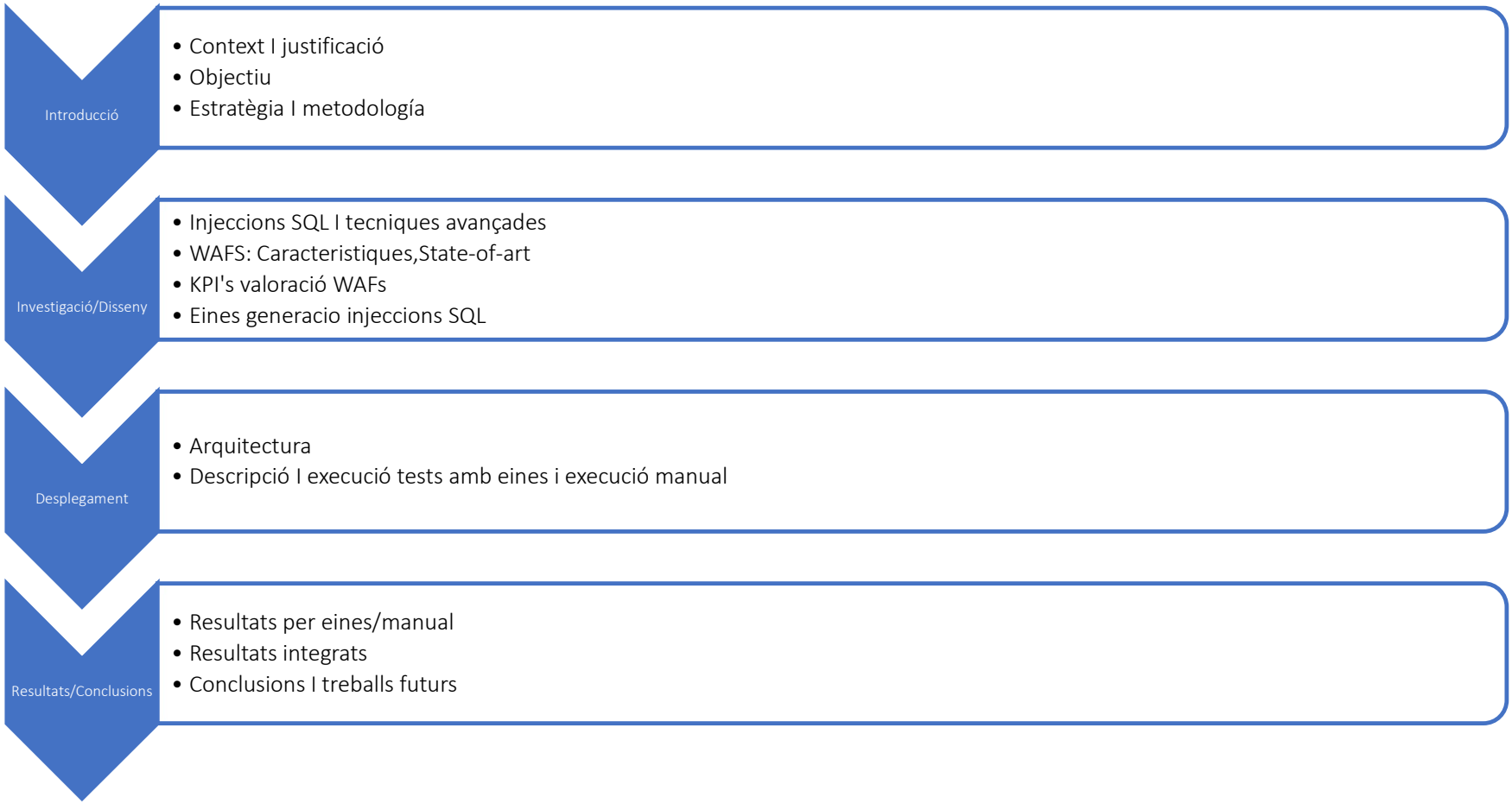
Master de Ciberseguretat i Privadesa
Seguretat Empresarial

Pere Gorchs Montaner

Anàlisi comparatiu comportament Open Source Web Application Firewalls davant SQL injections avançats

Universitat Oberta de Catalunya uoc.edu

Index



Context i justificació

- L'era de la digitalització incrementa l'aparició d'aplicacions empresarials.
- Majoria d'aplicacions web amb base de dades SQL com a repositori d'aquestes.
- Moltes no incorporen seguretat integrada en temps de creació o SDLC.
- Altres són aplicacions Legacy amb dificultat per incorporar-la.

- WAFS: Busquen aturar els atacs/injeccions a les aplicacions Web.
  - En determinades cirscumstàncies es bypassa el WAF i l'atac arriba a l'aplicació.

Objectiu

- Estudi comparatiu del comportament de WAF's amb i sense ML engine davant injeccions SQL avançades.
  - Recopilació de les injeccions SQL avançades en l'actualitat.
  - Estudiar comportament d'aquests atacs que "bypassen" WAF tradicional.
  - Estudiar comportament d'aquests atacs que "bypassen" WAF amb ML.

- Objetiu ODS: Impacte positiu en la dimensió de sostenibilitat.
  - Enfocament de proves mitjançant Maquines virtual, reduint impacte en recursos CPU,etc.. i en l'ús d'energia.
  - Alineació amb ODS 12 – Responsible consumption and production.

Estratègia i metodologia

- ESTRATÈGIA: Creació d'un entorn per testeig i l'observació empírica dels resultats determinant les conclusions que se'n desprenguin.

- METODOLOGIA: Aproximació metodologia Waterfall dividida en diverses fases.

Master de Ciberseguretat i Privadesa
Seguretat Empresarial

Investigació - Disseny

Injeccions SQL

- TIPUS:
  - In-band SQLi
    - Error Based
    - Union Based
  - Blind SQLi
    - Boolean
    - Time Based
  - Out-of-band SQLi

Tècniques evasió WAF: SQLi avançades

- Pre-processor explotation
- Impedance mismatch
  - HTTP Parameter pollution
  - HTTP Parameter Fragmentation
  - Doble URL Encoding
- Rule set bypassing
  - Brute force
  - "Reverse engineering" sobre les regles del WAF

WAFS: Concepte i caracteristiques

- CONCEPTE: Un Web Application Firewall és un programari que monitoritza el trànsit destinat a un website. L'anàlisi que efectua determina si la petició es maliciosa o inofensiva; es descarta o es deriva al lloc web segons el resultat.

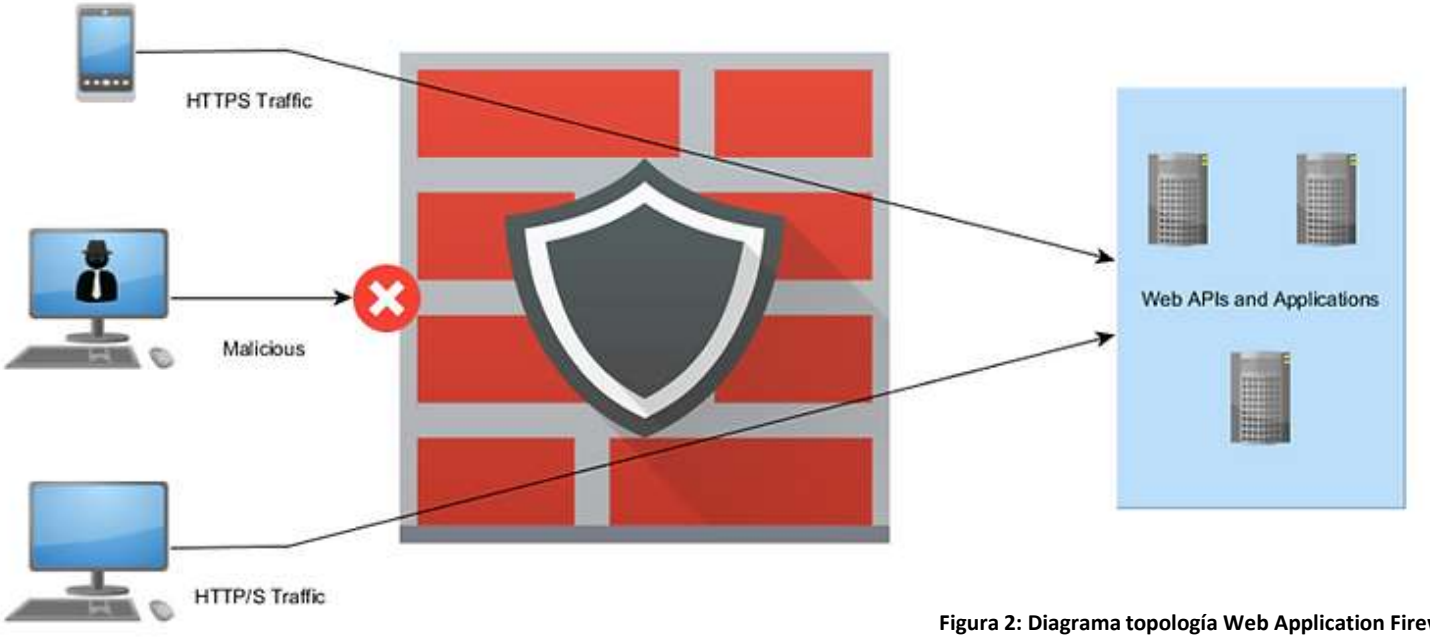


Figura 2: Diagrama topología Web Application Firewall (Extret de [9]).

WAFS: Concepte i caracteristiques

- Funcionalitats
  - Filtratge trànsit i monitorització en temps real
  - Protecció contra injeccions
  - Prevenció I detecció d'intrusions
  - Protecció sistemes back-end
  - Compliment regulatori
- Tipus
  - In-line Appliance
  - End-point
  - Cloud
- Segons config xarxa
  - Reverse Proxy
  - Bridge
  - Monitoring

WAFS: Concepte i característiques

- Models de seguretat
  - Model de seguretat POSITIVA o Whitelisting
  - Model de seguretat NEGATIVA o Blacklisting

WAFS: State-of-the-art

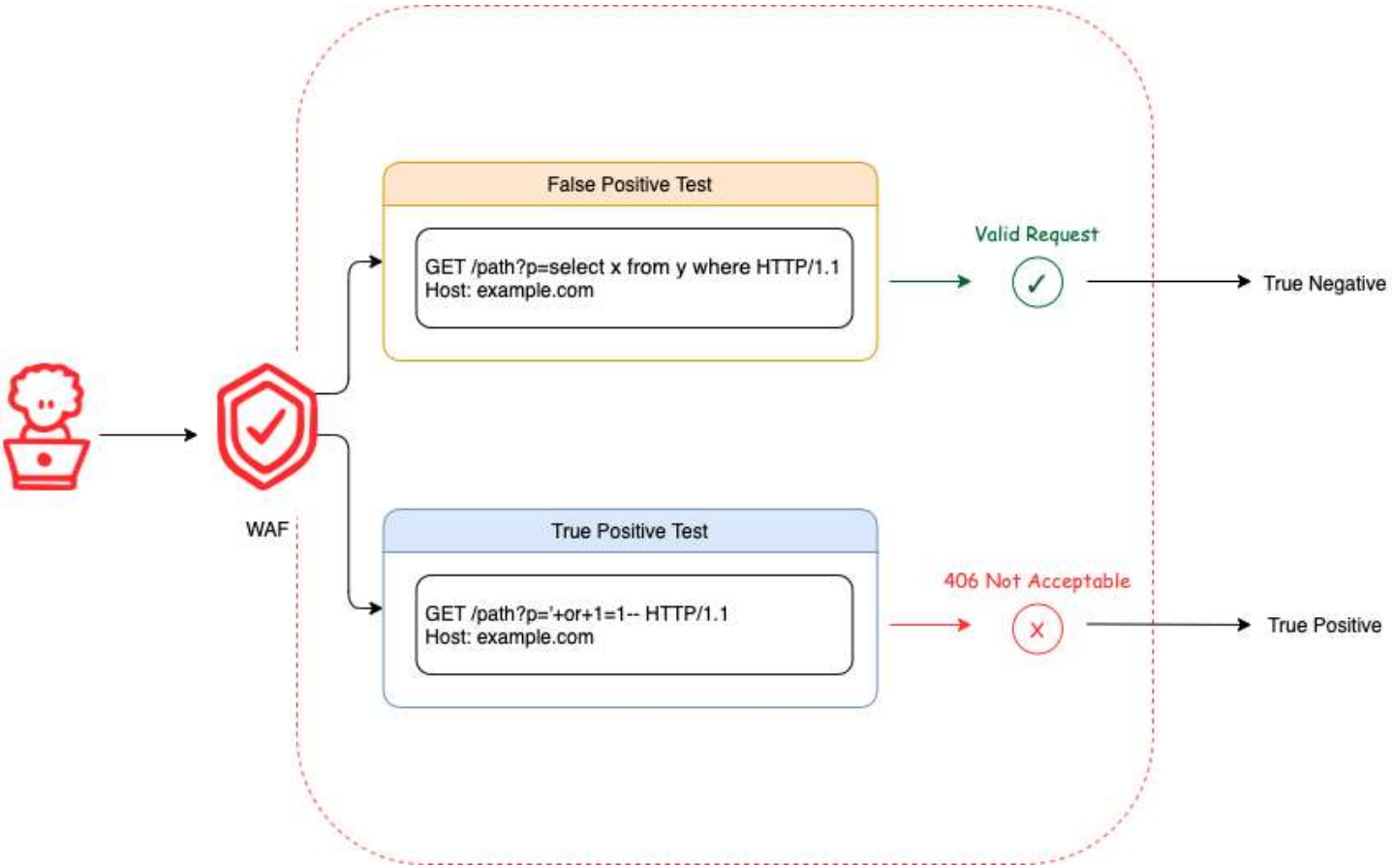
- **Modsecurity**
  - WAF per regles
  - Integració amb Webservers (Apache,Nginx,IIS)
  - Cobreix Top 10 OWASP
  - OWASP publica regles bàsiques (Core ruleset)

- **Naxsi**
  - Anti XSS & SQL injection
  - Modul per Webserver Nginx
  - WAF per regles amb whitelists
  - Corresponent a tallafocs Drop by Default

- **Coraza**
  - Desenvolupat amb Go
  - Compatible OWASP Core Ruleset
  - Cobreix Top 10 OWASP
  - Integracions, plugins amb dif. webservers

- **Open-appsec**
  - Seguretat a partir de ML
  - Cobreix Top10 OWASP
  - Atacs Zero-day (Log4J)
  - Anàlisi en 2 models ML (offline i online)

KPI's per valoració WAFS



- False positive:

Identificació correcta de peticions legítimes

- True positive:

Identificació correcta de peticions malicioses

Figura 5: Diagrama False/True Positive test (Extret de [19])

Eines Generació Injeccions SQL

WAF_COMPARISON_PROJECT

- Projecte Github amb payloads per comparar eficàcia WAFs.
- Testejar contra cada WAFs els payloads (legítims i maliciosos).
- Recol.lecta de dades respecte KPI's definits anteriorment.

MESURA EFICÀCIA:

- Qualitat de la seguretat TPR = True Positive/ (True Positive + False Negative)
- Qualitat de la detecció TNR = True Negative/ (True Negative + False Positive)
- Precisió equilibrada (Balanced Accuracy)
  Mitja aritmètica entre els valors anteriors. BA =(TPR+TNR)/2

Eines Generació Injeccions SQL

WAF_NINJA

- Eina CLI desenvolupada en Python, automatitza el penetration testing
- Payloads incorporats en l'eina
- Peticions de tipus GET I POST, aixi com ús de Cookies per pagines amb autenticació

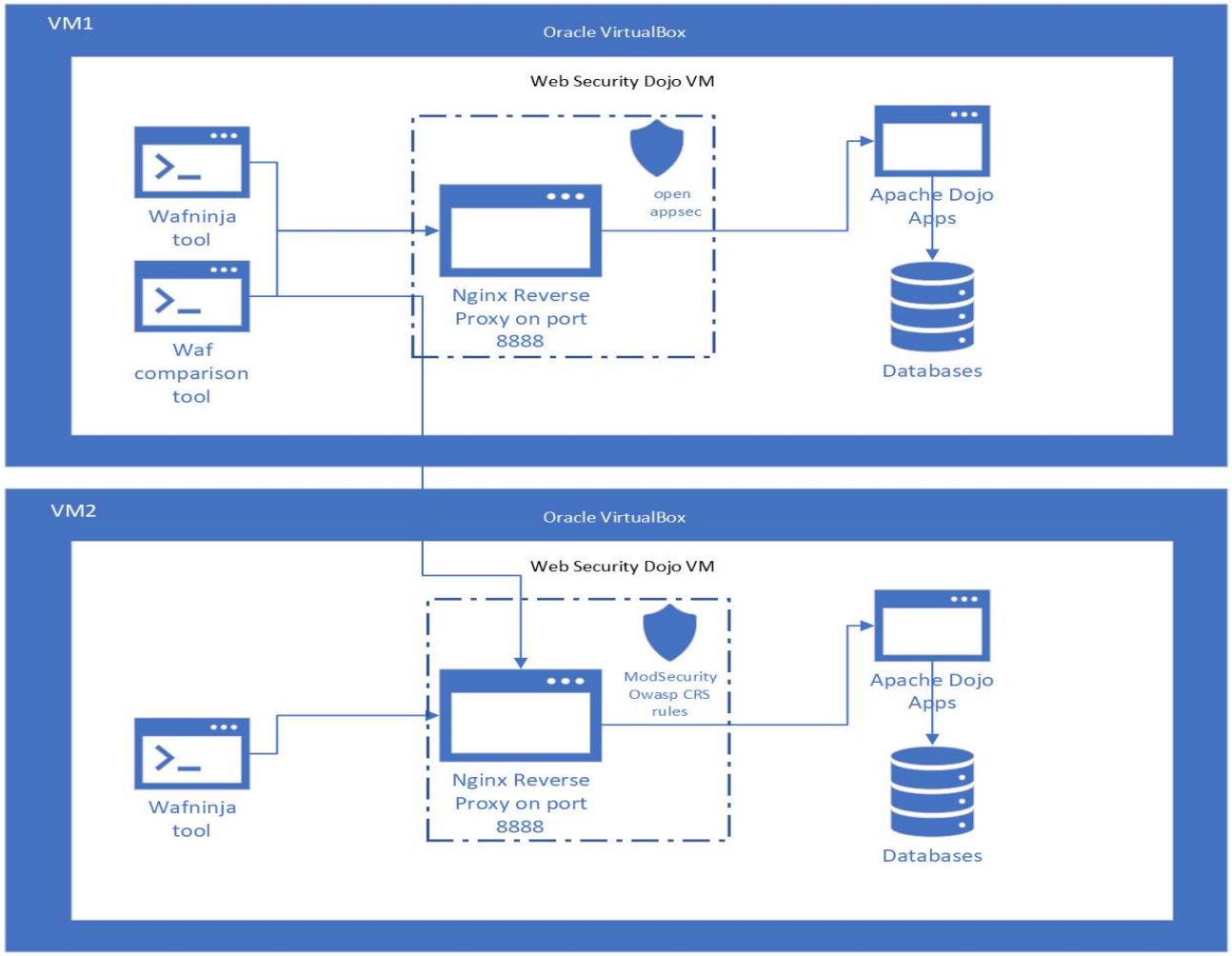
SORTIDA EXECUCIO

- Fuzz/Payload:
- HTTP Status:
- Content-Length:
- Expected (Fuzz):
- Output:
- Working:
  - Yes: No bloquejat i trobat en la resposta.
  - Probably:No bloquejat i no trobat en la resposta.
  - No: Bloquejat.

Master de Ciberseguretat i Privadesa
Seguretat Empresarial

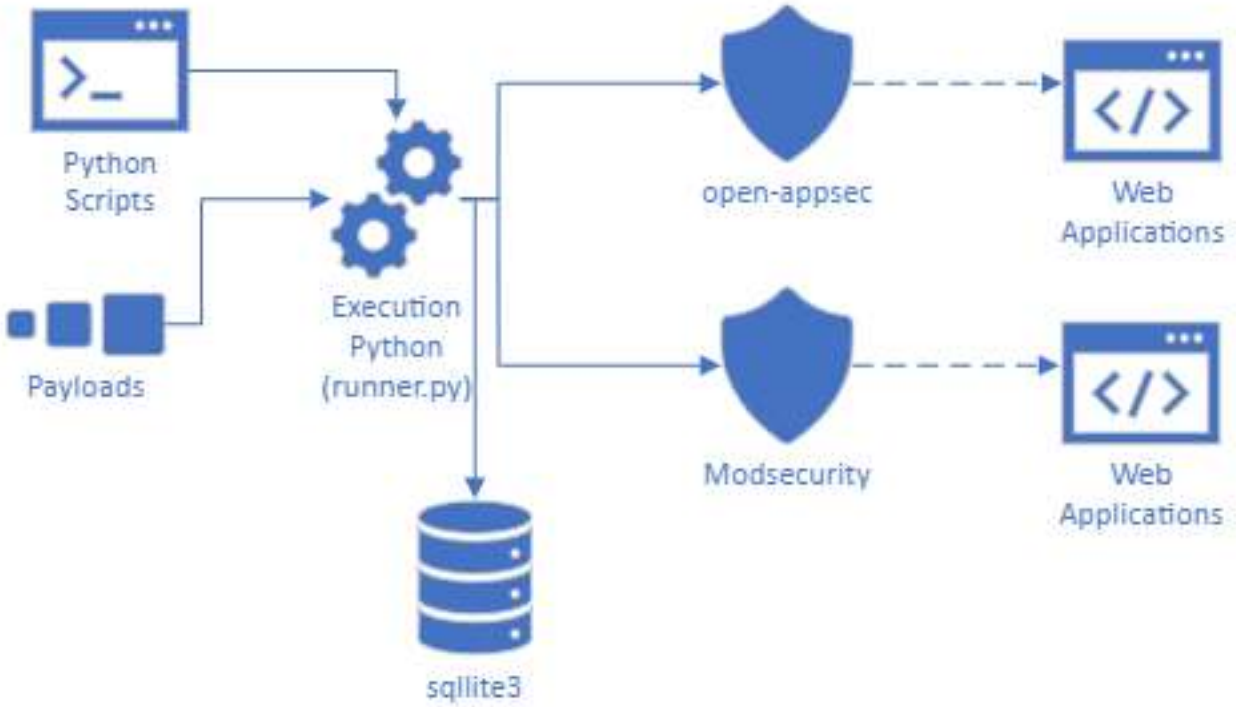
Desplegament

Arquitectura desplegada



- 2 VM's amb open project Web Security Dojo
- VM1
  - WAF open-appsec en "add-on" al reverse proxy Nginx
  - Port 8888 entrada al WAF
  - Eines SQLinjections
    - WAFninja local
    - WAF comparison project per testeig WAF local I WAF en VM2
- VM2
  - WAF Modsecurity (Libmodsecurity+connector+Nginx)
  - Port 8888 entrada al WAF
  - Eines SQLinjections
    - WAFninja local

Descripció i execució tests WAF_COMPARISON_PROJECT



- Mostra payloads de l'eina
  - HTTP lícits: 4300 payloads/peticions
  - HTTP malicioses: 916 peticions

Tipus payloads

- Generic SQL Injection Payloads
- Generic Error Based Payloads
- Generic Time Based Payloads
- Generic Union Select Payloads
- SQL Injection Auth Bypass Payloads

Descripció i execució tests WAF_NINJA

- Execució tests, a cada MV, contra el WAF corresponent
- Atac «força bruta» de payloads
- Anàlisi regles del WAF mitjançant enginyeria inversa

Descripció I execució tests manuals

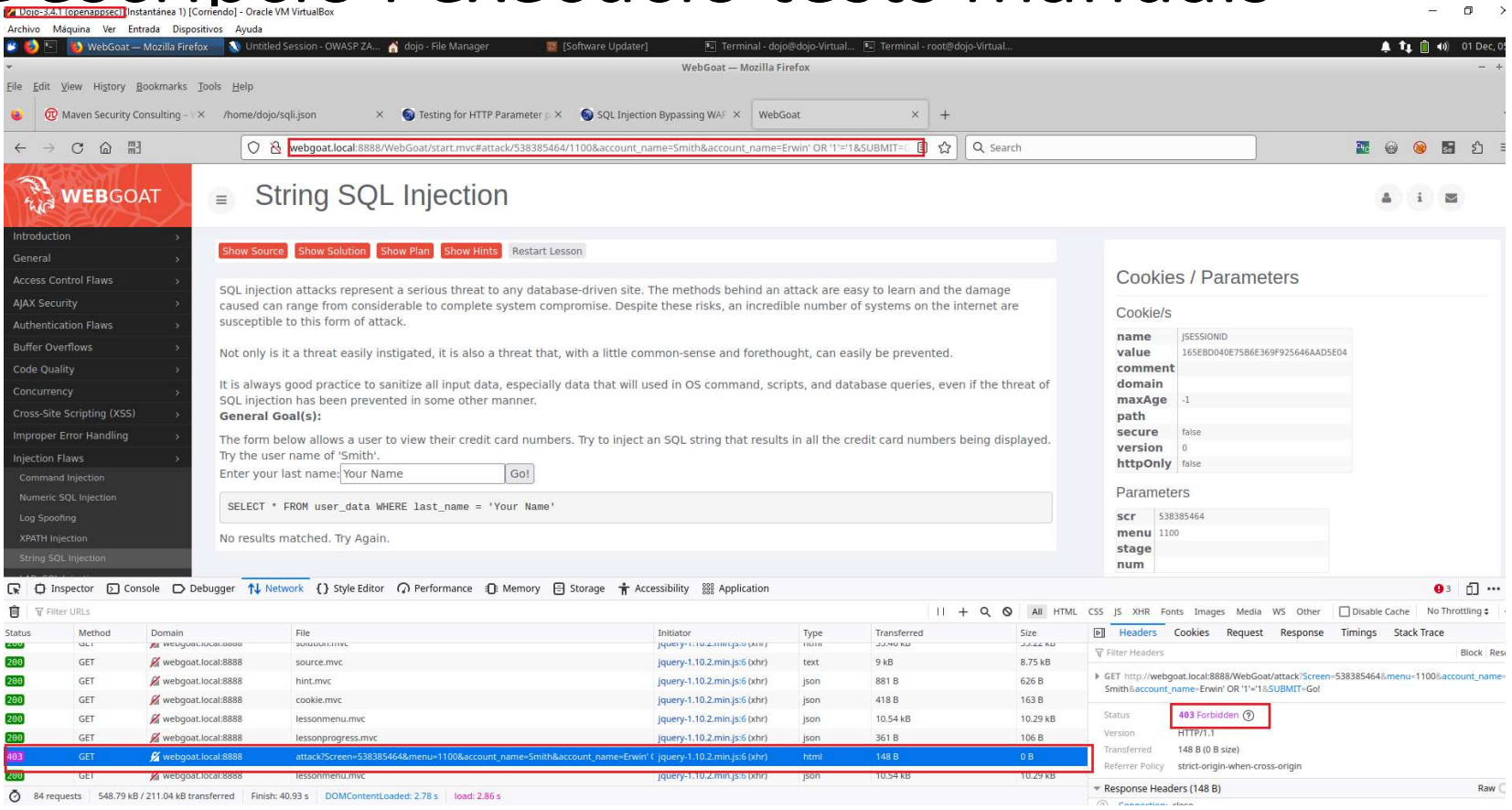
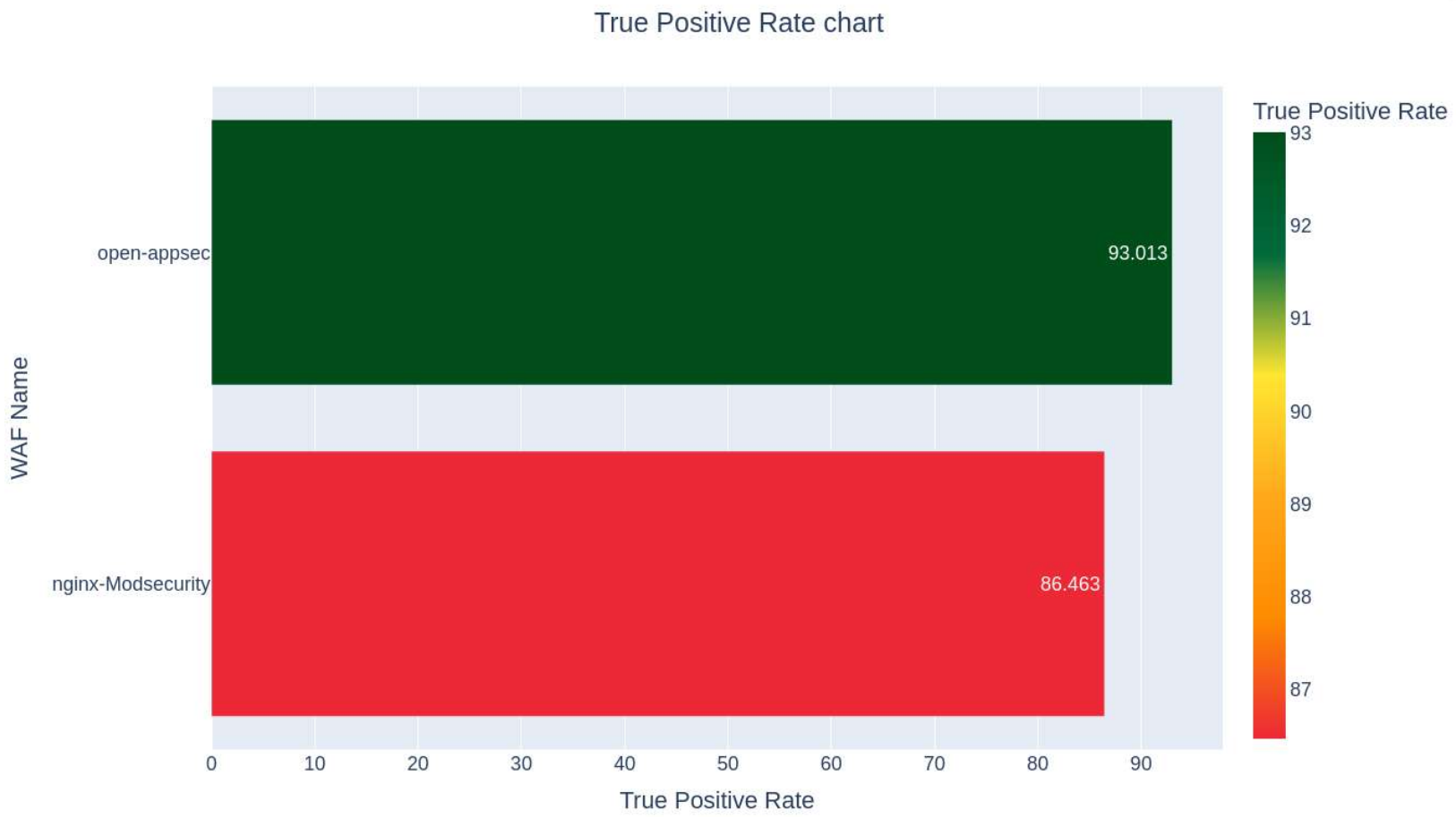


Figura 13: HTTP parameter pollution on open-appsec

Master de Ciberseguretat i Privadesa
Seguretat Empresarial

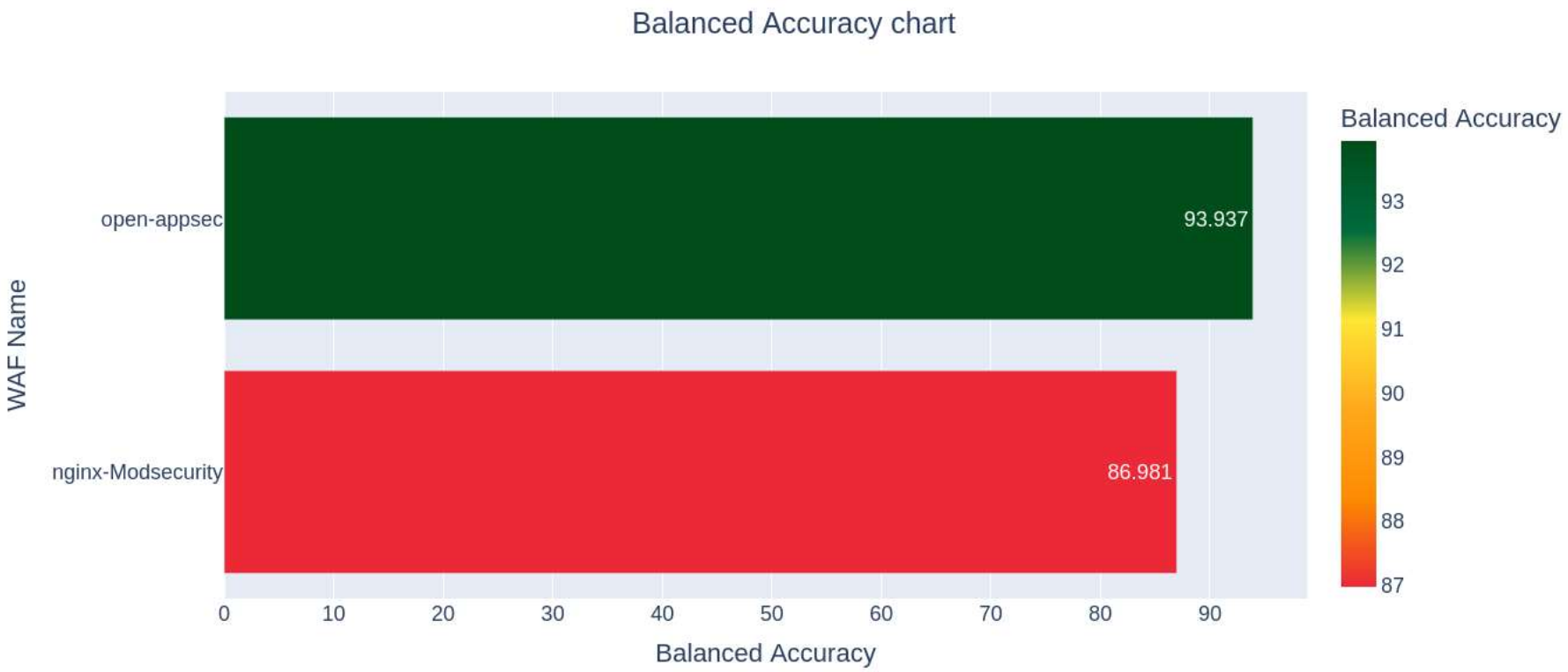
Resultats i conclusions

Resultats: WAF_COMPARISON_PROJECT



Resultats: WAF_COMPARISON_PROJECT

Resultats: WAF_COMPARISON_PROJECT



Resultats: WAF_NINJA

Fuzz	Tipus	Bypass Openappsec	Bypass Modsecurity
/*	special characters	No	No
/*--*/union/*--*/select/*--*/	inline comments	No	No
%55nion(%53elect 1,2,3)	URL encoded	Si	No
<!--	special characters	No	No
<=	special characters	No	Si
>=	special characters	No	Si
abc' --	line comments	No	No
ORDER/**/BY	inline comments	No	Si
seL/**/eCt	inline comments	No	Si
sleep(2)	Time Based	Si	No
system_user()	system functions	Si	No
uN/**/ioN	inline comments	No	Si
union all select	union statements	No	No
uNion all(sElect)	parentheses	Si	No
union distinct select	union statements	No	No
uniOn distiNct sElect	union statements	No	No
union select	union statements	No	No
uNion(sElect)	parentheses	Si	No
union/**/all/**/select	inline comments	No	Si
union/**/select	inline comments	No	Si
user()	system functions	Si	No

Conclusions

- Conclusions respecte a la realització del TFM

  - Objectius definits inicialment assolits
    - Comparativa de WAF tradicional I WAF amb ML mitjançant metriques
    - Identificats payloads que son mes habitualment bloquejats per cada WAF
  - S'ha seguit planificació I fases definides
  - Metodologia "Waterfall" utilitzada
  - Objectiu ODS Objectiu de Desenvolupament Sostenible "ODS 12 - Responsible consumption and production" realitzat amb VM's

Conclusions

- Conclusions respecte la comparativa WAFs
  - Segons mètriques definides, WAF open-appsec té un comportament **relativament millor** respecte el Modsecurity.
  - Per tipus de payload
    - Caràcters especials tipus aritmètic/comentaris bypas Modsecurity – bloqueja open-appsec
    - Payloads lógica booleana bypas Modsecurity – bloqueja open-appsec
    - Payloads amb unions i comentaris i/o URL encodings bypassen el WAF open-appsec
    - payloads amb «keywords», funcions del sistema, bypassen el WAF open-appsec
    - Payloads autenticació bloquejats per tots 2 WAFS
    - Payloads "time based" bloquejats per tots 2 WAFS
    - Tècniques "HTTP parameter pollution" bloquejats per tots 2 WAFS

Treballs futurs

- Comparar WAF's entrenant exhaustivament el model ML del WAF d'open-appsec.
- Comparar WAF's quan WAF open-appsec, en un futur, incorpori funcionalitats per limitar ratios (períodes, rang IP's...).
- Comparar WAF's amb paranoia levels superiors configurat en el WAF Modsecurity.

Agraïments

- Tutor del TFM: Manel Mendoza Flores
- Tutor del Master: Joan Josep Cabré
- Comissió avaluadora