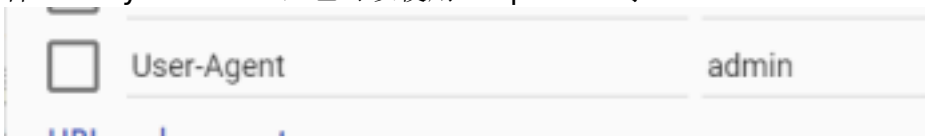
web-server

1.html-source code
该题仅需使用浏览器查看源代码功能即可：

```
<!--

Je crois que c'est vraiment trop simple là !

It's really too easy !

password : nZ^&@q5&sjJHev0

-->
```

2.open redirect
该题考察重定向，根据题目的三个例子可以知道（源代码也可知），发现结构为url=域名&h='hash'的方式，于是使用https://baidu.com，然后在使用cmd5生成hash，即url=https://baidu.com&h=bb6e082d5c360ce6a0c64f926feea905，拼接与原题干url拼接之后即可得到flag：

3.user agent
题目说user agent不是admin，即考察http header的编辑与重放，可以选择很多工具，比如chrome浏览器插件modify headers，也可以使用burpsuite等。



添加ua（user agent）之后再刷新即可。

4.Weak password
根据题干即可知道是考察弱口令
进入题目，发现是basic认证，猜测弱口令搭配，一般后台用户名均猜测为admin，密码多是admin

5.PHP - Command injection
命令执行题，进入题目发现需要输入一个ip地址，随便属于一个本地IP地址，发现下方出现ping的返回，则猜测题目执行ping +ip，这时需要加&号然后再执行我们想要的命令即可。比如输入，192.168.1.1&pwd。
此题我们ls发现，只有一个index.php文件，打开这个文件即可得到flag。
192.168.1.1&cat index.php

返回如下：出现两个框，原因是index.php里面存在html，此时查看源代码即可发现flag。

6.HTTP - Directory indexing
该题是路径题目，查看源代码发现一个路径，/admin/pass.html,没有发现啥，既然是路径题，直接访问/admin，发现索引，有个路径backup可疑，访问即得flag。

7.HTTP - POST
发现是个小游戏，随机获取一个数，当这个数大于999999即可，打开审查元素network，此时点击try it，发现分数是在post表单中，只需要更改score字段即可，使用burpsuite改包，重放即可得flag

8.HTTP - Improper redirect

9.HTTP - Cookies
进入题目，打开源代码

```
<fieldset>

<form method="POST" action="" name="a">
Email<br/>
<input type="text" name="mail" size="20" class="post
<input type="submit" name="jsep4b" size="20" class="
</form><!--SetCookie("ch7","visiteur");--><a href="?
```

设置cookie即可，使用burpsuite，抓题目中send的包，拦截，添加cookie，重放即可。

待续。。。