**CVE-2017-5638**

이 취약점은 Apache Struts 2.3.5 ~ 2.3.31 혹은 2.5 ~ 2.5.10 버전에 해당하는 취약점으로 HTTP request header의 content-type 부분을 변조하여 원격에서 코드 실행이 가능하도록 한다. Content-Type에 OGNL 표현식을 삽입할 경우 struts2의 Jakarta 플러그인 오류 처리 과정에서 임의의 코드가 실행될 수 있다고 한다.

OGNL의 경우 Object-Graph Navigation Language의 약자로 자세한 내용은 다음 링크를 참조하면 될 것 같다. https://blog.naver.com/ssong24/66954999

Metasploit을 통해 exploit을 진행할 때 기본적으로 설정할 내용은 rhost, rport, targeturi가 있다. 또한 이 모듈의 경우 check command를 통해 exploit 할 수 있는지 확인할 수 있기 때문에 설정이 제대로 되었는지 확인할 수 있다. targeturi의 경우 기본값이 주어져 있긴 하지만 수정해야 정상적으로 exploit 할 수 있다.

다음으로 payload를 지정하면 되는데 payload가 대략 300개 가량 되므로 자신이 필요한 것을 잘 선택할 필요가 있다. 여러 가지 payload 중 기본적인 것만 사용해보았다.

우선 cmd/unix/generic의 경우 cmd 인자 하나만을 가진다. 즉, cmd에서 지정한 명령을 target에서 실행시킨다. 예를 들면 tmp 디렉터리에 파일을 생성한다던가 말이다. 명령을 직접 지정할 수 있는 만큼 다양한 응용이 가능할 것으로 생각되나 netcat과 같이 동적인 명령은 실패하였다. (무엇이 문제일까)

다음으로는 cmd/unix/reverse 모듈이다. 이 모듈의 경우 기본적인 형태의 reverse shell을 연결할 수 있으며 lhost와 lport 인자를 가진다. 이 인자의 경우 reverse shell이므로 attacker의 정보를 사용하면 된다.