攻防世界Web赛题记录

原创

Bit0_ 于 2021-10-13 13:40:20 发布 2039 收藏
文章标签： 经验分享 web安全 网络安全

Cat

题目：

https://adworld.xctf.org.cn/task/answer?type=web&number=3&grade=1&id=4658&page=2

Writeup：

攻防世界-web-Cat(XCTF 4th-WHCTF-2017)_Sea_Sand息禅-CSDN博客

攻防世界 | CAT - laolao - 博客园

[CTF题目总结-web篇]攻防世界：Cat_T2hunz1-CSDN博客

知识点：

1.输入字符 get传递在网址中显示为%__ 为URL编码，URL编码中ascii字符的边界是%7F，输入大于此的%__可获得报错。

2.Django框架报错中可能存在数据库信息，找DATABASE

3.PHP通常使用cURL库与作为客户端与服务器通信，在cURL库的CURLOPT_POSTFILEDS选项中可以找到突破口，借此我们可以爆出数据库内容。GET传入@加文件路径，读取文件内容。

favorite_number

题目：

https://adworld.xctf.org.cn/task/answer?type=web&number=3&grade=1&id=5434&page=2

Writeup：

攻防世界 web高手进阶区 9分题 favorite_number_闵行小鱼塘-CSDN博客

攻防世界favorite_number_yjj哈哈哈的博客-CSDN博客

知识点：

1.POST传递数组 stuff[0]=admin

2.PHP数组溢出漏洞：数组中键值为0的元素与键值为4294967296的元素是同一个

3.绕过黑名单：使用跨行绕过 %0a 后接命令

4.命令ls 目录 可看指定目录

5.Linux系统 存储文件或文件夹的区域为索引节点inode， ls -i 查看

6.用tac绕过cat黑名单，从最后一行开始显示

7.用inode查找并显示文件 tac `find / -inum ____` inode对应必须是文件！不能是文件夹！

lottery

题目：

https://adworld.xctf.org.cn/task/answer?type=web&number=3&grade=1&id=4685&page=2

Writeup：

攻防世界Lottery&彩票系统 - LEOGG - 博客园

攻防世界Web lottery_hhh-CSDN博客_攻防世界lottery

攻防世界Web 高手进阶区：Lottery_feng的博客-CSDN博客

知识点：

1.扫目录robots.txt，提示.git获取源码

2.PHP弱类型比较：==的比较形式为弱类型，两端类型不一致时，会自动转换为同类型再比较。PHP中，当转换为 boolean 时，以下值被认为是 FALSE：布尔值 FALSE、本身整型值 0（零）、浮点型值 0.0（零）、空字符串，以及字符串 “0”、不包括任何元素的数组(注意,一旦包含元素,就算包含的元素只是一个空数组,也是true)、不包括任何成员变量的对象（仅 PHP 4.0 适用）、特殊类型 NULL（包括尚未赋值的变量）、从空标记生成的 SimpleXML 对象、所有其它值都被认为是 TRUE （包括任何资源）。所以 ture==任何非零数字 返回true。

FlatScience

题目：

https://adworld.xctf.org.cn/task/answer?type=web&number=3&grade=1&id=4809&page=2

Writeup：

FlatScience(SQLite注入) - HhhM

攻防世界-web：FlatScience - 顺时针--+ - 博客园

攻防世界web进阶区FlatScience详解 - 云+社区 - 腾讯云

知识点：

1.看源码提示<!-- TODO: Remove ?debug-Parameter! --> 添加debug参数

2.SQLite注入：

sqlite_master表中type/name/tbl_name/rootpage/sql记录着用户创建表时的相关信息

注入语句 1' union select 1,name from sqlite_master --+ //查询表名

1' union select 1,group_concat(sql) from sqlite_master --+ //查询建表时语句

3.sha1密文难以解密，根据提示，密文为文章中单词+Salz后进行sha1加密，解密方法为爬取所有文章中单词，依此+Salz后加密，判断是否与users表中admin对应加密后密码一致，枚举得到答案。

ics-07

题目：

https://adworld.xctf.org.cn/task/answer?type=web&number=3&grade=1&id=4921&page=2

Writeup：

XCTF-ics-07(floatval函数特性+Linux目录结构特性) - Hel10 - 博客园

攻防世界 ics-07 题_H9_dawn的博客-CSDN博客

XCTF:ics-07_羽的博客-CSDN博客

知识点：

1. SESSION无法伪造，必须根据代码流程改变SESSION的值。

2. floatval()函数将变量转换为浮点数，遇到字符时停止截取，返回值是一个数字。

PHP中 !== 意为不全等，即类型不同或值不同均true；!=意为不等，即类型转换后值不同为true，类型不同转换值相等为false，如$a=1,$b='1'，$a != $b不成立但是$a !== $b成立。题目中：

```
if (isset($_GET[id]) && floatval($_GET[id]) !== '1' && substr($_GET[id], -1) === '9')
```

floatval函数返回为数字，与'1'永远是满足 !== 所以只需考虑如何满足最后一位为9并正常查询id即可。因为sql查询语句中传入变量中碰见字符也会停止截取（好像是），所以此处传入1-9满足if，1和9之间有字符即可。

3.上传文件，绕过正则匹配。通常用1.php/.

```
preg_match('/.+\.ph(p[3457]?|t|tml)$/i', $filename)
```

- 文件名必须要包含 `.`
- 设置了文件后缀黑名单 `"php","php3","php4","php5","php7","pht","phtm","phtml","phar","phps"`，黑名单非常完善。
  - 如果文件名是通过get或post获取的，可采用 `php\n` 的方式绕过
  - 如果存在 `.htaccess` 可以通过上传 `.htaccess` 达到其他后缀的效果
  - 如果获取文件后缀的方式有问题，可以通过 `php/.` 方式绕过
- 文件内容不能包含 `<?`
  - 通过php小于7.0的可以通过 `<script lanague='php'>` 绕过
  - ```
    7.0.0   The ASP tags <%, %>, <%=, and the script tag <script language="php"> are rem
    5.4.0   The tag <?= is always available regardless of the short_open_tag ini setting
    ```
  - 如果能够控制文件名开头可以通过伪协议绕过： `php://filter` 等
- 文件要通过 `exif_imagetype` 的检查
  - 只检查文件头

4.chdir更改了代码执行目录，访问时要访问此目录下的代码指定的目录。
    ```

5.POST上传一句话木马时，<?php，?>与代码之间要有空格！

Confusion1

题目：

https://adworld.xctf.org.cn/task/answer?type=web&number=3&grade=1&id=4683&page=2

Writeup：

攻防世界-web-Confusion1（python模板注入SSTI、沙箱逃逸） - zhengna - 博客园

知识点：

1.根据提示得知网页搭建有python参与，优先考虑SSTI漏洞，尝试{{7*7}}，看返回结果判断。

2.运用常用模板注入被过滤，尝试request。

原payload:（使用<type 'file'>引用读取文件）

```
{{''.__class__.__mro__[2].__subclasses__()[40]('/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt').read()}}
```

request payload:

```
{{''[request.args.a][request.args.b][2][request.args.c]()[40]('/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.t
```

即把各方法传给a,b,c,d,并用request调用。

bug

题目：

https://adworld.xctf.org.cn/task/answer?type=web&number=3&grade=1&id=4768&page=2

Writeup：

攻防世界Web-bug - 高诺琪 - 博客园

攻防世界：web Bug_Zeker62的博客-CSDN博客

知识点：

1.登陆页面渗透，尝试找回密码，重置密码，抓取数据包分析,更改或获取管理员密码。

2.登陆后的请求数据头中，可能包含md5形式的加密认证字符串，可能为UID与用户名的组合，如UID:username.

3.XFF头绕过：127.0.0.1（最简单，不要想太多……

4.看见filemanager，估计与文件上传有关，upload

5.上传木马时，如果对内容进行php检测，使用

```
<script language="php">alert(@eval($_POST['cmd']))</script>
```

文件名改为php4