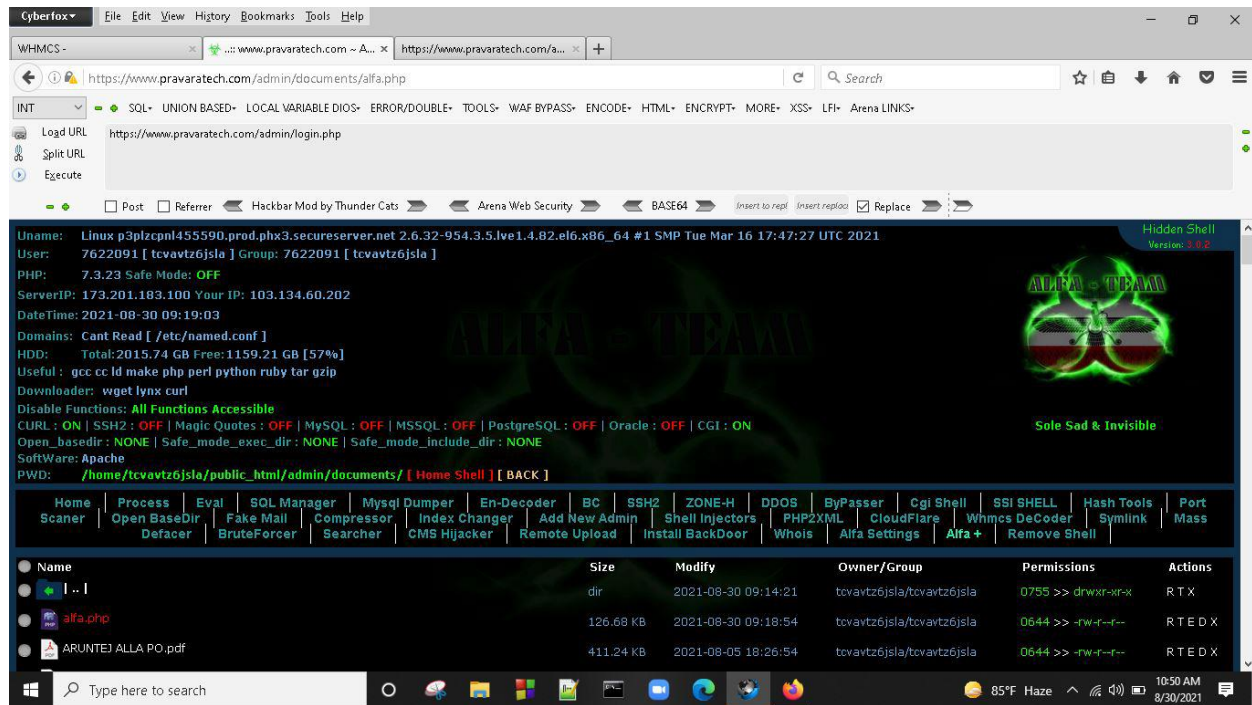
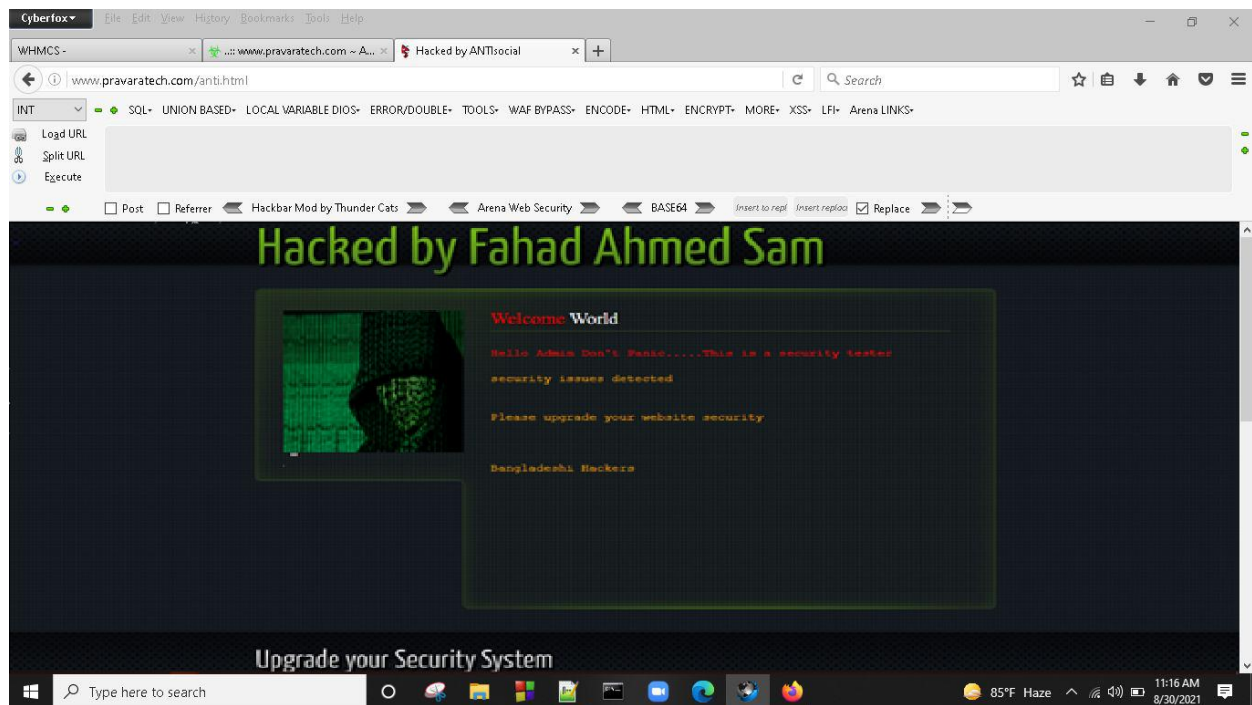


# 1). <https://www.pravaratech.com/admin/documents/alfa.php>



## Deface page: <http://www.pravaratech.com/anti.html>



## 2). <https://uimt.in/admin/uploads/alfa.php>

The screenshot shows a web browser window with the URL <https://uimt.in/admin/uploads/alfa.php>. The page displays a "Hidden Shell" interface with a green and black theme. The header includes the Alfa Team logo and the text "Sole Sad & Invisible". The main content area shows system information and a list of files.

System Information:

- uname: Linux nl-srv-web223.main-hosting.eu 4.18.0-147.8.1.el7h.lva.1.x86\_64 #1 SMP Mon Jun 29 09:05:02 EDT 2020 x86\_64 x86\_64 x
- User: 804692432 [ u804692432 ] Group: 1049367170 [ o49367170 ]
- PHP: 7.2.34 Safe Mode: OFF
- ServerIP: 194.5.156.40 Your IP: 103.134.60.202
- Date/Time: 2021-08-31 08:38:23
- Domains: Cant Read [ /etc/named.conf ]
- HDD: Total: 7392.13 GB Free: 2046.47 GB [ 27% ]
- Useful: `ld php tar gzip`
- Downloader: `wget curl`
- Disable Functions: All Functions Accessible
- CURL: ON | SSH2: OFF | Magic Quotes: OFF | MySQL: OFF | MSSQL: OFF | PostgreSQL: OFF | Oracle: OFF | CGI: ON
- Open\_basedir: NONE | Safe\_mode\_exec\_dir: NONE | Safe\_mode\_include\_dir: NONE
- SoftWare: LiteSpeed
- PWD: /home/u804692432/domains/uimt.in/public\_html/admin/uploads/ [ Home Shell ] [ BACK ]

Navigation Menu:

- Home Scanner
- Process Open BaseDir
- Eval Fake Mail
- SQL Manager
- Mysql Dumper
- En-Decoder
- BC
- SSH2
- ZONE-H
- DDOS
- ByPasser
- Cgi Shell
- SSI SHELL
- Hash Tools
- Port Mass
- Compressor
- Index Changer
- Add New Admin
- Shell Injectors
- PHP2XML
- CloudFlare
- Whmcs DeCoder
- Symlink
- Defacer
- BruteForcer
- Searcher
- CMS Hijacker
- Remote Upload
- Install BackDoor
- Whois
- Alfa Settings
- Alfa +
- Remove Shell

Name	Size	Modify	Owner/Group	Permissions	Actions
..		2021-08-04 19:39:22	u804692432/o49367170	0755 >> drwxr-xr-x	R T X
alfacgiapi		2021-08-31 08:38:24	u804692432/o49367170	0755 >> drwxr-xr-x	R T X
branch		2021-08-25 06:37:49	u804692432/o49367170	0755 >> drwxr-xr-x	R T X

## Deface page: <https://uimt.in/admin/uploads/anti.html>

The screenshot shows a defaced web page with the title "Hacked by Fahad Ahmed Sam". The page has a dark background with green and red text. The main content area displays a "Welcome World" message and a warning about security issues.

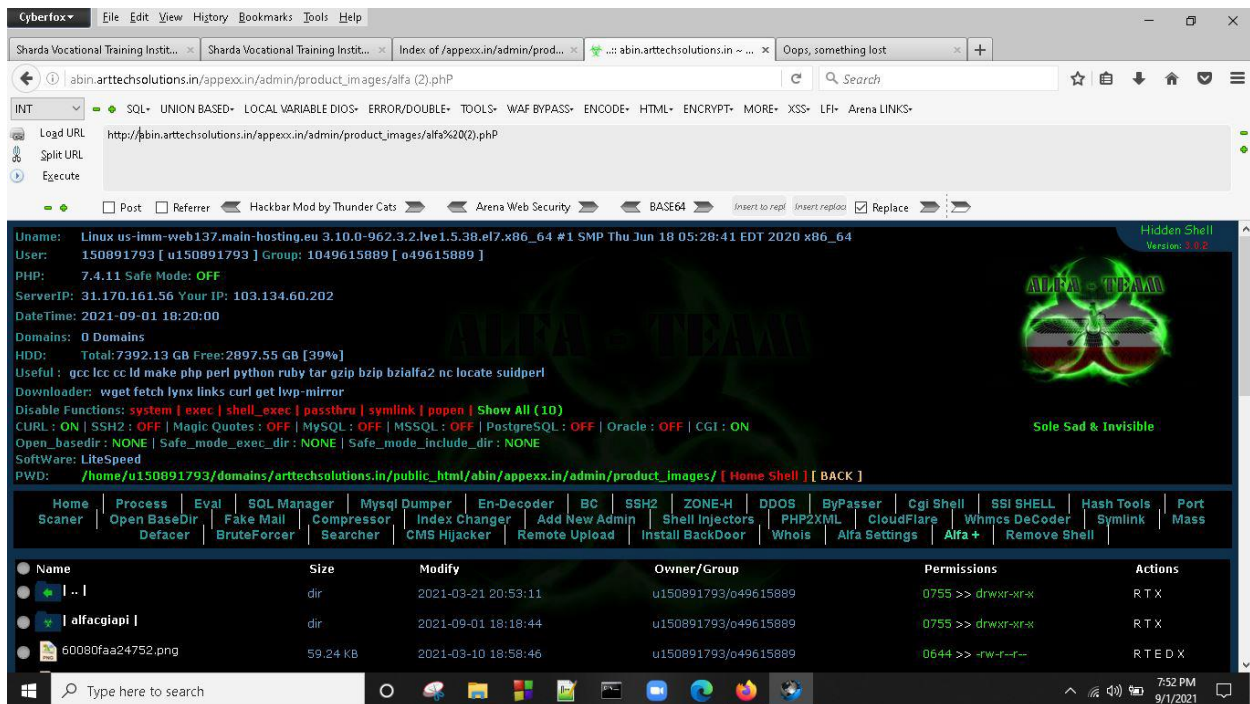
Page Content:

- Hacked by Fahad Ahmed Sam
- Welcome World
- Hello Admin Don't Panic.....This is a security tester
- security issues detected
- Please upgrade your website security
- Bangladeshi Hackers

Footer:

Upgrade your Security System

### 3). [http://abin.arttechsolutions.in/appexx.in/admin/product\\_images/alfa%20\(2\).php](http://abin.arttechsolutions.in/appexx.in/admin/product_images/alfa%20(2).php)



### Deface page: [https://abin.arttechsolutions.in/appexx.in/admin/product\\_images/anti.html](https://abin.arttechsolutions.in/appexx.in/admin/product_images/anti.html)

