47 Open redirection at https://chaturbate.com/auth/login/

Share:

State	Resolved (Closed)
Disclosed	October 22, 2018 3:50am +0200
Reported To	Chaturbate
Asset	https://chaturbate.com (Domain)
Weakness	Open Redirect
Bounty	$200
Severity	Low (0.1 ~ 3.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

shailesh4594 submitted a report to **Chaturbate**. Sep 20th (10 months ago)

Hi,

Summary

An attacker can redirect vicitm on an external website using https://chaturbate.com/auth/login/ endpoint because `next` parameter is not being validated properly. There is a protection existed but it's weak and can be bypassed.

`http` keyword is detected and protection works if payload contains `http` at beginning but that check can be bypassed using `Http` keyword. Though, only numeric is allowed after `Http:` so we can use decimal form of external domain/IP-address. In PoC, `3627732462` is decimal form of IP address of google.com.

Steps To Reproduce:

1. Open https://chaturbate.com/auth/login/?next=Http:3627732462
2. Get logged in
3. You will be redirected on https://google.com instead of a chaturbate website
4. Done

Suggested Fix:

Use more strong regular expression at this endpoint.

Impact

- Simplifies phishing attacks
- Reflected File Download

williammmllc updated the severity to Low. Sep 20th (10 months ago)

williammmllc changed the status to **Triaged**. Sep 20th (10 months ago)

Thanks for the report. This looks like a case when the browser tries to parse a path as a url. It looks like the CSP is blocking this, hence the low severity, however we will fix this.

Chaturbate rewarded shailesh4594 with a **$200** bounty. Sep 20th (10 months ago)

williammmllc closed the report and changed the status to **Resolved**. Sep 21st (10 months ago)

This is now resolved, thanks again for the report.

williammmllc requested to disclose this report. Sep 22nd (10 months ago)

This report has been disclosed. Oct 22nd (9 months ago)