Bug report

Information disclosure - some website

Report by : Quentin Le Bloa

Media : @zigzagCyberSec

Recipient : Kyle

Company : Lunsj.ai

Findings list

Number	Host	Ports	findings	Links
1	api.lunsj.ai	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

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

David Lassig was tasked with performing an internal penetration test towards EvilCorp Network. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate EvilCorps internal netowrk. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to EvilCorp.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on EvilCorps network. When performing the attacks, I was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. All systems were successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

Recommendations

Here you have some basics recommendations.

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

References

1. somewhere
2. Somewhere 2
3. Somewhere 2

Finding 2 - Information disclosure

Summary

Risk breakdown

Step to reproduce

Impact

Recommendations

References