The Ultimate Defacing Guide

Table Of Contents

INTRODUCTION

Alright everyone. Welcome to the ULTIMATE DEFACEMENT GUIDE. You probably may be thinking, "Wow this thread is just pointless." Well, today we will be covering the entire corner of exploits, compiling, shells, and etc. This will definitely not be a waste of your time, I promise, if you are new at this, you will learn something from this tutorial. So lets begin shall we?

WTF Is this "Defacement" everyone talks about?

Basically, they are referring to defacing a website by finding an exploit to gain access to their admin panel. Once they have access, they proceed to upload their shell. Which we will cover later on. Now, the person has uploaded their shell onto the website, which then displays the defacement or etc.

[color=#32CD32]Now that you know what the term "Defacement" is, and you have a good idea of how the "hackers" do it, you probably are thinking, OKAY I WANNA DO THIS! Umm, no. There is quite a bit more you need to learn before we begin.

Three MAIN Methods for Exploiting

The following are some of the most popular ways of gaining access to your victims website.

SQL Injection - SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.

The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.

The injection process works by prematurely terminating a text string and appending a new command. Because the inserted command may have additional strings appended to it before it is executed, the malefactor terminates the injected string with a comment mark "--". Subsequent text is ignored at execution time.

Want to use this method? Go here: http://hackforums.net/showthread.php?tid=45621

Cross Site Scripting - Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. After the data is collected by the web application, it creates an output page for the user containing the malicious data that was originally sent to it, but in a manner to make it appear as valid content from the website. Many popular guestbook and forum programs allow users to submit posts with html and javascript embedded in them. If for example I was logged in as "john" and read a message by "joe" that contained malicious javascript in it, then it may be possible for "joe" to hijack my session just by reading his bulletin board post. Further details on how attacks like this are accomplished via "cookie theft" are explained in detail below.
Want to use XSS? Go here: http://www.hackforums.net/showthread.php...ht=XSS+TUT

RFI - Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web applications. When web applications take user input (URL, parameter value, etc.) and pass them into file include commands, the web application might be tricked into including remote files with malicious code.

Almost all web application frameworks support file inclusion. File inclusion is mainly used for packaging common code into separate files that are later referenced by main application modules. When a web application references an include file, the code in this file may be executed implicitly or explicitly by calling specific procedures. If the choice of module to load is based on elements from the HTTP request, the web application might be vulnerable to RFI.
An attacker can use RFI for:

-Running malicious code on the server: any code in the included malicious files will be run by the server. If the file include is not executed using some wrapper, code in include files is executed in the context of the server user. This could lead to a complete system compromise.
-Running malicious code on clients: the attacker's malicious code can manipulate the content of the response sent to the client. The attacker can embed malicious code in the response that will be run by the client (for example, Javascript to steal the client session cookies).

PHP is particularly vulnerable to RFI attacks due to the extensive use of "file includes" in PHP programming and due to default server configurations that increase susceptibility to an RFI attack ([4,5]).
Go here to learn RFI:
http://www.hackforums.net/showthread.php...ht=rfi+tut

Alright now that you have learned the 3 TOP methods of hacking, lets move on to the next step.

Once You Have the Admin Password

Alright, we are excluding the other 2 and going to be using SQL Injection as an example since it shows off the best example. You Now have the admin username and password, and you have decrypted it. (We will cover this later) You are ready to login and upload your shell! First you will need to find the administrator panel login. You can search around on HackForums for some useful tutorials on how to find the administrator panel quickly.

Once you have found the correct page, login with the details. If everything works, Grats! You are ready to upload your shell. Now we must create our code. This is where the main part of the tutorial comes in to play.

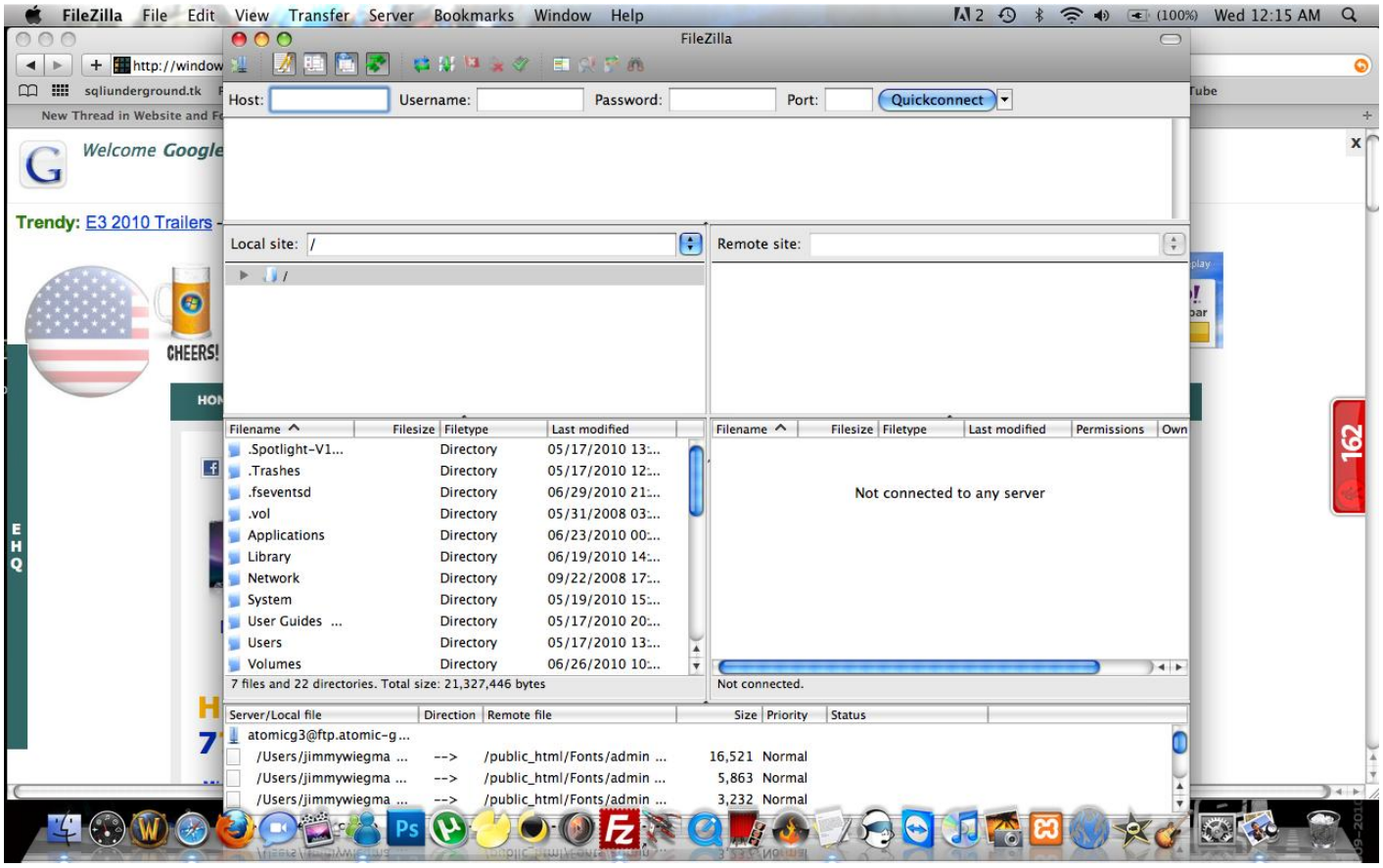
Compiling your Code

So you see all these epic deface sites, with these awesome skulls and music. And your asking HOW DO I DO THIS?!?! Well here is your answer. In order to do this, you must have some knowledge of HTML, as that is the default programming language I will be using. I also suggest that you join a defacement team, or ask a friend if they can provide you with a code you can upload. If you are clueless or just lazy, you can find an awesome application that can generate a random code for you!
Link: http://www.hackforums.net/showthread.php?tid=456483

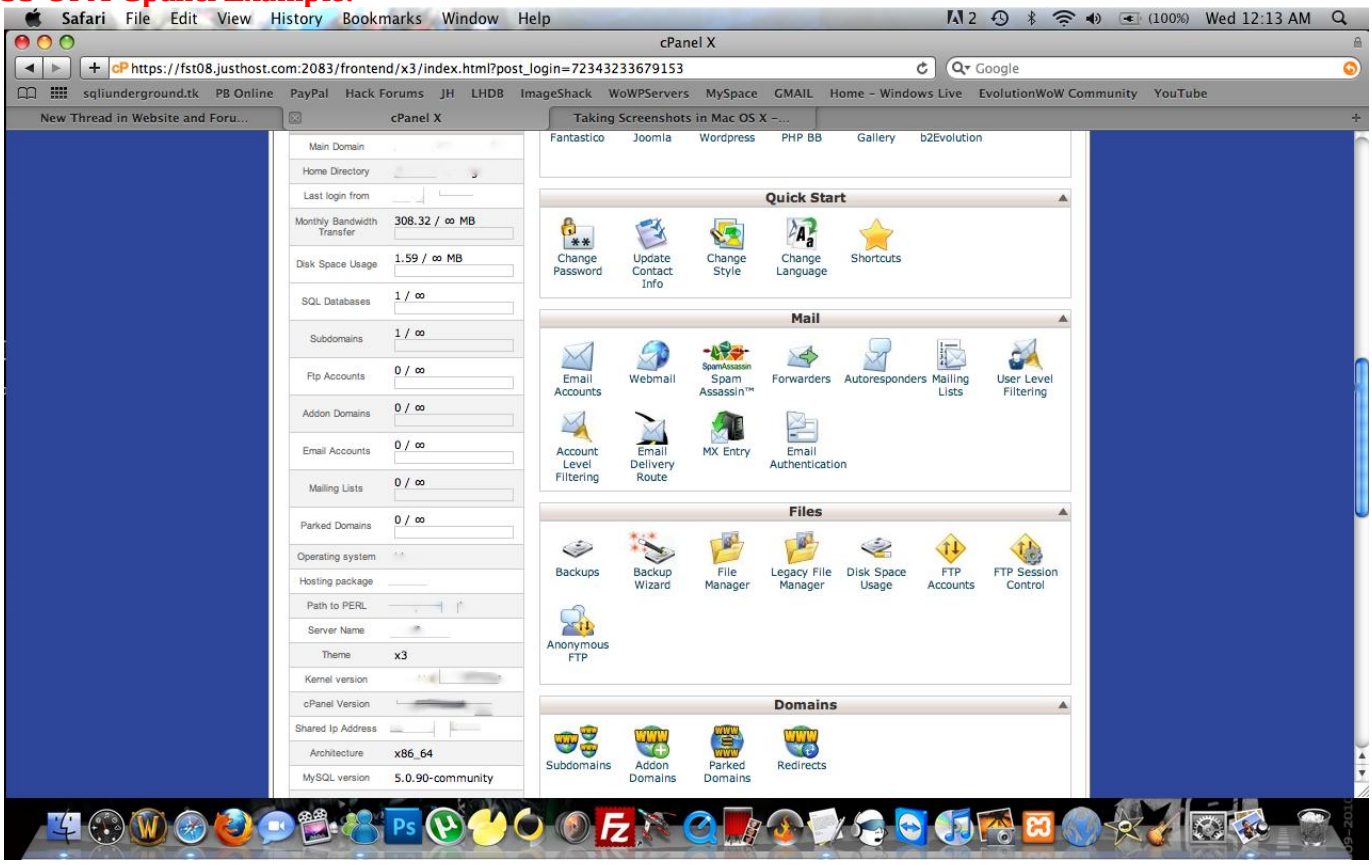
Uploading Your Defacement

Now that you have generated your code, you have it saved, and edited. Make sure to change to an .html file, or else it wont work on Firefox, Safari, GC, etc. Open up FileZilla, or your favorite FTP and connect to the FTP host which can usually be found somewhere on the website cpanel. Upload the file to public_html and make sure you delete are the other files (optional, helps protect you from getting traced). CHMOD the permissions, and then close out. Head on down the directory on which you installed the file, and you should see your deface page! Grats! You have successfully taken down a site.

Example of What FileZilla Looks Like:



SS Of A Cpanel Example:



Shells

I recommend this to advanced members. If you are an advanced defacer and would like to know how

to upload shells on vulnerable sites please go here:
http://www.hackforums.net/showthread.php...=shell+tut

Useful Tips

Selecting a good Proxy

Before you even think about defacing a website, please download a dedicated proxy/vpn. I recommend Cyberghost VPN. http://www.cyberghostvpn.com/ Make sure this is RUNNING AT ALL TIMES. I CANNOT STRESS THIS ENOUGH. The last thing you need is to go to jail for a few years because you did not mask your ip.

Prepare Yourself

Are you ready to actually hack someones website, destroy their content and upload a shell onto their webhost. Please ask yourself these questions before you continue. Clarify it with yourself, that you are doing something that is illegal and there is a chance you will be caught.

Decrypting

Most of the Passwords you find in SQL Injection will be an MD5 Hash and will sometimes be impossible to decrypt without the help of a skilled hacker or friend. Don't be afraid to ask on the forum for help with your crack! If you need help decrypting, feel free to send me a private message.

END

Well, its time for me to say goodbye. I hope you found this tutorial helpful in many ways. Not only does it tell you specifically how to upload your code/shell, but it also gives a definition on all exploits possible. Thank you to all the HF members who posted tutorials to also help me backup this tutorial. Thank you to the maker of the shell tutorial, as that really helped me out a lot. I worked very hard on this tutorial and I hope you all enjoy it.

~Convicted