

【知识点——越权基础知识和分类认识】

越权的定义

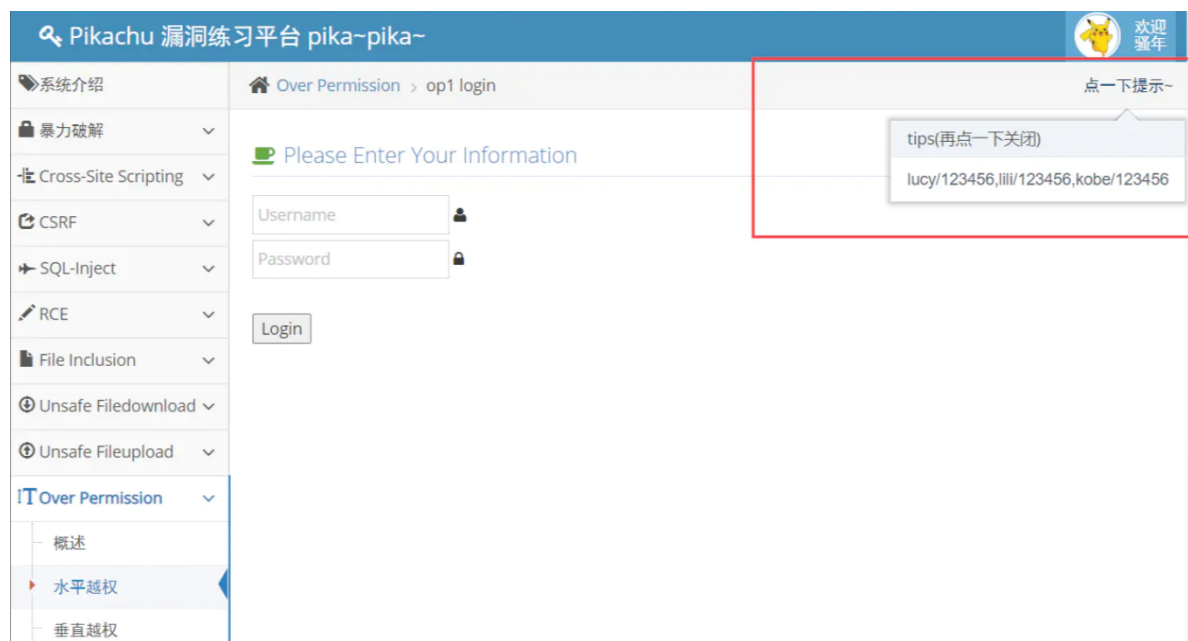
一个用户A一般只能对自己本身的信息进行增删改查，然而由于后台开发人员的疏忽，没有在信息进行增删改查时候进行用户判断，从而导致用户A可以对其他用户进行增删改查等等操作。

越权漏洞——分为水平越权和垂直越权。

越权原理

如果使用A用户的权限去操作B用户的数据，A的权限小于B的权限，如果能够成功操作，则称之为越权操作。越权漏洞形成的原因是后台使用了不合理的权限校验规则导致的。

【知识点——水平越权】



抓包查看信息

系统介绍

暴力破解

Cross-Site Scripting

CSRF

SQL-Inject

RCE

File Inclusion

Unsafe Filedownload

Unsafe Fileupload

Over Permission

概述

水平越权

垂直越权

..../

Over Permission > op2 admin

点一下提示~

用户管理

查看用户列表

添加用户

hi,admin欢迎来到后台会员中心 | 退出登录

用名	性别	手号	邮箱	地址	操作
vince	boy	18626545453	vince@pikachu.com	chain	删除
allen	boy	13676767767	allen@pikachu.com	nba 76	删除
kobe	boy	15988767673	kobe@pikachu.com	nba lakes	删除
grady	boy	13676765545	grady@pikachu.com	nba hs	删除
kevin	boy	13677676754	kevin@pikachu.com	Oklahoma City Thunder	删除
lucy	girl	12345678922	lucy@pikachu.com	usa	删除
lili	girl	18656565545	lili@pikachu.com	usa	删除

用低权限用户登录，提示只有查看权限

Pikachu 漏洞练习平台 pika~pika~

欢迎 鉴年

系统介绍

暴力破解

Cross-Site Scripting

CSRF

SQL-Inject

RCE

File Inclusion

Unsafe Filedownload

Unsafe Fileupload

Over Permission

概述

水平越权

垂直越权

..../

Over Permission > op2 user

点一下提示~

欢迎来到后台管理中心,您只有查看权限! | 退出登录

用名	性别	手机	邮箱	地址
vince	boy	18626545453	vince@pikachu.com	chain
allen	boy	13676767767	allen@pikachu.com	nba 76
kobe	boy	15988767673	kobe@pikachu.com	nba lakes
grady	boy	13676765545	grady@pikachu.com	nba hs
kevin	boy	13677676754	kevin@pikachu.com	Oklahoma City Thunder
lucy	girl	12345678922	lucy@pikachu.com	usa
lili	girl	18656565545	lili@pikachu.com	usa

抓包注意修改来源和refer

BP测试越权插件, Authorize

burp suite professional v1.7.20 - temporary project - licensed to Larry_Lau - Unlimited by mxcx@tosec.vn

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Extensions BApp Store APIs Options

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Detail
Asset Discovery	<input type="checkbox"/>	★★★★☆	Pro extension
Attack Surface Detector	<input type="checkbox"/>	★★★★★	
Auth Analyzer	<input type="checkbox"/>	★★★★★	
Authentication Token Obtai...	<input type="checkbox"/>	★★★★★	
AuthMatrix	<input type="checkbox"/>	★★★★★	
Authz	<input type="checkbox"/>	★★★★★	
Auto Repeater	<input checked="" type="checkbox"/>	★★★★★	
Auto-Drop Requests	<input type="checkbox"/>	★★★★★	
Authorize	<input checked="" type="checkbox"/>	★★★★★	
Autowasp	<input type="checkbox"/>	★★★★★	Pro extension
AWS Security Checks	<input type="checkbox"/>	★★★★★	Pro extension
AWS Signer	<input type="checkbox"/>	★★★★★	
AWS Sigv4	<input type="checkbox"/>	★★★★★	
Backslash Powered Scanner	<input type="checkbox"/>	★★★★★	Pro extension
Batch Scan Report Generator	<input type="checkbox"/>	★★★★★	Pro extension
BeanStack - Stack-trace Fin...	<input type="checkbox"/>	★★★★★	Pro extension
Blazer	<input type="checkbox"/>	★★★★★	

Authorize

Authorize is an extension aimed at helping the pen time-consuming tasks in a web application penet

It is sufficient to give to the extension the cookies (extension automatically repeats every request with

It is also possible to repeat every request without : authorization ones.

The plugin works without any configuration, but is authorization enforcement conditions and also wh of the plugin and to export a report of the authoriza

The reported enforcement statuses are the followi

1. Bypassed! - Red color
2. Enforced! - Green color
3. Is enforced??? (please configure enforc

对话框内设置不同权限用户的认证信息

ID	Meth...	URL	Orig. Len	Modif. ...	Unauth...	Authz. ...	Unauth...
1	GET	http://192.168.3.162:885/vul/overpermission/op2/op2_admin...	35911	31046	31046	Enforc...	Enforc...
2	GET	http://192.168.3.162:885/vul/overpermission/op2/op2_admin...	34541	34543	31046	Is enfor...	Enforc...
3	POST	http://192.168.3.162:885/vul/overpermission/op2/op2_admin...	34541	34543	31046	Is enfor...	Is enfor...
4	GET	http://192.168.3.162:885/vul/overpermission/op2/op2_admin...	36245	31046	31046	Enforc...	Enforc...
5	GET	http://detectportal.firefox.com:80/canonical.html	90	90	90	Bypass...	Bypas...
6	GET	http://detectportal.firefox.com:80/success.bt?ip6	8	8	8	Bypass...	Bypas...
7	GET	http://detectportal.firefox.com:80/success.bt?ip4	8	8	8	Bypass...	Bypas...
8	GET	http://192.168.3.162:885/vul/overpermission/op2/op2_admin...	36414	31046	31046	Enforc...	Enforc...
9	GET	http://192.168.3.162:885/vul/overpermission/op2/op2_admin...	36409	31046	31046	Is enfor...	Is enfor...
10	GET	http://192.168.3.162:885/vul/overpermission/op2/op2_login.p...	34813	34813	34813	Bypass...	Bypas...
11	GET	http://detectportal.firefox.com:80/canonical.html	90	90	90	Bypass...	Bypas...
12	GET	http://192.168.3.162:885/vul/overpermission/op1/op1_login.p...	34781	34781	34781	Bypass...	Bypas...
13	GET	http://detectportal.firefox.com:80/success.bt?ip6	8	8	8	Bypass...	Bypas...
14	GET	http://detectportal.firefox.com:80/success.bt?ip4	8	8	8	Bypass...	Bypas...
15	POST	http://192.168.3.162:885/vul/overpermission/op1/op1_login.p...	34781	34781	34781	Bypass...	Bypas...
16	GET	http://192.168.3.162:885/vul/overpermission/op1/op1_mem.p...	33976	33976	33972	Bypass...	Enforc...
17	GET	http://detectportal.firefox.com:80/canonical.html	90	90	90	Bypass...	Bypas...
18	GET	http://detectportal.firefox.com:80/success.bt?ip4	8	8	8	Bypass...	Bypas...
19	GET	http://detectportal.firefox.com:80/success.bt?ip6	8	8	8	Bypass...	Bypas...

Request/Response Viewers Configuration

Authorize is off ☒ Ignore 304/204 status code res; ☐ Prevent 304 Not Modified status ☐ Intercept requests from Repeats ☒ Check unauthenticated

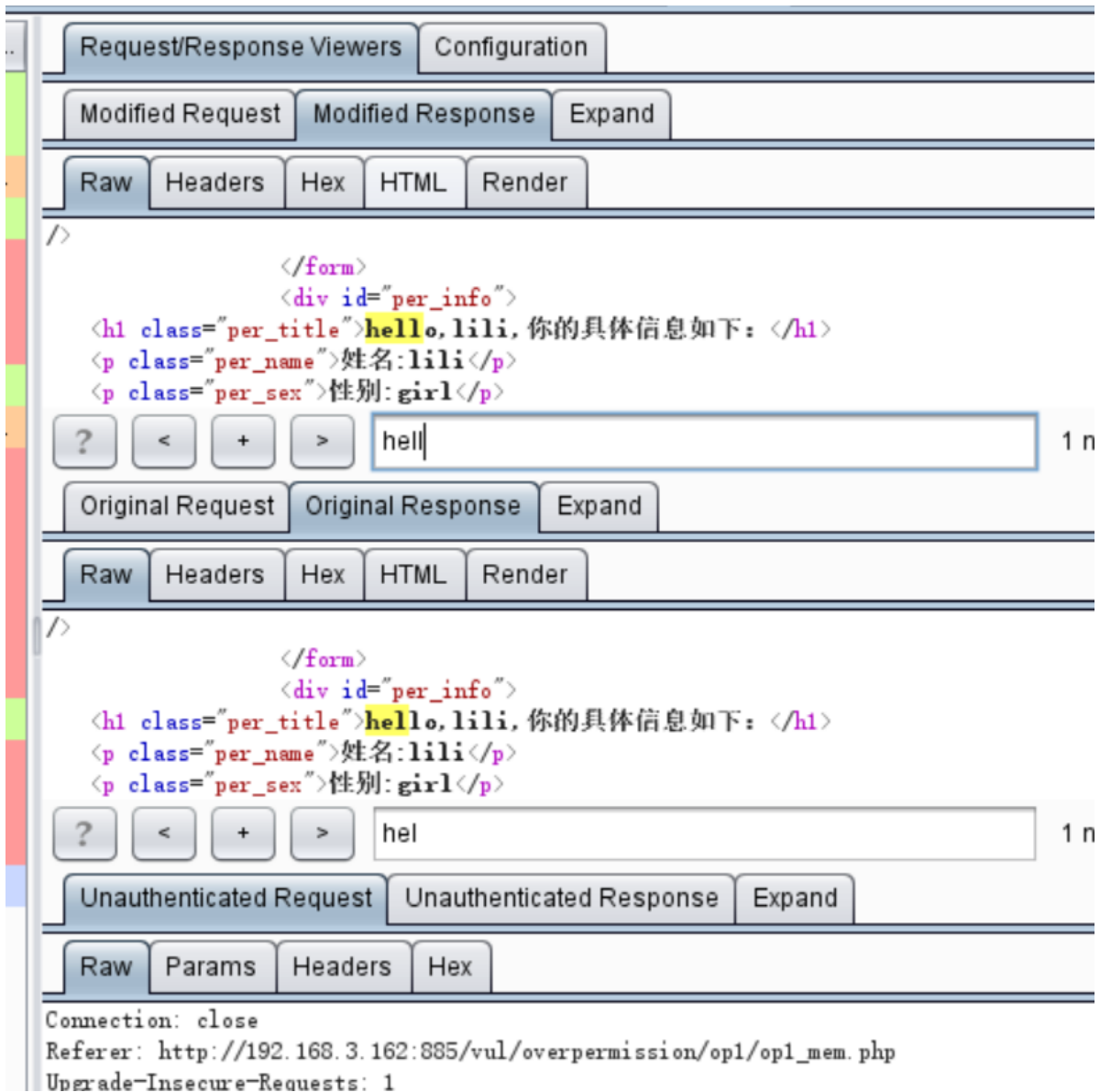
Clear List ☐ Auto Scroll

Cookie: PHPSESSID=d98hm3inaopkfavrb1cppvp9h5

Fetch cookies from last request

Enforcement Detector Detector Unauthenticated Interception Filters Match/Re

正常访问数据，数据包信息会显示在左侧，红色为可能存在越权，可在此模块对比修改前后的数据包。



越权漏洞修复

- 1、前端和后端同时对用户输入信息进行校验，双重验证机制
- 2、调用功能前验证用户是否有权限调用相关功能
- 3、执行关键操作前必须验证用户身份，验证用户是否具备操作数据的权限