

Progress Report

Target Site 1 : namakghar.com

What We Did?

Enumerated two usernames from API Keys

- ngharadnim having id 1
- nguser having id 4

Moreover, we found passwords paths from those same APIs.

- /wp/v2/users/(?P<user_id>(?:[\d]+|me))/application-passwords
- /wp/v2/users/(?P<user_id>(?:[\d]+|me))/application-passwords/introspect
- /wp/v2/users/(?P<user_id>(?:[\d]+|me))/application-passwords/(?P<uuid>[\w\-\+] +)

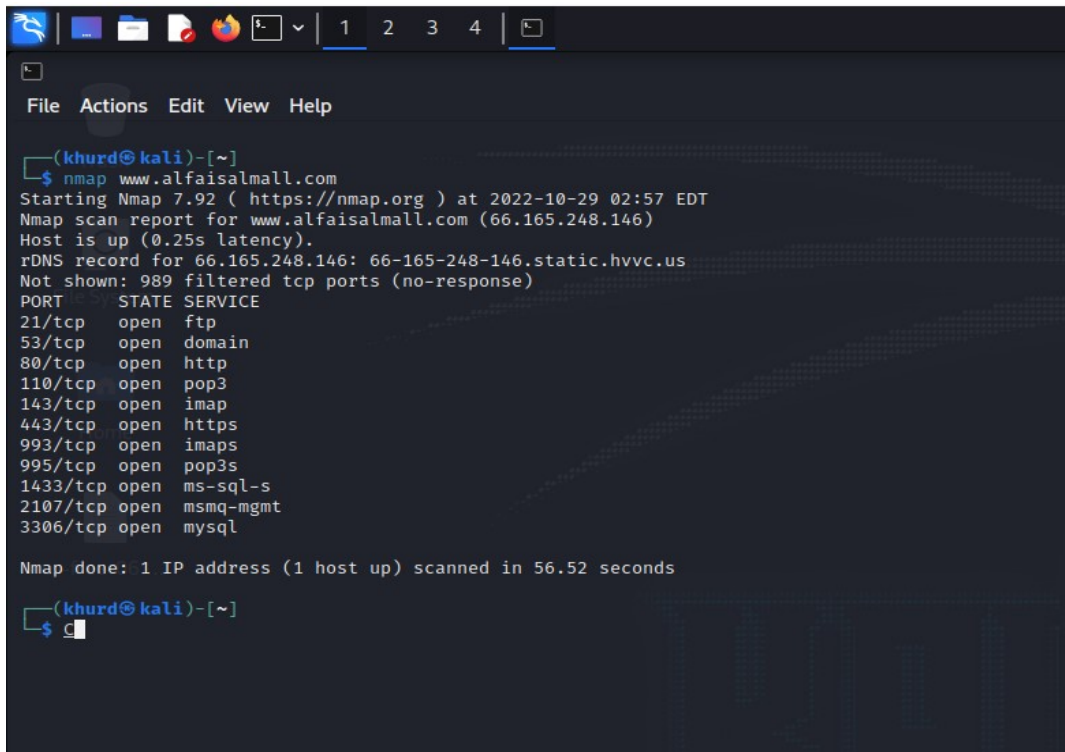
What we could not do?

We could not bypass cloudflare so far.

Target Site 2 : alfaisalmall.com

It is a new-born site so it's not using any CDN services so far.

Nmap on the website:



```
(khurd@kali)-[~]
$ nmap www.alfaismall.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-29 02:57 EDT
Nmap scan report for www.alfaismall.com (66.165.248.146)
Host is up (0.25s latency).
rDNS record for 66.165.248.146: 66-165-248-146.static.hvvc.us
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
993/tcp   open  imaps
995/tcp   open  pop3s
1433/tcp  open  ms-sql-s
2107/tcp  open  msmq-mgmt
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 56.52 seconds

(khurd@kali)-[~]
$
```

About the Website

Server IP address : 66.165.248.146

Operating System : Windows Server

Web Server : Microsoft-IIS/10.0

Web Framework : Microsoft ASP.NET 4.0.30319

Hosting Panels : Plesk

Javascript Libraries : JQuery 1.12.4 , OWL Carousel, Slick, Isotope

CPE: cpe:/o:microsoft:windows

FTP: 220 microsoft FTP Services

```

(khurd@kali)~$ nmap -sV 66.165.248.146
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-29 03:35 EDT
Nmap scan report for 66-165-248-146.static.hvvc.us (66.165.248.146)
Host is up (0.25s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft FTPd
52/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
110/tcp   open  pop3         MailEnable POP3 Server
143/tcp   open  imap         MailEnable imapd
443/tcp   open  ssl/http     Microsoft IIS httpd 10.0
993/tcp   open  ssl/imap     MailEnable imapd
995/tcp   open  ssl/pop3     MailEnable POP3 Server
1801/tcp  open  msmq?
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
3306/tcp  open  mysql        MySQL 5.5.5-10.3.36-MariaDB
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF:Port993-TCP:V=7.92%T=SSL%T=78D=10/29%Time=635CD825XP=x86_64-pc-linux-gn
SF:Ukr(NULL,32,"%*\x200K\x20IMAP4rev1\x20server\x20ready\x20at\x2010/29/22
SF:\x2012:37:05)r\n")Kr(GenericLines,62,"%*\x200K\x20IMAP4rev1\x20server\x
SF:20ready\x20at\x2010/29/22\x2012:37:12)r\n\r\n\x20BAD\x20UNKNOWN\x20Comm
SF:and\r\n\r\n\x20BAD\x20UNKNOWN\x20Command\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 146.22 seconds
zsh: segmentation fault  nmap -sV 66.165.248.146
(khurd@kali)~$

```

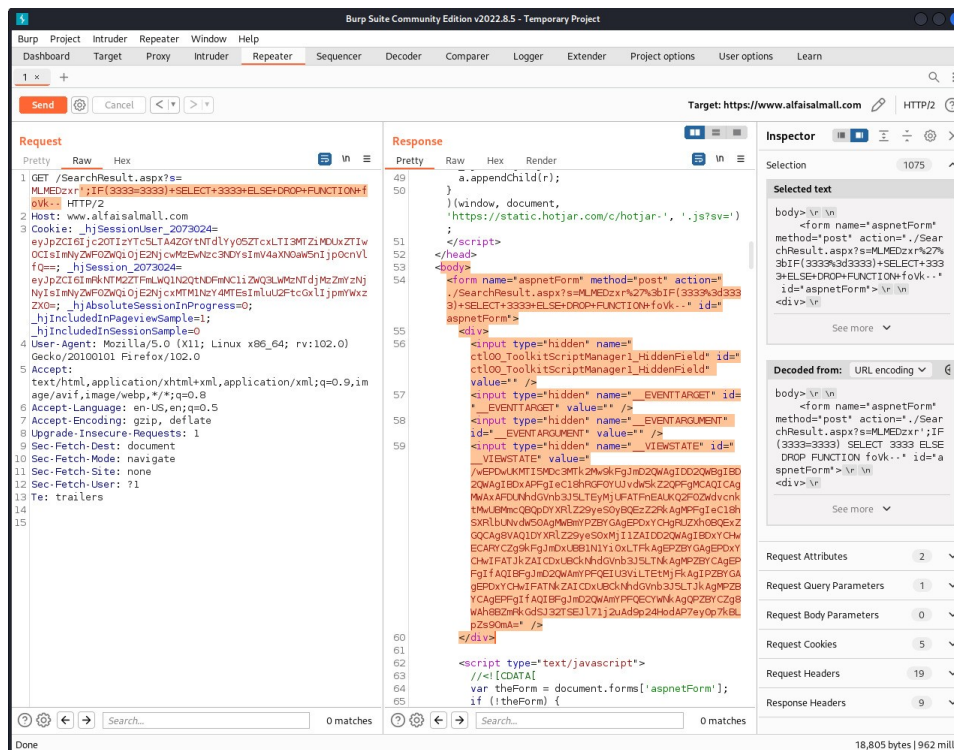
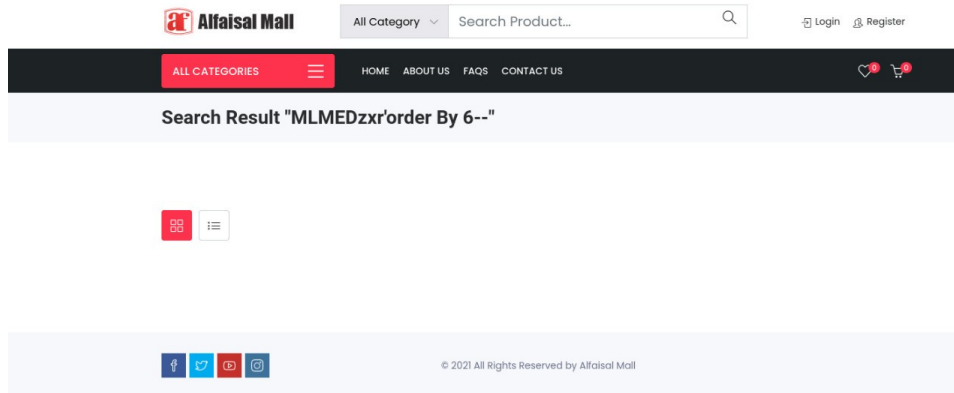
Vulnerabilities

1- Vulnerable JQuery Library (1.12.4)

- CVE-2020-11023
- CVE-2020-11022
- CVE-2015-9251
- CVE-2019-11358

2- Website is using Vulneable Http Headers; X-Powered-by and also supports X-Forwarded Host.

3- It is using Microsoft SQL server and is vulnerable to SQL Injection.



4- Missing Anti-CSRF and Anti-clickjacking Tokens

5- Content Security Policy (CSP) header not set