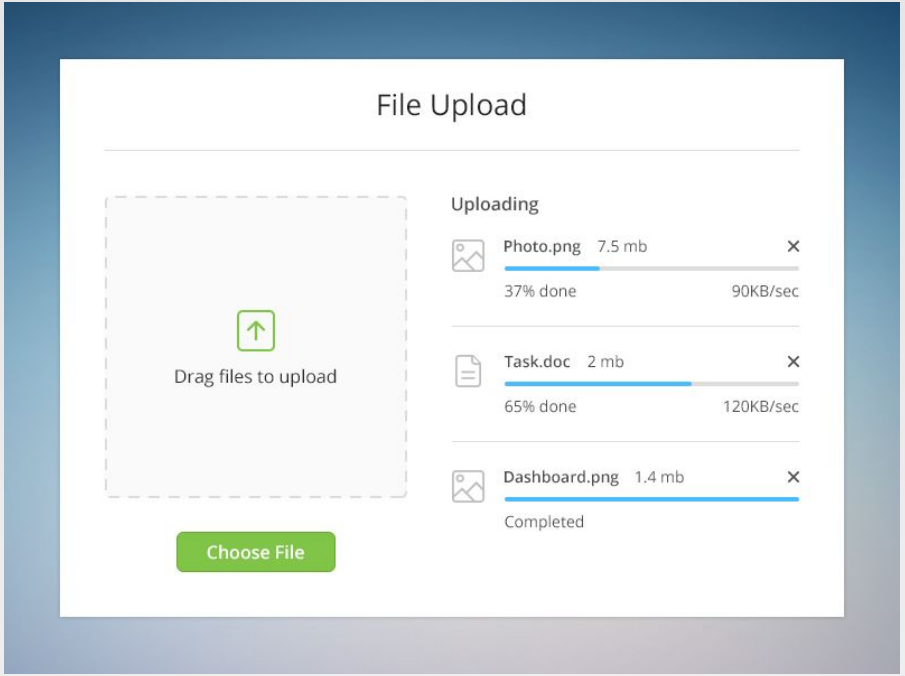
File Upload Security (AppSec)

Ben Whitney - February 2020

Introduction

My name is Ben Whitney, and I want to help make your web application more secure.

Many sites accept file uploads



Many sites accept file uploads

Which sites

- Large SaaS Applications
- SMB websites
- Web apps and mobile servers
- Hobbyist websites

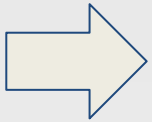
What kind of files?

- Photos
  - Profile Pictures
  - Photo Sharing
  - Company Logos
- Documents
  - Signed documents
  - Receipts
- Videos

What happens when you upload

Client

- Client pops a dialog to let you select a file
- You choose the file to upload to the server
- Click Submit
- Client side validation
- The file gets uploaded...



Web Server

- An endpoint receives the file upload
- Server side validation
- Service saves the file to disk
- Adds an entry in the database
- Returns a success to the client

Vulnerabilities and Potential Risks

Accepting and serving files from clients increases our attack surface.

Risks to our Web Application

- Broken Access Controls
- Sensitive Data Exposure (like db passwords)
- Denial of Service
- Remote Code Execution

Risks to our Clients

- Malware
- Sensitive Data Exposure

Goals for this talk

- Awareness of some of the risks involved
- Ensure you validate all requests that take customer input

Agenda

File Access Vulnerabilities

- File Enumeration
- Directory Traversal

Dangerous File Uploads

- Large File Uploads
- Zip Bomb
- Malware
- Remote Code Execution

Conclusion

File Access Vulnerabilities

The risks in serving files

File Enumeration

When you serve documents, there is a risk of **file enumeration** vulnerabilities.

Nova Scotia

Teen charged in Nova Scotia government breach says he had 'no malicious intent'

19-year-old says he believed documents were 'free to just download' from province's FOIPOP web portal

Jack Julian · CBC News · Posted: Apr 16, 2018 5:21 PM AT | Last Updated: April 16, 2018

https://www.cbc.ca/news/canada/nova-scotia/freedom-of-information-request-privacy-breach-teen-speaks-out-1.4621970

Real World Example

- Individual made a Access to Information Request to get some public records
- Got a link to download their file at:
  - https://somewebsite.gov.ns.ca/docs/12345
- Realize that they can just change the numbers on the request to another number to download someone else's request.
- Realized that they could write a CURL script to download all the requests to their computer, just for fun.
- The government realized the mistake and attempted to charge them with hacking

How to Prevent

File Enumeration

1. Don’t give files a **numeric sequence** or guessable name
2. Put in place **access controls** if files are not public

File Access Vulnerabilities

Directory Traversal

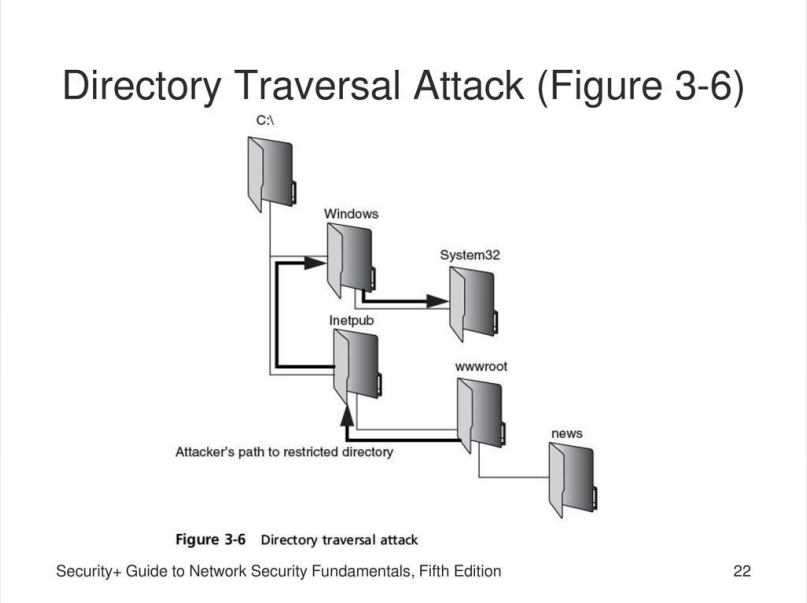
Directory Traversal Attack

GetFile.aspx?filename=terms_and_conditions.pdf

- Often we want to provide the ability to download files rather than view them
- This web function obtains whatever file you add to the **filename** parameter and downloads it to the client
- However, it may be vulnerable to path characters which change the directory

How it works…

- For example, calling GetFile.aspx with filename="../../../Windows/system.ini"
- When retrieving the ../ sequence tells the software to go up three directories to the root of the C: drive
- It then travels down to the windows folder for the target file
- If you know the path to any target file, you can download it if the permissions are not properly set



https://slideplayer.com/slide/12274560/

How to Prevent

Directory Traversal Attack

1. **Block** path characters like .. / \ : and | from file requests
2. **Validate** that downloads are served from the expected directory
3. Put in **access controls** to restrict your IIS_IUSRS web account or other service accounts.

Dangerous Files

Protect yourself from uploads!

What makes a file dangerous

- If it can cause **denial of service**
- Or cause damage or harm to the **server**
- Danger to **other users** of the site

Dangerous Files

Large File Uploads

Large File Uploads

- Job search website that allows users to upload their resume, cover letter and profile picture
- What happens if someone can upload a 4GB file?
- What happens if they upload thousands of files?

Consequences:

- Hard disk can fill up, causing errors and denial of service
- OS can’t write logs or temporary files
- Can cause loss of data and other harm

How to Prevent

Large File Uploads

1. Enforce a **maximum file size** for uploads (e.g. 10 MB)
2. **Restrict** uploads per account
3. Store files in **cloud storage** (AWS S3 buckets) to prevent running out of space
4. Ensure **adequate logging** to audit actions

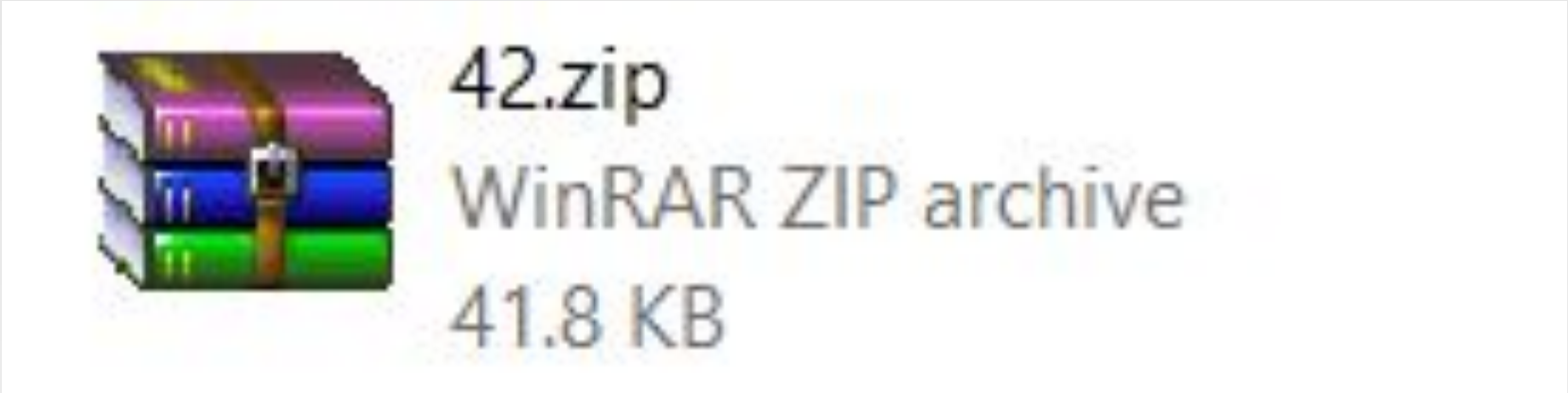
42.zip

Dangerous Files

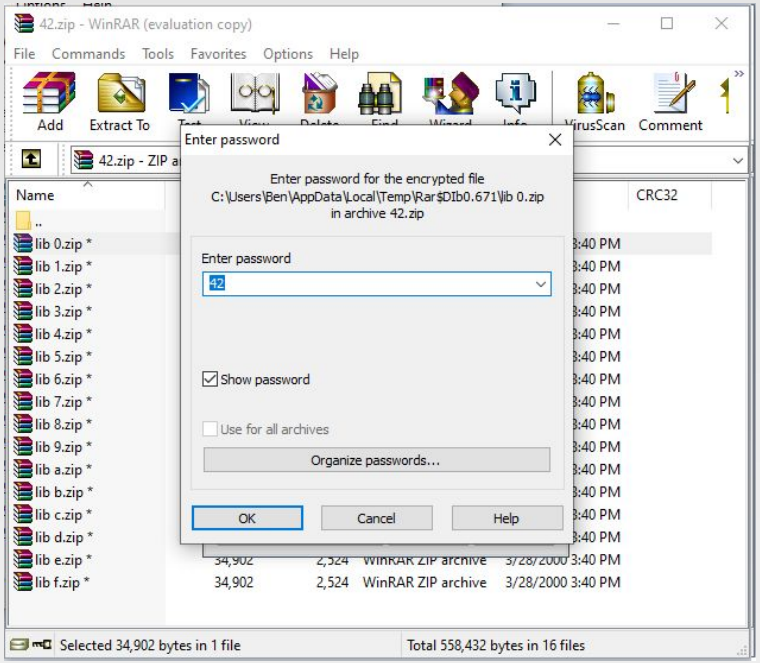
Zip Bomb

It’s bigger on the inside…

Zip Bomb



Zip Bomb


42.zip - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add
Extract To
VirusScan
Comment
42.zip - ZIP a
Name
CRC32
lib 0.zip *
lib 1.zip *
lib 2.zip *
lib 3.zip *
lib 4.zip *
lib 5.zip *
lib 6.zip *
lib 7.zip *
lib 8.zip *
lib 9.zip *
lib a.zip *
lib b.zip *
lib c.zip *
lib d.zip *
lib e.zip *
lib f.zip *
34,902 2,524 WinRAR ZIP archive 3/28/2000 3:40 PM
Enter password
Enter password for the encrypted file
C:\Users\Ben\AppData\Local\Temp\Rar$DIb0.671\lib 0.zip
in archive 42.zip
Enter password
42
Show password
Use for all archives
Organize passwords...
OK
Cancel
Help
Selected 34,902 bytes in 1 file
Total 558,432 bytes in 16 files

Zip Bomb

42.zip - WinRAR (evaluation copy)

File Commands Tools Favorites Options Help

Add Ext

Name

..

lib 0.zip *
lib 1.zip *
lib 2.zip *
lib 3.zip *
lib 4.zip *
lib 5.zip *
lib 6.zip *
lib 7.zip *
lib 8.zip *
lib 9.zip *
lib a.zip *
lib b.zip *
lib c.zip *
lib d.zip *
lib e.zip *
lib f.zip *

Selecte

lib 0.zip - WinRAR (evaluation copy)

File Commands Tools Favorites Options Help

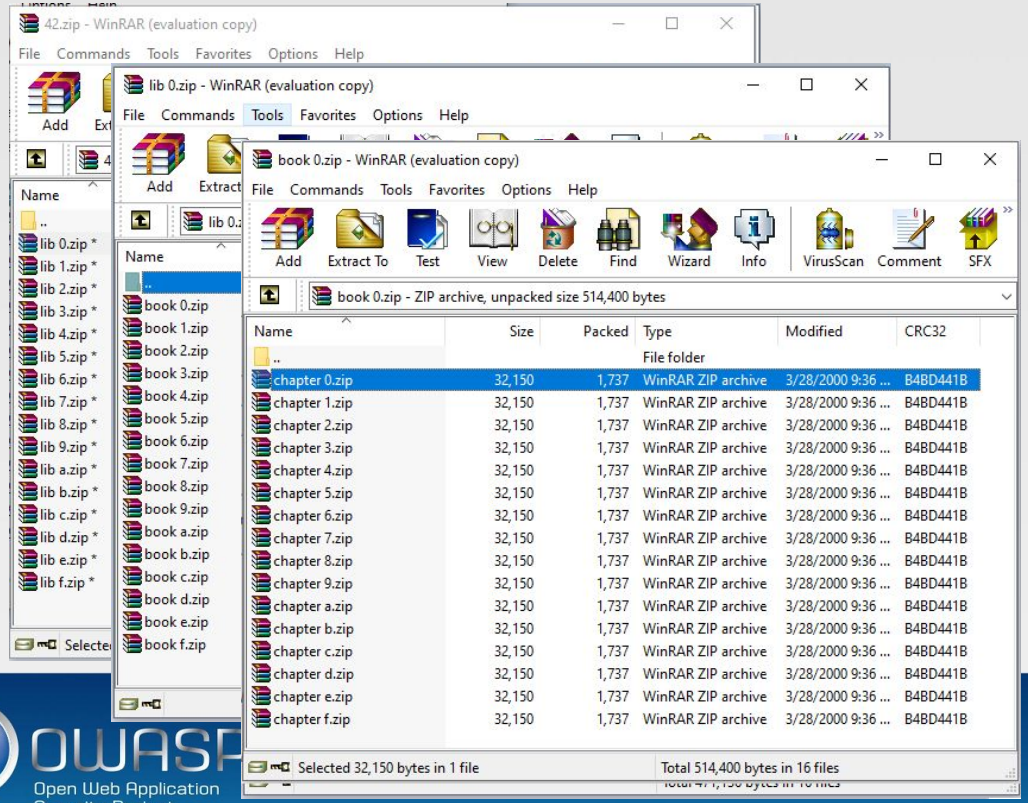
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

lib 0.zip - ZIP archive, unpacked size 471,136 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
book 0.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book 1.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book 2.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book 3.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book 4.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book 5.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book 6.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book 7.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book 8.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book 9.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book a.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book b.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book c.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book d.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book e.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6
book f.zip	29,446	2,084	WinRAR ZIP archive	3/28/2000 9:38 ...	01EB60C6

Total 471,136 bytes in 16 files

Zip Bomb


42.zip - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add
Name
lib 0.zip *
lib 1.zip *
lib 2.zip *
lib 3.zip *
lib 4.zip *
lib 5.zip *
lib 6.zip *
lib 7.zip *
lib 8.zip *
lib 9.zip *
lib a.zip *
lib b.zip *
lib c.zip *
lib d.zip *
lib e.zip *
lib f.zip *
lib 0.zip - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add
Extract
Name
book 0.zip
book 1.zip
book 2.zip
book 3.zip
book 4.zip
book 5.zip
book 6.zip
book 7.zip
book 8.zip
book 9.zip
book a.zip
book b.zip
book c.zip
book d.zip
book e.zip
book f.zip
book 0.zip - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX
book 0.zip - ZIP archive, unpacked size 514,400 bytes
Name Size Packed Type Modified CRC32
File folder
chapter 0.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter 1.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter 2.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter 3.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter 4.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter 5.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter 6.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter 7.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter 8.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter 9.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter a.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter b.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter c.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter d.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter e.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
chapter f.zip 32,150 1,737 WinRAR ZIP archive 3/28/2000 9:36 ... B4BD441B
Selected 32,150 bytes in 1 file
Total 514,400 bytes in 16 files

Zip Bomb

A zip bomb is a 42KB file
which contains 16 zip files

- each containing 16 zip files
  - each containing 16 zip files
    - each containing 16 zip files
      - each containing 16 zip files
        - each containing a 4 GB file!

Total 1,048,576 files * 4 GB =
4.5 Petabytes when unzipped!

Fills up disk if unzipped, crashes programs if they run out of memory.

How to Prevent

Zip Bomb

1. Run antivirus software to detect zip bombs.
2. If you have code to open zip files, make sure you have enough space to extract the zip file
3. Test your code against zip bomb attacks
4. Other files are zip files, like MS Office .docx, .pptx, and .xlsx

Dangerous Files

Malware

Malware

What's stopping someone from uploading a virus to your website?

- While your server might not **execute** the file and be affected, **clients** who download the files are

Malware

- Obviously block files of type .exe and .com
- But what about:

- .action
- .apk
- .app
- .bin
- .cmd
- .command
- .cpl
- .csh
- .gadget
- .inf
- .ins
- .inx
- .ipa
- .isu
- .job
- .jse
- .ksh
- .lnk
- .msc
- .msi
- .ps1
- .reg
- .scr
- .run
- .vbs
- .vbscript
- .workflow
- .ws
- .shf
- .wsh

How to Prevent

Malware

- Make a whitelist of allowed file types
- Always run anti-malware on your server
- You can test your site using the EICAR antivirus test file.

Dangerous Files

Remote Code Execution

Remote Code Execution

- One of the most dangerous vulnerabilities
- Allows an attacker to execute arbitrary commands on your webserver.

Remote Code Execution

- What happens if we don’t block uploads for .aspx files, or .php?
- The files get executed on the server

Home Page - VulnerableApp

Not secure | fileshare.owasp/

Guest

VulnerableApp Home My Uploads Best Cat Videos Trending Uploads Privacy

file share

Share your files with everyone ~~securely~~!

Welcome. Share some files with us!

Choose File No file chosen

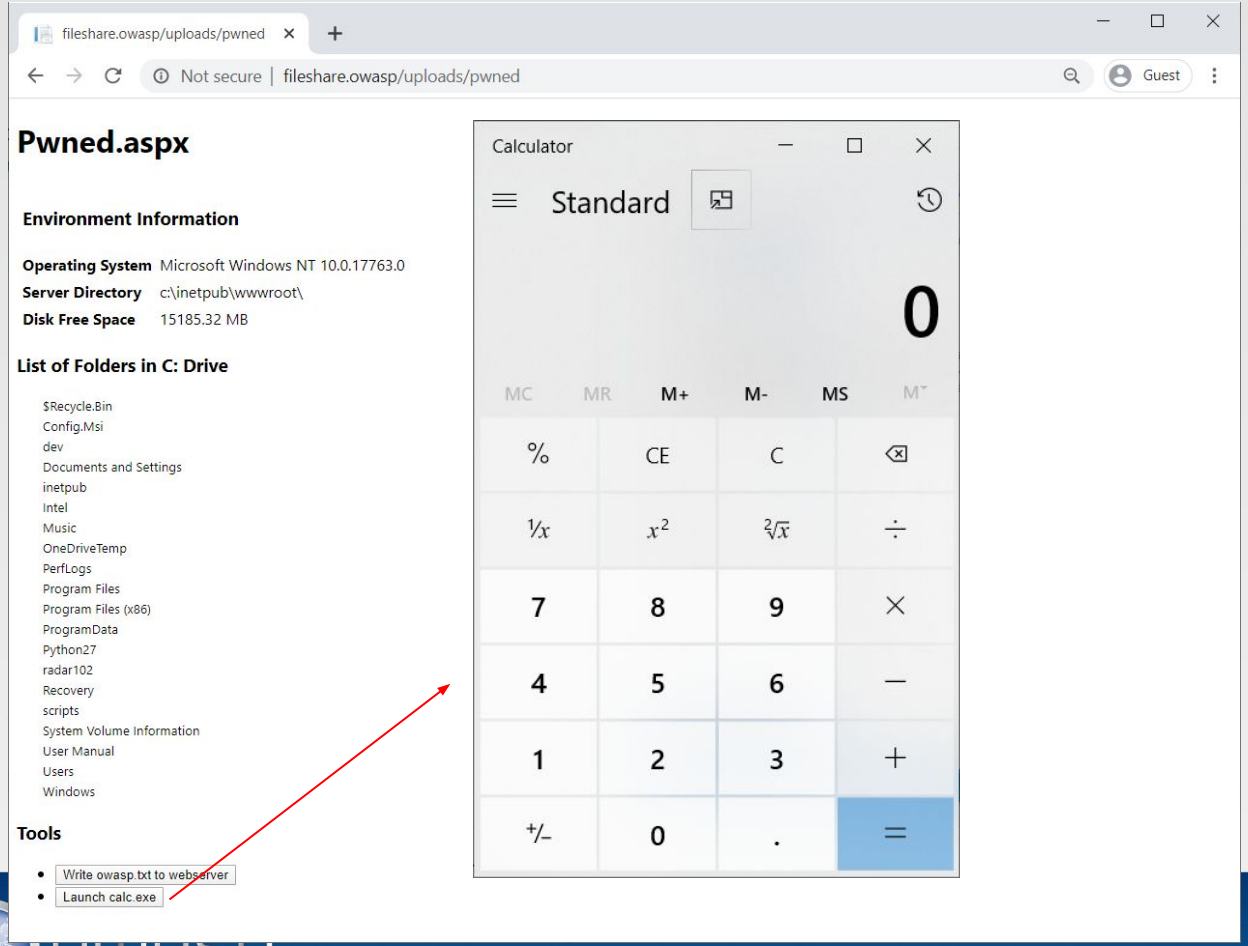
Upload

Recent Uploads

eicar.txt	Download Now
helloworld.aspx	Download Now
owasp.txt	Download Now
photo.jpg	Download Now
pwned.aspx	Download Now

Here's a vulnerable app that allows .aspx files to be uploaded.

I've uploaded pwned.aspx to demonstrate this vulnerability.



Our malicious ASPX file can:

- Read environment variables
- Get free disk space
- Get list of files on C: drive
- Write a file to the web server directory
- Launch a process (e.g. calc.exe)

As the webserver executes this file like a trusted script, it can perform any action the web server account is permitted to do.

A file like this can totally compromise your web server.

How to Prevent

Remote Code Execution

1. Enforce all **validation at the server**, not just the client
2. Use a **whitelist of allowed file types**, rather than a blacklist
3. **Disable execution** of scripts in file shares

OWASP
Open Web Application
Security Project

Conclusion

Conclusion

- Demonstrated:
  - File enumeration
  - Directory traversal
  - Denial of service and zip bombs
  - Antivirus software
  - Remote code execution
- Update components with known vulnerabilities
- Whitelist instead of blacklist
- Never trust the client -- always validate at the server!

Thank You!

Any questions?

Ben Whitney on owaspottawa.slack.com