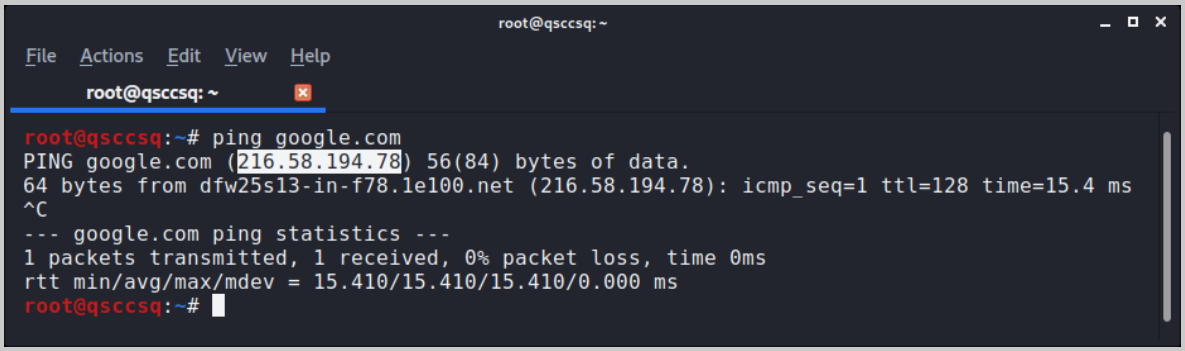
URLs on the Programmer Perspective

Uniform Resource Locator (URL) is the best way to access websites. For example, "google.com" is the URL we use to access the Google Search Engine. Using URL is a useful method for programmers to transfer both coding and created content. In order to better understand the URLs, the concept of Domain should be briefly examined. The websites actually transmit the content on the ports owned by IP addresses to us. For example, port 80 shows us HTML content. (Remember the document about the Ports you saw earlier.) However, entering long numbers (IP Addresses) to access a website would not make sense. Let's look at the working principle of the Domain concept with a short example.

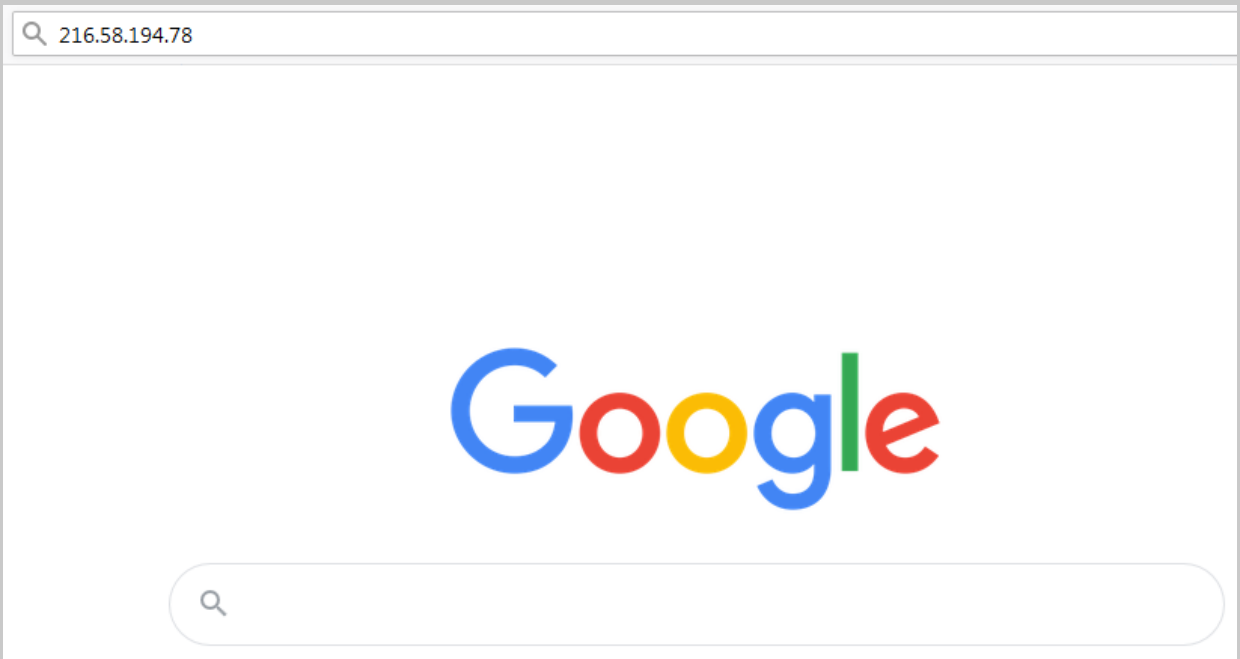
Let's learn the IP address of "google.com" address by opening a terminal on Kali Linux;

Code: ping google.com After 2 sec. Ctrl + C (for stopping)

IP: 216.58.194.78



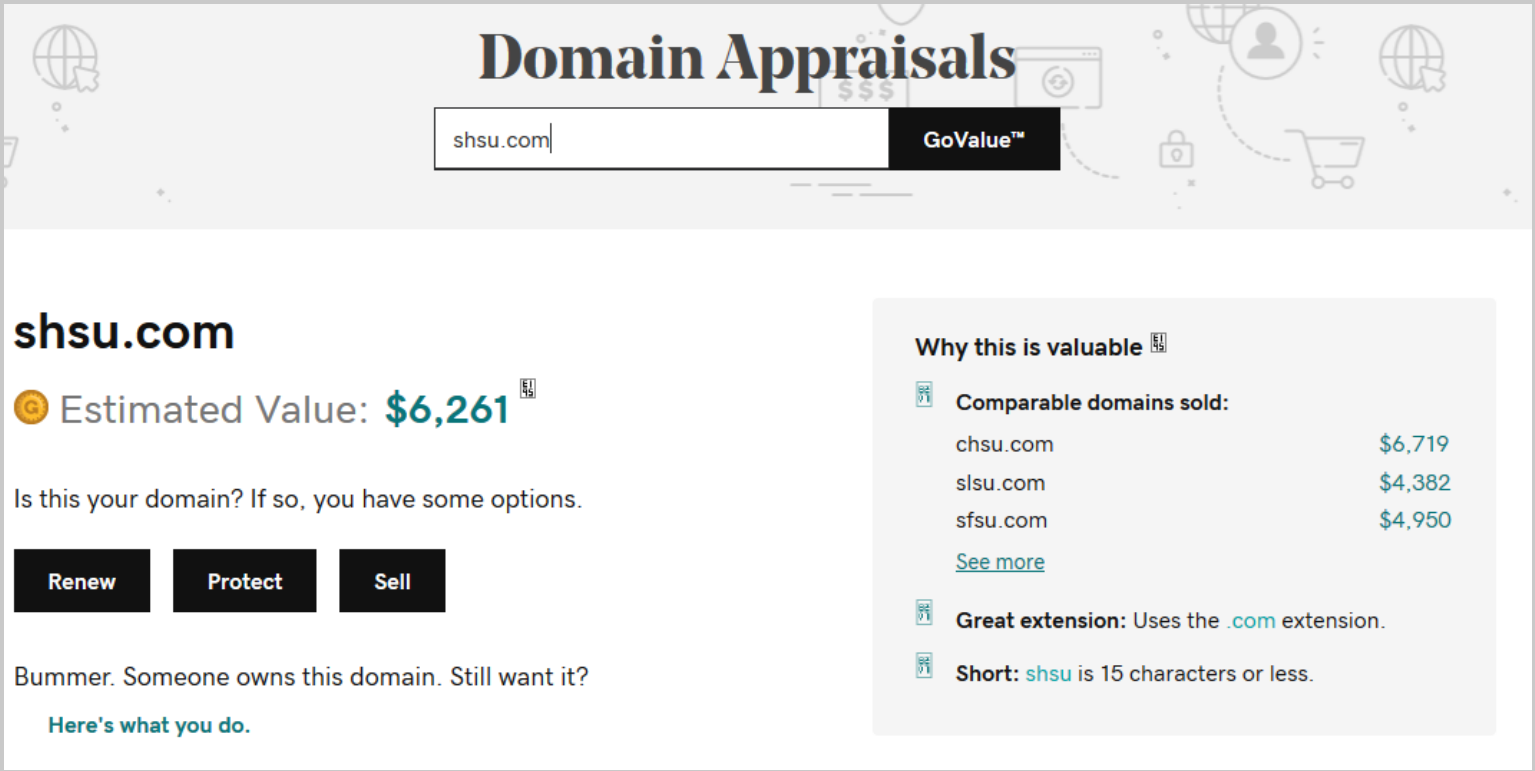
Now, let's write the IP address we obtained on the web browser and observe the result;



As can be seen, the address "216.58.194.78" that we wrote on the web browser directed us to the "google.com" site. The screen we see now is the 80th port number of the specified IP address. In fact, it needs to be searched as "216.58.194.78:80", but we did not need to write an additional port address because the websites automatically forward their contents to port number 80.

As stated, we use Domains instead of IP addresses to make websites easier to detect and use. In addition, Domains have their own market and this market is at a level that will not be underestimated. Let's use the application of a company that is a Domain provider to control the pricing of domain addresses;

https://www.godaddy.com/domain-value-appraisal



Since we perceive the concept of domain, we can return to the URL content. To give an example of the URL addresses from daily life, it can be used to represent the rooms of our homes. In this example, we can use Domain addresses as home addresses. Let's try to name the rooms according to the addresses in our URL addresses;

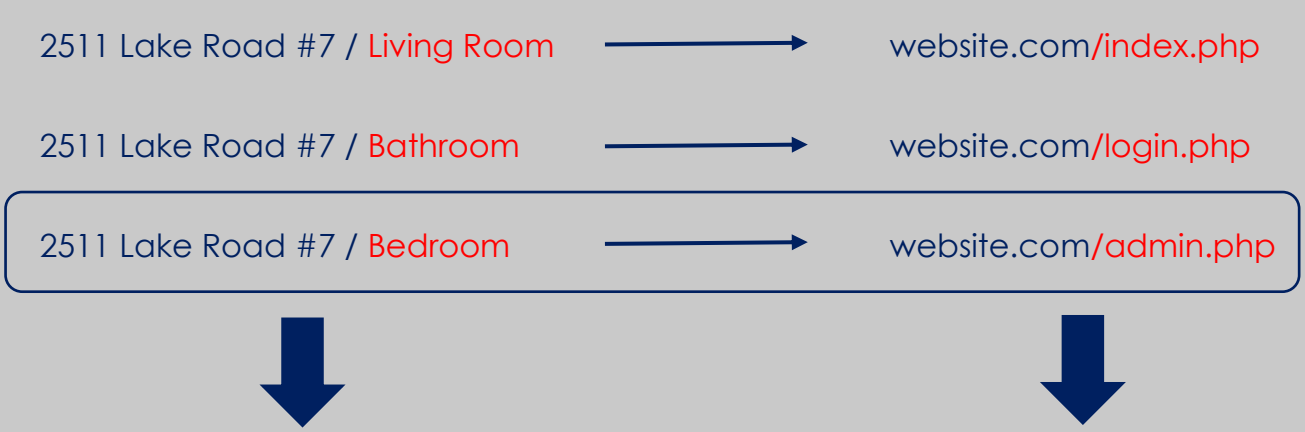
Home Address: 2511 Lake Road #7

Guest

URL: website.com

User

Now, let's look at the changes that our guest will make to visit the rooms on the URL;



As can be seen in the example, websites can only contain sections dedicated to administrators. However, according to the protocols of the websites, there is no precise and functional method to keep the guests away. For example, as an administrator, you can only grant access to a room from your IP address, but if you want to access your website somewhere else someday, you will fail. So what is the solution phase of programmers? Usually, programmers use only addresses known by administrators for private URL access. For example, instead of /admin.php, they can use addresses like /youcantfind.php.

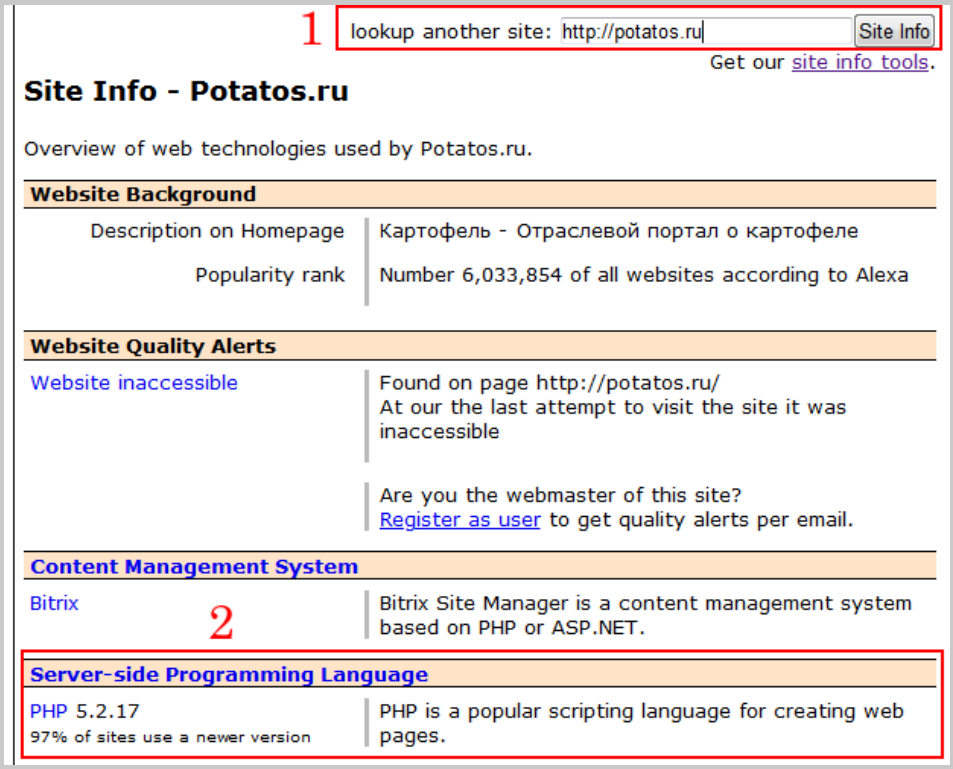
URLs on the Hacker Perspective

It is of great importance to identify URL addresses by hackers because the majority of the hacking processes performed are done through the Upload and Admin panels. For example, files with vulnerability codes such as r57 and c99 can be used on the target if access to the Upload panel is provided. In addition, a login panel is required to use the admin username and password obtained by the SQL Injection method. So what can be done to access admin and upload URL addresses changed by programmers? Kali Linux has many applications for the mentioned methods. One of the best practices is called Dirbuster. Dirbuster is a useful application to find all the URL addresses of the target website.

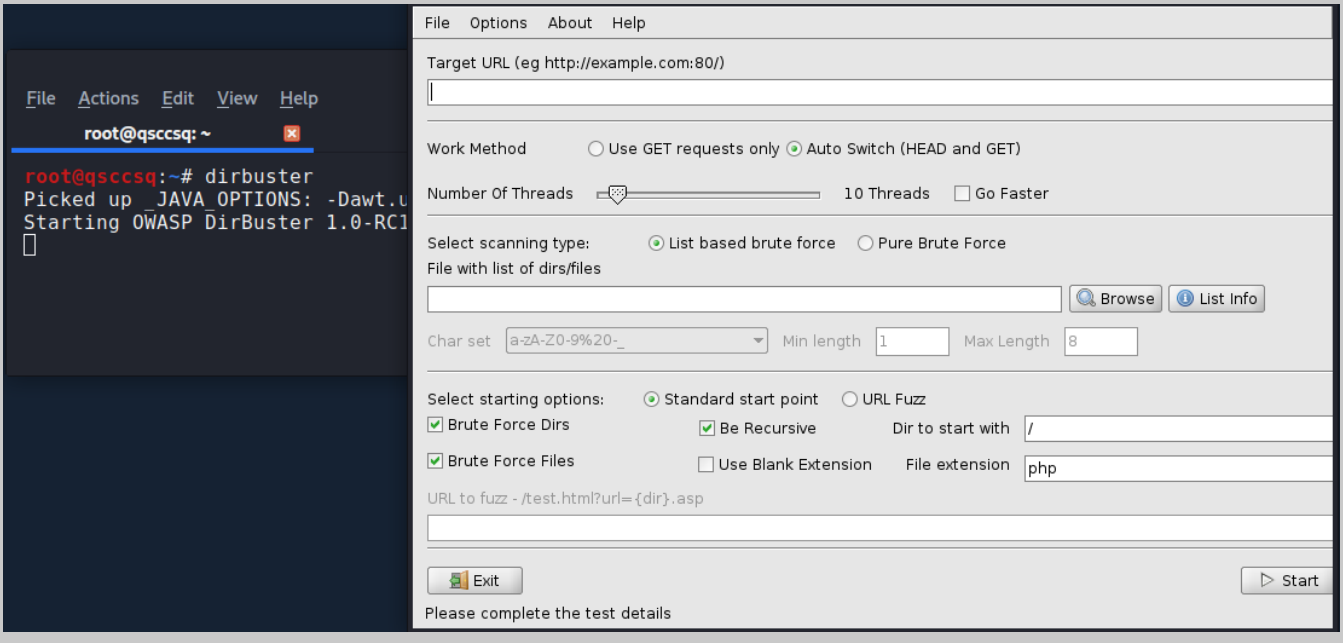
Let's try to access the admin panel of a target. All we have to do is access the application called Dirbuster via Kali Linux and then gather some information about the target;

Target: http://potatos.ru

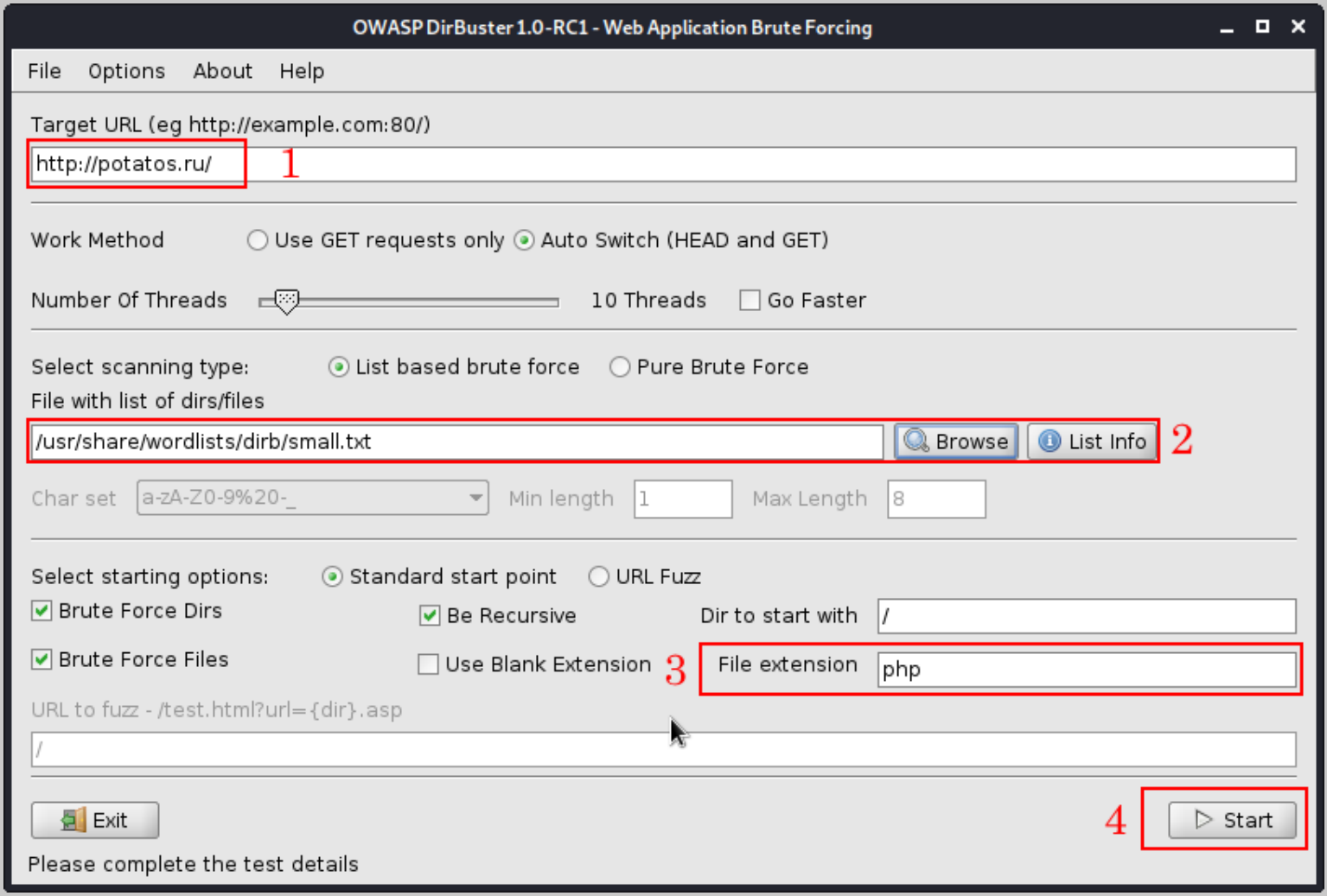
Information Gathering Website: https://w3techs.com/sites



According to the data we obtained from https://w3techs.com/sites (1), our target uses PHP technology (2). So the names of the rooms will end in .php. Let's check all the rooms (URL addresses) using Dirbuster. Let's type Dirbuster to the Kali Linux's terminal;



Now, let's prepare our application called Dirbuster to scan URL addresses;

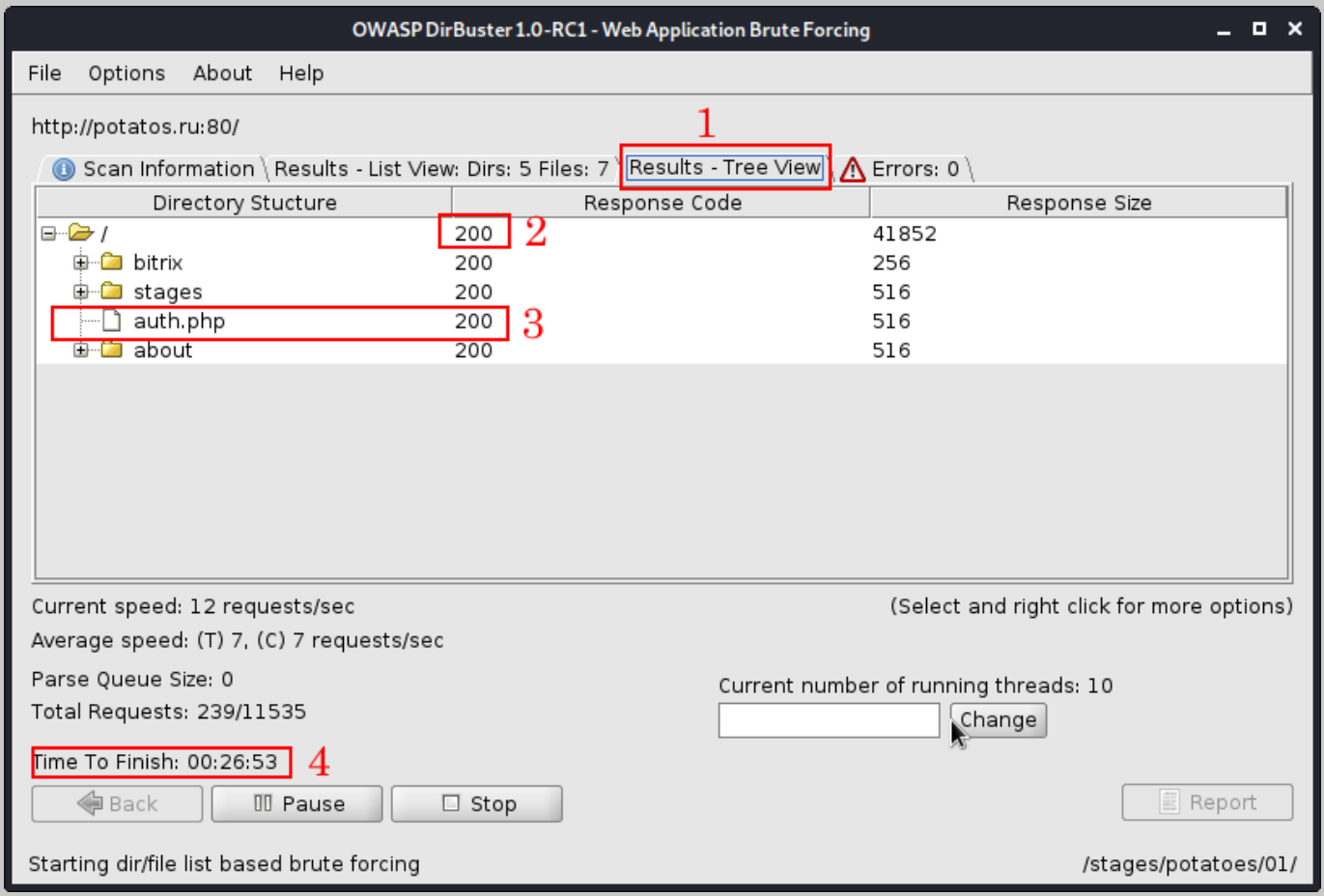


1: Type target address. (Don't forget http:// or https://)

2: Type /usr/share/wordlists/dirb/small.txt

3: We know that target technology is PHP then just type php. (If your target .NET type asp)

4: Let's Go!



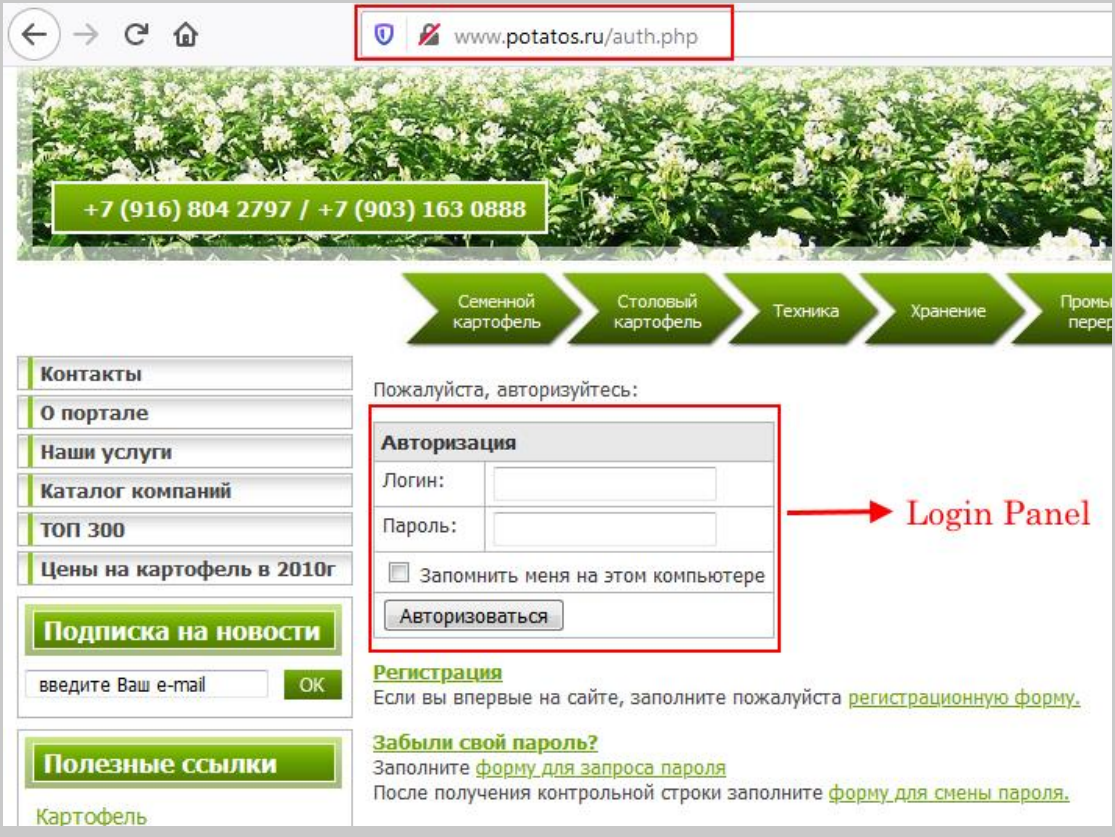
1: Click on it to see results.

2: Response number 200 means connection is OK.

3: Interesting URL (room) it could be a login page.

4: Time to Finish.

Let's look at the result by trying the URL address at number three;



Homework:

Target: https://www.realwire.com/

Don't forget that your website could be HTTP or HTTPS. First of all, try to find technology of website with https://w3techs.com/sites. Then, provide asp or php extension to Dirbuster. Don't rush, Dirbuster's working principle depends on your network speed. It could be take a while. Find target's login pages (TWO LOGIN PAGES EXIST). Take screenshots and create your own doc file.