Bug report

Report by : zigzag

@zigzagCyberSec

Recipient : Bob

Company : yolo company

Findings list

Number	Host	Ports	findings	Links
1	api.yolo.com	80	Information disclosure	Go to finding
2				Go to finding
3				Go to finding
4				Go to finding
5				Go to finding

Finding 1 - Information disclosure

Summary

An API is accessible without authentication. It is possible to query its endpoints to get information about the company and the clients. This could lead to the compromision of confidential data and help in the the attackers to build a more advance attack.

Risk breakdown

Likelihood : Low / Medium / High
Attack Complexity : Low / Medium / High
Risk : Low / Medium / High

Impact metrics :

☑ Confidentility

□ Integrity

□ Availibilty

Criticity : Low / Medium / High

Step to reproduce

Here are the step by step walkthrough to reproduce the bug.

```
  def foo
    puts 'bar'
  end
```

```
A) Target IP: 192.168.100.1
--------------------------------------

Main Objectives:
- Get shell on machine
- Obtain Account of Domain Controller

B) Target IP: 192.168.100.2
--------------------------------------

Main Objectives:
- Get root shell access to machine
- Dump full Database
```

Impact

Just explain how bad it is !

Recommendations

Here you have some basics recommendations.

- There a list
- Again some stuff
    - and the end

References

1. somewhere
2. Somewhere 2
3. Somewhere 3

Finding 2 - New finding

Summary

Risk breakdown

Step to reproduce

Impact

Recommendations

References