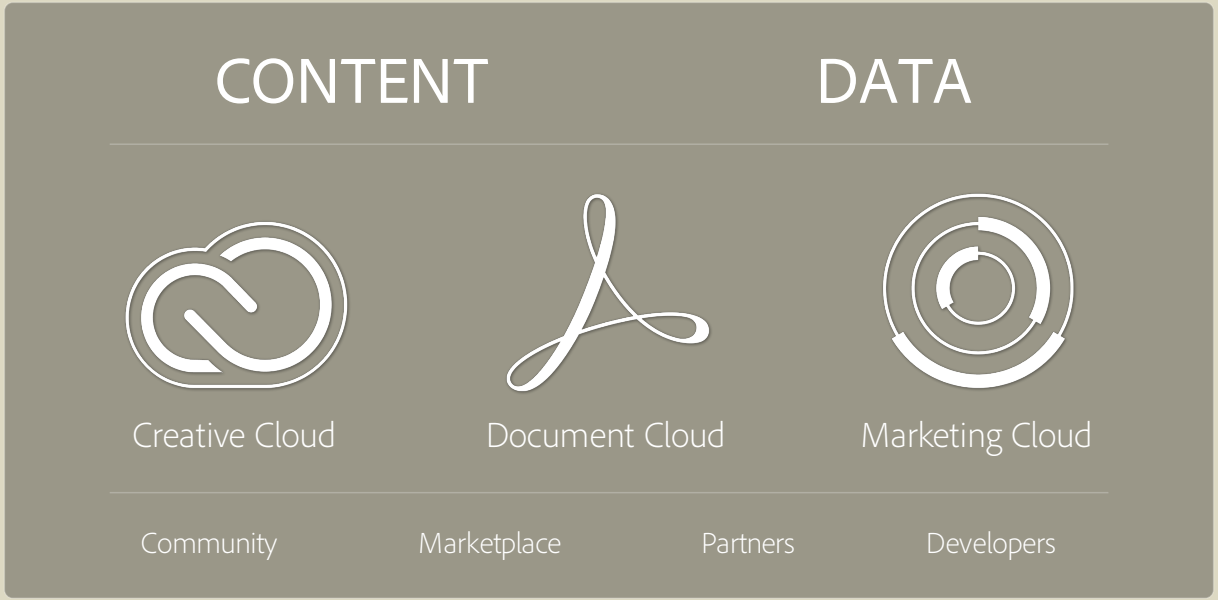
Security Automation Using ZAP

About us

- **Vaibhav Gupta**
  - Loves to be both, a defender and attacker ☺
  - Security Researcher @ Adobe (For bread, butter & beer!)
  - Delhi Chapter Leader – OWASP & Null
- **Sandeep Sigh** (Not with us today ☹)
  - Security Engineer @ ESSEL Group
  - Delhi Chapter Leader – OWASP & Null

APPSEC EUROPE

About Adobe


CONTENT
DATA
Creative Cloud
Document Cloud
Marketing Cloud
Community
Marketplace
Partners
Developers

Agenda

- What is ZAP
- Quick run through of ZAP GUI
- Understanding what can be automated
- Automating ZAP
- Few considerations/hacks
- Use cases

APPSEC EUROPE

What is ZAP

- Zed Attack Proxy
- Automated Web Application Security Scanner
- An OWASP Project
- Voted as No. 1 Security Tool as per ToolsWatch Survey

Ref: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Quick run through of ZAP GUI

- Contexts
- Request/Response
- Options
- Spider
- Scan Alerts
- Scan policy manager

Understanding what can be automated

- Configuration
- Spidering
- Passive Scan
- Active Scan
- Authentication
- Many additional capabilities ☺

APPSEC EUROPE

Automating ZAP

- ZAP APIs (http://zap/UI/)
- pip install python-owasp-zap-v2.4

- Example 1: Initializing ZAP in python
- Example 2: Spidering web application
- Example 3: Passive scanning
- Example 4: Active scanning
- Example 5: Simple authenticated scanning
- Example 6: Some other important APIs

Example 1: Initializing ZAP in python

```
from zapv2 import ZAPv2

zap = ZAPv2()
or
zap = ZAPv2(proxies={'http': 'http://x.x.x.x:yyyy',
                     'https': 'http://x.x.x.x:yyyy'})
```

APPSEC EUROPE

Example 2: Spidering web application

```
zap.spider.scan(input_target, apikey = API_Key)

while (int(zap.spider.status()) < 100):
    print 'Spider progress %: ' + zap.spider.status()
    time.sleep(2)

zap.ajaxSpider.scan(url = input_target, apikey = API_Key)
```

APPSEC EUROPE

Example 3: Passive scanning

```
zap.pscan.disable_all_scanners(apikey = API_Key)

zap.pscan.enable_scanners(ids = 10040, apikey = API_Key)

zap.pscan.enable_all_scanners(apikey = API_Key)

zap.pscan.set_enabled(enabled = True, apikey = API_Key)
```

Ref: http://zap/UI/pscan/view/scanners/

Example 4: Active scanning

```
zap.ascan.scan(target, apikey = API_Key)

while (int(zap.ascan.status()) < 100):
    print 'Scan progress %: ' + zap.ascan.status()

zap.ascan.scan(input_target, scanpolicyname =
input_policy, apikey = API_Key)
```

APPSEC EUROPE

Example 5: Simple authenticated scanning

```
zap.ascan.scan_as_user(url = input_target, contextid = 1,
userid = 4, apikey = API_Key)
```

- http://zap/UI/context/view/context/
- http://zap/UI/users/view/usersList/

Example 6: Some other important APIs

- http://zap/UI/spider/action/setOptionMaxDepth/
- http://zap/UI/context/action/importContext/
- http://zap/UI/context/action/includeInContext/
- http://zap/UI/context/action/newContext/
- http://zap/UI/core/other/xmlreport/
- http://zap/UI/core/action/shutdown/

Few considerations/hacks

- Ajax spidering
- Importing contexts/configs
- Random sleeps
- Scan output for a particular context/scan
- Documentation
- Custom scripting!

APPSEC EUROPE

Lets Discuss few Use Cases

- Scanning at scale
- Integration with CI/CD systems like Jenkins
- Custom authentication
- Unit security test cases
- Research at scale!
- The list is endless… ☺

ZAP Resources

- Getting Started Guide (pdf) - an introductory guide
- Tutorial Videos
- User Guide - online version of the ZAP's user guide
- User Group - ask questions about using ZAP
- Add-ons - help for the optional add-ons you can install
- StackOverflow - because some people use this for everything ;-)

Thank you! ☺

Vaibhav Gupta
Vaibhav.Gupta@owasp.org
Twitter: @VaibhavGupta_1
Blog: www.exploits.work

Security portal: https://www.adobe.com/security
Security @Adobe blog: https://blogs.adobe.com/security
Twitter: @AdobeSecurity

APPSEC EUROPE