```
The Ip and Ping details here
-----------------------------------
PING scanme.nmap.org (45.33.32.156) 56(84) bytes of data.
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=1 ttl=128 time=287 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=2 ttl=128 time=286 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=3 ttl=128 time=295 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=4 ttl=128 time=357 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=5 ttl=128 time=313 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=6 ttl=128 time=296 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=7 ttl=128 time=419 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=8 ttl=128 time=475 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=9 ttl=128 time=307 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=10 ttl=128 time=285 ms

--- scanme.nmap.org ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9019ms
rtt min/avg/max/mdev = 284.644/331.784/475.002/62.337 ms


The open ports are
-----------------------------------
22
80
443


The Services and Versions are
-----------------------------------
ssh
http
https


The found directories are
-----------------------------------
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.28.44
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                gobuster/wordlist.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/12/14 13:51:09 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 234] [--> http://10.10.28.44/images/]
/blog                 (Status: 301) [Size: 232] [--> http://10.10.28.44/blog/]
/sitemap              (Status: 200) [Size: 0]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.28.44/feed/]
/login                (Status: 302) [Size: 0] [--> http://10.10.28.44/wp-login.php]

[!] Keyboard interrupt detected, terminating.
===============================================================
2021/12/14 13:52:05 Finished
===============================================================


The emails are
-----------------------------------
```

```
table results already exists

\033[93m************************************************************************
*  _   _                                            _                        *
* | |_| |__   ___    /\  /\__ _ _ _____   _____  ___| |_ ___ _ __  _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| '_ \| |  *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    | | | |  *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    |_| |_|  *
*                                                                          *
* theHarvester 3.1.0                                        *
* Coded by Christian Martorella                                            *
* Edge-Security Research                                                   *
* cmartorella@edge-security.com                                            *
*                                                                          *
****************************************************************************

 \033[0m
\033[94m[*] Target: nu.edu.pk
 \033[0m
\033[94m[*] Searching Google. \033[0m
        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
        Searching 300 results.
        Searching 400 results.
        Searching 500 results.

[*] No IPs found.

[*] Emails found: 7
----------------------
abdul.aziz@nu.edu.pk
k070064@nu.edu.pk
last@nu.edu.pk
mubashra.fayyaz@nu.edu.pk
muhammad.asim@nu.edu.pk
muneeb.aadil@nu.edu.pk
zulfiqar.ali@nu.edu.pk

[*] Hosts found: 11
---------------------
admissions.nu.edu.pk:203.124.45.203
fast-nu-www.nu.edu.pk:
flexstudent.nu.edu.pk:210.56.9.82
isb.nu.edu.pk:66.219.22.238
khi.nu.edu.pk:166.62.27.185
lhr.nu.edu.pk:68.66.205.190
slate.nu.edu.pk:210.56.27.170
www.nu.edu.pk:203.124.43.201
x3ekhi.nu.edu.pk:
x3elhr.nu.edu.pk:


The web technologies used are  are
--------------------------------------
WhatWeb report for http://10.10.28.44
Status    : 200 OK
Title     : <None>
IP        : 10.10.28.44
Country   : RESERVED, ZZ

Summary   : Apache, X-Frame-Options[SAMEORIGIN], Script, HTTPServer[Apache], UncommonHeaders[x
-mod-pagespeed], HTML5
```

Detected Plugins:
[Apache]
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Google Dorks: (3)
Website : http://httpd.apache.org/

[HTML5]
HTML version 5, detected by the doctype declaration

[HTTPServer]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.

String : Apache (from server string)

[Script]
This plugin detects instances of script HTML elements and returns the script language/type.

[UncommonHeaders]
Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version. Info about headers can be found at www.http-stats.com

String : x-mod-pagespeed (from headers)

[X-Frame-Options]
This plugin retrieves the X-Frame-Options value from the HTTP header. - More Info:
http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx

String : SAMEORIGIN

HTTP Headers:
HTTP/1.1 200 OK
Date: Tue, 14 Dec 2021 18:54:20 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
Vary: Accept-Encoding
X-Mod-Pagespeed: 1.9.32.3-4523
Content-Encoding: gzip
Cache-Control: max-age=0, no-cache
Content-Length: 677
Connection: close
Content-Type: text/html

The result of robots.txt

```
User-agent: *
fsocity.dic
key-1-of-3.txt


The result of sitemap.xml
---------------------------------------


The subdomains are
---------------------------------------
www.nu.edu.pk
admissions.nu.edu.pk
apply.nu.edu.pk
cfd.nu.edu.pk
www.cfd.nu.edu.pk
autodiscover.cfd.nu.edu.pk
cpanel.cfd.nu.edu.pk
dev.cfd.nu.edu.pk
www.dev.cfd.nu.edu.pk
mail.cfd.nu.edu.pk
staging.cfd.nu.edu.pk
www.staging.cfd.nu.edu.pk
webdisk.cfd.nu.edu.pk
webmail.cfd.nu.edu.pk
cifb.nu.edu.pk
daira.nu.edu.pk
fan.nu.edu.pk
www.fan.nu.edu.pk
flex.nu.edu.pk
www.flex.nu.edu.pk
flexstudent.nu.edu.pk
fsd.nu.edu.pk
www.fsd.nu.edu.pk
autodiscover.fsd.nu.edu.pk
cpanel.fsd.nu.edu.pk
mail.fsd.nu.edu.pk
webdisk.fsd.nu.edu.pk
webmail.fsd.nu.edu.pk
fsmlhr.nu.edu.pk
icet.nu.edu.pk
www.icet.nu.edu.pk
isb.nu.edu.pk
www.isb.nu.edu.pk
cpanel.isb.nu.edu.pk
cpcalendars.isb.nu.edu.pk
cpcontacts.isb.nu.edu.pk
fcs.isb.nu.edu.pk
www.fcs.isb.nu.edu.pk
mail.fcs.isb.nu.edu.pk
ieee.isb.nu.edu.pk
www.ieee.isb.nu.edu.pk
mail.ieee.isb.nu.edu.pk
mail.isb.nu.edu.pk
webdisk.isb.nu.edu.pk
webmail.isb.nu.edu.pk
khi.nu.edu.pk
www.khi.nu.edu.pk
acm.khi.nu.edu.pk
www.acm.khi.nu.edu.pk
coderscup.acm.khi.nu.edu.pk
www.coderscup.acm.khi.nu.edu.pk
cpanel.acm.khi.nu.edu.pk
```

developersday.acm.khi.nu.edu.pk
www.developersday.acm.khi.nu.edu.pk
gearup.acm.khi.nu.edu.pk
www.gearup.acm.khi.nu.edu.pk
hackathon.acm.khi.nu.edu.pk
www.hackathon.acm.khi.nu.edu.pk
mail.acm.khi.nu.edu.pk
mobileapps.acm.khi.nu.edu.pk
www.mobileapps.acm.khi.nu.edu.pk
nabil.acm.khi.nu.edu.pk
www.nabil.acm.khi.nu.edu.pk
qoverflow.acm.khi.nu.edu.pk
www.qoverflow.acm.khi.nu.edu.pk
speedtracker.acm.khi.nu.edu.pk
www.speedtracker.acm.khi.nu.edu.pk
webdisk.acm.khi.nu.edu.pk
webmail.acm.khi.nu.edu.pk
autodiscover.khi.nu.edu.pk
beta.khi.nu.edu.pk
www.beta.khi.nu.edu.pk
betakhi.khi.nu.edu.pk
www.betakhi.khi.nu.edu.pk
buddy.khi.nu.edu.pk
www.buddy.khi.nu.edu.pk
autodiscover.buddy.khi.nu.edu.pk
cpanel.buddy.khi.nu.edu.pk
mail.buddy.khi.nu.edu.pk
webdisk.buddy.khi.nu.edu.pk
webmail.buddy.khi.nu.edu.pk
cpanel.khi.nu.edu.pk
cpcalendars.khi.nu.edu.pk
cpcontacts.khi.nu.edu.pk
cpt.khi.nu.edu.pk
www.cpt.khi.nu.edu.pk
autodiscover.cpt.khi.nu.edu.pk
cpanel.cpt.khi.nu.edu.pk
mail.cpt.khi.nu.edu.pk
webdisk.cpt.khi.nu.edu.pk
webmail.cpt.khi.nu.edu.pk
crais.khi.nu.edu.pk
www.crais.khi.nu.edu.pk
mail.crais.khi.nu.edu.pk
datascience.khi.nu.edu.pk
www.datascience.khi.nu.edu.pk
autodiscover.datascience.khi.nu.edu.pk
cpanel.datascience.khi.nu.edu.pk
mail.datascience.khi.nu.edu.pk
webdisk.datascience.khi.nu.edu.pk
webmail.datascience.khi.nu.edu.pk
decs.khi.nu.edu.pk
www.decs.khi.nu.edu.pk
autodiscover.decs.khi.nu.edu.pk
cpanel.decs.khi.nu.edu.pk
mail.decs.khi.nu.edu.pk
webdisk.decs.khi.nu.edu.pk
webmail.decs.khi.nu.edu.pk
desc.khi.nu.edu.pk
www.desc.khi.nu.edu.pk
devday.khi.nu.edu.pk
www.devday.khi.nu.edu.pk
devsoc.khi.nu.edu.pk
www.devsoc.khi.nu.edu.pk
application.devsoc.khi.nu.edu.pk

www.application.devsoc.khi.nu.edu.pk
autodiscover.devsoc.khi.nu.edu.pk
cpanel.devsoc.khi.nu.edu.pk
feedback.devsoc.khi.nu.edu.pk
www.feedback.devsoc.khi.nu.edu.pk
files.devsoc.khi.nu.edu.pk
www.files.devsoc.khi.nu.edu.pk
hci.devsoc.khi.nu.edu.pk
www.hci.devsoc.khi.nu.edu.pk
mail.devsoc.khi.nu.edu.pk
webdisk.devsoc.khi.nu.edu.pk
webmail.devsoc.khi.nu.edu.pk
workshop.devsoc.khi.nu.edu.pk
www.workshop.devsoc.khi.nu.edu.pk
fpc.khi.nu.edu.pk
www.fpc.khi.nu.edu.pk
autodiscover.fpc.khi.nu.edu.pk
cpanel.fpc.khi.nu.edu.pk
mail.fpc.khi.nu.edu.pk
webdisk.fpc.khi.nu.edu.pk
webmail.fpc.khi.nu.edu.pk
fsm.khi.nu.edu.pk
www.fsm.khi.nu.edu.pk
fyp.khi.nu.edu.pk
www.fyp.khi.nu.edu.pk
autodiscover.fyp.khi.nu.edu.pk
cpanel.fyp.khi.nu.edu.pk
mail.fyp.khi.nu.edu.pk
vdl.fyp.khi.nu.edu.pk
www.vdl.fyp.khi.nu.edu.pk
autodiscover.vdl.fyp.khi.nu.edu.pk
cpanel.vdl.fyp.khi.nu.edu.pk
mail.vdl.fyp.khi.nu.edu.pk
webdisk.vdl.fyp.khi.nu.edu.pk
webmail.vdl.fyp.khi.nu.edu.pk
webdisk.fyp.khi.nu.edu.pk
webmail.fyp.khi.nu.edu.pk
graduates.khi.nu.edu.pk
www.graduates.khi.nu.edu.pk
autodiscover.graduates.khi.nu.edu.pk
cpanel.graduates.khi.nu.edu.pk
mail.graduates.khi.nu.edu.pk
moocs.graduates.khi.nu.edu.pk
www.moocs.graduates.khi.nu.edu.pk
webdisk.graduates.khi.nu.edu.pk
webmail.graduates.khi.nu.edu.pk
icetst.khi.nu.edu.pk
www.icetst.khi.nu.edu.pk
ieee.khi.nu.edu.pk
www.ieee.khi.nu.edu.pk
autodiscover.ieee.khi.nu.edu.pk
cpanel.ieee.khi.nu.edu.pk
mail.ieee.khi.nu.edu.pk
webdisk.ieee.khi.nu.edu.pk
webmail.ieee.khi.nu.edu.pk
intellinet.khi.nu.edu.pk
www.intellinet.khi.nu.edu.pk
autodiscover.intellinet.khi.nu.edu.pk
cpanel.intellinet.khi.nu.edu.pk
intellinet.intellinet.khi.nu.edu.pk
www.intellinet.intellinet.khi.nu.edu.pk
webdisk.intellinet.khi.nu.edu.pk
webmail.intellinet.khi.nu.edu.pk

it.khi.nu.edu.pk
www.it.khi.nu.edu.pk
jobs.khi.nu.edu.pk
www.jobs.khi.nu.edu.pk
lib.khi.nu.edu.pk
www.lib.khi.nu.edu.pk
lost.khi.nu.edu.pk
www.lost.khi.nu.edu.pk
autodiscover.lost.khi.nu.edu.pk
cpanel.lost.khi.nu.edu.pk
mail.lost.khi.nu.edu.pk
webdisk.lost.khi.nu.edu.pk
webmail.lost.khi.nu.edu.pk
mail.khi.nu.edu.pk
maps.khi.nu.edu.pk
www.maps.khi.nu.edu.pk
autodiscover.maps.khi.nu.edu.pk
cpanel.maps.khi.nu.edu.pk
mail.maps.khi.nu.edu.pk
webdisk.maps.khi.nu.edu.pk
webmail.maps.khi.nu.edu.pk
nuprocom.khi.nu.edu.pk
www.nuprocom.khi.nu.edu.pk
research.khi.nu.edu.pk
www.research.khi.nu.edu.pk
riddle.khi.nu.edu.pk
www.riddle.khi.nu.edu.pk
autodiscover.riddle.khi.nu.edu.pk
cpanel.riddle.khi.nu.edu.pk
mail.riddle.khi.nu.edu.pk
webdisk.riddle.khi.nu.edu.pk
webmail.riddle.khi.nu.edu.pk
rwd.khi.nu.edu.pk
www.rwd.khi.nu.edu.pk
sdn.khi.nu.edu.pk
www.sdn.khi.nu.edu.pk
autodiscover.sdn.khi.nu.edu.pk
cpanel.sdn.khi.nu.edu.pk
mail.sdn.khi.nu.edu.pk
webdisk.sdn.khi.nu.edu.pk
webmail.sdn.khi.nu.edu.pk
sibss.khi.nu.edu.pk
www.sibss.khi.nu.edu.pk
autodiscover.sibss.khi.nu.edu.pk
cpanel.sibss.khi.nu.edu.pk
mail.sibss.khi.nu.edu.pk
webdisk.sibss.khi.nu.edu.pk
webmail.sibss.khi.nu.edu.pk
sportics.khi.nu.edu.pk
www.sportics.khi.nu.edu.pk
autodiscover.sportics.khi.nu.edu.pk
cpanel.sportics.khi.nu.edu.pk
mail.sportics.khi.nu.edu.pk
webdisk.sportics.khi.nu.edu.pk
webmail.sportics.khi.nu.edu.pk
syslab.khi.nu.edu.pk
www.syslab.khi.nu.edu.pk
autodiscover.syslab.khi.nu.edu.pk
cpanel.syslab.khi.nu.edu.pk
mail.syslab.khi.nu.edu.pk
webdisk.syslab.khi.nu.edu.pk
webmail.syslab.khi.nu.edu.pk
tlc.khi.nu.edu.pk

www.tlc.khi.nu.edu.pk
autodiscover.tlc.khi.nu.edu.pk
cpanel.tlc.khi.nu.edu.pk
mail.tlc.khi.nu.edu.pk
webdisk.tlc.khi.nu.edu.pk
webmail.tlc.khi.nu.edu.pk
tnc.khi.nu.edu.pk
www.tnc.khi.nu.edu.pk
autodiscover.tnc.khi.nu.edu.pk
cpanel.tnc.khi.nu.edu.pk
fasttech.tnc.khi.nu.edu.pk
www.fasttech.tnc.khi.nu.edu.pk
mail.tnc.khi.nu.edu.pk
webdisk.tnc.khi.nu.edu.pk
webmail.tnc.khi.nu.edu.pk
twm.khi.nu.edu.pk
www.twm.khi.nu.edu.pk
webdisk.khi.nu.edu.pk
webmail.khi.nu.edu.pk
webmasters.khi.nu.edu.pk
www.webmasters.khi.nu.edu.pk
autodiscover.webmasters.khi.nu.edu.pk
cpanel.webmasters.khi.nu.edu.pk
mail.webmasters.khi.nu.edu.pk
riddles.webmasters.khi.nu.edu.pk
www.riddles.webmasters.khi.nu.edu.pk
webdisk.webmasters.khi.nu.edu.pk
webmail.webmasters.khi.nu.edu.pk
whm.khi.nu.edu.pk
lhr.nu.edu.pk
mail.lhr.nu.edu.pk
mail.nu.edu.pk
neonofficeisb.nu.edu.pk
neonofficekhi.nu.edu.pk
neonofficelhr.nu.edu.pk
neonofficepwr.nu.edu.pk
pwr.nu.edu.pk
www.pwr.nu.edu.pk
acm.pwr.nu.edu.pk
www.acm.pwr.nu.edu.pk
ieee.pwr.nu.edu.pk
www.ieee.pwr.nu.edu.pk
mail.pwr.nu.edu.pk
nutec.pwr.nu.edu.pk
www.nutec.pwr.nu.edu.pk
slate.nu.edu.pk
slateisb.nu.edu.pk
student.nu.edu.pk

The whois Data is

Domain Name: GLOCKIA.COM
Registry Domain ID: 2171100659_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.onlinenic.com
Registrar URL: http://www.onlinenic.com
Updated Date: 2021-10-09T23:04:40Z
Creation Date: 2017-10-06T10:12:43Z
Registry Expiry Date: 2022-10-06T10:12:43Z
Registrar: OnlineNIC, Inc.
Registrar IANA ID: 82
Registrar Abuse Contact Email: abuse@onlinenic.com
Registrar Abuse Contact Phone: +1 833-678-1173

```
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.REDMONDDC.COM
   Name Server: NS2.REDMONDDC.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-12-14T07:33:26Z <<<
Domain Name: glockia.com

Registry Domain ID: 2171100659_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.onlinenic.com
Registrar URL: http://www.onlinenic.com
Updated Date: 2021-10-09T19:04:33Z
Creation Date: 2017-10-06T04:00:00Z
Registrar Registration Expiration Date: 2022-10-06T04:00:00Z
Registrar: Onlinenic Inc
Registrar IANA ID: 82
Registrar Abuse Contact Email: abuse@onlinenic.com
Registrar Abuse Contact Phone: +1.5107698492
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Zeeshan Qaiser
Registrant Organization: Trading Icons
Registrant Street: House no. 75 Street no. 5 Gulraiz Phase 3,
Registrant City: Rawalpindi
Registrant State/Province: Punjab
Registrant Postal Code: 46000
Registrant Country: PK
Registrant Phone: +92.03212366699
Registrant Phone Ext:
Registrant Fax: +92.03212366699
Registrant Fax Ext:
Registrant Email: zeeshanqaiser1@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Zeeshan Qaiser
Admin Organization: Trading Icons
Admin Street: House no. 75 Street no. 5 Gulraiz Phase 3,
Admin City: Rawalpindi
Admin State/Province: Punjab
Admin Postal Code: 46000
Admin Country: PK
Admin Phone: +92.03212366699
Admin Phone Ext:
Admin Fax: +92.03212366699
Admin Fax Ext:
Admin Email: zeeshanqaiser1@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: Zeeshan Qaiser
Tech Organization: Trading Icons
Tech Street: House no. 75 Street no. 5 Gulraiz Phase 3,
Tech City: Rawalpindi
Tech State/Province: Punjab
Tech Postal Code: 46000
Tech Country: PK
Tech Phone: +92.03212366699
Tech Phone Ext:
Tech Fax: +92.03212366699
Tech Fax Ext:
Tech Email: zeeshanqaiser1@gmail.com
Name Server: ns1.redmonddc.com
Name Server: ns2.redmonddc.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-10-09T19:04:33Z <<<
```

The possible vulnerabilities are

```
------------------------------------
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
---------------------------------- ------------------------------------------
 Exploit Title

                                   |  URL
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
---------------------------------- ------------------------------------------
Adaware Web Companion version 4.8.2078.3950 - 'WCAssistantService' Unquoted Service Path

                                   | https://www.exploit-db.com/exploits/47597
Adobe Flash - Out-of-Bounds Read in UTF Conversion

                                   | https://www.exploit-db.com/exploits/37862
Adobe Flash Player 9/10 - SWF Version Null Pointer Dereference Denial of Service

                                   | https://www.exploit-db.com/exploits/32452
Adobe Shockwave - 'ShockwaveVersion()' Stack Overflow (PoC)

                                   | https://www.exploit-db.com/exploits/4613
Adobe Version Cue 1.0/1.0.1 (OSX) - '-lib' Local Privilege Escalation

                                   | https://www.exploit-db.com/exploits/1186
Adobe Version Cue 1.0/1.0.1 (OSX) - Local Privilege Escalation

                                   | https://www.exploit-db.com/exploits/1185
Alibaba Clone Diamond Version - SQL Injection

                                   | https://www.exploit-db.com/exploits/12544
Alibaba Clone Tritanium Version - 'news_desc.html' SQL Injection

                                   | https://www.exploit-db.com/exploits/27605
Apache Subversion - Remote Denial of Service

                                   | https://www.exploit-db.com/exploits/38422
Apache Subversion 1.6.x - 'mod_dav_svn/lock.c' Remote Denial of Service

                                   | https://www.exploit-db.com/exploits/38421
Apache UNO / LibreOffice Version: 6.1.2 / OpenOffice 4.1.6 API - Remote Code Execution

                                   | https://www.exploit-db.com/exploits/46544
Apple Mac OSX Adobe Version Cue - Local Privilege Escalation (Bash)

                                   | https://www.exploit-db.com/exploits/680
Apple Mac OSX Adobe Version Cue - Local Privilege Escalation (Perl)

                                   | https://www.exploit-db.com/exploits/795
Apple QuickTime /w IE .qtl Version XAS - Remote

                                   | https://www.exploit-db.com/exploits/4424
Asn Guestbook 1.5 - 'footer.php?version' Cross-Site Scripting

                                   | https://www.exploit-db.com/exploits/26021
Asn Guestbook 1.5 - 'header.php?version' Cross-Site Scripting

                                   | https://www.exploit-db.com/exploits/26020
ASPPortal Free Version - 'Topic_Id' SQL Injection
```

| https://www.exploit-db.com/exploits/5775
Betsy CMS versions 3.5 - Local File Inclusion

| https://www.exploit-db.com/exploits/10189
Centrinity FirstClass HTTP Server 5.50/5.77/7.0/7.1 - Long Version Field Denial of Service

| https://www.exploit-db.com/exploits/23234
CLUB-Nuke [XP] 2.0 LCID 2048 (Turkish Version) - SQL Injection

| https://www.exploit-db.com/exploits/2150
CollabNet Subversion Edge Log Parser - HTML Injection

| https://www.exploit-db.com/exploits/34691
CollabNet Subversion Edge Management 4.0.11 - Local File Inclusion

| https://www.exploit-db.com/exploits/37442
CP3 Studio PC Version - Denial of Service

| https://www.exploit-db.com/exploits/13838
Crystal Reports CrystalPrintControl - ActiveX ServerResourceVersion Property Overflow (Metaspl
oit)
| https://www.exploit-db.com/exploits/23472
Downline Goldmine paidversion - SQL Injection

| https://www.exploit-db.com/exploits/6950
eWebeditor ASP Version - Multiple Vulnerabilities

| https://www.exploit-db.com/exploits/11295
file upload Ar Version - Arbitrary File Upload

| https://www.exploit-db.com/exploits/10689
FileCOPA FTP Server (Pre 18 Jul Version) - 'LIST' Remote Buffer Overflow (Metasploit)

| https://www.exploit-db.com/exploits/16733
Foxit Products GIF Conversion - 'DataSubBlock' Memory Corruption

| https://www.exploit-db.com/exploits/36335
Foxit Products GIF Conversion - 'LZWMinimumCodeSize' Memory Corruption

| https://www.exploit-db.com/exploits/36334
Foxit Reader - '.png' Conversion Parsing tEXt Chunk Arbitrary Code Execution

| https://www.exploit-db.com/exploits/37699
Gbook MX 4.1.0 (Arabic Version) - Remote File Inclusion

| https://www.exploit-db.com/exploits/10986
GNU UnRTF 0.19.3 - Font Table Conversion Buffer Overflow

| https://www.exploit-db.com/exploits/25030
Google Android - libutils UTF16 to UTF8 Conversion Heap Buffer Overflow

| https://www.exploit-db.com/exploits/40354
Hikvision IP Camera versions 5.2.0 - 5.3.9 (Builds 140721 < 170109) - Access Control Bypass

| https://www.exploit-db.com/exploits/44328
HTML2HDML 1.0.3 - File Conversion Buffer Overflow

| https://www.exploit-db.com/exploits/25011
IBM DB2 DTS To String Conversion - Denial of Service

| https://www.exploit-db.com/exploits/24677
iOS < 12.2 / macOS < 10.14.4 XNU - pidversion Increment During execve is Unsafe

| https://www.exploit-db.com/exploits/46648
JaWiki - 'versionNo' Cross-Site Scripting

| https://www.exploit-db.com/exploits/36828
Joomla! Component com_versioning - SQL Injection

| https://www.exploit-db.com/exploits/17264
Joomla! Component versioning 1.0.2 - 'id' SQL Injection

| https://www.exploit-db.com/exploits/5989
Joomla! Convert Forms version 2.0.3 - Formula Injection (CSV Injection)

| https://www.exploit-db.com/exploits/44447
KioWare Server Version 4.9.6 - Weak Folder Permissions Privilege Escalation

| https://www.exploit-db.com/exploits/46093
Live For Speed 2 Version Z - '.Mpr' Local Buffer Overflow

| https://www.exploit-db.com/exploits/9142
Live For Speed 2 Version Z - '.mpr' Local Buffer Overflow (SEH)

| https://www.exploit-db.com/exploits/9148
LocatePC 1.05 (Ligatt Version + Others) - SQL Injection

| https://www.exploit-db.com/exploits/16152
Microsoft ASP.NET 1.0/1.1 - Unicode Character Conversion Multiple Cross-Site Scripting Vulnera
bilities
| https://www.exploit-db.com/exploits/25110
Microsoft IIS 2.0/3.0/4.0 - ISAPI GetExtensionVersion()

| https://www.exploit-db.com/exploits/19376
Microsoft Windows - Path Conversion

| https://www.exploit-db.com/exploits/27851
Microsoft Windows Media Player 11 - '.AVI' File Colorspace Conversion Remote Memory Corruption

| https://www.exploit-db.com/exploits/33770
Mono 1.0.5 - Unicode Character Conversion Multiple Cross-Site Scripting Vulnerabilities

| https://www.exploit-db.com/exploits/25148
Mozilla Firefox 3.5.3 - Floating Point Conversion Heap Overflow

| https://www.exploit-db.com/exploits/33312
Mozilla Suite/Firefox - InstallVersion->compareTo() Code Execution (Metasploit)

| https://www.exploit-db.com/exploits/16306
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Vers
ions)
| https://www.exploit-db.com/exploits/32764
Opera 6.0.1 / Microsoft Internet Explorer 5/6 - JavaScript Modifier Keypress Event Subversion

| https://www.exploit-db.com/exploits/21636
Orbit Downloader - URL Unicode Conversion Overflow (Metasploit)

| https://www.exploit-db.com/exploits/18515
Paintshop Pro X7 - '.gif' Conversion Heap Memory Corruption 'LZWMinimumCodeSize' (Denial of Se
rvice)
| https://www.exploit-db.com/exploits/37346
Phaos R4000 Version - 'file' Remote File Disclosure

| https://www.exploit-db.com/exploits/5420
Phorum 5.2 - 'versioncheck.php?upgrade_available' Cross-Site Scripting

| https://www.exploit-db.com/exploits/32913
PostgreSQL 8.3.6 - Conversion Encoding Remote Denial of Service

| https://www.exploit-db.com/exploits/32849
Prime95 Version 29.8 build 6 - Buffer Overflow (SEH)

| https://www.exploit-db.com/exploits/47802
Pserv 2.0 - HTTP Version Specifier Buffer Overflow

| https://www.exploit-db.com/exploits/22056
RealNetworks RealPlayer 16.0.3.51/16.0.2.32 - '.rmp' Version Attribute Buffer Overflow

| https://www.exploit-db.com/exploits/30468
sCssBoard (Multiple Versions) - 'pwnpack' Remote s

| https://www.exploit-db.com/exploits/5149
SeedDMS versions < 5.1.11 - Remote Command Execution

| https://www.exploit-db.com/exploits/47022
Shopping Portal ProVersion 3.0 - Authentication Bypass

| https://www.exploit-db.com/exploits/47834
Site-Assistant 0990 - 'paths[version]' Remote File Inclusion

| https://www.exploit-db.com/exploits/3285
Skulltag 0.96f - Version String Remote Format String (PoC)

| https://www.exploit-db.com/exploits/1708
Solaris/Open Solaris UCODE_GET_VERSION IOCTL - Denial of Service

| https://www.exploit-db.com/exploits/11351
Squid < 3.1 5 - HTTP Version Number Parsing Denial of Service

| https://www.exploit-db.com/exploits/8021
Subversion - Date Svnserve (Metasploit)

| https://www.exploit-db.com/exploits/16284
Subversion 0.3.7/1.0.0 - Remote Buffer Overflow

| https://www.exploit-db.com/exploits/4537
Subversion 1.0.2 - 'svn_time_from_cstring()' Remote Overflow

| https://www.exploit-db.com/exploits/304
Subversion 1.0.2 - Date Overflow (Metasploit)

| https://www.exploit-db.com/exploits/9935
Subversion 1.6.6/1.6.12 - Code Execution

| https://www.exploit-db.com/exploits/40507
Sun Java Applet 1.x - Invocation Version Specification

| https://www.exploit-db.com/exploits/24778
ta3arof [dating] Script (Arabic Version) - Arbitrary File Upload

| https://www.exploit-db.com/exploits/10718
Titan FTP Server Version 2019 Build 3505 - Directory Traversal / Local File Inclusion

| https://www.exploit-db.com/exploits/46611
Ublog access version - Arbitrary Database Disclosure

| https://www.exploit-db.com/exploits/8610
Web Companion versions 5.1.1035.1047 - 'WCAssistantService' Unquoted Service Path

| https://www.exploit-db.com/exploits/47522
WU-FTPD 2.4.2/2.5 .0/2.6.0/2.6.1/2.6.2 - FTP Conversion

| https://www.exploit-db.com/exploits/20563
Yahoo! Widget < 4.0.5 - 'GetComponentVersion()' Remote Overflow

| https://www.exploit-db.com/exploits/4250
Zimplit CMS - 'English_manual_version_2.php?client' Cross-Site Scripting

| https://www.exploit-db.com/exploits/35064

--- ---

--- ---
Shellcode Title

| URL

--- ---
iOS Version-independent - Null-Free Shellcode

| https://www.exploit-db.com/shellcodes/13290

--- ---

--- ---
Exploit Title

| URL

--- ---
Adaware Web Companion version 4.8.2078.3950 - 'WCAssistantService' Unquoted Service Path

| https://www.exploit-db.com/exploits/47597
Adobe Flash - Out-of-Bounds Read in UTF Conversion

| https://www.exploit-db.com/exploits/37862
Adobe Flash Player 9/10 - SWF Version Null Pointer Dereference Denial of Service

| https://www.exploit-db.com/exploits/32452
Adobe Shockwave - 'ShockwaveVersion()' Stack Overflow (PoC)

| https://www.exploit-db.com/exploits/4613
Adobe Version Cue 1.0/1.0.1 (OSX) - '-lib' Local Privilege Escalation

| https://www.exploit-db.com/exploits/1186
Adobe Version Cue 1.0/1.0.1 (OSX) - Local Privilege Escalation

| https://www.exploit-db.com/exploits/1185
Alibaba Clone Diamond Version - SQL Injection

| https://www.exploit-db.com/exploits/12544
Alibaba Clone Tritanium Version - 'news_desc.html' SQL Injection

| https://www.exploit-db.com/exploits/27605
Apache Subversion - Remote Denial of Service

| https://www.exploit-db.com/exploits/38422
Apache Subversion 1.6.x - 'mod_dav_svn/lock.c' Remote Denial of Service

| https://www.exploit-db.com/exploits/38421
Apache UNO / LibreOffice Version: 6.1.2 / OpenOffice 4.1.6 API - Remote Code Execution

| https://www.exploit-db.com/exploits/46544
Apple Mac OSX Adobe Version Cue - Local Privilege Escalation (Bash)

| https://www.exploit-db.com/exploits/680
Apple Mac OSX Adobe Version Cue - Local Privilege Escalation (Perl)

| https://www.exploit-db.com/exploits/795
Apple QuickTime /w IE .qtl Version XAS - Remote

| https://www.exploit-db.com/exploits/4424
Asn Guestbook 1.5 - 'footer.php?version' Cross-Site Scripting

| https://www.exploit-db.com/exploits/26021
Asn Guestbook 1.5 - 'header.php?version' Cross-Site Scripting

| https://www.exploit-db.com/exploits/26020
ASPPortal Free Version - 'Topic_Id' SQL Injection

| https://www.exploit-db.com/exploits/5775
Betsy CMS versions 3.5 - Local File Inclusion

| https://www.exploit-db.com/exploits/10189
Centrinity FirstClass HTTP Server 5.50/5.77/7.0/7.1 - Long Version Field Denial of Service

| https://www.exploit-db.com/exploits/23234
CLUB-Nuke [XP] 2.0 LCID 2048 (Turkish Version) - SQL Injection

| https://www.exploit-db.com/exploits/2150
CollabNet Subversion Edge Log Parser - HTML Injection

| https://www.exploit-db.com/exploits/34691
CollabNet Subversion Edge Management 4.0.11 - Local File Inclusion

| https://www.exploit-db.com/exploits/37442
CP3 Studio PC Version - Denial of Service

| https://www.exploit-db.com/exploits/13838
Crystal Reports CrystalPrintControl - ActiveX ServerResourceVersion Property Overflow (Metaspl
oit)

| https://www.exploit-db.com/exploits/23472
Downline Goldmine paidversion - SQL Injection

| https://www.exploit-db.com/exploits/6950
eWebeditor ASP Version - Multiple Vulnerabilities

| https://www.exploit-db.com/exploits/11295
file upload Ar Version - Arbitrary File Upload

| https://www.exploit-db.com/exploits/10689
FileCOPA FTP Server (Pre 18 Jul Version) - 'LIST' Remote Buffer Overflow (Metasploit)

| https://www.exploit-db.com/exploits/16733
Foxit Products GIF Conversion - 'DataSubBlock' Memory Corruption

| https://www.exploit-db.com/exploits/36335
Foxit Products GIF Conversion - 'LZWMinimumCodeSize' Memory Corruption

| https://www.exploit-db.com/exploits/36334
Foxit Reader - '.png' Conversion Parsing tEXt Chunk Arbitrary Code Execution

| https://www.exploit-db.com/exploits/37699
Gbook MX 4.1.0 (Arabic Version) - Remote File Inclusion

| https://www.exploit-db.com/exploits/10986
GNU UnRTF 0.19.3 - Font Table Conversion Buffer Overflow

| https://www.exploit-db.com/exploits/25030
Google Android - libutils UTF16 to UTF8 Conversion Heap Buffer Overflow

| https://www.exploit-db.com/exploits/40354
Hikvision IP Camera versions 5.2.0 - 5.3.9 (Builds 140721 < 170109) - Access Control Bypass

| https://www.exploit-db.com/exploits/44328
HTML2HDML 1.0.3 - File Conversion Buffer Overflow

| https://www.exploit-db.com/exploits/25011
IBM DB2 DTS To String Conversion - Denial of Service

| https://www.exploit-db.com/exploits/24677
iOS < 12.2 / macOS < 10.14.4 XNU - pidversion Increment During execve is Unsafe

| https://www.exploit-db.com/exploits/46648
JaWiki - 'versionNo' Cross-Site Scripting

| https://www.exploit-db.com/exploits/36828
Joomla! Component com_versioning - SQL Injection

| https://www.exploit-db.com/exploits/17264
Joomla! Component versioning 1.0.2 - 'id' SQL Injection

| https://www.exploit-db.com/exploits/5989
Joomla! Convert Forms version 2.0.3 - Formula Injection (CSV Injection)

| https://www.exploit-db.com/exploits/44447
KioWare Server Version 4.9.6 - Weak Folder Permissions Privilege Escalation

| https://www.exploit-db.com/exploits/46093
Live For Speed 2 Version Z - '.Mpr' Local Buffer Overflow

| https://www.exploit-db.com/exploits/9142
Live For Speed 2 Version Z - '.mpr' Local Buffer Overflow (SEH)

| https://www.exploit-db.com/exploits/9148
LocatePC 1.05 (Ligatt Version + Others) - SQL Injection

| https://www.exploit-db.com/exploits/16152
Microsoft ASP.NET 1.0/1.1 - Unicode Character Conversion Multiple Cross-Site Scripting Vulnera
bilities
| https://www.exploit-db.com/exploits/25110
Microsoft IIS 2.0/3.0/4.0 - ISAPI GetExtensionVersion()

| https://www.exploit-db.com/exploits/19376
Microsoft Windows - Path Conversion

| https://www.exploit-db.com/exploits/27851
Microsoft Windows Media Player 11 - '.AVI' File Colorspace Conversion Remote Memory Corruption

| https://www.exploit-db.com/exploits/33770
Mono 1.0.5 - Unicode Character Conversion Multiple Cross-Site Scripting Vulnerabilities

| https://www.exploit-db.com/exploits/25148
Mozilla Firefox 3.5.3 - Floating Point Conversion Heap Overflow

| https://www.exploit-db.com/exploits/33312
Mozilla Suite/Firefox - InstallVersion->compareTo() Code Execution (Metasploit)

| https://www.exploit-db.com/exploits/16306
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Vers
ions)
| https://www.exploit-db.com/exploits/32764
Opera 6.0.1 / Microsoft Internet Explorer 5/6 - JavaScript Modifier Keypress Event Subversion

| https://www.exploit-db.com/exploits/21636
Orbit Downloader - URL Unicode Conversion Overflow (Metasploit)

| https://www.exploit-db.com/exploits/18515
Paintshop Pro X7 - '.gif' Conversion Heap Memory Corruption 'LZWMinimumCodeSize' (Denial of Se
rvice)
| https://www.exploit-db.com/exploits/37346
Phaos R4000 Version - 'file' Remote File Disclosure

| https://www.exploit-db.com/exploits/5420
Phorum 5.2 - 'versioncheck.php?upgrade_available' Cross-Site Scripting

| https://www.exploit-db.com/exploits/32913
PostgreSQL 8.3.6 - Conversion Encoding Remote Denial of Service

| https://www.exploit-db.com/exploits/32849
Prime95 Version 29.8 build 6 - Buffer Overflow (SEH)

| https://www.exploit-db.com/exploits/47802
Pserv 2.0 - HTTP Version Specifier Buffer Overflow

| https://www.exploit-db.com/exploits/22056
RealNetworks RealPlayer 16.0.3.51/16.0.2.32 - '.rmp' Version Attribute Buffer Overflow

| https://www.exploit-db.com/exploits/30468
sCssBoard (Multiple Versions) - 'pwnpack' Remote s

| https://www.exploit-db.com/exploits/5149
SeedDMS versions < 5.1.11 - Remote Command Execution

| https://www.exploit-db.com/exploits/47022
Shopping Portal ProVersion 3.0 - Authentication Bypass

| https://www.exploit-db.com/exploits/47834
Site-Assistant 0990 - 'paths[version]' Remote File Inclusion

| https://www.exploit-db.com/exploits/3285
Skulltag 0.96f - Version String Remote Format String (PoC)

| https://www.exploit-db.com/exploits/1708
Solaris/Open Solaris UCODE_GET_VERSION IOCTL - Denial of Service

| https://www.exploit-db.com/exploits/11351
Squid < 3.1 5 - HTTP Version Number Parsing Denial of Service

| https://www.exploit-db.com/exploits/8021
Subversion - Date Svnserve (Metasploit)

| https://www.exploit-db.com/exploits/16284
Subversion 0.3.7/1.0.0 - Remote Buffer Overflow

| https://www.exploit-db.com/exploits/4537
Subversion 1.0.2 - 'svn_time_from_cstring()' Remote Overflow

| https://www.exploit-db.com/exploits/304
Subversion 1.0.2 - Date Overflow (Metasploit)

| https://www.exploit-db.com/exploits/9935
Subversion 1.6.6/1.6.12 - Code Execution

| https://www.exploit-db.com/exploits/40507
Sun Java Applet 1.x - Invocation Version Specification

| https://www.exploit-db.com/exploits/24778
ta3arof [dating] Script (Arabic Version) - Arbitrary File Upload

| https://www.exploit-db.com/exploits/10718
Titan FTP Server Version 2019 Build 3505 - Directory Traversal / Local File Inclusion

| https://www.exploit-db.com/exploits/46611
Ublog access version - Arbitrary Database Disclosure

| https://www.exploit-db.com/exploits/8610
Web Companion versions 5.1.1035.1047 - 'WCAssistantService' Unquoted Service Path

| https://www.exploit-db.com/exploits/47522
WU-FTPD 2.4.2/2.5 .0/2.6.0/2.6.1/2.6.2 - FTP Conversion

| https://www.exploit-db.com/exploits/20563
Yahoo! Widget < 4.0.5 - 'GetComponentVersion()' Remote Overflow

| https://www.exploit-db.com/exploits/4250
Zimplit CMS - 'English_manual_version_2.php?client' Cross-Site Scripting

| https://www.exploit-db.com/exploits/35064

--- ---

Shellcode Title

| URL

--- ---
iOS Version-independent - Null-Free Shellcode

| https://www.exploit-db.com/shellcodes/13290

--- ---

Exploit Title

| URL

--- ---
Adaware Web Companion version 4.8.2078.3950 - 'WCAssistantService' Unquoted Service Path

| https://www.exploit-db.com/exploits/47597
Adobe Flash - Out-of-Bounds Read in UTF Conversion

| https://www.exploit-db.com/exploits/37862
Adobe Flash Player 9/10 - SWF Version Null Pointer Dereference Denial of Service

| https://www.exploit-db.com/exploits/32452
Adobe Shockwave - 'ShockwaveVersion()' Stack Overflow (PoC)

| https://www.exploit-db.com/exploits/4613
Adobe Version Cue 1.0/1.0.1 (OSX) - '-lib' Local Privilege Escalation

| https://www.exploit-db.com/exploits/1186
Adobe Version Cue 1.0/1.0.1 (OSX) - Local Privilege Escalation

| https://www.exploit-db.com/exploits/1185
Alibaba Clone Diamond Version - SQL Injection

| https://www.exploit-db.com/exploits/12544
Alibaba Clone Tritanium Version - 'news_desc.html' SQL Injection

| https://www.exploit-db.com/exploits/27605
Apache Subversion - Remote Denial of Service

| https://www.exploit-db.com/exploits/38422
Apache Subversion 1.6.x - 'mod_dav_svn/lock.c' Remote Denial of Service

| https://www.exploit-db.com/exploits/38421
Apache UNO / LibreOffice Version: 6.1.2 / OpenOffice 4.1.6 API - Remote Code Execution

| https://www.exploit-db.com/exploits/46544
Apple Mac OSX Adobe Version Cue - Local Privilege Escalation (Bash)

| https://www.exploit-db.com/exploits/680
Apple Mac OSX Adobe Version Cue - Local Privilege Escalation (Perl)

| https://www.exploit-db.com/exploits/795
Apple QuickTime /w IE .qtl Version XAS - Remote

| https://www.exploit-db.com/exploits/4424
Asn Guestbook 1.5 - 'footer.php?version' Cross-Site Scripting

| https://www.exploit-db.com/exploits/26021
Asn Guestbook 1.5 - 'header.php?version' Cross-Site Scripting

| https://www.exploit-db.com/exploits/26020
ASPPortal Free Version - 'Topic_Id' SQL Injection

| https://www.exploit-db.com/exploits/5775
Betsy CMS versions 3.5 - Local File Inclusion

| https://www.exploit-db.com/exploits/10189
Centrinity FirstClass HTTP Server 5.50/5.77/7.0/7.1 - Long Version Field Denial of Service

| https://www.exploit-db.com/exploits/23234
CLUB-Nuke [XP] 2.0 LCID 2048 (Turkish Version) - SQL Injection

| https://www.exploit-db.com/exploits/2150
CollabNet Subversion Edge Log Parser - HTML Injection

| https://www.exploit-db.com/exploits/34691
CollabNet Subversion Edge Management 4.0.11 - Local File Inclusion

| https://www.exploit-db.com/exploits/37442
CP3 Studio PC Version - Denial of Service

| https://www.exploit-db.com/exploits/13838
Crystal Reports CrystalPrintControl - ActiveX ServerResourceVersion Property Overflow (Metaspl
oit)
| https://www.exploit-db.com/exploits/23472
Downline Goldmine paidversion - SQL Injection

| https://www.exploit-db.com/exploits/6950
eWebeditor ASP Version - Multiple Vulnerabilities

| https://www.exploit-db.com/exploits/11295
file upload Ar Version - Arbitrary File Upload

| https://www.exploit-db.com/exploits/10689
FileCOPA FTP Server (Pre 18 Jul Version) - 'LIST' Remote Buffer Overflow (Metasploit)

| https://www.exploit-db.com/exploits/16733
Foxit Products GIF Conversion - 'DataSubBlock' Memory Corruption

| https://www.exploit-db.com/exploits/36335
Foxit Products GIF Conversion - 'LZWMinimumCodeSize' Memory Corruption

| https://www.exploit-db.com/exploits/36334
Foxit Reader - '.png' Conversion Parsing tEXt Chunk Arbitrary Code Execution

| https://www.exploit-db.com/exploits/37699
Gbook MX 4.1.0 (Arabic Version) - Remote File Inclusion

| https://www.exploit-db.com/exploits/10986
GNU UnRTF 0.19.3 - Font Table Conversion Buffer Overflow

| https://www.exploit-db.com/exploits/25030
Google Android - libutils UTF16 to UTF8 Conversion Heap Buffer Overflow

| https://www.exploit-db.com/exploits/40354
Hikvision IP Camera versions 5.2.0 - 5.3.9 (Builds 140721 < 170109) - Access Control Bypass

| https://www.exploit-db.com/exploits/44328
HTML2HDML 1.0.3 - File Conversion Buffer Overflow

| https://www.exploit-db.com/exploits/25011
IBM DB2 DTS To String Conversion - Denial of Service

| https://www.exploit-db.com/exploits/24677
iOS < 12.2 / macOS < 10.14.4 XNU - pidversion Increment During execve is Unsafe

| https://www.exploit-db.com/exploits/46648
JaWiki - 'versionNo' Cross-Site Scripting

| https://www.exploit-db.com/exploits/36828
Joomla! Component com_versioning - SQL Injection

| https://www.exploit-db.com/exploits/17264
Joomla! Component versioning 1.0.2 - 'id' SQL Injection

| https://www.exploit-db.com/exploits/5989
Joomla! Convert Forms version 2.0.3 - Formula Injection (CSV Injection)

| https://www.exploit-db.com/exploits/44447
KioWare Server Version 4.9.6 - Weak Folder Permissions Privilege Escalation

| https://www.exploit-db.com/exploits/46093
Live For Speed 2 Version Z - '.Mpr' Local Buffer Overflow

| https://www.exploit-db.com/exploits/9142
Live For Speed 2 Version Z - '.mpr' Local Buffer Overflow (SEH)

| https://www.exploit-db.com/exploits/9148
LocatePC 1.05 (Ligatt Version + Others) - SQL Injection

| https://www.exploit-db.com/exploits/16152
Microsoft ASP.NET 1.0/1.1 - Unicode Character Conversion Multiple Cross-Site Scripting Vulnera
bilities
| https://www.exploit-db.com/exploits/25110
Microsoft IIS 2.0/3.0/4.0 - ISAPI GetExtensionVersion()

| https://www.exploit-db.com/exploits/19376
Microsoft Windows - Path Conversion

| https://www.exploit-db.com/exploits/27851
Microsoft Windows Media Player 11 - '.AVI' File Colorspace Conversion Remote Memory Corruption

| https://www.exploit-db.com/exploits/33770
Mono 1.0.5 - Unicode Character Conversion Multiple Cross-Site Scripting Vulnerabilities

| https://www.exploit-db.com/exploits/25148
Mozilla Firefox 3.5.3 - Floating Point Conversion Heap Overflow

| https://www.exploit-db.com/exploits/33312
Mozilla Suite/Firefox - InstallVersion->compareTo() Code Execution (Metasploit)

| https://www.exploit-db.com/exploits/16306
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Vers
ions)
| https://www.exploit-db.com/exploits/32764
Opera 6.0.1 / Microsoft Internet Explorer 5/6 - JavaScript Modifier Keypress Event Subversion

| https://www.exploit-db.com/exploits/21636
Orbit Downloader - URL Unicode Conversion Overflow (Metasploit)

| https://www.exploit-db.com/exploits/18515
Paintshop Pro X7 - '.gif' Conversion Heap Memory Corruption 'LZWMinimumCodeSize' (Denial of Se
rvice)
| https://www.exploit-db.com/exploits/37346
Phaos R4000 Version - 'file' Remote File Disclosure

| https://www.exploit-db.com/exploits/5420
Phorum 5.2 - 'versioncheck.php?upgrade_available' Cross-Site Scripting

| https://www.exploit-db.com/exploits/32913
PostgreSQL 8.3.6 - Conversion Encoding Remote Denial of Service

| https://www.exploit-db.com/exploits/32849
Prime95 Version 29.8 build 6 - Buffer Overflow (SEH)

| https://www.exploit-db.com/exploits/47802
Pserv 2.0 - HTTP Version Specifier Buffer Overflow

| https://www.exploit-db.com/exploits/22056
RealNetworks RealPlayer 16.0.3.51/16.0.2.32 - '.rmp' Version Attribute Buffer Overflow

| https://www.exploit-db.com/exploits/30468
sCssBoard (Multiple Versions) - 'pwnpack' Remote s

| https://www.exploit-db.com/exploits/5149
SeedDMS versions < 5.1.11 - Remote Command Execution

| https://www.exploit-db.com/exploits/47022
Shopping Portal ProVersion 3.0 - Authentication Bypass

| https://www.exploit-db.com/exploits/47834
Site-Assistant 0990 - 'paths[version]' Remote File Inclusion

| https://www.exploit-db.com/exploits/3285
Skulltag 0.96f - Version String Remote Format String (PoC)

| https://www.exploit-db.com/exploits/1708
Solaris/Open Solaris UCODE_GET_VERSION IOCTL - Denial of Service

| https://www.exploit-db.com/exploits/11351
Squid < 3.1 5 - HTTP Version Number Parsing Denial of Service

| https://www.exploit-db.com/exploits/8021
Subversion - Date Svnserve (Metasploit)

| https://www.exploit-db.com/exploits/16284
Subversion 0.3.7/1.0.0 - Remote Buffer Overflow

| https://www.exploit-db.com/exploits/4537
Subversion 1.0.2 - 'svn_time_from_cstring()' Remote Overflow

| https://www.exploit-db.com/exploits/304
Subversion 1.0.2 - Date Overflow (Metasploit)

| https://www.exploit-db.com/exploits/9935
Subversion 1.6.6/1.6.12 - Code Execution

| https://www.exploit-db.com/exploits/40507
Sun Java Applet 1.x - Invocation Version Specification

| https://www.exploit-db.com/exploits/24778
ta3arof [dating] Script (Arabic Version) - Arbitrary File Upload

| https://www.exploit-db.com/exploits/10718
Titan FTP Server Version 2019 Build 3505 - Directory Traversal / Local File Inclusion

| https://www.exploit-db.com/exploits/46611
Ublog access version - Arbitrary Database Disclosure

| https://www.exploit-db.com/exploits/8610
Web Companion versions 5.1.1035.1047 - 'WCAssistantService' Unquoted Service Path

| https://www.exploit-db.com/exploits/47522
WU-FTPD 2.4.2/2.5 .0/2.6.0/2.6.1/2.6.2 - FTP Conversion

| https://www.exploit-db.com/exploits/20563
Yahoo! Widget < 4.0.5 - 'GetComponentVersion()' Remote Overflow

| https://www.exploit-db.com/exploits/4250
Zimplit CMS - 'English_manual_version_2.php?client' Cross-Site Scripting

| https://www.exploit-db.com/exploits/35064

Shellcode Title	URL
iOS Version-independent - Null-Free Shellcode	https://www.exploit-db.com/shellcodes/13290