

Forum:[Hack Forums](#)

Thread: [All about SHELLS](#)

AoEMonk - June 18, 2011, 12:10 pm

Welcome to my tutorial: All about SHELLS!

I am sure many have you have read about "Hacked / Defaced with shells", So I am pretty sure that the first thing that comes to your mind is "What the heck are these shells?" . So this article would give you complete idea about shells and its use.

Difference between FTP & Shells:

Many times I see that some of us know how to use the shell but once they have uploaded they get confused. So to start with, Let me give you some information about FTP:

Spoiler ([Click to View](#))File Transfer Protocol

Whenever you want to open your website, the first thing you will do is to get some web hosting for your self. That cud be either free or paid. When your get your hosting services, you create a website on your computer first and then upload it to your hosting server so it becomes a World Wide Web. This process of uploading the documents from your computer to your hosting server is done through FTP [File Transfer Protocol]. It basically looks like a program with 2 columns, one column shows your computer files and another shows your servers files. Just like when you copy the stuffs from some USB drive to your computer. So here, I will show you an example is how you would connect if you own go4expert. So when you want to connect your self to your web hosting server, following information is required in order to authenticate yourself:

Server : <ftp.go4expert.com>

Username: shabbir

password: whatever

So, once you put in this information, server understands that you are shabbir and gives you access to all the files on the server so you can work on it.

Shells:

Spoiler ([Click to View](#))Since you understand the FTP now, we know that none of us will get access to Go4expert's server because we don't have the username and password authenticate yourself. Somehow we can manage to get the access to G4E's FTP we can easily remove/edit/replace files. So we can destroy this entire forum and upload our own stuffs. That is when shells comes into the picture. Shells are a malicious PHP files which you will need to upload to any website, and once you execute it you will get access to its server directly WITHOUT authenticating your self.

Logic

Spoiler ([Click to View](#))Shell is not a tool that you can run and complete your work. As I said, its just a normal ".php" file, you have to find a way in any website to upload that shell. The Idea is, you upload the shell to any website so it will be saved on their server and it will give you the access to it.

Phase 1 : Uploading a shell:

Spoiler ([Click to View](#)) Suppose you want to hack "something.com". So the first thing that you will do is, open up "something.com", and try to find some place from where you can upload the files on the website. There are many such places for example, "file uploads, avatars, resume upload, cooking recipe uploads, upload your photo". So these are the places which will give you an opportunity to upload your shell. All you have to do is, try to upload the shell.php which is located in your computer and click on submit. So suppose you went to the webpage "something.com/submit_resume.php" and you uploaded your resume.

Phase 2 : Executing your uploaded shell:

Spoiler ([Click to View](#)) Once we have uploaded the shell as shown in "Phase:1", we know that its sitting on the server. The only thing we need to do now is to execute the shell from a browser so we get access to it.

Example:

So suppose i uploaded my shell as an attachment in THIS THREAD. SO now taht attachment is sitting on G4E's server. Now if we want to executive it, we will use following URL:

Code <http://www.go4expert.com/forums/attachment.php?attachmentid=456&d=1249607339> So that is the DIRECT url to the attachment which is called EXECUTION. In the same way if you execute your shell, it will take you to a webpage where you will see everything thats on the server. And you will have FULL ACCESS to remove/edit/replace/delete the files. So you are another shabbir!

Phase 3 : Defacing:

Spoiler ([Click to View](#)) Defacing is a word which means "replacing the current index file with our own index with our motive and slogan on it. So once you have access to the server, you are the king.

Different types of shells:

Spoiler ([Click to View](#)) There are many shells available, most of them are public and some of them are private. Most of them does the samething to give you the access of the server. "c99, r57, b0yzone, j32" are some very common and easily available shells.

Important Piece of advice:

Spoiler ([Click to View](#)) I would suggest you to download Code <http://www.wampserver.com/en/>, which lets you make your own server on your comptuer. And then try to use shells on it. Which will help you avoid hacking in live environment. Because, if webmaster is smart then, he can simply check the logs for that shell fine and track down your IP which executed the shell. Then you might be in problem.

Thanks for your time reading the article. Hope you liked it. Also guys, I'm taking suggestions on what to make a new tutorial :)

Dead Status - June 18, 2011, 1:13 pm

Excellent tutorial! It really helped to understand shells and how they work. I could never find a guide or tutorial. Thanks.

AoEMonk - June 18, 2011, 1:31 pm

No problem and thanks :) If you got any requests I'll gladly do a tutorial about it.

Dead_Status - June 18, 2011, 1:40 pm

Alright, i'll remember to keep that in mind.

PregoPastaSauce - June 23, 2011, 1:23 am

I would love a tutorial on the how to make some private shells :) PM me about it? :D

rubanrecobath - June 23, 2011, 1:38 am

awsome tutorial man great job

AoEMonk - June 23, 2011, 3:21 am

Thanks for the great feedback guys :)

Johnny87au - June 23, 2011, 3:29 am

awesome write up dude, could you explain in a full detailed tutorial how to do everything though
???? Check your pm box also hehe

depojones - June 23, 2011, 4:02 am

Great tutorial! Didn't know the difference until now :)

zacharyfxx - June 23, 2011, 4:32 am

Bumpity Bump Bumped nice tut

Frostbite™ - June 23, 2011, 4:51 am

Wow amazing thread, I didn't know what they were before. I'll definitely be using them a lot more now :)

Obi-Wan Cannabis - June 23, 2011, 4:57 am

I was just about to go search on wikipedia what were shells. The first thing I found was that shitty turtle of Mario Games. :D

Thanks for the tutorial!

AoEMonk - June 23, 2011, 5:00 am

Lol. Thanks for the feedback guys :)

thestapler42 - June 24, 2011, 9:30 am

great tut! love the practice website download haha ill definitely try it there!

!ron m@n - June 24, 2011, 11:47 am

N1ce tutorial keep it bro :)

beastboy46 - June 24, 2011, 11:50 am

the great tut ...really even the greatest noob can get it....wonderful explanation +1

Hmily[LCG] - June 24, 2011, 11:52 am

Excellent!!! Thank you very much! #1tutorial for this thread

Pok3-terr0r - June 24, 2011, 1:52 pm

wow nice tutorial i like it much!

Ephemeral - June 24, 2011, 1:56 pm

Nice tutorial, could do with a tad more detail, but still helpful to the newer lot!

Big Baller Shot Caller - June 24, 2011, 2:13 pm

I know what shells are used for now.

Are they the same one like people use for booters?

bernardbear - June 24, 2011, 10:01 pm

waw now i know what is shells . . .lol

M44M31 - July 8, 2011, 4:56 am

i knoes what shells are but this is def a good tutorial

oktalWind - July 8, 2011, 5:46 am

Thanks for this tutorial.

I wish you could write a tutorial on how to code our own shells, and how shells actually work.

But anyway, very good and very simple (maybe a bit too simple) intro on what a shell is.

conan_1 - July 8, 2011, 6:23 am

Nothing to say, Just a useful and helful tutorial

Thanks a lot mate, It'll comes in handy !! ;)

jalal77 - July 8, 2011, 6:27 am

man +Rep for u nice tuth...keep it up

shikhar.db - July 8, 2011, 11:40 am

Extremely nice tutorial and well defined. Hats off to you dude. <3

Gangsta. - July 8, 2011, 11:43 am

Really nice tut bro! Will help people out a lot. ?

Killer12 - July 8, 2011, 12:02 pm

Very nice tutorial

Thank you so much

answered a shitload of questions i had :D

Toaster - July 8, 2011, 1:22 pm

Is there any way of finding where the shell is stored on the server or is it just look until you find it?

1M S0 ViP - August 16, 2011, 11:57 pm

Thanks You! This was absolutely perfect. Explains it perfectly for people who have little or no prior knowledge to it. Much like myself. Thanks Man. Keep It Up!

AoEMonk - August 17, 2011, 7:48 am

No problem mate :) Glad you liked the tut, recommend it to others too!

Ace™ - August 17, 2011, 8:00 am

Awesome tutorial bro thanks alot for the share. Will help alot

Commodent - August 17, 2011, 8:35 am

Highly informative and clean tutorial. Bookmarked! :)

DataBus - August 17, 2011, 8:50 am

this is a good service very googd tutorial keep it up

Sychotik - August 17, 2011, 8:53 am

Thank you very much! Very good, and helped me a lot.

Are there types of shells that only work for different types of websites..or are they all universal?

AoEMonk - August 17, 2011, 9:10 am

I'm glad you guys like the tutorial :) It means the world to me.

-=WUNDERKIND=- - August 22, 2011, 6:07 pm

Server : <http://ftp.go4expert...>

Username: shabbir -->>dang man you put my name in Ther Dang
password: whatever

DsntExist - September 19, 2011, 8:58 pm

I read this article somewhere before I know it...

But anyway, it can't really be THIS easy to deface a website right?

Dr_RoX - September 20, 2011, 3:43 am

Thanks you bro nice tuto , Good djob

syngress - September 20, 2011, 4:34 am

tHIS WAS a great tut thanks for this xD hehehe

AoEMonk - September 20, 2011, 5:32 am

Thanks, glad you liked it! Tell me what you want on the next Tut.

Kommerzgandalf - September 20, 2011, 6:37 am

Nice tut bro,I'm about to try this :)

noober1001 - September 20, 2011, 6:51 am

Great tutorial.

I am using shells from many months.

But didn't know about these details.

Thank you so much for sharing this.

cka - September 20, 2011, 8:12 am

I liked the post its excellent very nicet and use full Can you make the tutorial of sql injuction when it done please alert me

tsukeru - October 6, 2011, 11:12 pm

Thankyou very much! Been looking around for a good tut to explain simple terms, this was a very useful read :P

Normally don't post as i feel to noobie to post a comment but had to for this one ;)

Now back to reading around for more explanation on things :D

sexynsmartjenny - October 8, 2011, 6:07 pm

ok, so now I understand how shells work, but where do i get some SHELLS? Can you give me

some shells to work with?