Recommended Enhancements to the Florida Courts E-Filing Portal Security

Contents

Document Version Control

Date	Version #	Editor	Description of Change
10/18/2016	0.01		Creation

Purpose of this document

The purpose of this document is to address the common threats public web applications, such as the Florida Courts E-Filing Portal (Portal), face from bots and browser automation and provide recommendations to detect and limit the risks from such threats. This document is NOT an all-inclusive security policy/standards document. The focus of this document is narrowly limited to the topic of threats from bots and browser/script automation applications.

Portal History

The Portal provides a common entry point for court electronic filings in the State of Florida and was developed, in compliance with the E-Filing rules set forth in Florida Rule of Judicial Administration 2.525, by the Florida Courts E-Filing Authority Board.

The Portal consists of:

a. Florida Courts E-Filing Web Site and
b. Electronic interfaces (implemented as web services) that can be consumed by external (external to E-Portal) application(s)/system(s).

The Portal can electronically receive pleadings/documents through one of the following methods approved by the Florida Courts E-Filing Authority Board:

1. Florida Courts E-Filing web site (approved as part of the Agreement creating the E-Filing Authority Board)
2. Electronic Interfaces
    a. Portal/State Attorney Exchange for Criminal Case Filings (a/k/a CBI Interface) - (approved as part of the criminal E-Filing mandate. While no formal certification was required, access is limited to governmental agencies such as State Attorney/Public Defender/Judicial Circuit system(s) and applications)
    b. Portal/Third Party Vendor Exchange for Case Filings (a/k/a TPV Interface) (While not currently in production, it has been approved by the Board and access to the interface requires certification. Third Party vendors can be per profit entities in addition to judicial entities supported in the earlier interface.)

Terms and Definitions

Portal

Common entry point for court electronic filings in the State of Florida.

Bot

Web crawler or Web spider, a computer program that does automated tasks. Internet bot, a computer program that does automated tasks. Zombie computer, a computer that is part of a botnet.

Internet bot

An Internet bot, also known as web robot, WWW robot or simply bot, is a software application that runs automated tasks (scripts) over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. The largest use of bots is in web spidering (web crawler), in which an automated script fetches, analyzes and files information from web servers at many times the speed of a human.

WebDriver

The W3C WebDriver API is a platform and language-neutral interface and wire protocol allowing programs or scripts to control the behavior of a web browser. WebDriver enables developers to create automated tests that simulate user interaction.

OWASP
The Open Web Application Security Project is an online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

Denial-of-service attack (DoS)
DoS attack is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Distributed Denial-of-service attack(DDoS)
A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Captcha
A CAPTCHA (a backronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a type of challenge-response test used in computing to determine whether or not the user is human.

reCAPTCHA
reCAPTCHA is a CAPTCHA-like system designed to establish that a computer user is human (normally in order to protect websites from bots) and, at the same time, assist in the digitization of books.

Content Scraping
Content scraping is the duplication of website content either manually, through copy and paste, or through running a site scraper program that picks up the content.

Honeypot technique
The honeypot technique is a technique to prevent spam bots from submitting forms. Spam bots love form fields and when they encounter a form field they will fill it out, even if the field is hidden from the user interface.

Comprehensive Case Information System
The Comprehensive Case Information System (CCIS), offered by Florida's Clerks of Court, is a secured single point of search for state wide court case information. The information held by the Clerks of Court that may be accessed through CCIS includes court case information, Official Records and performance and accountability measures.

References

- Bot Definition - http://techterms.com/definition/bot
- Web Driver - https://www.w3.org/TR/webdriver/
- OWASP - https://www.owasp.org/index.php/Main_Page
- Denial of service attack https://en.wikipedia.org/wiki/Denial-of-service_attack
- Captcha - https://en.wikipedia.org/wiki/CAPTCHA

- reCAPTCHA - https://www.google.com/recaptcha/intro/index.html https://en.wikipedia.org/wiki/ReCAPTCHA
- OWASP automated threat Hand book - https://www.owasp.org/images/3/33/Automated-threat-handbook.pdf
- Florida Courts E-Filing Portal - Browser Automation and Impact to Portal Security - S:\COMMON\EPortal\40-Technical
- CCIS - https://www.flccis.com/ocrs/login.xhtml

Types of Threats

The most frequently used automated attacks identified by OWASP are

1. Credential stuffing
2. Scraping
3. Application layer DDoS
4. Captcha Bypass
5. Card Cracking
6. Credential cracking
7. Cashing Out
8. Carding

While the Portal may not be susceptible to all the threats listed above, by nature of its functions, it can be susceptible to scraping and DDoS style attacks.

Need for Security Enhancements

1) The Portal provides a common entry point for submission of pleadings electronically to the courts and DoS style attacks on the Portal can have an adverse effect.

2) The Portal provides access to the case information and underlying docket sheet, documents in CCIS. For example, authorized Portal users can access the docket sheet and the underlying documents in CCIS for a given court case, into which they have electronically submitted a pleading.

3) Recent review of audit data maintained by the Portal identified a BOT like application signing into the system 87 times with different valid credentials in a sixty-minute window. While no malicious activity is identified, potential to use such an application as a DDos agent exists and should be addressed

Security Alert

The Portal shall add the following warning as appropriate

##WARNING##
This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of any data contained

herein or in transit to/from this system may constitute a violation of Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.
########ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING############

Recommendation

1) Implement firewall/network based solutions to detect, limit bots.

2) Enhance Portal security to limit number of logins from a specific IP address in a short interval. For example, if someone attempts to login more than once in a 5-minute interval, ask the user to confirm that he/she is a human and not a bot.

3) If a user logs in from a IP address that is not recognized, ask the user to confirm that he/she is a human and not a bot

4) Implement Honey Pot technique in Portal forms. While this technique may not limit access to a custom automation application explicitly created to automate Portal functions, it can prevent spam bots from logging into the Portal.

5) Limit access to approved methods.

6) Add Security Alert to appropriate Portal pages (Example Login Page, Account created email, Terms of Use Page) and Portal generated email(s).