

Forum:[Hack Forums](#)

Thread: [\[TUT\] Webdav Hacking And Defacing \[TUT\]](#)

IPhiLG - October 26, 2010, 2:20 pm

Okay then its my first tutorial so urm i blame The person who starts page 2 =] k then lets begin my epic fail tutorial on how to Deface/Plant a shell in a Habbo/WOW private server (or anything else that has webdav)

Step 1:

Pretty simple.

find a website that goes www.website.com/webdav

that then says as its content "WebDav Test" or somthing like that eh :D

Step 2:

Opening Up The "Map Network Drive"

Meth0d 1(Right Click On MyComputer) WINDOWS XP

Meth0d 2(Click The Start Bar) WINDOWS 7

Step 3:

Click on "sign up for online storage of conect to a network server"

Itll load. Click Next. "Choose Another Network Location".

Step 4:

Input www.site.com/webdav

Login Username Is Default: wampp

Login Password Is Default: xampp

Login.

Step 5:

Browse Files Until you see The "WebDav" Directory and copy your shell.php usually c99shell.php or whatever shell you have .php.

Step 6:

go to www.site.com/webdav/shell.php replace shell.php with the name of your shell.

step 7:

Go back to all the files. go to htdocs. go to global.php edit to deface page. edit index.html to deface save them username and password is the password you used to login.

POW

-=-=-

[= Tutorial By My Mind =]

HaxOr? - October 26, 2010, 3:16 pm

Not working :S

[short] Too shrt [/short]

PrOx3rStY13 - October 26, 2010, 3:32 pm

thanx will try it..
[short] Too shrt [/short]

IPhiLG - October 27, 2010, 2:05 am

(Oct 26, 2010 03:16 PM)HaX0r^ Wrote: [\[CITE\]](#) Not working :S

[short] Too shrt [/short]

It is either that they have changed username and pass
or they deleted WebDav directoy :D Sorry if this didnt help?

gsy - October 27, 2010, 2:51 am

it works but for me only for 10% of whole wo has a /webdav folder i scanned whole Poland and found only 51 Vurn pages/ip's

IPhiLG - October 27, 2010, 3:18 am

(Oct 27, 2010 02:51 AM)gsy Wrote: [\[CITE\]](#) it works but for me only for 10% of whole wo has a /webdav folder i scanned whole Poland and found only 51 Vurn pages/ip's
well atleast it worked ;)

zZach - October 27, 2010, 3:24 am

Sir,

step1 has a broken link
kindly check it out :D

Asus - October 27, 2010, 3:26 am

It works and this exploit is selling very good.

BuyOMC - October 27, 2010, 3:36 am

way to go trying to release my tutorial

give me credits

Dennis - October 27, 2010, 3:40 am

Old stuff is old lol.

On a side-note this is not an exploit..

Last time Apachefriends left the phpmyadmin user 'root' blank passworded, this time they set a stock user for webdav.

Asus - October 27, 2010, 3:43 am

(Oct 27, 2010 03:36 AM)Gids Wrote: [\[CITE\]](#) way to go trying to release my tutorial

give me credits

Well yeah for mentioning and bringing it back alive. It took me 30 mins to figure out your exploit. I just need IP's to scan and im complete.

IPhiLG - October 27, 2010, 3:50 am

(Oct 27, 2010 03:36 AM)Gids Wrote: [\[CITE\]](#) way to go trying to release my tutorial

give me credits

Its not yours i wrote it so go suck urself =]

H@cker - October 27, 2010, 10:18 am

(Oct 27, 2010 02:51 AM)gsy Wrote: [\[CITE\]](#) it works but for me only for 10% of whole wo has a /webdav folder i scanned whole Poland and found only 51 Vurn pages/ip's so you found 51 site 10% , so what are you saying is that there is only 510 polish websites?

how you find websites with /webdav

can someone give me link from some website with /webdav , I just wanna see source code so I could make scanner...

gsy - October 27, 2010, 10:59 am

(Oct 27, 2010 10:18 AM)H@cker Wrote: [\[CITE\]](#) so you found 51 site 10% , so what are you saying is that there is only 510 polish websites?

how you find websites with /webdav

can someone give me link from some website with /webdav , I just wanna see source code so I could make scanner...

there where only 510 polish ip's on the page which could use that app

PS: And you should know that if you found a page it could be that the pass is changed.
here the source:

Code <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"

"http://www.w3.org/TR/html4/loose.dtd">

<html>

<head>

<meta name="author" content="Kai Oswald Seidler, Kay Vogelgesang, Carsten Wiedmann">

<title></title>

</head>

<body>

<center>WebDAV testpage</center>

</body>

</html>

[/code]

IPhiLG - October 28, 2010, 1:25 am

(Oct 27, 2010 01:19 PM)nathanha17 Wrote: [\[CITE\]](#) Dude This Is Gids -.- Stop Taking CREDITS u fagget -.-

Dude i wrote it all myself i had never even heard of Gids! so im taking credit for what i have done!

BuyOMC - October 28, 2010, 1:28 am

this is my guide

i have contacted mod to lock this thread

IPhiLG - October 28, 2010, 1:29 am

(Oct 28, 2010 01:28 AM)Gids Wrote: [\[CITE\]](#) this is my guide

i have contacted mod to lock this thread

well i never seen ur thread so its "my guide" and whats the point?

nobody is gunan find urs again unless u so yh just

leave it open!

BuyOMC - October 28, 2010, 1:31 am

(Oct 28, 2010 01:29 AM)Pamperz Wrote: [\[CITE\]](#) well i never seen ur thread so its "my guide" and whats the point?

nobody is gunan find urs again unless u so yh just

leave it open!

explain why my guide was the FIRST one

IPhiLG - October 28, 2010, 1:33 am

(Oct 28, 2010 01:31 AM)Gids Wrote: [\[CITE\]](#) explain why my guide was the FIRST one

because i havnt been here very long and u probs have, but i didnt

know about your little topic i searched, but no results

BuyOMC - October 28, 2010, 1:34 am

(Oct 28, 2010 01:33 AM)Pamperz Wrote: [\[CITE\]](#) because i havnt been here very long and u probs have, but i didnt

know about your little topic i searched, but no results

because i removed it.

next time you steal my guide word by word i recommend u give credits.

IPhiLG - October 28, 2010, 1:35 am

(Oct 28, 2010 01:34 AM)Gids Wrote: [\[CITE\]](#) because i removed it.

next time you steal my guide word by word i recommend u give credits.

when did you remove it then?

BuyOMC - October 28, 2010, 1:36 am

(Oct 28, 2010 01:35 AM)Pamperz Wrote: [\[CITE\]](#) when did you remove it then?

less than a week is when i removed

IPhiLG - October 28, 2010, 1:37 am

(Oct 28, 2010 01:36 AM)Gids Wrote: [\[CITE\]](#) less than a week is when i removed

i ent been here for a week! so how could i see it>?

BuyOMC - October 28, 2010, 1:38 am

(Oct 28, 2010 01:37 AM)Pamperz Wrote: [\[CITE\]](#) i ent been here for a week! so how could i see it>?
remove your guide right now

IPhiLG - October 28, 2010, 1:39 am

because u just got proven wrong? Pwned. And No its my guide i put my time into it. so its staying.

BuyOMC - October 28, 2010, 1:42 am

(Oct 28, 2010 01:39 AM)Pamperz Wrote: [\[CITE\]](#) because u just got proven wrong? Pwned. And No its my guide i put my time into it. so its staying.
lol so you think i never wrote this guide?

<https://hackforums.net/showthread.php?tid=756493>

STFU skid

IPhiLG - October 28, 2010, 1:44 am

well i have never seen it before. and this was my HANDWRITTEN tutorial. why dont we just end this conv? and just ignore eachother (ur keeping my thread alive :))
but still i never copied urs

bigiboro - October 28, 2010, 1:45 am

It works , but not always ;)

BuyOMC - October 28, 2010, 1:46 am

(Oct 28, 2010 01:44 AM)Pamperz Wrote: [\[CITE\]](#) well i have never seen it before. and this was my HANDWRITTEN tutorial. why dont we just end this conv? and just ignore eachother (ur keeping my thread alive :))
but still i never copied urs
lol you never copied mine..

how many people said that and got banned/limited after they got caught...

IPhiLG - October 28, 2010, 1:46 am

(Oct 28, 2010 01:45 AM)bigiboro Wrote: [\[CITE\]](#) It works , but not always ;)
thanks for feedback :)
hope u enjoy doing it
(Oct 28, 2010 01:46 AM)Gids Wrote: [\[CITE\]](#) lol you never copied mine..

how many people said that and got banned/limited after they got caught...but the thing is. i wont get banned/limited because i didnt copy it!

lilacscripts - October 28, 2010, 2:31 am

(Oct 28, 2010 01:37 AM)Pamperz Wrote: [\[CITE\]](#) i ent been here for a week! so how could i see it>?
You only joined HackForums yesterday? You couldn't have seen the guide...

CrackingTheUncrackable - October 28, 2010, 3:26 am

Sorry but this doesn't work -_-

IPhiLG - October 28, 2010, 9:20 am

(Oct 28, 2010 03:26 AM)CrackingTheUncrackable Wrote: [\[CITE\]](#) Sorry but this doesn't work -_-
it is possible that they changed the password for webdav ;)?

Crup - October 28, 2010, 11:57 am

You said open "Map Network Drive", Do you have to download that or is it already there?

IPhiLG - October 28, 2010, 11:59 am

(Oct 28, 2010 11:57 AM)Crup Wrote: [\[CITE\]](#) You said "Map Network Drive", Do you have to download that or is it already there?
if u have windows XP,7 i know it comes with it but other OS im not sure about ;)

Crup - October 28, 2010, 12:00 pm

Well, I think I have Windows XP 7, but I suggest telling where to find the so called "Map Network Drive"

IPhiLG - October 28, 2010, 12:16 pm

(Oct 28, 2010 12:00 PM)Crup Wrote: [\[CITE\]](#) Well, I think I have Windows XP 7, but I suggest telling where to find the so called "Map Network Drive"

yh it does ? :D

Spoiler ([Click to View](#))short

Crup - October 30, 2010, 5:47 pm

How do you get a shell? either downloading or tell how to get it?

iQosmo - October 30, 2010, 9:01 pm

great tut dude thanks alot lolz.

Lightangel - October 31, 2010, 12:12 am

Can you give us some google dorks to try this.

fish71 - November 8, 2010, 10:43 pm

yeh.. what are some good Dorks for webdav??

axmetmcl - November 9, 2010, 3:25 am

(Nov 8, 2010 11:43 PM)fish71 Wrote: [\[CITE\]](#) yeh.. what are some good Dorks for webdav?? thanks for the tut. but i m curious about that too?

IPhiLG - November 10, 2010, 12:33 pm

Wth is a dork people?

Dont say a nerd/geek the term dork.

diskordia - November 29, 2010, 9:14 pm

this site is vulnerable? <http://190.233.51.52/>

IPhiLG - December 4, 2010, 2:51 pm

(Nov 29, 2010 10:14 PM)diskordia Wrote: [\[CITE\]](#) this site is vulnerable? <http://190.233.51.52/> Find out urself ;)?

DarkOrigins - December 4, 2010, 3:51 pm

(Nov 10, 2010 01:33 PM)Pamperz Wrote: [\[CITE\]](#) Wth is a dork people?

Dont say a nerd/geek the term dork.

You don't know what a dork is? Sweet Jesus, what are you doing on HackForums.

A dork is a thing you can use to search for vulnerabilities in sites. Like inurl:id=1 is an SQLi dork.

IPhiLG - December 10, 2010, 10:57 am

Ahh but atleast i can program so thats one thing.

batm3n - January 4, 2011, 12:15 pm

I have a list of several websites with webdav that I can log in to. But I cannot upload anything at all, do I have to wait until I find one I can upload stuff too. Or is it just not working?

I'm trying to upload a small .txt so that I can test to see if the upload has worked by going to server/test.txt

IPhiLG - January 6, 2011, 6:11 am

try editing something? some sites dont allow uploading. :)

iNk Jr. - January 7, 2011, 2:32 pm

I cant get it to work :(!

NoSe - January 25, 2011, 5:07 pm

why to me when I put user and pass does not log ?

IPhiLG - February 9, 2011, 12:23 pm

some websites are different, and have different logins,

Valour - February 9, 2011, 1:17 pm

@Pamperz

Nah man..tried with 10-12 webservers...failed always.maybe they changed the login credentials..

For that dorks

I was using this dork

inurl:".com/webdav"

u can edit anything according to your needs...

preferably change the ".com" to something else and try out.. Din have time so got to search only with one single dork :(

Crup - February 28, 2011, 5:14 pm

How do u upload the shell?

IPhiLG - May 4, 2011, 11:04 am

i monitored some people doing it via a utube vid so try that

lord111 - May 4, 2011, 12:30 pm

GOOD thanks mane and forwarded

KongenT - May 4, 2011, 1:21 pm

nice!

Spoiler ([Click to View](#)) Too Short Message!

IPhiLG - May 6, 2011, 11:39 am

Glad my tutorial helped you :)

qwerty156 - June 21, 2011, 9:01 pm

Could you tell us how to secure teh server as well?

Pixelblocker - June 24, 2011, 8:43 am

Ive a problem... I have around the 15 sites that have /webdav but the name and pass do not work... Please help me

CarterMendez - June 24, 2011, 8:51 am

Nice one, i learnt something from this :p

IPhiLG - June 24, 2011, 10:30 am

if the username and password i provided do not work, it is possible they changed it.

PhantomCracker - June 24, 2011, 10:41 am

Old but good
thank you for this Pamperz ;)

Saintzfan - June 24, 2011, 10:46 am

Thank you for this good tut :D ill use this

manabox - June 24, 2011, 10:46 am

Pamperz can u give me the PASSWORD of this admin panel

avacadoserver.net/forum/admin/

Hmily[LCG] - June 24, 2011, 12:34 pm

anyways,thanks for your tutorial.maybe someone can get the point.

IPhiLG - July 16, 2011, 10:26 am

haha, no i cant do that site as it appears to be offline/shutdown?

Anvio - July 16, 2011, 11:58 am

Quite a nice solid concept - basically it is just a matter of figuratively winning the lottery by trying to find a site that has this vulnerability.

IPhiLG - July 16, 2011, 12:03 pm

Anvio say what about lottery now?

h4kr! - August 6, 2011, 5:31 pm

this doesn't work on windows 7.
i'm not sure why it just doesn't.

IPhiLG - August 8, 2011, 12:49 pm

(Aug 6, 2011 05:31 PM)h4kr! Wrote: [\[CITE\]](#) this doesn't work on windows 7.

i'm not sure why it just doesn't.

Is your win7 Legit? or was it downloaded and burnt?

@€CKI€SS - August 8, 2011, 2:12 pm

(Oct 27, 2010 03:24 AM)zZach Wrote: [\[CITE\]](#) Sir,

step1 has a broken link
kindly check it out :D
ROFL FACEPALM BRO
Spoiler [\(Click to View\)](#) LOOLOLOLLOOLOLOLOLOLL

inushakolla - August 8, 2011, 2:17 pm

How can i find sites with /webdav ? I tried loadzz
Every single site.

IPhiLG - August 9, 2011, 1:33 pm

As i said, they are mainly WoW sites and Habbo Retros..

IPhiLG - August 18, 2011, 11:52 am

they are usually ones that run on XAMPP OR WAMP

