2017 – Equifax Data Breach

CVE-2017-5638 vulnerability at Apache Struts

What Happened?

In 2017, cyber-criminals breached Equifax by ex- ploiting a remote code execution vulnerability in their web app development framework. They spread across various hosts due to weak network segmentation and discovered an unencrypted data-store containing database credentials. They used these credentials to ac- cess the company databases and exfiltrated customers' personally identifiable information and payment card records.

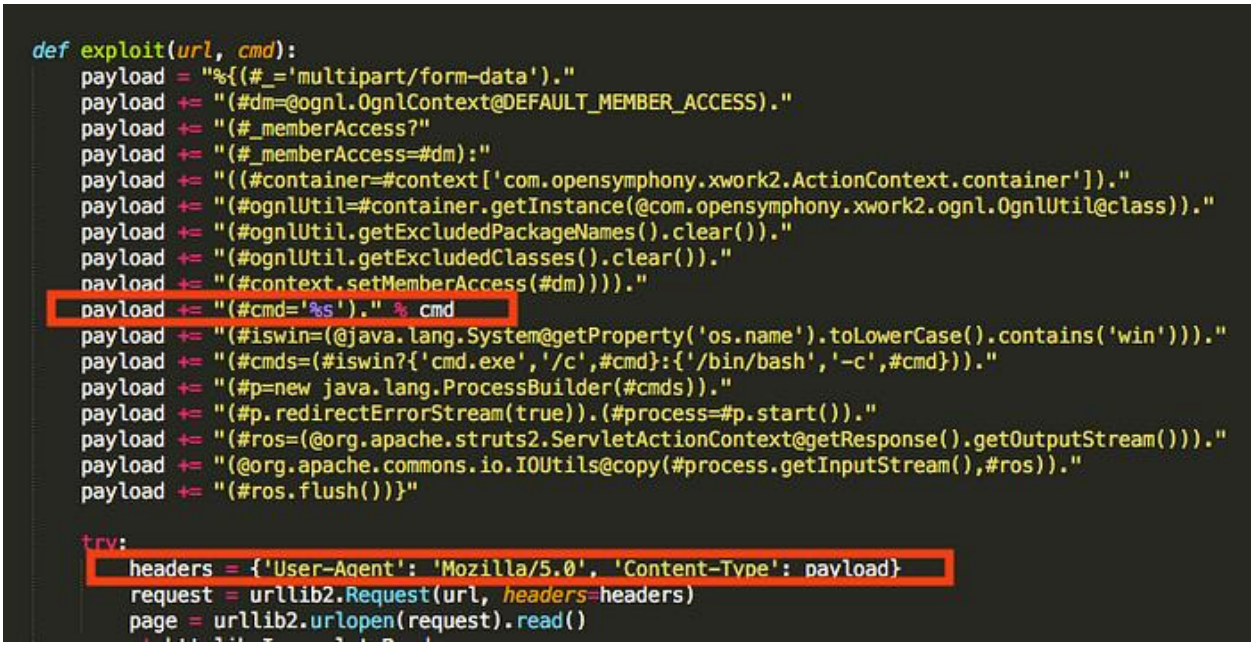
How the attack has happened

Being this document is an overview, you can directly search internet for more details.

Attacker expolited a remote code execution vulnerabilty at Apache Struts servers in Equifax, and gained remote Access to execute arbitrary commands with crafted Content-Type header value in HTTP request.

Then attacker discovered the databases and stole data with querying databases more than 9000 times over 76 days.

How ALISA could help?



ALISA can understand if there is a deviation or anomaly in every single header and every single query string, URL, URI.

As seen from the figure, the attacker executes codes using Content-Type header. Since ALISA examines the deviations for all the headers and values, ALISA can easily detect the attack coming to web application in Content-Type header and creates custom signatures for WAFs for these packets.