Blog

If you want to find vulnerabilities and make a money bug bounty hunting you may want to get a copy of my book. BUY NOW!

Google Exposed Firebase Database

Slack Group

Before we get started I have started a slack group dedicated to hacking. We welcome everyone from beginner to advanced to join. I will be on everyday answer questions, doing CTFs, and talking about cool hacks. If you enjoy hacking and are looking for like minded people join below:

NEW Hacking Group Slack Channel

Introduction

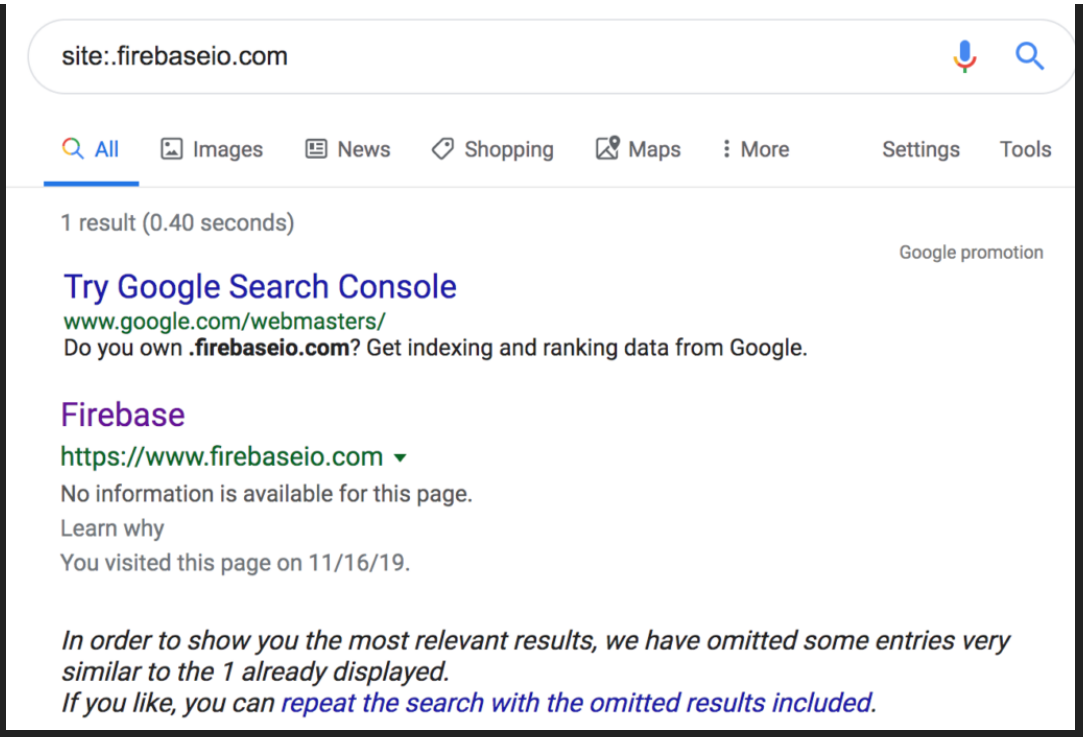
Firebase is Google's mobile platform that helps you quickly develop high-quality apps and grow your business. This post is going to focus on the Firebase Database that many mobile developers use in their applications. There is nothing special about Googles Firebase Database, it's just like any other cloud based database.

Expose Firebase Database

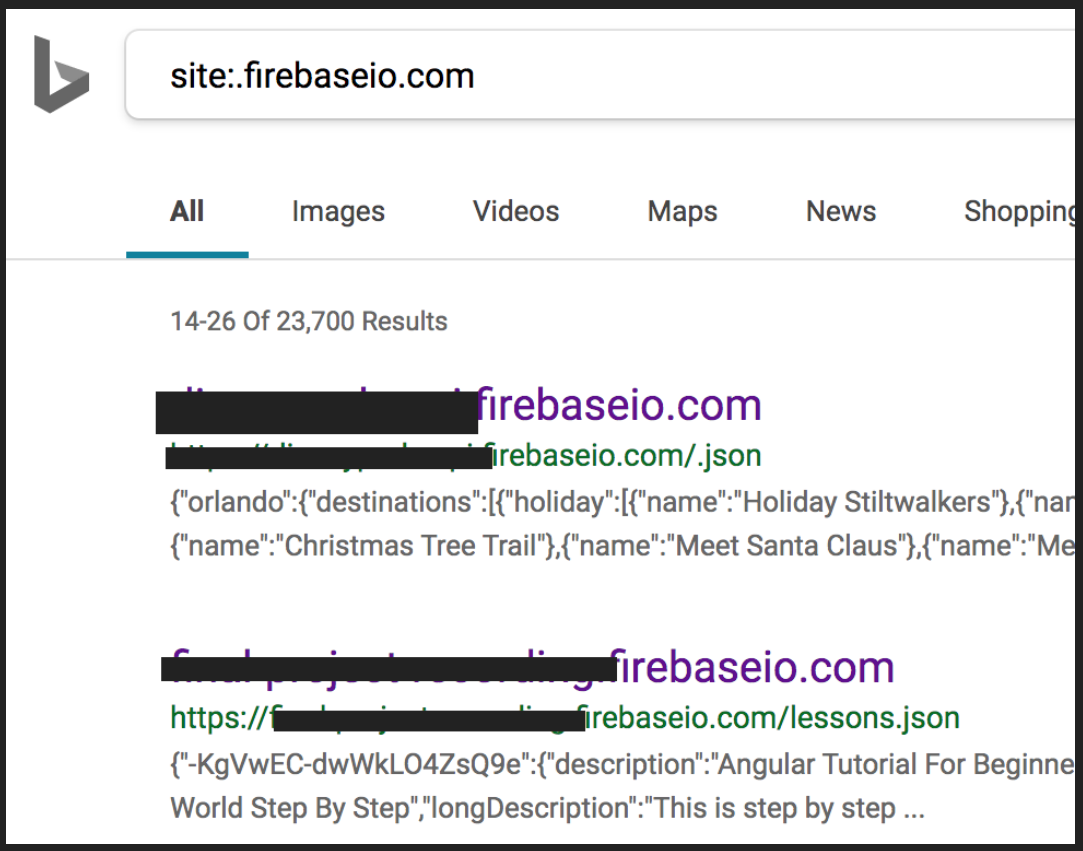
An issue can arise in firebase when developers fail to enable authentication. This vulnerability is very similar to every other database misconfiguration, theres no authentication. Leaving a database exposed to the world unauthenticated is an open invite for malicious hackers.

It seems that Google is well aware of the problem. If you try to do a Google dork search for vulnerable endpoints you wont get any results. This is because the results are scrubbed by Google.

```
site:.firebaseio.com "COMPANY NAME HERE"
```



However, if you use Bing or any other search engine you will get plenty of results.



Nothing against Google, I just found it interesting how Google is trying to hide this vulnerability instead of getting to the root of the problem.

Exploiting this misconfiguration is extremely easy. Append **".json"** to the end of a firebase url and if you are able to see their database they are vulnerable.

As you can see in the above image I was able to find an endpoint with a bunch of exposed passwords. Iv also been able to find endpoints with user messages, social security numbers, credit card details, and much more.

If your looking for a tool to automate this process I would suggest:

```
https://github.com/Turr0n/firebase
```

Conclusion

The vast majority of developers and hunters are unaware of the pitfalls that come with using firebase database. You can easily dump an entire database by simply visiting a URL. It is important to learn the misconfigurations is popular tech-stacks so you can find these easy wins and get paid.

Filed under: database, firebase, misconfiguration

← Exposed Log and Configuration Files

Post Comment

TWITTER

SLACK CHANNEL

GITHUB