ASSIGNMENT

Website Information Gathering

Submitted By:

Rana Sahban

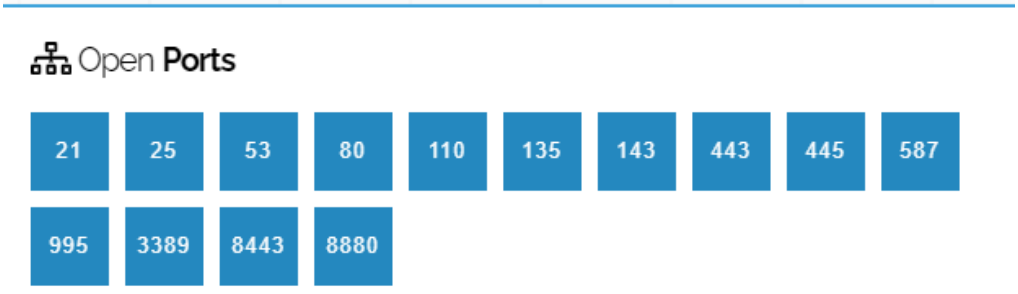
Nauman Qureshi

Submitted To:

Muhammad Bilal

Target Website Name	Delhi Public School Society
Domain	dpsfamily.org
IP Address	67.227.141.78
Sub domain	
admission.dpsfamily.org	101.53.154.165
intranet.dpsfamily.org	67.227.236.120
www.dpsfamily.org	67.227.141.78
autodiscover.intranet.dpsfamily.org	
cpanel.intranet.dpsfamily.org	
mail.intranet.dpsfamily.org	
webdisk.intranet.dpsfamily.org	
webmail.intranet.dpsfamily.org	
www.intranet.dpsfamily.org	

Open Ports



Vulnerabilities

Critical

CVE-2010-3972	10 Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information.
CVE-2010-2730	9.3 Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability."

Medium

CVE-2010-1899	4.3 Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability."

Technologies

Hosting panels

Plesk

Programming languages

Adobe Flash

Web frameworks

Microsoft ASP.NET

Operating systems

Windows Server

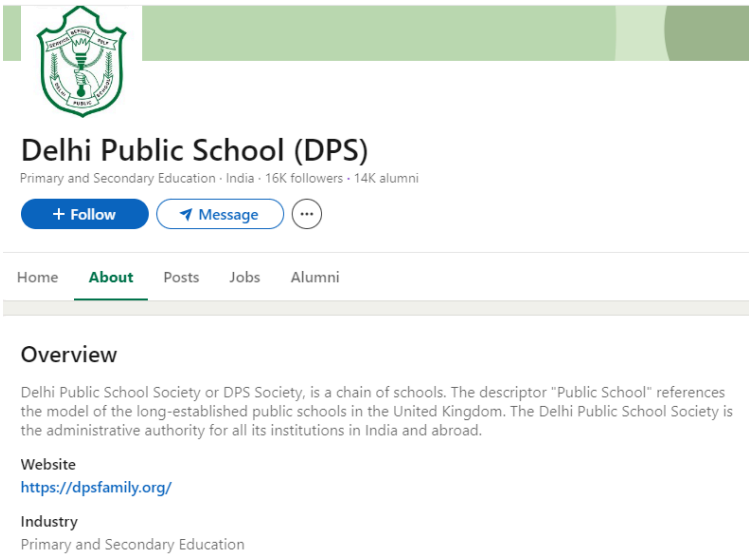
Web servers

IIS 7.5

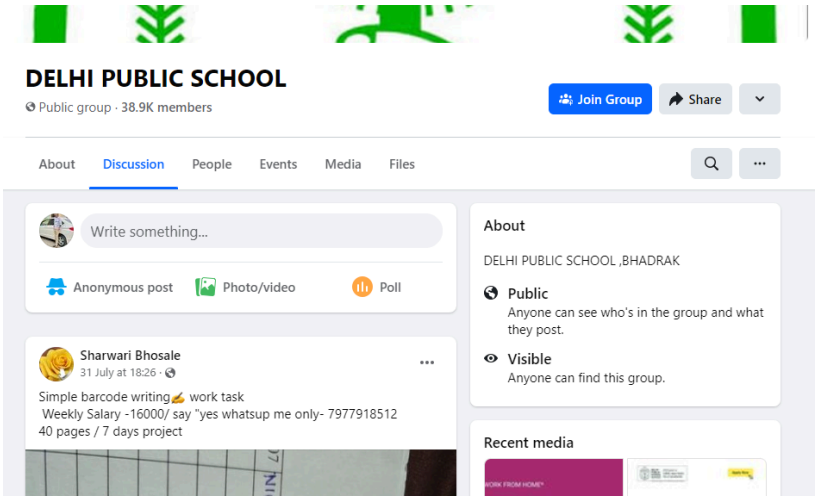
JavaScript libraries

jQuery 1.7.1

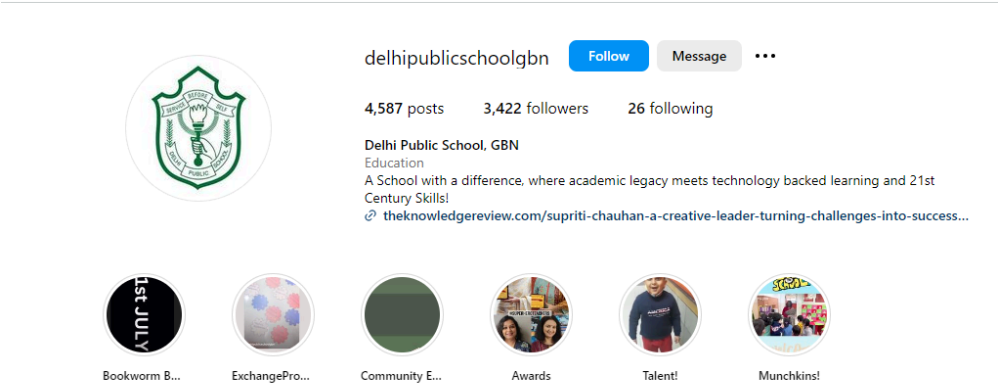
Linkedin



Facebook



Instagram



Company size

201-500 employees

709 associated members

Location

City	New Delhi
State	Delhi
Country	India

Postal Address

The Delhi Public School Society

F-Block, East of Kailash

New Delhi 110065, India

Phone

+91-11-43126700

+91-11-26223173

Email

secretary@dpsfamily.org

Fax

+91-11-26472002

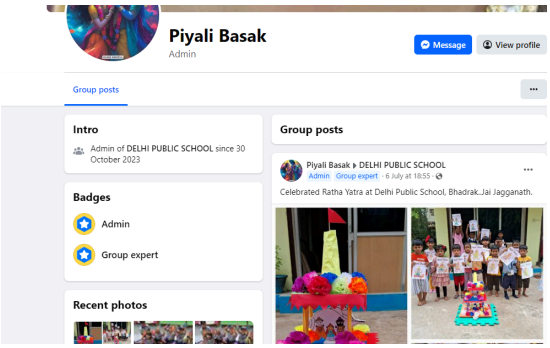
+91-11-26288911

Ip Details

```
ip: "67.227.141.78",
hostname: "777networks.com",
city: "Lansing",
region: "Michigan",
country: "US",
loc: "42.7325,-84.5555",
org: "AS32244 Liquid Web, L.L.C",
postal: "48901",
```

```
asn: "AS32244",
name: "Liquid Web, L.L.C",
domain: "liquidweb.com",
route: "67.227.128.0/17",
type: "hosting",
company: Object,
name: "XS Infosol Pvt. Ltd",
domain: "xsinfosol.com",
```


Facebook Group Admin

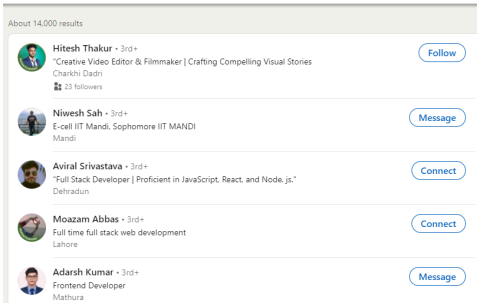
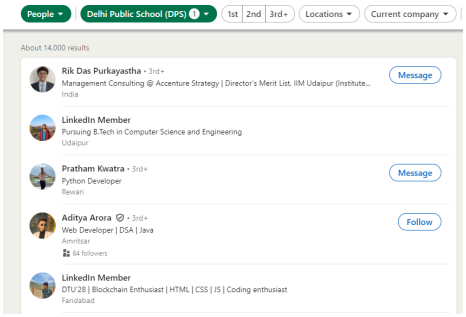


Fees Structure

Fee Structure

	Particulars	Amount (In Rs.)
i	**Composite Fee (per month) (inclusive of the Tuition Fee)**	**9400**
ii	Composite Fee (If paid quarterly) - 9400 x 3 = 28200/-	28200
iii	Additional Annual charges (to be paid in two installment of Rs.6600/- each in the month of April and October)	13200
C	Optional Fee Components :	

students are there in Delhi public school?

Over 10000

Some Followers