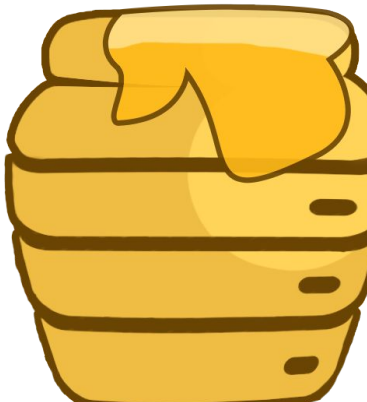
HoneyMod

Apache honeypot module

Popescu Daniel
Coordonator: Conf. Dr. Sabin Corneliu Buraga



Honeypot

- Ce este un honeypot?
- Principalele motive pentru a instala un honeypot
  - Analizarea modurilor de atac
  - Dovezi impotriva atactorului
- Existing honeypots and communities

Concepte folosite in proiect si prezentare

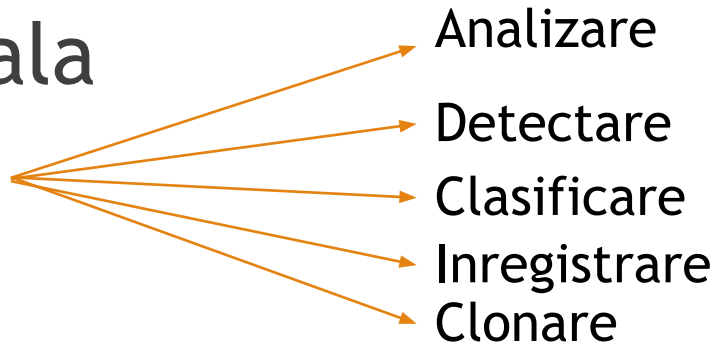
- Request HTTP
- Structura modular Apache
- “Content generator” in Apache
- Filtre Apache

HoneyMod

- Modul Apache
- Detecteaza atacuri
- Clasifica atacuri
- Creeaza clone atacabile
- Independent de content generator
- Verifica atacatorul

Structura proiectului

- Aplicatia principala
  - Modulul Apache



- Aplicatii ajutatoare
  - Site atacabil
  - Interfata admin

Atacuri tratate

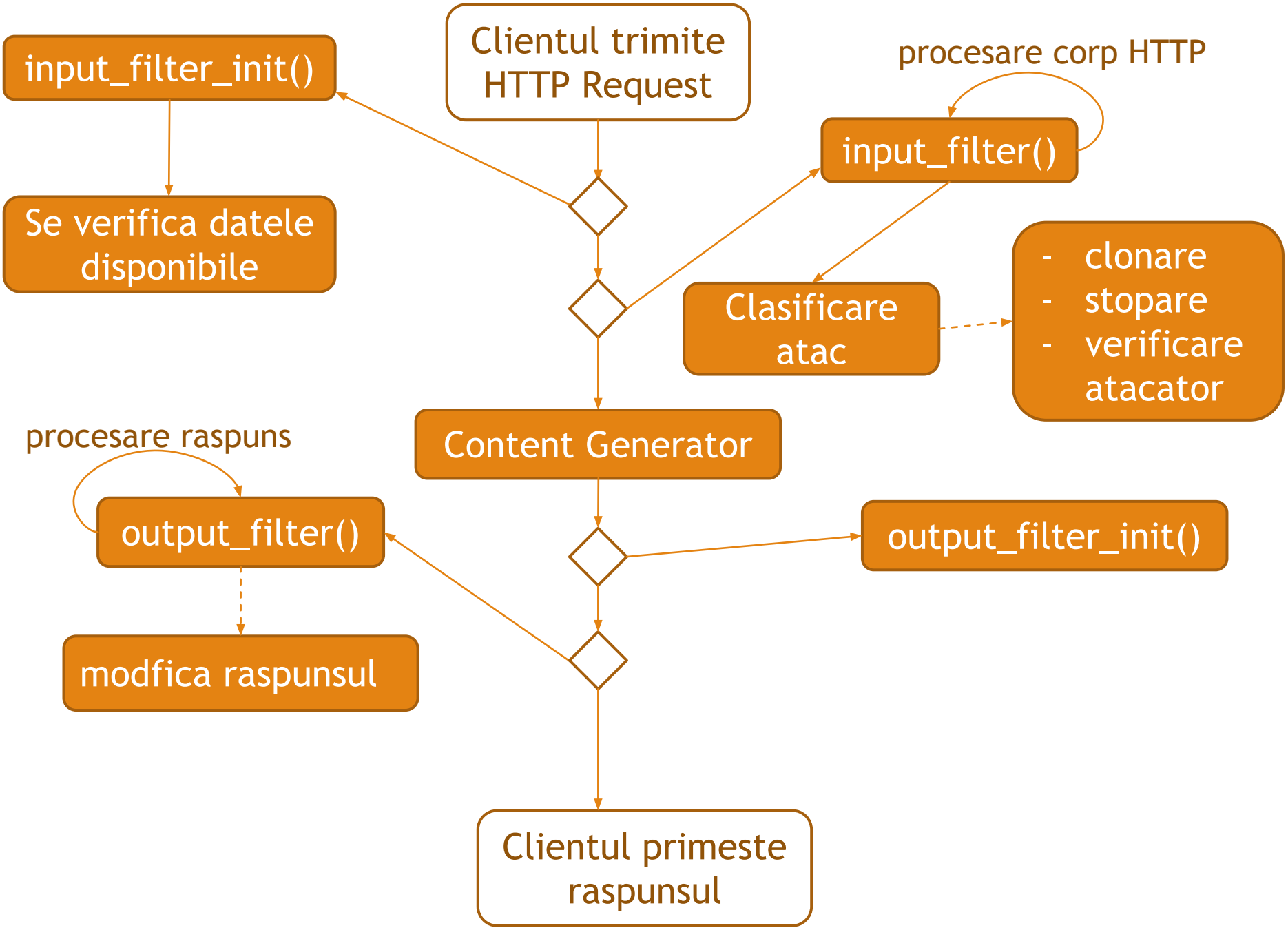
	Rate de Detectie	Rate de Clasificare
SQL injections	99%	80%
XSS	70%	80%
User/Password guessing	70%	100%
Cookie meddling	50%	-
Buffer overflow	80%	100%
Command execution	30%	-
Brute force	70%	70%
Canonicalization	99%	-

Detectarea/Clasificarea unui atac

Analizand informatiile:

- Url
- Parametrii GET si POST
- Header de intrare
- Atacuri sau vizite precedente ale atacatorului

- Utilizand expresii regulate
- Utilizand interpretor Lex&Yacc


Clientul trimite HTTP Request
input_filter_init()
Se verifica datele disponibile
procesare corp HTTP
input_filter()
Clasificare atac
- clonare
- stopare
- verificare atacator
Content Generator
procesare raspuns
output_filter()
modfica raspunsul
output_filter_init()
Clientul primeste raspunsul

Directii de viitor

- Folosirea de retele neuronale pentru atacuri si atacatori
- Imbunatatirea ratelor de detectie si clasificare a atacurilor
- Contributie active in comunitatile honeypot
- Stabilirea unui protocol prin care diferite honeypots sa comunice si sa se ajute intre ele.