Web Application Hacking

Blind SQLi, Stored XSS
Alessandro Morabito @ Epicode

1 Introduzione

In questo progetto si vuole sfruttare una vulnerabilità nel servizio `Java RMI` in ascolto su porta `1099`. `Java RMI` (`Java Remote Method Invocation` permette l'accesso ad oggetti in un'altra `Java VM`.

2 Scansione con `nmap`

Per velocizzare il processo di scansione, sapendo che vogliamo andare a controllare unicamente i servizi sulla porta `1099`, restringo lo *scope* a quella porta.

```
Nmap scan report for 192.168.1.105
Host is up (0.00020s latency).

PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry
```

3 Exploit con `metasploit-framework`

Dopo aver individuato il servizio in ascolto sulla porta ho utilizzato `metasploit` per cercare exploit per tali servizio. Dopo averlo selezionato ho inizialmente provato il payload `java/meterpreter/reverse_tcp` di default.

4 Conclusioni

In questo progetto si è fatto in maniera tale di simulare un attacco ad applicazioni web attaccando sia la sezione di back-end della DVWA (Database, tramite query `SQL`), sia la sezione di front-end (con codice *JavaScript*). Entrambe le vulnerabilità sono dovute a un inefficace filtro dell'input inserito dall'utente, che è quindi in grado di inserire un codice malevolo.