[The Art of 0-Day Vulnerabilities, Part 1: STATIC ANALYSIS](https://null-byte.wonderhowto.com/how-to/art-0-day-vulnerabilities-part-1-static-analysis-0165311/)

* BY [**MR\_NAKUP3NDA**](https://creator.wonderhowto.com/q403_access_denied/)
* 10/13/2015 2:34 PM

APOLOGIZE

Hello my masters and colleagues, first of all I would like to apologize for my absence during the past month, to say that i was busy with some projects and decide to leave the white-side for a while and made some visits on the dark-side(every good COP has a dealer friend),i left null byte last month to learn more and come here to share with you ... I spent almost the whole last month trying to practice my knowledge, and there were moments where the systems were well protected, not that they were impossible to be hacked but hard or complicated, so I decided to start investigating deeply the functioning of these systems to see if I could find flaws instead of simple scans with some tools, I began by analyzing the code of applications in the case of open source , sending abnormal data and more, and in the end most were hacked and still others are in process.

btw gr33tz t0 :Ciuffy ghost\_ Phoenix750 f0r the gr3at j0b

INTRODUCTION

[](https://img.wonderhowto.com/img/original/46/41/63580338910890/0/635803389108904641.jpg)

According to wikipedia a zero-day (also known as zero-hour or 0-day) vulnerability is an undisclosed and uncorrected computer application vulnerability that could be exploited to adversely affect the computer programs, data, additional computers or a network.1 It is known as a "zero-day" because once a flaw becomes known, the programmer or developer has zero days (before disclosure) to fix it.

If you can find a flaw that the software authores do not know aobut "bingo" you got the gold.

The proccess

1-Responsible disclosure  
contact the sellers and give them time to fix(you can set a time limit before you put it public)

2-full disclosure  
go public with technical details of the bug without first giving the vendor an opportunity to fix it

As a white-hat you have the obligation to use the responsible disclousure some might give you money while others just greetings, but for black-hat guys some spread the vulnerabilities in some forums, use the vulnerabilities for their own benefits and more, I have personally seen exchanging vulnerabilities between black-hat guys and so on.

HOW TO FIND VULNERABILITIES?

[](https://img.wonderhowto.com/img/original/37/86/63580335104015/0/635803351040153786.jpg)

There are a lot of way to find a 0 day vulnerability, i will show you some of the most common ways to do it.

1-Open source or when you have access to the source code

1.1-Manual code review

when you have access to the source code its pretty much easier, what you can do is manual code review depending on which language it was made, here you need some programming skills in order to understand the code and find possible flaws

1.2- static analysis  
depending on the plataform which you are working with you can find a tool to automatically analyse the code.  
here is a good list of them  
<https://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis>  
my reconmendations:  
cppcheck  
flawfinder  
rats  
vcg  
its always good to combine all of them because they will produce different coverage

2-No access to the source code

2.1-Reverse enginnering

also called back engineering, is the processes of extracting knowledge or design information from anything man-made and re-producing it or reproducing anything based on the extracted information. The process often involves disassembling something and analyzing its components and workings in detail.

2.2-Binary static analysis  
tool that i used recently  
<http://www.veracode.com/products/binary-static-analysis-sast>

2.3 fuzzing "do random testing"

fuzzing is the art of inputing unexpected data in order to uncover unexpected behavior, fuzzing is often used to find vulnerabilities..

an example of that are the famous sql injections:  
'or''='  
ADMIN' OR 1=1#

using one of these tests above as username and password in some weak web forms can bypass the password authentication giving you the power to find a 0day sql injection.

[](https://img.wonderhowto.com/img/original/60/68/63580342040171/0/635803420401716068.jpg)

EXAMPLE :  
<?php  
$ip = getip();  
$tablename = $wpdb->prefix."limit*login";  
$tablerows = $wpdb->get*results( "SELECT `login*id`,  
`login*ip`,`login*attempts`,`attempt*time`,`locked*time` FROM `$tablename`  
WHERE `login*ip` = '$ip' ORDER BY `login*id` DESC LIMIT 1 " );*

function getip(){  
if (!empty($SERVER'HTTP\_CLIENT\_IP')) {  
$ip = $*SERVER'HTTP\_CLIENT\_IP';  
} elseif (!empty($*SERVER'HTTP\_X\_FORWARDED\_FOR')) {  
$ip = $*SERVER'HTTP\_X\_FORWARDED\_FOR';  
} else {  
$ip = $*SERVER'REMOTE\_ADDR';  
if($ip=='::1'){  
$ip = '127.0.0.1';  
}  
}  
return $ip;  
}  
?>

as example i will leave here this part of code that contains a vulnerability i know, its php and mysql, i hope you can find a 0 day vulnerability on it and leave it in comments.

for now thats all soon i will be going through all the ways we can find 0 days bugs and specific bugs for specific plataform..keep coming and dont forget to greet me if you find a 0 day vulnerability..