21

Open redirect on chaturbate.com (tipping/purchase_success)

Share:

State	○ Resolved (Closed)
Disclosed	**October 25, 2018 3:42am +0200**
Reported To	Chaturbate
Asset	https://chaturbate.com (Domain)
Weakness	Open Redirect
Bounty	$250
Severity	▭ Low (0.1 ~ 3.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

glc submitted a report to **Chaturbate**. Sep 24th (10 months ago)

Hi,

I would like to report an open redirect issue on `https://chaturbate.com/`

Description

An attacker can redirect a user to any external website using the parameter `prejoin_data`, this parameter seems to miss sanitization.

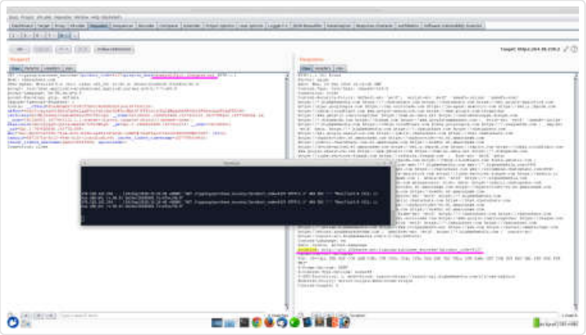
Steps to Reproduce

Visit the following url:
https://64.38.230.2/tipping/purchase_success/?product_code=4137&prejoin_data=domain%2Fpoc.10degres.net
This will redirect you to my website `http://poc.10degres.net`

Browsers Verified In:

- Firefox 56.0, Ubuntu 16.04

PoC



Impact

By modifying untrusted URL input to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials. Because the server name in the modified link is identical to the original site, phishing attempts may have a more trustworthy appearance.

Remediation

Use a whitelist approach to allow redirection to trusted domains.

See also

https://www.owasp.org/index.php/Unvalidated_Redirects_and_Forwards_Cheat_Sheet

Best regards,

Gwen

1 attachment:
F350390: 20180924-open-redirect.png

williammmllc updated the severity to Low. Sep 24th (10 months ago)

williammmllc changed the status to ○ **Triaged**. Sep 24th (10 months ago)

Thanks for the report, we'll get this fixed

Chaturbate rewarded glc with a **$250** bounty. Sep 24th (10 months ago)

williammmllc closed the report and changed the status to ○ **Resolved**. Sep 24th (10 months ago)

We have removed this redirect, can you confirm? Thanks again for the report.

williammmllc requested to disclose this report. Sep 25th (10 months ago)

glc posted a comment. Sep 25th (10 months ago)

Hi, I confirm that I cannot reproduce this bug. Thank you :)

This report has been disclosed. Oct 25th (9 months ago)