Open Redirect in Linkedin and Yahoo

Vitor "r0t" Oliveira
Sep 24, 2015 · 3 min read

At our company we had a pentesting job to a Node.js web application. After some research I found https://nodesecurity.io, a great website with node.js vulnerabilities. Since the web app from our client was using express.js, the next thing was to look for vulnerabilities to express.js.

And this is what I found, https://nodesecurity.io/advisories/serve-static-open-redirect, a vulnerability found by Pierre-Élie Fauché:

> *"When using serve-static middleware version < 1.7.2 and it's configured to mount at the root it creates an open redirect on the site.*
>
> *For example: If a user visits http://example.com//www.google.com/%2e%2e they will be redirected to //www.google.com/%2e%2e, which some browsers interpret as http://www.google.com/%2e%2e."*

P.S: This vulnerability doesn't work in Google Chrome but works in Firefox and Opera.

I tested in my client's app and it was vulnerable.

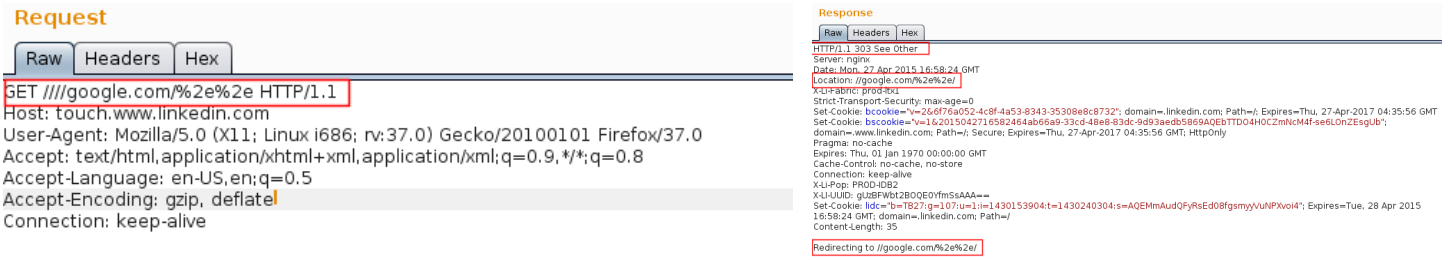
After a couple of days me, **@fabiopirespt** and **@fjreis** decided to search for top websites using express.js and we found 2 websites from **Yahoo** and the **mobile website from Linkedin**.

Time to test them!

We started with Linkedin's mobile website:

https://touch.www.linkedin.com

Issuing the request in burp suite we found that it was not working with two slashes (as Pierre describes in his vulnerability), so we tested with 4 slashes and this is what we got:



Request and Response from touch.www.linkedin.com

Open redirect, yey!

Proof of Concept

Android: https://vimeo.com/126193891
iOS: https://vimeo.com/126193892

> *Report timeline:*
> *April 28, 2015 — **Bug reported to Linkedin***
> *April 28, 2015 — Confirmation from Linkedin's security team*
> *May 28, 2015 — Pinged Linkedin team*
> *May 28, 2015 — **Bug fixed***
> *September 24, 2015 — **Public disclosure***

. . .

developer.yahoo.com and **publish.yahoo.com**

Request and Response from developer.yahoo.com

Request and Response from publish.yahoo.com

Proof of Concept

Android: https://vimeo.com/126305222
iOS: https://vimeo.com/126320994
Android: https://vimeo.com/126305223

Since Yahoo is using HackerOne and open redirects are out of scope, we contacted Yahoo by email.

> *Report timeline:*
> *May 28, 2015 — **Bug reported to Yahoo***
> *May 28, 2015 — **Yahoo's security team** tells to report in **HackerOne***
> *May 28, 2015 — **Bug reported to HackerOne***
> *May 28, 2015 — **Response from HackerOne**: "Thank you for your submission to Yahoo! We are aware of this functionality on our site and it is working as designed. Open redirects have been out of scope since January 1st, 2014. Please continue to send us vulnerability reports!"*
> *September 24, 2015 — **Public disclosure***

LinkedIn Yahoo Security

5 claps

WRITTEN BY

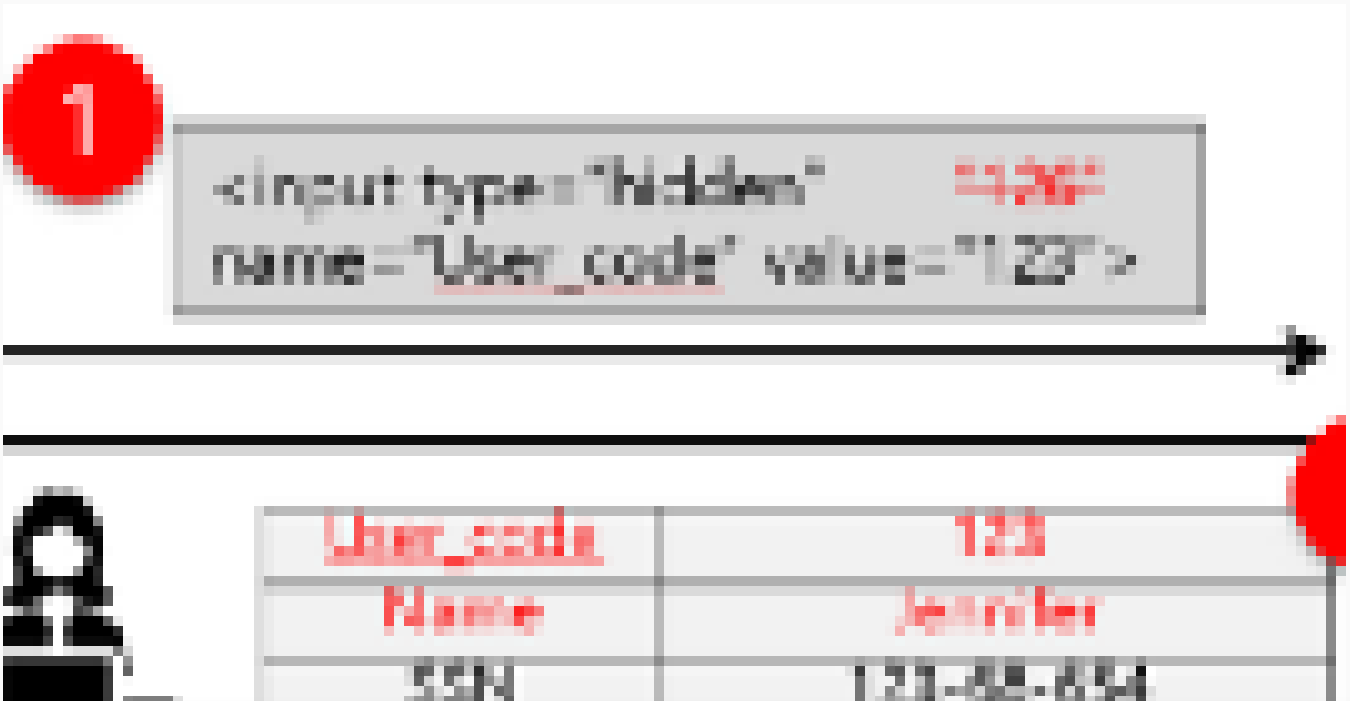
Vitor "r0t" Oliveira

Pentester, red teamer, OSINT guy.

Follow

More From Medium

Related reads

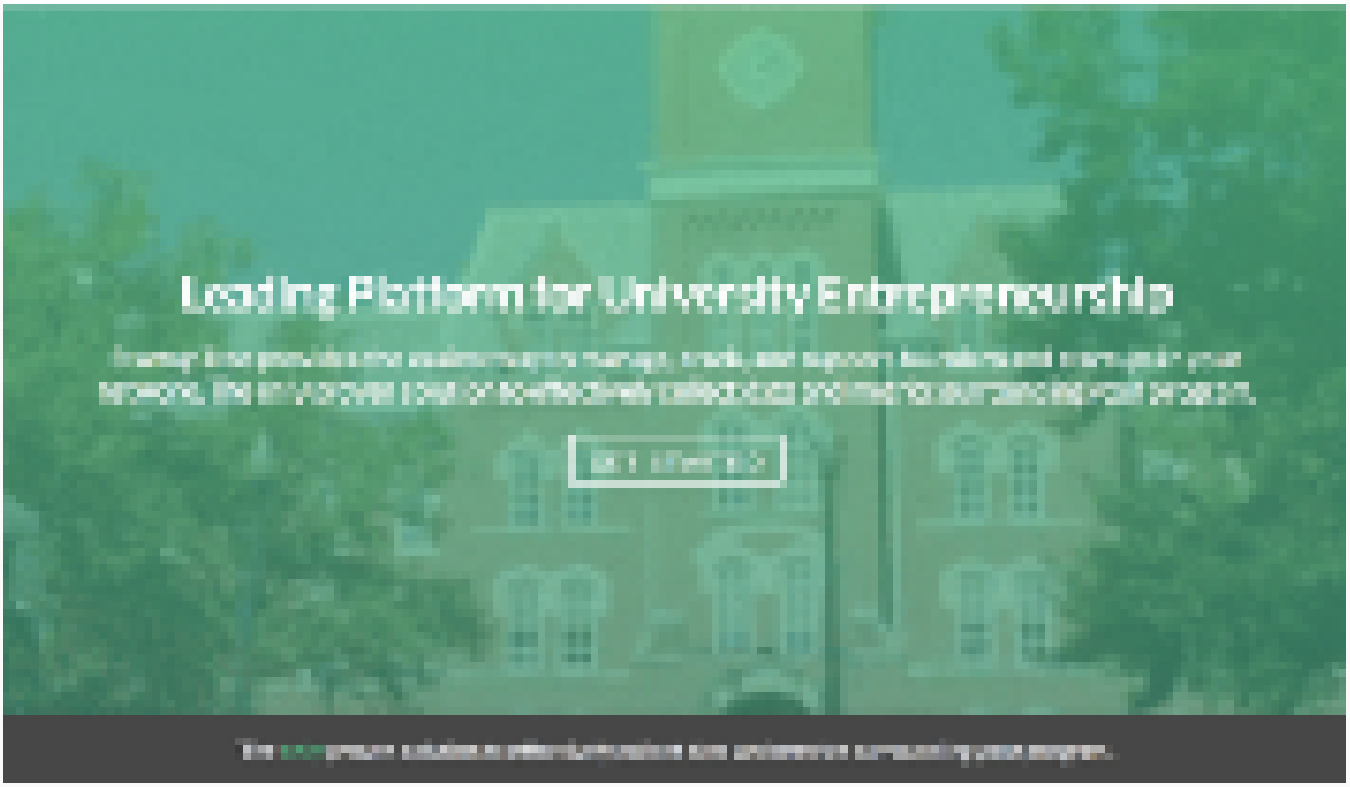


what is Parameter Tampering

MRunal
Jun 21 · 7 min read ★

207

Related reads

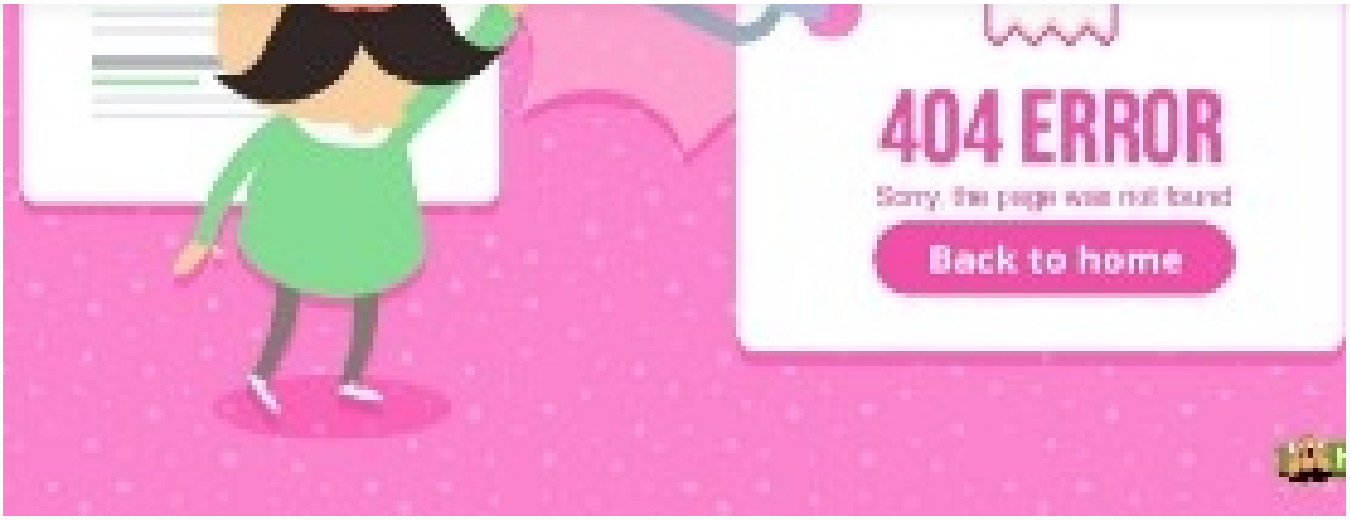


Open Redirects & Security Done Right!

Akshay 'Ax' Sharma
Jun 19, 2018 · 3 min read ★

518

Related reads



Everything You Need to Know About the 404 Page

HostPapa
May 13 · 8 min read ★