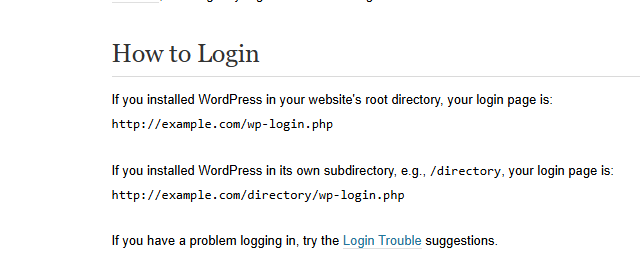
### **Log Analysis — Compromised WordPress**

**Scenario**: One of our WordPress sites has been compromised but we’re currently unsure how. The primary hypothesis is that an installed plugin was vulnerable to a remote code execution vulnerability which gave an attacker access to the underlying operating system of the server.

#### **Tasks**

1. **Identify the URI of the admin login panel that the attacker gained access to (include the token)**

A quick google search about the Wordpress login page revealed that the login page would usually be http://example.com/directory/wp-login.php.



So we need to search for wp-login.php in our log file to answer this question.

cat access.log | grep wp-login.php



**Answer:** /wp-login.php?itsec-hb-token=adminlogin

**2. Can you find two tools the attacker used?**

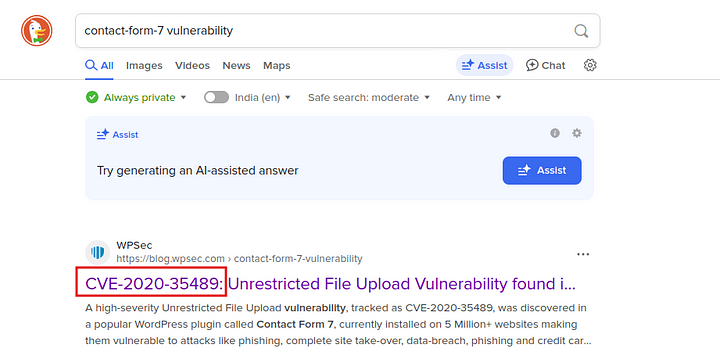
We can check the user agent string in the logs to figure out which tools were used by the attacker.

cat access.log | cut -d "\"" -f 6 | uniq | sort



**Answer:** sqlmap wpscan

**3. The attacker tried to exploit a vulnerability in ‘Contact Form 7’. What CVE was the plugin vulnerable to? (Do some research!)**

****

**Answer:** CVE-2020–35489

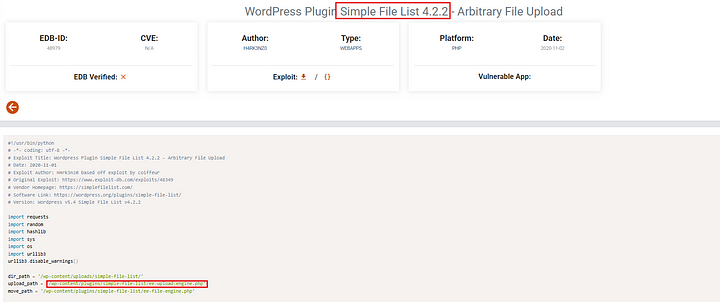
**4. What plugin was exploited to get access?**

If we search for the POST requests to the plugins folder we see at the very end a POST request to wp-content/plugins/simple-file-list/ee-file-engine.php.

grep -E 'POST.\*plugin' access.log



A simple google search with the path revealed the version of the plugin that is vulnerable.

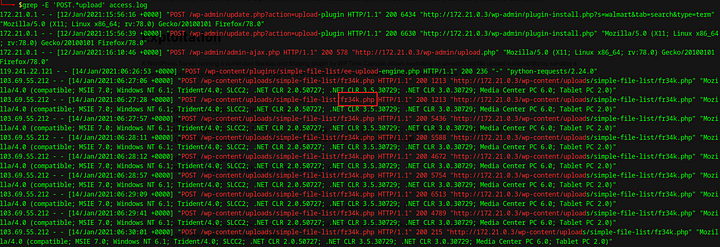


**Answer:** Simple file list 4.2.2

**5. What is the name of the PHP web shell file?**

Let us search for the files uploaded to this path.

grep -E 'POST.\*upload' access.log



**Answer:** fr34k.php

**6. What was the HTTP response code provided when the web shell was accessed for the final time?**

Search for the logs that had this file name in them.

grep -E 'fr34k.php' access.log



The response code in the last log record is our answer

**Answer:** 404

This is the end of this walkthrough.