LAB 1 WRITE UP (Reconnaissance)

Name : Shriram Karpoora Sundara Pandian
Course : Computer System Security

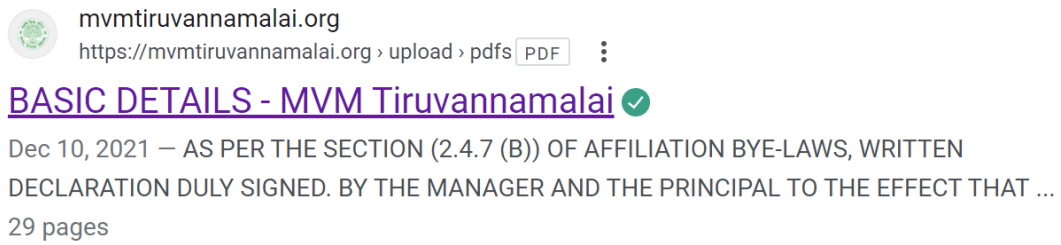
These are the points discussed

- What is the critical piece of information?
- What tools or sources did you use?
- What value might this information have to an attacker and how might they use it?

Target : The target I have chosen is a popular school at Tiruvannamalai, TamilNadu, India. www.mvmtiruvannamalai.org

I started my information gathering using google dorking as a basic step.

Google dorking
First Command : inurl:mvmtiruvannamalai.org intext:username | password
Result I got is rich and all the personal information of the principal of the School



ADDRESS	MAHARISHI VIDYA MANDIR,58/3, 4 MELATHIKAN VILLAGE,THENMATHUR POST	**AFFILIATION CODE**	1930172
PRINCIPAL	MRS C KALYANI	**PRINCIPAL'S CONTACT NUMBER**	9500669776
PRINCIPAL'S EMAIL ID	kalyanichinna1998@gmail.com	**PRINCIPAL'S RETIREMENT DATE**	10/12/2021
SCHOOL'S CONTACT NUMBER	0000-7092160410	**SCHOOL'S EMAIL ID**	mvmtvm12010@rediffmail.
SCHOOL'S WEBSITE	www.mvmtiruvannamalai.org	**SCHOOL'S FAX NUMBER**	0000000

Value from this document :

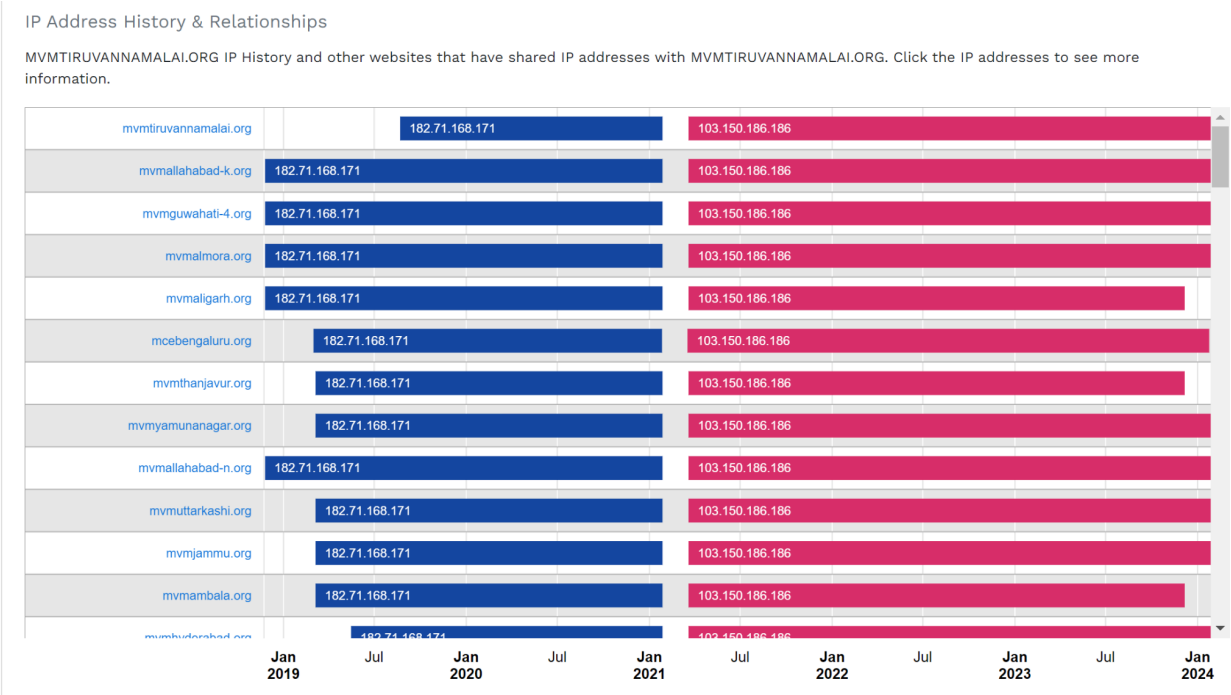
- Personnel Email address of the principal
- Contact phone number
- All the dates they have used for registration

How can I use it ?

- I can personally send a phishing email to her personnel email address to update the account.
- Send malicious links to update the tax information which is mandatory and due in 5 days etc, which may be later useful form
- My intention is to report the vulnerabilities to them and make money, or take their site down to demand money, or send phishing emails and social engineering them to know more information and again get back to them.

Builtwith.com

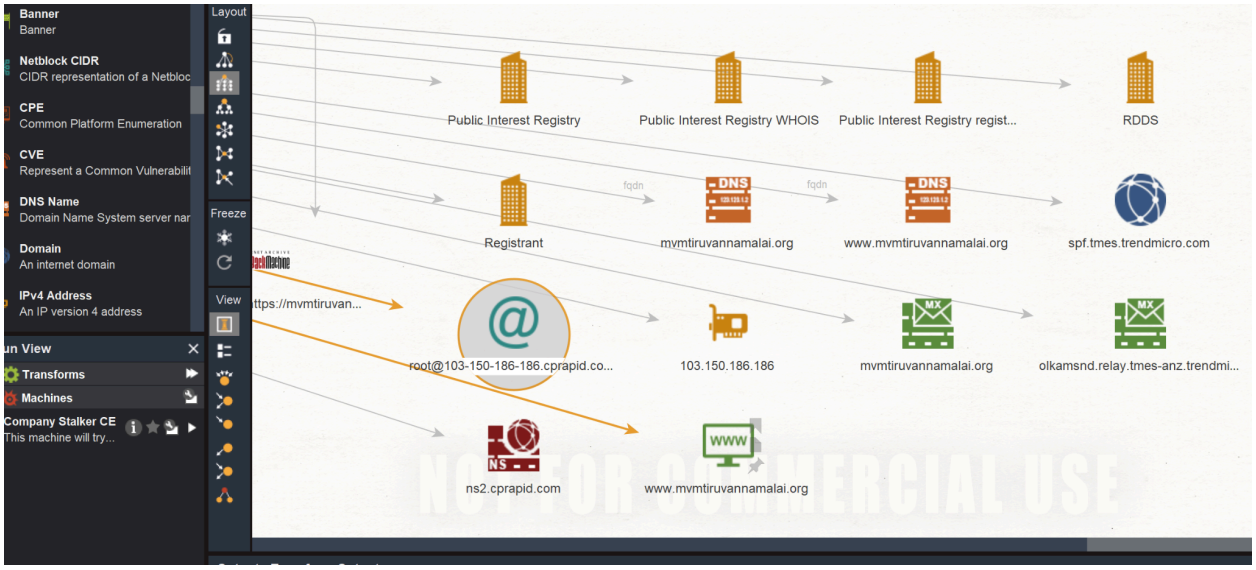
I ran this tool to know whether this school has branches all over India if so they are connected to the root domain in other words do they have single root domain.



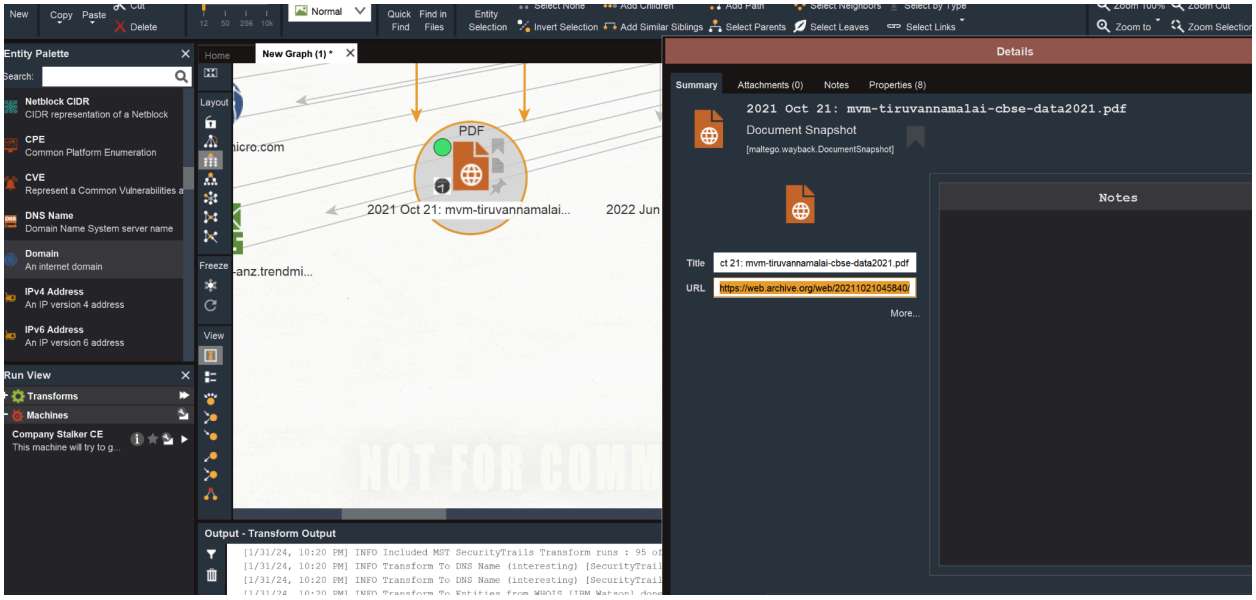
It seems like their branches have same root domain and lot of domains we gathered and we can repeat this process to all the branches separately which are operated by different principals.

Maltego

We are able to see the root Ip of the domain and trying to find more public document they have shared to retrieve more important information of the people in the organization.



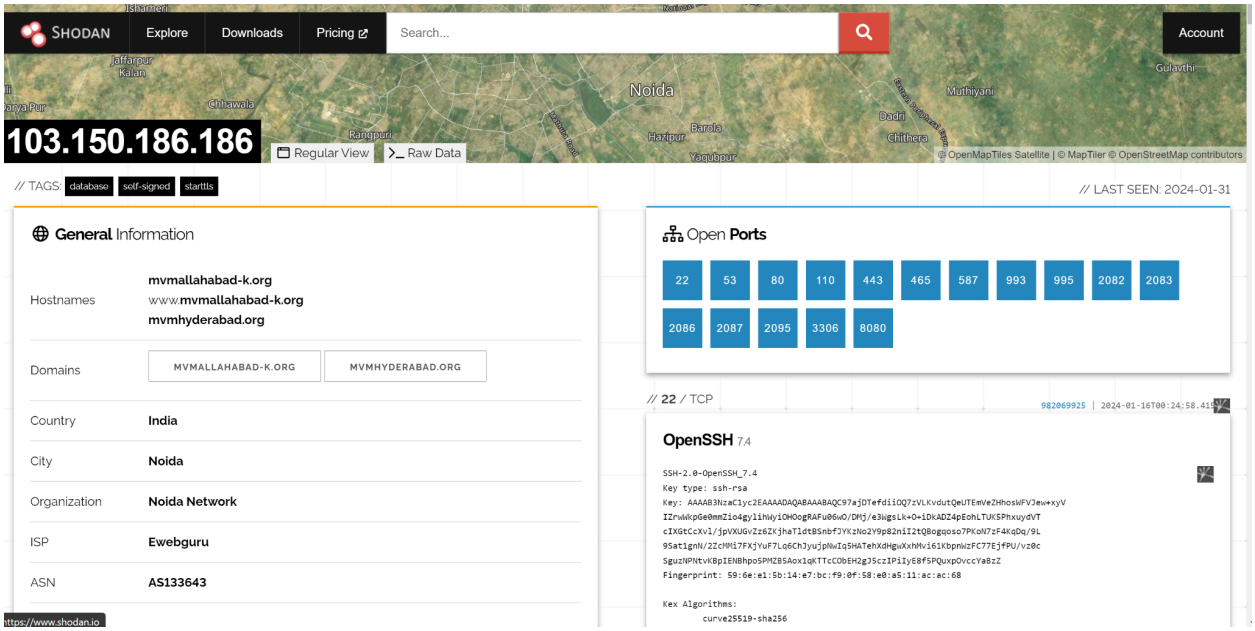
Successfully, we got a link for the main pdf registry which discloses personal information of the Chairman of Maharishi Schools and It has a lot more information about the school (location, all the necessary information like, building management documents, tax document, Electricity bill etc.



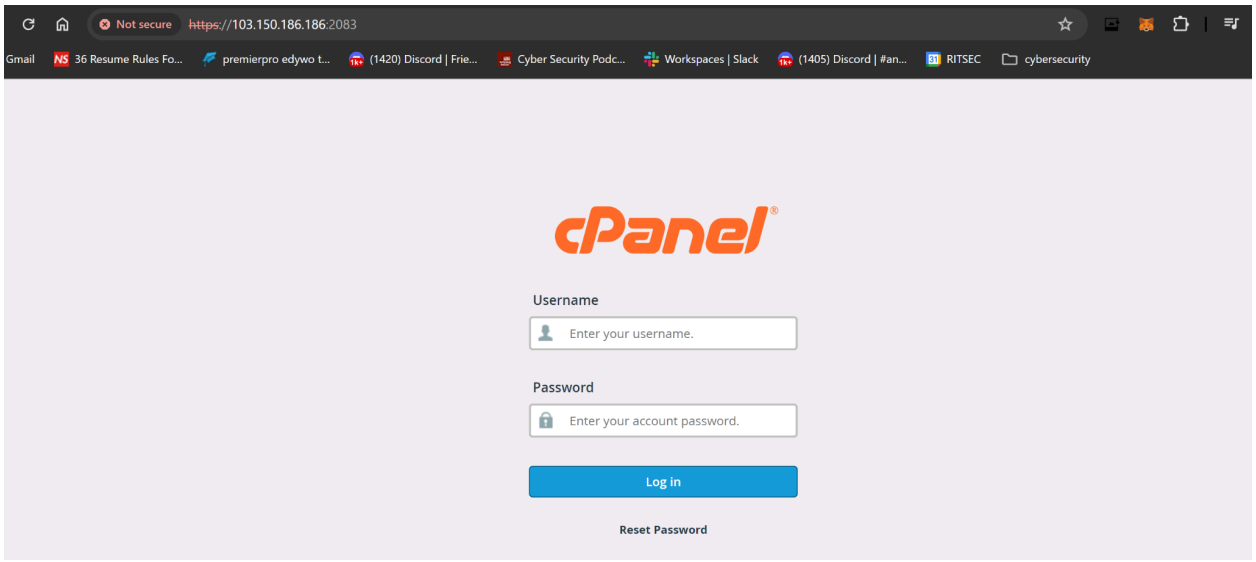
CHAIRMAN/PRESIDENT'S/ CORRESPONDENT NAME	DR GRISH CHANDRA VARMA	**CHAIRMAN/PRESIDENT'S/ CORRESPONDENT ADDRESS**	Maharishi Vidya Mandir Campus, Lambhakeda, Bhopal.
CHAIRMAN/PRESIDENT'S/ CORRESPONDENT PHONE (OFFICE)	0755-6767100	**CHAIRMAN/PRESIDENT'S/ CORRESPONDENT PHONE (RESIDENCE)**	07554000623

How can I use this information ?
We got personnel information of the chairman, not the email yet, but using phone number we can ask their email address through Social Engineering for example " I am calling from web server management (cPanel Management), I have a report to send, please give me your personnel email address, so that I can forward the document.

Shodan :

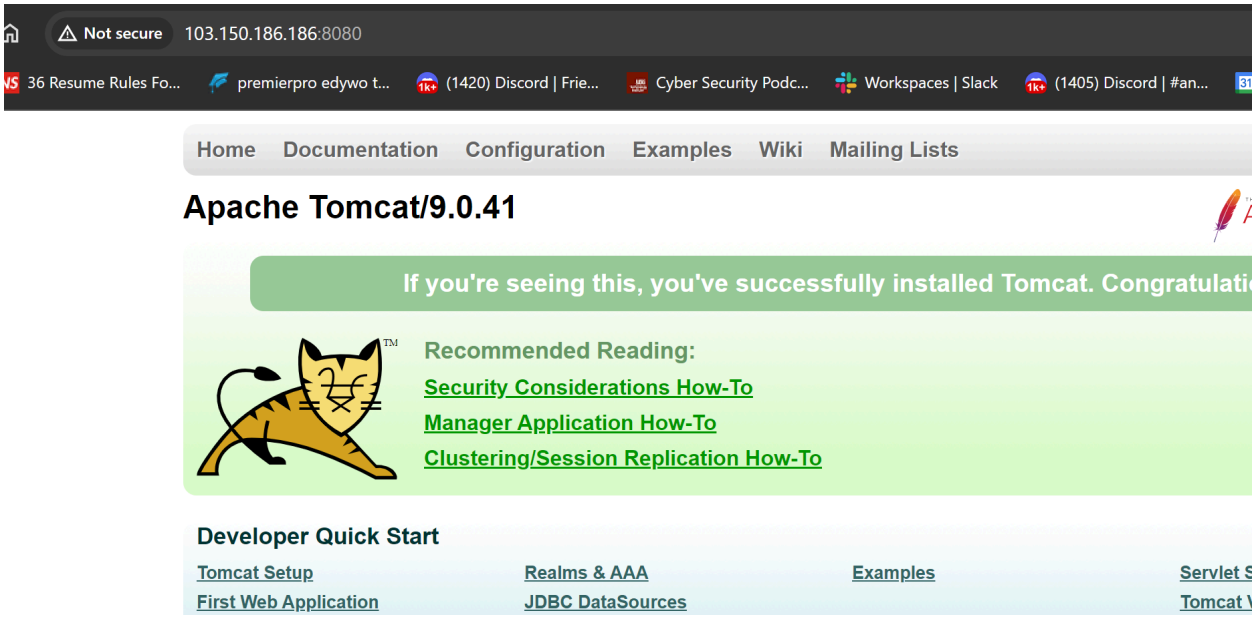


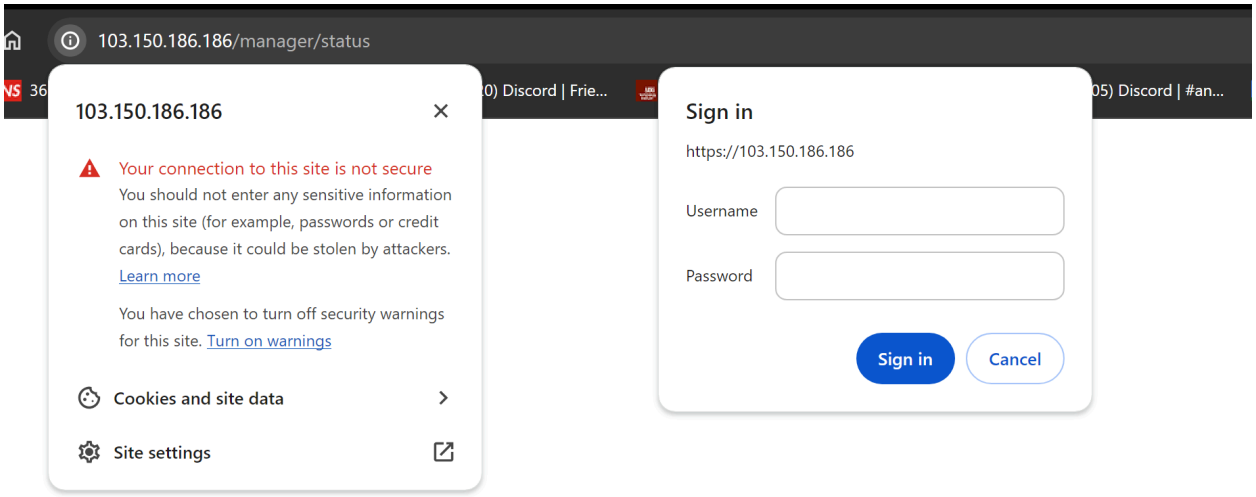
Shodan gave a lot of information too and it gave rich information about the server management and server side like ports and non secure communication and open admin login portal's etc which is shown in the below screenshots.



Admin portal for managing the server is open and not secure, On further analysis we can bring this site down.

Also the tomcat server is running at port 8080 which is open.





If we can social engineer them for username and password, the server will be easily taken over.

Conclusion :

From the initial analysis using OSINT tools, we can see that a lot of rich information is available for this website, and the school seems to be more religious and cultural, which is a good topic for influencing them for phishing. Almost using Google Dorking, I got all the information through pdfs and the documents they have uploaded on Google. Shodan revealed all the open ports, and we also have the email ID of the principal of the school for further phishing attacks. Overall, I would write a lot of vulnerabilities for this site, and there is a lot to take advantage of.