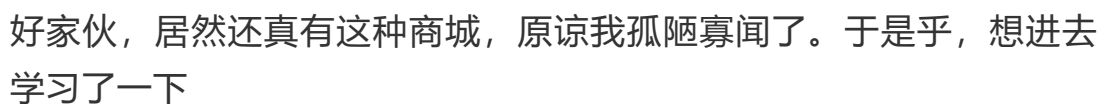


原创 硝基苯 HACK学习呀

某天挖 edu 挖到自闭，然后想着 fofa 一下，看看有没有什么好玩的站点



首先，进行了一下初步的信息收集



基本上都是伪静态的，没有什么发现可以明显判断其网站后端语言的地方在搜索框点击搜索后

可以发现这个地址并不能帮助我们判断该站的类型但也要尝试一下SQL注入



然后直接被Ban IP了，索性放弃对这个地方的继续研究，继续翻找其他功能点。当我们点击订单查询时



可以发现Url 产生了变化

shopcart/login.asp?ref=orders

手机版 | 您好, 欢迎您! | 订单查询 | 会员中心 | 品牌

品牌正品 诚信保障 | 100% 安全材质 | 超长60天 退换货 | 10重 隐私保护

首页 | 女性用品 | 男性用品 | 情趣内衣 | 两性情趣 | 润滑液 | 避孕安全

Q 搜索 热门导航: 情趣跳蛋 | 震动棒 | 女用转珠棒 | 假阳具 | 电动自慰杯 | 女人名器 | 延时喷射 | 充

新用户注册 REGISTER 登录 LOGIN

邮箱: (请输入邮箱) 用户名: (邮箱/手机号/会员名)

密码: (必填) 密码: HACK学习呀

跳转到了登录注册页面，既然来都来了，注册一个看看有没有其他业务，黑不走空，哈哈哈

会员中心

您的位置: 首页 >> 用户资料维护

我的帐户概况
用户资料修改
用户密码修改
收货信息维护
订单管理
管理优惠券(0张)

用户名: 1234@qq.com

昵称: 1232 会员登录后显示昵称

电子邮箱: 1234@qq.com * 如有亲

固定电话:

邮政编码:

提交 HACK学习呀

昵称处尝试打 Xss，发现也会被 Ban IP，那就先放一下，找找有没有什么业务逻辑漏洞吧。尝试购买一些商品，之前一直听说支付漏洞，但弟弟从没有真正遇到过，碰碰运气吧

雷霆 雷霆G点萌兔后庭拉珠 造型粉嫩娇盈 内核震力强劲 带来饱满酥

货 号： **056078** ---电话订购和短信订购只需说明[货号]即可

品 牌： 雷霆 [查看授权书](#)

促销价： **75 - 88元**

物 流： （全国城市1-2天达，偏远乡镇及农村3-5日达）

已售出： 1170件

评 价： ★★★★★ [共有0条评价](#)

促 销： [促销活动](#) [优惠活动进行中，购满300送300>>](#)

规格：	<input type="button" value="兔小弟（长8.8cm）"/>	<input type="button" value="兔老二（长9.7cm）"/>
	<input type="button" value="兔金刚（长9.4cm）"/>	<input type="button" value="兔司机（长10.4cm）"/>

数量： 个

[\[快速购物通道\]](#)

 HACK学习呀

支付： [\[货到付款\]](#) [\[支付宝\]](#) [\[在线支付\]](#) [\[银行汇款\]](#)

点击购买，抓包发现 cookie 中出现了一个奇怪的参数

```
GET /shopcart/ HTTP/1.1
Host: www.
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://www. product-8927.html
Cookie: Hm_lvt_907ba150c09e199a126d5059b6f21731=1612020051; Hm_lvt_907ba150c09e199a126d5059b6f21731=1612022712; ASPSESSIONIDACFTAA=J9HLL0GLJAGI3HNEED-JCE; Hm_lvt_d0e6730dea72a00ed4f40fa939c1ae60=1612020127; Hm_lvt_d0e6730dea72a00ed4f40fa939c1ae60=1612022051; user_name=test40test.com; user_from=0; user_type=1; user_username=E4E83A0E558E6C4E4BC9A5E591590; user_zhekou=100; sub_to=123; sub_tel=18313345987; sub_ads=E4E8B0A1E6B5B7E9A95BF4E5A5E101E5A8CBA; province=2; city=321; district=2703; cartList=892717C1E91981B71E919C1860E71821B91E919018C1E5A851941E5A901DE1E5A8A1AD1E618B1891E718F1A0_1E31801901E91A71841E61A01B_1E8A1EFA1BC1801E91951BF10_4cmEFA1BC1891E31801917C8817C8817C17C05607817C17C017C17C
Upgrade-Insecure-Requests: 1
```

我们拿去urldecode 一下，看看是什么东西

 HACK学习呀

8927|雷霆G点萌兔后庭拉珠_【规格:兔司机(长10.4cm)】|1|1|10|056078||0||

```
牛马商店 GET /shopcart/ HTTP/1.1
Host: www.
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://www.....product-8927.html
Connection: close
Cookie: Hm_lvt_9d7ba15dc09e199a12c4d505bf6217311=1612020051; Hm_lvt_9d7ba15dc09e199a12c4d505bf6217311=1612022712; ASPSESSIONIDC6CBQ8AB=FJMLGOGCCMKCFBLBGEDDMXC; ASPSESSIONIDIACTFAAA=JRMLOGGCJAHJNBEBNBJUCB; Hm_lvd_c0d6730dae73a00ed4f48fa95c1ae60=f6161202127; ASPD6730dae73a00ed4f48fa95c1ae60=f61612022091; user_name=test140tencat; user_from=0; user_type=1; user_address=1E6B3A40AE596BCAE4BCF9A9EA5A91V90; user_zhekou=100; sub_t=123; sub_tel=10313345907; sub_type=te44B06Ade4B58B7BF5E9A5E4E81E5A0CB4B; province=; city=123; district=2703; cartList=te44B06Ade4B58B7BF5E9A5E4E81E5A0CB4B; Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

商品编号	商品名称	单价	数量	优惠	商品合计	操作
056078	 雷霆G点萌兔后庭拉珠_【规格:兔司机 (长10.4cm)】	¥ 1.00	<input type="text" value="10"/>	--	¥ 10.00	删除

 清空购物车
  刷新购物车
 得到积分: 10分
 商品总额: **¥ 10.00**

 **收货人信息**

提交订单，修改cookie内的值，然后继续，页面跳转到了支付宝付款页面

改成 1 后，果然享受了一折优惠，哈哈哈哈

列表 您是【注册会员】，购物享受1折(促销商品除外)

商品名称	单价	数量	优惠	商品合计	操作
 枕边增大器bathmate X30 助勃器	¥1380.00	<input type="text" value="1"/>	¥1366.00	¥14.00	删除

刷新购物车 得到积分: 14分 商品总额: **¥14.00**

收货地址: (必填) *省份、城市、地区必须正确选择
 (必填) *收货地址尽可能详细，以便及时送达!

手机号码: (必填) * 请正确填写手机号码，方便送货联系!

收货人: (必填) * 如不想留全名,可填写:[某某]先生/小姐/女士;如您姓张,可填写:张先生、张小姐或张女士

可以发现，只用支付 14 元了，享受 1 折优惠继续缴费操作，然后还有7元邮费<万恶的商家居然不包邮>，然后支付21元，即可把增*器带回家，想想就刺激呢！



文末总结:

- 1、挖洞还是就一句话，**心细则挖天下！**
- 2、面对逻辑漏洞，一定要注意每个页面交互跳转时的参数，尽可能的去猜测传的每一个参数的作用是什么。Burp看不方便的话 F12

也可以看到，看自己喜好和习惯了。一定要细心去测，不要放过一些细小的点，说不定就会有惊喜

3、订单查询都没发现可以越权，没想到支付点居然是前端可控的，
嘿嘿嘿



推荐阅读：

逻辑漏洞 | 支付漏洞学习

小程序渗透 | 对酒店房间自助售货机的支付漏洞挖掘

SRC逻辑漏洞挖掘详解以及思路和技巧

SRC漏洞挖掘经验+技巧篇

干货 | 登录点测试的Tips


漏洞挖掘 | 单点登录的网站通过Referer盗取用户授权

记一次短信验证码的"梅开五度"

2021年性价比最高-网络安全系列课程

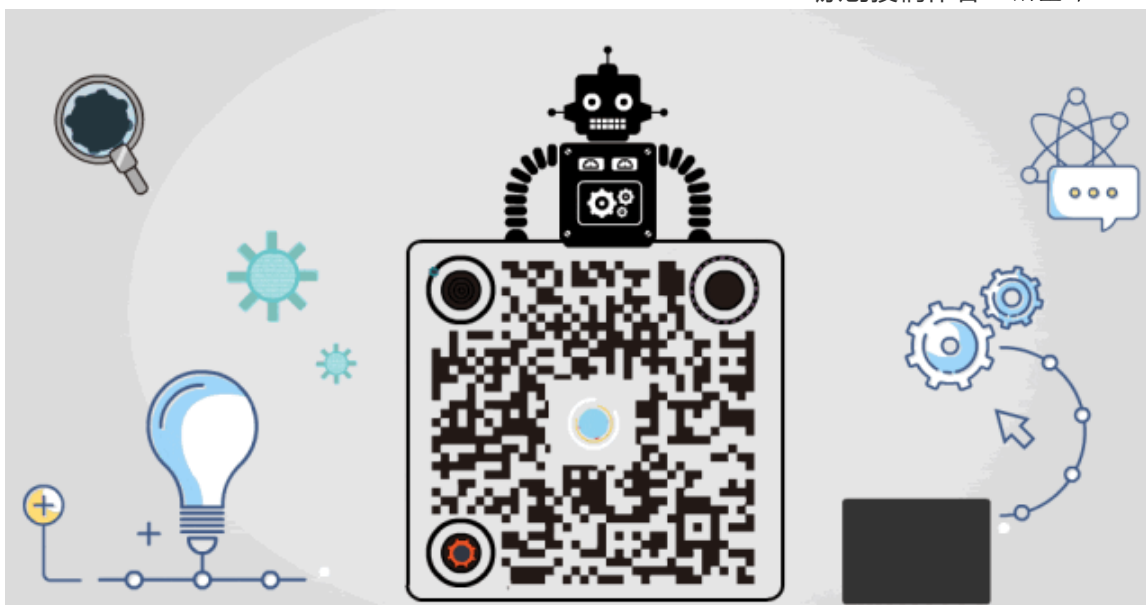
报名线上学习

从零开始学习白帽黑客

 HACK学习呀

点赞，转发，在看

原创投稿作者：硝基苯



精选留言

用户设置不下载评论