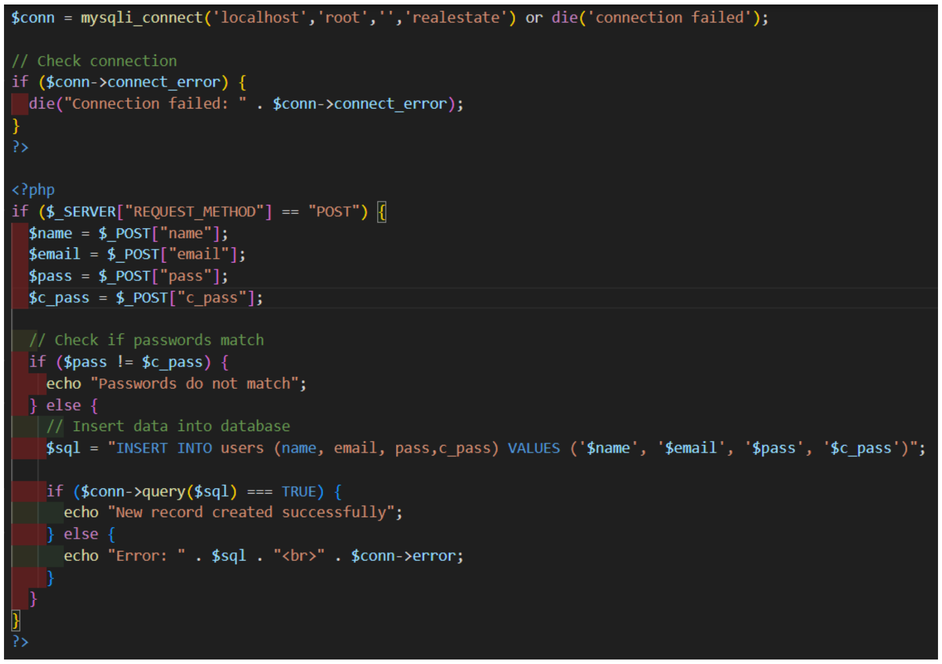
	id	name	email	pass	c_pass
Edit Copy Delete	1	keyur patel	keyur.n.patel100@gmail.com	123456	123456
Edit Copy Delete	2	Krishiv Patel	krishiv.p@somaiya.edu	pass123	pass123

Step-3) Form code for account.



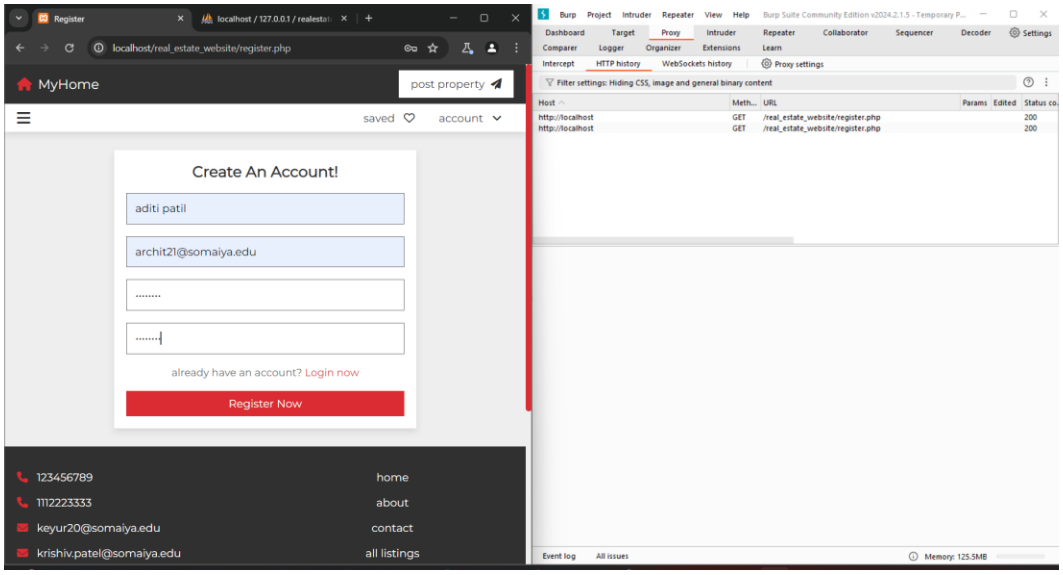
```
<form action="<?php echo $_SERVER['PHP_SELF'];?>" method="POST">
   <h3>create an account!</h3>
   <input type="tel" name="name" required maxlength="50" placeholder="enter your name" class="box">
   <input type="email" name="email" required maxlength="50" placeholder="enter your email" class="box">
   <input type="password" name="pass" required maxlength="20" placeholder="enter your password" class="box">
   <input type="password" name="c_pass" required maxlength="20" placeholder="confirm your password" class="box">
   <p>already have an account? <a href="login.php">Login now</a></p>
   <input type="submit" value="register now" name="submit" class="btn">
</form>
```

Step-4) Form is submitted using post method in users table.



```
$conn = mysqli_connect('localhost','root','','realestate') or die('connection failed');

// Check connection
if ($conn->connect_error) {
  die("Connection failed: " . $conn->connect_error);
}
?>

<?php
if ($_SERVER["REQUEST_METHOD"] == "POST") {
  $name = $_POST["name"];
  $email = $_POST["email"];
  $pass = $_POST["pass"];
  $c_pass = $_POST["c_pass"];

  // Check if passwords match
  if ($pass != $c_pass) {
    echo "Passwords do not match";
  } else {
    // Insert data into database
    $sql = "INSERT INTO users (name, email, pass,c_pass) VALUES ('$name', '$email', '$pass', '$c_pass')";

    if ($conn->query($sql) === TRUE) {
      echo "New record created successfully";
    } else {
      echo "Error: " . $sql . "<br>" . $conn->error;
    }
  }
}
?>
```

Step-5) Entering the credentials in burpsuite browser when intercept is switched off.



Register
localhost / 127.0.0.1 / realestat
localhost/real_estate_website/register.php
MyHome
post property
saved
account

Create An Account!

aditi patil

archit21@somaiya.edu

....

....

already have an account? Login now

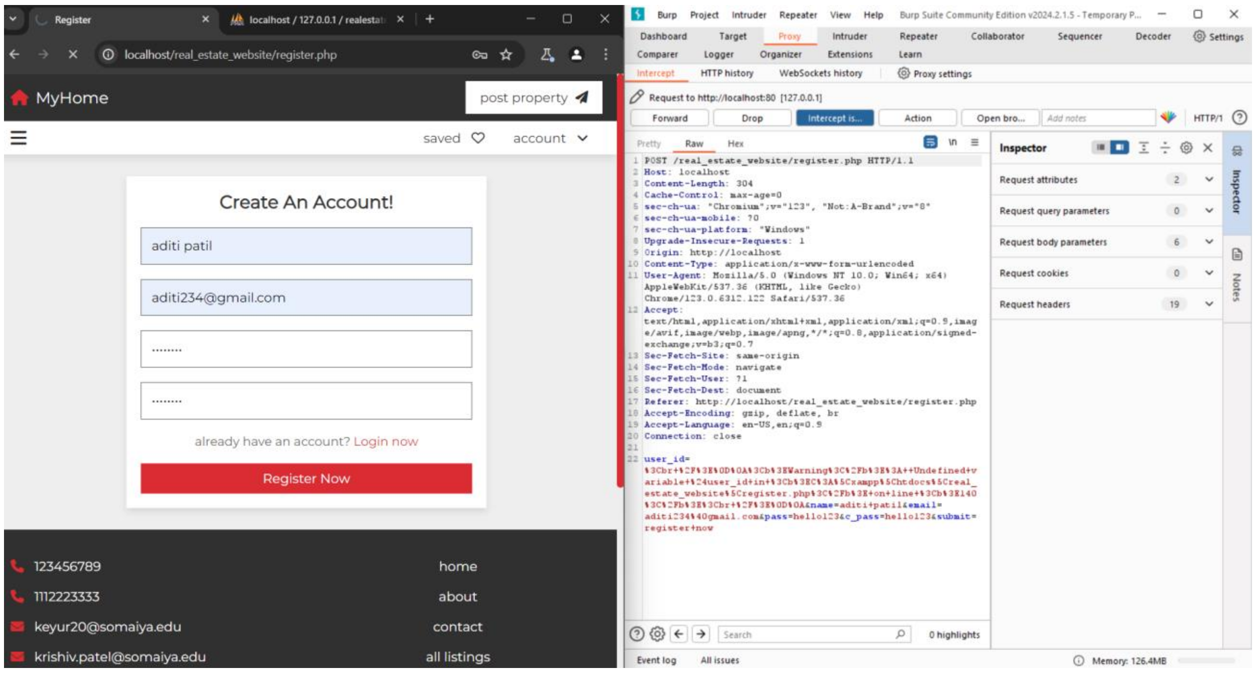
Register Now

123456789
1112223333
keyur20@somaiya.edu
krishiv.patel@somaiya.edu
home
about
contact
all listings
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.2.1.5 - Temporary P...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Event log All issues Memory: 125.5MB

Filter settings: Hiding CSS, image and general binary content

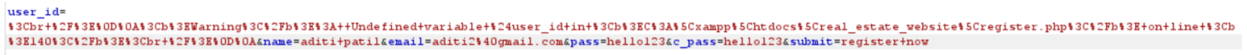
Host	Meth...	URL	Params	Edited	Status co...
http://localhost	GET	/real_estate_website/register.php			200
http://localhost	GET	/real_estate_website/register.php			200

Step-6) Switch on the intercept in proxy tab ,after then click on ‘Register now’ button you will see that request is intercepted by burpsuite.


Register
localhost / 127.0.0.1 / realestat
localhost/real_estate_website/register.php
MyHome
post property
saved
account
Create An Account!
aditi patil
aditi234@gmail.com
already have an account? Login now
Register Now
123456789
1112223333
keyur20@somaiya.edu
krishiv.patel@somaiya.edu
home
about
contact
all listings
Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.2.1.5 - Temporary P...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is... Action Open bro...
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 6
Request cookies 0
Request headers 19
0 highlights
Event log All issues
Memory: 126.4MB

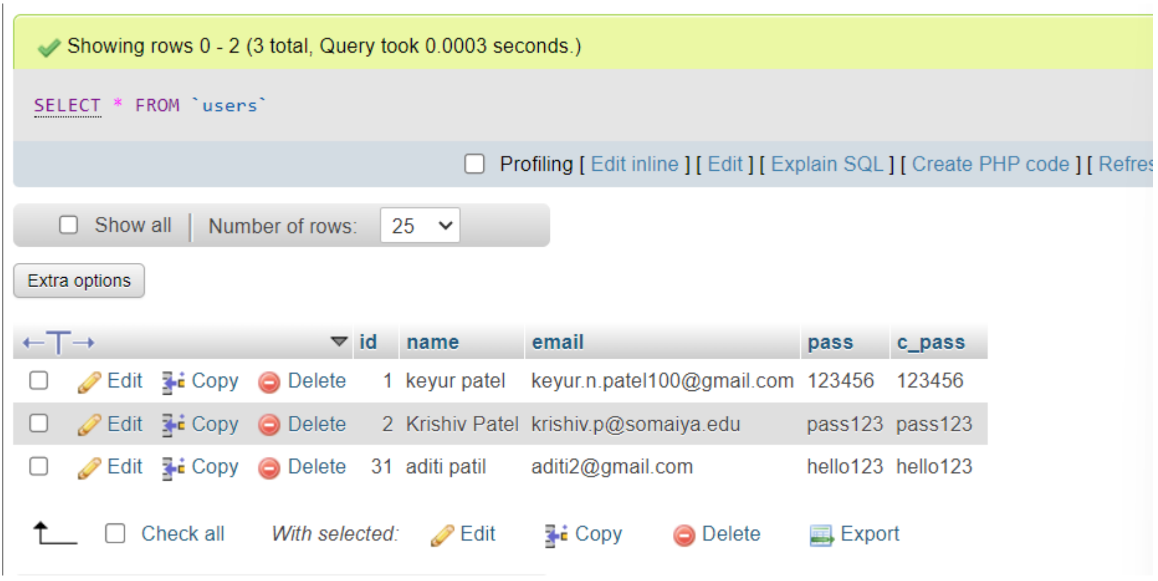
```
POST /real_estate_website/register.php HTTP/1.1
Host: localhost
Content-Length: 304
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/real_estate_website/register.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

user_id=
%3Cbr+%2F%3E%0D%0A%3Cb%3EWarning%3C%2Fb%3E%3A++Undefined+v
ariable+%24user_id+in+%3Cb%3EC%3A%5Cxampp%5Chtdocs%5Creal_
estate_website%5Cregister.php%3C%2Fb%3E+on+line+%3Cb%3E140
%3C%2Fb%3E%3Cbr+%2F%3E%0D%0A&name=aditi+patil&email=
aditi234%40gmail.com&pass=hello123&c_pass=hello123&submit=
register+now
```

Step-7) Modify the email for user and click on forward option at intercept to send modified data to database.



```
user_id=
%3Cbr+%2F%3E%0D%0A%3Cb%3EWarning%3C%2Fb%3E%3A++Undefined+variable+%24user_id+in+%3Cb%3EC%3A%5Cxampp%5Chtdocs%5Creal_estate_website%5Cregister.php%3C%2Fb%3E+on+line+%3Cb
%3E140%3C%2Fb%3E%3Cbr+%2F%3E%0D%0A&name=aditi+patil&email=aditi2%40gmail.com&pass=hello123&c_pass=hello123&submit=register+now
```

Step-8) Email is modified at phpMyAdmin which was done by unauthorized person.



Showing rows 0 - 2 (3 total, Query took 0.0003 seconds.)

```
SELECT * FROM `users`
```

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refres
Show all
Number of rows: 25
Extra options

	id	name	email	pass	c_pass
Edit Copy Delete	1	keyur patel	keyur.n.patel100@gmail.com	123456	123456
Edit Copy Delete	2	Krishiv Patel	krishiv.p@somaiya.edu	pass123	pass123
Edit Copy Delete	31	aditi patil	aditi2@gmail.com	hello123	hello123

Mitigation:

- ***Implement Access Control Checks:*** Ensure that every object a user tries to access is checked against the user's permissions. This means verifying that the user has the right to view or modify the object before allowing the action. This can be achieved by checking the user's session information against the object's ownership or permissions.

- ***Verify User Permissions:*** Every time an access attempt is made, verify the user's permission. This can be implemented structurally using the recommended approach for your web framework. For example, when looking up objects based on primary keys, ensure that the datasets users have access to are used.

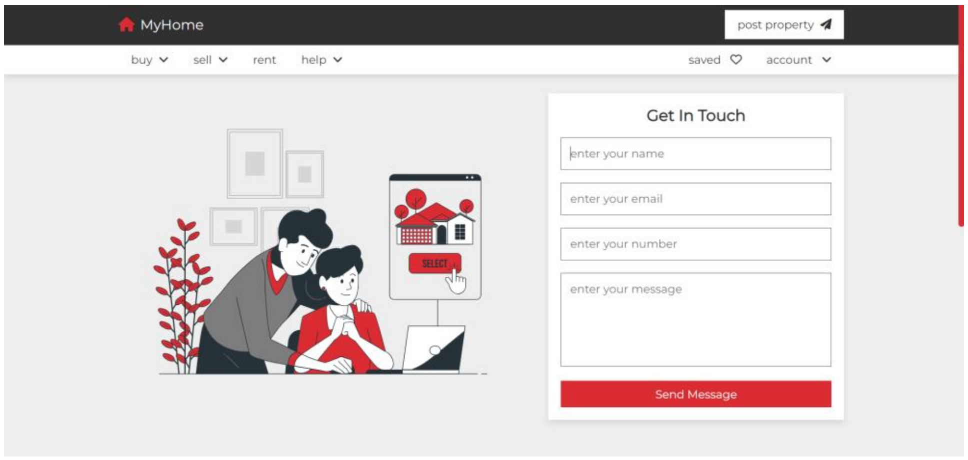
- ***Use Prepared Statements for Database Queries:*** To prevent SQL Injection, which is a related vulnerability, use prepared statements for database queries. This ensures that user input is treated as data and not.

Vulnerability - 2 (CWE – 353 Missing Support for Integrity Check)

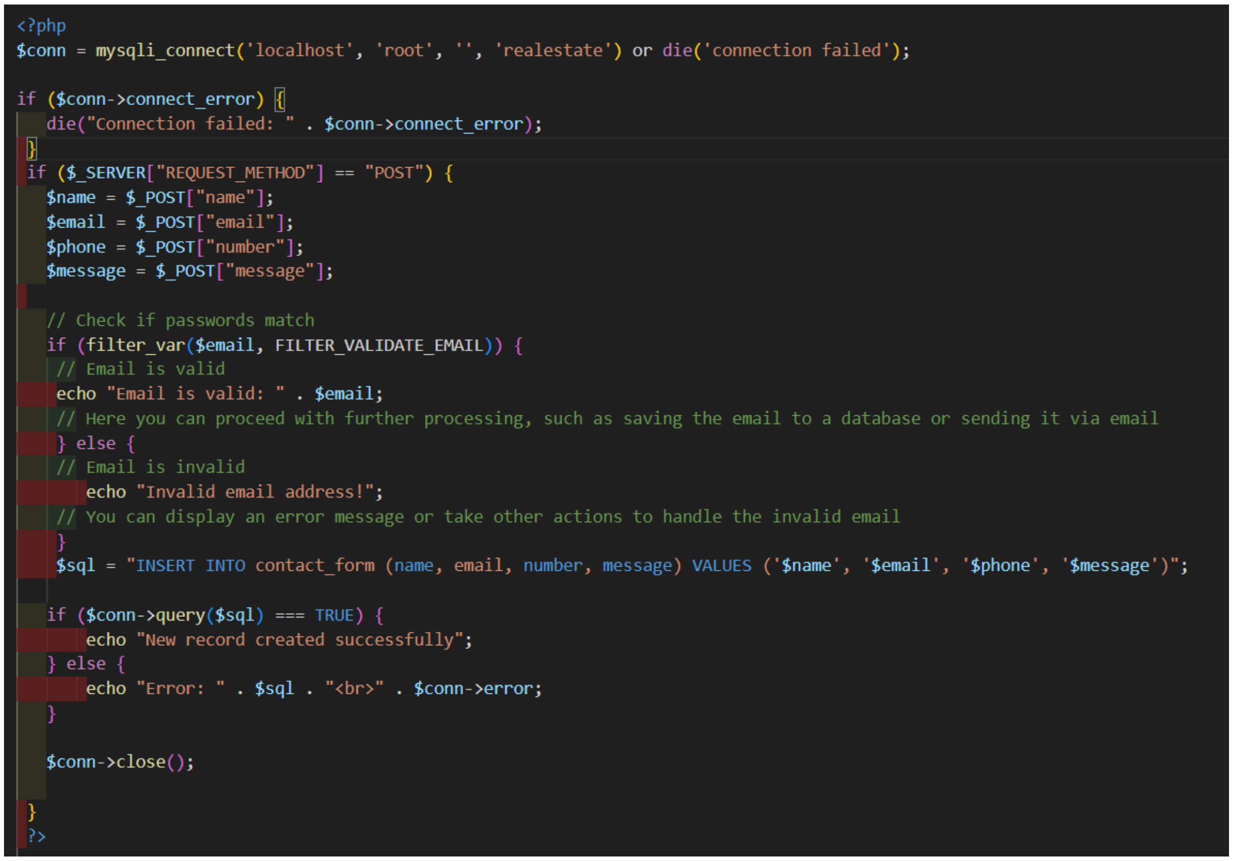
If integrity check values or "checksums" are omitted from a protocol, there is no way of determining if data has been corrupted in transmission. The lack of checksum functionality in a protocol removes the first application-level check of data that can be used. The end-to-end philosophy of checks states that integrity checks should be performed at the lowest level that they can be completely implemented. Excluding further sanity checks and input validation performed by applications, the protocol's checksum is the most important level of checksum, since it can be performed more completely than at any previous level and takes into account entire messages, as opposed to single packets.

Procedure to Expose Vulnerability:

Step-1) Go to Contact us webpage for users. Here we are going to expose integrity of data being tampered by attacker without any checksum provided.

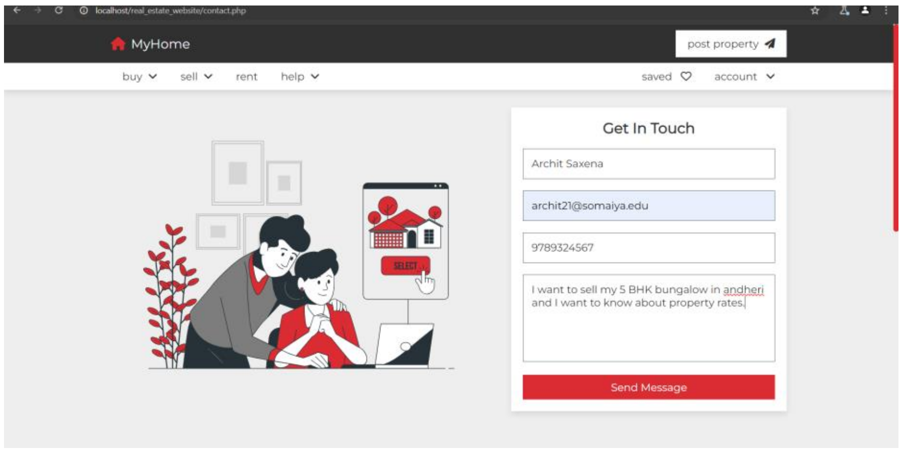


Step-2) PHPCode for submission after entering the message which is then sent to database in phpMyAdmin using post method.



```
<?php
$conn = mysqli_connect('localhost', 'root', '', 'realestate') or die('connection failed');

if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
 if ($_SERVER["REQUEST_METHOD"] == "POST") {
    $name = $_POST["name"];
    $email = $_POST["email"];
    $phone = $_POST["number"];
    $message = $_POST["message"];

    // Check if passwords match
    if (filter_var($email, FILTER_VALIDATE_EMAIL)) {
     // Email is valid
     echo "Email is valid: " . $email;
     // Here you can proceed with further processing, such as saving the email to a database or sending it via email
     } else {
     // Email is invalid
        echo "Invalid email address!";
     // You can display an error message or take other actions to handle the invalid email
     }
     $sql = "INSERT INTO contact_form (name, email, number, message) VALUES ('$name', '$email', '$phone', '$message')";

    if ($conn->query($sql) === TRUE) {
        echo "New record created successfully";
    } else {
        echo "Error: " . $sql . "<br>" . $conn->error;
    }

    $conn->close();

 }
 ?>
```

Step-3) Enter the form details when intercept is off.



Get In Touch

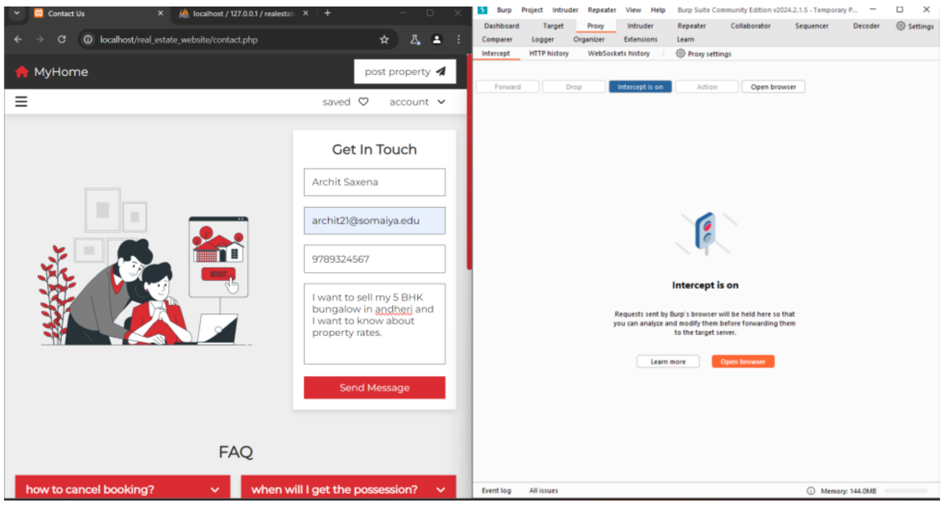
Archit Saxena

archit21@somaiya.edu

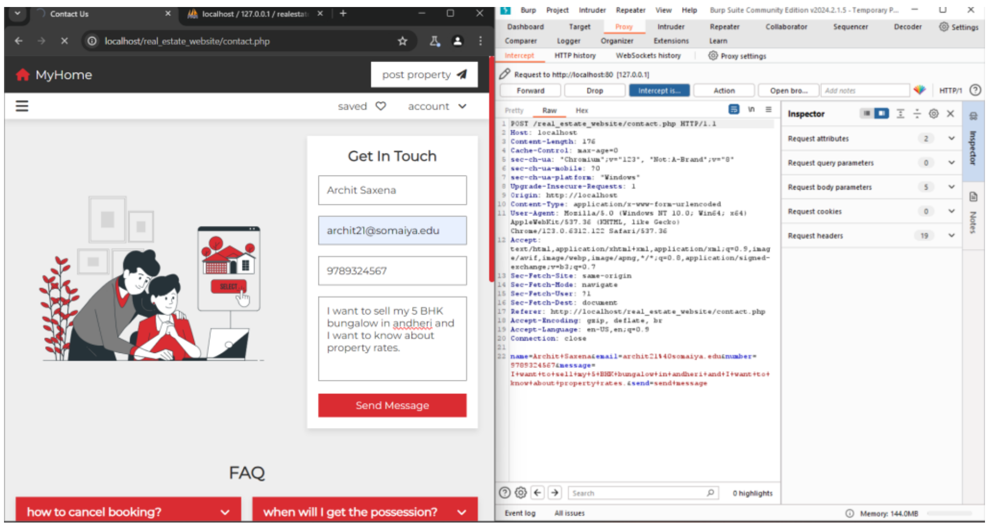
9789324567

I want to sell my 5 BHK bungalow in andheri and I want to know about property rates.

Step-4) Click on the Intercept option and then submit “get in touch” form.

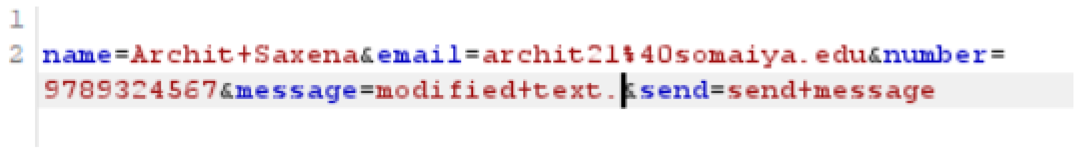


Step-5) The Request is then redirected to burpsuite which shows what is sent by user.



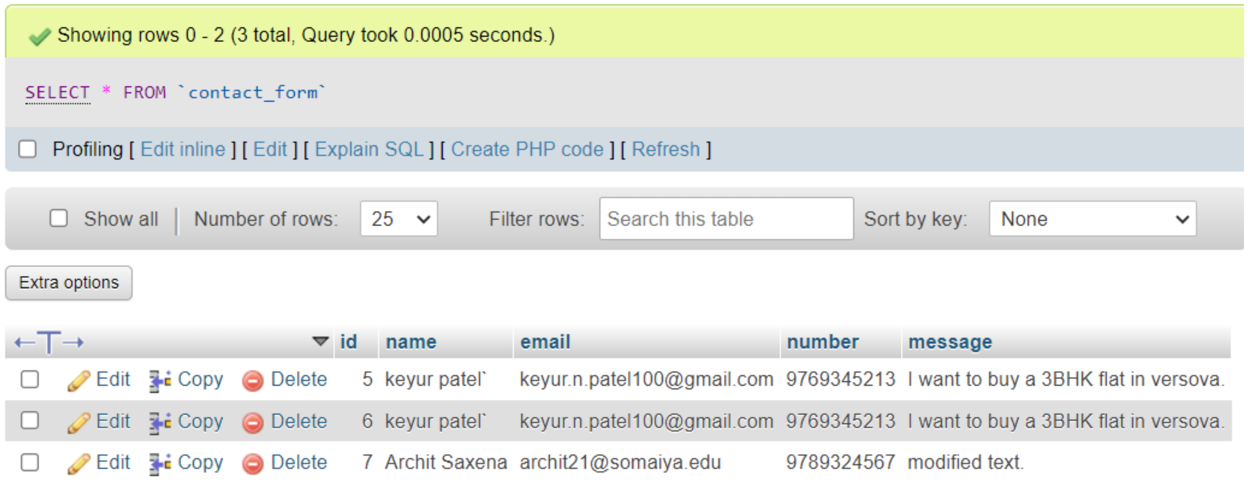
```
POST /real_estate_website/contact.php HTTP/1.1
Host: localhost
Content-Length: 176
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/real_estate_website/contact.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

name=Archit+Saxena&email=archit21%40somaiya.edu&number=
9789324567&message=
I+want+to+sell+my+5+BHK+bungalow+in+andheri+and+I+want+to+
know+about+property+rates.&send=send+message
```

Step-4) The Attacker modifies the message and tampers the integrity of message.



```
name=Archit+Saxena&email=archit21%40somaiya.edu&number=
9789324567&message=modified+text.&send=send+message
```

Step-5) Then forward the modifed message to database. You will see that data is modified as *"modified text"*.



Showing rows 0 - 2 (3 total, Query took 0.0005 seconds.)

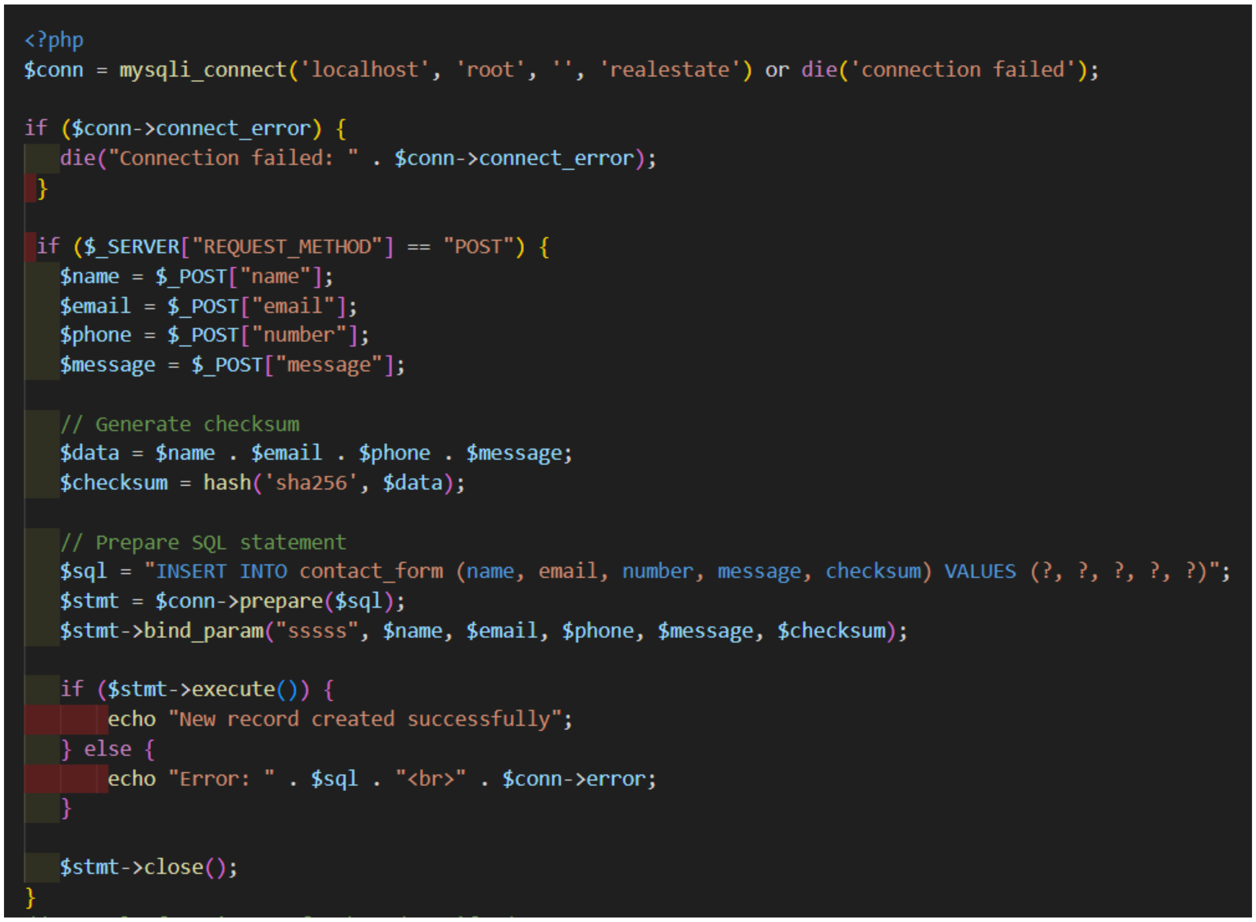
```
SELECT * FROM `contact_form`
```

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all
Number of rows: 25
Filter rows: Search this table
Sort by key: None
Extra options

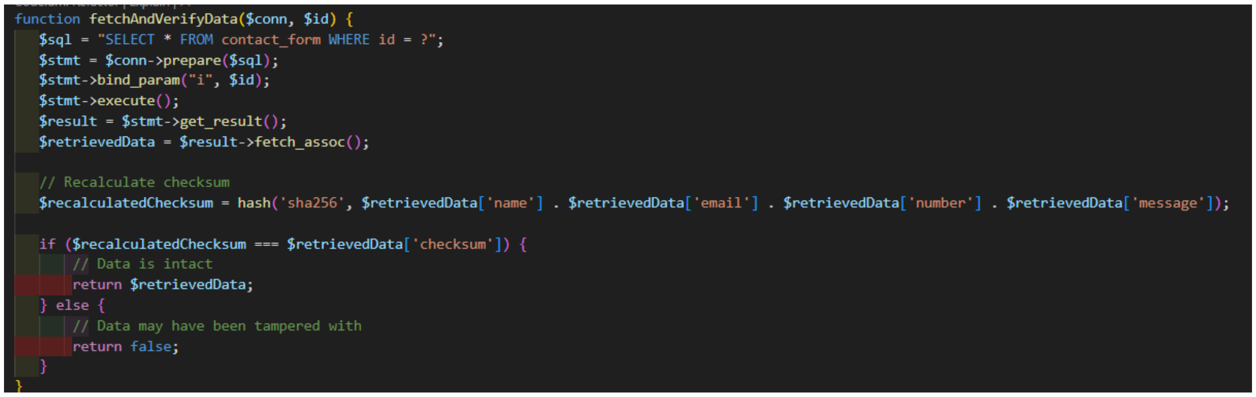
	id	name	email	number	message
Edit Copy Delete	5	keyur patel`	keyur.n.patel100@gmail.com	9769345213	I want to buy a 3BHK flat in versova.
Edit Copy Delete	6	keyur patel`	keyur.n.patel100@gmail.com	9769345213	I want to buy a 3BHK flat in versova.
Edit Copy Delete	7	Archit Saxena	archit21@somaiya.edu	9789324567	modified text.

Mitigation:

Step-1) The modified PHP code having function for fetch and verify data which includes checksum and hashes the text for ‘message’.

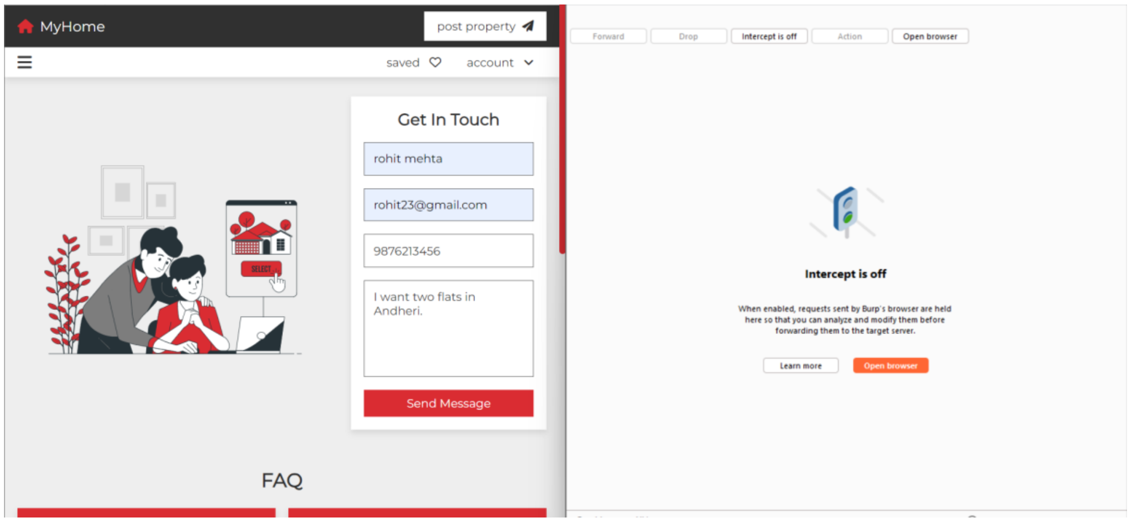


```php
<?php
$conn = mysqli_connect('localhost', 'root', '', 'realestate') or die('connection failed');

if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

if ($_SERVER["REQUEST_METHOD"] == "POST") {
    $name = $_POST["name"];
    $email = $_POST["email"];
    $phone = $_POST["number"];
    $message = $_POST["message"];

    // Generate checksum
    $data = $name . $email . $phone . $message;
    $checksum = hash('sha256', $data);

    // Prepare SQL statement
    $sql = "INSERT INTO contact_form (name, email, number, message, checksum) VALUES (?, ?, ?, ?, ?)";
    $stmt = $conn->prepare($sql);
    $stmt->bind_param("sssss", $name, $email, $phone, $message, $checksum);

    if ($stmt->execute()) {
        echo "New record created successfully";
    } else {
        echo "Error: " . $sql . "<br>" . $conn->error;
    }

    $stmt->close();
}
```



```php
function fetchAndVerifyData($conn, $id) {
    $sql = "SELECT * FROM contact_form WHERE id = ?";
    $stmt = $conn->prepare($sql);
    $stmt->bind_param("i", $id);
    $stmt->execute();
    $result = $stmt->get_result();
    $retrievedData = $result->fetch_assoc();

    // Recalculate checksum
    $recalculatedChecksum = hash('sha256', $retrievedData['name'] . $retrievedData['email'] . $retrievedData['number'] . $retrievedData['message']);

    if ($recalculatedChecksum === $retrievedData['checksum']) {
        // Data is intact
        return $retrievedData;
    } else {
        // Data may have been tampered with
        return false;
    }
}
```

Step-2) Entering The form details when intercept is off.



Get In Touch

rohit mehta

rohit23@gmail.com

9876213456

I want two flats in Andheri.

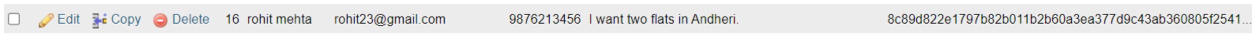
Send Message

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

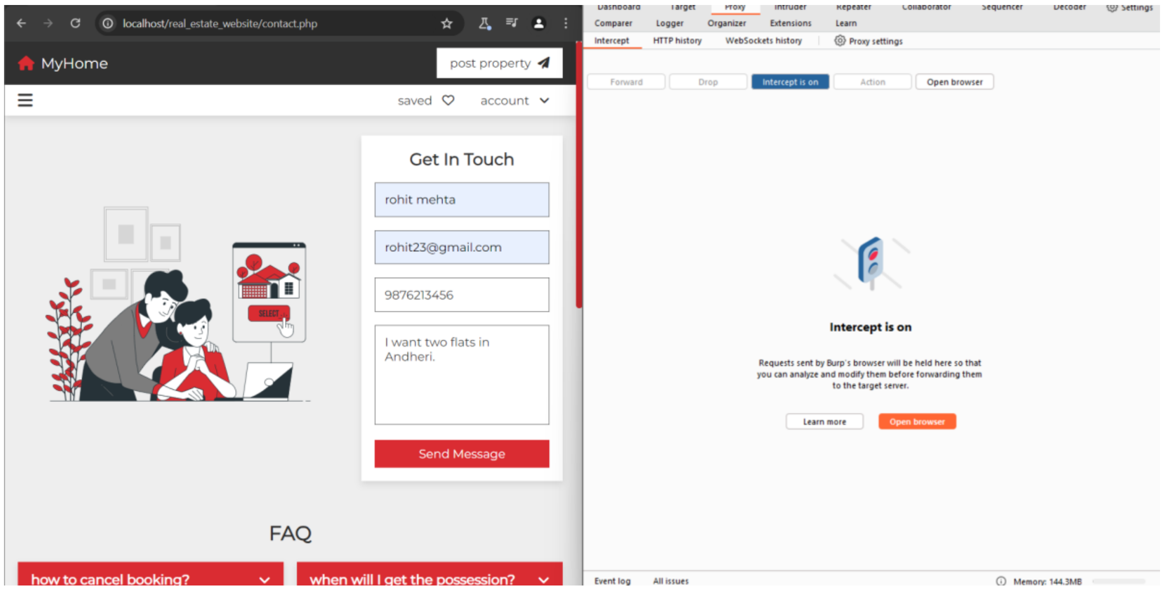
Step-3) The checksum generated for “I want two flats in Andheri” is

Checksum:
8c89d822e1797b82b011b2b60a3ea377d9c43ab360805f25413171f008bc43c8



Edit	Copy	Delete	16	rohit mehta	rohit23@gmail.com	9876213456	I want two flats in Andheri.	8c89d822e1797b82b011b2b60a3ea377d9c43ab360805f2541...

Step-4) Then Click on the intercept option and send the message.



Get In Touch

rohit mehta

rohit23@gmail.com

9876213456

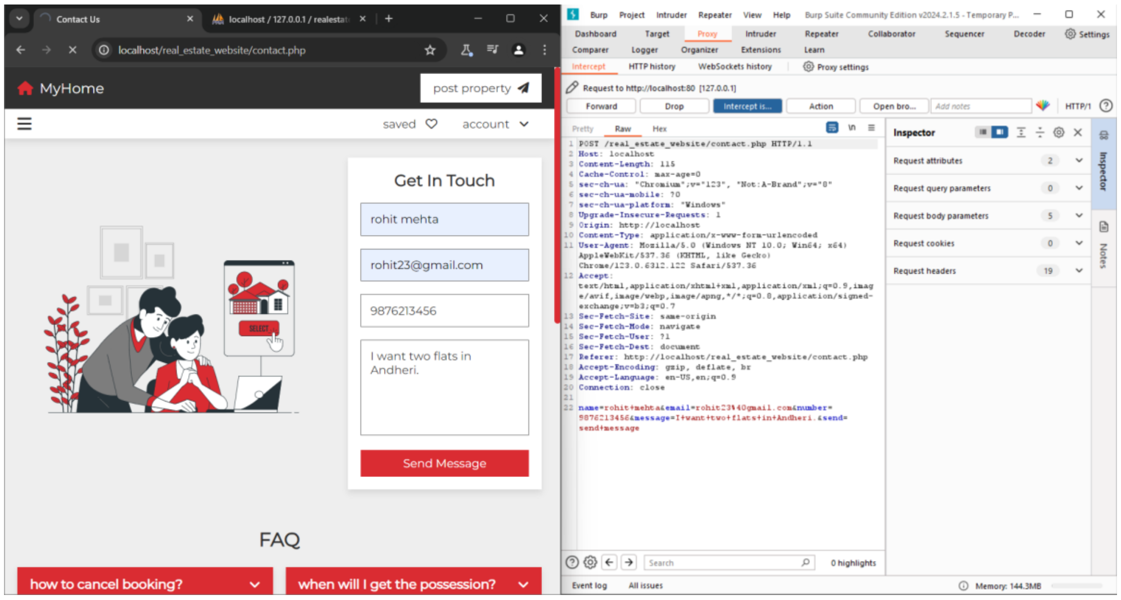
I want two flats in Andheri.

Send Message

Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

Step-4) Then the request is redirected to burpsuite where we will modify the text “I want two flats in Andheri” to “I want four flats in Andheri”.



Get In Touch

rohit mehta

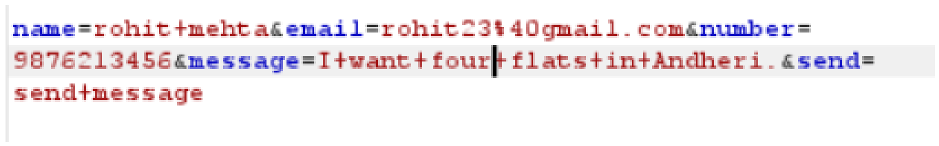
rohit23@gmail.com

9876213456

I want two flats in Andheri.

Request to http://localhost:80 [127.0.0.1]

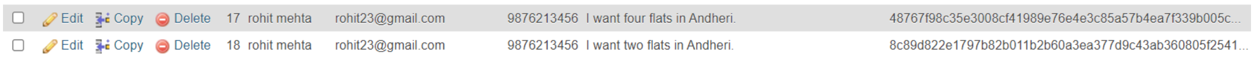
```
POST /real_estate_website/contact.php HTTP/1.1
Host: localhost
Content-Length: 115
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/123.0.6312.122 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/real_estate_website/contact.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

name=rohit+mehta&email=rohit23%40gmail.com&number=
9876213456&message=I+want+two+flats+in+Andheri.&send=
send+message
```



```
name=rohit+mehta&email=rohit23%40gmail.com&number=
9876213456&message=I+want+four+flats+in+Andheri.&send=
send+message
```

Step-5) The checksum generated for "I want four flats in Andheri" is

Checksum:
48767f98c35e3008cf41989e76e4e3c85a57b4ea7f339b005c61dd748fc023aa



☐	Edit	Copy	Delete	17	rohit mehta	rohit23@gmail.com	9876213456	I want four flats in Andheri.	48767f98c35e3008cf41989e76e4e3c85a57b4ea7f339b005c...
☐	Edit	Copy	Delete	18	rohit mehta	rohit23@gmail.com	9876213456	I want two flats in Andheri.	8c89d822e1797b82b011b2b60a3ea377d9c43ab360805f2541...

Thus we can determine if data integrity is modified through change in hash values and compare it with original text.