**StringFixer**

**Submitted by :- Binay Chaudhary**

**Submitted to :- Er. Suman Basnet**

**Table of Contents page no**

**Introduction 3**

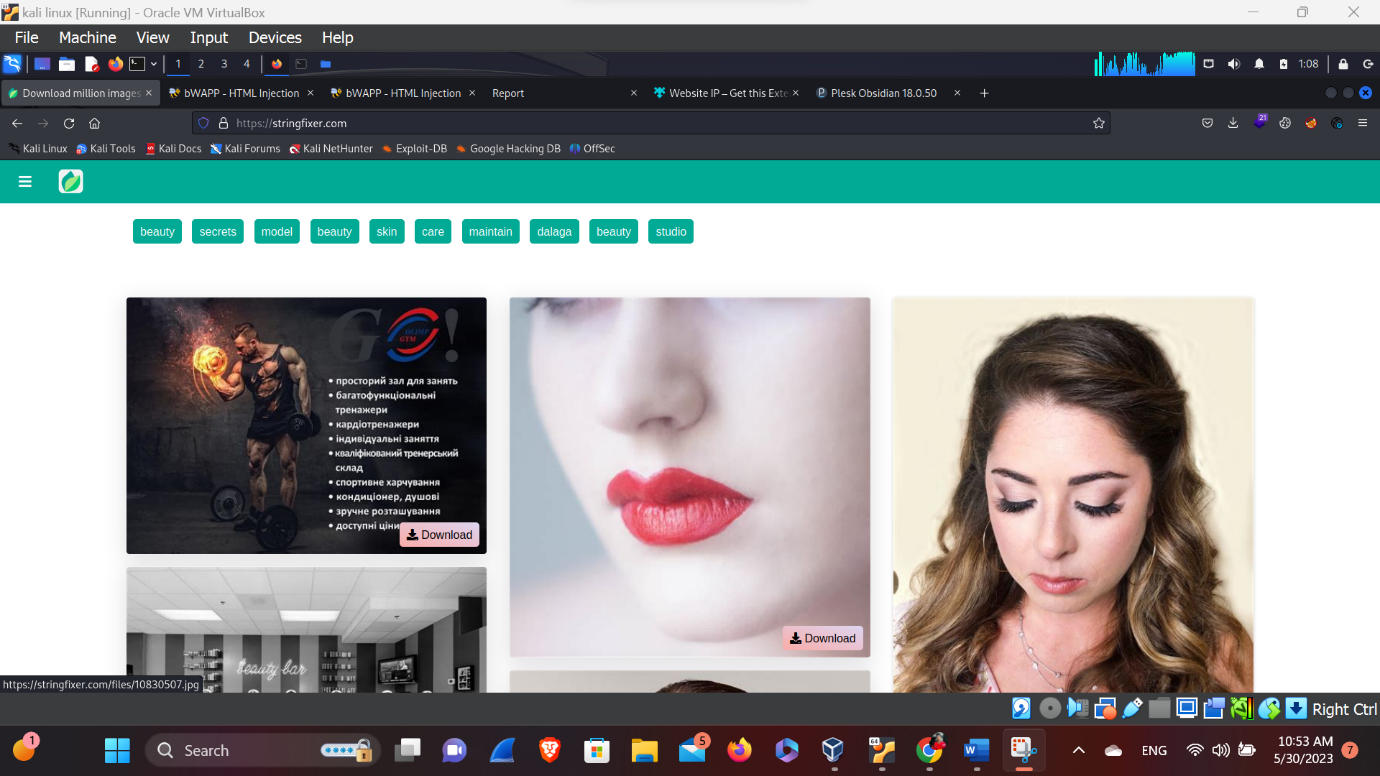
**Dirsearch 4**

**FUZZING 5**

**Exploitation 6**

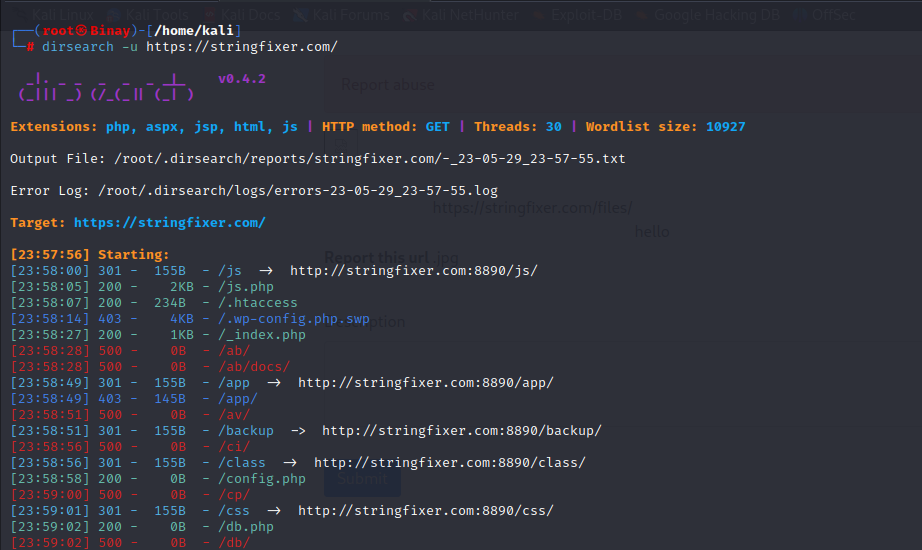
**Conclusion 7**

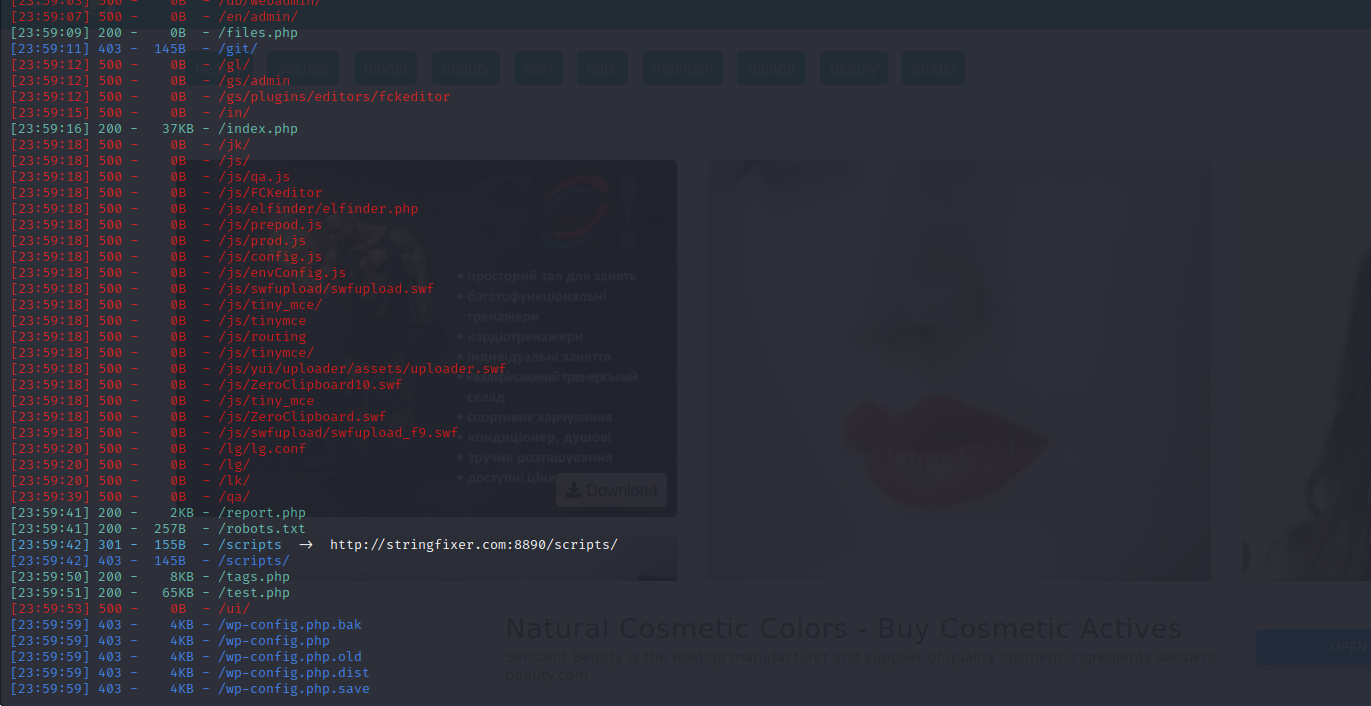
**Introduction**



Here, this site is a includes the beauty, Secrets, Models, beauty, skin etc. for that this site is a bunch of photography related and skin related. So, let’s explore for it’s hidden pages with the help of dirsearch.

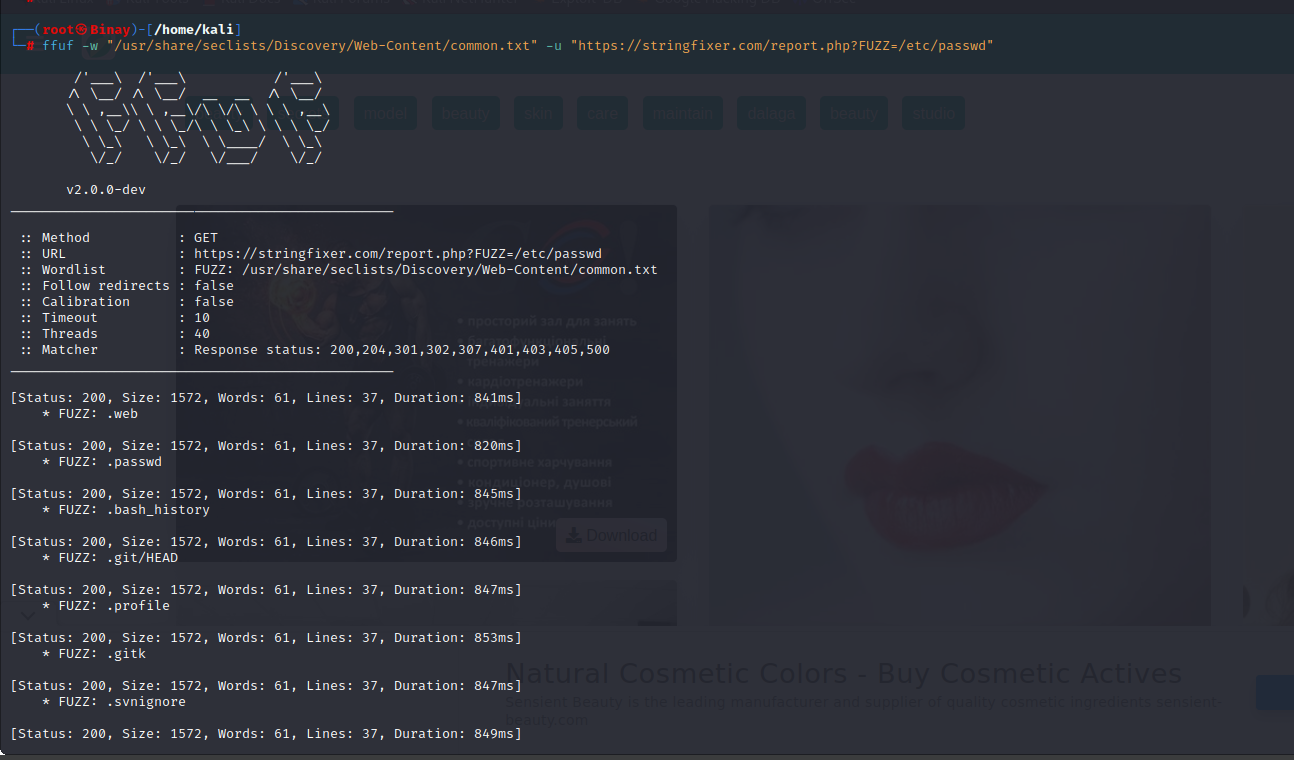
**Dirsearch**



Here, in this above picture we have found the directory that are hidden. So, let’s try to explore them one by one.

Here, in this picture we have found other file location so, let’s try to explore it. So, we have found some suspicious directory like /reports.txt. so, let’s try to fuzz them.

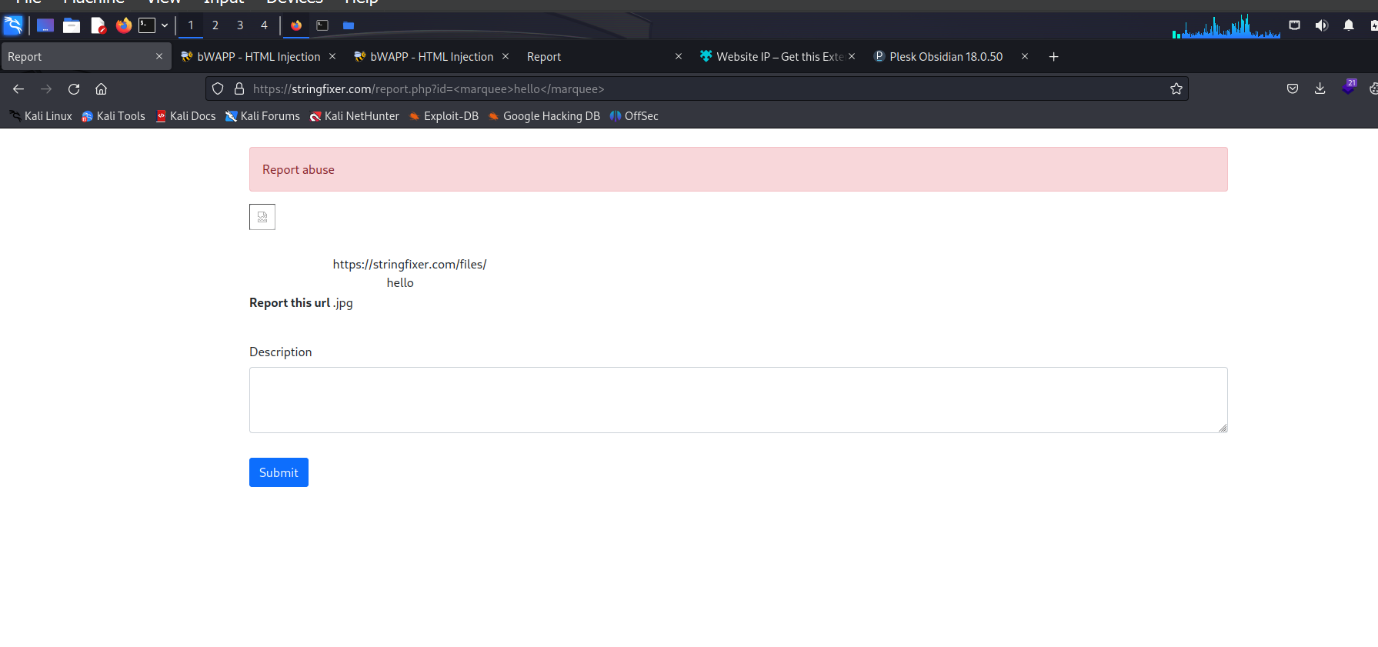
**FUZZING**



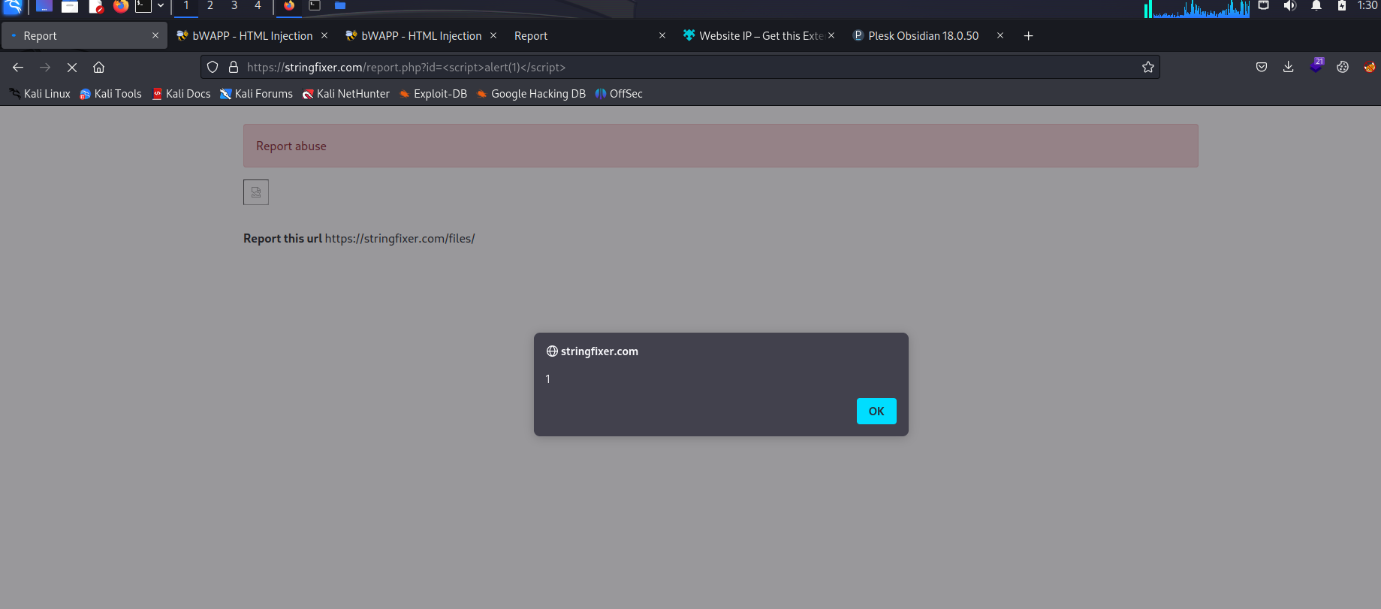
Here, we have found something by fuzzing so, lets try to remove the file size from the file that we’ve found.



Here, we have remove the file size and we’ve found that there is some get parameters called id.

**Exploiting**

Here, in this above picture we have found that there is some bug while putting the some of scripts in url like <marquee>hello</marquee>. So, try to put xss injection.



Here, in this above picture we have noticed something is popup due to the scripts of the javascript. So, we have founded alert box by using xss scripts like :- <script>alert(1)</alert>.

**Conclusion**

**Here, in this report we have to make sure that we have to sanitize the id parameters that are vulnerable to javascript so, we have to sanitize the javascript code.**