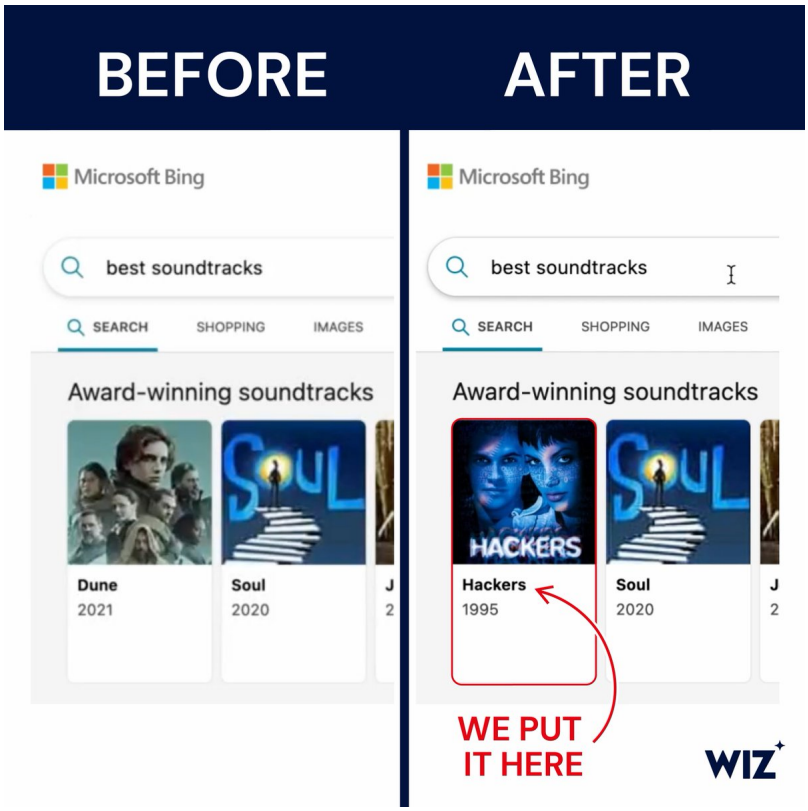
Hillai Ben-Sasson **@hillai** *Wed Mar 29 18:33:13 +0000 2023*

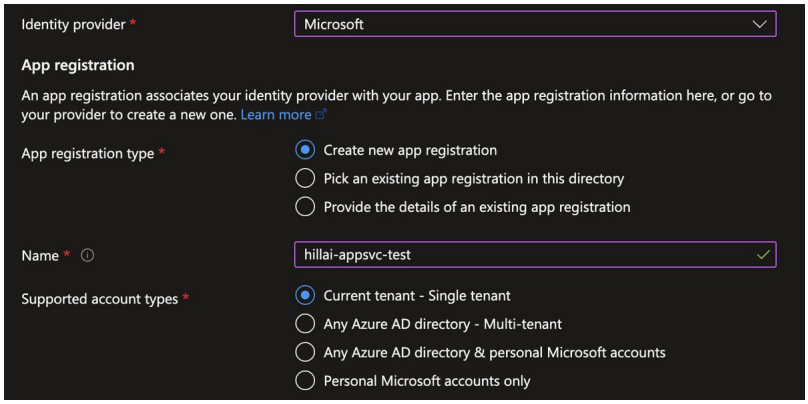
I hacked into a @Bing CMS that allowed me to alter search results and take over millions of @Office365 accounts.

How did I do it? Well, it all started with a simple click in @Azure… ■

This is the story of #BingBang ■■■ **https://t.co/9pydWvHhJs**

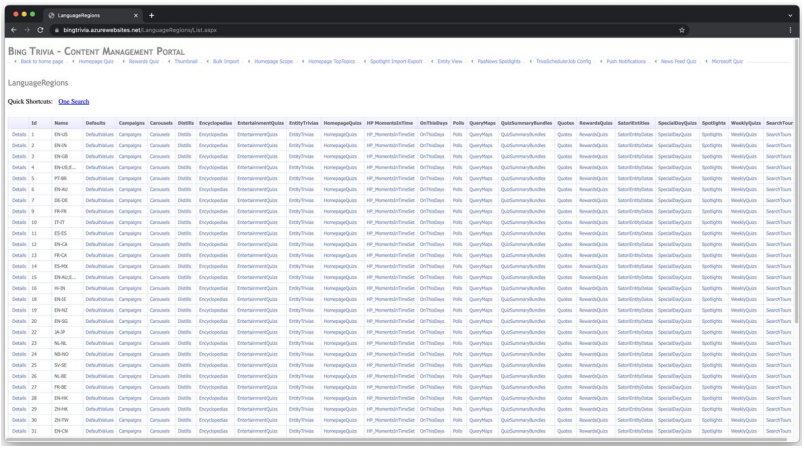


My research started when our Research Team at @wiz_io first noticed a strange configuration in Azure. A single checkbox is all that separates an app from becoming “multi-tenant” – which by default, allows ALL USERS to log in. **https://t.co/B8EgUEENod**



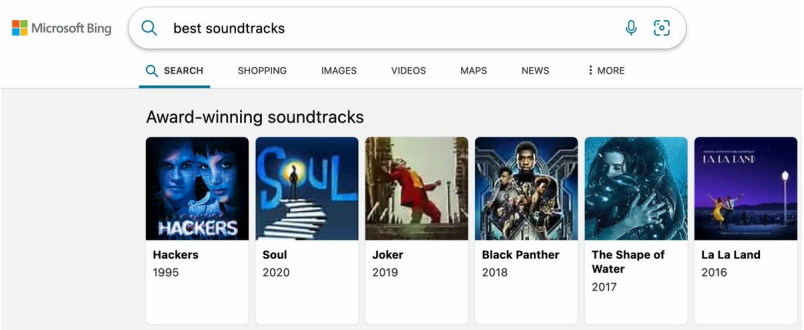
I found a Microsoft app configured like this, and… just logged in ■■■■■

My user was immediately granted access to this “Bing Trivia” page. Don’t let the name fool you – it controls much more than just trivia. In fact, as I came to find out, it can control ACTUAL SEARCH RESULTS ■ **https://t.co/fhBvwtCQ7q**



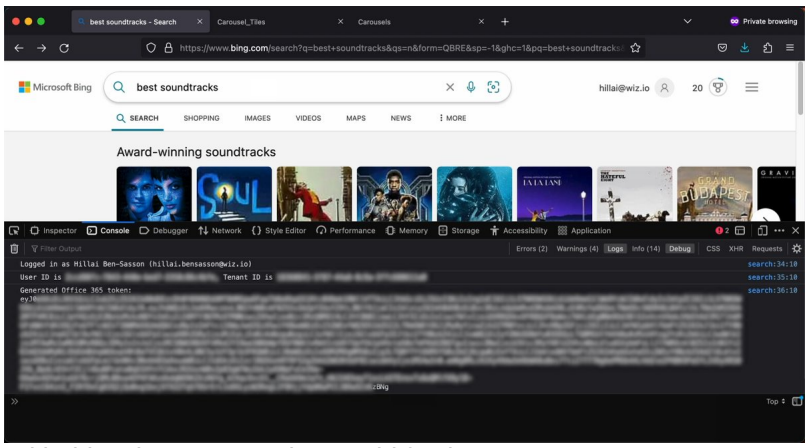
I started looking around to realize the app's purpose and why I had access. I then found a section that contained some keywords and corresponding search results, which raised the question – could this app actually modify search results on **http://Bing.com**? ■

I tested this theory by selecting the "best soundtracks" keyword and switching the first result from "Dune (2021)" to my personal favorite, "Hackers (1995)". I was surprised to see this result immediately appear on **http://Bing.com**! **https://t.co/DE0uohmwIP**



I then checked for XSS viability, by adding a harmless payload into my new result. I refreshed the page, and my payload successfully executed! I quickly reverted my changes and reported everything to Microsoft, but one question remained on my mind – what can I do with this XSS?

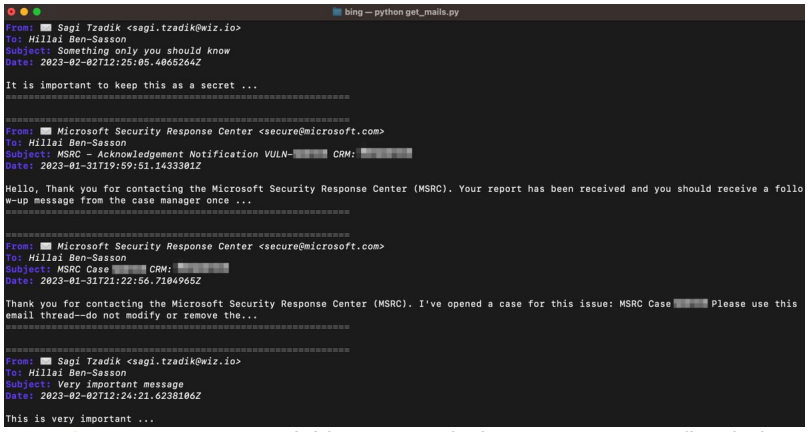
When inspecting Bing requests, I noticed an endpoint being used for Office 365 communications. As it turns out, Bing is allowed to issue Office tokens for any logged-on user. I quickly crafted an XSS payload utilizing this functionality, tested it on myself, and it worked! **https://t.co/uP0MXuRF36**



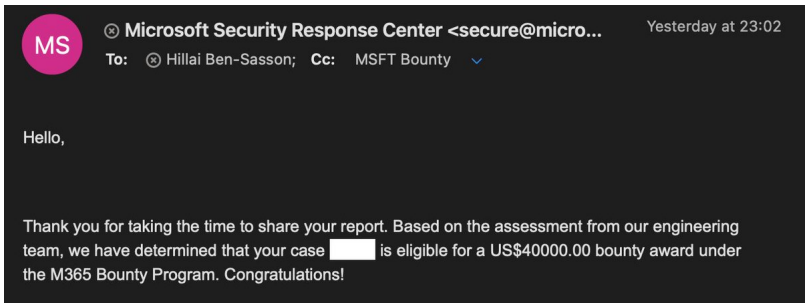
With this token, an attacker could fetch:

Outlook emails ✉■
Calendars ■
Teams messages ■
SharePoint documents ■
OneDrive files ■
And more, from any Bing user!

Here you can see my personal inbox being read on our “attacker machine”, using the exfiltrated Bing token: **https://t.co/f6aHiXYWvD**



@msftsecresponse quickly responded to our report, fixed the vulnerable applications, and introduced some AAD product and guidance changes to help customers mitigate this issue. For this, they awarded us with $40,000 bug bounty, which we will donate ■ **https://t.co/sV4rtTiqCy**



Read the full technical details here >>
https://www.wiz.io/blog/azure-active-directory-bing-misconfiguration

Check out our full attack flow here >>
https://youtu.be/hctqRgQW4lU