Workpop ADP Security Pretest

# Overview

ADP has approved all of the remediations required by their findings, detailed [in our writeup](https://docs.google.com/document/d/1Dhj_lkRvwrMo2bi1UKWCLy7pIkzQfsX3iqAriTBBpLY/edit) and their [original findings document](https://drive.google.com/file/d/1gI-h7Lqn85C8fpxn14DRGxWHzbeQYQGe/view), except for one: Input Validation on File Uploads.

Upon a 2nd remediation scan, the following results were returned, detailed [here](https://drive.google.com/file/d/0B6Q9F673vJ71NVYtRC1sVTBUcG96Ri1sUzNhbkIzdHZFNkY0/view).

## Highlights from the 2nd scan:

The application doesn't allow eicar files to be uploaded to server at the mentioned location but still allows macro enabled .doc which can be malicious.

Steps:

======

1) Use any malicious .doc file (sample file in attachment)

2) Request following URL and log into the application with valid credentials: https://sandbox.workpop.com

3) Navigate to "My Applications" tabs and click on "Manage Resume" button.

4) Now, click on "Upload Resume" button present in left side of the browser.

5) Click on "Choose File" option and select the file mentioned in Step 1.

Observe that the application uploads the macro enabled file.

Note: The documents tab also allows uploading malicious pdf files and hence rating hasn't changed.

# Remediation

ADP Suggestions include 5 detailed items. They send the same 5 items for this type of vulnerability regardless of the details as soon as they discover a failure of any kind. As a result, all of the remediation suggestions CAN be checked on the 3rd and final scan even if they weren’t touched on a previous scan. This is a drag, but at least we know this for sure.

## ADP Remediation Requirements

Ensure that the following steps are taken to sanitize the file being received:

1. Limit the types of files that can be uploaded not only by extension but also by content.
   1. Check file extensions - specify a whitelist of allowed values and verify against it. You should avoid allowing the upload of scripts, executables.
   2. Binaries and source code such as exe, com, pl, sh, bin, java, class, php, jsp, xlsm, xlsb, etc.
   3. Check file content (e.g. MIME type) in accordance of the allowed file types above
   4. Scan for viruses. If you accept compressed archives be sure the expand them and scan the files in them. Some AV vendors have built-in support for this but require configuration to enable.
   5. Only allow newer versions of MS office files which do not contain macros (xlsx, docx, etc.). If older versions are required to be uploaded, check for existence of macros with in the office files.
2. ~~Do not allow the end user to control the name of the file or location where it is stored on the server.~~
3. ~~Do not place the file in a directory accessible by Web users. It is preferable for this location to be outside of the document root.~~
4. ~~Ensure that strict permissions are set on both the uploaded file and the directory it is located in.~~
5. ~~If uploaded files will be passed on to ADP Clients, then content should be parsed, and written to an ADP generated file prior to distribution.~~

## Workpop Remediation Steps Taken

Code is deployed to <https://sandbox.workpop.com> only.

Branches include

* <https://github.com/workpop/workpop-web/tree/adp-security-changes>
* <https://github.com/Workpop/mozaic/tree/adp-security>
* <https://github.com/Workpop/Workpop-Web-Schemas/tree/av>
* <https://github.com/Workpop/pop/tree/av>

### Steps Detail

* All files from uploaded via FileField react component on both ww and mozaic will now include a /cache=false path parameter to indicate the file will not be cached at any layer, and fetched from s3 each time its accessed.
* AWS [Lambda Function](https://console.aws.amazon.com/lambda/home?region=us-east-1#/functions/av-scanner-nonprod?tab=graph) that scans each and every object created in s3 buckets and sets metadata values AV-Status to CLEAN / INFECTED
  + hris.develop.workpop.com
  + hris.demo.workpop.com
  + hris.workpop.com
  + hris.staging.workpop.com
  + filepicker.dev.workpop.com
* A file is marked INFECTED if any of the following are true
  + Its mime type is not from the approved list in source [here](https://github.com/Workpop/bucket-antivirus-function/blob/master/mime.py#L10).
    - We get mime from the file itself after downloading it from s3
    - We use python library [python-magic](https://github.com/ahupp/python-magic) which wraps libmagic which is an implementation of UNIX file program.
  + It is contains any VBA Macros as detected by [olevba](http://www.decalage.info/en/vba_tools). Any file that olevba does not support, passes this step. Olevba supports the following
    - Word/Excel/PowerPoint 97-2003
    - Word/Excel/PowerPoint 2007+
    - Word 2003 XML (.xml)
    - Word/Excel MHTML, aka Single File Web Page (.mht)
  + clamAV returns a status of INFECTED on the file
    - clamAV virus definitions are updated automatically every 3 hours
* A file is marked CLEAN if none of the above checks fail
* After a file is marked INFECTED, GetObject permissions are revoked by this IAM [policy](https://console.aws.amazon.com/iam/home?region=us-east-1#/policies/arn:aws:iam::298201760365:policy/deny-non-av-clean-objects$jsonEditor) attached to the [filepicker-dev](https://console.aws.amazon.com/iam/home?region=us-east-1#/users/filepicker-dev) IAM user. This prevents cdn.filestackcontent.com/cache=false/<file handle> urls from returning the file. Instead a 403 response is sent.
* When uploading a file anywhere on the site, the FileField polls for file metadata via this graphql [resolver](https://github.com/Workpop/Workpop-Web/blob/adp-security-changes/imports/files/graphql/resolvers.js#L7) in w-w until it gets a terminal status CLEAN/INFECTED for ALL files uploaded. Multi file upload IS supported.
  + Only after receiving CLEAN for all uploaded files, the file urls are dispatched back to the react form.
  + If an INFECTED file is detected, no form update is issued

# Pretest Groups

Documents - Alex

Tasks - Alex

Brand - Alex

* Bug found where preview images dont load because /cache=false and /transform are not compatible. Leaving as is for now.

Video Intro - Rami - Check what happens + disable on all jobs

* What is the url of the video? - Videos go directly to cameratag and are NOT stored in our own s3 bucket
* Disable this feature as a whole

Custom Forms - Alex

Profile Photos - Alex

Application Flow - Travis

My Resume - Alex

* Bug found where avatar photo cannot be updated...need to update @workpop/types to my prerelease on applications service

Employments - Alex

* Found and fixed one bug, employee could not submit direct deposit form (voided check image input is gone). Updated schema.

Unit tests - Alex