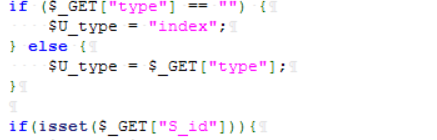
漏洞分析

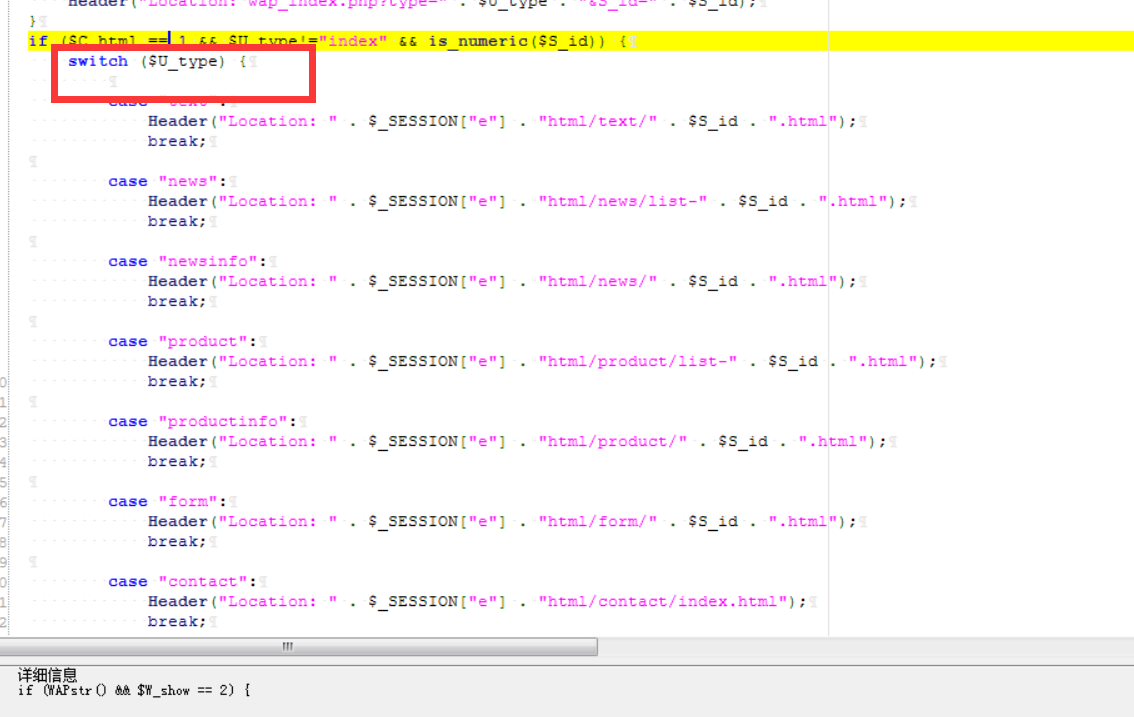
漏洞url

<http://192.168.138.132/edu/?type=newsinfo%3Cscript%3Ealert(/xss/)%3C/script%3E&S_id=28>

源码分析



这里可以看到对type参数的定义，然后跟踪下一个



这里可以看到type参数没有做任何过滤直接带入执行所以导致恶意语句可以被带入执行

