-CEH – Report regarding information gathering and vulnerabilities about specific target.  
-Group Members : Muhammad Ibrahim , Faisal Malik  
-Submitted to : Sir Bilal

:Report Data Gathering:

Name : Modern High School for Girls:

Link : <Https://www.mhsforgirls.edu.in/>

IP Address : 207.174.215.236

-Ports And Services--

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

26/tcp open rsftp

53/tcp open domain

80/tcp open http

110/tcp open pop3

143/tcp open imap

443/tcp open https

465/tcp open smtps

587/tcp open submission

993/tcp open imaps

995/tcp open pop3s

2222/tcp open EtherNetIP-1

3306/tcp open mysql

-- Total Sub domains--

Subdomain IP CloudFlare

cpanel.mhsforgirls.edu.in 207.174.215.236 CloudFlare is off

cpcalendars.mhsforgirls.edu.in 207.174.215.236 CloudFlare is off

cpcontacts.mhsforgirls.edu.in 207.174.215.236 CloudFlare is off

mail.mhsforgirls.edu.in 207.174.215.236 CloudFlare is off

webdisk.mhsforgirls.edu.in 207.174.215.236 CloudFlare is off

webmail.mhsforgirls.edu.in 207.174.215.236 CloudFlare is off

www.mhsforgirls.edu.in 207.174.215.236 CloudFlare is off

via: https://subdomainfinder.c99.nl/

--Technologies used for development of website:--

-Web servers-

Apache HTTP Server

-Programming languages-

PHP

-JavaScript libraries-

Retina.js

Hammer.js

OWL Carousel

jQuery Migrate

jQuery

1.10.2

-UI frameworks

Bootstrap

--linked in profile--

Handle::

school/modern-high-school-for-girls

Estimated Annual Revenue

$0-$1M

Employees Range

1-10

Vulnerabilities from the targeted website:

Nmap scan report for cp-48.webhostbox.net (207.174.215.236)

Host is up (0.29s latency).

Not shown: 981 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

21/tcp open ftp Pure-FTPd

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

| vulners:

| cpe:/a:openbsd:openssh:7.4:

| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408

| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23\*EXPLOIT\*

| 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623\*EXPLOIT\*

| CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778

| SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 EXPLOIT

| PACKETSTORM:173661 7.5 https://vulners.com/packetstorm/PACKETSTORM:173661 EXPLOIT

| F0979183-AE88-53B4-86CF-3AF0523F3807 7.5 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807\*EXPLOIT\*

| 1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 EXPLOIT

| CVE-2021-41617 7.0 https://vulners.com/cve/CVE-2021-41617

| EDB-ID:46516 6.8 https://vulners.com/exploitdb/EDB-ID:46516 EXPLOIT

| EDB-ID:46193 6.8 https://vulners.com/exploitdb/EDB-ID:46193 EXPLOIT

| CVE-2019-6110 6.8 https://vulners.com/cve/CVE-2019-6110

| CVE-2019-6109 6.8 https://vulners.com/cve/CVE-2019-6109

| C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3\*EXPLOIT\*

| 10213DBE-F683-58BB-B6D3-353173626207 6.8 https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207\*EXPLOIT\*

| CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385

| CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795

| CVE-2020-14145 5.9 https://vulners.com/cve/CVE-2020-14145

| CVE-2019-6111 5.9 https://vulners.com/cve/CVE-2019-6111

| EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 EXPLOIT

| EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 EXPLOIT

| 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 EXPLOIT

| 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 EXPLOIT

| MSF:AUXILIARY-SCANNER-SSH-SSH\_ENUMUSERS- 5.3 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH\_ENUMUSERS- EXPLOIT

| EDB-ID:45939 5.3 https://vulners.com/exploitdb/EDB-ID:45939 EXPLOIT

| EDB-ID:45233 5.3 https://vulners.com/exploitdb/EDB-ID:45233 EXPLOIT

| CVE-2018-20685 5.3 https://vulners.com/cve/CVE-2018-20685

| CVE-2018-15919 5.3 https://vulners.com/cve/CVE-2018-15919

| CVE-2018-15473 5.3 https://vulners.com/cve/CVE-2018-15473

| CVE-2017-15906 5.3 https://vulners.com/cve/CVE-2017-15906

| CVE-2016-20012 5.3 https://vulners.com/cve/CVE-2016-20012

| SSH\_ENUM 5.0 https://vulners.com/canvas/SSH\_ENUM EXPLOIT

| PACKETSTORM:150621 5.0 https://vulners.com/packetstorm/PACKETSTORM:150621 EXPLOIT

| EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 EXPLOIT

| EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0 https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 EXPLOIT

| 1337DAY-ID-31730 5.0 https://vulners.com/zdt/1337DAY-ID-31730 EXPLOIT

| CVE-2021-36368 3.7 https://vulners.com/cve/CVE-2021-36368

| PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 EXPLOIT

| PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/PACKETSTORM:140261 EXPLOIT

|\_ 1337DAY-ID-30937 0.0 https://vulners.com/zdt/1337DAY-ID-30937 EXPLOIT

25/tcp filtered smtp

26/tcp open smtp Exim smtpd 4.96.2

| smtp-vuln-cve2010-4344:

|\_ The SMTP server is not Exim: NOT VULNERABLE

53/tcp open domain ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)

| vulners:

| cpe:/a:isc:bind:9.11.4-p2:

| CVE-2021-25216 9.8 https://vulners.com/cve/CVE-2021-25216

| CVE-2020-8616 8.6 https://vulners.com/cve/CVE-2020-8616

| CVE-2020-8625 8.1 https://vulners.com/cve/CVE-2020-8625

| CVE-2023-50387 7.5 https://vulners.com/cve/CVE-2023-50387

| CVE-2023-3341 7.5 https://vulners.com/cve/CVE-2023-3341

| CVE-2023-2828 7.5 https://vulners.com/cve/CVE-2023-2828

| CVE-2022-38178 7.5 https://vulners.com/cve/CVE-2022-38178

| CVE-2022-38177 7.5 https://vulners.com/cve/CVE-2022-38177

| CVE-2022-3488 7.5 https://vulners.com/cve/CVE-2022-3488

| CVE-2021-25215 7.5 https://vulners.com/cve/CVE-2021-25215

| CVE-2020-8623 7.5 https://vulners.com/cve/CVE-2020-8623

| CVE-2020-8617 7.5 https://vulners.com/cve/CVE-2020-8617

| CVE-2019-6470 7.5 https://vulners.com/cve/CVE-2019-6470

| CVE-2018-5744 7.5 https://vulners.com/cve/CVE-2018-5744

| CVE-2018-5743 7.5 https://vulners.com/cve/CVE-2018-5743

| BB688FBF-CEE2-5DD1-8561-8F76501DE2D4 7.5 https://vulners.com/githubexploit/BB688FBF-CEE2-5DD1-8561-8F76501DE2D4\*EXPLOIT\*

| 1337DAY-ID-34485 7.5 https://vulners.com/zdt/1337DAY-ID-34485 EXPLOIT

| CVE-2021-25220 6.8 https://vulners.com/cve/CVE-2021-25220

| CVE-2021-25214 6.5 https://vulners.com/cve/CVE-2021-25214

| CVE-2020-8622 6.5 https://vulners.com/cve/CVE-2020-8622

| CVE-2018-5741 6.5 https://vulners.com/cve/CVE-2018-5741

| CVE-2019-6471 5.9 https://vulners.com/cve/CVE-2019-6471

| CVE-2022-2795 5.3 https://vulners.com/cve/CVE-2022-2795

| CVE-2021-25219 5.3 https://vulners.com/cve/CVE-2021-25219

| CVE-2019-6465 5.3 https://vulners.com/cve/CVE-2019-6465

| PACKETSTORM:157836 5.0 https://vulners.com/packetstorm/PACKETSTORM:157836 EXPLOIT

| FBC03933-7A65-52F3-83F4-4B2253A490B6 5.0 https://vulners.com/githubexploit/FBC03933-7A65-52F3-83F4-4B2253A490B6\*EXPLOIT\*

| CVE-2018-5745 4.9 https://vulners.com/cve/CVE-2018-5745

| CVE-2020-8624 4.3 https://vulners.com/cve/CVE-2020-8624

| cpe:/o:redhat:enterprise\_linux:7:

| CVE-2022-1665 8.2 https://vulners.com/cve/CVE-2022-1665

|\_ CVE-2014-8181 5.5 https://vulners.com/cve/CVE-2014-8181

80/tcp open http Apache httpd

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|\_http-dombased-xss: Couldn't find any DOM based XSS.

|\_http-csrf: Couldn't find any CSRF vulnerabilities.

110/tcp open pop3 Dovecot pop3d

143/tcp open imap Dovecot imapd

443/tcp open ssl/http Apache httpd

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|\_http-csrf: Couldn't find any CSRF vulnerabilities.

|\_http-dombased-xss: Couldn't find any DOM based XSS.

465/tcp open ssl/smtp Exim smtpd 4.96.2

587/tcp open smtp Exim smtpd 4.96.2

993/tcp open imaps?

995/tcp open pop3s?

1719/tcp filtered h323gatestat

1720/tcp filtered h323q931

2222/tcp open ssh OpenSSH 7.4 (protocol 2.0)

| vulners:

| cpe:/a:openbsd:openssh:7.4:

| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408

| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23\*EXPLOIT\*

| 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623\*EXPLOIT\*

| CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778

| SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 EXPLOIT

| PACKETSTORM:173661 7.5 https://vulners.com/packetstorm/PACKETSTORM:173661 EXPLOIT

| F0979183-AE88-53B4-86CF-3AF0523F3807 7.5 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807\*EXPLOIT\*

| 1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 EXPLOIT

| CVE-2021-41617 7.0 https://vulners.com/cve/CVE-2021-41617

| EDB-ID:46516 6.8 https://vulners.com/exploitdb/EDB-ID:46516 EXPLOIT

| EDB-ID:46193 6.8 https://vulners.com/exploitdb/EDB-ID:46193 EXPLOIT

| CVE-2019-6110 6.8 https://vulners.com/cve/CVE-2019-6110

| CVE-2019-6109 6.8 https://vulners.com/cve/CVE-2019-6109

| C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3\*EXPLOIT\*

| 10213DBE-F683-58BB-B6D3-353173626207 6.8 https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207\*EXPLOIT\*

| CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385

| CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795

| CVE-2020-14145 5.9 https://vulners.com/cve/CVE-2020-14145

| CVE-2019-6111 5.9 https://vulners.com/cve/CVE-2019-6111

| EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 EXPLOIT

| EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 EXPLOIT

| 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 EXPLOIT

| 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 EXPLOIT

| MSF:AUXILIARY-SCANNER-SSH-SSH\_ENUMUSERS- 5.3 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH\_ENUMUSERS- EXPLOIT

| EDB-ID:45939 5.3 https://vulners.com/exploitdb/EDB-ID:45939 EXPLOIT

| EDB-ID:45233 5.3 https://vulners.com/exploitdb/EDB-ID:45233 EXPLOIT

| CVE-2018-20685 5.3 https://vulners.com/cve/CVE-2018-20685

| CVE-2018-15919 5.3 https://vulners.com/cve/CVE-2018-15919

| CVE-2018-15473 5.3 https://vulners.com/cve/CVE-2018-15473

| CVE-2017-15906 5.3 https://vulners.com/cve/CVE-2017-15906

| CVE-2016-20012 5.3 https://vulners.com/cve/CVE-2016-20012

| SSH\_ENUM 5.0 https://vulners.com/canvas/SSH\_ENUM EXPLOIT

| PACKETSTORM:150621 5.0 https://vulners.com/packetstorm/PACKETSTORM:150621 EXPLOIT

| EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 EXPLOIT

| EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0 https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 EXPLOIT

| 1337DAY-ID-31730 5.0 https://vulners.com/zdt/1337DAY-ID-31730 EXPLOIT

| CVE-2021-36368 3.7 https://vulners.com/cve/CVE-2021-36368

| PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 EXPLOIT

| PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/PACKETSTORM:140261 EXPLOIT

|\_ 1337DAY-ID-30937 0.0 https://vulners.com/zdt/1337DAY-ID-30937 EXPLOIT

3306/tcp open mysql MySQL 5.7.23-23

|\_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)

5060/tcp filtered sip

5061/tcp filtered sip-tls

Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise\_linux:7