

Forum:[Hack Forums](#)

Thread: [Creating a Joomla Exploit Scanner - Part 1](#)

realsunjester - April 30, 2019, 5:24 pm

One of the first things we need to do is install Joomla. If you need a tutorial for it (which I hope not) [you can look at one here](#). Next, we need to find a way to determine if a website is actually a Joomla based website. First, we should establish a way to accept arguments, one of which will be the URL in question.

```
Code /* joomla exploit scanner by sunjester */
using System;

namespace Jex
{
    class Scanner
    {
        private static string url = string.Empty;

        static void Main(string[] args)
        {
            for(int i=0;i<args.Length;i++)
            {
                switch(args[i])
                {
                    case "-url":
                        Scanner.url = args[i+1];
                        Console.WriteLine(Scanner.url);
                        break;
                }
            }

            static bool isJoomla()
            {
                return true;
            }
        }
    }
}
```

Above the code has two methods. A main method that is accepting arguments and a method named isJoomla(), that will eventually determine if a website we provide to "Jex" (our joomla exploit scanner) is a Joomla based website. Below you can see how to compile and run Jex, and running it with an argument called -url.

We are going to need a method to get the source of a website or just a way to get the response code or a URL. Below you can see how we implemented the code and how it works.

```
Code          static string getResponseCode()
```

```

{
    if(Scanner.url == string.Empty) return "404";

    HttpWebRequest req = (HttpWebRequest)WebRequest.Create(Scanner.url);
    req.AllowAutoRedirect = false;
    HttpWebResponse res = (HttpWebResponse)req.GetResponse();
    return ((int)res.StatusCode).ToString();
}

```

In the video you can see that we have an error when the site returns a 404, we will address that with a simple try/catch block, but that's not important. In the video you can see we check for the directory administrator/. That directory is the default directory in Joomla for the admin panel, and on that page the default image is "joomla.png", we could use that as a way to check for a valid Joomla install. So that directory will be one to check for.

After thinking about it for a moment I thought of a simple way to determine at what percentage the site may be a Joomla site. We can check the directories and based on how many are found is a way to determine the percentage at which we think the site is a Joomla based website. For example, if we have 13 directories to check and 7 of them are 202 responses, our percentage is 54% (rounded up). Using this kind of formula (a simple one) we can eliminate the need to scan unwanted websites.

```

Code      static float isJoomla()
          {
            int found = 0;
            float perc;

            string[] joomlaDirs = {
                "administrator/",
                "templates/protostar/favicon.ico"
            };

            foreach(string dir in joomlaDirs)
            {
                string curUrl = Scanner.url + dir;
                Console.WriteLine("Checking directory: " + curUrl);

                if(getResponseCode() == "200")
                {
                    found++;
                }
            }

            perc = (found/joomlaDirs.Length)*100;
            return perc;
        }

```

So let's see if we can find some more directories to check in order to determine the percentage level for a possible Joomla based website. You can add more as you find them, however, let's go ahead and try this out on a live website.

Now obviously not all Joomla sites will have the above directories we are trying but the default

ones, probably vulnerable ones, will.