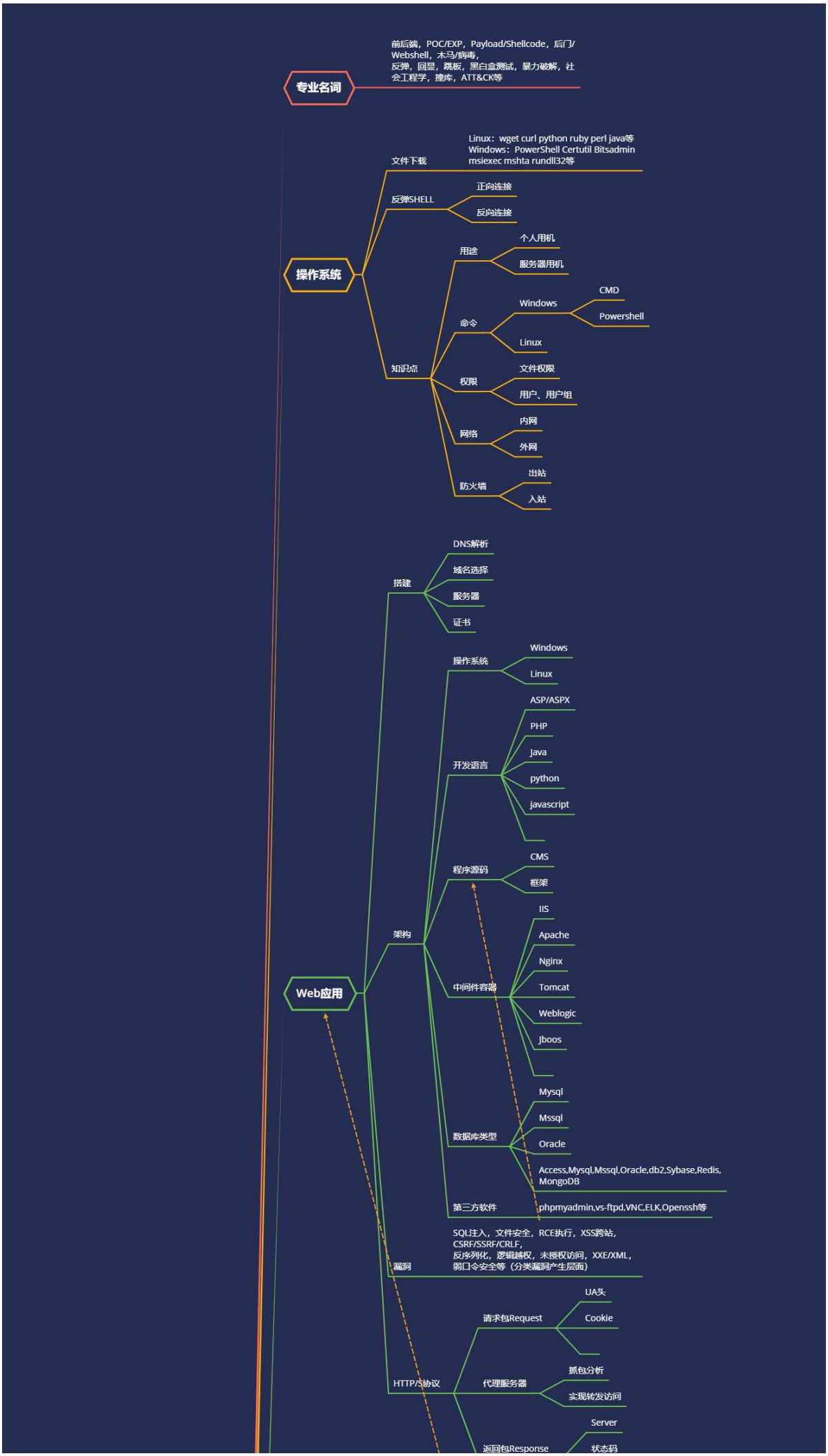
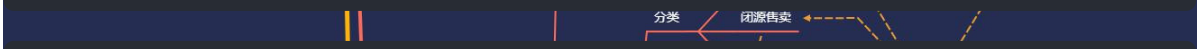
Day15　PHP 开发-个人博客项目&登录验证&Cookie&Session&验证码安全

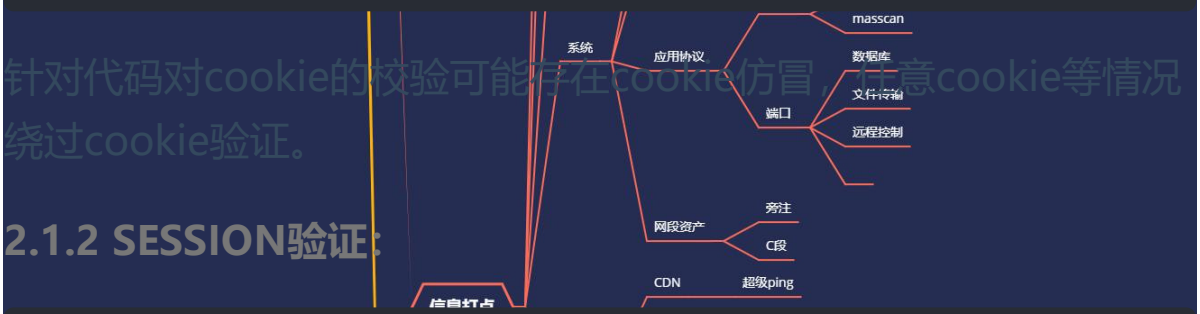

专业名词
前后端，POC/EXP，Payload/Shellcode，后门/Webshell，木马/病毒，
反弹，回显，跳板，黑白盒测试，暴力破解，社会工程学，撞库，ATT&CK等
操作系统
文件下载
Linux：wget curl python ruby perl java等
Windows：PowerShell Certutil Bitsadmin mshta rundll32等
反弹SHELL
正向连接
反向连接
知识点
用途
个人用机
服务器用机
命令
Windows
CMD
Powershell
Linux
权限
文件权限
用户、用户组
网络
内网
外网
防火墙
出站
入站
Web应用
搭建
DNS解析
域名选择
服务器
证书
架构
操作系统
Windows
Linux
开发语言
ASP/ASPX
PHP
Java
python
javascript
程序源码
CMS
框架
中间件容器
IIS
Apache
Nginx
Tomcat
Weblogic
Jboos
数据库类型
Mysql
Mssql
Oracle
Access,Mysql,Mssql,Oracle,db2,Sybase,Redis,MongoDB
第三方软件
phpmyadmin,vs-ftpd,VNC,ELK,Openssh等
漏洞
SQL注入，文件安全，RCE执行，XSS跨站，
CSRF/SSRF/CRLF，
反序列化，逻辑越权，未授权访问，XXE/XML，
弱口令安全等（分类漏洞产生层面）
HTTP/S协议
请求包Request
UA头
Cookie
代理服务器
抓包分析
实现转发访问
返回包Response
Server
状态码


```php
<form action="" method="POST">

    帐号：<input type="text" name="user">
    密码：<input type="password" name="pass">
    <input type="submit" value="提交">

</form>
<?php
header("Content-Type:text/html;charset=utf-8");
include('../config/conn.php');
/**
 * Created by PhpStorm.
 * User: xiaodi
 * Date: 2021/12/30
 * Time: 12:28
 */
$username=$_POST['user'];
$password=md5($_POST['pass']);
//echo $password;
```

```php
$sql="select * from sy_adminuser where username='$username' and password='$password'";
echo $sql;
$result=mysql_query($sql,$conn);
if (mysql_num_rows($result)){
    setcookie('user',$username,0,'/');
    header('Location: index.php');
}
```




```php
<?php
/**
 * Created by PhpStorm.
 * User: xiaodi
 * Date: 2021/12/30
 * Time: 12:28
 */
header("Content-Type:text/html;charset=utf-8");
$user=$_COOKIE['user'];
if ($user==""){
    header("Location: login.php");
    exit;
}else{
    echo "欢迎登陆管理员首页！";
}
```



针对代码对cookie的校验可能存在cookie仿冒，任意cookie等情况绕过cookie验证。

2.1.2 SESSION验证：

```php
<form action="" method="POST">

```

```
    帐号：<input type="text" name="user">
    密码：<input type="password" name="pass">
    <input type="submit" value="提交">

</form>
<?php
header("Content-Type:text/html;charset=utf-8");
include('../config/conn.php');
/**
 * Created by PhpStorm.
 * User: xiaodi
 * Date: 2021/12/30
 * Time: 12:28
 */
$username=$_POST['user'];
$password=md5($_POST['pass']);
$captcha=$_POST['captcha'];
//echo $password;
$sql="select * from sy_adminuser where
username='$username' and password='$password'";
echo $sql;
$result=mysql_query($sql,$conn);
while($row=mysql_fetch_array($result)){
    session_start();
    $_SESSION['username'] = $row['username'];
    //echo $_SESSION['username'];
    header('Location: index.php');
}
```

```
<?php
/**
 * Created by PhpStorm.
```

```
 * User: xiaodi
 * Date: 2021/12/30
 * Time: 12:28
 */
header("Content-Type:text/html;charset=utf-8");
session_start();
$username=$_SESSION['username'];
if($username=='admin'){
    echo '欢迎登陆管理员首页！';
}else{
    echo "请登录后访问！";
}
```

针对session验证问题，可能会产生会话劫持问题，当用户登录某个页面时，会在服务器端产生session信息，攻击者盗用用户session欺骗目标网站。

2.2 后台验证-验证码&万能密码等

2.2.1 验证码问题

代码：

```
<?php
session_start();//必须位于脚本的最顶端
$image=imagecreatetruecolor(100,
30);//imagecreatetruecolor函数建一个真彩色图像
//生成彩色像素
$bgcolor=imagecolorallocate($image, 255, 255,
255);//白色背景      imagecolorallocate函数为一幅图像分配颜色
$textcolor=imagecolorallocate($image,0,0,255);//蓝色文本
//填充函数，xy确定坐标，color颜色执行区域填充颜色
```

```
8  imagefill($image, 0, 0, $bgcolor);
9  $captch_code="";//初始空值
10
11 //该循环,循环取数
12 for($i=0;$i<4;$i++){
13     $fontsize=6;
14     $x=($i*25)+rand(5,10);
15     $y=rand(5,10);//位置随机
16     //  $fontcontent=$i>2?
   chr(rand(97,122)):chr(rand(65,90));//是小写，否则是
   大写
17     $data='abcdefghijkmnpqrstuvwxyz3456789';
18
    $fontcontent=substr($data,rand(0,strlen($data)-
   1),1);
19
    $fontcolor=imagecolorallocate($image,rand(0,100
   ),rand(0,100),rand(0,100));//随机的rgb()值可以自己
   定
20
21
    imagestring($image,$fontsize,$x,$y,$fontcontent
   ,$fontcolor); //水平地画一行字符串
22     $captch_code.=$fontcontent;
23 }
24 $_SESSION['authcode']=$captch_code;//将变量保存再
   session的authcode变量中
25
26
27 //该循环,循环画背景干扰的点
28 for($m=0;$m<=600;$m++){
29
```

```
30      $x2=rand(1,99);
31      $y2=rand(1,99);
32
     $pointcolor=imagecolorallocate($image,rand(0,25
    5),rand(0,255),rand(0,255));
33      imagesetpixel($image,$x2,$y2,$pointcolor);//
    水平地画一串像素点
34  }
35
36  //该循环,循环画干扰直线
37  for ($i=0;$i<=10;$i++){
38      $x1=rand(0,99);
39      $y1=rand(0,99);
40      $x2=rand(0,99);
41      $y2=rand(0,99);
42
     $linecolor=imagecolorallocate($image,rand(0,255
    ),rand(0,255),rand(0,255));
43
     imageline($image,$x1,$y1,$x2,$y2,$linecolor);//
    画一条线段
44
45  }
46  header('content-type:image/png');
47  imagepng($image);
48  //销毁
49  imagedestroy($image);
50  ?>
```

```
1  <!DOCTYPE html>
2  <html lang="en">
3  <head>
```

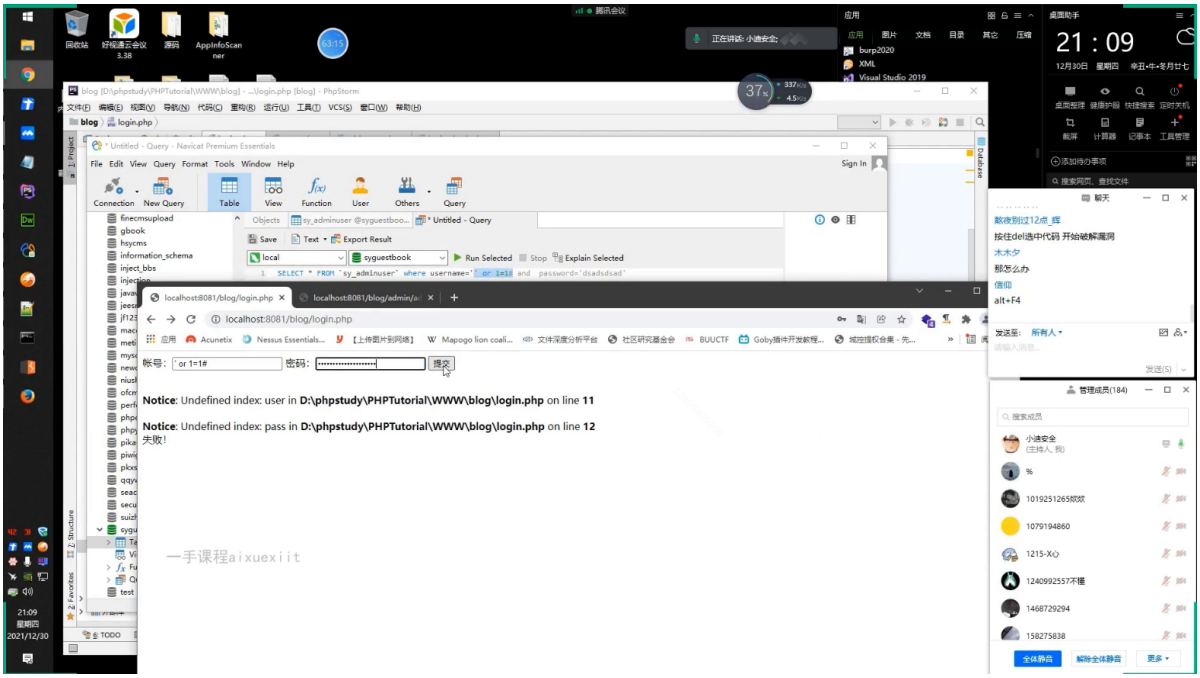
```
    <!-- 简单的表单提交代码 -->
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>简单验证码的实现</title>
</head>
<body>
<form method="post" action="">
    帐号：<input type="text" name="user">
    密码：<input type="password" name="pass">
    <p>验证码图片:<img src="code.php" onClick="this.src='code.php?nocache='+Math.random()" style="cursor:hand" alt="点击换一张"/>点击图片可更换验证码</p>
    <p>请输入图片中的内容:<input type="text" name="authcode" value=""/></p>
    <p><input type="submit" width="20px" height=19px value="提交"></input></p>
</form>

</body>
</html>

<?php
include('config/conn.php');
header("Content-type: text/html; charset=utf-8");
// session 存值并匹配用户输入值
if (isset($_REQUEST['authcode'])) {
    session_start();
```

```php
    if (strtolower($_REQUEST['authcode'])==$_SESSION['authcode']) {//strtolower转化为小写的函数
        echo"输入正确！";
        $username=$_POST['user'];
        $password=md5($_POST['pass']);
        $sql="select * from sy_adminuser where username='$username' and password='$password'";
        $result=mysql_query($sql,$conn);
        if(mysql_num_rows($result)){
            $row=mysql_fetch_array($result);
            echo '成功！';
            session_start();

 $_SESSION['user']=$row['username'];//讲查询结果的数据进行赋值
            header("Location: admin/add_news.php");
        }else{
            echo '失败！';
            //header("Location: login.php");
        }
        # code...
    }
    else{
        echo"输入错误！";
    }
    exit();
}
?>
```

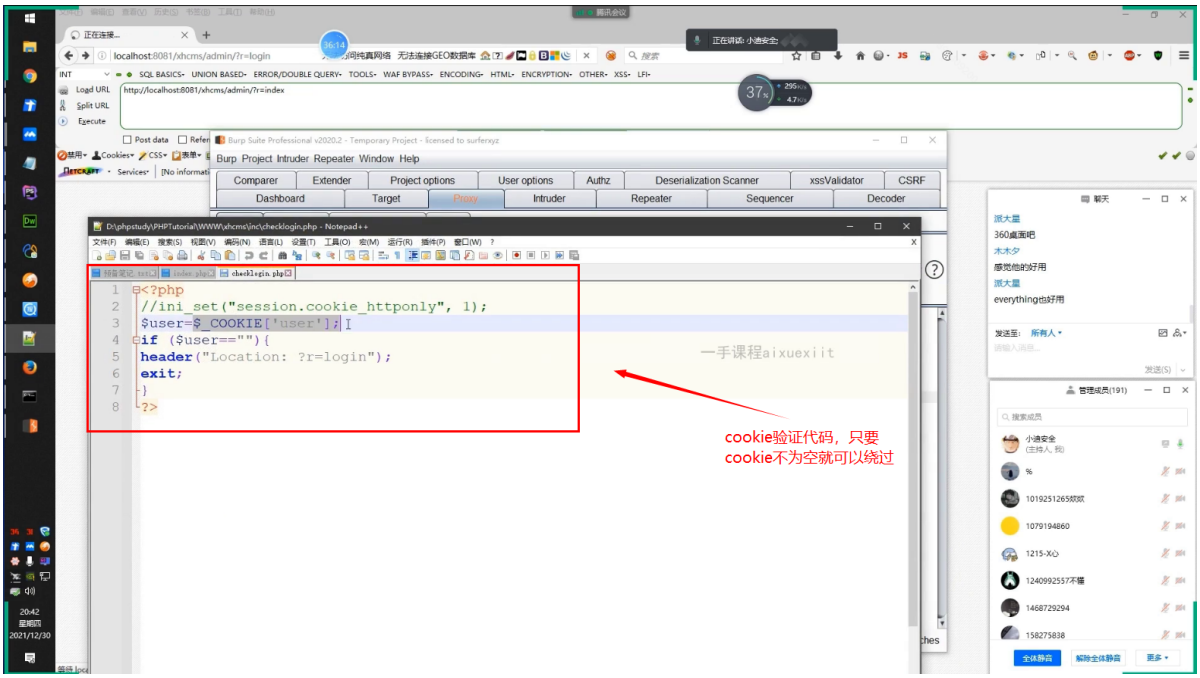
针对以上代码，验证码在输入错误时并没有销毁session信息，导致下一次重新登陆的时候，依然可以使用上一次的session信息，这样验证码就形同虚设，可以对用户名密码采用暴力破解，而不用管验证码。

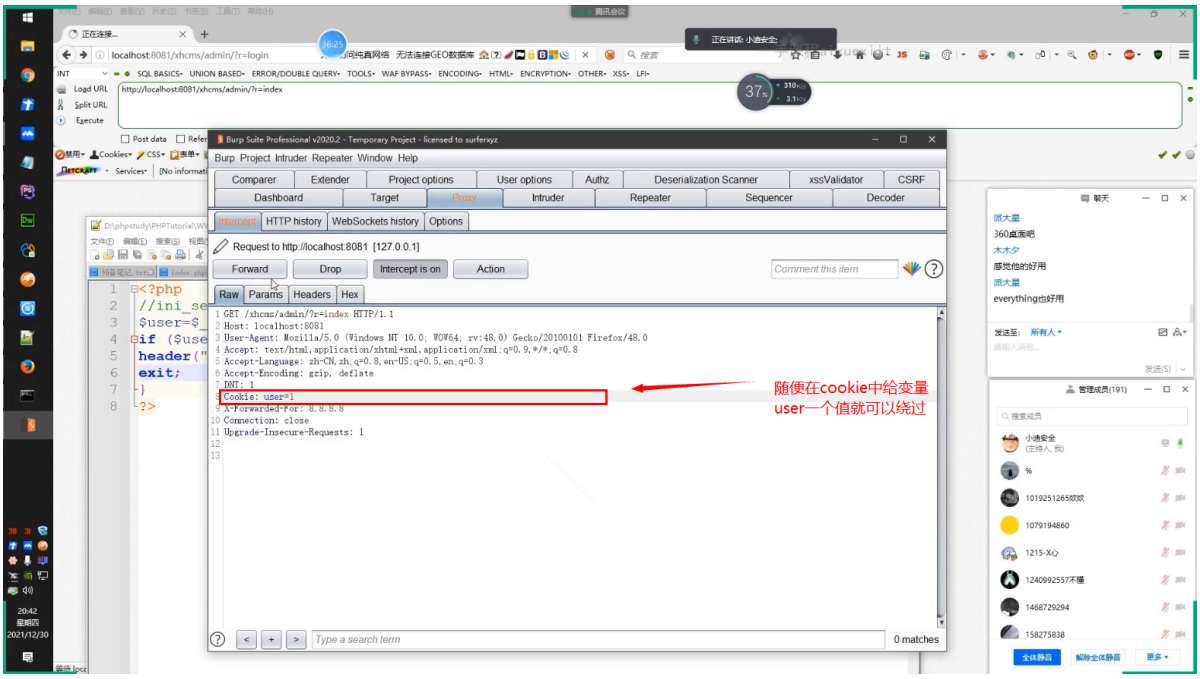
2.2.2 万能密码问题

有些程序员对用户名密码校验的代码写的不严谨，可以直接使用万能钥匙将用户名密码做修改，带入数据库查询：



2.2 本地靶场-某 CMS 后台登录验证 COOKIE 脆弱





不用账号密码直接进入后台：