

Target: <https://gitee.com/jspxcms/jspxcms>

Version: v10.2.0

Cross-site scripting vulnerability exists in /ext/collect/find_text.do

source passes poclink

In find_text.do

```
@RequestMapping(value = "find_text.do")
public void findText(String source, String search, @RequestParam(defaultValue = "false") boolean isReg,
    @RequestParam(defaultValue = "true") boolean isFirst, HttpServletResponse response) {
    StringBuilder result = new StringBuilder();
    if (isFirst) {
        result.append(Collect.findFirst(source, search, isReg));
    } else {
        for (String s : Collect.find(source, search, isReg)) {
            result.append(s).append('\n');
        }
        if (result.length() > 1) {
            result.setLength(result.length() - 1);
        }
    }
    Servlets.writeHtml(response, result.toString());
}
```

successed

