Securing Apache with ModSec

Ronald Osure

KENET Cyber Security Training
October 26th - 30th 2015

About Apache

- The Apache HTTP Server, colloquially called Apache, is the world's most used web server software
- Apache is modular
- Apache is developed and maintained by an open community
- Usage as of June 2013, Apache was estimated to serve 54.2% of all active websites and 53.3% of the top servers across all domains

Security on Apache.. Introducing ModSecurity

- Extra security measures must be taken after initial setup
- **ModSecurity** is an open source intrusion detection and prevention engine for Web applications.

Modsecurity

- ModSecurity supplies an array of request filtering and other security features to the Apache HTTP Server, IIS and NGINX.
- ModSecurity is a web application layer firewall.
- ModSecurity is free software released under the Apache license 2.0.
- Runs as an apache server module

Modsecurity cont'

- It is a set of rules with regular expressions that helps to instantly ex-filtrate the commonly known exploits
- Modsecurity obstructs the processing of invalid data (code injection attacks) to reinforce and nourish server's security.

Advantages of Modsecurity

- No network side configuration
- Easy management.
- Free as in Beer
- HTTP intrusion detection and prevention

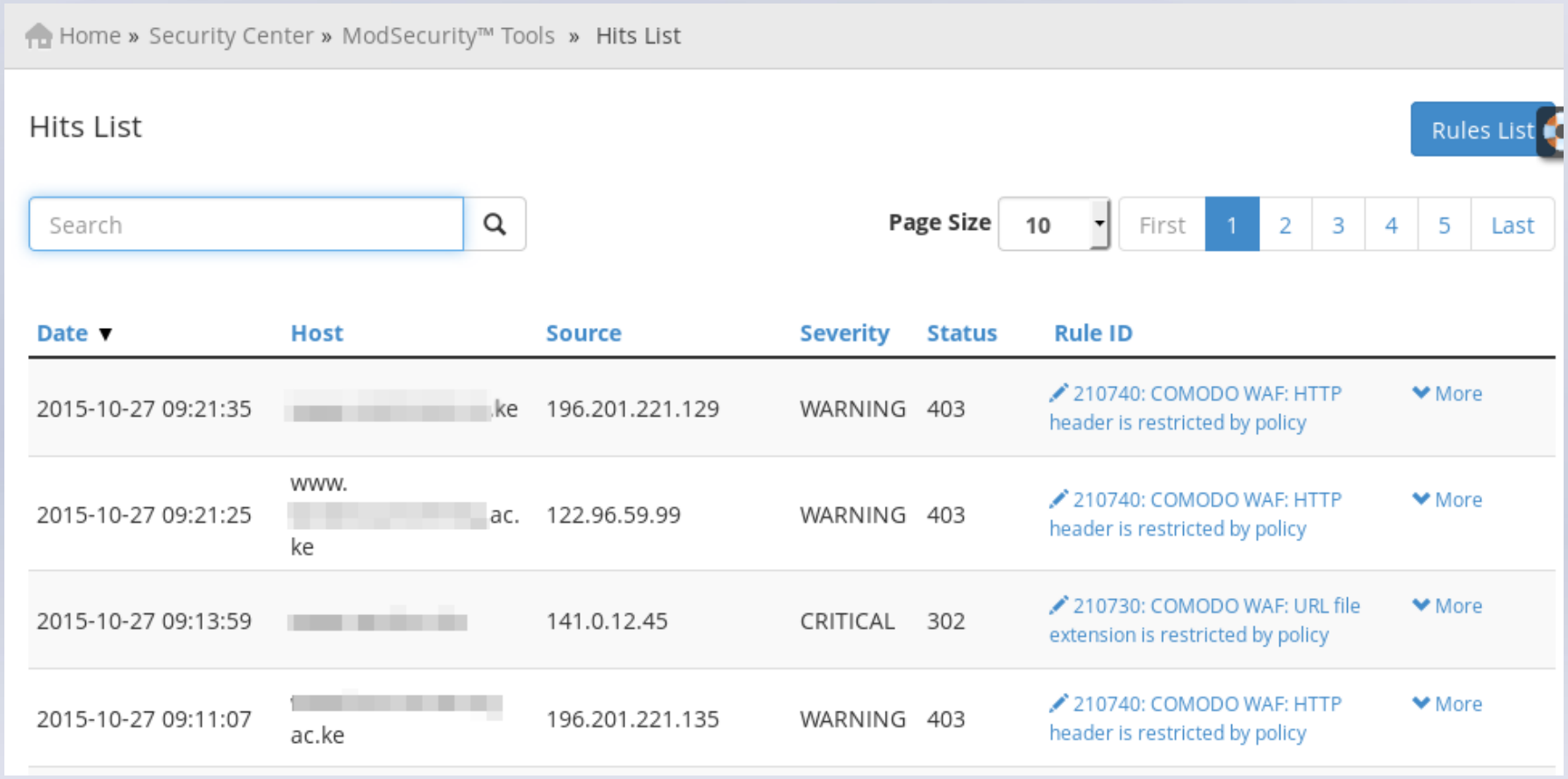
Disadvantages of Modsecurity

- Knowledge on protocols
- Manual Configurations
- Performance degradation
- Some applications might not work well e.g moodle

Modsecurity Rules

- Free updated rules from COMODO:
  https://modsecurity.comodo.com/
- You can also write your own custom rules

Modsecurity redacted grab from webserver



Home » Security Center » ModSecurity™ Tools » Hits List

Hits List

Rules List

Search

Page Size 10 First 1 2 3 4 5 Last

Date ▼	Host	Source	Severity	Status	Rule ID	
2015-10-27 09:21:35	[redacted].ke	196.201.221.129	WARNING	403	210740: COMODO WAF: HTTP header is restricted by policy	More
2015-10-27 09:21:25	www.[redacted]ac.ke	122.96.59.99	WARNING	403	210740: COMODO WAF: HTTP header is restricted by policy	More
2015-10-27 09:13:59	[redacted]	141.0.12.45	CRITICAL	302	210730: COMODO WAF: URL file extension is restricted by policy	More
2015-10-27 09:11:07	[redacted]ac.ke	196.201.221.135	WARNING	403	210740: COMODO WAF: HTTP header is restricted by policy	More

Modsecurity Reviews

On February 13, 2013, a comparative penetration testing analysis report was published by Zero Science Lab, showing that **ModSecurity** is more effective than **CloudFlare** and **Incapsula**, but it has more false positives than Incapsula.

References

- http://www.modsecurity.org/
- http://www.supportpro.com/blog/2009/08/mod_security-intro/
- http://www.inmotionhosting.com/support/website/modsecurity/what-is-modsecurity-and-why-is-it-important
- https://modsecurity.comodo.com/

QUESTIONS?

rosure@kenet.or.ke