```
┌──(zuhra㉿zukhra)-[~]
└─$ nmap -sn --script hostmap-crtsh cambridge.uz -oN zuhra_cambridge.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 03:40 EDT
Nmap scan report for cambridge.uz (93.170.6.43)
Host is up (0.013s latency).

Host script results:
| hostmap-crtsh:
|   subdomains:
|     www.cambridge.uz
|     cloud.cambridge.uz
|     university.cambridge.uz
|     webmail.cambridge.uz
|     samarqand.cambridge.uz
|     sub.cambridge.uz
|     cafe.cambridge.uz
|     acca.cambridge.uz
|     cpanel.cambridge.uz
|     students.cambridge.uz
|     staff.cambridge.uz
|     autodiscover.cambridge.uz
|     hemis.cambridge.uz
|     vebinar.cambridge.uz
|     www.university.cambridge.uz
|     moodle.cambridge.uz
|     old.cambridge.uz
|     student.cambridge.uz
|     grand.cambridge.uz
|     www.college.cambridge.uz
|     hackathon.cambridge.uz
|     stmail.cambridge.uz
|     webdisk.cambridge.uz
|     mail.cambridge.uz
|     test.cambridge.uz
|     core.cambridge.uz
|     back.cambridge.uz
|_    college.cambridge.uz

Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ nmap -sn --script hostmap-crtsh millatumidi.uz -oN zuhra_millatumidi.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 03:44 EDT
Nmap scan report for millatumidi.uz (93.170.6.43)
Host is up (0.014s latency).

Host script results:
| hostmap-crtsh:
|   subdomains:
|     control.millatumidi.uz
|     crm.millatumidi.uz
|     mik.millatumidi.uz
|     dev.api.millatumidi.uz
|     proxy.millatumidi.uz
|     mail.millatumidi.uz
|     vtiger.millatumidi.uz
|     pbx.millatumidi.uz
|     tvt.millatumidi.uz
|     moodle.millatumidi.uz
|     test.millatumidi.uz
|     dev.api.admission.millatumidi.uz
|     api.millatumidi.uz
|     conf.millatumidi.uz
|     old.millatumidi.uz
|     cloud.millatumidi.uz
|     admission.millatumidi.uz
|     dev.my.millatumidi.uz
|     bot.millatumidi.uz
|     www.millatumidi.uz
|     api.admission.millatumidi.uz
|     new.millatumidi.uz
|     dev.admission.millatumidi.uz
|     dev.millatumidi.uz
|     tel.millatumidi.uz
|     newmoodle.millatumidi.uz
|     extra.millatumidi.uz
|     unify.millatumidi.uz
|     test1.millatumidi.uz
|_    hp.millatumidi.uz

Nmap done: 1 IP address (1 host up) scanned in 11.03 seconds
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ cat zuhra_millatumidi.txt | grep -oP '\b(?:[\w.-]+\.)+millatumidi\.uz\b' | sort -u > zuhra_millatum
idi_subdomains.txt

┌──(zuhra㉿zukhra)-[~]
└─$ while read domain; do dig +short "$domain"; done < zuhra_millatumidi_subdomains.txt > zuhra_millatu
midi_targets.txt

┌──(zuhra㉿zukhra)-[~]
└─$ sudo nano zuhra_millatumidi_subdomains.txt

┌──(zuhra㉿zukhra)-[~]
└─$ sudo nano zuhra_millatumidi_targets.txt

┌──(zuhra㉿zukhra)-[~]
└─$ while read domain; do ip=$(dig +short "$domain" | tail -n1); echo "$domain - $ip"; done < zuhra_mil
latumidi_subdomains.txt > zuhra_millatumidi_targets.txt

┌──(zuhra㉿zukhra)-[~]
└─$ sudo nano zuhra_millatumidi_targets.txt

┌──(zuhra㉿zukhra)-[~]
└─$ sudo nano zuhra_millatumidi_subdomains.txt

┌──(zuhra㉿zukhra)-[~]
└─$
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ cat zuhra_millatumidi_targets.txt
admission.millatumidi.uz - 185.146.3.134
api.admission.millatumidi.uz - 93.170.6.179
api.millatumidi.uz - 93.170.6.43
bot.millatumidi.uz - 84.54.75.249
cloud.millatumidi.uz - 84.54.75.249
conf.millatumidi.uz - 84.54.75.249
control.millatumidi.uz - 84.54.75.249
crm.millatumidi.uz - 84.54.75.249
dev.admission.millatumidi.uz - 93.170.6.43
dev.api.admission.millatumidi.uz - 93.170.6.43
dev.api.millatumidi.uz - 93.170.6.43
dev.millatumidi.uz - 93.170.6.43
dev.my.millatumidi.uz - 93.170.6.43
extra.millatumidi.uz - 84.54.75.249
hp.millatumidi.uz - 84.54.75.249
mail.millatumidi.uz - 84.54.75.249
mik.millatumidi.uz - 84.54.75.249
moodle.millatumidi.uz - 95.47.124.97
new.millatumidi.uz - 93.170.6.43
newmoodle.millatumidi.uz - 84.54.75.249
old.millatumidi.uz - 93.170.6.43
pbx.millatumidi.uz -
proxy.millatumidi.uz - 84.54.75.249
tel.millatumidi.uz - 84.54.75.249
test1.millatumidi.uz - 84.54.75.249
test.millatumidi.uz - 84.54.75.249
tvt.millatumidi.uz - 84.54.75.249
unify.millatumidi.uz - 84.54.75.249
vtiger.millatumidi.uz -
www.millatumidi.uz -
```

```
┌──(zuhra㉿ zukhra)-[~]
└─$ cat zuhra_cambridge_targets.txt
acca.cambridge.uz - 185.215.4.16
autodiscover.cambridge.uz -
back.cambridge.uz - 139.162.133.90
cafe.cambridge.uz - 139.162.133.90
cloud.cambridge.uz - 93.170.6.59
college.cambridge.uz - 143.42.57.191
core.cambridge.uz - 139.162.133.90
cpanel.cambridge.uz -
grand.cambridge.uz - 139.162.133.90
hackathon.cambridge.uz -
hemis.cambridge.uz - 195.158.3.34
mail.cambridge.uz - 95.47.124.45
moodle.cambridge.uz - 95.47.124.97
old.cambridge.uz - 172.104.137.169
samarqand.cambridge.uz - 139.162.133.90
staff.cambridge.uz -
stmail.cambridge.uz - 95.47.127.102
student.cambridge.uz - 195.158.3.34
students.cambridge.uz -
sub.cambridge.uz - 95.47.127.168
test.cambridge.uz - 172.104.137.169
university.cambridge.uz - 93.170.6.43
vebinar.cambridge.uz - 139.162.133.90
webdisk.cambridge.uz -
webmail.cambridge.uz -
www.cambridge.uz - 93.170.6.43
www.college.cambridge.uz -
www.university.cambridge.uz -
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ while read domain; do dig +short "$domain"; done < zuhra_millatumidi_subdomains.txt > zuhra_millatu
midi_ip.txt

┌──(zuhra㉿zukhra)-[~]
└─$ while read domain; do dig +short "$domain"; done < zuhra_cambridge_subdomains.txt > zuhra_cambridge
_ip.txt
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ cat zuhra_cambridge_ip.txt
185.215.4.16
139.162.133.90
139.162.133.90
93.170.6.59
143.42.57.191
139.162.133.90
139.162.133.90
195.158.3.34
95.47.124.45
95.47.124.97
172.104.137.169
139.162.133.90
95.47.127.102
195.158.3.34
95.47.127.168
172.104.137.169
93.170.6.43
139.162.133.90
93.170.6.43

┌──(zuhra㉿zukhra)-[~]
└─$
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ cat zuhra_millatumidi_ip.txt
lb.bitrix24.site.
185.146.3.134
93.170.6.179
93.170.6.43
84.54.75.249
84.54.75.249
93.170.6.59
84.54.75.249
84.54.75.249
84.54.75.249
93.170.6.43
93.170.6.43
93.170.6.43
93.170.6.43
93.170.6.43
84.54.75.249
93.170.6.43
84.54.75.249
84.54.75.249
84.54.75.249
95.47.124.97
93.170.6.43
84.54.75.249
93.170.6.43
84.54.75.249
84.54.75.249
84.54.75.249
84.54.75.249
84.54.75.249
84.54.75.249

┌──(zuhra㉿zukhra)-[~]
└─$
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ nmap -iL zuhra_cambridge_ip.txt --top-ports 16 -oN zuhra_cambridge_ports.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 04:27 EDT
Nmap scan report for 185.215.4.16
Host is up (0.059s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   open     http
110/tcp  filtered pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
8080/tcp filtered http-proxy

Nmap scan report for 139-162-133-90.ip.linodeusercontent.com (139.162.133.90)
Host is up (0.098s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   closed   ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   filtered http
110/tcp  filtered pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ nmap -iL zuhra_cambridge_ip.txt --top-ports 16 --open -oN zuhra_cambridge_open_ports.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 04:49 EDT
Nmap scan report for 185.215.4.16
Host is up (0.057s latency).
Not shown: 14 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 93.170.6.59
Host is up (0.023s latency).
Not shown: 13 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap scan report for 195.158.3.34
Host is up (0.046s latency).
Not shown: 11 filtered tcp ports (no-response), 3 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 45.124.47.95.in-addr.arpa (95.47.124.45)
Host is up (0.045s latency).
Not shown: 10 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https

Nmap scan report for 95.47.124.97
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ nmap -iL zuhra_millatumidi_ip.txt --top-ports 16 --open -oN zuhra_millatumidi_open_ports.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 04:53 EDT
Nmap scan report for lb.bitrix24.site. (185.146.3.134)
Host is up (0.053s latency).
Not shown: 7 filtered tcp ports (host-prohibited), 7 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 93.170.6.179
Host is up (0.014s latency).
Not shown: 11 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 93.170.6.43
Host is up (0.013s latency).
Not shown: 8 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https

Nmap scan report for 84.54.75.249
Host is up (0.014s latency).
Not shown: 11 filtered tcp ports (no-response), 3 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ nmap -iL zuhra_millatumidi_ip.txt --top-ports 16 -oN zuhra_millatumidi_ports.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 04:52 EDT
Nmap scan report for lb.bitrix24.site. (185.146.3.134)
Host is up (0.052s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   open     http
110/tcp  filtered pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
8080/tcp filtered http-proxy

Nmap scan report for 93.170.6.179
Host is up (0.014s latency).

PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   open     domain
80/tcp   open     http
110/tcp  filtered pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
1723/tcp filtered pptp
3306/tcp filtered mysql
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ nmap -iL zuhra_millatumidi_ip.txt -A -oN zuhra_millatumidi_OS.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 05:14 EDT
Nmap scan report for lb.bitrix24.site. (185.146.3.134)
Host is up (0.054s latency).
Not shown: 974 filtered tcp ports (no-response), 23 filtered tcp ports (host-prohibited)
PORT    STATE  SERVICE  VERSION
80/tcp  open   http     OpenResty web app server
|_http-server-header: Bitrix24.Sites
113/tcp closed ident
443/tcp open   ssl/http OpenResty web app server
|_http-title: Bitrix24 account does not exist or has been deleted
| ssl-cert: Subject: commonName=*.bitrix24.site
| Subject Alternative Name: DNS:*.bitrix24.site, DNS:bitrix24.site
| Not valid before: 2024-08-29T17:21:45
|_Not valid after:  2025-09-30T17:21:45
|_http-server-header: Bitrix24.Sites
Aggressive OS guesses: IPFire 2.25 firewall (Linux 4.14) (91%), Linux 3.10 - 3.12 (91%), Linux 4.0
4 (91%), Linux 4.9 (90%), Linux 3.10 (89%), Linux 3.2 - 3.8 (88%), Linux 3.11 - 4.9 (87%), Linux 4.
87%), Linux 4.19 - 5.15 (87%), Linux 4.4 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 18 hops

TRACEROUTE (using port 113/tcp)
HOP RTT      ADDRESS
-   Hops 1-2 are the same as for 84.54.75.249
3   6.25 ms  172.16.243.13 (172.16.243.13)
4   ... 9
10  70.01 ms gw-as35168.retn.net (87.245.230.97)
11  51.66 ms 89.38.167.194
12  52.25 ms 89.38.167.194
13  ... 16
17  51.54 ms 10.226.17.187 (10.226.17.187)
18  53.90 ms 185.146.3.134

Nmap scan report for 93.170.6.179
Host is up (0.015s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE  SERVICE  VERSION
21/tcp    open   ftp      vsftpd 2.0.8 or later
| ssl-cert: Subject: commonName=admission.millatumidi.uz/organizationName=Hestia Control Panel/stat
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ nmap -iL zuhra_cambridge_ip.txt --script vuln -oN zuhra_cambridge_vul.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 06:20 EDT
Nmap scan report for 185.215.4.16
Host is up (0.057s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
|_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.
443/tcp open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

Nmap scan report for 139-162-133-90.ip.linodeusercontent.com (139.162.133.90)
Host is up (0.096s latency).
Not shown: 964 filtered tcp ports (no-response), 35 filtered tcp ports (port-unreach)
PORT   STATE  SERVICE
22/tcp closed ssh

Nmap scan report for 93.170.6.59
Host is up (0.017s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_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.
443/tcp open  https
|_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.

Nmap scan report for 195.158.3.34
Host is up (0.018s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT    STATE  SERVICE
80/tcp  open   http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ dig millatumidi.uz

; <<>> DiG 9.20.4-4-Debian <<>> millatumidi.uz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57661
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ae4f38bcbb9bd09d6dfa332267efc59a7dc908891ba1e4f0 (good)
;; QUESTION SECTION:
;millatumidi.uz.                        IN      A

;; ANSWER SECTION:
millatumidi.uz.         300     IN      A       93.170.6.43

;; AUTHORITY SECTION:
millatumidi.uz.         3606    IN      NS      ns2.linode.com.
millatumidi.uz.         3606    IN      NS      ns4.linode.com.
millatumidi.uz.         3606    IN      NS      ns1.linode.com.
millatumidi.uz.         3606    IN      NS      ns3.linode.com.

;; ADDITIONAL SECTION:
ns1.linode.com.         169782  IN      A       92.123.94.2
ns3.linode.com.         167744  IN      A       92.123.95.3
ns4.linode.com.         167744  IN      A       92.123.95.4
ns2.linode.com.         163719  IN      A       92.123.94.3
ns1.linode.com.         163106  IN      AAAA    2600:14c0:6::2
ns3.linode.com.         146254  IN      AAAA    2600:14c0:7::3
ns4.linode.com.         167744  IN      AAAA    2600:14c0:7::4
ns2.linode.com.         170717  IN      AAAA    2600:14c0:6::3

;; Query time: 136 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Fri Apr 04 07:42:05 EDT 2025
;; MSG SIZE  rcvd: 345
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ nmap -iL zuhra_cambridge_ip.txt -sV \
--script "http-vuln*,ftp-vsftpd-backdoor,smb-vuln*,ssl-enum-ciphers,ssl-cert" \
-oN zuhra_cambridge_vul.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 10:11 EDT
Nmap scan report for 185.215.4.16
Host is up (0.056s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      ddos-guard
| http-server-header:
|   ddos-guard
|_  ngjit
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 400 Bad Request
|     Server: ddos-guard
|     Connection: close
|     Set-Cookie: __ddg8_=w26XO84aYtNZ8mkp; Domain=.; Path=/; Expires=Fri, 04-Apr-2025 14:32:40 GMT
|     Set-Cookie: __ddg10_=1743775960; Domain=.; Path=/; Expires=Fri, 04-Apr-2025 14:32:40 GMT
|     Set-Cookie: __ddg9_=213.230.93.72; Domain=.; Path=/; Expires=Fri, 04-Apr-2025 14:32:40 GMT
|     Set-Cookie: __ddg1_=xrJUiPtnWoVLUDrvNuvq; Domain=.; HttpOnly; Path=/; Expires=Sat, 04-Apr-2026 14:12:4
0 GMT
|     date: Fri, 04 Apr 2025 14:12:40 GMT
|     content-type: text/html
|     x-tilda-server: 27
|     x-tilda-imprint: c7830dad-dd5d-4566-80e2-780d901be96e
|     <!DOCTYPE html><html><head><title>400</title></head><body><center><h1> </h1><h1>400</h1><h2> 
;</h2><pre>Request b4962984188aa1e846ac14851e25a924 with error: 400 - Bad Request</pre></center></body></htm
l>
|   HTTPOptions:
|     HTTP/1.1 400 Bad Request
|     Server: ddos-guard
|     Connection: close
|     Set-Cookie: __ddg8_=PqbKd4uA70KPvlNi; Domain=.; Path=/; Expires=Fri, 04-Apr-2025 14:32:41 GMT
|     Set-Cookie: __ddg10_=1743775961; Domain=.; Path=/; Expires=Fri, 04-Apr-2025 14:32:41 GMT
|     Set-Cookie: __ddg9_=213.230.93.72; Domain=.; Path=/; Expires=Fri, 04-Apr-2025 14:32:41 GMT
|     Set-Cookie: __ddg1_=aXJtxWbjQFpih2aNvsox; Domain=.; HttpOnly; Path=/; Expires=Sat, 04-Apr-2026 14:12:4
1 GMT
|     date: Fri, 04 Apr 2025 14:12:41 GMT
|     content-type: text/html
|     x-tilda-server: 28
|     x-tilda-imprint: 68804f6f-26be-43dc-889d-7deb14bdc0b4
|     <!DOCTYPE html><html><head><title>400</title></head><body><center><h1> </h1><h1>400</h1><h2> 
;</h2><pre>Request 0e55b8629792e197e2c663664382d588 with error: 400 - Bad Request</pre></center></body></htm
l>
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
```

```
┌──(zuhra㉿zukhra)-[~]
└─$ nmap -iL zuhra_millatumidi_ip.txt -sV --script "http-vuln*,ftp-vsftpd-backdoor,smb-vuln*,ssl-enum-ciphers,ssl-cert" -oN zuhra_millatumidi_vul.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 10:46 EDT
Nmap scan report for lb.bitrix24.site. (185.146.3.134)
Host is up (0.054s latency).
Not shown: 980 filtered tcp ports (no-response), 17 filtered tcp ports (host-prohibited)
PORT    STATE  SERVICE  VERSION
80/tcp  open   http     OpenResty web app server
|_http-server-header: Bitrix24.Sites
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
113/tcp closed ident
443/tcp open   ssl/http OpenResty web app server
|_http-server-header: Bitrix24.Sites
| ssl-cert: Subject: commonName=*.bitrix24.site
| Subject Alternative Name: DNS:*.bitrix24.site, DNS:bitrix24.site
| Issuer: commonName=Go Daddy Secure Certificate Authority - G2/organizationName=GoDaddy.com, Inc./stateOrProvinceName=Arizona/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-08-29T17:21:45
| Not valid after:  2025-09-30T17:21:45
| MD5:   1d72:4c33:ae6c:a799:d6e0:db5c:558f:8212
|_SHA-1: 2a1b:c7d7:9066:7a0f:c0fa:a2ab:379e:4614:6791:5487
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (ecdh_x25519) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (ecdh_x25519) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.2:
```