Security 101

Protecting Your ColdFusion Applications

Pete Freitag, Foundeo Inc.

About Me
Pete Freitag

- 25+ Years ColdFusion Experience
- Company: Foundeo Inc.
  - Products: FuseGuard, HackMyCF, Fixinator
  - Consulting: Code Reviews, Server Review, CFML Security Training
- You might also know me from:
  - Lockdown Guides CF9 - CF2025
  - CFDocs.org, cfscript.me, cfbreak.com
  - blog: petefreitag.com
  - twitter/github: @pfreitag

Security Basics

- Unexpected inputs
  - Use Validation, Parameterization, Encoding
- Logic Flaws
  - Code Review

Photo by Jakub Dziubak on Unsplash

Things
To watch out for

- Files and File Paths
- Network Requests (eg cfhttp)
- Auth Logic (use SSO)
- Untrusted input data
- Crypto

Photo by Rob Martin on Unsplash

IDOR

Insecure Direct Object Reference

- Example: /secret-documents.cfm?user_id=1
  - When the attacker changes the user_id they see a different users documents.
  - Could also be a form variable, cookie, part of a JSON payload, etc.
  - Flawed Authorization Logic

IDOR Example

Bank of Insecurity: PDF Statement

Photo by J M on Unsplash

SQL Injection Example

foundeo inc.

```
<cfquery>
  SELECT story
  FROM news
  WHERE id = #url.id#
</cfquery>
```

Risk: Whenever you have a variable inside a SQL Statement

SQL Injection Example

Bank of Insecurity: News Story

Fixing SQL Injection

foundeo inc.

```
<cfquery>
  SELECT story
  FROM news
  WHERE id = <cfqueryparam value="#url.id#">
</cfquery>
```

Fixing SQL Injection

Lists

foundeo inc.

```
<cfquery>
  SELECT story
  FROM news
  WHERE topic IN (
    <cfqueryparam value="#url.type#" list="true">
  )
</cfquery>
```

SQL Injection
cfqueryparam

- cfsqltype shortcut:
    - You can simply use integer instead of cf_sql_integer
    - The cf_sql_ prefix is no longer required as of ColdFusion 11
- Add maxlength when possible.
- More tips: Mastering cfqueryparam

#3 SQL Injection

With queryExecute

foundeo inc.

```
queryExecute("SELECT story
  FROM news
  WHERE id = #url.id#”);
```

```
queryExecute("SELECT story
  FROM news
  WHERE id = :id”, {id=url.id} );
```

#3 SQL Injection

With queryExecute

foundeo inc.

```
queryExecute("SELECT story
 FROM news
 WHERE id = :id", {
   id={
     value=url.id,
     cfsqltype="integer"
   }
 });
```

SQL Injection

Other Places to Look

- ORMExecuteQuery
- Stored Procedures - if proc builds SQL statements dynamically from inputs
- new Query() - removed as of CF2025

SQL Injection

When Parameters Don’t Work

- Places that parameters *may (depending on DB)* not work:
    - ORDER BY clause
    - SELECT TOP n
    - LIMIT / OFFSET
- Validate!
- Use SELECT TOP #int(url.n)#
- Use cfqueryparam whenever you can

Cross Site Scripting (XSS)

foundeo inc.

```
<cfoutput>Hello #url.name#</cfquery>
```

XSS Example

Bank of Insecurity: Login Form

Fixing XSS

Methods to encode variables

foundeo inc.

```
<cfoutput>Hello #encodeForHTML(url.name)#</cfquery>
```

```
<cfoutput encodefor="html">Hello #url.name#</cfquery>
```

Fixing XSS

Picking the correct encoder

foundeo inc.

Context	Method
HTML	`encodeForHTML(variable)`
HTML Attribute	`encodeForHTMLAttribute(variable)`
JavaScript	`encodeForJavaScript(variable)`
CSS	`encodeForCSS(variable)`
URL	`encodeForURL(variable)`

Fixing XSS
Other Techniques

- Encoding is best, but is not always possible:
  - Sanitize HTML: isSafeHTML, getSafeHTML
  - Content-Security-Policy

Server-Side Request Forgery (SSRF)

- SSRF occurs when your server makes a HTTP request to an arbitrary URL
- Can allow attacker to hit other http services behind the firewall (dbs, caches)
- Cloud Metadata APIs (eg: 169.254.169.254) can leak access keys or other sensitive info:
  - Tip: on AWS Disable IMDSv1 and use IMDSv2 instead

SSRF

Some Functions / Tags That Can Request a URL

foundeo inc.

- cfhttp
- PDF: cfdocument / cfhtmltopdf (within HTML: img, iframe, etc)
- Images: isImageFile
- XML: XmlParse, XmlSearch, XmlValidate
- Additional List: https://hoyahaxa.blogspot.com/2021/04/ssrf-in-coldfusioncfml-tags-and.html

Command Injection

- Take care when using cfexecute, or other APIs that may wrap a native command.
- Avoid untrusted variables in the name and arguments.

```
<cfexecute name="c:\bin\tool.exe" arguments="-n #url.n#">
```

Remote Code Execution (RCE)

- A few different ways this can happen in CFML, most common:
  - Evaluate
  - IIF
  - cfinclude

RCE Example

Bank of Insecurity: Contact Form

Fixing RCE

Replace IIF with Ternary Operator

foundeo inc.

```
iif( len(name), de("#name#"), de("Anonymous") )
```

```
len(name) ? name : "Anonymous"
```

Fixing RCE
Fixing Evaluate

foundeo inc.

```
evaluate("url.#name#")
```

```
url[name]
```

Rid your code of evaluate() - terrible for both performance and security

Fixing RCE
Fixing Evaluate

foundeo inc.

```
#evaluate("x+y")#
```

```
#x+y#
```

Rid your code of evaluate() - terrible for both performance and security

RCE

Good News / Bad News

- Good News
  - Easy to find
  - Easy to fix
- Bad News
  - Very Dangerous
  - Might have a lot if your code was written early 2000’s

File Uploads

- Regularly review all your file upload code:
  - Always checks the file extensions of uploaded files against a list of allowed extensions. Use the **`allowedExtensions`** attribute of cffile.
  - Do not upload directly under the web root (at least not before validation)
  - Don’t rely on mime type checks alone, they can be bypassed!
  - Set **`this.blockedExtForFileUpload`** to full list of executable extensions.

Path Traversals

- Happens when you construct a file path with unsafe variables.
- Example:

```
<cfinclude template="html/#url.name#">
```

Path Traversals

- Be careful whenever file paths are constructed dynamically
  - cffile, cfdocument, cfinclude, cfmodule, cfspreadsheet
  - fileOpen, fileRead, fileWrite, etc.
  - cfdirectory, directoryList, etc.

Cross-Site Request Forgery (CSRF)

- Causing a request to be made by an **authenticated** and **authorized** user's browser to perform an unwanted action.

CSRF

Best Example

foundeo inc.

- Netflix in 2006 - Remember when they rented DVDs?
  - To Add a Movie to your Queue:
    - Request to: **http://www.netflix.com/AddToQueue**
    - Pass a movie id: **movieid=70011204**

CSRF

Netflix Example

foundeo inc.

Step 1: Create a Web Page With The Following img tag:

```
<img src="http://www.netflix.com/AddToQueue?movieid=70011204">
```

Step 2: Get People to Visit the Page

Step 3: Millions of people added *Sponge Bob Square Pants the Movie* to their Queue

CSRF

Fixing CSRF

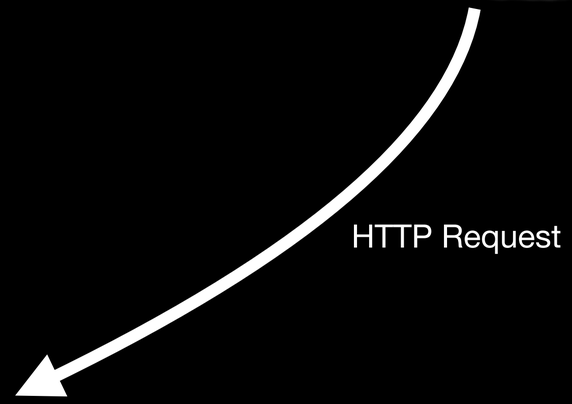
foundeo inc.

- SameSite Cookies
- Check HTTP Method (eg: require POST)
- CAPTCHAs - Helpful but causes usability issues / AI
- Inspect Sec-Fetch and Origin Request Headers
- Use a CSRF Token
  - CFML Functions: CSRFGenerateToken() and CSRFVerifyToken()

CSRF

Fixing CSRF Sec-Fetch Headers (Modern Browsers)

```
<img src="http://www.netflix.com/AddToQueue?movieid=70011204">
```




```
GET /AddToQueue?movieid=70011204
Host: www.netflix.com
Sec-Fetch-Dest: image
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
```

Quick Wins

- **Validation** - more validation = less vulnerabilities
- **Logging & Monitoring** - know when problems arise
- **Code Scanning** - continuously look for issues, find known vulnerabilities

Photo by Klim Musalimov on Unsplash

OWASP Top 10
2021 Edition

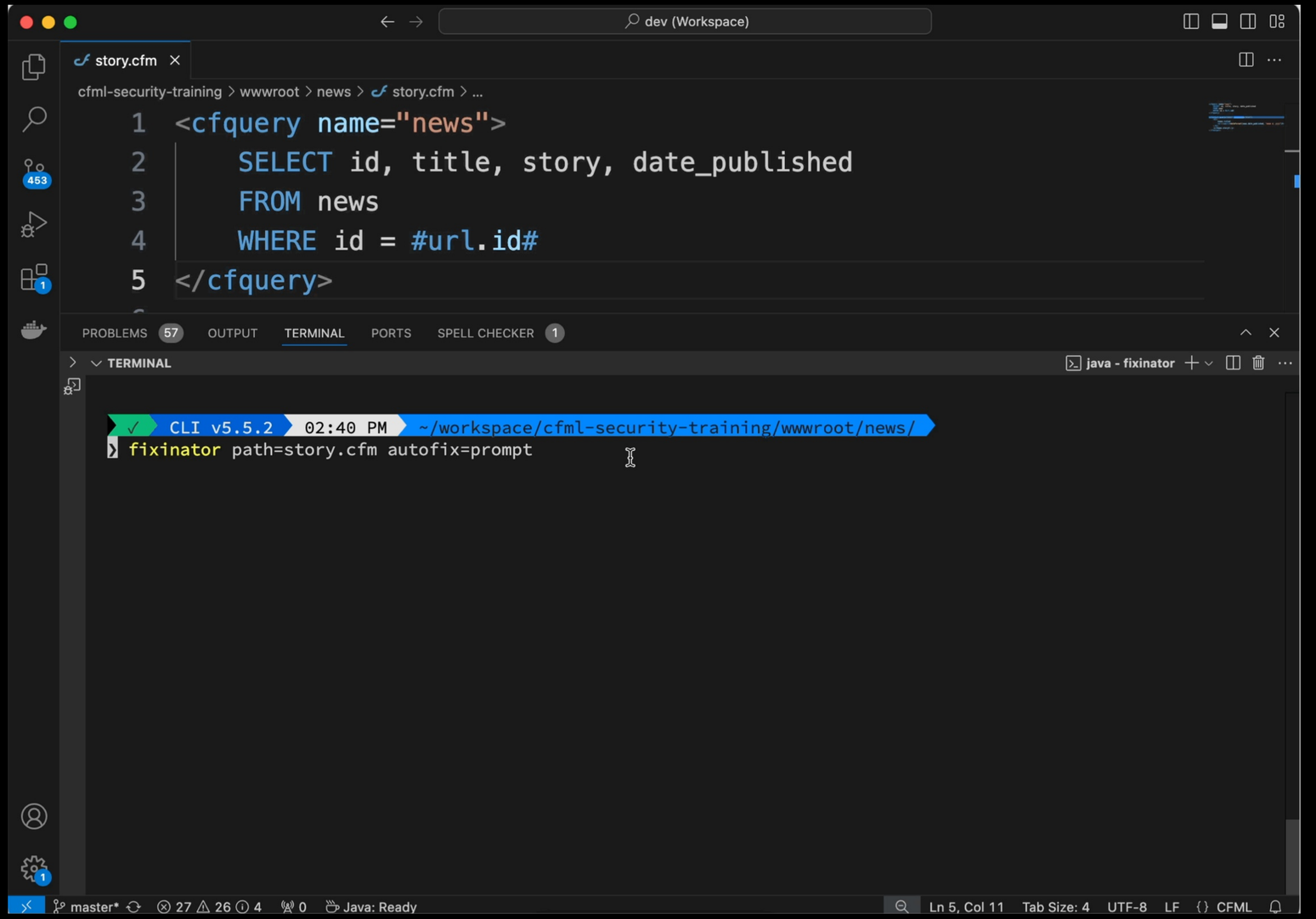
1. **Broken Access Control** - IDOR
2. **Cryptographic Failures** - Weak Algo, Key Storage, Incorrect Implementation
3. **Injection** - XSS, SQLi
4. **Insecure Design** - Error Disclosure, Unprotected Credentials
5. **Security Misconfiguration** - Configuration
6. **Vulnerable and Outdated Components** - KEV
7. **Identification and Authentication Failures** - Logic or Weak Implementation
8. **Software and Data Integrity Failures** - Supply Chain
9. **Security Logging and Monitoring Failures** - Insufficient Logging, Log4Shell
10. **Server-Side Request Forgery** - SSRF

DoD photo by Staff Sgt. Luisito Brooks, U.S. Army/Released

Fixinator

foundeo inc.

- Fixinator can scan your code and fix certain vulnerabilities



Learn More

foundeo inc.

- ColdFusion Security Guide
  - https://foundeo.com/security/guide/
- Ask Me
- Resources: OWASP, CWE Site

Adobe ColdFusion Developer Week $100 Gift Card

Q: In what version of ColdFusion was cfqueryparam introduced?

First person with correct answer in the chat wins

Thank You!

foundeo inc.

pete@foundeo.com

Weekly CFML Community Newsletter: cfbreak.com