Dorking Adventures 1

Hacking “Orona Ltd.” and “Sociedade Ponto Verde”.

Jaden Furtado

Foreword:

As the title suggests, this is the 1st in a series of articles that I hope to write on Google Dorking. Google is a powerful tool, not just for work and studies, but also for hackers, as a lot of information is readily available online, for those who know where and how to look for it. In this series I am going to be using Google to hack various companies/people and show how I did it.

I do not work for said companies and neither have I been asked to do any of this by them. I have done it simply because I can!

Goes without saying, hacking should not be done to blackmail any company or person. I have informed all the companies/people involved in this series of articles about their vulnerabilities and most of them have fixed their vulnerabilities.

These views in this article do not represent the companies for which I have interned/worked before. They are solely my own.

Jaden Furtado

Disclaimer:

Hacking is a punishable offense in India with imprisonment up to 3 years, or with fine up to two lakh rupees, or with both.

Chapter IX Section 43 of IT act, 2000 prescribes a penalty for the damage to computer or computer system. It is a common thing which happens whenever a computer system is hacked. Black hats damage the system that they hack and steal the information. This enumerative provision includes a lot of activities.

I do not encourage hacking in any way and am doing this solely from an educational objective. I am doing this in the best interest of said companies, to force their hands and fix the issues.

Introduction:

Before we get to the attack, it is important that we understand what BMC's remedy system does.

BMC Remedy is a powerful and amazing tool which is used by the whole organization. It is one of those critical applications on which operations run. Each and every activity is tracked and managed by the Remedy tool. IT and Non-IT operations are carried by this tool. It is widely used software across the IT Industry.

Pros and Cons

- Remedy tool is used for incident management and there are several categories bound with SLAs(Service level agreement) which ensures the closures.
- It is also used for change management across the organization for different environments which make sure all the processes are followed.
- It has a knowledge article section where KBs are generated for known issues which are handy for Business as usual.

- Sometimes it is hard to mention details when several other activities are happening and we need to refresh the page as by that time we lost the data we entered.
- It could use a light version like Angular JS or React JS so the server load gets reduce.
- There is no chat facility provided, if it is possible, I reckon it will better facilitate the incident management.

Also, I am not an expert at any of this, just happened to run across this while on google!

With this knowledge in mind, let's get to the attack.

The attack:

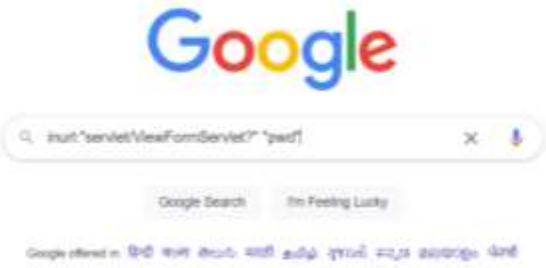
Part 1:

I start by Googling/ Dorking for the term

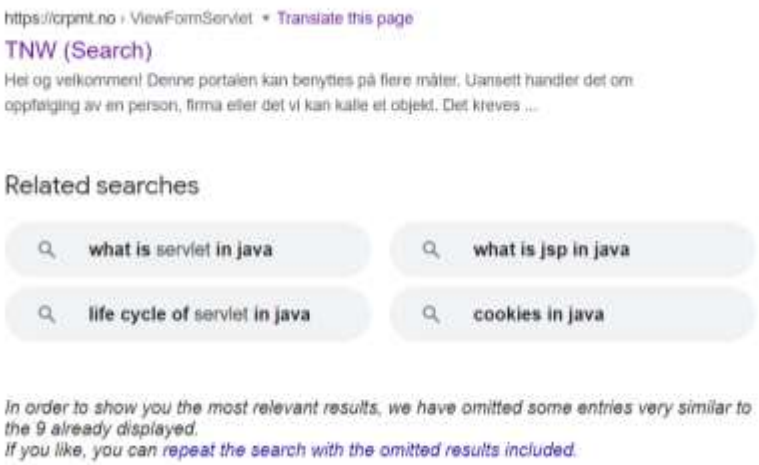
" **inurl:"servlet/ViewFormServlet?" "pwd"** "

To break it down for someone who does not know Google dorking, " inurl: abc" ensures that the term "abc" is present in the search result. In our case, we are looking for "**servlet/ViewFormServlet?**" along with pwd, which is short for password. In short, this should disclose the username and passwords in the URL parameters.

Part 2:



On going through the various search results, this one catches my eye:



The link: https://crpmt.no/arsys/servlet/ViewFormServlet?form=TNW&server=app-test&view=TNW&mode=query&username=tnw&pwd=TnW@2019

And this is what I got:

While just this may not seem like much at 1st, I am really interested in the URL that redirected me here.

https://crpmt.no/arsys/servlet/ViewFormServlet?form=TNW&server=app-test&view=TNW&mode=query&username=tnw&pwd=TnW@2019

As you can see, the username and password have been disclosed in the above link.

I get username=tnw and password=TnW@2019

I now try and login using these details at the portal of this company, i.e.

https://crpmt.no/arsys/

This is what I got:

As you can see, this is the admin panel of the companies BMC remedy AR system's server. And I have root privileges!

On, going to some of the records in this server, this is what I get:

ANSATTE

Navn+	Ansattnr	BrukerID+	e-mail - jobb	Mobil	Ansatt fra	Ansatt til	Avdeling	Team	Stillingsbr	Telefon - priv
[redacted] Bertelsen		[redacted]	[redacted] @ orona.no	[redacted]	01/03/ 2002		[redacted]	[redacted]		
[redacted] B e r g l i [redacted]		[redacted]	[redacted] @ orona.no	[redacted]	01/03/ 2002		[redacted]	[redacted]		
[redacted] Grüner		[redacted]	[redacted] @ orona.no	[redacted]7	01/03/ 2003		[redacted]	[redacted]		
[redacted] W e s t [redacted]		[redacted]	[redacted] @ orona.no	[redacted]	01/06/ 2005		[redacted]	[redacted]		[redacted]

Ansatte is Norwegian for Employees. And more records:

In all, I got my hands on nearly 1000 pages of sensitive company records. These contained everything from details of past employees, to quotations, receipts, confidential company projects, etc.

As I had root privileges, I could modify as well as delete said records.

These belong to a Norwegian company named Orona, which manufactures Lifts, elevators, etc. I disclosed the vulnerability to them. This was their response:

As the admin of their server mentioned, this was a test/staging server. A lot of the data that I got was rather old and would not hold much value.

However, had I been a malicious user, I could use this server as an entry point to target this company. Really glad the team at Orona fixed their server. Kudos to them!

##

Part 2:

On googling, another link which caught my eye was:

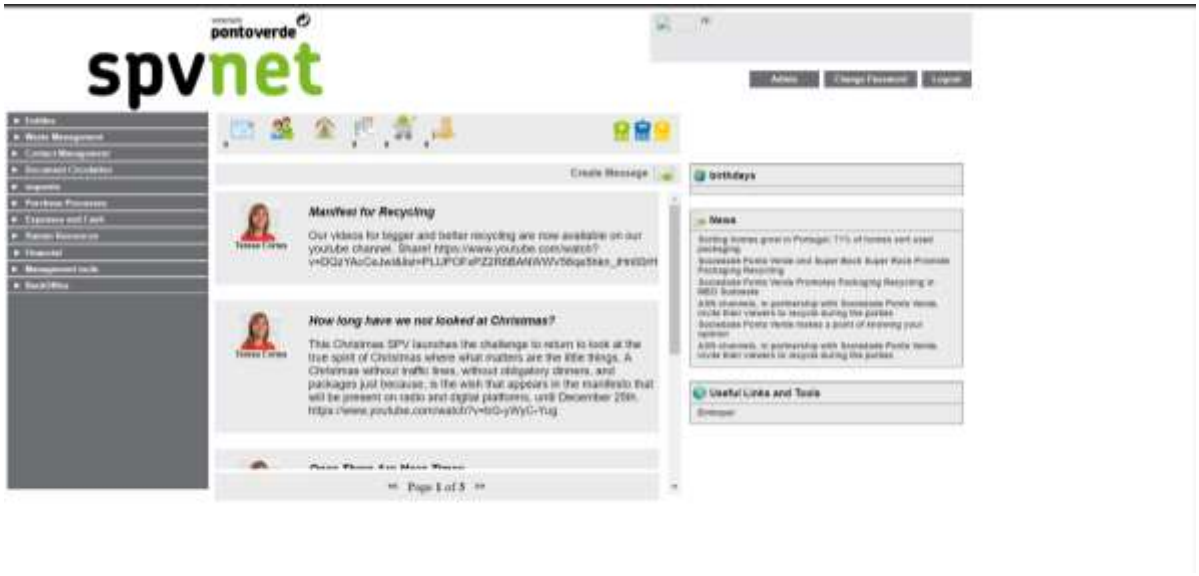
https://spvnet.pontoverde.pt/arsys/servlet/ViewFormServlet?form=PQVP_DGR_PQUA_ApresentacaoCandidaturaDisplay&server=srvp-spvars01&mode=Search&username=local.get&pwd=form.redirect&usertimezone=Asia/Calcutta

And again, we can go through the same process as before. In this case, username is "local.get" and password is "form.redirect". The ideal login page is this:

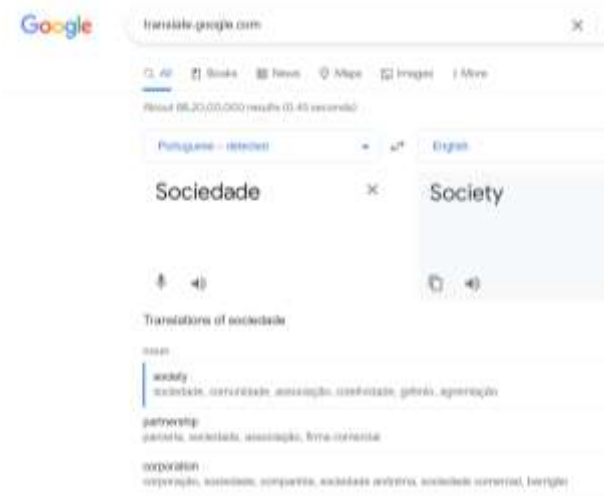
This shows that 2FA has been implemented (or so they think). You see, the username and password aren't something that are used normally. This is a misconfiguration in the server. Instead of asking me for an access token, it redirects me to this page.

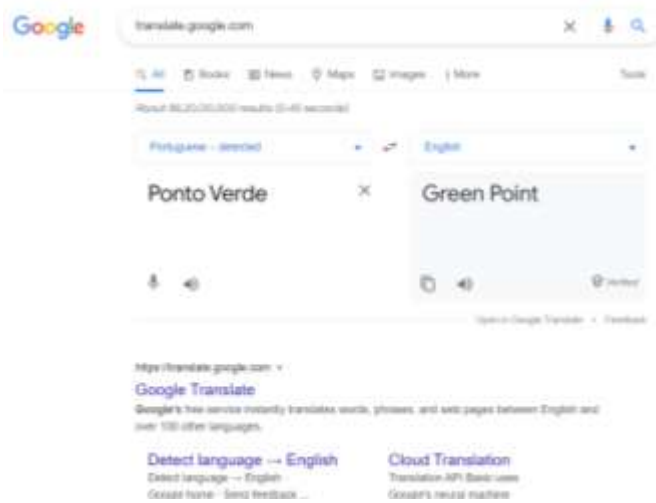
On entering the credentials again, I get the following:

The english translation of the page:

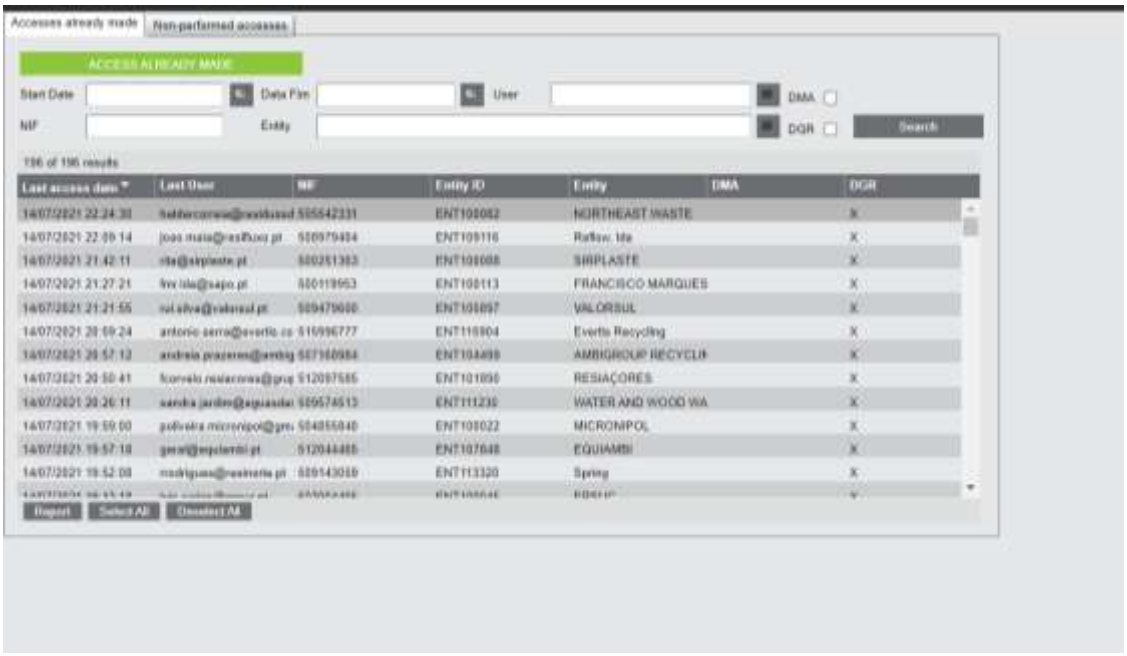


As you can see, the name of this organization is “Sociedade Ponto Verde”. On translation it is:





The below shows that the server is still in use:



Having root privilege, I have freedom to modify, delete, add whatever I want to this production server. These include accounts, banking details, HR, company details, etc.

Because, this is BMC remedy, I am also able to send messages to all employees, thus exposing this NGO along with all companies/organizations that are associated with them to a phishing attack.

They are present of Instagram at: https://www.instagram.com/pontoverde.pt/

With 18.4k followers on Instagram, this is a sizable NGO. Being an NGO I decided to alert them about their vulnerability, but unfortunately, I have still to receive a reply from them about the same. I will update this once they reply to me or fix the vulnerability.

Threat Prevention:

As the problem in these servers is primarily with the URL, this is the recommendation by BMC about the same:

“

You can add an inclusion list of URLs to be redirected to when you log on to the mid tier and when you log out of the mid tier. An inclusion list of URLs is allowed in the goto request parameter of LoginServlet and LogoutServlet so that the user is automatically redirected to the specified URL.

To add an inclusion list, add the following property in the **<midTierInstallDirectory>/WEB-INF/classes/config.properties** file:

arsystem.inclusion_goto_urls=http://www.google.com,http://www.microsoft.com,

http://<midTierServer>/

Note

The inclusion list must also contain the mid tier's own URL to allow the mid tier to redirect to itself.

”

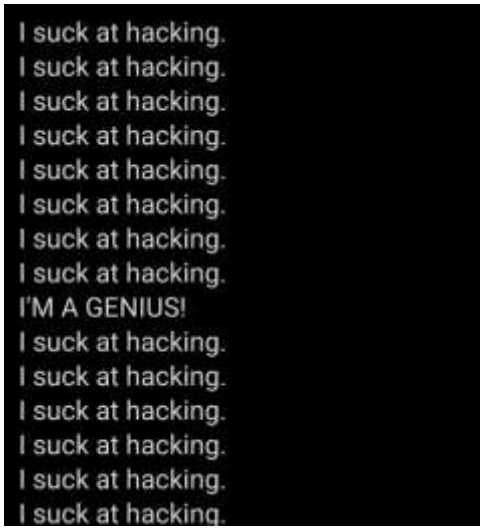
My suggestion is that only users having a certain IP address should be allowed to login. This is difficult to enforce, but worth the pain, given the sensitive data we are dealing with in this case.

Something better than a password would be passwordless authentication:

Final word:

These two organizations had the same vulnerability in the same type of server caused due to a misconfiguration. One got back to me, the other did not!

Google Dorking, as I showed, is an easy way of finding vulnerabilities in websites and can be used to hack if you know what you are doing. In the next article, I will show how to find usernames and passwords of live accounts for full account takeovers. Developing the skills to successfully exploit a vulnerability takes time and it is easy to get demotivated, but this just the way hacking is.



Until next time!

Useful Links:

Google Dorking: https://en.wikipedia.org/wiki/Google_hacking

Link to all recommendations by BMC: https://docs.bmc.com/docs/brid2002/understanding-security-threats-and-preventing-security-risks-918961066.html