

Forum: [Hack Forums](#)

Thread: [\[TuT\] Exploiting Microsoft/IIS 6.0 WebDAV - Uploading Files.](#)

Phizo - April 12, 2011, 9:23 am

Today I will be teaching a way to exploit very common a vulnerability and upload your shell and/or deface page to a Microsoft IIS 6.0 based website.

What you will need:

A windows machine.

Basic knowledge of shells.

A Microsoft/IIS 6.0 website with WebDAV enabled.

An ASP shell. - <http://www.#!/?d=YU209ET7> << Download link for the shell. (Do not even try a PHP shell, it won't work. You can use your ASP shell to upload your PHP shell after though.)

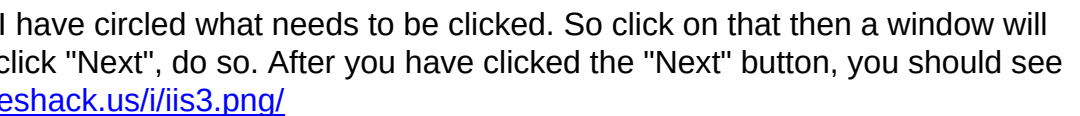
This is how to perform the exploit in Windows 7:

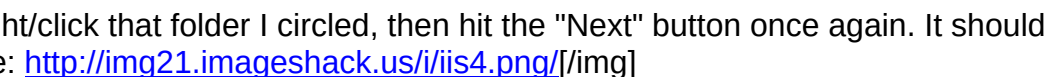
Click start > Computer.

You will see this page: <http://img851.imageshack.us/i/iis1.png/>

Next you will want to click "Map network drive", it has been circled in the picture above.

Now a window will pop-up, it should look like this: <http://img638.imageshack.us/i/iis2.png/>

As you can see again. I have circled what needs to be clicked. So click on that then a window will come up asking you to click "Next", do so. After you have clicked the "Next" button, you should see this: <http://img850.imageshack.us/i/iis3.png/>

You will need to highlight/click that folder I circled, then hit the "Next" button once again. It should redirect you to this page: <http://img21.imageshack.us/i/iis4.png/>

I put "www.vulnerablesite.com" as an example. You have to type in "http://vulnerablesite.com" otherwise it will not work. It requires HTTP, not WWW. You will receive an error unless you use HTTP (once again, <http://vulnerablesite.com>)

Hit the "Next" button again, then it should come up with the site name with the output "vulnerablesite.com", you can name it whatever you like, this is what I put:

<http://img130.imageshack.us/i/iis5.png/>

Except I changed it to "IIS 6.0 Exploit for HF - Phizo".

It doesn't matter what you put, just make sure you remember it.

Make sure the box is ticked (open when finished) then go ahead and hit finish.

Okay, we've exploited the website. Now we want to upload our files to the website. A new window has just opened, as you can see, we're connected to the websites files, however we're not aloud to view the files as we're unauthorized. No matter, we can still upload our shells and what other files we would like to upload.

Okay, I don't think I will need to put any pictures in this one, it's that simple. Follow my instructions:

#1 - Open the directory of where your ASP shell is (example: desktop, documents, or custom folder). Your ASP shell should have a name similar to "shell.asp;anything.jpg".

#2 - Drag your ASP shell from your custom folder into the website folder we just exploited. It should just go straight in there with no problems.

Tada! We have successfully uploaded our shell! Now all we have to do is go to:

<http://vulnerablesite.com/shell.asp;anything.jpg>.

I hope this helps.

Please do not leech this. I spent all my time making it. Full credit to me (Phizo).

My other webhacking tutorials:

MySQL injection: <https://hackforums.net/showthread.php?tid=1219987>

Cross Site Scripting: <https://hackforums.net/showthread.php?tid=1212236>

Remote File Inclusion: <https://hackforums.net/showthread.php?tid=1213488>

ihasdevkit - April 12, 2011, 9:29 am

thanks for the tut, this works better on IIS 5.0 ...
when i try to upload my shell it says file to large.
i tired to upload a text file.
its been trying to upload it for like 5mins now..
help PM -- TV me please??

Coffee - April 12, 2011, 9:30 am

great tut mate thanks :) attempting it now :)

Phizo - April 12, 2011, 9:31 am

(Apr 12, 2011 09:29 AM)ihasdevkit Wrote: [\[CITE\]](#) thanks for the tut, this works better on IIS 5.0 ...
when i try to upload my shell it says file to large.
i tired to upload a text file.
its been trying to upload it for like 5mins now..
help PM -- TV me please??
That's odd. I attempted to run this exploit on an IIS 5.0 website and it didn't work. PM me your TV info.

pepon - April 12, 2011, 9:48 am

Good clear and well written tutorial, thanks.

Phizo - April 12, 2011, 9:49 am

(Apr 12, 2011 09:48 AM)pepon Wrote: [\[CITE\]](#) Good clear and well written tutorial, thanks.
Thanks for the feedback ;).

Pain25 - April 12, 2011, 10:30 am

thats a nice tutorial, but i have a problem. i cant connect to the site that i want to hack, because the have only a www. site.
This means i can connect with my webbrowser on "http://www.mysite.de" but not on "http://mysite.de" .
Can anybody help me?

Sorry for my bad english. I hope you understand me.

JoinSeventh - April 12, 2011, 10:33 am

I haven't looked in to this exploit to much, so correct me if I'm wrong.

Every IIS 6.0 server with Webdav enabled is vulnerable?

Echt - April 12, 2011, 10:34 am

great amazingly written tutorial man.
thanks a bunch.

Phizo - April 12, 2011, 10:39 am

(Apr 12, 2011 10:33 AM)Join7 Wrote: [\[CITE\]](#) I haven't looked in to this exploit to much, so correct me if I'm wrong.

Every IIS 6.0 server with Webdav enabled is vulnerable?

To my knowledge, yes. I've never came across failure exploiting a IIS 6.0 website with Webdav enabled.

sumit8510 - April 12, 2011, 11:31 am

I'll try it out.

And then post the result.

Doesn't it work on vista as well?

Thanks

********* - April 12, 2011, 1:30 pm

(Apr 12, 2011 10:39 AM)Phizo Wrote: [\[CITE\]](#) To my knowledge, yes. I've never came across failure exploiting a IIS 6.0 website with Webdav enabled.

how do you check if its enabled??

CyberM@X - April 12, 2011, 2:57 pm

Well I always get this error ! :D - what do I do wrong here :S... I can't find the folder .. even though it's a vuln site.. It ask me for username & password if I add ftp:// ...

[IMG]<http://img820.imageshack.us/img820/8496/ignore.jpg>[/IMG]

Hope someone helps me :P

********* - April 12, 2011, 5:54 pm

(Apr 12, 2011 02:57 PM)Mr.Suxi Wrote: [\[CITE\]](#) Well I always get this error ! :D - what do I do wrong here :S... I can't find the folder .. even though it's a vuln site.. It ask me for username & password if I add ftp:// ...

[IMG]<http://img820.imageshack.us/img820/8496/ignore.jpg>[/IMG]

Hope someone helps me :P

maybe try this?

<http://www.exploit-db.com/exploits/8806/>

BTW, how do you know its vulnerable?

v?x? - April 12, 2011, 5:59 pm

Pretty sweet bro p =p =p =p

Phizo - April 12, 2011, 7:33 pm

(Apr 12, 2011 02:57 PM)Mr.Suxi Wrote: [\[CITE\]](#) Well I always get this error ! :D - what do I do wrong here :S... I can't find the folder .. even though it's a vuln site.. It ask me for username & password if I add ftp:// ...

[IMG]<http://img820.imageshack.us/img820/8496/ignore.jpg>[/IMG]

Hope someone helps me :P

If you actually read the tutorial. You need to put "http://website.com" not "website.com".

NightsSiners - April 12, 2011, 8:13 pm

XD BEST TUTORIAL EVER THIS IS HILARIOUS I CANT BELIEVE ITS THIS EASY!!!! IVE BEEN LOOKING FOR A EXPLOIT FOR EVER !!!!

Phizo - April 12, 2011, 8:16 pm

(Apr 12, 2011 08:13 PM)NightsSiners Wrote: [\[CITE\]](#) XD BEST TUTORIAL EVER THIS IS HILARIOUS I CANT BELIEVE ITS THIS EASY!!!! IVE BEEN LOOKING FOR A EXPLOIT FOR EVER !!!!

I know. It's quite amusing.

UDP Flood - April 12, 2011, 8:18 pm

I have searched for a tutorial like this for so long. If I had a paypal I would send you money.
Thanks man.

Phizo - April 12, 2011, 8:18 pm

(Apr 12, 2011 08:18 PM)UDP Flood Wrote: [\[CITE\]](#) I have searched for a tutorial like this for so long. If I had a paypal I would send you money.

Thanks man.

Haha. It's all good man. Enjoy ;).

Rowdy - April 12, 2011, 9:19 pm

Know any dorks for finding these sites?

DaRKCraCk3r - April 12, 2011, 9:23 pm

good one bro can be very helpfull for all people ..
keep it up man....

Phizo - April 12, 2011, 9:59 pm

(Apr 12, 2011 09:23 PM)DaRKCraCk3r Wrote: [\[CITE\]](#) good one bro can be very helpfull for all people ..

keep it up man....

Thanks.

No, there is no way to search for these types of websites with dorks. You will just have to scan the website and see if it uses IIS 6.0.

hermiod - April 13, 2011, 12:38 am

great tut mate thanks :) attempting it now :)

Phizo - April 13, 2011, 3:21 am

(Apr 13, 2011 12:38 AM)R??d? Wrote: [\[CITE\]](#) great tut mate thanks :) attempting it now :)

Thanks. Any problems, let me know.

Morbsy - April 13, 2011, 3:31 am

Very clear and helpful tutorial.

Just what I have been looking for :)

Thanks alot!

+rep

Cadis - April 13, 2011, 3:38 am

how can I find the IIS version and if its Webdav enabled?

Thanks! ;)

Morbsy - April 13, 2011, 3:41 am

(Apr 13, 2011 03:38 AM)Cadis Wrote: [\[CITE\]](#) how can I find the IIS version and if its Webdav enabled?

Thanks! ;)

I use Acunetix 7

too short

Cadis - April 13, 2011, 4:59 am

Aight I connected to the folder but whenever I try to copy some file there it says
0x80070780

The file cannot be accessed by the system

Unexpected error is keeping you from copying the file.

Phizo - April 13, 2011, 5:47 am

(Apr 13, 2011 04:59 AM)Cadis Wrote: [\[CITE\]](#) Aight I connected to the folder but whenever I try to copy some file there it says

0x80070780

The file cannot be accessed by the system

Unexpected error is keeping you from copying the file.

What happens when you try to create a new text document inside the folder?

Does the same error happen?

Cadis - April 13, 2011, 6:41 am

(Apr 13, 2011 05:47 AM)Phizo Wrote: [\[CITE\]](#) What happens when you try to create a new text document inside the folder?

Does the same error happen?

yep exactly :/ probably its somehow secured

Phizo - April 13, 2011, 6:57 am

(Apr 13, 2011 06:41 AM)Cadis Wrote: [\[CITE\]](#) yep exactly :/ probably its somehow secured

I think there may be a patch out for sites with WebDAV enabled. They must have some sort of script that stops outsiders from uploading files.

Not sure if there is a way to bypass it though.

Grey Hat Hacker - April 13, 2011, 8:02 am

Phizo, I thought you were better than this. Remember leS?

Phizo - April 13, 2011, 8:04 am

(Apr 13, 2011 08:02 AM)Grey Hat Hacker Wrote: [\[CITE\]](#) Phizo, I thought you were better than this. Remember leS?

I am better than this. I'm teaching everyone else basic exploitation.

Sora, we haven't spoken in so long, where have you been?

Also, Popc0rn won't even consider re-instating leS :\nIt was fun while it lasted.

Grey Hat Hacker - April 13, 2011, 8:09 am

(Apr 13, 2011 08:04 AM)Phizo Wrote: [\[CITE\]](#) I am better than this. I'm teaching everyone else basic exploitation.

Sora, we haven't spoken in so long, where have you been?

Also, Popc0rn won't even consider re-instating leS :\n

It was fun while it lasted.I've been banned from this forum, so I just started playing online games for the lulz. Now I'm back here. :P

Phizo - April 13, 2011, 8:10 am

(Apr 13, 2011 08:09 AM)Grey Hat Hacker Wrote: [\[CITE\]](#) I've been banned from this forum, so I just started playing online games for the lulz. Now I'm back here. :P

If you still have MSN, add me.

Grey Hat Hacker - April 13, 2011, 8:10 am

(Apr 13, 2011 08:10 AM)Phizo Wrote: [\[CITE\]](#) If you still have MSN, add me.
what is yours? btw, I still have vhr95zw@hotmail.com

Phizo - April 14, 2011, 1:37 am

Bump, can't let this thread go to waste.

Phizo - April 23, 2011, 3:57 am

Bump for epicness. Can't let this go to waist.

ice³ - April 23, 2011, 8:35 am

Sounds good, will try this if I can find some 'sploitable servers.

Fluxify - April 23, 2011, 8:47 am

@Phizo, What is the best way to find some exploiteable servers? or Dedi ips?

NotTy_rAJ - April 23, 2011, 9:14 am

Yet i have did this kinda IIS exploit but u realy explained nicely

...GReat tut dude ...Easy to understand...to any one....thnx 4r the share ?

mainly while adding the site name...people write in www format either of http:// so IIS doest happens,,,,,) that was the main thing many get stucked to..
apricited ...?

Phizo - April 23, 2011, 11:41 am

(Apr 23, 2011 09:14 AM)NotTy_rAJ Wrote: [\[CITE\]](#) Yet i have did this kinda IIS exploit but u realy explained nicely

...GReat tut dude ...Easy to understand...to any one....thnx 4r the share ?

mainly while adding the site name...people write in www format either of http:// so IIS doest happens,,,,,) that was the main thing many get stucked to..
apricited ...?

No problem, enjoy everyone :).

Gangstar - April 23, 2011, 12:57 pm

Amazing TUT thanks 4 share sir

jalal77 - April 23, 2011, 1:11 pm

dude i m newbe .i want help.i uploaded asp shell succcessfull..now i want to deface front page(home page)so where i upload my deface page?? help mee..

Phizo - April 23, 2011, 2:12 pm

(Apr 23, 2011 01:11 PM)jalal77 Wrote: [\[CITE\]](#) dude i m newbe .i want help.i uploaded asp shell succcessfull..now i want to deface front page(home page)so where i upload my deface page?? help mee..

Use the upload feature on ASP shell. Name you deface "index.html", the sites homepage will then be defaced.

24601 - April 23, 2011, 8:38 pm

I really want to deface something right now, so anyone got a good IIS 6.0 website I can hack? ;) seriously though

Phizo - April 24, 2011, 2:14 am

(Apr 23, 2011 08:38 PM)andrecito77 Wrote: [\[CITE\]](#) I really want to deface something right now, so anyone got a good IIS 6.0 website I can hack? ;) seriously though
Just use google, you will be suprised what pops up.

zion_rulz - April 24, 2011, 4:23 am

Can anyone tell if this works with IIS 7 as well? Hope to get a quick response.

Cheers :)

Phizo - April 24, 2011, 4:34 am

(Apr 24, 2011 04:23 AM)zion_rulz Wrote: [\[CITE\]](#) Can anyone tell if this works with IIS 7 as well? Hope to get a quick response.

Cheers :)

I believe it doesn't, hence why it's named "IIS 6.0 exploit".

zion_rulz - April 24, 2011, 5:03 am

@ Phizo: Thanks for your quick response; it was my bad that I didn't notice the caption minutely.
Another query : I tried on a site "http://mysite.co.uk" and got an error "The folder you entered does not appear to be valid. Please choose another."

Hope to get some light. Thanks once again.

Cheers :)

(Apr 24, 2011 04:34 AM)Phizo Wrote: [\[CITE\]](#) I believe it doesn't, hence why it's named "IIS 6.0 exploit".

Phizo - April 24, 2011, 5:06 am

(Apr 24, 2011 05:03 AM)zion_rulz Wrote: [\[CITE\]](#) @ Phizo: Thanks for your quick response; it was my bad that I didn't notice the caption minutely.
Another query : I tried on a site "http://mysite.co.uk" and got an error "The folder you entered does not appear to be valid. Please choose another."

Hope to get some light. Thanks once again.

Cheers :)

That's because it doesn't have WebDAV service enabled on it ;).

zion_rulz - April 24, 2011, 5:21 am

Thanks for the share indeed. Take care :)

ice³ - April 26, 2011, 10:56 am

Did some Googling for a nice dork:

"Microsoft-IIS/* server at" intitle:index.of

Although they might not have WebDAV on, of course.

Phizo - April 26, 2011, 2:08 pm

(Apr 26, 2011 10:56 AM)Sm3t Wrote: [\[CITE\]](#) Did some Googling for a nice dork:

"Microsoft-IIS/* server at" intitle:index.of

Although they might not have WebDAV on, of course.

Nice find.

Msg2fknsh0rt.

lordlogic - April 27, 2011, 7:00 am

wen i use this it works fine until the folder of webserver open but wen i try uploading any shell or things i get error that "u need permission to perform this action" sometimes i get "error 0x8007003a : the specified server cannot perform this operation"

Phizo - April 27, 2011, 7:03 am

(Apr 27, 2011 07:00 AM)lordlogic Wrote: [\[CITE\]](#) wen i use this it works fine until the folder of webserver open but wen i try uploading any shell or things i get error that "u need permission to perform this action" sometimes i get "error 0x8007003a : the specified server cannot perform this operation"

Can you upload other files?

Example: Pictures, HTML files, etc. You won't be able to upload a PHP shell.

lordlogic - April 27, 2011, 7:13 am

no i cant upload any kind of file (any how very very thanks for ur fast reply n this is one the best tut i ever found)

can i pm u the website addres

Phizo - April 27, 2011, 7:22 am

(Apr 27, 2011 07:13 AM)lordlogic Wrote: [\[CITE\]](#) no i cant upload any kind of file (any how very very thanks for ur fast reply n this is one the best tut i ever found)

can i pm u the website addres

Someone asked me about that error before. Unfortunately, I do not know of any way around it...Sorry :\

There are many other sites that you can attempt to exploit though ;)

lordlogic - April 27, 2011, 9:38 pm

phizo could u plss tell me any dork or search word to find these site cuz most of them i found wont

get connected or if connected tyhough copying of files wont b possible so phizo plss tell me some dorks or pm me some sites which i can hack n practise this

CyberM@X - April 27, 2011, 11:37 pm

Thanks that's an old post :) - but anyway, I like it :) - it's HQ, easy readable..

I already knew this :D! - but what would be more great, is that if you uploaded an ASP shell to some website so we could download it and use it for our own (;

Kindly regards,

Phizo - April 28, 2011, 1:09 am

(Apr 27, 2011 11:37 PM)Mr.Suxi Wrote: [\[CITE\]](#) Thanks that's an old post :) - but anyway, I like it :) - it's HQ, easy readable..

I already knew this :D! - but what would be more great, is that if you uploaded an ASP shell to some website so we could download it and use it for our own (;

Kindly regards,

Thanks bro, appreciated ;)

Sure, I'll upload an ASP shell right now :).

lordlogic - May 1, 2011, 8:12 am

bro can u plss tell how to be secure n hide my ip while doing this hack as proxys n hidemy ip software only works with broiswer what can i do to hide my ip

Phizo - May 1, 2011, 2:29 pm

(May 1, 2011 08:12 AM)lordlogic Wrote: [\[CITE\]](#) bro can u plss tell how to be secure n hide my ip while doing this hack as proxys n hidemy ip software only works with broiswer what can i do to hide my ip

Just use a proxy. Search for proxies on Google.

lordlogic - May 2, 2011, 3:21 am

no body wen we r using my computer to connect proxys dun work proxy only works with browsers

Phizo - May 2, 2011, 3:26 am

(May 2, 2011 03:21 AM)lordlogic Wrote: [\[CITE\]](#) no body wen we r using my computer to connect proxys dun work proxy only works with browsers

You can use programs such as proxy switcher to do that.

ice³ - May 25, 2011, 1:55 pm

Sorry to slightly dig the thread (deserves a though) but will this work on IPs? (<http://xx.xx.xx.xx/>) As I can scan for IPs fairly easy but having a hard time finding websites with webdav + IIS6,

Hound - May 25, 2011, 1:57 pm

This looks fun!

Attempting to fail now. . .

Phizo - May 26, 2011, 1:12 am

(May 25, 2011 01:57 PM)Harold Camping Wrote: [\[CITE\]](#) This looks fun!

Attempting to fail now. . .

Haha. Best of luck bro ;).

nikhil.thakur929 - May 27, 2011, 7:40 am

bro im nt able to paste anything in their box
no shell nothing

ice³ - May 27, 2011, 7:43 am

(May 27, 2011 07:40 AM)nikhil.thakur929 Wrote: [\[CITE\]](#) bro im nt able to paste anything in their box
no shell nothing
You sure it has Microsoft IIS 6?

Phizo - May 27, 2011, 6:57 pm

(May 27, 2011 07:40 AM)nikhil.thakur929 Wrote: [\[CITE\]](#) bro im nt able to paste anything in their box
no shell nothing
Care to elaborate? It's hard when you don't explain in detail.

skim - May 27, 2011, 8:42 pm

This is a very useful method, it might be bigger than SQLi.

pankajsharma - June 8, 2011, 7:54 am

bro i have done this Webdave before but when i try to open the url To which i have uplaoded my shell.asp;it just comes as a popup for download.

Can u help me?

Phizo - June 8, 2011, 9:03 am

(Jun 8, 2011 07:54 AM)pankajsharma Wrote: [\[CITE\]](#) bro i have done this Webdave before but when i try to open the url To which i have uplaoded my shell.asp;it just comes as a popup for download.

Can u help me?

Send me the link to your site.

pankajsharma - June 8, 2011, 11:02 am

(Jun 8, 2011 09:03 AM)Phizo Wrote: [\[CITE\]](#) Send me the link to your site.
Sent the links bro!
thanks !

Mrbadguy - June 8, 2011, 11:16 am

it says i dont have permission to access the directory and hence im not able to move the shell there
:|

Indir00t - June 9, 2011, 1:30 am

i have successfully mapped the device but i am unable to drag and drop

whats the problem dude plz help me

and i know the webdav is on

thanh159 - June 9, 2011, 3:14 am

i cant drag drop file . ??

CyberM@X - June 9, 2011, 3:52 am

This is an old school way ... never had worked for me : /

I got at the FTP and wrote something like "www.scootergalleri.dk" and nothing ... Mostly companies use a login :)..

asifali2000 - June 9, 2011, 5:54 am

BEST tutorial keep it more up

Phizo - June 9, 2011, 6:17 am

(Jun 9, 2011 05:54 AM)asifali2000 Wrote: [\[CITE\]](#) BEST tutorial keep it more up
Thank you ;).

Razor4x 5_0 - June 9, 2011, 6:21 am

Ehy Phizo, I tried this but i can't upload any files!!! when i try to put also a txt it tells me that there is an error to transferring the file!!!

Mx. - June 9, 2011, 11:01 am

Kinda crappy servers, most deny, and other 99% won't let u upload, nice tutorial though.

Phizo - June 14, 2011, 1:07 am

(Jun 9, 2011 11:01 AM)Mx. Wrote: [\[CITE\]](#) Kinda crappy servers, most deny, and other 99% won't let u upload, nice tutorial though.

Yeah, I know. Just use Google for searching.

VLxKaihoe - June 14, 2011, 2:35 am

You might want to add that this vulnerability affects only misconfigured IIS web servers that have PUT HTTP method enabled and writable directory/ies.

vb0xed - June 14, 2011, 3:02 am

thanks for the tuto , i will try it :)
bookmarked :)

Phizo - June 14, 2011, 11:29 pm

(Jun 14, 2011 03:02 AM)vb0xed Wrote: [\[CITE\]](#) thanks for the tuto , i will try it :)
bookmarked :)
You're most welcome my friend :).

kemnebunu1 - July 11, 2011, 7:13 am

m8 how do i search in google for servers with webdav ? i know how to search for servers with iis 6 but with webdav

Thanks in advance

marvelvarghese - September 13, 2011, 7:59 am

@kemnebunu1

Yup that's a problem. It's really sad to see that many people still use IIS 6.0 ... I always prefer NginX over all web servers.

dumar - September 21, 2011, 2:02 pm

Thank you very much, I have just found vulnerable website.
It helped me much :)

darkn3ssking - September 21, 2011, 2:47 pm

sound good tutorial, i think u can find in metasploit too

Gongoozle - January 25, 2012, 7:33 pm

thanks man ,this is very helpful,nice and simple,I like it

px-1 - January 27, 2012, 4:52 pm

This is a good lesson thanks a lot, unfortunately I do not have win 7...

px-1 - February 2, 2012, 10:21 am

(Jun 8, 2011 11:16 AM)Mrbadguy Wrote: [\[CITE\]](#) it says i dont have permission to access the directory and hence im not able to move the shell there :|
yes it says the same to me too ? "

BeggFoMercy - February 2, 2012, 10:49 am

thanks i like the simple tut ;) keep it up

Phizo - April 11, 2012, 5:33 am

(Sep 21, 2011 02:02 PM)dumar Wrote: [\[CITE\]](#) Thank you very much, I have just found vulnerable website.

It helped me much :)

I'm glad I helped out :).

Good luck to everyone.

deiski - April 12, 2012, 11:58 am

This is a really good tutorial, how many webserver are currently running IIS 6.0 (estimate a percentage or something)?

kma9090 - May 18, 2012, 5:37 am

really good tutorial however I am having a problem uploading a shell. I can upload a text file and images however when I try to upload the shell I get this error:

Error 0x80070780: The file cannot be accessed by the system

ViKtory1324 - May 27, 2012, 4:51 am

Bump.

I cannot upload anything, everytime I try it gives me error 0x80070780 or it says I do not have the rights. :/

Dogelan - May 29, 2012, 2:50 pm

<http://vulnerablesite.com>

It's an actual website LOL.

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

Crysan - May 29, 2012, 3:53 pm

It's the way how 1995 sites got hacked, but really nice tutorial for beginners.

I like your other tutorials too, keep that up bra.

NIIGHT HAWKE - July 19, 2012, 8:01 pm

really nice tutorial sir , thanku so much sir :)

Neqativ - September 8, 2012, 6:38 am

I cant find good sites ;| Any good dorks or sites ?

- Faity

N3p BoY - November 1, 2012, 6:34 am

Good clear and well written tutorial, thanks.

vimal - December 21, 2012, 8:14 am

Is there any way to overwrite existing image of an website with new one??

skyle17 - January 23, 2013, 1:06 am

(Apr 12, 2011 09:23 AM)Phizo Wrote: [\[CITE\]](#) Today I will be teaching a way to exploit very common a vulnerability and upload your shell and/or deface page to a Microsoft IIS 6.0 based website.

What you will need:

A windows machine.

Basic knowledge of shells.

A Microsoft/IIS 6.0 website with WebDAV enabled.

An ASP shell. - [http://www.\[removed\].com/?d=YU209ET7](http://www.[removed].com/?d=YU209ET7) << Download link for the shell. (Do not even try a PHP shell, it won't work. You can use your ASP shell to upload your PHP shell after though.)

This is how to perform the exploit in Windows 7:

Click start > Computer.

You will see this page: <http://img851.imageshack.us/i/iis1.png/>

Next you will want to click "Map network drive", it has been circled in the picture above.

Now a window will pop-up, it should look like this: <http://img638.imageshack.us/i/iis2.png/>

As you can see again. I have circled what needs to be clicked. So click on that then a window will come up asking you to click "Next", do so. After you have clicked the "Next" button, you should see this: <http://img850.imageshack.us/i/iis3.png/>

You will need to highlight/click that folder I circled, then hit the "Next" button once again. It should redirect you to this page: <http://img21.imageshack.us/i/iis4.png/>

I put "www.vulnerablesite.com" as an example. You have to type in "http://vulnerablesite.com" otherwise it will not work. It requires HTTP, not WWW. You will receive an error unless you use HTTP (once again, <http://vulnerablesite.com>)

Hit the "Next" button again, then it should come up with the site name with the output "vulnerablesite.com", you can name it whatever you like, this is what I put: <http://img130.imageshack.us/i/iis5.png/>

Except I changed it to "IIS 6.0 Exploit for HF - Phizo".

It doesn't matter what you put, just make sure you remember it.

Make sure the box is ticked (open when finished) then go ahead and hit finish.

Okay, we've exploited the website. Now we want to upload our files to the website. A new window has just opened, as you can see, we're connected to the websites files, however we're not aloud to view the files as we're unauthorized. No matter, we can still upload our shells and what other files we would like to upload.

Okay, I don't think I will need to put any pictures in this one, it's that simple. Follow my instructions:
#1 - Open the directory of where your ASP shell is (example: desktop, documents, or custom folder). Your ASP shell should have a name similar to "shell.asp;anything.jpg".

#2 - Drag your ASP shell from your custom folder into the website folder we just exploited. It should just go straight in there with no problems.

Tada! We have successfully uploaded our shell! Now all we have to do is go to:

<http://vulnerablesite.com/shell.asp:anything.jpg>.

I hope this helps.

Please do not leech this. I spent all my time making it. Full credit to me (Phizo).

My other webhacking tutorials:

MySQL injection: <https://hackforums.net/showthread.php?tid=1219987>

Cross Site Scripting: <https://hackforums.net/showthread.php?tid=1212236>

Remote File Inclusion: <https://hackforums.net/showthread.php?tid=1213488> thanks for this....

i am ddoser,iis hacker...?

Dyme - January 24, 2013, 3:46 am

I tried searching with this dork

Code "Microsoft-IIS/* server at" intitle:index.of

And none didn't work till page 6 (I'm at page 6 now)

It keeps saying that the map is invalid.

And I used HTTP://

Could it be patched?

eliekhoury123 - April 19, 2013, 9:40 am

phizio can iu have your email i need to talk to you

Phizo - April 19, 2013, 10:20 am

Why do people have to grave-dig stupid threads?

-?Divine- - April 19, 2013, 10:24 am

(Apr 19, 2013 10:20 AM)Phizo Wrote: [\[CITE\]](#) Why do people have to grave-dig stupid threads?

Because this.

(Jan 23, 2013 02:06 AM)skyle17 Wrote: [\[CITE\]](#) thanks for this....

i am ddoser,iis hacker...?

Oh and they want your email. Because fuck PMs.

danoon - April 19, 2013, 11:20 am

Haha nice tutorial really like this

#Skyline - April 19, 2013, 8:32 pm

(Apr 19, 2013 10:20 AM)Phizo Wrote: [\[CITE\]](#) Why do people have to grave-dig stupid threads?

Because there dumb. And don't look at a thread date.

tranceport - July 18, 2013, 1:13 pm

I can not see pictures.

pls reupload pictures

SHADOW REALM - September 17, 2013, 6:07 pm

Just tried it on an IIS 6 site then and it didn't work. Was there a patch for it (Or was just patch just update to 6.5)

Classy Llama - September 18, 2013, 3:41 am

(Sep 17, 2013 06:07 PM)LevelUp Wrote: [\[CITE\]](#) Just tried it on an IIS 6 site then and it didn't work.
Was there a patch for it (Or was just patch just update to 6.5)
Some one like your self should realize this thread is 5 months dead.

Phizo - September 18, 2013, 4:00 am

(Sep 18, 2013 03:41 AM)-ICE Wrote: [\[CITE\]](#) Some one like your self should realize this thread is 5 months dead.

Yup, hence why I'm going to close it.

This was written in 2011; I'm surprised people continue to dig it up.