From broken link to subfolder takeover on Bukalapak

wis4nggeni Follow
Dec 23 · 4 min read

Bukalapak is one of the biggest online marketplace and “unicorn” startup located in Indonesia. One day when I was taking a break and checking their website to buy something, I noticed that they held a Bug Bounty Program and I think it would be cool if I could carve my name on their lovely “Wall of fame”.

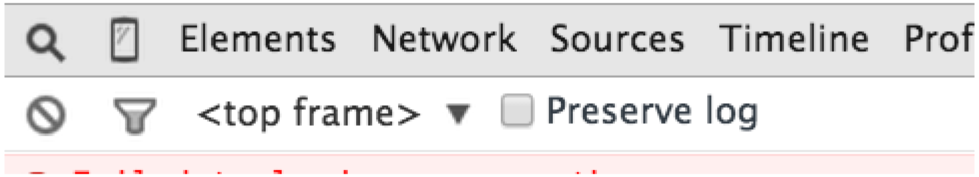
I am especially interested to look for vulnerability on one of their new feature that is hosted on a specific subdomain, *REDACTED*.bukalapak.com.

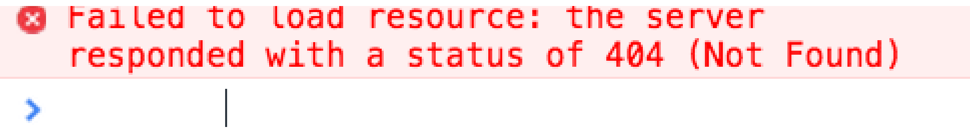
Simply because it's a new feature, so I think it's more likely that they missed something which could lead to a vulnerability.

Long story short, after some time, I couldn't find anything interesting beside some minor or very low severity bug-like clickjacking with no sensitive action, etc.

But, when I did inspect element on one of the pages to check if my XSS payload fired or not (it's not, sadly), I found something that catches my eye on the browser console. The page is trying to fetch an Image on another subdomain, but failed and return a 404 response printed on the browser console. The URL looks like this:

https://REDACTED.bukalapak.com/img/some-random-text.jpg

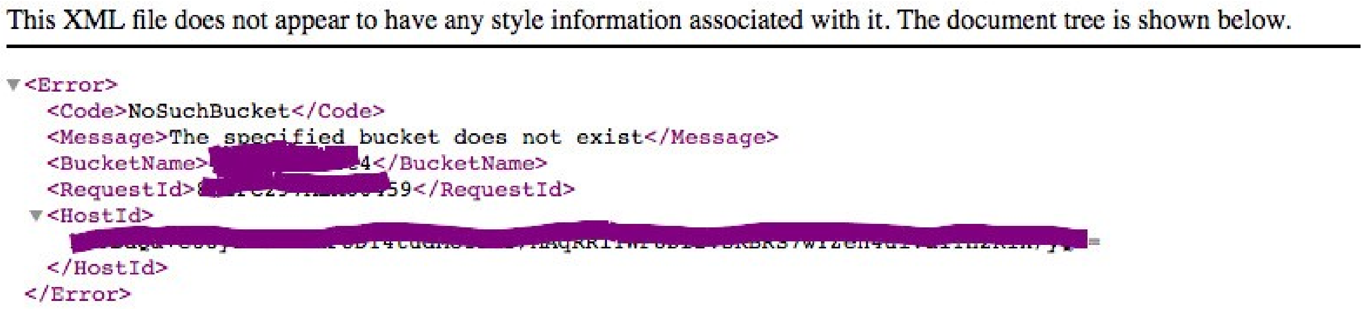




```
Failed to load resource: the server
responded with a status of 404 (Not Found)
>
```

Broken link

I got curious and opened the link on a new tab, and surprisingly, i got that beautiful “NoSuchBucket” error page from Amazon S3 along with the bucket name. :D



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>NoSuchBucket</Code>
   <Message>The specified bucket does not exist</Message>
   <BucketName>[redacted]</BucketName>
   <RequestId>[redacted]</RequestId>
  ▼<HostId>
    [redacted]
   </HostId>
 </Error>
```

Beautiful...

At this point, I know that takeover is mostly possible, but I’m curious because previously, the tools that I used can’t detect this. So I strip the URL to find the main address that pointed to the unclaimed Amazon S3 Bucket.

I found out that the URL is something like this :

https://REDACTED.bukalapak.com/img/

Turns out that the *REDACTED*.bukalapak.com is up and well, it host another feature from bukalapak website and work beautifully. That's why I decided to write this as "Subfolder takeover" and not "Sub domain takeover" because I took over a subfolder and not a subdomain, although it has the same methodology.

After taking a sip of my coffee, I started the take over the process, i made an Amazon S3 Bucket with the name printed on the error page. When choosing a region, actually I've read somewhere that we could do some more recon to know which region is used. But considering bukalapak is located in Indonesia, I decided to just choose the nearest region (Asia Pacific), and turns out i'm right. Take over is complete, the subfolder is now pointed to my controlled Amazon S3 bucket, very nice!

So, what I could achieve by taking over this subfolder?

The first one comes to my mind is stored XSS, i found out that their cookies is set to a wildcard subdomain, so basically they used the same cookies everywhere, XSS is possible. The second one, because this subfolder is hosted in one of their subdomain, clickjacking is possible on any page with X-Frame Options set to “Same-Origin”, which most of the times contain sensitive actions. I could also host a phishing content too, which if combined with the XSS and clickjacking, could be a very powerful attack vector.

But I didn’t exploit further because I’m afraid it’s against their rule, so i decided to report it right away and let them decide the severity. Surprisingly, their Cyber Incident Responder replies my report within less than half an hour! very cool response time. They asked me to upload a specific file to confirm my findings so I do it right away.

Timeline:

- **August 13 2019**: report sent.

- **August 13 2019 (Less than half an hour later)**: Cyber incident responder reply to my email, asking me to upload a specific file to confirm my findings.
- **August 14 2019**: report validated, categorized as misconfiguration with High severity level. They asked me my data to be posted on their Wall of Fame and for bounty payment.
- **August 26 2019**: they carved my name on their Wall of Fame. (Lovely!)
- **September 24 2019**: $$$ paid with a thank you note.
- **December 23 2019**: disclose request approved by security team, write-ups published.

Follow Infosec Write-ups for more such awesome write-ups.

InfoSec Write-ups

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub...

medium.com

)

Writeup Bug Bounty

225 claps

WRITTEN BY

wis4nggeni

Follow

Bug Bounty Hunter from Indonesia. Feel free to contact me anytime : https://t.me/wis4nggeni.

InfoSec Write-ups

Follow

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. Maintained by Hackrew

Write the first response