WTF

Amichai Shulman, CTO
Yaniv Azaria, Security Research TL

Amichai Shulman – CTO Imperva

- 20 year information security veteran
- Speaker at Industry Events
  - RSA, Sybase Techwave, Info Security UK, Black Hat
- Lecturer on Info Security
  - Technion - Israel Institute of Technology
- Former security consultant to banks & financial services firms
- Leads the Application Defense Center (ADC)
  - Discovered over 20 commercial application vulnerabilities
    - Credited by Oracle, MS-SQL, IBM and others

IMPERVA®

Yaniv Azaria – Security Research TL

- Long time software and security professional
- Security research TL in Imperva's ADC
  - Credited for a number of Oracle DB vulnerabilities discovery
  - ERP database security research
  - Author of Scuba 2.0 – a free database vulnerability assessment tool
- Formerly software developer for a database security startup and web application developer

IMPERVA®

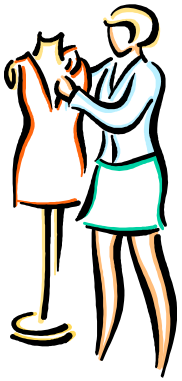
Agenda

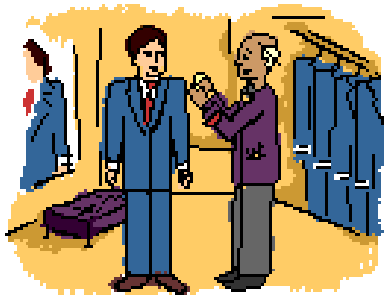
- WAF Evaluation Etat d'Affaire
  - Goals
  - Current practices (and their shortcomings)
  - What is missing
- Introducing WTF
  - Concept
  - Architecture
  - Walk Through
  - Feature Road Map
- WTF in Practice
  - Sample IPS test
  - Sample WAF test
- Summary and Conclusions

WAF Evaluation Etat d’Affaire

Goals

- Buy the right stuff
  - Feature set
  - Performance / scale
  - Quality
    - Quality = Protection
- Deploy correctly
  - Provide optimal protection to the target application
  - *The common theme among critics was that problems stemmed from customers' ineffective management practices in WAF deployment and tuning of rules**

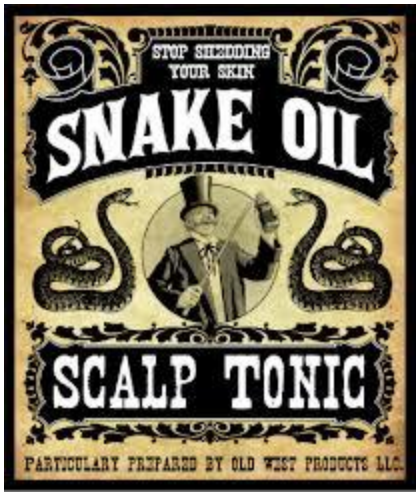


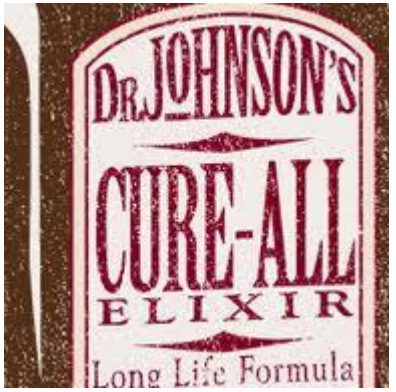


*https://securosis.com/blog/new-research-paper-pragmatic-waf-management

Current Practices (1)

- Ask the vendor!



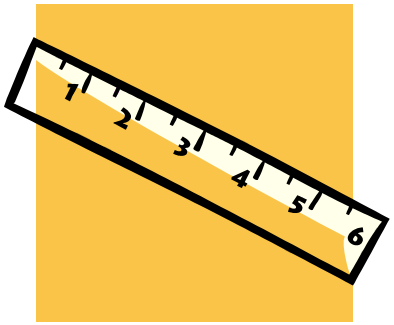


Current Practices (2)

- WAFEC
  - + An improved version of "ask the vendor"
  - + Covers the "feature set" aspect to some extent

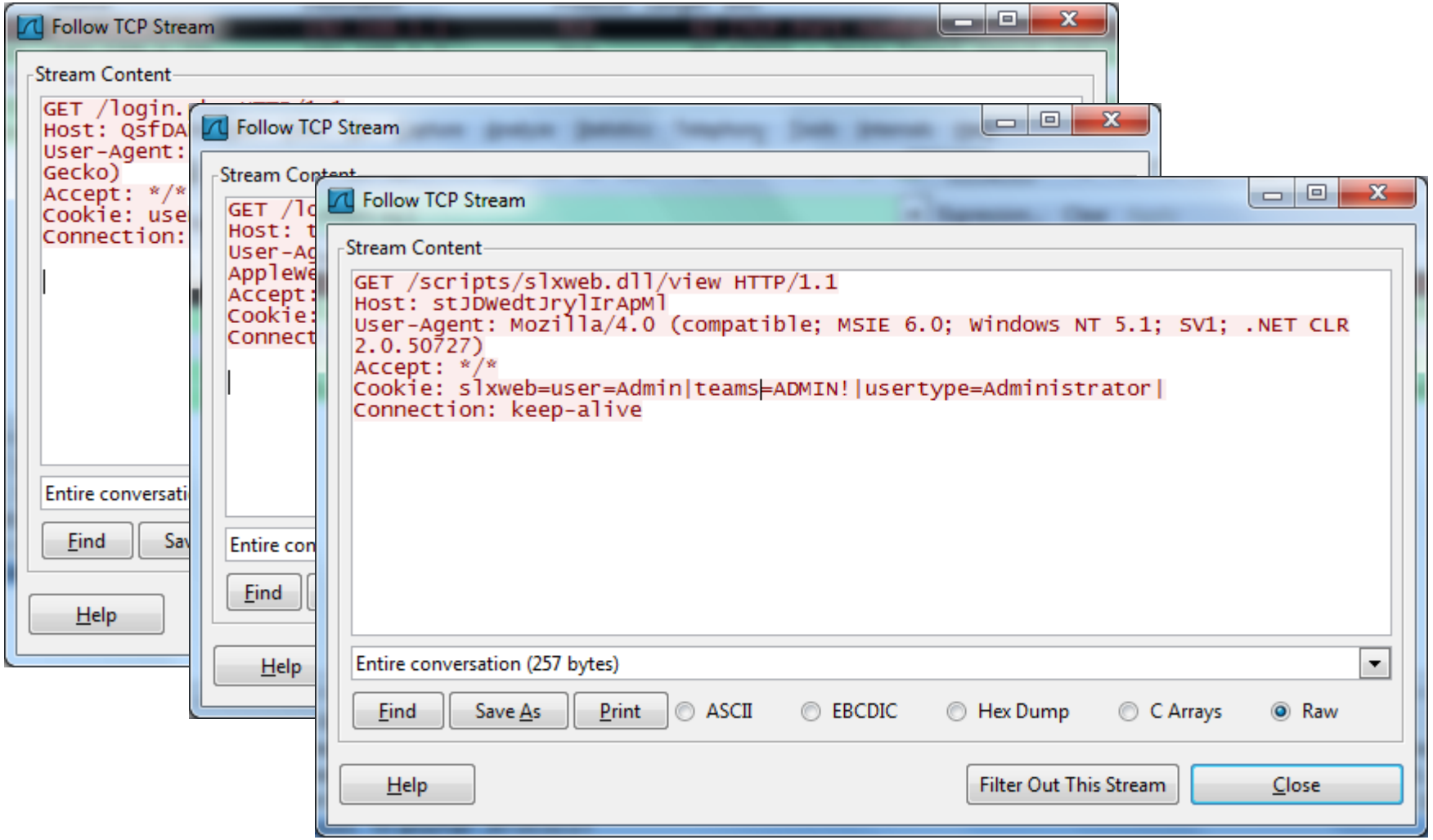
Current Practices (3)

- Security benchmarking products
  - Examples:
    - IXIA BreakingPoint
    - Spirent Studio Security



  - Focused on quantity and breadth rather than quality and depth
    - Many protocols
    - Client and server attacks mixed
  - Exploit based rather than vulnerability based tests
  - Weak on application layer evasion techniques
  - Stateless attacks
  - Success = block all traffic!

Current Practices (3.5)



Current Practices (4)

- Web Vulnerability Scanners
  - + Painful trade-off between effort and thoroughness
  - + Success = no detected vulnerabilities
  - + Success = block all traffic

“Good WAF”

Client

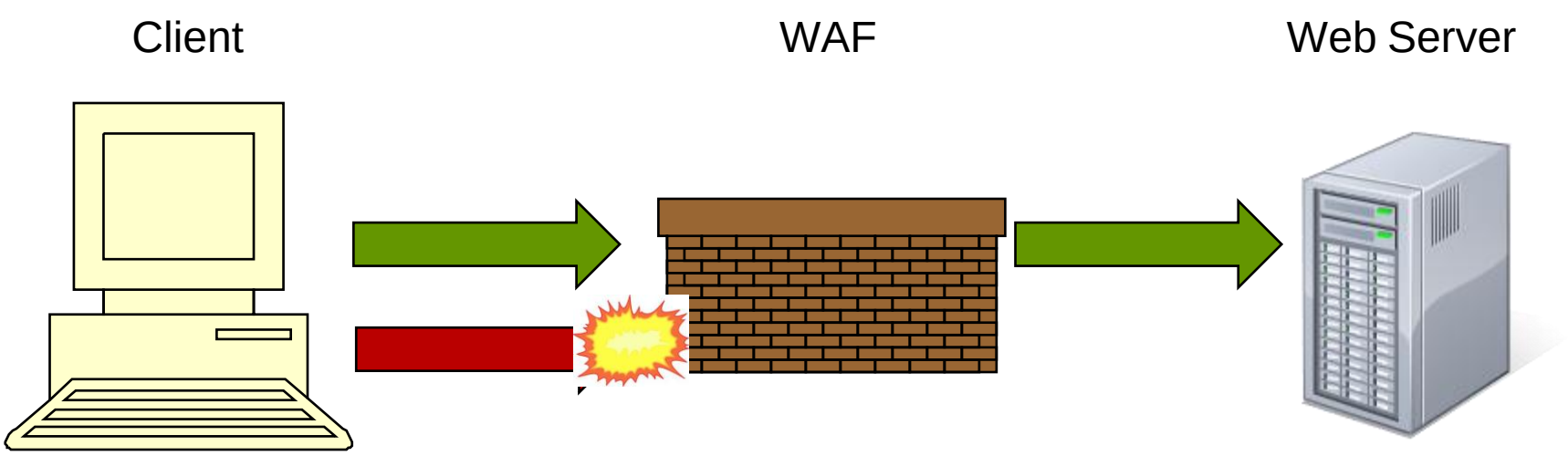
WAF

Web Server

What is Missing

- More than 75% of traffic is good traffic
- Success criteria only reflect the ability to flag some traffic as bad
  - A device that blocks all traffic would pass the test with flying colors
- A true evaluation must test the ability to distinguish between good traffic and bad traffic

Truly Good WAF



Introducing WTF

Concept

- Truly evaluate the effectiveness of a WAF
- Combine good traffic and bad traffic
- Measure two parameters
  - + Good traffic being blocked (False Positives)
    - – Use the Gutenberg project as a source for statements
  - + Bad traffic being overlooked (False Negatives)
- Provide a total understanding of the balance between security and business continuity

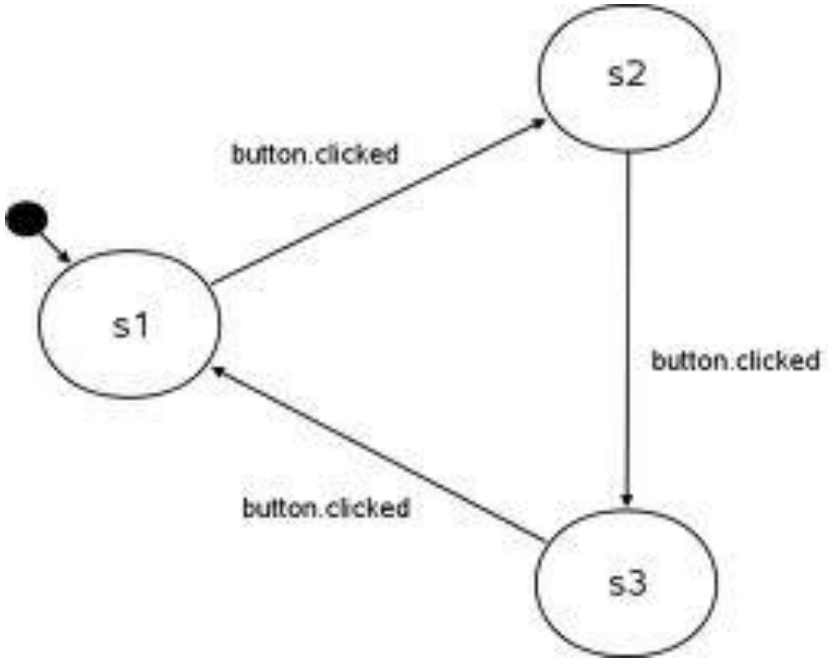
Design Goal – Simplicity

- Point-and-shoot user interface
- Bundled with a sample application
- Simple, comprehensible, reports

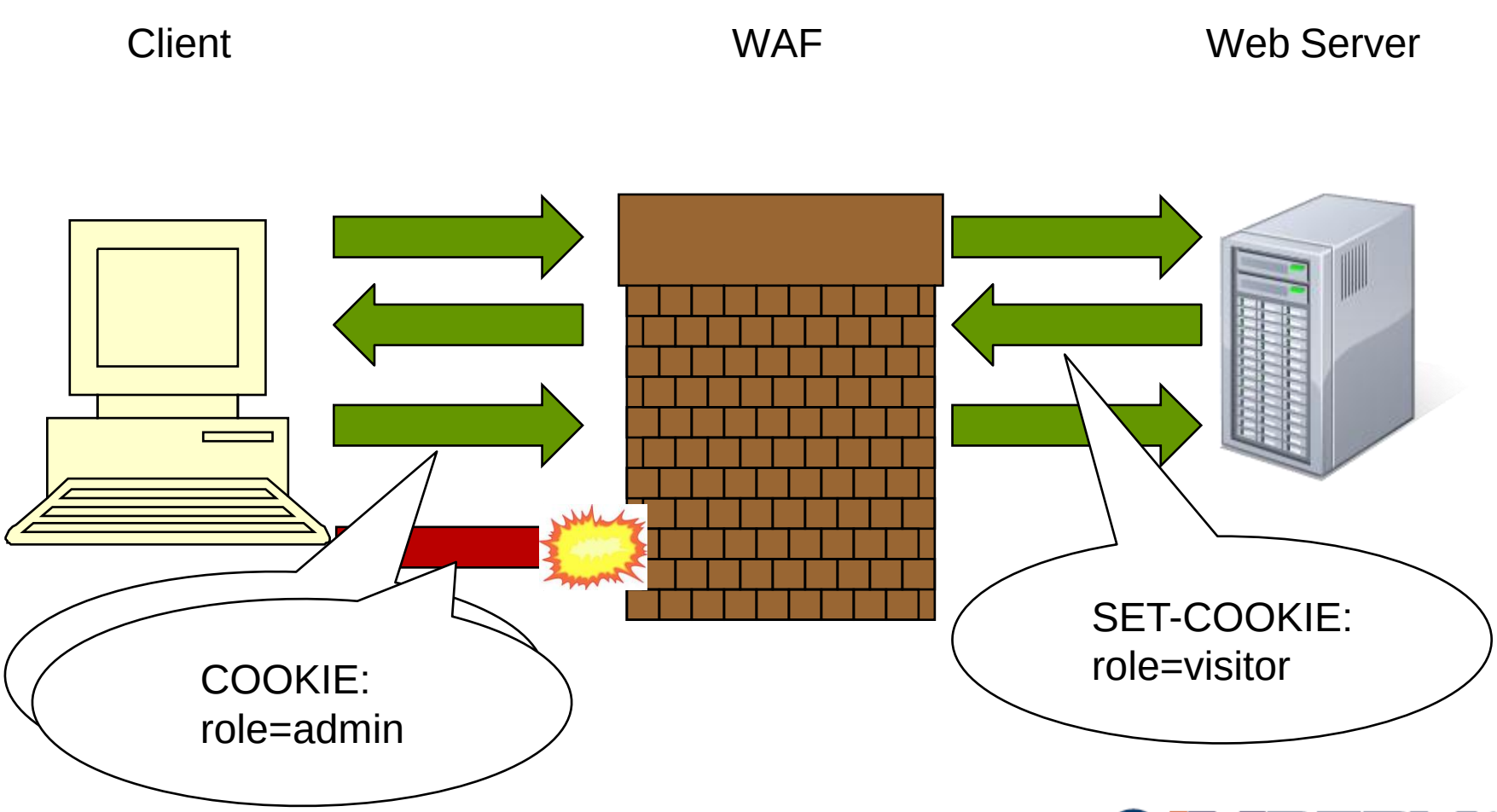
IMPERVA®

Design Goal - Completeness

- Stateful testing
  - + Cookie poisoning
  - + CSRF

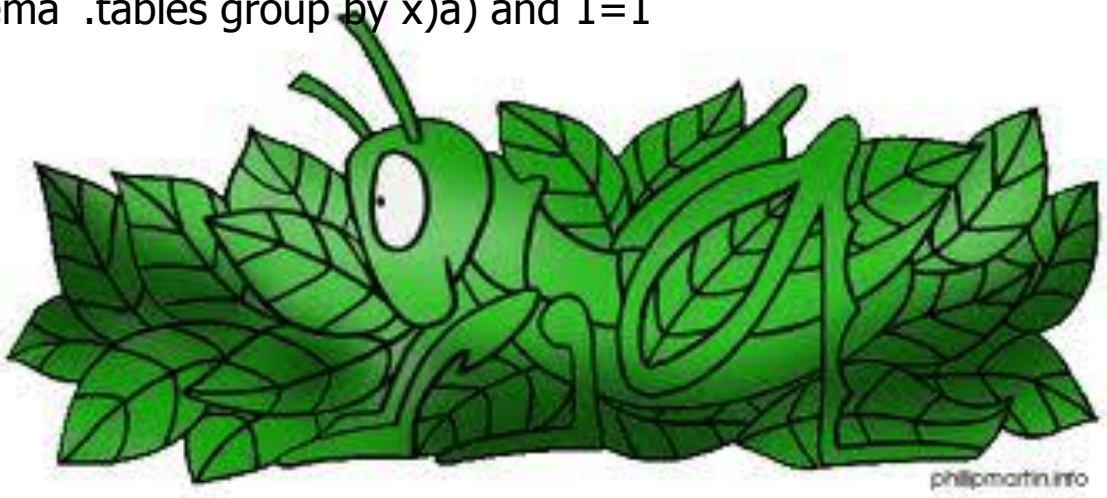


Design Goal – Completeness (Stateful Testing)



Design Goal - Completeness

- Application layer evasion techniques
  - + Parameter pollution
  - + Complex SQL queries
    - – 1 and(select 1 from(select count(*),concat((select (select (select distinct concat(0x7e,0x27,unhex(Hex(cast(table_name as char))),0x27,0x7e) from `information_schema`.tables where table_schema=0x61746D61696C limit 61,1)) from `information_schema`.tables limit 0,1),floor(rand(0)*2))x from `information_schema`.tables group by x)a) and 1=1



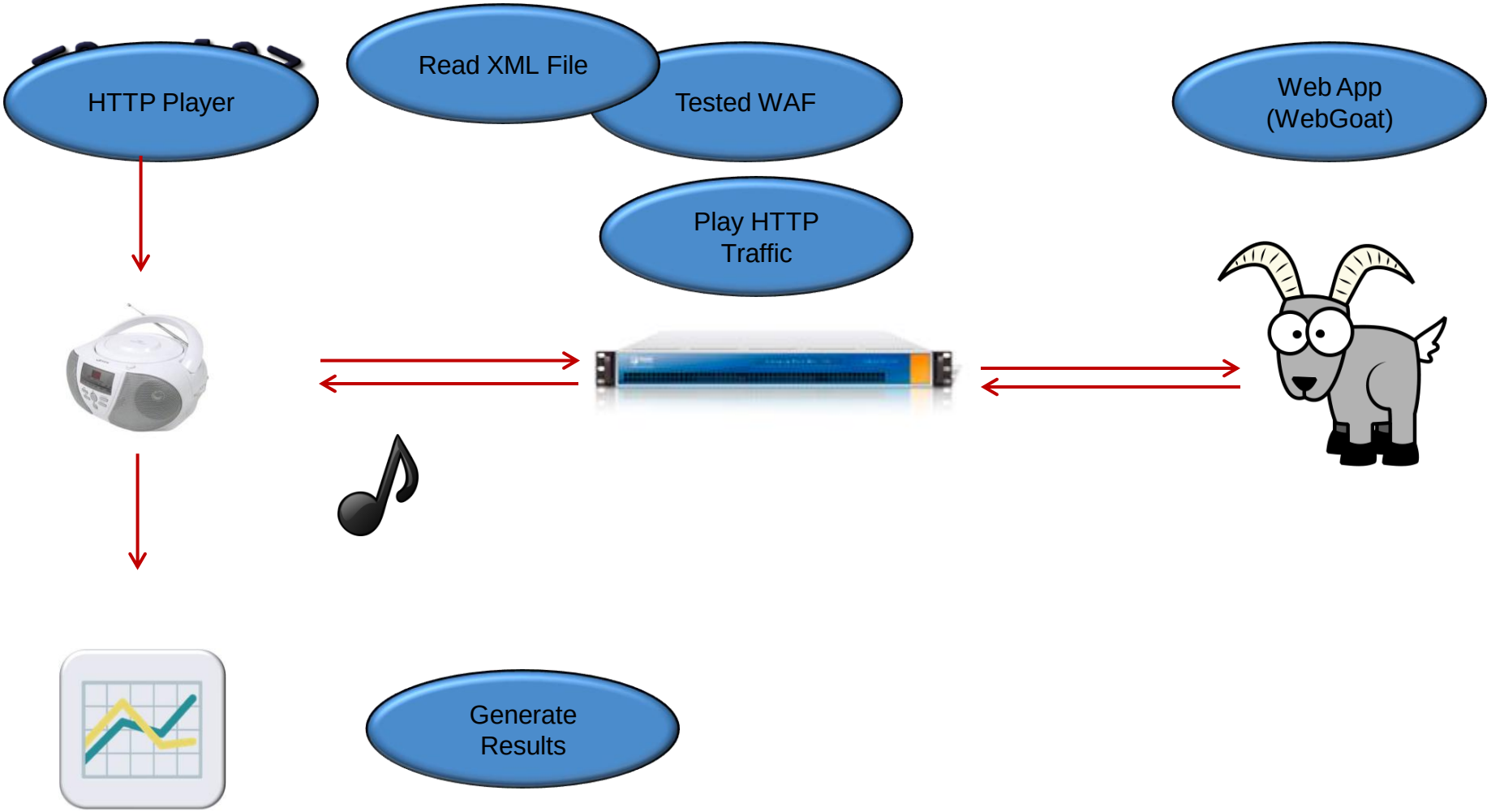
Design Goal - Flexibility

- XML based configuration file for tests
- Tests can be added / removed by selecting a different set of files
- Users can create custom tests using a text editor
- The entire set of tests can be adapted (using a text editor) to a different application

WTF – Facts Sheet

- Pure Java Application
- XML Based Test Description
- Bundled with WebGoat by OWASP
- Http Traffic generated using *Commons HTTP Client* by Apache

Tool Deployment and Workflow



IMPERVA®

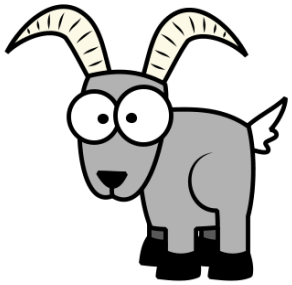
Request Evaluation – Blocked Request

HTTP Player

Http Request

Error Page

WAF Blocks Request



IMPERVA®

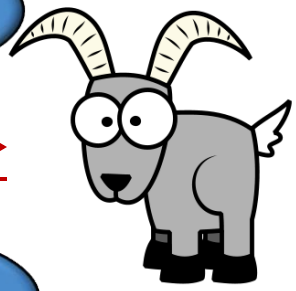
Request Evaluation – Allowed Request

HTTP Player

Http Request

WAF Allows Request

Request Sent to Application

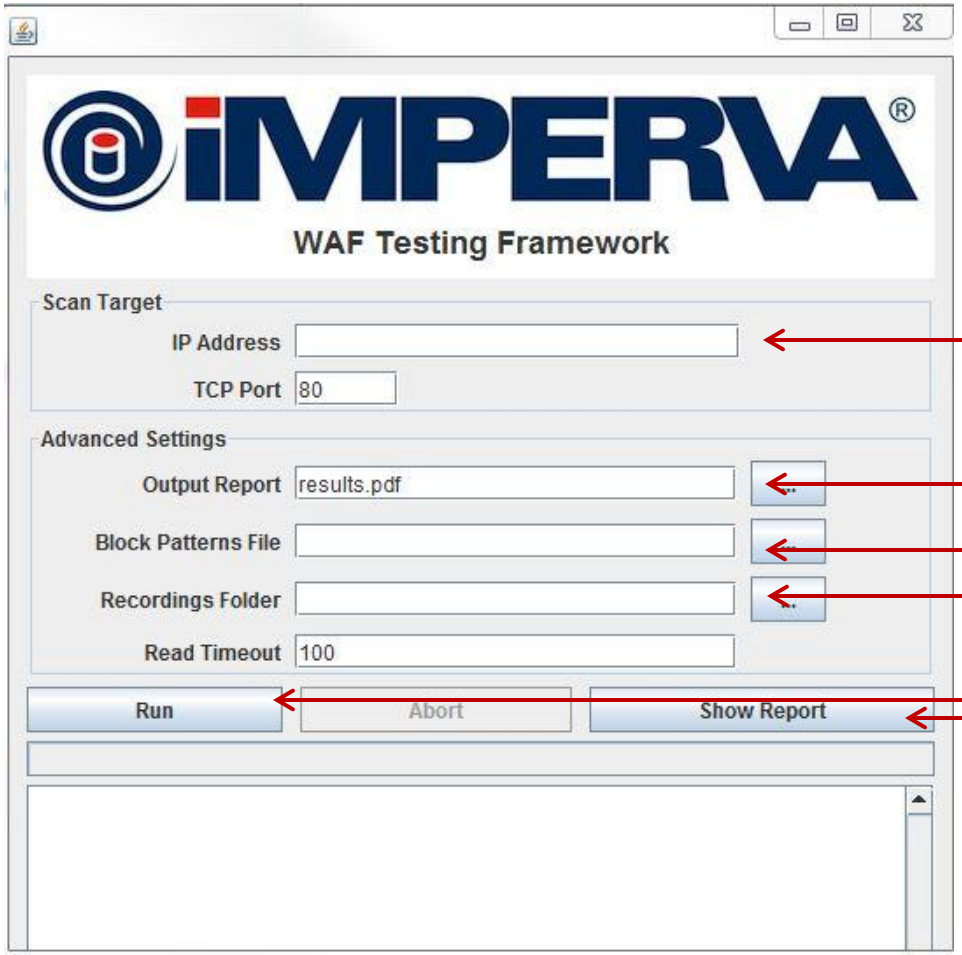


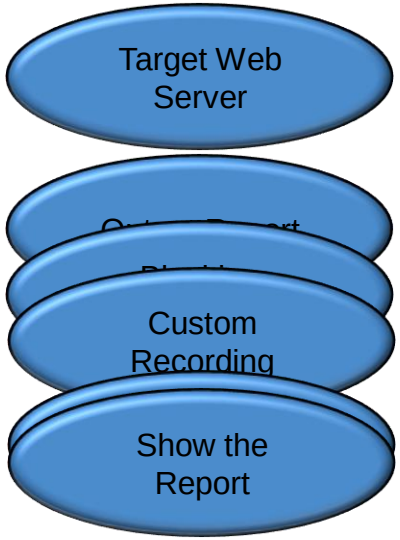
Standard Response

Standard Response

IMPERVA®

User Interface





Feature Road Map

- Generate test configuration files directly from network capture
- Add more tests
  - Both good traffic and attack traffic
  - Focus on statefulness
- Increase set of evasion techniques
  - Build on Ivan Ristic's work

WTF in Practice

Testing an IPS

- Some organizations settle for an IPS
- We tested an open source IPS
  - SNORT
  - VRT certified rules
- Further testing to include
  - Strict rules suggested by community members
  - Virtual patching examples

Testing an Open Source WAF

- Mod_Security is considered by many to be an entry level WAF
- We installed mod_security OWASP core rule set

Summary & Conclusions

Summary

- Testing WAF is important
  - Make the right choice
  - Validate deployment
- Testing methodology must consider real world constraints and scenarios
  - Most of the traffic is good
  - Attackers are using evasion techniques
  - WAF is about web application attacks

Conclusions

- WTF Rules!
  - Real world oriented
  - Easy to use
  - Extensible
- First step – release to community
  - Expected time – End of Year
  - "Closed source"
  - Test base is configurable
- Next step – release as open source

Questions?