OWASP
The Open Web Application Security Project

OWASP IL - 06/2016

PROXY BASED ASSERTION

https://www.owasp.org/index.php/Proxyassertion

[redacted]

Erez Kalman
Security Expert

[redacted]

About me

- Over a decade in the IS field
- Don’t have time to publish many articles.. Sorry..
- CISSP-ISSAP, CCSK, Certified Systems Analyst, CCSE, CCSA,….
- My creed: base your decisions on in-depth knowledge but THINK before you allow or cancel an architectural design and use security that works (effective) in terms of mitigating security risks
- I did NOT invent proxy based assertion (PBA)

OWASP IL 06/2016

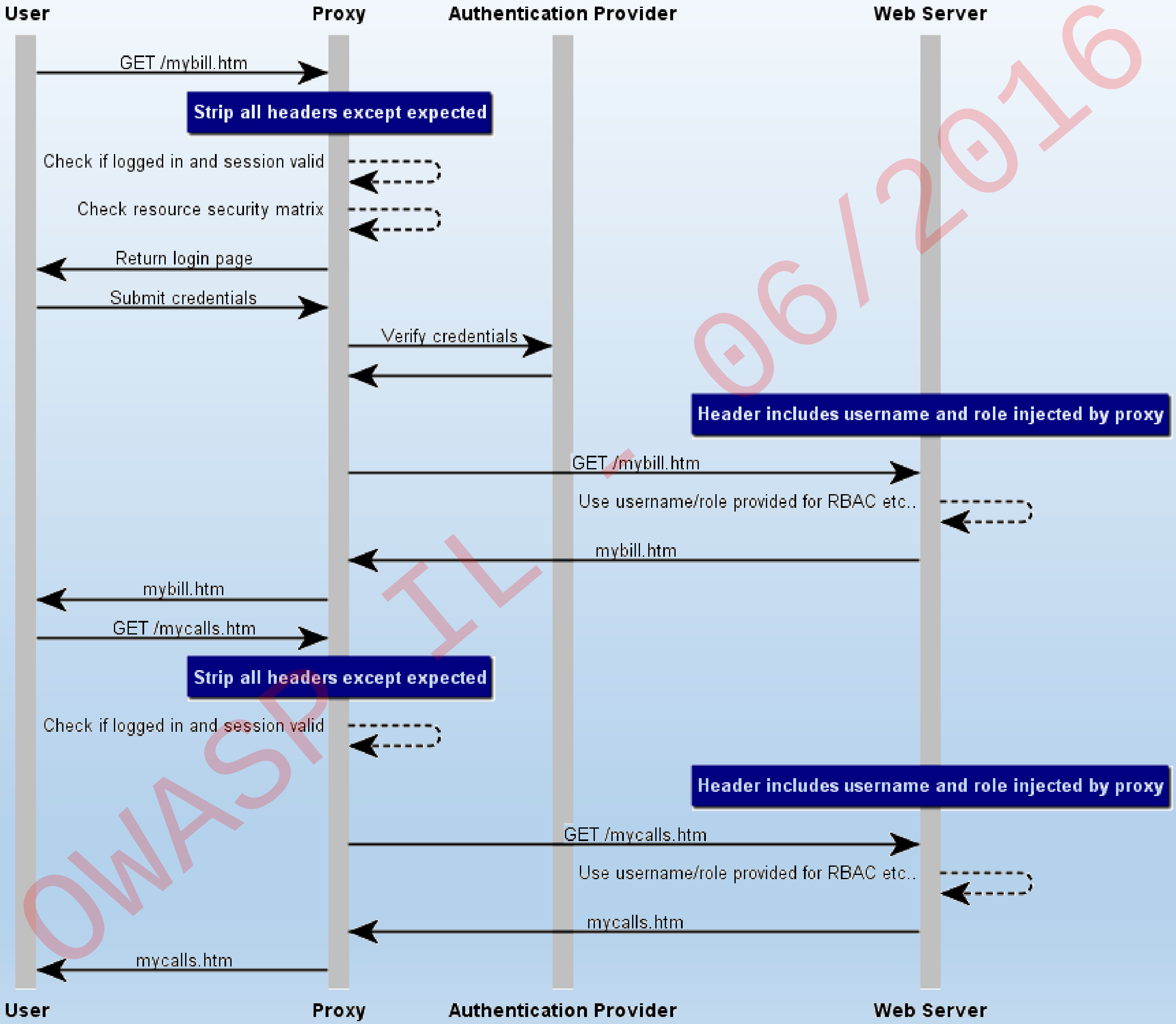
OWASP IL - 06/2016

Proxy based assertion (PBA)

- All communications traverse’s the proxy
- The proxy reads needed http headers (e.g. cookies) and strips them
- Proxy examines target permissions matrix (if needed) to conclude
  - Destination is anonymous access only
  - Destination is secure access only
  - Destination is mixed access
- For non anonymous destinations: authenticate the user, inject assertion headers (username, role/for anonymous only: anon, anon)
- Log and pass-thru to target
- Other architectural designs also possible

OWASP IL - 06/2016

PBA - Proxy Based Assertion



User

Proxy

Authentication Provider

Web Server

GET /mybill.htm

Strip all headers except expected

Check if logged in and session valid

Check resource security matrix

Return login page

Submit credentials

Verify credentials

Header includes username and role injected by proxy

GET /mybill.htm

Use username/role provided for RBAC etc..

mybill.htm

mybill.htm

GET /mycalls.htm

Strip all headers except expected

Check if logged in and session valid

Header includes username and role injected by proxy

GET /mycalls.htm

Use username/role provided for RBAC etc..

mycalls.htm

mycalls.htm

User

Proxy

Authentication Provider

Web Server

OWASP IL - 06/2016

Headers from client

- **GET** http://www.areyoureallyreadingthis.com/mybill.htm HTTP/1.1
- Host: www.areyoureallyreadingthis.com
- Proxy-Connection: keep-alive
- User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate, sdch
- Accept-Language: en,he;q=0.8
- Cookie: ses=5sdfg199sdfghsvb4fg548fgh02; SID=YAP838OHjhjkgb7M3znWLsp6XbWRm3h-U6WFA9flGjDXhP5-zgJ6hUVQ
- ASSRT: U=Alice; R=CSR

OWASP IL 06/2016

Proxy action on GET

- **GET** http://www.areyoureallyreadingthis.com/mybill.htm HTTP/1.1
- ~~Host: www.areyoureallyreadingthis.com~~
- ~~Proxy-Connection: keep-alive~~
- User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate, sdch
- Accept-Language: en,he;q=0.8
- Cookie: ses=5sdfg199sdfghsvb4fg548fgh02; SID=YAP838OHjhjkgb7M3znWLsp6XbWRm3h-U6WFA9flGjDXhP5-zgJ6hUVQ
- ~~ASSRT: U=Alice; R=CSR~~

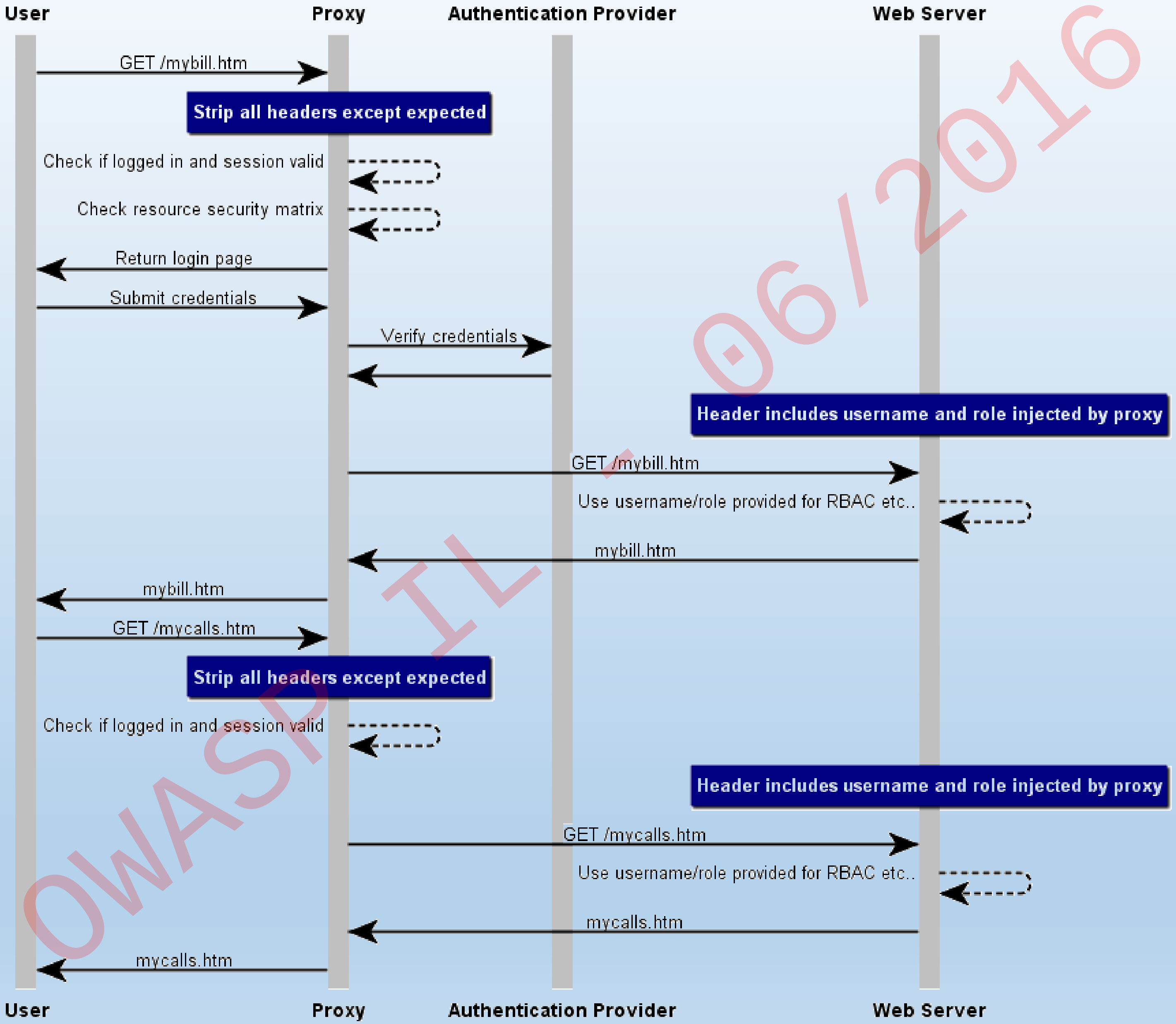
OWASP IL 06/2016

Proxy action after validation

- **GET** http://www.areyoureallyreadingthis.com/mybill.htm HTTP/1.1
- User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate, sdch
- Accept-Language: en,he;q=0.8
- Cookie: ses=5sdfg199sdfghsvb4fg548fgh02; SID=YAP838OHjhjkgb7M3znWLsp6XbWRm3h-U6WFA9flGjDXhP5-zgJ6hUVQ
- ASSRT: U=Bob; R=Customer

OWASP IL - 06/2016

PBA - Proxy Based Assertion



User

Proxy

Authentication Provider

Web Server

GET /mybill.htm

Strip all headers except expected

Check if logged in and session valid

Check resource security matrix

Return login page

Submit credentials

Verify credentials

Header includes username and role injected by proxy

GET /mybill.htm

Use username/role provided for RBAC etc..

mybill.htm

mybill.htm

GET /mycalls.htm

Strip all headers except expected

Check if logged in and session valid

Header includes username and role injected by proxy

GET /mycalls.htm

Use username/role provided for RBAC etc..

mycalls.htm

mycalls.htm

User

Proxy

Authentication Provider

Web Server

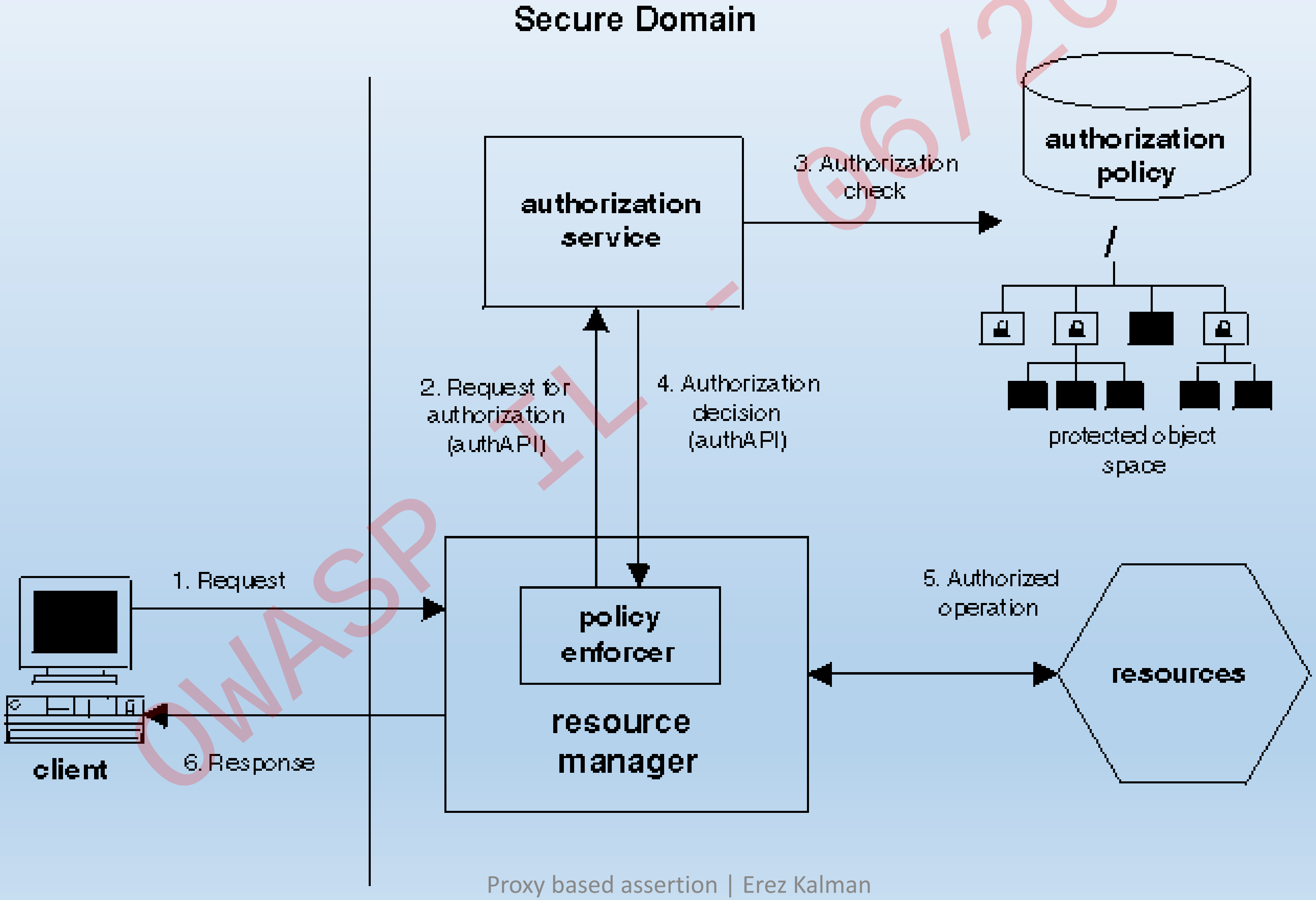
OWASP IL - 06/2016

Proxy based assertion (PBA)

- May, obviously, be used with external authority
- Can be implemented using Apache, mod_sec, mod_proxy or off-the-shelf solutions from Oracle, IBM, etc..
- Used WW by large enterprises (Telco's, Banks,…)

OWASP IL - 06/2016

IBM WebSEAL Junction



OWASP IL - 06/2016

You should still…

- Have multiple layers (defense in depth):
  - Two Firewalls (if possible, one as a bare minimum)
  - WAF
  - Change control for security components
  - SIEM
  - And more..
- OWASP top 10 & SANS 20 recommendations
- TLS 1.2 with client certificate between servers
- Have proper network, and other aspects, secure

OWASP IL - 06/2016

What if

nothing exists and we're all in somebody's *dream*?

OWASP IL - 06/2016

What if..

- The firewall is misconfigured
  - This would be a network breach, network must be properly engineered
- What if the firewall is breached
  - Use a better firewall ☺
  - Use multiple firewall’s from different vendors
- What if the proxy is breached
  - Best practices need to be in place, in any implementation, latest versions (fully patched) must be in place
  - WAF is recommended
  - Use secure repository for credentials
  - Make sure proper hardening is in place including, where possible SELinux / AppArmor
  - FIM is recommended

OWASP IL - 06/2016

What if..

- A malicious administrator performs ARP poisoning or..
  - This would be a network breach, network must be properly engineered
  - Staff hiring and fraud procedures should handle this…
- Why shouldn’t we use SAML ?
  - I am in no way suggesting SAML should not be used!
  - Not all solutions support SAML
  - Proxy can be used for SAML login and achieve SSO
  - SAML has some recurring periodic administrative overhead
  - System to system via SAML is difficult and as such one of the following is usually used
    - No authentication
    - Static username and password
    - Client certificate
    - HMAC
    - PBA is another option – support PBA and no additional method is needed

OWASP IL - 06/2016

Pro's

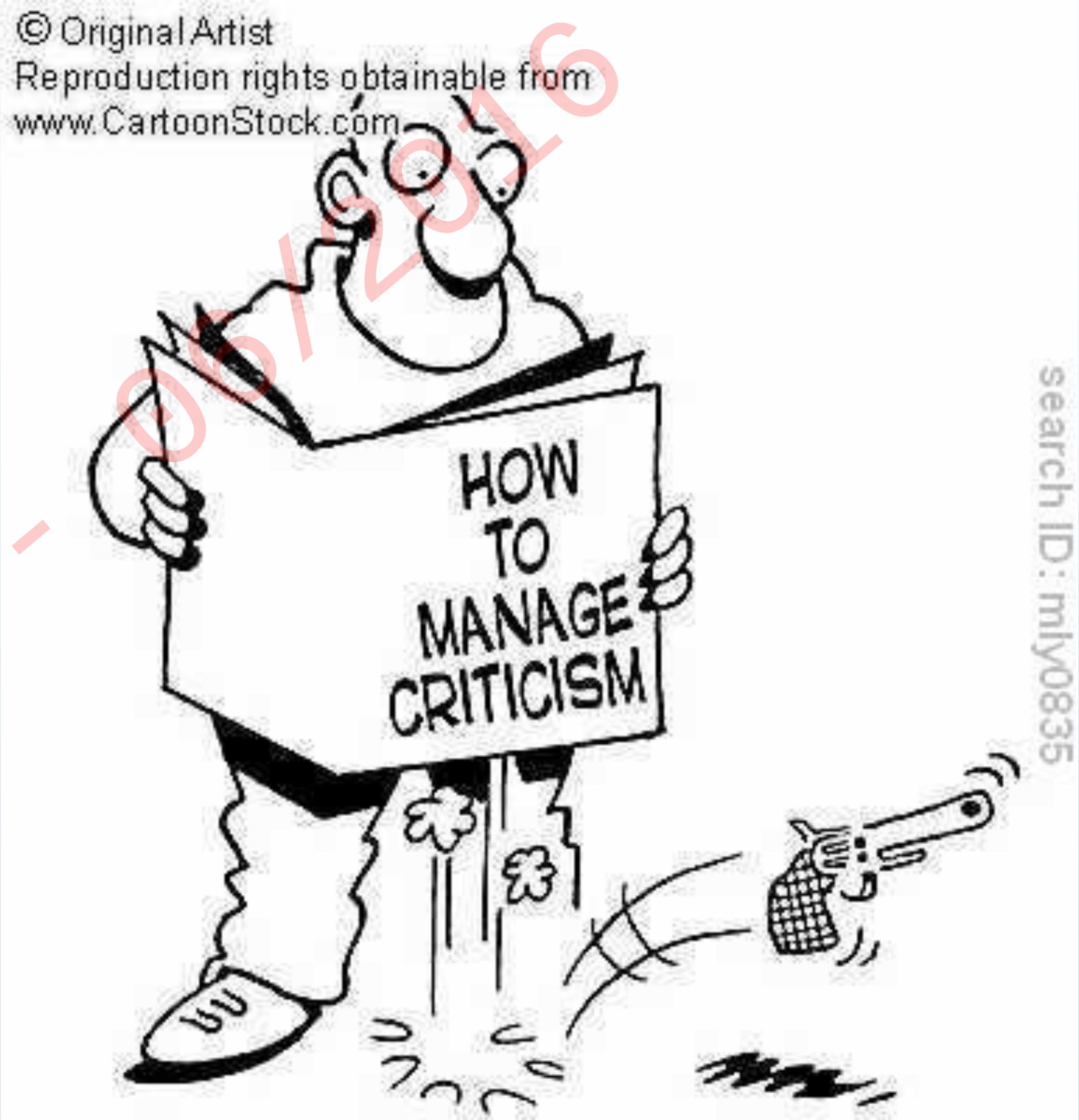
- Low CR cost
- Single management location for authentication methods
- SSO
- Single access point to DC
- Back-ends supporting SAML can continue using SAML
- No recurring periodic process required

Con's

- Not all solutions support header parsing – CR cost (usually very low)
- May open a door for malicious employee's if not properly engineered
- PBA concept is not well known as other techniques, but is widely used WW in large enterprises (banks, telco's,…)
- Proxy and backend systems must be properly secured

OW IL - 06/2016

Q & A



OWASP IL - 06/2016

תודה

Dankie Gracias

Спасибо شكراً

Merci Takk

Köszönjük Terima kasih

Grazie Dziękujemy Dėkojame

Ďakujeme Vielen Dank Paldies

Kiitos Täname teid 谢谢

Thank You

Tak

感謝您 Obrigado Teşekkür Ederiz

감사합니다

Σας ευχαριστούμε ขอบคุณ

Bedankt Děkujeme vám

ありがとうございます

Tack

OWASP IL - 06/2016