

漏洞描述:

上海甲鼎信息技术有限公司就业信息服务平台存在通用信息泄露漏洞, 攻击者可以通过构建 URL 地址导致 IIS 中间件报错, 从而直接获取到网站的真实物理路径, 为下一步攻击做准备。

公司主页:

<http://www.infojiading.cn/gyjd.html>

复现:

鹰图语法:

title="就业"&&body="甲鼎"

序号	资产名称	IP	端口	域名	应用/组件	站名	状态	ICP备案企业	地理位置	更新时间
1	-	124.221.190.10	8176	http	124.221.190.10	Microsoft ASP.NET	共7条	上海平教大学...	上海市	2022
2	-	202.121.199.214	80	http	zbb.shu.edu.cn	IIS IIS/10.0	共7条	上海大学就业信...	上海市	2022
3	-	202.121.199.214	443	https	zbb.shu.edu.cn	Font Awesome	共7条	上海大学就业信...	上海市	2022
4	-	202.120.223.81	80	http	91ust.edu.cn	jQuery	共7条	上海理工大学...	上海市	2022
5	-	116.239.14.65	443	https	iyshu.edu.cn	Modernizr	共7条	上海师范大学...	上海市	2022
6	-	222.204.192.237	443	https	job.shup.edu.cn	Bootstrap	共7条	上海政法学院...	上海市	2022
7	-	116.239.14.65	80	http	iyshu.edu.cn	Bootstrap	共7条	上海师范大学...	上海市	2022
8	-	162.255.119.136	80	http	opportunities.m...	IIS IIS/8.5	共7条	上海理工大学...	上海市	2022
9	-	202.120.108.170	443	https	career.acust.edu.cn	Modernizr	共5条	华东理工大学...	上海市	2022
10	-	117.144.202.152	8080	http	117.144.202.152	Modernizr	共5条	上海中侨职业...	上海市	2022

具体过程

正常 URL:: <http://地址>

POC: /1

URLPOC: <http://地址/1>

在 url 后面直接拼接/1 访问

案例一（上海海事大学）:

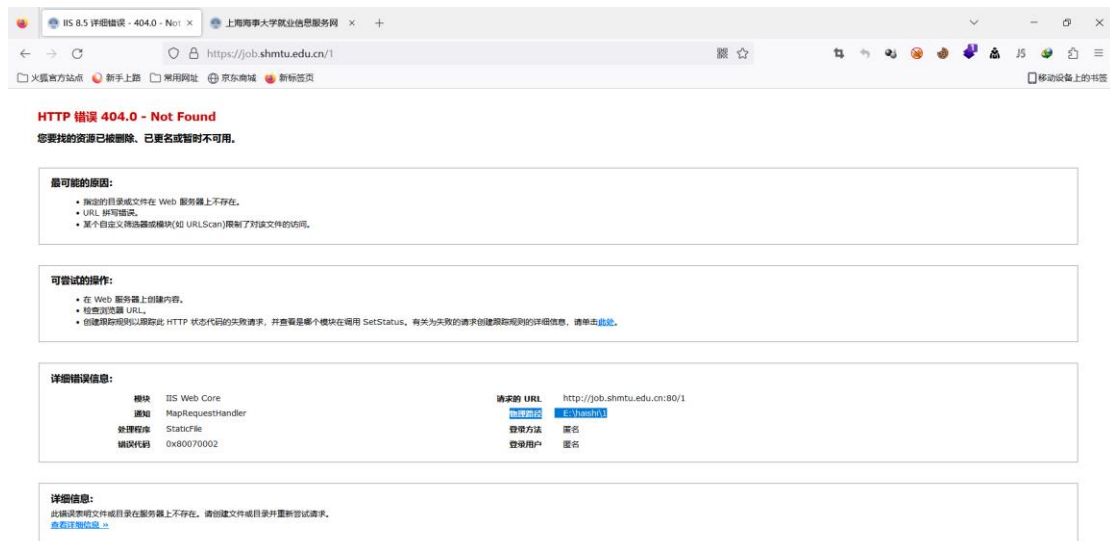
正常 URL:

<https://job.shmtu.edu.cn/>



POCURL:

<https://job.shmtu.edu.cn/1>



案例二（上海师范大学天华学院）:

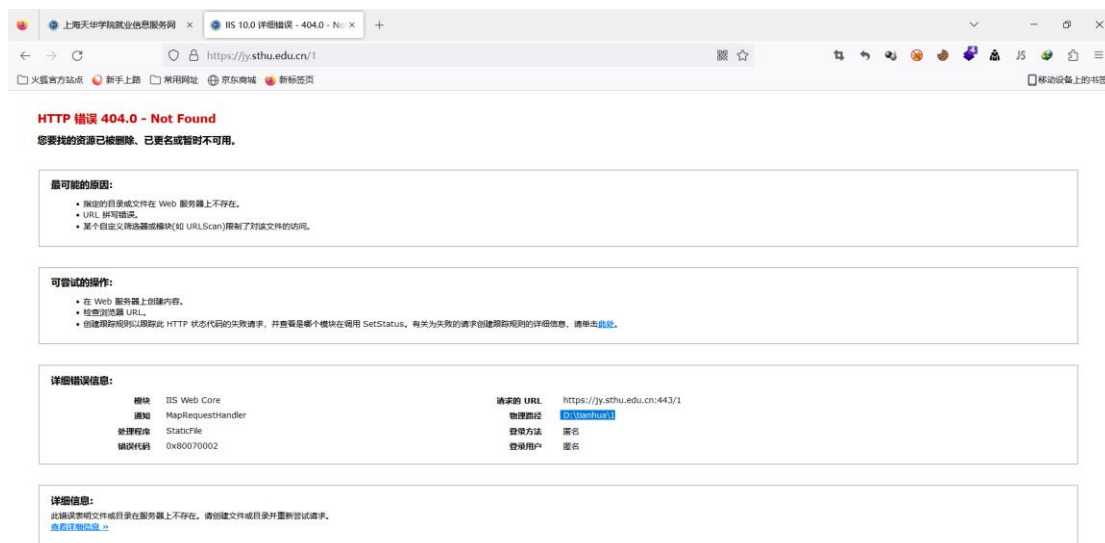
正常 URL:

<https://jy.sthu.edu.cn/>



POCURL:

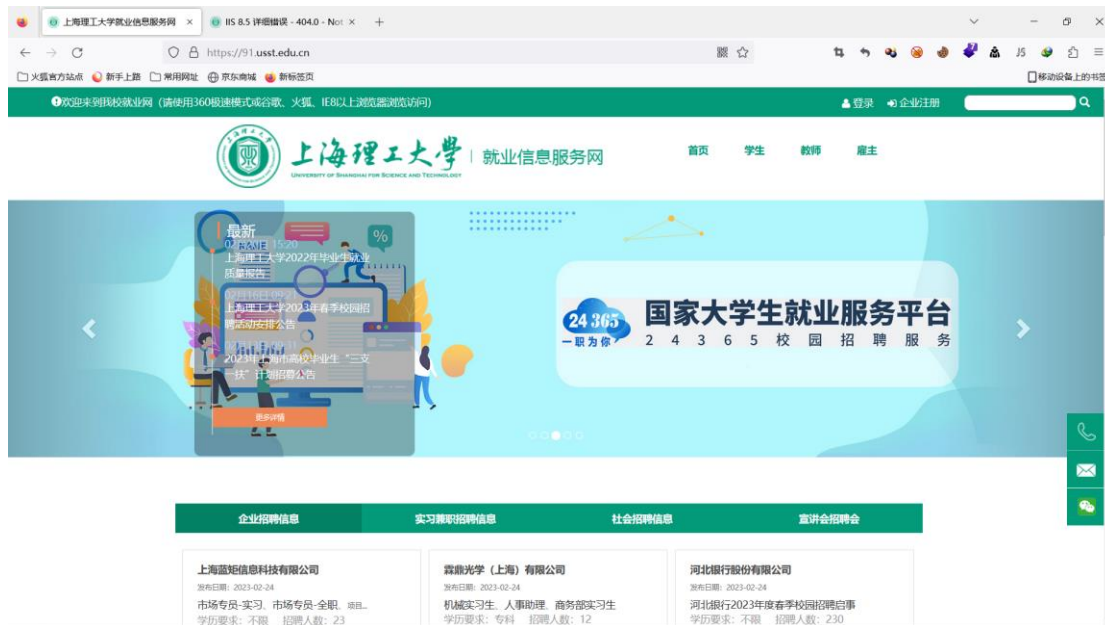
<https://jy.sthu.edu.cn/1>



案例三（上海理工大学）:

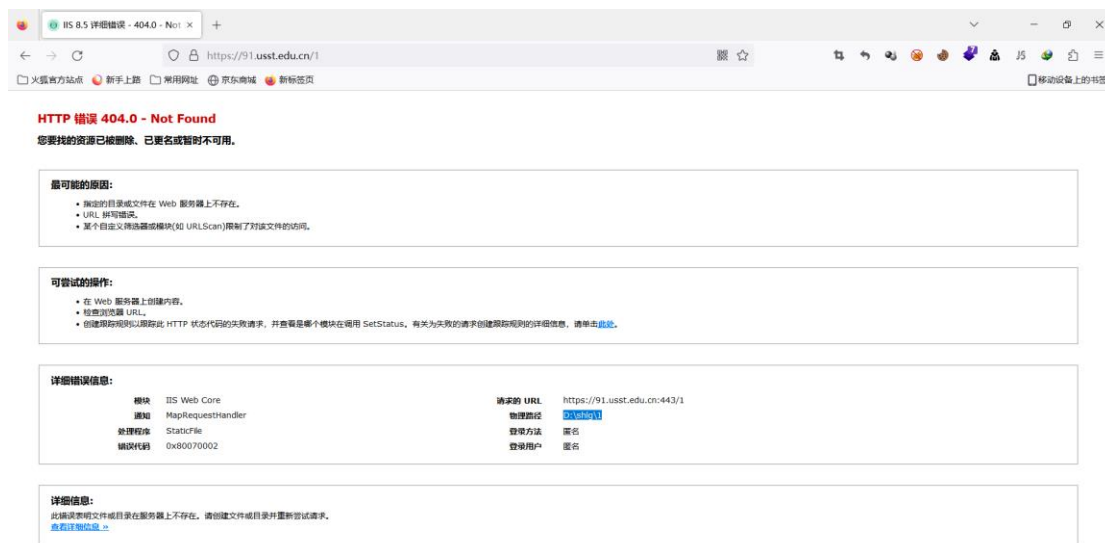
正常 URL:

<https://91.usst.edu.cn/>



POCURL:

<https://91.usst.edu.cn/1>



其他地址:

<http://124.221.190.10:8176>

<http://zbb.shu.edu.cn>

<https://zbb.shu.edu.cn>

<http://91.usst.edu.cn>

<https://jy.sthu.edu.cn>

<https://job.shupl.edu.cn>

<http://jy.sthu.edu.cn>

<http://opportunities.xn--cesx9m.com>

<https://career.ecust.edu.cn>

<http://117.144.202.152:8080>

<https://job.shmtu.edu.cn>

<http://117.144.202.152>

<http://job.shmtu.edu.cn>

修复建议：

- (1) 媒体链接和超链接采用相对路径的表达方式；
- (2) 报错信息中不对外输出网站物理路径等敏感信息。