Student Internship Report

By

Ganji Pavan Sai

Intern at spyry

(ST#IN17B9)

Acknowledgement

I would like to express my deepest appreciation to all those who provided me the possibility to complete this Internship.

A special gratitude to my internship mentors, **Mr. Prameel Arjun** and **Mr. Bharath Kumar** for providing me with training, encouragement and support in completing the internship.

I also would like to take the opportunity to express our thanks to **Dr. Rama Devi,** Professor & Head of CSE Department, CBIT for her valuable suggestions and moral support.

I am grateful to our Principal **Dr. B. Chenna Kesava Rao,** Chaitanya Bharathi Institute of Technology, for his cooperation and encouragement.

Finally, we also thank all the staff members, faculty of Dept. of CSE, CBIT, our friends, and all our family members who with their valuable suggestions and support, directly or indirectly helped us in completing this internship.

-G Pavan Sai

Declaration

I, **G Pavan Sai**, student of **Chaitanya Bharathi Institue of technology**, studying in 3rd year CSE have completed my internship at **Spyry Technologies**, Bangalore which was held from 3rd July 2017 to 19th July 2017.

This report is being submitted for fullfillment of my internship and for record purposes.

G Pavan Sai Date: 5th August 2017.

(ST#IN17B9)

Executive Summary

The following document is the summary of work that I have done during my internship at Spyry Technologies LLP. It begins right from what I learnt during the training sessions and ends at the final penetration test report that I have submitted as to full-fill the requirements of the internship.

The report starts with a brief description of the organaisation followed by the listing of the tasks that have been assigned and later describing how I approached each task and how they were performed.

Finally the report ends with the outcomes of the internship.

Table Of Contents

1. ABOUT THE ORGANISATION

1.1 A Brief History of the Organaisation

Spyry Technologies, a Cyber Security leader is a reputed brand for companies that need to protect their identities, businesses and brand online from

Cyber Attacks and also a pioneer leader in IT industry, is operating based out of Bangalore.

Spyry Technologies with its foundation pillars as Innovation, Information and Intelligence is exploring indefinitely as a Technology Service Provider and as a Training Organization.

In today's world of ever increasing cyber crime and threats to every individual and organization, Spyry is a one-stop shop that caters to all your information security needs.

Mission:

To secure. To strengthen. To simplify.

Our mission is to provide comprehensive web space security to our clients and inculcate a knowledge based culture of safe and secure use of cyber space to eliminate the disruptions to your business and life.

Vision:

To create a virtual, safe and secured Cyber Space.

We create a world where all internet users operate on a level playing field. We want to provide services that make the internet a virtual utopia – a place where knowledge is nestled in a package that is beautiful yet strong, and is completely safe from prying eyes and devious hackers.

Spyry Deliverables:

- Cyber Security Training
- Information Security Consultancy and Solutions
- Annual Cyber Security Contracts
- VAPT & Emergency Incident Response

1.2 Areas of service

Corporates

1.1 WSPT(Web Space Penetration Testing) - One Time Scan & Patching.
1.2 ASSC (Annual Security Scan Contract) - Regular Monthly Scanning
1.3 Corporate Training - Specialized Skill Development Courses

Government Departments

2.1 IT Risk Assessment – For their main Web Portal & other applications / IT Infrastructure that their departments might be using (as a part of e-governance or others) for a security assessment.
2.2 Cyber Police Training – Specialized training to various cyber cells of Law Enforcement Agencies and senior Bureaucrats.

Academia

3.1 Roving Courses by 2/3 Day Workshops for Faculty and Students along with Summer and Winter 1 month trainings in Universities & Colleges

3.2 In-House Courses by 2 Month/6 Month Training & Internship at Spyry Office.

3.3 Complete course on information security and digital forensics.

Our Corporate Clients

On VAPT and IT Risk Assessment Front Spyry Tech has worked with multiple companies in providing critical and timely support for their cyber security/information security needs. Some of the clients of Spyry Tech include :

- 2 of the top 50 IT Companies in India
- 1 of the Largest Private Banks in India
- 2 of the top 10e-Commerce Websites of India

1.3 Milestones in Training & Development

- Spyry Tech has got experience of more than 5,000 Contact Hours of information security training to individuals.
- Trained over 10,000 individuals on various aspects of Information Security ranging from Engineering Students to Cyber Police.
- Have conducted our courses / workshops / training sessions in over 50 establishments till date.

- We provide training in Innovating and Trending Technologies to Govt. Officials, Corporate Houses and Colleges.
- Spyry is a Limca Book of Record Holder - for organizing a 50 hour 10 min Non Stop Marathon Workshop on Cyber Security at PSCMR College of Engineering, Vijayawada in February 2016

Spyry Trainers have conducted workshops, seminars and courses on Cyber Security / Ethical Hacking at the following educational institutions and organizations:

- Chaitanya Bharathi Institute of Technology, Hyderabad
- Vardhaman College of Engineering, Hyderabad
- VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad
- Pondicherry University, Pondicherry
- Sir CR Reddy College of Engineering, Eluru
- Eluru College of Engineering and Technology, Eluru
- IIT Kharagpur
- Lakkireddy Balireddy College of Engineering, Vijayawada
- DNR Engineering College, Bhimavaram
- RISE Group of Institutions, Ongole
- Raghu Engineering College, Vizag
- Chaitanya Engineering College, Vizag
- Andhra Loyola Engineering College, Vijayawada
- Eswar Engineering College, Guntur
- VR Siddartha Engineering College, Vijayawada
- Guntur Engineering College, Guntur
- Rotary Club, Vijayawada
- Visakha Public Library, Vizag

and many more corporate &one-one sessions.

1.4 Spyry Tech Key Team

Prameel Arjun – CEO, Spyry Technologies

He is a 22-year-old, one of the country's efficient and youngest Information SecurityAnalyst. The young student hacker has solved many issues with the vulnerabilities present in various websites and databases, given a solution in clearing the loopholes in order to protect the data to be leaked from the databases. Besides Hacking, he has a major passion in Blogging. He is a author of many renowned blogs in the internet. He is a expert in SEO as well.

While pursuing his Engineering (CSE) itself, he has trained around 5000+ people through various workshops, seminars and presentations and this makes him one of the youngest student trainer in the country.

At the age of 18 he conducted his first workshop in Ethical hacking which was the beginning to hissuccess in this field and now he has a handful workshops to train students in Andhra Pradesh and he is the only student trainer who started conducting workshop for his peers and professors. He conducts workshops on Ethical Hacking, Information Security, Cyber Security, Blogging/SEO and Forensic Investigation corporate organisations as well. With around 6-7 articles about him in various newspapers, he's now a well-recognized face in the country.

Certifications/Awards/Recognitions at a glance

- Certified Ethical Hacker (CEH)
- EC Council Certified Security Analyst (ECSA)
- Microsoft Technology Associate (MTA)
- Associate Member of National Cyber Safety and Security Standards (NCSSS)
- Cyber Wiz Kid award by Science Olympiad Foundation at the age of 12
- Certified for his Computer Skills by New South Wales University, Australia at the age of 13
- World's 22nd Youngest Blogger
- Maxthon Ambassador and Head of Marketing Events – India
- Cambridge Certified Security Associate by CIU
- Cambridge Certified Internet Associate by CIU
- Appreciated by various Foreign Universities, Organizations and Technocrats

Bharath Kumar – Cyber Security Head, Spyry Technologies

He is an avid security researcher with special interest in network exploitation and web application security analysis. He has an experience of training more than 1000 individuals directly and more than 5000+ students personally through online platform. He has found multiple security flaws on various websites and helped the admins to patch them. He exclusively maintains an active Facebook group with over 7000+ users and teaches them various tricks and tips related to Tech.

1.5 Featurettes and Reviews

SPYRY TECHNOLOGIES IS FEATURED IN

THE HINDU

ఆంధ్రజ్యోతి

సాక్షి

THE HANS INDIA

ఈనాడు

THE NEW INDIAN EXPRESS

“I really love the way spyry EDUTAIN people ...it was really fun learning new things at SPYRY.Arjun sir you really rock the show.It is really appreciable the way you respond to all our requests and queries I find very less people with this level of commitment towards their respective professions”

- Guru Charan, Student, Hyderabad

“The workshop was really awesome.We got to know a lot of important security related stuff we did not know before. Arjun Sir's examples were on point. His interaction with us was very friendly and it did not feel like a lecture at all and it literally grabbed my attention. Santosh Sir enlightened us on a lot us things and him being grounded was inspiring”
- Sai Praneet, Student, Hyderabad

"Being an intern at Spyry is a great learning experience where I gained a greater knowledge about cyber security and all the tools used in it. Training under Arjun Sir who is such a hardworking CEO and a great expert in cyber security is awesome. I came to know the value of fun combined with education or work that is emphasized as "edutainment" by Santosh sir. For a person who has a great enthusiasm and passion for learning and for cyber security, Spyry is the right place.
- Sai Lakshmi Yadlapati, Student, Hyderabad

“The best of exploring new about cyber security is all of SPYRY had a great experience in exploring new things, it was completely an edutainment. Thank you Spyry we will be heading back soon to explore more”
- Bhargav Simhadri, Student, Hyderabad

"Had a wonderful journey with spyry internship... The way of teaching, motivation, motives, friendly nature and guidance are simply superb... Happy to be a spyry intern... Keep going..."
- Sharon Christina, Student, Eluru

“It was an excellent practical training by the Spyry. Got to know lot of good things in a short period.Thank you, Arjun Sir.”
- Nithin Revanna, Student, Bengaluru

“Unparalleled in their knowledge will to teach”
- Amurt Purohit, Student, Bengaluru

“One of the best cyber security service provider...I strongly believe this could extend to more and more areas and maintain its excellent standards ever.”

- Sravya, Corporate Employee, Hyderabad

“I have a dream to work with them” **- Sai Nandan, Student, Hyderabad**

2. TASKS

Regular tasks were assigned to monitor and analyse my performance throughout the internship.

2.1 Tasks Assigned

Day:Date	Task Assigned	Task Outcome	Time Taken
Day 1: July 4th	Learn about google dorking to find vulnerable websites. Find out about DNS records.	Learnt about google dorking to find vulnerable websites. Learnt about DNS records and how to find the DNS information of a website	1 day
Day 2: July 5th	Write a report on footprinting a website. Use maltego. Perform L1 , L2 , XXL foot prints on a website	Learnt about using maltego to footprint a website also using whois and other sites to gain more information of a website	1 day
Day 3: July 6th	Nmap – perform various types of scans and analyse the report	Knowledge about various terminologies of a, network devices and the services they provide, collecting information of a website.	1 day
Day 4: July 7th	Nessus – perform a scan on a website and learn about vulnerabilites. Learn Directory traversal	The process of automating a network scan , generating report and analysing the report. Learnt about directory traversal	1 day
Day 5: July 8th	Learn what is SQL injection and perform SQL injection on vulnerable sites	Learnt and performed SQL injection on various websites	1 day
Day 6:July 10th	Learn about acunetix and analyse the report and submit the total findings from Nmap, Nessus, Acunetix in the form of a report	Learnt about acunetix and analysed the vulnerabilities present in a website using Acunetix,Nmap,Nessus.	1 day

Day 7: July 11th	Learn about Cookie stealing and use burpsuite to replicate a session.	Learnt about cookie stealing and replicated a session in one of the login site.	1 day
Day 8: July 12th	Learn about different types of cross site scripting and find some websites that have this vulnerability	Learnt abot XSS and tested some websites for XSS	1 day
Day 9: July 13th	Learn about CSRF and Havij tool and revise for the test.	Learnt about CSRF and learnt about Havij tool which is an automated SQL injection tool and used havij on a website , revised everything	1 day
Day 10: July 14th	Learnt about hping3, robots.txt, .htaccess.	Hping3 to craft tcp packets and robots.txt for avoiding search bots and .htaccess for securing a website.	1 day
Day 11: July 15th	Test	Took the test for measuring my performance	1 day
Day 12-13: July 16-17th	Perform a penetration test on Thinking Nirvana and report the findings	Following the actual CEH methodology to approach a real time client website and a black box testing experience	2 days
Day 14: July 18th	PPT	A revision of all the topics that have been taught at the intern and a chance to express your presentation skills and get reviewed by peers.	1 day

2.2 Tasks Performed

Day 1

It started off with of some basic terminologies of ethical hacking followed by the types of information security threats, phases of ethical hacking and ended with practising a method of the first phase i.e footprinting.

Terminologies learned :

Hack-value, Exploit, Vulnerability, Zero Day attack /vulnerability, The Security Triangle, C.I.A triad.

Types of **Information Security threats** and their **threat agents** :

- Natural threats - Earth quakes etc.
- Physical security threats - dumpster diving, loss or damage of physical.
- Human threats- hackers, social engineering, insiders.
- Social Engineering-Art of convincing to reveal info.
- Network threats - denial of service, sniffing, spoofing, password attacks.
- Host threads – Malware,DOS,Password,Physical
- Application Threats – SQL injection,Cross site scripting,Authentication attacks.

Phases Of Ethical Hacking:

- Footprinting
- Scanning
- Gaining access
- Maintaining access
- Clearing tracks

Footprinting :

It is a process of collecting as much information as possible about a target network , for identifying various ways to intrude into an organisations network system. Processes involved are:

- collect basic information about a target and its network
- Determining the os, platforms, web servers etc.
- Performing who is, ns lookup and exploits for launching attacks.

Foot printing methodologies:

- search engines
- website footprinting

- email footprinting
- Competitive intelligence
- Who is footprinting
- DNS footprinting
- Network footprinting
- Through Social engineering
- Through Social networking sites

Footprinting using Google: This refers to creating search queries to extract sensitive information. It helps attackers to find vulnerable targets.

Some popular google dorks: Inurl, Intitle, Filetype, Site, Cache, Info.

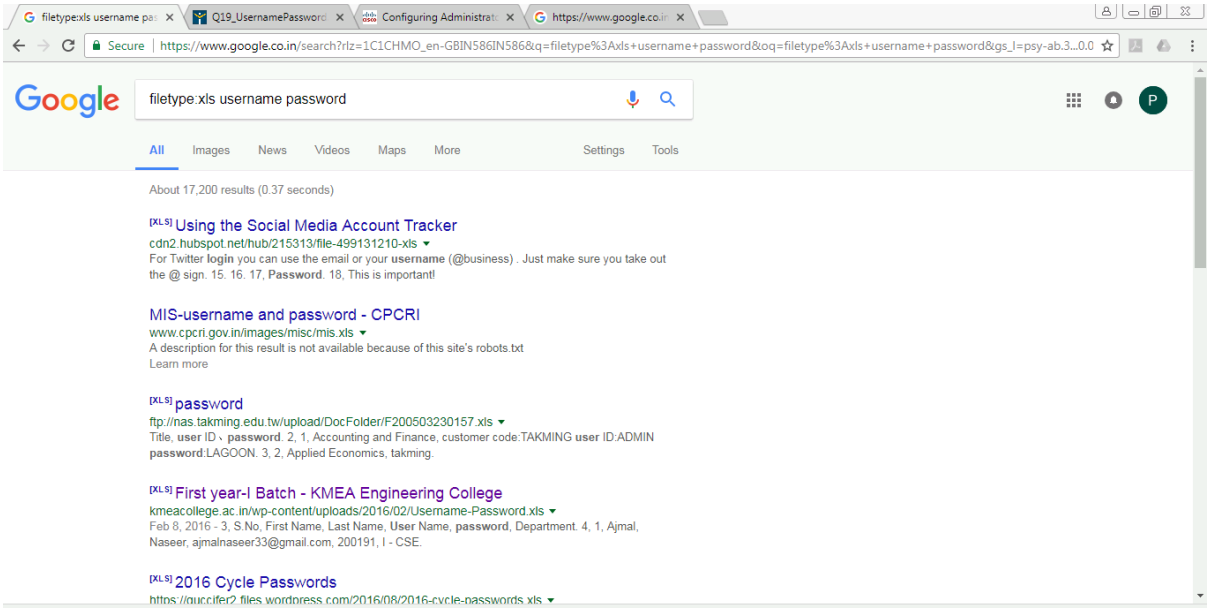


Fig 2.1 Google dork filetype:xls username password

Footprinting using httrack:

Httrack tool allows us to download the front end of a website.

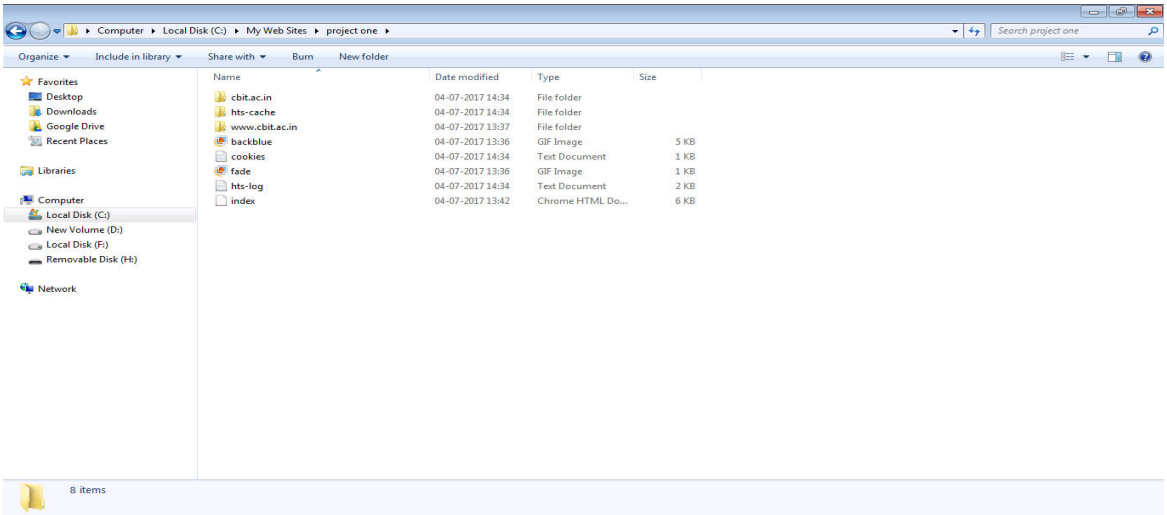


Fig 1.2 Httrack of cbit.ac.in

Footprinting using wayback machine:

WayBack machine(archive.org) allows us to get a snapshot of a website in the past

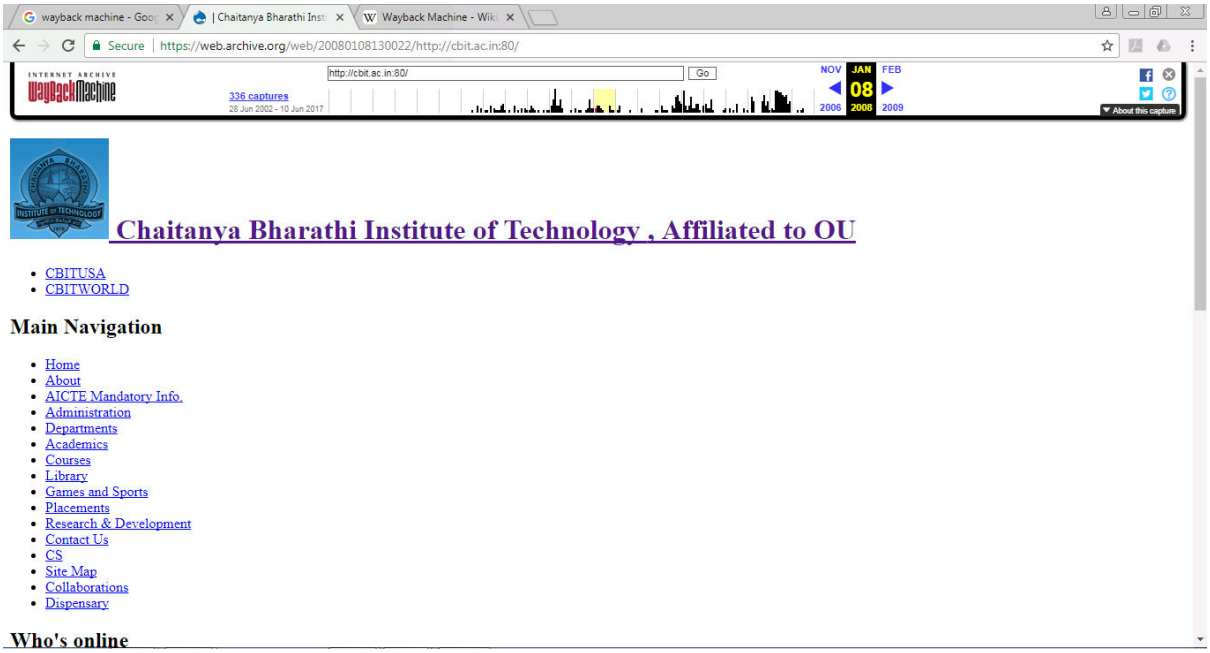


Fig 1.3 cbit website on jan 8 2008 using archive.org

Day 2

Next I learned about DNS system and the types of records present in the zone file in name servers.

DNS records:

A – Points to host ip address (Ipv4)

AAAA – Points to host ip address (Ipv6)

Cname – cannonnical naming, allows alias to a host

NS – Points to host name server.

SOA – Indicate authority for a domain

MX – points to domain mail server.

PTR – Map ip to host name

TXT – Unstructured text record

Hinfo – Host information including CPU type & OS.

DNS foot printing is done using dnsstuff.com,dnsqueries.com,network-tools.com

Whois : It is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system.

Whois.com site is used for querying whois database.

Network Scanning: This helps us to find ip address,mac address and host status and helps us to create a map of target network.

Tools: Advanced ip scanner, Ping and traceroute,Maltego.

Footprinting on osmania.ac.in using whois.com,dnsstuff.com, network-tools.com, Maltego, ping, traceroute

Whois on osmania.ac.in gave

DOMAIN INFORMATION

Domain:	osmania.ac.in
Registrar:	ERNET India (R9-AFIN)
Registration Date:	2002-12-31
Expiration Date:	2018-12-31
Updated Date:	2016-03-08
Status:	ok
Name Servers:	ns1.osmania.ac.in 14.139.82.38

Fig 2.1 who is on osmani.ac.in

Registrant ID:R-R04060720364
Registrant Name:Dr.Gopal Naik
Registrant Organization:Osmania University
Registrant Street1:University Road
Registrant City:Hyderabad
Registrant Postal Code:500007
Registrant Country:IN
Registrant Phone:+91.4027095192
Registrant Email:director_is@osmania.ac.in
Admin ID:A-R04060720364
Admin Name:Dr.Gopal Naik

Ping on osmania.ac.in gave

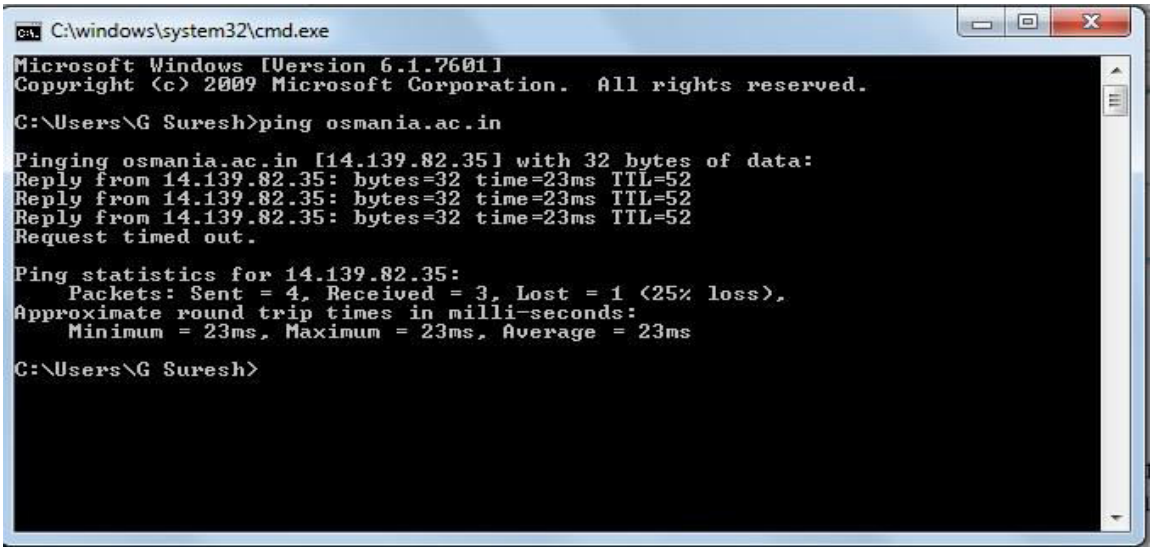


Fig 2.2 Ping on osmani.ac.in

DNS footprinting on osmania.ac.in

Dns records:

Retrieving DNS records for **osmania.ac.in**...

DNS servers

ns1.osmania.ac.in [14.139.82.38]

Answer records

osmania.ac.in	TXT	google-site-verification=KR1eZG5CYE6bcx7jMppaJjsCHFbsKUPtoYjGVAT0inc	86400s
osmania.ac.in	MX	preference:	1086400s
		exchange:	aspmx2.googlemail.com
osmania.ac.in	MX	preference:	1086400s
		exchange:	aspmx3.googlemail.com
osmania.ac.in	MX	preference:	186400s
		exchange:	aspmx.l.google.com
osmania.ac.in	MX	preference:	586400s
		exchange:	alt1.aspmx.l.google.com
osmania.ac.in	MX	preference:	586400s
		exchange:	alt2.aspmx.l.google.com
osmania.ac.in	SOA	server:	ns1.osmania.ac.in86400s
		email:	hostmaster@osmania.ac.in
		serial:	2012101500
		refresh:	1200
		retry:	120
		expire:	1209600
		minimum ttl:	86400
osmania.ac.in	NS	ns1.osmania.ac.in	86400s
osmania.ac.in	A	14.139.82.35	86400s

Authority records

Additional records

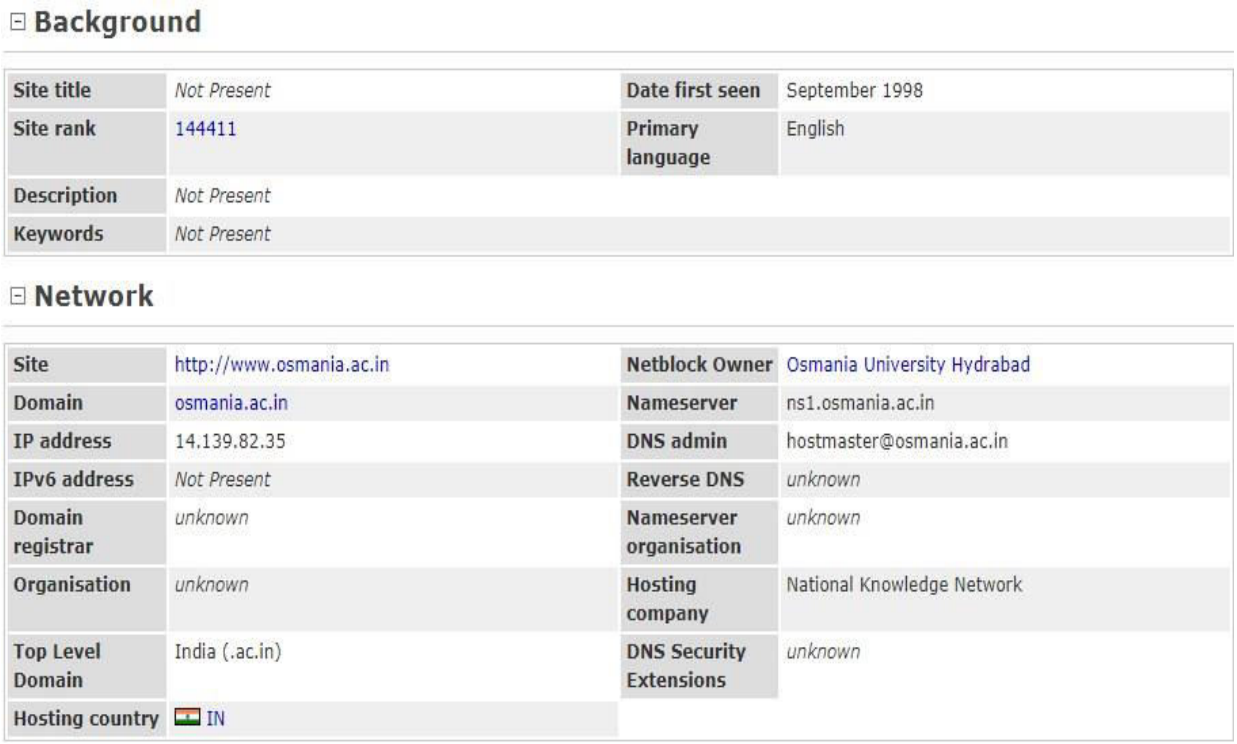
ns1.osmania.ac.in	A	14.139.82.38	86400s

Fig 2.3 DNS records of osmani.ac.in

Reverse IP domain check on osmania.ac.in

Fig 2.4 Reverse ip check

Netcraft on osmani.ac.in



Background

Site title	*Not Present*	**Date first seen**	September 1998
Site rank	144411	**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		

Network

Site	http://www.osmania.ac.in	**Netblock Owner**	Osmania University Hydrabad
Domain	osmania.ac.in	**Nameserver**	ns1.osmania.ac.in
IP address	14.139.82.35	**DNS admin**	hostmaster@osmania.ac.in
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	National Knowledge Network
Top Level Domain	India (.ac.in)	**DNS Security Extensions**	*unknown*
Hosting country	IN		

Fig 2.5 Netcraft on osmania.ac.in

Hosting history:

⊟ Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Osmania University Hydrabad	14.139.82.35	-	Apache/2.2.15 CentOS	4-Dec-2016
Osmania University Hydrabad	14.139.82.35	Linux	Apache/2.2.15 CentOS	4-Dec-2016
Osmania University Hydrabad	14.139.82.35	Linux	Apache/2.2.6 Unix mod_jk/1.2.20 mod_ssl/2.2.6 OpenSSL/0.9.8b DAV/2	17-Jun-2014
NIB National Internet Backbone Bharat Sanchar Nigam Limited 8th Floor,148-B,Statesman House, Barakhamba Road, descr New Delhi-110001	117.211.84.27	Linux	Apache/2.2.6 Unix mod_jk/1.2.20 mod_ssl/2.2.6 OpenSSL/0.9.8b DAV/2	29-Dec-2010
OSMANIA UNIV,HYD,AP O U CAMPUS HYDERABAD AP	210.212.217.67	Linux	Apache/2.2.6 Unix mod_jk/1.2.20 mod_ssl/2.2.6 OpenSSL/0.9.8b DAV/2	10-Nov-2010
Internet Service Provider TATA Communications formerly VSNL is Leading ISP, Data and Voice Carrier in India	115.118.6.3	Linux	Apache/2.2.6 Unix mod_jk/1.2.20 mod_ssl/2.2.6 OpenSSL/0.9.8b DAV/2	30-Jun-2010
osmania university registrar,administrative building osmania university, Hyderabad-7 Hyderabad-7	218.248.1.163	Linux	Apache/2.2.6 Unix mod_jk/1.2.20 mod_ssl/2.2.6 OpenSSL/0.9.8b DAV/2	16-Jun-2009
osmania university registrar,administrative building osmania university, Hyderabad-7 Hyderabad-7	218.248.1.163	Linux	unknown	22-Jul-2008
osmania university registrar,administrative building osmania university, Hyderabad-7 Hyderabad-7	218.248.1.163	Linux	Apache/2.2.6 Unix mod_jk/1.2.20 mod_ssl/2.2.6 OpenSSL/0.9.8b DAV/2	4-Jun-2008
osmania university registrar,administrative building osmania university, Hyderabad-7 Hyderabad-7	218.248.1.163	Solaris 9/10	Apache/2.2.6 Unix mod_jk/1.2.20 mod_ssl/2.2.6 OpenSSL/0.9.8b DAV/2	3-Sep-2007

Fig 2.6 Hosting history of osmnia.ac.in

Traceroute on osmania.ac.in

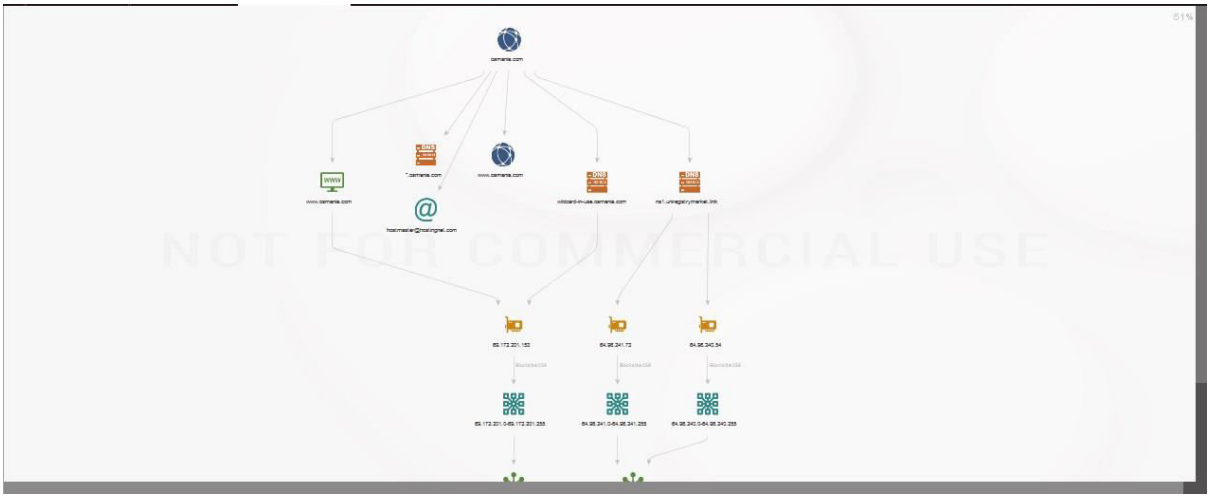
Traceroute Results for osmania.ac.in [14.139.82.35] Share

Hop	ICMP	UDP	TCP	IP	Hostname	Country	Time
▶ 1	0.91	*	0.62	10.10.0.1	NA	not found	Linux: 09:13:34
▶ 2	0.99	*	0.60	74.115.12.2	NA	US	Unix: 09:13:34
▶ 3	0.79	*	0.50	207.207.44.81	207-207-44-81.fwd.datafoundry.com.	US	Unix: 09:13:34
▶ 4	0.94	*	0.56	207.207.35.185	207-207-35-185.fwd.datafoundry.com.	US	Unix: 09:13:34
▶ 5	0.85	*	0.59	209.66.92.121	ae1.mpr1.aus3.us.above.net.	US	Linux: 09:13:35
▶ 6	1.48	*	1.17	64.125.31.24	ae3.mpr1.aus1.us.zip.zayo.com.	US	Linux: 09:13:35
▶ 7	7.52	*	6.29	64.125.27.29	ae1.cr1.dfw2.us.zip.zayo.com.	US	Linux: 09:13:35
▶ 8	7.52	*	7.12	64.125.20.66	ae11.er1.dfw2.us.zip.zayo.com.	US	Linux: 09:13:35
▶ 9	6.66	*	6.22	66.110.56.173	ix-ae-13-0.tcore1.DT8-Dallas.as6453.net.	US	Linux: 09:13:35
▶ 10	41.22	*	40.62	66.110.56.6	if-ae-2-2.tcore2.DT8-Dallas.as6453.net.	US	Linux: 09:13:35
▶ 11	43.61	*	40.95	66.110.57.21	if-ae-34-2.tcore1.LVW-Los-Angeles.as6453.net.	US	Linux: 09:13:35
▶ 12	238.70	*	235.64	66.110.59.114	NA	IN	Linux: 09:13:36

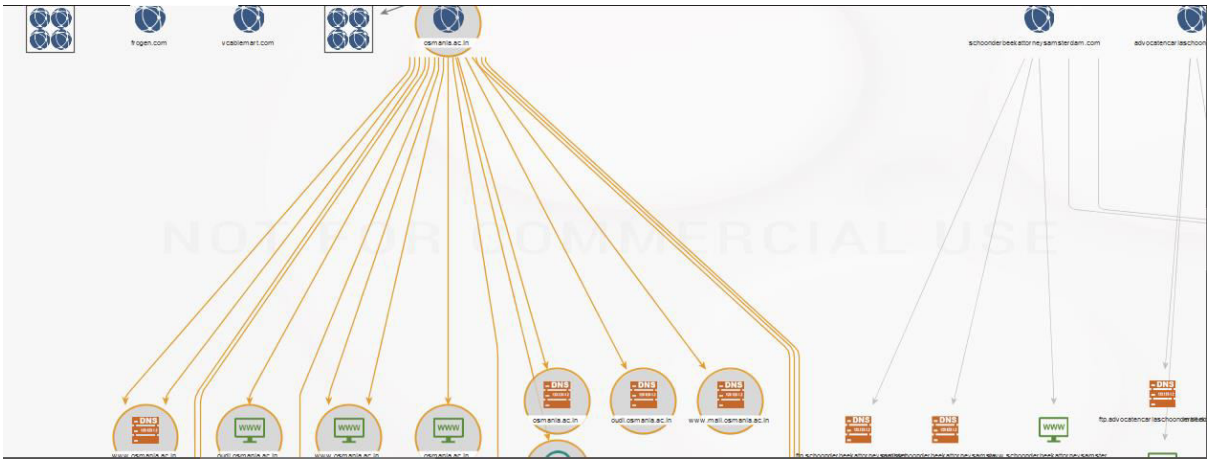
```
Tracing route to osmania.ac.in [14.139.82.35]
over a maximum of 30 hops:

  1    13 ms     1 ms    <1 ms  192.168.1.1
  2   182 ms     5 ms    53 ms  10.244.0.1
  3     2 ms     2 ms     2 ms  broadband.actcorp.in [202.83.20.205]
  4     2 ms     2 ms     2 ms  broadband.actcorp.in [202.83.26.1]
  5    10 ms     3 ms    14 ms  14.141.145.5.static-Bangalore.vsnl.net.in [14.14
1.145.5]
  6    42 ms    46 ms    28 ms  172.29.253.33
  7   162 ms    61 ms    43 ms  115.113.207.206.static-hyderabad.vsnl.net.in [11
5.113.207.206]
  8     *        *        *     Request timed out.
  9    35 ms    36 ms    26 ms  14.139.82.33
 10     *        *       22 ms  14.139.82.35
 11     *       28 ms    44 ms  14.139.82.35
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14    28 ms    30 ms    33 ms  14.139.82.35

Trace complete.

C:\Users\G Suresh>
```

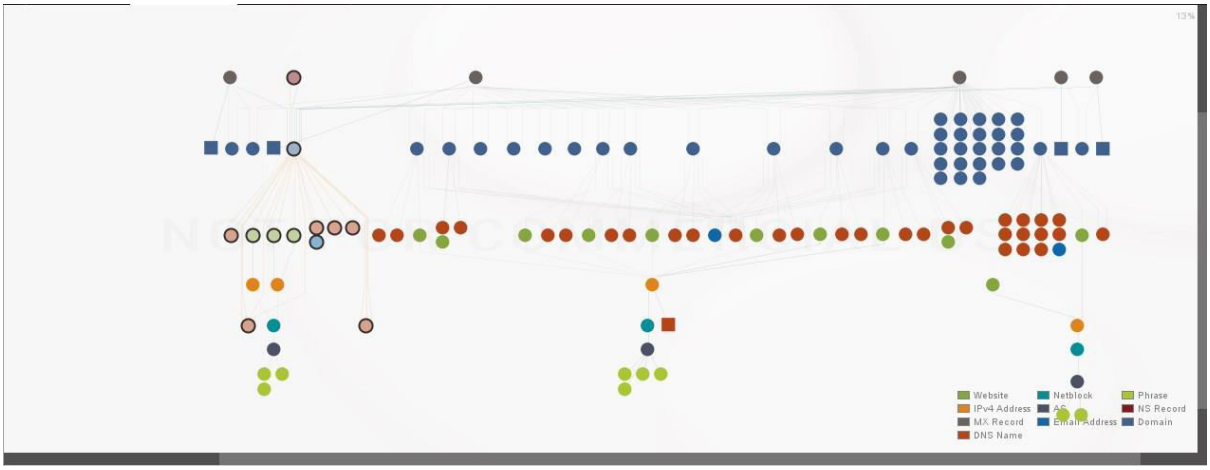
Fig 2.7 Traceroute on osmania.ac.in

Maltego footprint L1:

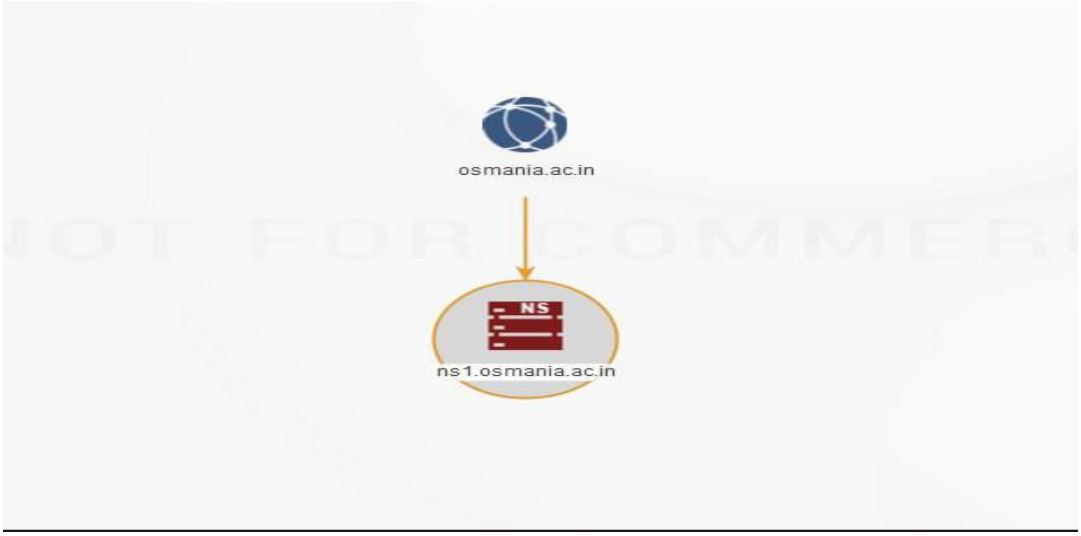


Maltego footprint L2:





Maltego XXL:



SUMMARY:

Domain Name: osmania.ac.in

IP address : 14.139.82.35

Server : Apache

Operating System : Linux

Some Emails: director_is@osmania.ac.in, venu@osmania.ac.in

Name Server : ns1.osmania.ac.in(14.139.82.38)

Hosting provider: Osmania University Hydrabad

Status : OK

Location of server: hyderabad, telangana

Reverse ip domain check: found 6 domains hosted on the same web server as osmania.ac.in

Day 3

Analysing Nmap slow comphrehensive scan of cbit.ac.in

```
Starting Nmap 7.50 ( https://nmap.org ) at 2017-07-10 16:25 India Standard Time
NSE: Loaded 275 scripts for scanning.          //Nmap Scripting Engine
NSE: Script Pre-scanning.
Initiating NSE at 16:25
NSE: [mrinfo] Nsock connect failed immediately
NSE: [mtrace] A source IP must be provided through fromip argument.
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey
argument
Completed NSE at 16:26, 13.72s elapsed
Initiating NSE at 16:26
Completed NSE at 16:26, 0.00s elapsed
Initiating NSE at 16:26
Completed NSE at 16:26, 0.00s elapsed
Pre-scan script results:
| lltd-discovery:
|   192.168.1.1
|     Hostname: Linksys11058
|     Mac: c8:b3:73:24:12:ed (Cisco-Linksys)
|_  Use the newtargets script-arg to add the results as targets
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Initiating Ping Scan at 16:26                                   //Ping
Scanning cbit.ac.in (202.65.141.231) [7 ports]
Completed Ping Scan at 16:26, 0.38s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:26
Completed Parallel DNS resolution of 1 host. at 16:26, 0.18s elapsed

Initiating SYN Stealth Scan at 16:26                            //Stealth Scan
Scanning cbit.ac.in (202.65.141.231) [1000 ports]
Discovered open port 25/tcp on 202.65.141.231
Discovered open port 3306/tcp on 202.65.141.231
Discovered open port 53/tcp on 202.65.141.231
Discovered open port 22/tcp on 202.65.141.231
Completed SYN Stealth Scan at 16:26, 1.96s elapsed (1000 total ports)

Initiating UDP Scan at 16:26                                    //UDP Scan
Scanning cbit.ac.in (202.65.141.231) [1000 ports]
Increasing send delay for 202.65.141.231 from 0 to 50 due to max_successful_tryno
increase to 5
Increasing send delay for 202.65.141.231 from 50 to 100 due to 11 out of 14 dropped
probes since last increase.
UDP Scan Timing: About 9.01% done; ETC: 16:31 (0:05:13 remaining)
Increasing send delay for 202.65.141.231 from 100 to 200 due to 11 out of 11 dropped
probes since last increase.
```

Increasing send delay for 202.65.141.231 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 202.65.141.231 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 12.90% done; ETC: 16:34 (0:06:52 remaining)
UDP Scan Timing: About 15.89% done; ETC: 16:35 (0:08:02 remaining)
Discovered open port 5353/udp on 202.65.141.231
UDP Scan Timing: About 18.89% done; ETC: 16:36 (0:08:40 remaining)
UDP Scan Timing: About 26.43% done; ETC: 16:38 (0:09:14 remaining)
Discovered open port 111/udp on 202.65.141.231
UDP Scan Timing: About 35.41% done; ETC: 16:39 (0:08:36 remaining)
UDP Scan Timing: About 43.14% done; ETC: 16:40 (0:07:56 remaining)
UDP Scan Timing: About 48.97% done; ETC: 16:40 (0:07:12 remaining)
UDP Scan Timing: About 54.94% done; ETC: 16:40 (0:06:30 remaining)
UDP Scan Timing: About 60.69% done; ETC: 16:40 (0:05:45 remaining)
UDP Scan Timing: About 66.21% done; ETC: 16:40 (0:04:59 remaining)
UDP Scan Timing: About 71.96% done; ETC: 16:41 (0:04:12 remaining)
UDP Scan Timing: About 77.36% done; ETC: 16:41 (0:03:26 remaining)
Discovered open port 53/udp on 202.65.141.231
UDP Scan Timing: About 82.70% done; ETC: 16:41 (0:02:37 remaining)
UDP Scan Timing: About 87.93% done; ETC: 16:41 (0:01:50 remaining)
Increasing send delay for 202.65.141.231 from 800 to 1000 due to max_successful_tryno increase to 6
UDP Scan Timing: About 93.33% done; ETC: 16:41 (0:01:02 remaining)
Warning: 202.65.141.231 giving up on port because retransmission cap hit (6).
Completed UDP Scan at 16:42, 987.28s elapsed (1000 total ports)

Initiating Service scan at 16:42 **//Service Scan**
Scanning 64 services on cbit.ac.in (202.65.141.231)
Service scan Timing: About 12.50% done; ETC: 16:55 (0:11:26 remaining)
Discovered open port 32768/udp on 202.65.141.231
Discovered open|filtered port 32768/udp on cbit.ac.in (202.65.141.231) is actually open
Service scan Timing: About 60.94% done; ETC: 16:48 (0:02:05 remaining)
Completed Service scan at 16:45, 195.14s elapsed (64 services on 1 host)

Initiating OS detection (try #1) against cbit.ac.in (202.65.141.231) **//OS detection**
Retrying OS detection (try #2) against cbit.ac.in (202.65.141.231)

Initiating Traceroute at 16:46 **//Traceroute**
Completed Traceroute at 16:46, 3.03s elapsed

Initiating Parallel DNS resolution of 4 hosts. at 16:46 **//Parallel DNS resolution**
Completed Parallel DNS resolution of 4 hosts. at 16:46, 11.05s elapsed

NSE: Script scanning 202.65.141.231
Initiating NSE at 16:46

```
NSE: [ip-geolocation-maxmind] You must specify a Maxmind database file with the
maxmind_db argument.
NSE: [ip-geolocation-maxmind] Download the database from
http://dev.maxmind.com/geoip/legacy/geolite/
Completed NSE at 16:46, 32.83s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 3.21s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 0.03s elapsed
Nmap scan report for cbit.ac.in (202.65.141.231)
Host is up (0.022s latency).
rDNS record for 202.65.141.231: www.cbit.ac.in
Not shown: 1915 closed ports, 56 open|filtered ports    //port description

PORT     STATE    SERVICE       VERSION

22/tcp    open     ssh           OpenSSH 4.7 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_4.7
| ssh-hostkey:
|   1024 ba:f2:c2:f8:9c:33:9f:5c:ac:9a:80:41:74:ee:10:b7 (DSA)     //ssh public keys
|_  2048 94:78:6c:bd:34:d6:31:6e:4d:a2:cc:99:19:97:54:ea (RSA)
| ssh2-enum-algos:
|   kex_algorithms: (4)                                            //Alogorithms employed
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|       ssh-rsa
|       ssh-dss
|   encryption_algorithms: (13)
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       arcfour128
|       arcfour256
|       arcfour
|       aes192-cbc
|       aes256-cbc
|       rijndael-cbc@lysator.liu.se
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|   mac_algorithms: (7)
|       hmac-md5
|       hmac-sha1
```

```
|       umac-64@openssh.com
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
25/tcp    open     smtp?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest,
HTTPOptions, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString,
NCP, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq,
TLSSessionReq, TerminalServer, WMSRequest, X11Probe, afp, giop, oracle-tns:
|_    500 Syntax error, command unrecognized
|_smtp-commands: Couldn't establish connection on port 25
53/tcp    open     domain        ISC BIND 9.5.0a6
79/tcp    filtered finger
80/tcp    filtered http
111/tcp   filtered rpcbind
113/tcp   filtered ident
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   filtered https
445/tcp   filtered microsoft-ds
512/tcp   filtered exec
513/tcp   filtered login
514/tcp   filtered shell
515/tcp   filtered printer
1025/tcp  filtered NFS-or-IIS
1026/tcp  filtered LSA-or-nterm
1063/tcp  filtered kyoceranetdev
1080/tcp  filtered socks
1434/tcp  filtered ms-sql-m
3128/tcp  filtered squid-http
3306/tcp  open     mysql         MySQL 5.0.45
| banner: 4\x00\x00\x00\x0A5.0.45\x00\x17\xBD\x06\x00kVNc'5sf\x00,\xA2\x0
|_8\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00(/S5NjM...

| mysql-info:                          //MySQL database info
|   Protocol: 10
|   Version: 5.0.45
|   Thread ID: 441624
|   Capabilities flags: 41516
|   Some Capabilities: ConnectWithDatabase, SupportsCompression, Support41Auth,
Speaks41ProtocolNew, SupportsTransactions, LongColumnFlag
|   Status: Autocommit
```

```
|_  Salt: 75C2oZW#I%{`L;$B]1y3
4662/tcp  filtered edonkey
6123/tcp  filtered backup-express
6129/tcp  filtered unknown
53/udp    open     domain        ISC BIND 9.5.0a6
| dns-nsid:
|_  bind.version: 9.5.0a6
|_dns-recursion: Recursion appears to be enabled
111/udp   open     rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/0  rpcbind
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100024  1         32768/udp  status
|_  100024  1         44875/tcp  status
5353/udp  open     mdns          DNS-based service discovery
| dns-service-discovery:
|   9/tcp workstation
|     Address=202.65.141.231 fe80:0:0:0:20f:feff:fe10:ecbc
|   22/tcp ssh
|_    Address=202.65.141.231 fe80:0:0:0:20f:feff:fe10:ecbc
32768/udp open     status        1 (RPC #100024)


Device type: general purpose|firewall|proxy server|PBX|WAP|broadband router|remote
management
//OS guessing
Running (JUST GUESSING): Linux 2.6.X (95%), Cisco embedded (94%), Riverbed embedded
(94%), Ruckus embedded (93%), Zhone embedded (91%), AVM embedded (91%), Dell
embedded (91%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.9 cpe:/o:linux:linux_kernel:2.6 cpe:/h:cisco:sa520
cpe:/h:riverbed:steelhead_200 cpe:/h:cisco:uc320w cpe:/h:ruckus:7363
cpe:/h:avm:fritz%21box_fon_wlan_7170 cpe:/h:dell:remote_access_card:5
Aggressive OS guesses: Linux 2.6.9 (95%), Linux 2.6.18 (95%), Linux 2.6.9 - 2.6.27 (95%),
Linux 2.6.32 (94%), Cisco SA520 firewall (Linux 2.6) (94%), Riverbed Steelhead 200 proxy
server (94%), Cisco UC320W PBX (Linux 2.6) (93%), Ruckus 7363 WAP (93%), Linux 2.6.9
(CentOS 4.4) (92%), Linux 2.6.28 (92%
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 31.589 days (since Fri Jun 09 02:38:00 2017)
Network Distance: 12 hops

Host script results:
| asn-query:                    //info about IP's AS Number
| BGP: 202.65.141.0/24 | Country: IN
|   Origin AS: 18229 - CTRLS-AS-IN CtrlS Datacenters Ltd., IN
|_    Peer AS: 4755 9498
```

```
| fcrdns:                          //Forward confirmed reverse DNS
|   www.cbit.ac.in:
|     status: pass
|     addresses:
|_      202.65.141.231
|_firewalk: ERROR: Script execution failed (use -d to debug)
|_hostmap-robtex: ERROR: Script execution failed (use -d to debug)
| ip-geolocation-geoplugin:
|_202.65.141.231 (cbit.ac.in)
|_ipidseq: ERROR: Script execution failed (use -d to debug)
|_path-mtu: ERROR: Script execution failed (use -d to debug)
|_qscan: ERROR: Script execution failed (use -d to debug)
| resolveall:
|   Host 'cbit.ac.in' also resolves to:
|_  Use the 'newtargets' script-arg to add the results as targets

| traceroute-geolocation:              //Traceroute
|   HOP  RTT    ADDRESS                    GEOLOCATION
|   1    2.00   192.168.1.1                 - ,-
|   2    3.00   10.244.0.1                 - ,-
|   3    ...
|   4    3.00   broadband.actcorp.in (202.83.26.1)  20.000,77.000 India ()
|   5    ...
|   6    ...
|   7    ...
|   8    ...
|   9    ...
|   10   ...
|   11   ...
|_  12   14.00  www.cbit.ac.in (202.65.141.231)     17.375,78.474 India (Andhra Pradesh)


| whois-domain:                        //WHOis Information
|
| Domain name record found at whois.inregistry.net
| Access to .IN WHOIS information is provided to assist persons in determining the contents
of a domain name registration record in the .IN registry database. The data in this record is
provided by .IN Registry for informational purposes only, and .IN does not guarantee its
accuracy.  This service is intended only for query-based access. You agree that you will use
this data only for lawful purposes and that, under no circumstances will you use this data to:
(a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of
mass unsolicited, commercial advertising or solicitations to entities other than the data
recipient's own existing customers; or (b) enable high volume, automated, electronic
processes that send queries or data to the systems of Registry Operator, a Registrar, or
Afilias except as reasonably necessary to register domain names or modify existing
registrations. All rights reserved. .IN reserves the right to modify these terms at any time. By
submitting this query, you agree to abide by this policy.
```

|
| Domain ID:D14106-AFIN\x0D
| Domain Name:CBIT.AC.IN\x0D
| Created On:30-Apr-2003 04:00:00 UTC\x0D
| Last Updated On:27-Apr-2016 10:59:36 UTC\x0D
| Expiration Date:30-Apr-2019 04:00:00 UTC\x0D
| Sponsoring Registrar:ERNET India (R9-AFIN)\x0D
| Status:OK\x0D
| Reason:\x0D
| Registrant ID:R-R03031106782\x0D
| Registrant Name:Chaitanya Bharathi Institute of Technology\x0D
| Registrant Organization:\x0D
| Registrant Street1:Chaitanya Bharathi Institute of Technology\x0D
| Registrant Street2:\x0D
| Registrant Street3:\x0D
| Registrant City:Gandipet, Hyderabad, 50009\x0D
| Registrant State/Province:Andhra Pradesh\x0D
| Registrant Postal Code:\x0D
| Registrant Country:AQ\x0D
| Registrant Phone:\x0D
| Registrant Phone Ext.:\x0D
| Registrant FAX:\x0D
| Registrant FAX Ext.:\x0D
| Registrant Email:missing-address@example.info\x0D
| Admin ID:A-R03031106782\x0D
| Admin Name:Dr. B.Chennakesava Rao\x0D
| Admin Organization:\x0D
| Admin Street1:Chaitanya Bharathi Institute of Technology\x0D
| Admin Street2:\x0D
| Admin Street3:\x0D
| Admin City:Gandipet, Hyderabad,\x0D
| Admin State/Province:\x0D
| Admin Postal Code:500075\x0D
| Admin Country:IN\x0D
| Admin Phone:+91.9866141821\x0D
| Admin Phone Ext.:\x0D
| Admin FAX:\x0D
| Admin FAX Ext.:\x0D
| Admin Email:raobck@rediffmail.com\x0D
| Tech ID:T-R03031106782\x0D
| Tech Name:E.Sanjeeva Reddy\x0D
| Tech Organization:\x0D
| Tech Street1:Chaitanya Bharathi Institute of Technology\x0D
| Tech Street2:\x0D
| Tech Street3:\x0D
| Tech City:.Gandipet, Hyderabad,\x0D
| Tech State/Province:\x0D

```
| Tech Postal Code:500075\x0D
| Tech Country:IN\x0D
| Tech Phone:+91.9666002348\x0D
| Tech Phone Ext.:\x0D
| Tech FAX:\x0D
| Tech FAX Ext.:\x0D
| Tech Email:sreddye@gmail.com\x0D
| Name Server:NS1.CBIT.AC.IN\x0D
| Name Server:NS2.CBIT.AC.IN\x0D

TRACEROUTE (using port 3389/tcp)
HOP RTT      ADDRESS
1   2.00 ms  192.168.1.1
2   3.00 ms  10.244.0.1
3   ...
4   3.00 ms  broadband.actcorp.in (202.83.26.1)
5   ... 11
12  14.00 ms www.cbit.ac.in (202.65.141.231)


NSE: Script Post-scanning.
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1268.50 seconds
          Raw packets sent: 2749 (98.838KB) | Rcvd: 206539 (27.040MB)
```

Day 4

We learnt about Nessus which is an automated vulnerability scanner. Using Nessus, scanned cbit.ac.in

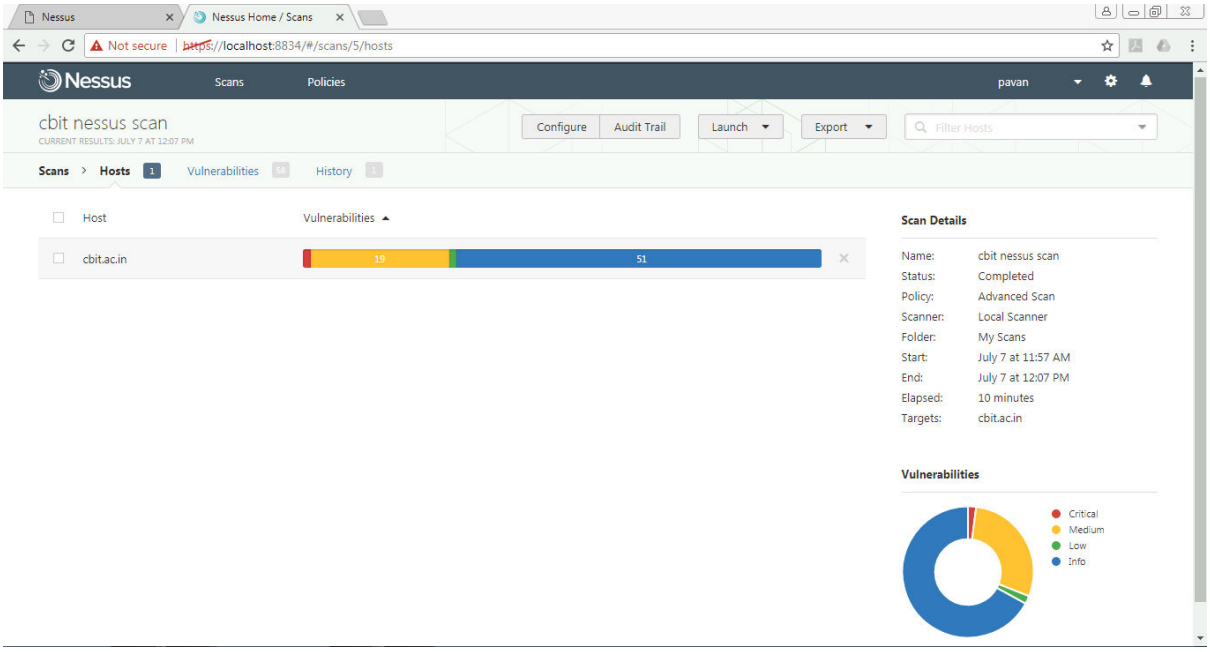


Fig 4.1 Nessus scan on cbit.ac.in

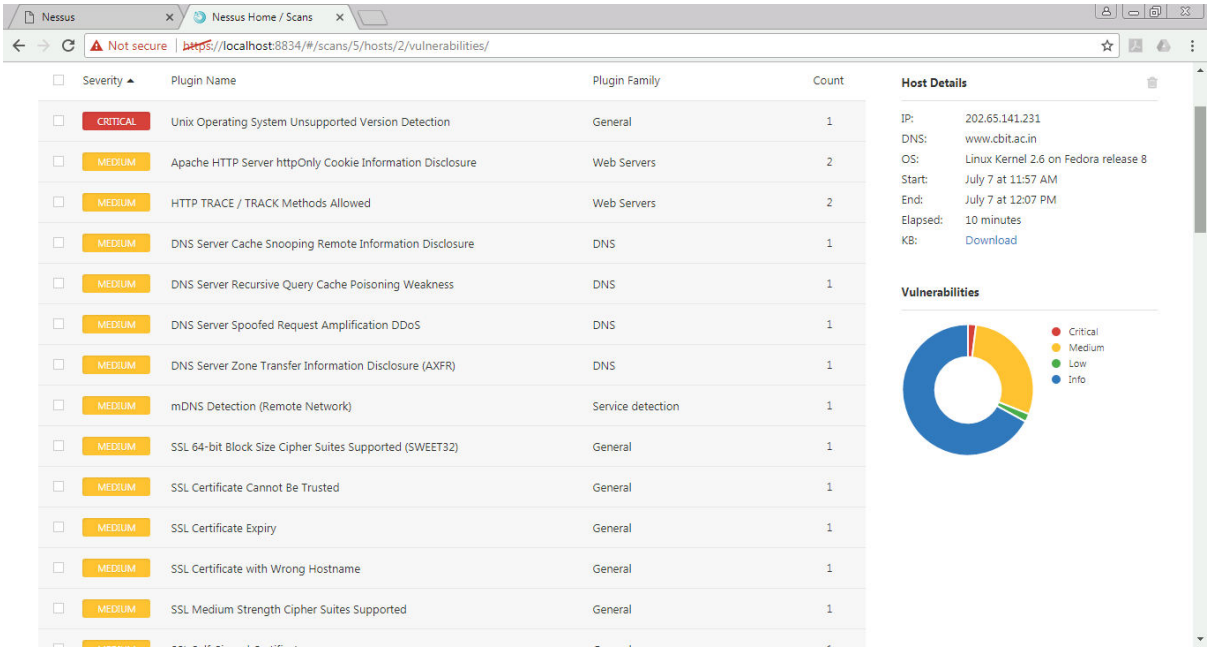


Fig 4.2 Vulnerabilities shown by Nessus

Directory Traversal:

This allows attackers to access restricted directories, configuration and critical system files that execute commands outside of root servers directories. In this atackers use

../sequence to navigate between directories and gain knowledge of the application and its construction, lpcate source code, discover user ids and passwords hidden inside files.

Patch for directory Traversal:

Linux: configure .htaccess file

IIS: configure ACLs

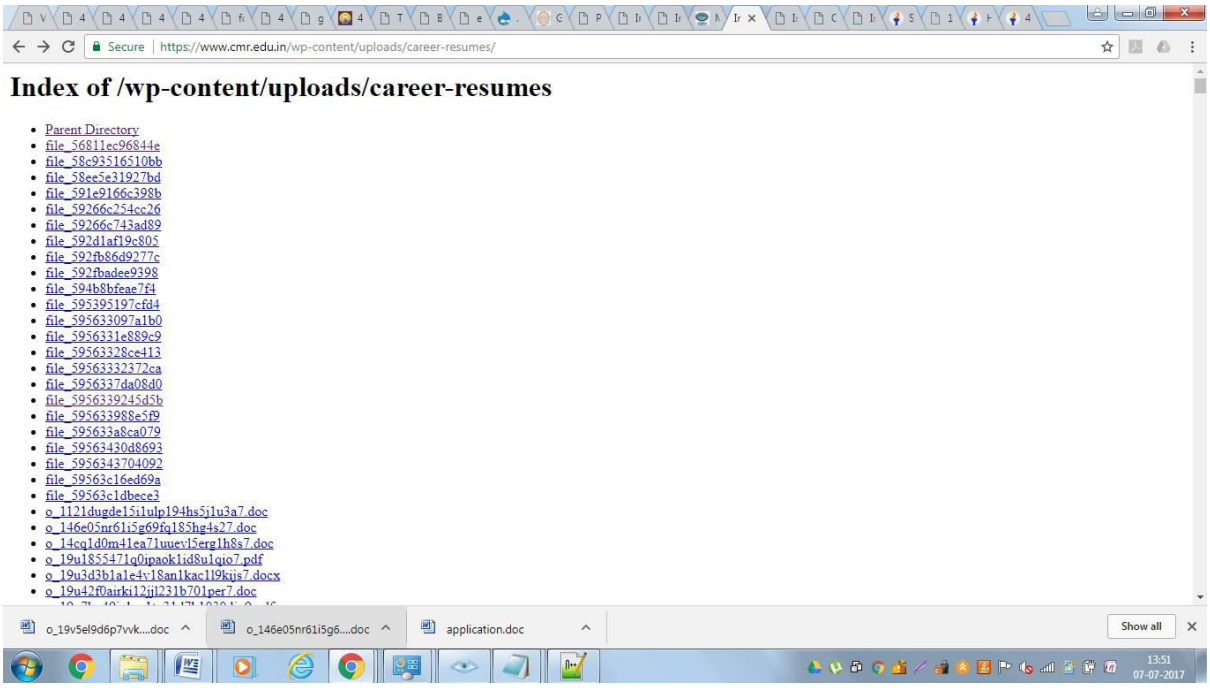


Fig 4.3 Directory traversal revealing career resumes

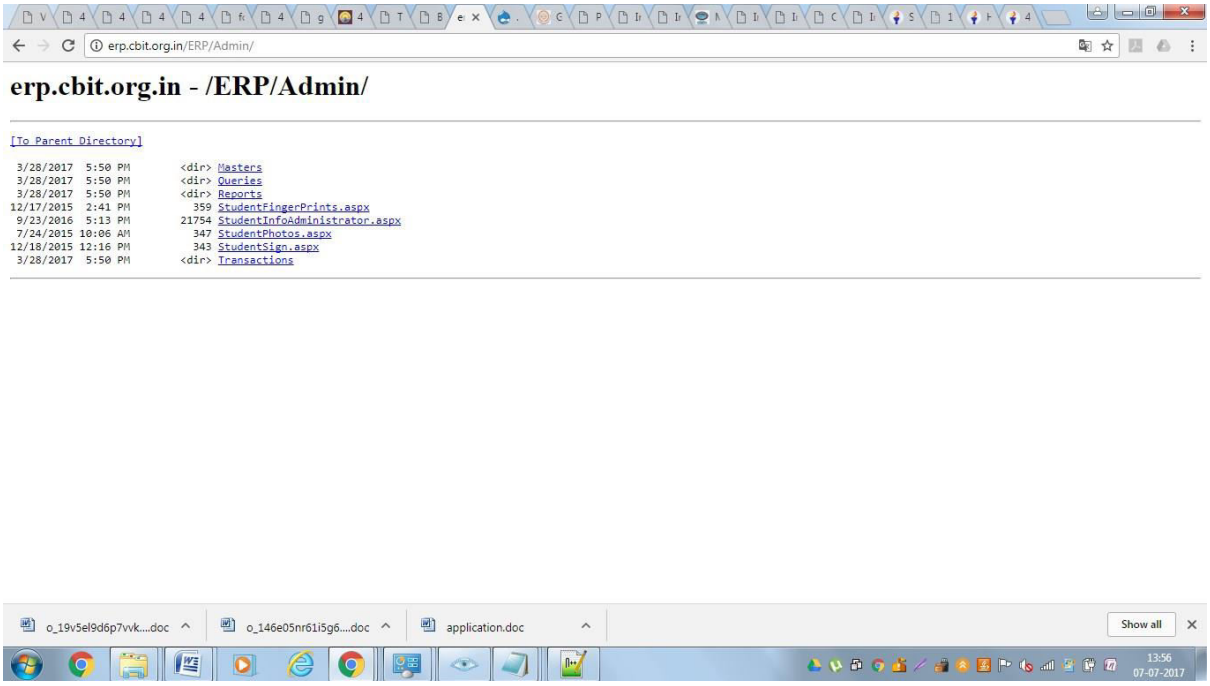


Fig 4.4 Directory traversal of cbit.ac.in

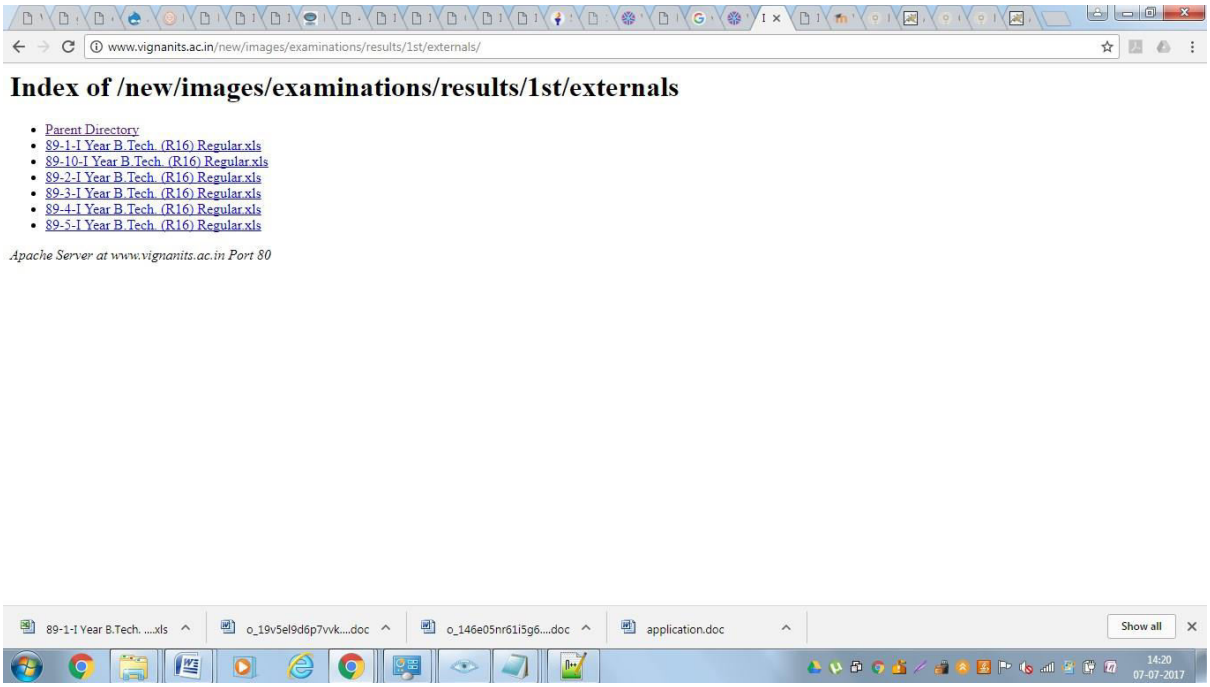


Fig 4.5 Directory traversal revealing external results

Some directory traversal links:
https://www.cmr.edu.in/wp-content/uploads/career-resumes/
http://erp.cbit.org.in/ERP/Admin/
http://www.vignanits.ac.in/new/images/examinations/results/1st/externals/
http://www.osmania.ac.in/images/
http://www.griet.ac.in/images1/

Day 5

This day we learnt about SQL injection.

SQL injection is a technique usd to take advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a backend database. It is a basic attack usede to gain unauthorized access or to retrieve information directly from the website

Blind SQL: The attacker can steal the data by asking a series of true or false questions through SQL staatements.

Union based: This is used when the user uses the union commandthe attacker checks for the vulnerability by adding a single quote at the end of the url(php?id=).

Error based : The attacker makes use of database level error messages disclosed by an application.

Tools: Havij,SQL Map,SQL inject me.

Fig 5.1 tdap.gov.pk site

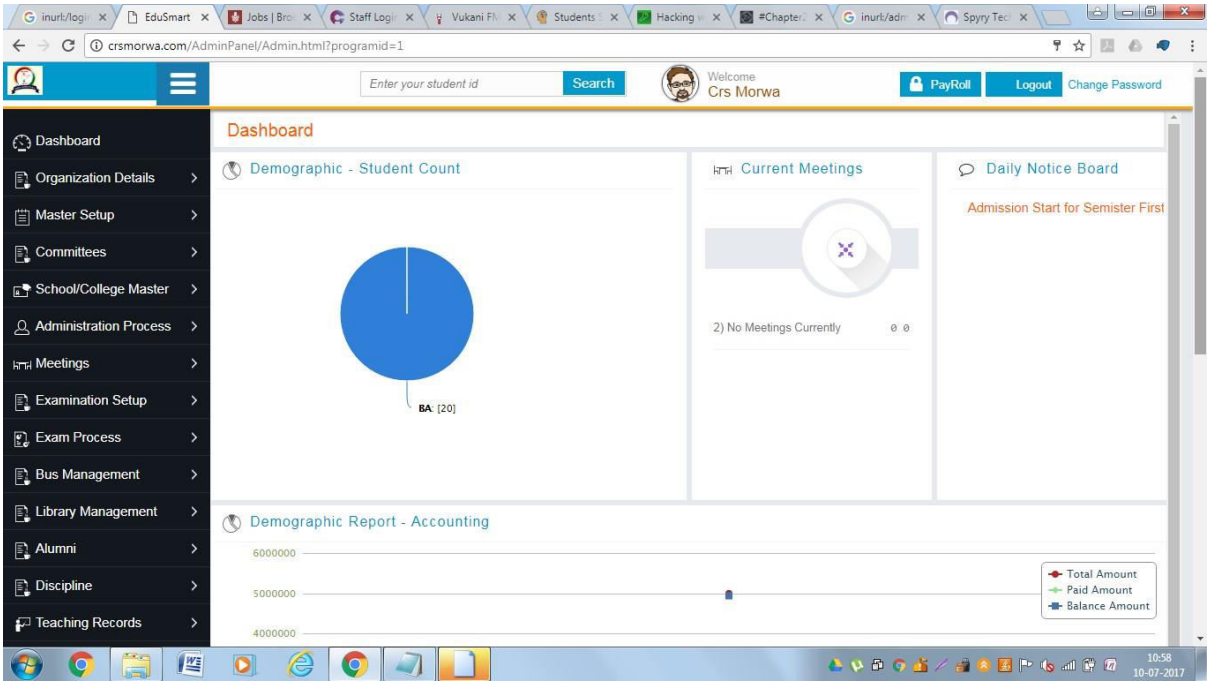


Fig 5.2 crsmorwa admin login

Some websites which are accessible using SQL injection:

http://www.i2t2.com/admin/login.php password ' or '1'='1
http://www.globalengineeringcollege.com/login.html password ' or 0=0 --
http://haflonggovtcollege.org/login.html password admin
http://www.tdap.gov.pk/texpo/mission-admin/login.php password ' or '1'='1
http://crsmorwa.com/AdminPanel/login.html password ' or '1'='1
http://www.sandemanseeds.com/info.asp password ' or '1'='1

Security Patch:
Enable input validation and accept only expected values

Day 6

Acunetix is an automated vulnerability scanner which shows us all the vulnerabilities in the website.

Acunetix report on cbit

Server information	
Responsive	True
Server banner	Apache/2.2.6 (Fedora)
Server OS	Unix
Server technologies	PHP

Threat level

acunetix threat level
Level 3: High

Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	912
High	3
Medium	162
Low	35
Informational	712

Alerts summary:

Alerts summary

CVS web repository

Affects	Variation
/sites/oldelectret.cbit.ac.in/modules/feedback	1
/sites/oldelectret.cbit.ac.in/modules/feedback/po	1

Slow HTTP Denial of Service Attack

Affects	Variation
Web Server	1

Apache 2.x version older than 2.2.8

Affects	Variation
Web Server	1

Apache 2.x version older than 2.2.9

Affects	Variation
Web Server	1

Acunetix Website Audit 2

Apache httpd remote denial of service

Affects	Variation
Web Server	1

Apache httpOnly cookie disclosure

Affects	Variation
Web Server	1

High level Alerts:

CVS web repository — Severity HIGH

Vulnerability description

CVS Web Repository found on this webpage. The CVS directory is a special directory. CVS/Entries lists files and subdirectories registered into the server. CVS/Repository contains the path to the corresponding directory in the repository. CVS/Root contains the path to the repository.

Affected items

- /sites/oldelectret.cbit.ac.in/modules/feedback
- /sites/oldelectret.cbit.ac.in/modules/feedback/po

The impact of this vulnerability

These files may expose sensitive information that may help an malicious user to prepare more advanced attacks.

How to fix this vulnerability

Remove the file from production systems.

Web references

- Ximbiot - CVS Wiki

Slow HTTP Denial of Service Attack — Severity HIGH

Vulnerability description

Your web server is vulnerable to Slow HTTP DoS (Denial of Service) attacks.

Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service.

Affected items

- Web Server

The impact of this vulnerability

A single machine can take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.

How to fix this vulnerability

Consult Web references for information about protecting your web server against this type of attack.

Web references

- Slowloris HTTP DoS

Medium level alerts:

Apache 2.x version older than 2.2.8

Apache 2.x version older than 2.2.8

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (Version_Check.script)

Description

This alert was generated using only banner information. It may be a false positive.
Fixed in Apache httpd 2.2.8:

- low: mod_proxy_ftp UTF-7 XSS CVE-2008-0005
A workaround was added in the mod_proxy_ftp module. On sites where mod_proxy_ftp is enabled and a forward proxy is configured, a cross-site scripting attack is possible against Web browsers which do not correctly derive the response character set following the rules in RFC 2616.
- low: mod_proxy_balancer DoS CVE-2007-6422
A flaw was found in the mod_proxy_balancer module. On sites where mod_proxy_balancer is enabled, an authorized user could send a carefully crafted request that would cause the Apache child process handling that request to crash. This could lead to a denial of service if using a threaded Multi-Processing Module.
- low: mod_proxy_balancer XSS CVE-2007-6421
A flaw was found in the mod_proxy_balancer module. On sites where mod_proxy_balancer is enabled, a cross-site scripting attack against an authorized user is possible.
- moderate: mod_status XSS CVE-2007-6388
A flaw was found in the mod_status module. On sites where mod_status is enabled and the status pages were publicly accessible, a cross-site scripting attack is possible. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.
- moderate: mod_imagemap XSS CVE-2007-5000
A flaw was found in the mod_imagemap module. On sites where mod_imagemap is enabled and an imagemap file is publicly available, a cross-site scripting attack is possible.

Affected Apache versions (up to 2.2.6).

Impact

Check references for details about every vulnerability.

Recommendation

Upgrade Apache 2.x to the latest version.

References

Apache homepage
Apache httpd 2.2 vulnerabilities

Apache httpd remote dos

Apache httpd remote denial of service MEDIUM

Vulnerability description

A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server:

http://seclists.org/fulldisclosure/2011/Aug/175

An attack tool is circulating in the wild. Active use of this tools has been observed. The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server.

This alert was generated using only banner information. It may be a false positive.

Affected Apache versions (1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19).

Affected items

- Web Server

The impact of this vulnerability

Remote Denial of Service

Directory listing: Enables usere to access important infomation about the website.

- /files/color
- /files/color/garland-9f2cb905

- /files/u85
- /files/u85/support
- /files/u85/support/openconf.php_files
- /files/u85/support/photos
- /includes
- /misc
- /misc/farbtastic
- /modules/book
- /modules/cck
- /modules/cck/email
- /modules/cck/imagefield
- /modules/cck/po
- /modules/cck/theme
- /modules/img_assist
- /modules/img_assist/drupalimage
- /modules/img_assist/drupalimage/images
- /modules/img_assist/drupalimage/langs
- /modules/img_assist/po
- /modules/nice_menus
- /modules/node
- /modules/og
- /modules/og/po
- /modules/og/tests
- /modules/system
- /modules/user
- /modules/views_bonus
- /profiles

Fix: You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.

Html sites with no CSRF protection:

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Affected items:

- /
- /files/html/feedback.html
- /files/u85/support/paper.html
- /files/u85/support/submit.php.htm.bak
- /modules/fckeditor/fckeditor/_samples/html/sample02.html
- /modules/fckeditor/fckeditor/_samples/html/sample09.html
- /modules/fckeditor/fckeditor/_samples/html/sample10.html
- /modules/fckeditor/fckeditor/editor/dialog/fck_link.html
- /modules/fckeditor/fckeditor/editor/dialog/fck_spellerpages/spellerpages/controls.html
- /modules/fckeditor/fckeditor/editor/filemanager/browser/default/connectors/test.html
- /modules/fckeditor/fckeditor/editor/filemanager/browser/default/frmupload.html
- /modules/fckeditor/fckeditor/editor/filemanager/upload/test.html

Fix: Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Source code disclosure:

Affected items:

- /includes/bootstrap.inc
- /includes/cache.inc
- /includes/common.inc
- /includes/database.inc
- /includes/database.mysql.inc
- /includes/database.mysqli.inc
- /includes/database.pgsql.inc
- /includes/file.inc
- /includes/form.inc
- /includes/image.inc
- /includes/install.inc
- /includes/install.mysql.inc
- /includes/install.mysqli.inc
- /includes/install.pgsql.inc
- /includes/locale.inc
- /includes/menu.inc
- /includes/module.inc
- /includes/pager.inc
- /includes/path.inc
- /includes/session.inc
- /includes/tablesort.inc
- /includes/theme.inc
- /includes/unicode.inc
- /includes/xmlrpc.inc
- /includes/xmlrpcs.inc
- /modules/book/book.install
- /modules/book/book.module
- /modules/cck/content.install
- /modules/cck/content.module
- /modules/cck/content_admin.inc
- /modules/cck/content_copy.module
- /modules/cck/content_crud.inc
- /modules/cck/content_pathauto.inc
- /modules/cck/content_views.inc
- /modules/cck/email/email.module
- /modules/cck/fieldgroup.install
- /modules/cck/fieldgroup.module
- /modules/cck/imagefield/imagefield.install
- /modules/cck/imagefield/imagefield.module
- /modules/cck/nodereference.install
- /modules/cck/nodereference.module
- /modules/cck/number.install
- /modules/cck/number.module
- /modules/cck/optionwidgets.install
- /modules/cck/optionwidgets.module
- /modules/cck/text.install
- /modules/cck/text.module
- /modules/cck/userreference.install
- /modules/cck/userreference.module
- /modules/img_assist/img_assist.install
- /modules/img_assist/img_assist.module
- /modules/nice_menus/nice_menus.module
- /modules/node/content_types.inc

- /modules/node/node.module
- /modules/og/og.install
- /modules/og/og.module
- /modules/og/og_views.inc
- /modules/og/og_xmlrpc.inc
- /modules/og/tests/og_post.test
- /modules/og/tests/og_subscribe.test
- /modules/system/system.install
- /modules/system/system.module
- /modules/user/user.module
- /modules/views_bonus/views_bonus.module
- /profiles/default/default.profile
- /scripts/code-style.pl
- /sites/oldelectret.cbit.ac.in/modules/feedback/feedback.install
- /sites/oldelectret.cbit.ac.in/modules/feedback/feedback.module
- /themes/chameleon/chameleon.theme
- /themes/engines/phptemplate/phptemplate.engine
- /themes/garland/color/color.inc
- /themes/garland/minnelli/color/color.inc

User Credentials sent in clear text:

User credentials are sent in clear text Severity MEDIUM

Vulnerability description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Affected items

- /
- /files/u85/support/submit.php.htm.bak
- /phpMyAdmin

The impact of this vulnerability

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

How to fix this vulnerability

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Low level threats:

1. Apache 2.x version older than 2.2.10

   Affected item: Web Server.

   How to fix this vulnerability: Upgrade Apache 2.x to the latest version.

2. Clickjacking: X-Frame-Options header

   Affected item: Web Server

   How to fix this vulnerability: Configure your web server to include an X-Frame-Options header.

3. Documentation Files:

   Affected items:
   - /CHANGELOG.txt
   - /INSTALL.txt
   - /modules/cck/CHANGELOG.txt
   - /modules/cck/README.txt
   - /modules/img_assist/CHANGELOG.txt
   - /modules/img_assist/INSTALL.txt
   - /modules/img_assist/README.txt
   - /modules/nice_menus/README.txt
   - /modules/og/readme.txt

   How to fix: Remove or restrict all documentation files accessible from internet.

4. File Upload: This page allows visitors to upload files to the server
   Affected items:
   - /modules/fckeditor/fckeditor/editor/dialog/fck_link.html
   - /modules/fckeditor/fckeditor/editor/filemanager/browser/default/connectors/test.html
   - /modules/fckeditor/fckeditor/editor/filemanager/browser/default/frmupload.html
   - /modules/fckeditor/fckeditor/editor/filemanager/upload/test.html
   - /openconf/author/submit.php

   How to fix: Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.

5. Possible sensitive directories:
   Affected items:
   - /backup
   - /modules/fckeditor
   - /modules/statistics
   - /modules/system
   - /modules/upload
   - /phpMyAdmin

   How to fix: Restrict access to the directory or remove from website.

6. Possible sensitive files:
   Affected Item: /files/php.ini
   How to fix: access to the directory or remove from website.

7. Session Cookie without HttpOnly flag set
   Affected item: /
   Fix: if posible you should set the HttpOnly flag for this cookie.

8. Session cookie without Secure Flage Set:
   Affected Items: /
   Fix: if posible you should set the Secure flag for this cookie.

9. Session Token In URL:
   Affected Item:

- /phpMyAdmin/index.php (740e31e476ea2e5b6da26197c94850a1)
- /phpMyAdmin/phpmyadmin.css.php (ec82dfddac6a1bd43a026e14ad249898)

   Fix: The Session Should be maintained using cookies(or hidden input fields)

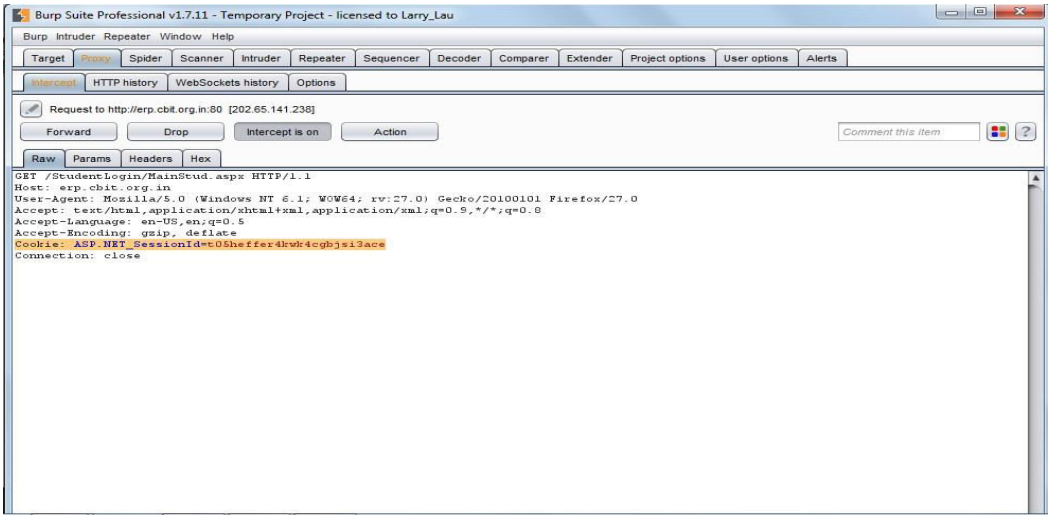
10. Trace Method is enabled:
    Affected Item: Web Server
    Fix: Disable Trace method on web server.

Day 7

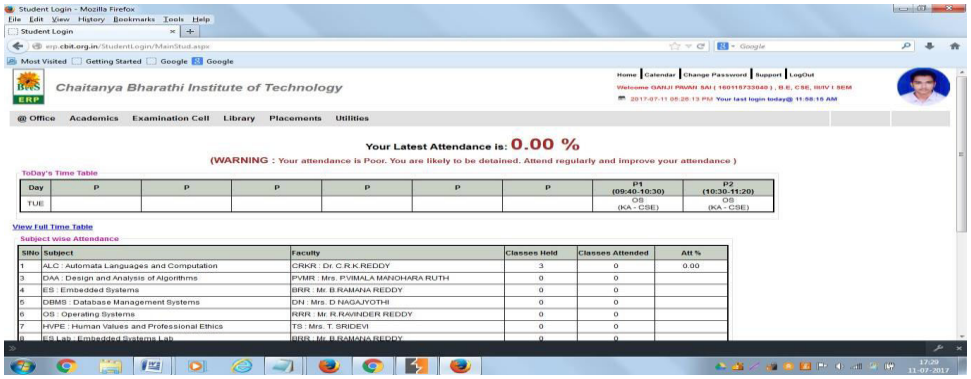
Used Burpsuite to replace cookie to login.

Copy the session id and url

Opened the same url in firefox and replace the session id of firefox with chromes



And you are session hijacking



To continue to browse the links in the page without getting logged out replace everytime the session id in firefox with chrome's.

Day 8

Learnt about Cross Site scripting

Cross Site scripting is a code injection attack that allows an attacker to execute malicious script in user's browser. Here the attacker cannot directly target hids victim. Instead he exploits a vulnerability in a website that the victim visits, in order to get the website to deliver the malicious script to him.

Types of XSS

1. Stored: This involves an attacker injecting a script that is permanentlt stored in target application for instance a database. When the victim navigates to affected webpage in the browser, the XSS payload will be served as a part of webpage.This means the victims will inadvertently end up executing the malicious scriptonce the page is viewed in browser.

2. Reflected: In reflected XSS the payload has to be a part of the request which is sent to the webserver and reflected back in such a way that the https response includes payload from http request. Using phishing email and other social engineering techniques the attacker tricks the victim to inadvertently make a request to the server which cont8.1 ains the XSS payload and ends up ends up executing the script that get reflected and executed inside the browser.
3. DOM based: The data is read from the DOM by the webapplication and outputted to the browser. If the data is incorrectly handled, an attacker can inject a payload which will be stored as a part of the DOM and executed when the data is read back from the DOM.

Stored:

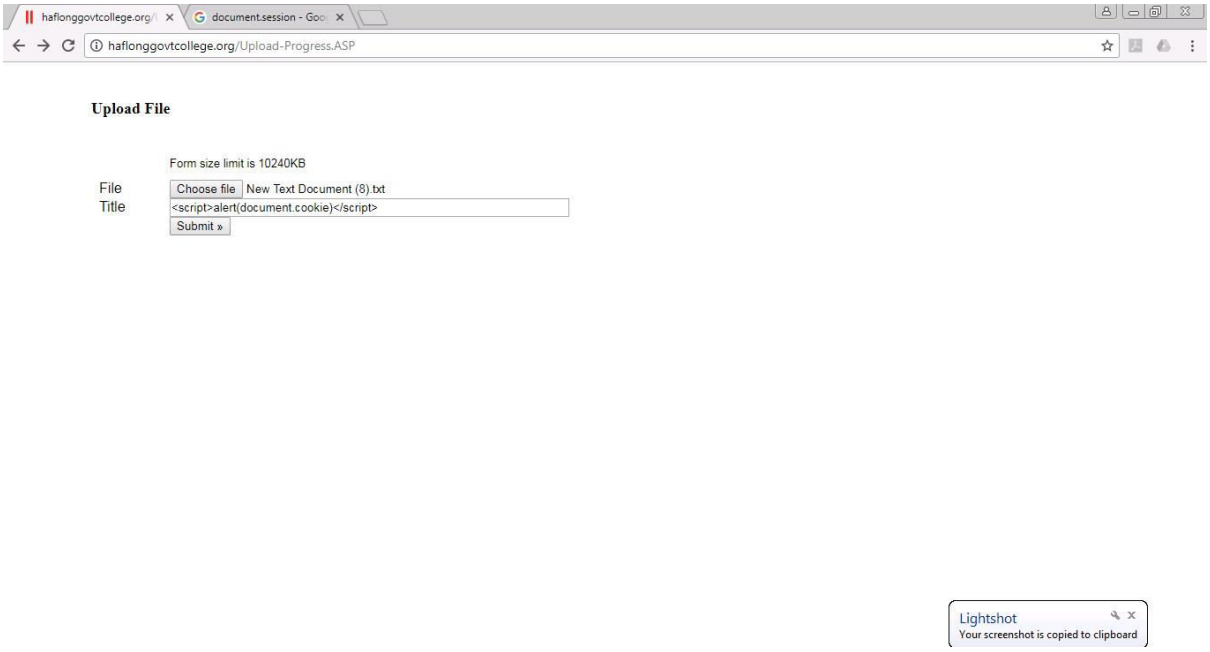


Fig 8.1 Giving a script in title for calender

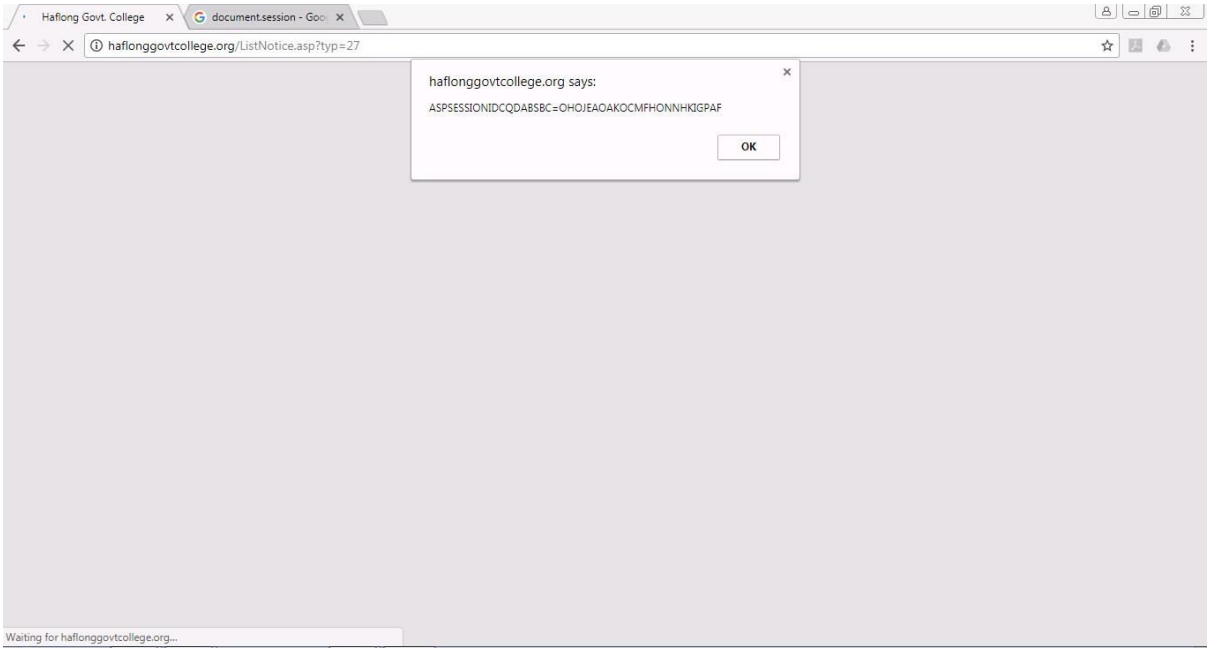


Fig 8.2: Gives session id when user visits the page

Reflected:

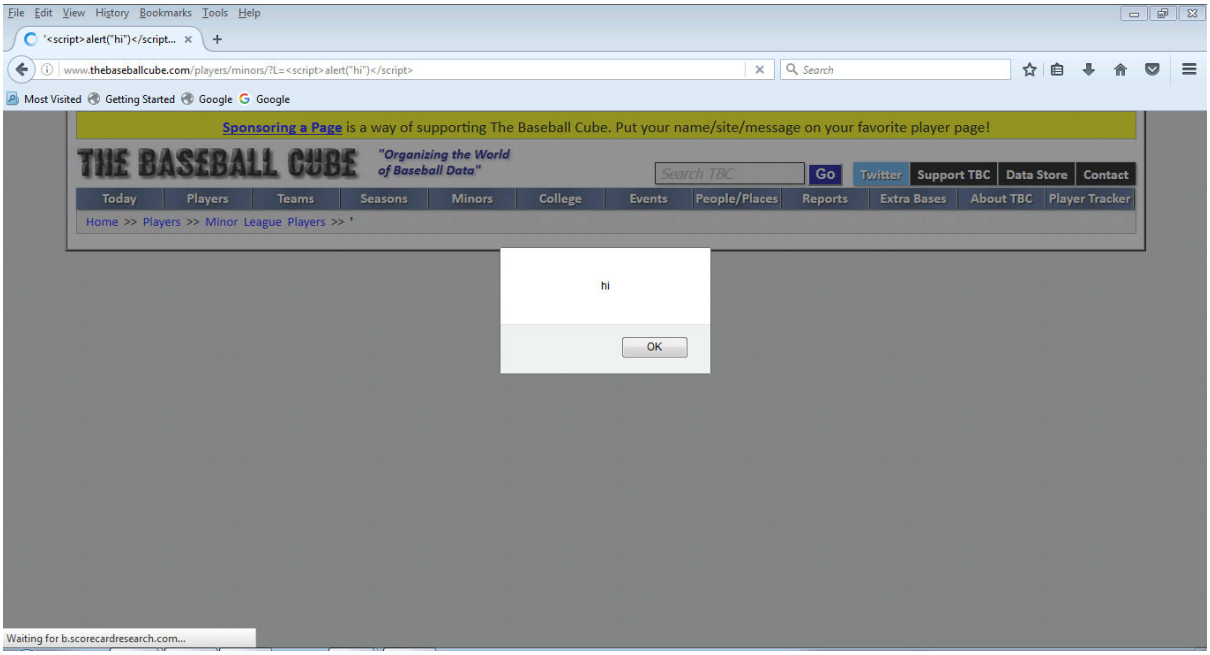


Fig 8.3 the script code is given in the url itself

Day 9

Cross Site request forgery is an attack that forces an end user to execute unwanted actions on a web application in which he is currently authenticated.

With help of social engineering an attacker may force the users of a web application to execute actions of attackers choosing.

Used Havij which is an automated SQL injection tool to get database of a website

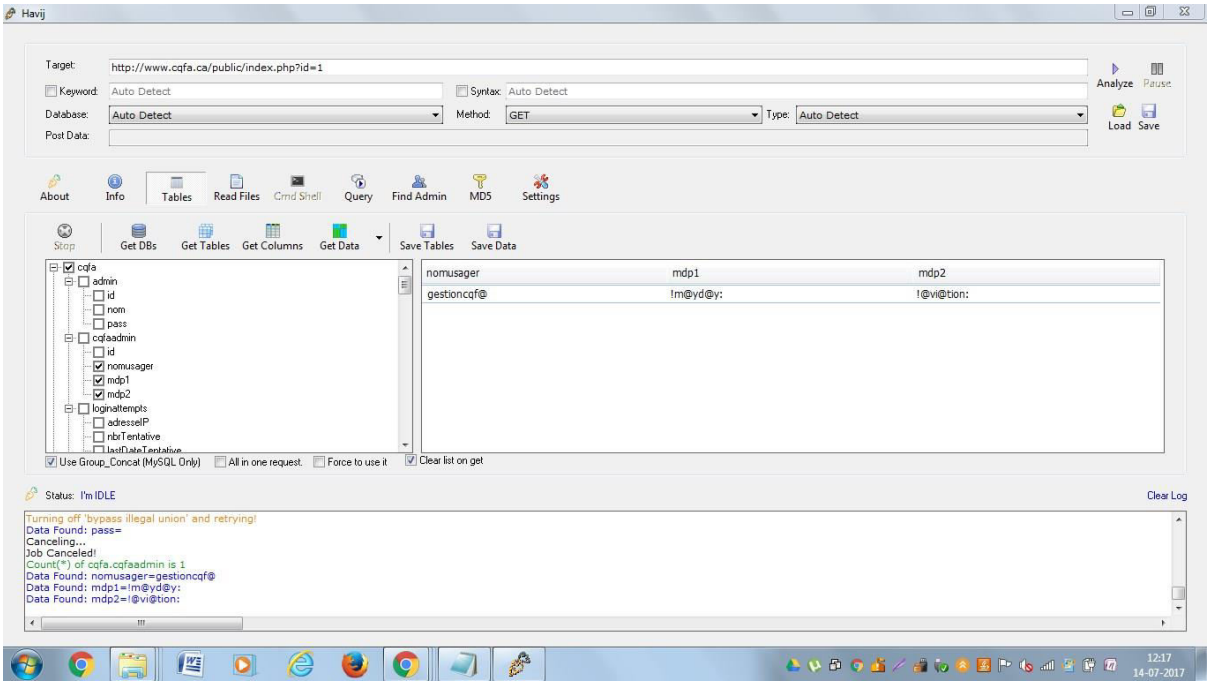


Fig 9.1 Havij showing database of a website and showing the username and password

Day 10

Learnt about hping3, .htaccess,robots.txt

Hping3

Hping3 is a packet crafting/analysing software on kali linux which is used to craft different tcp and udp packets. This can be used to perform scans on ports of a website and also be used to perform DOS attack on a target

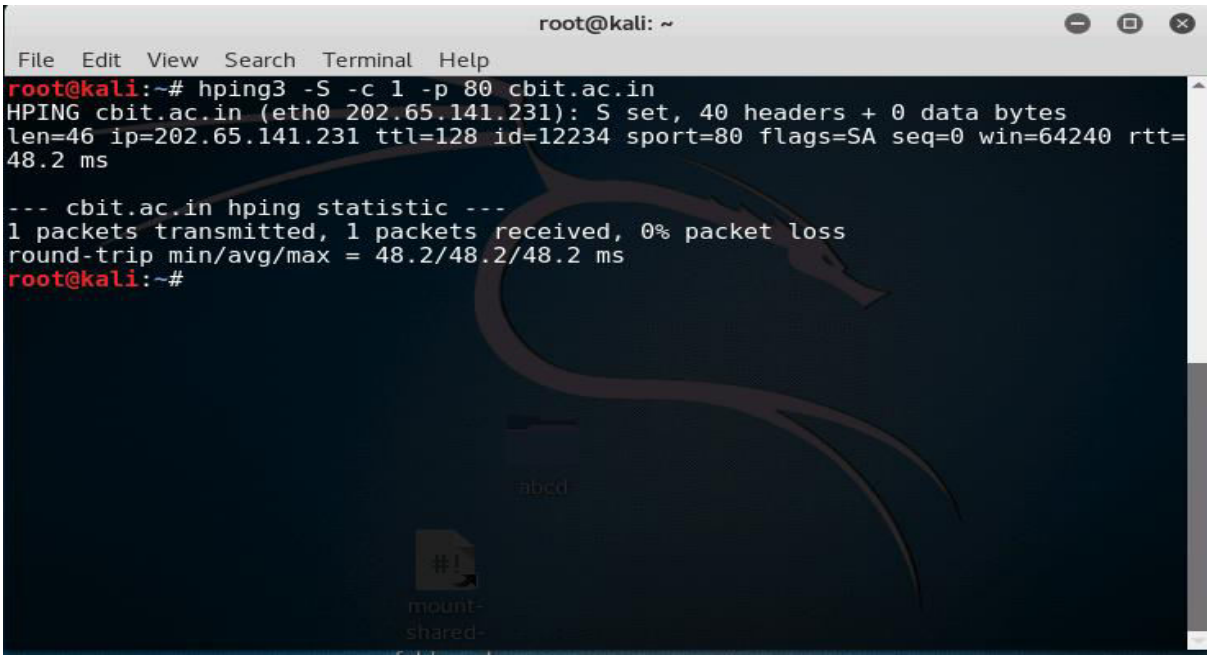


Fig 10.1 Using Hping3 to sedn a syn packet to cbit.ac.in to port 80

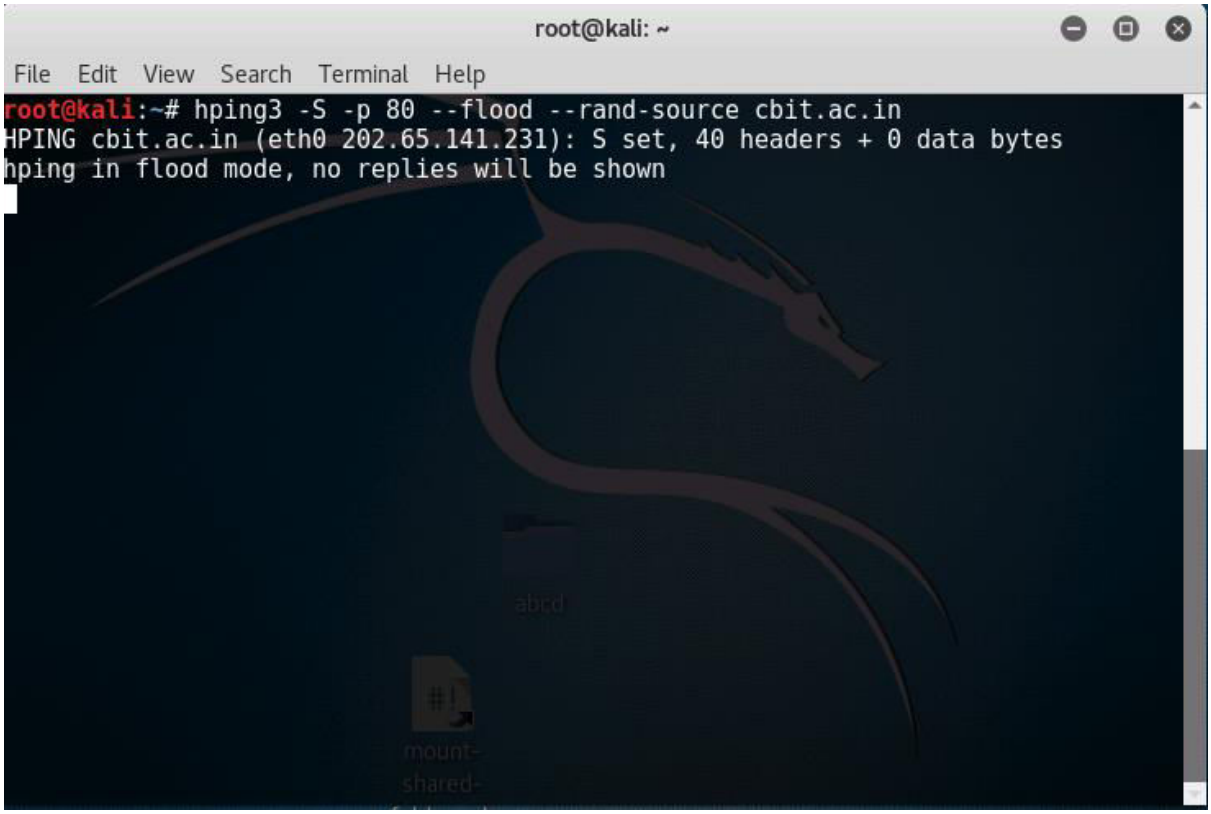


Fig 10.2 Using Hping3 to perform a DOS attack

In the Dos attack performed above commands used are

-S To set SYN flag

-p 80 To send to port 80

--flood to send all packets as soon as possible

--rand-source to hide our ip address and send from a random ip address

cbit.ac.in is the destination of the attack (you can also give the ip address of the website)

.htaccess

.htaccess file is placed in a directory which is in turn 'loaded via the Apache Web Server', then the .htaccess file is detected and executed by the Apache Web Server software. These .htaccess files can be used to alter the configuration of the Apache Web Server software to enable/disable additional functionality and features that the Apache Web Server software has to offer. These facilities include basic redirect functionality, for instance if a 404 file not found error occurs, or for more advanced functions such as content password protection or image hot link prevention.

Some of the custom error pages for redirecting the user to are:

400 – Bad request

401 – Authorization Required

403 – Forbidden

404 – File Not Found

500 – Internal Server Error

Eg: ErrorDocument 404 /filenotfound.html
ErrorDocument 500 /servererror.html

You can also deny users having specific ip address from visiting the site

order allow,deny
deny from 255.0.0.0
deny from 123.45.6.
allow from all

By pasting the above code in .htaccess file you can deny access to ussers having ip addresses 255.0.0.0 and 123.45.6.0-255.

Robots.txt

Web site owners use the /robots.txt file to give instructions about their site to web robots; this is called The Robots Exclusion Protocol. We can prevent bots which serach the web from finding our website
We enter records of what bots can find the website
Eg:
User-agent: *
Disallow: /
This excludes all bots (* means all and / is the root directory)

User-agent: *
Disallow:

Since we didn't give '/',ita allows access for al bots.

User-agent: Google
Disallow:

User-agent: *
Disallow: /

This allows only google bot

User-agent: *
Disallow: /abc/abc.html

This is used to exclude some pages (abc.html).

Day 12-13

Analyse the website thinkingnirvana.in for vulnerabilities and prepare a report

Key Findings

The key vulnerablities which are found are dicussed below

1. Slow HTTP Denial of service attack

HTTP requests by design are to be recieved completely recieved by the server before they are processed. Therefore an attacker may send an incomplete request or may send request at very low speed. This causes the server to keep its resources busy and if all of server resouce is used this creates a denial of service i.e. other users may not be able to access the website.

***Solution**:* Use number of apache modules such as **mod_reqtimeout** to set timeouts for http requests, **mod_qos** to provide different levels of priority to different requests and **mod_security** which is a web application fire wall which is used with apache server (for more information refer: https://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/).

2. wp-login.php page is accessible

The login page www.thinkingnirvana.in/wp-login.php is accessible publicly. An attacker may brute force admin username and password to gain access.

Solution: You can lock down the WordPress admin login with some .htaccess rules to prevent unauthorized login attempts. (visit this link http://hgpqr.com/change-htaccess-on-hostgator.html on how to configure your.htaccess file) In .htaccess file paste these lines.

```
order deny,allow
deny from all
allow from <your ip>
```

where in <your ip> keep ip adress which is used to access the login.

3. Password type input with auto complete

When username and password are submitted in www.thinkingnirvana.in/wp-login.php they get saved in web browser cache. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Solution: Use a wordpress autocomplete disbale plugin(https://wordpress.org/plugins/disable-autocomplete/#installation) or modify input tag

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

4. Website does not have secure login

Login forms

http://www.thinkingnirvana.in/wp-login.php

ftp://ftp.thinkingnirvana.in/

http://webmail.thinkingnirvana.in:2095/

These forms are not secure login

An attacker can be able to see the information which user submits via the form.

Solution: For secure login implement HTTPS and SSL. This encrypts your data and makes it harder for attacker to see the sensitive form data. To implement HTTPS you need to have a SSL certificate which is provided by your host (hostgator). HTTPS requires extra Apache Modules (mod_ssl) to be enabled, port 443 to be opened, properly configured, other settings including VirtualHost configuration to be properly configured. After this you can change the HTTP URLS to HTTPS in general settings. As there is no need to serve the whole website with both HTTPS URLs and HTTP URLs, you have to redirect with .htaccess rules to 301 redirect HTTPS to HTTP or vice versa.(for more information visit https://make.wordpress.org/support/user-manual/web-publishing/https-for-wordpress/)

5. Wordpress Site is user enumerable

An acttacker can run scripts to determine author name in the wordpress website. If your username is also the author name then attacker can gain access by using the author name.

Solution : Modify .htaccess to include a rule to block user enmeration.(Source: https://wordpress.stackexchange.com/questions/46469/can-i-prevent-enumeration-of-usernames)

```
RewriteCond %{REQUEST_URI}  ^/$
RewriteCond %{QUERY_STRING} ^/?author=([0-9]*)
RewriteRule ^(.*)$ http://yoursite.com/somepage/? [L,R=301]
```

6. ClickJacking

Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

Solution: Log into cPanel >> File Manager, take a backup of wp-config.php, edit the file and add the following line: header('X-Frame-Options: SAMEORIGIN'); . Or use a plugin.

7. Session cookie without HTTP only flag and Secure flag set

When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Solution: Take a backup of wp-config.php, edit the file and add the following lines:

@ini_set('session.cookie_httponly', true);

@ini_set('session.cookie_secure', true);

@ini_set('session.use_only_cookies', true);

Or use a plugin

8. Weak SSL and SSH ciphers

SSL 64 bit cipher was spotted which can be exploited by a MITMA(Man in the middle attack). Also no NULL chiper suites are supported which offer no encryption (for port 993/tcp/imap and 995 / tcp / pop3).Also SSH server is using Arcfour stream cipher or no cihper at all(for port 22/tcp/ssh).

Solution: Reconfigure the affected application if possible to avoid use of medium strength ciphers. Contact the vendor or consult product documentation to remove the weak ciphers.

Classification of vulnerabilities

Classifiaction	Vulnerability Name	Solution
High level	Slow HTTP denial of service of attack	Use mod_reqtimeout, mod_qos, mod_security; apache modules
Medium Level	wp-login.php page is accessible	Modify .htaccess file to prevent unauthorized access.
Medium Level	Weak SSL and SSH ciphers	Contact the vendor or consult product documentation to remove the weak ciphers.
Medium Level	Website does not have a secure login	Implement HTTPS.
Low level	Wordpress site is user enumerable	Modify .htaccess file to prevent enumeration.
Low Level	Password auto complete	Use a plugin or modify the input tag.
Low Level	ClickJacking	Add: header('X-Frame-Options: SAMEORIGIN'); to “wp-login.php” file or use a plugin
Low Level	HTTPonly flag and Secure Flag not set	Add: @ini_set('session.cookie_httponly', true); @ini_set('session.cookie_secure', true); @ini_set('session.use_only_cookies', true); To “wp-login.php” file Or use a plugin

Technical Report

1. About the domain

Domain: thinkingnirvana.in
Registrar: GoDaddy.com, LLC (R101-AFIN)
Registration Date: 2017-03-08
Expiration Date: 2018-03-08
Updated Date: 2017-05-07
Name Servers: ns2.md-in-72.hostgatorwebservers.com
ns1.md-in-72.hostgatorwebservers.com

2.Trace Route

```
Tracing route to thinkingnirvana.in [45.113.122.63]
over a maximum of 30 hops:

  1    12 ms    10 ms    34 ms  192.168.1.1
  2    63 ms     7 ms     *     10.244.0.1
  3    76 ms    19 ms     4 ms  broadband.actcorp.in [202.83.20.205]
  4     2 ms     3 ms    14 ms  broadband.actcorp.in [202.83.26.1]
  5     8 ms     3 ms     3 ms  14.141.145.197.static-Bangalore.vsnl.net.in [14.
141.145.197]
  6    68 ms    64 ms    18 ms  172.29.250.33
  7    61 ms    33 ms    80 ms  172.23.78.238
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    63 ms    22 ms    19 ms  md-in-72.webhostbox.net [45.113.122.63]
```

3. Ports

Port	State	Service	Version
21/tcp	open	ftp	Pure-FTPd
22/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
25/tcp	open	smtp?	
53/tcp	open	domain	ISC BIND 9.8.2rc1
80/tcp	open	http	Apache httpd
110/tcp	open	pop3	Dovecot pop3d
143/tcp	open	imap	Dovecot imapd
443/tcp	open	ssl/ssl	Apache httpd (SSL-only mode)
465/tcp	open	ssl/smtp	Exim smtpd 4.87
587/tcp	open	smtp	Exim smtpd 4.87
993/tcp	open	ssl/imap	Dovecot imapd
995/tcp	open	ssl/pop3	Dovecot pop3d
2077/tcp	open	webdav	cPanel webdav
2078/tcp	open	ssl/http	cPanel httpd (unauthorized)
2079/tcp	open	http	cPanel httpd (unauthorized)
2080/tcp	open	ssl/http	cPanel httpd (unauthorized)
2082/tcp	open	infowave?	
2083/tcp	open	http	cPanel httpd 11.58.0.50
2086/tcp	open	gnunet?	
2087/tcp	open	http	cPanel httpd 11.58.0.50
2095/tcp	open	nbx-ser?	
2096/tcp	open	http	cPanel httpd 11.58.0.50
3306/tcp	open	mysql	MySQL 5.6.35-80.0-log
8083/tcp	open	http	Apache httpd
60108/tcp	open	unknown	

Ports Assessment

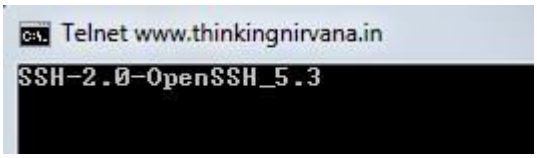
There are many ports which are open. This may cause a vulnerability. Remove unwanted ports.

Remove the unauthorized cPanel ports (keep only one port for cPanel) and 8083 Apache httpd port.

Port 21 banner grab

Dont allow unauthorized connection to port 21(ftp)

Port 22 banner grab



Modify httpd.config file for ports which give banner data. This prevents attacker from knowing the vulnerabilities based on versionsof services running on ports

Remove Dovecot ports since they give a connection to unauthorized users.

Also port 587 has clear text login permitted. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used. To solve this configure the service to support less secure authentication mechanisms only over an encrypted channel.

Also on port 110 the remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. To solve this contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.

5. Banner Grabbing

Webserver Apache

Operating System Linux Kernel 2.6

6. DNS records

DNS servers
ns2.md-in-72.hostgatorwebservers.com
ns1.md-in-72.hostgatorwebservers.com

Answer records

thinkingnirvana.in	MX	preference:	0	14400s
		exchange:	thinkingnirvana.in	
thinkingnirvana.in	SOA	server:	ns1.md-in-72.hostgatorwebservers.com	86400s
		email:	cpanel@webhostbox.net	
		serial:	2017030803	
		refresh:	86400	
		retry:	7200	
		expire:	3600000	
		minimum ttl:	86400	
thinkingnirvana.in	NS	ns1.md-in-72.hostgatorwebservers.com		86400s
thinkingnirvana.in	NS	ns2.md-in-72.hostgatorwebservers.com		86400s
thinkingnirvana.in	A	45.113.122.63		14400s

Authority records

Additional records

thinkingnirvana.in	A	45.113.122.63	14400s

DNS Assessment

- The SOA REFRESH value determines how often secondary nameservers check with the master nameserver for updates.Your SOA REFRESH value is 86400 seconds which is very high (about 3600-7200 seconds is good althought RFC1912 2.2 recommends a value between 1200 to 43200 seconds).
- The expire value is how long a secondary nameserver will wait before considering its DNS data stale if it can't reach the primary nameserver. Your SOA EXPIRE value is 3600000 seconds which is very high (as suggested by RFC1912 a value between 1209600 to 2419200 seconds is good).
- I found that you have only one MX record. If this mail server goes down this can cause mail delivery delays or even mail loss. This acceptable but consider increasing the number of your MXs.

  To change your DNS records, login to your hosting account(which is hostgator) and change the records according to the assessment.
  (for more information refer: http://hgpgr.com/hostgator-change-dns-records.html).

3. Outcomes

Technical Outcomes

1. During the course of the internship I was exposed to known and unkown technologies, tools, concepts, terminologies of the various domains of cyber security.

2. As this was my first internship, though we were not subjected to a proper work environment I leant some professional work ethics of the cyber security industry and how a client approaches a company for a security assessment/audit.

3. Was exposed to the CEH approved penetration tester's methodology on how to perform a security assessment.

4. Each day of the intern helped me to improve soft skills and hard skills

Non-Technical Outcomes

1. I realised to, perform hacking and penetration testing one requires a lot of patience and hardwork.

2. Made some new friends.