Bizness HTB

User Reconnaissance

1. We can check where is the webpage with curl

```
┌──(kali㉿kali)-[~]
└─$ curl -I 10.10.11.252
HTTP/1.1 301 Moved Permanently
Server: nginx/1.18.0
Date: Sat, 10 Feb 2024 01:31:08 GMT
Content-Type: text/html
Content-Length: 169
Connection: keep-alive
Location: https://bizness.htb/
```

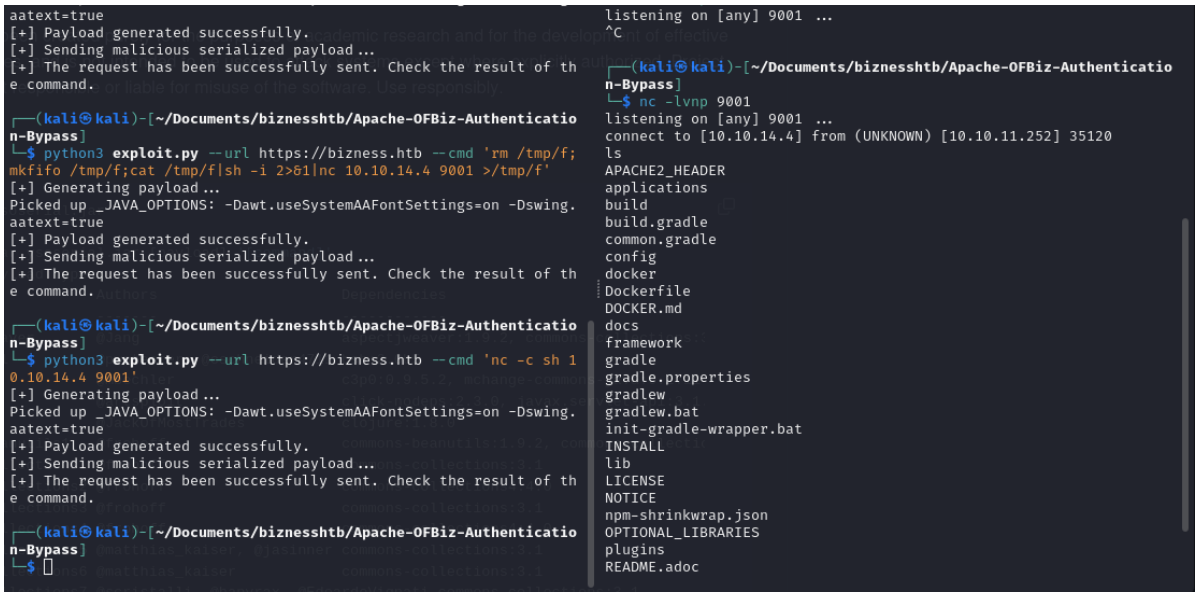
2. Result of dirsearch show /solr/admin, upon openning we are redirected to this page.

```
[20:35:49] 404 -  682B  - /META-INF/app-config.xml
[20:35:49] 404 -  682B  - /META-INF
[20:35:49] 404 -  682B  - /META-INF/CERT.SF
[20:35:49] 404 -  682B  - /META-INF/
[20:35:49] 404 -  682B  - /META-INF/application.xml
[20:35:49] 404 -  682B  - /META-INF/jbosscmp-jdbc.xml
[20:35:49] 404 -  682B  - /META-INF/jboss-ejb-client.xml
[20:35:49] 404 -  682B  - /META-INF/context.xml
[20:35:49] 404 -  682B  - /META-INF/ejb-jar.xml
[20:35:49] 404 -  682B  - /META-INF/container.xml
[20:35:49] 404 -  682B  - /META-INF/eclipse.inf
[20:35:49] 404 -  682B  - /META-INF/beans.xml
[20:35:49] 404 -  682B  - /META-INF/jboss-app.xml
[20:35:49] 404 -  682B  - /META-INF/jboss-client.xml
[20:35:49] 404 -  682B  - /META-INF/jboss-deployment-structure.xml
[20:35:49] 404 -  682B  - /META-INF/ironjacamar.xml
[20:35:49] 404 -  682B  - /META-INF/jboss-webservices.xml
[20:35:49] 404 -  682B  - /META-INF/jboss-ejb3.xml
[20:35:49] 404 -  682B  - /META-INF/MANIFEST.MF
[20:35:49] 404 -  682B  - /META-INF/openwebbeans/openwebbeans.properties
[20:35:49] 404 -  682B  - /META-INF/ra.xml
[20:35:49] 404 -  682B  - /META-INF/SOFTWARE.SF
[20:35:49] 404 -  682B  - /META-INF/spring/application-context.xml
[20:35:49] 404 -  682B  - /META-INF/weblogic-application.xml
[20:35:49] 404 -  682B  - /META-INF/weblogic-ejb-jar.xml
[20:35:49] 404 -  682B  - /META-INF/persistence.xml
[20:36:03] 200 -   21B  - /solr/admin/file/?file=solrconfig.xml
[20:36:03] 200 -   21B  - /solr/admin/
[20:36:03] 302 -    0B  - /solr/  →  https://bizness.htb/solr/control/checkLogin/
[20:36:11] 404 -  682B  - /WEB-INF/applicationContext.xml
[20:36:11] 404 -  682B  - /WEB-INF/application-client.xml
[20:36:11] 404 -  682B  - /WEB-INF/cas-servlet.xml
[20:36:11] 404 -  682B  - /WEB-INF
[20:36:11] 404 -  682B  - /WEB-INF/
```

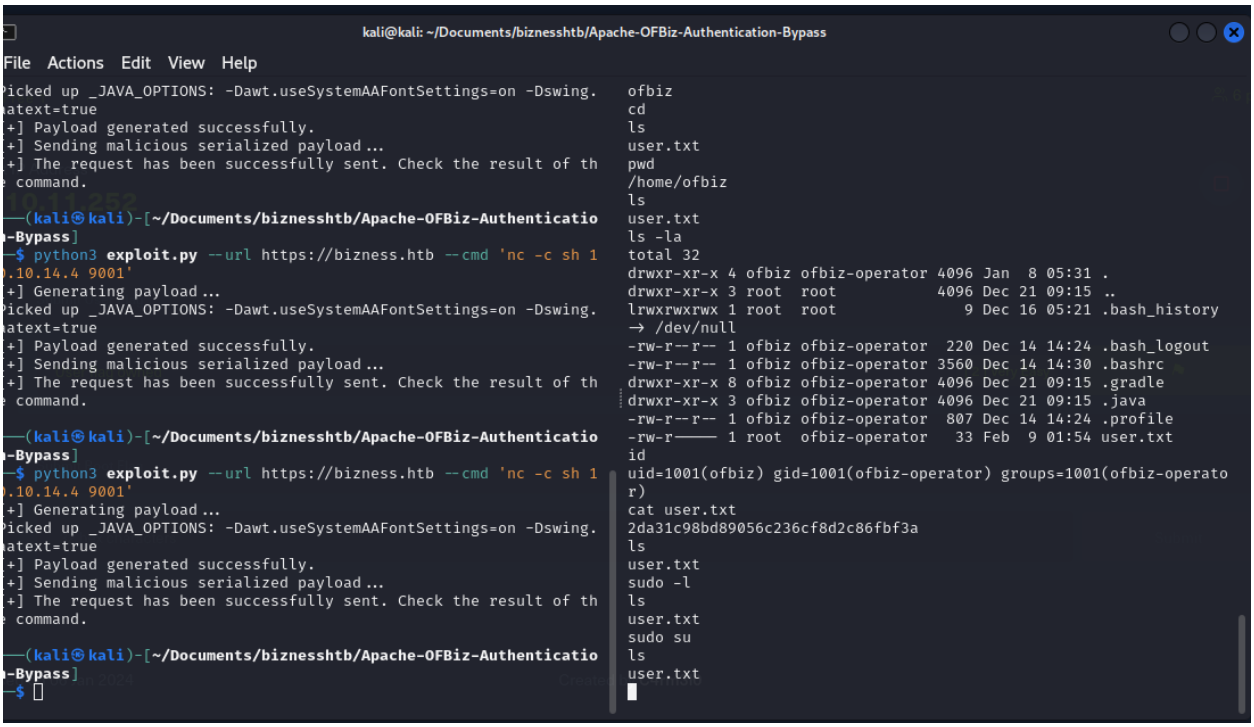
---

3. We can find a CVE about ofbiz here

   https://github.com/jakabakos/Apache-OFBiz-Authentication-Bypass?tab=readme-ov-file



User flag



Privilege Escalation

grep -arin -o -E '(\w+\W+){0,5}password(\W+\w+){0,5}'