How to deface websites?

In this post, I will go over how skript kiddies deface other peoples websites, the tools they use, how they do it and what drives them to do it.

To deface websites there are a few ways to do it, first and most common is using SQLi to bypass or uncover admin credentials to then login to the site as an admin, after that they depend on a local file inclusion vulnerability which allows for files such as .php extensions to be submitted to the site(some sites only allow .jpg, .png, etc, extensions so to bypass this you need to put shell.php.jpg, shell.jpg.php, etc). After that they open their “image” (shell) in a separate tab (Right click the uploaded image and click "copy link location", then paste the link in a separate tab) and then log into their shell, after that they select a directory such as index.html, copy and paste their .html source code into the respective field and then press “add defacement”, after this, they navigate to the home page and watch as the home page of the site has now been replaced with their .html page.

So are web defacements targeted attacks? No, at least not most of the time, most of the time the skript kiddie is using a technique called “Google Dorking” to locate vulnerable websites that align with their dork.

Example of Google Dorks:

inurl:admin/index.php

inurl:administrator.php

inurl:administrator.asp

inurl:admin/index.php

inurl:adminlogin.aspx

As you can see the google dorks are looking for URLs that have “admin.aspx”, “Login”, “Admin panel”, etc. This tells Google to index websites with these URLs throwing back results to exposed administration panels. Most of the google dorks are outdated in terms of their design and security.

SQLi (Sequel injection) is used to bypass the login. Example of a SQLi payload is 1'or'1'='1. If one equals one, return the result if true. So next step is to copy and paste the sequel injection into the admin panel and hope (hackers don't hope) that it bypasses the login. A SQL injection attack takes advantage of a vulnerability in a web application that allows hackers to modify the queries that are being executed on the underlying database. Web applications that directly execute user inputs as a query are those that fall prey to SQL injections. This allows attackers to execute malicious queries, also known as malicious payloads on database servers.

Local file inclusion and Remote file inclusion is used to upload a shell.php file to the website so that the skid can upload their .html defacement page.

What you'll need to perform a website defacement:

Google Dork

SQLi payloads

LFI/RFI Vulnerabilities

Shell.php

File.html

In conclusion, web defacement's are not impressive, takes literally no skill, and is frowned upon among other hackers. The real hackers are the ones who develop the web shells that the skript kiddies use to copy and paste code into. You can go to sites like zone-h where these individuals fight to see who can deface the most websites.

Other common ways to deface sites is XSS, but we won't talk about cross site scripting in this post.

This is generally how all those Zone-H kids deface websites. They might also DOS the websites home page while they do it. You can use slowloris for this (sudo pip3 install slowloris).

Zone-H: https://www.zone-h.org

Written by Adam Wallwork (OP).