Atitit 登录票据安全法

目录

[1.1. cookie对象规范 1](#_Toc15556)

[1.2. Cookie加解密 1](#_Toc15046)

[1.3. Cookie密文动态更换，根据一个时间3天比如 1](#_Toc8656)

[1.4. 服务端撤销key 1](#_Toc23154)

[1.5. 有效期设置 1](#_Toc29816)

## cookie对象规范

Utype

Uname

Uid

Createtime

Key4svrTickAnyTime

## Cookie加解密

## Cookie密文动态更换，根据一个时间3天比如

## 服务端撤销key

可以从服务端撤销客户端的票据 都根据一个相同key验证加密，如果变换，那么验证失败

## 有效期设置

function setCookie4login()

{

$secret\_key = "abcdefgh";

    $token['Key4svrTickAnyTime'] = "Key4svrTickAnyTimeTb26";

    $token['createTime'] = date('Y-m-d H:i:s');

    $token['loginacc\_utype'] = $\_GET['usertype'];

    $token['loginacc'] = $\_GET['loginacc'];

    $token\_json\_str = json\_encode($token);

    $token\_ecr=openssl\_encrypt($token\_json\_str, 'AES-128-ECB', $secret\_key, 0, "");

    setcookie("logincookie", $token\_ecr, time() + 3600 \* 24, "/");

    print\_r($token\_json\_str) ;

    setcookie("loginacc", $\_GET['loginacc'], time() + 3600 \* 24, "/");

    setcookie("loginacc\_utype", $\_GET['usertype'], time() + 3600 \* 24, "/");

    echo "ok";

}

验证cookie

$secret\_key = "abcdefgh";

//echo openssl\_encrypt($data, $this->method, $this->secret\_key, $this->options, $this->iv);

$logincookie = openssl\_decrypt($\_COOKIE['logincookie'], 'AES-128-ECB', $secret\_key, 0, "");

if (!$logincookie) {

    throw new Exception("logincookie decrypt err");

}