SECURITY AUTOMATION IN CI PIPELINE

Hello

I am Abdo

@n3tg33k

AGENDA

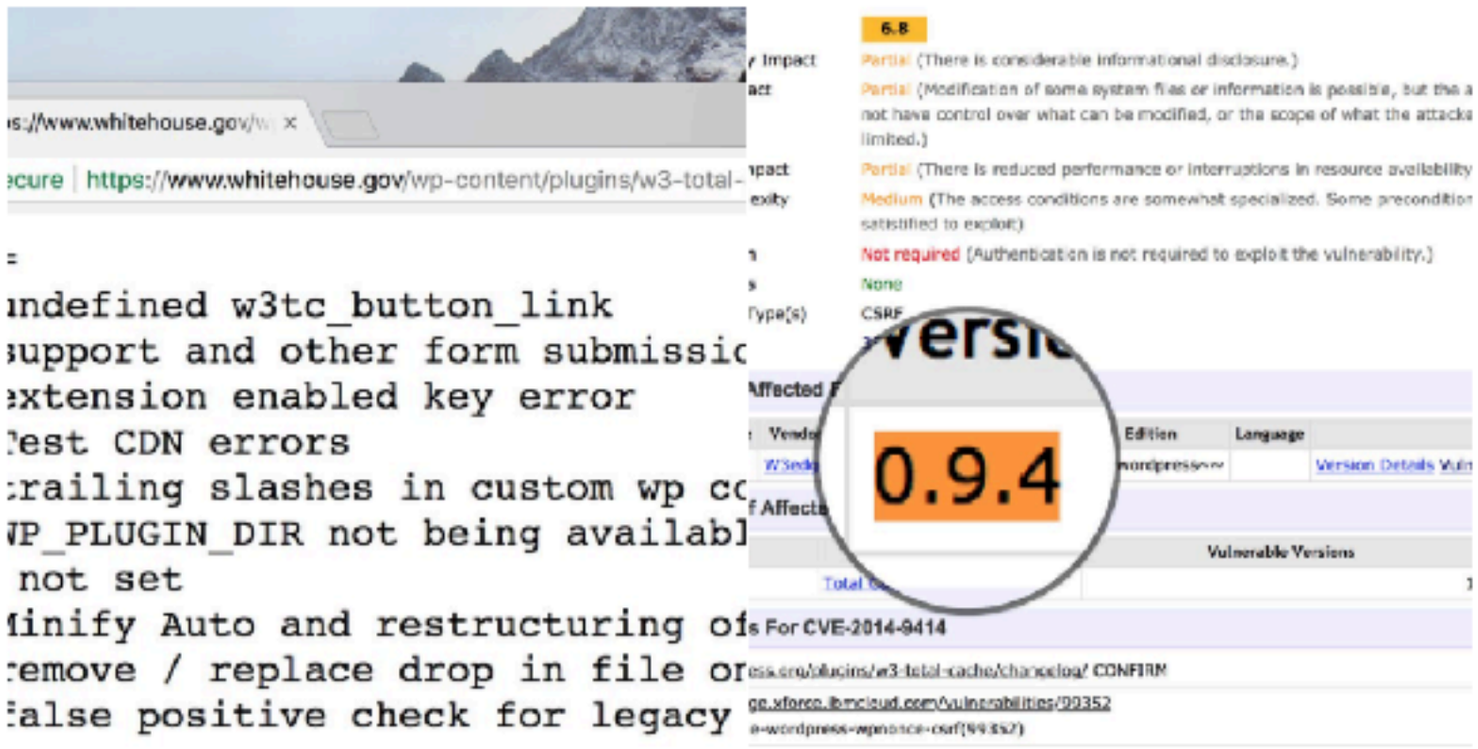
- The concepts and culture
- What is the best practice?
- How can we make the most out of it
- An implementation example

Zack Whittaker
@zackwhittaker

Following

Oh no... the White House is running outdated WordPress plugins with known vulnerabilities.... I'd better alert the authorities...

"guys your website is vuLNerabLe k thx bye"



8:09 AM - 8 Mar 2018

24 Retweets **36** Likes

4 24 36

THE LINGO?

Security

DevOps

SecOps

DevSecOps

Continuous Delivery

Continuous Integration

Continuous Security

Continuous Intrusion

*OPS

Agile

Continuous

Development

DevSecOps

Security

Operation

Development Team

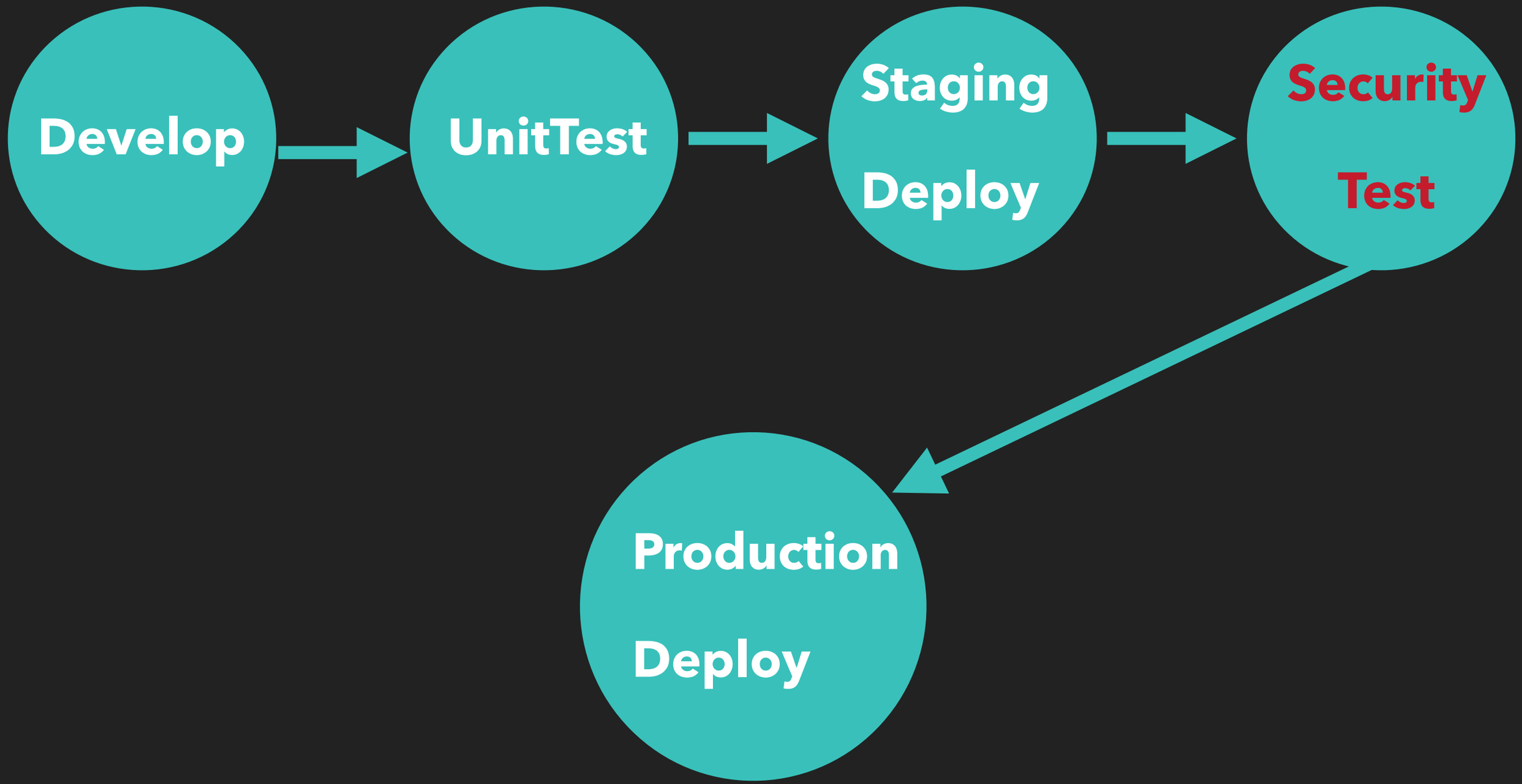
Security Team

https://goo.gl/bwMcef


ONE DOES NOT SIMPLY
ACHIEVE DEVSECOPS NIRVANA
imgflip.com

WE SHOULD...

- **Break stuff in early stages**
- **Use already made DevOps infrastructure**
- **Integrate with developers tools (Issue trackers)**

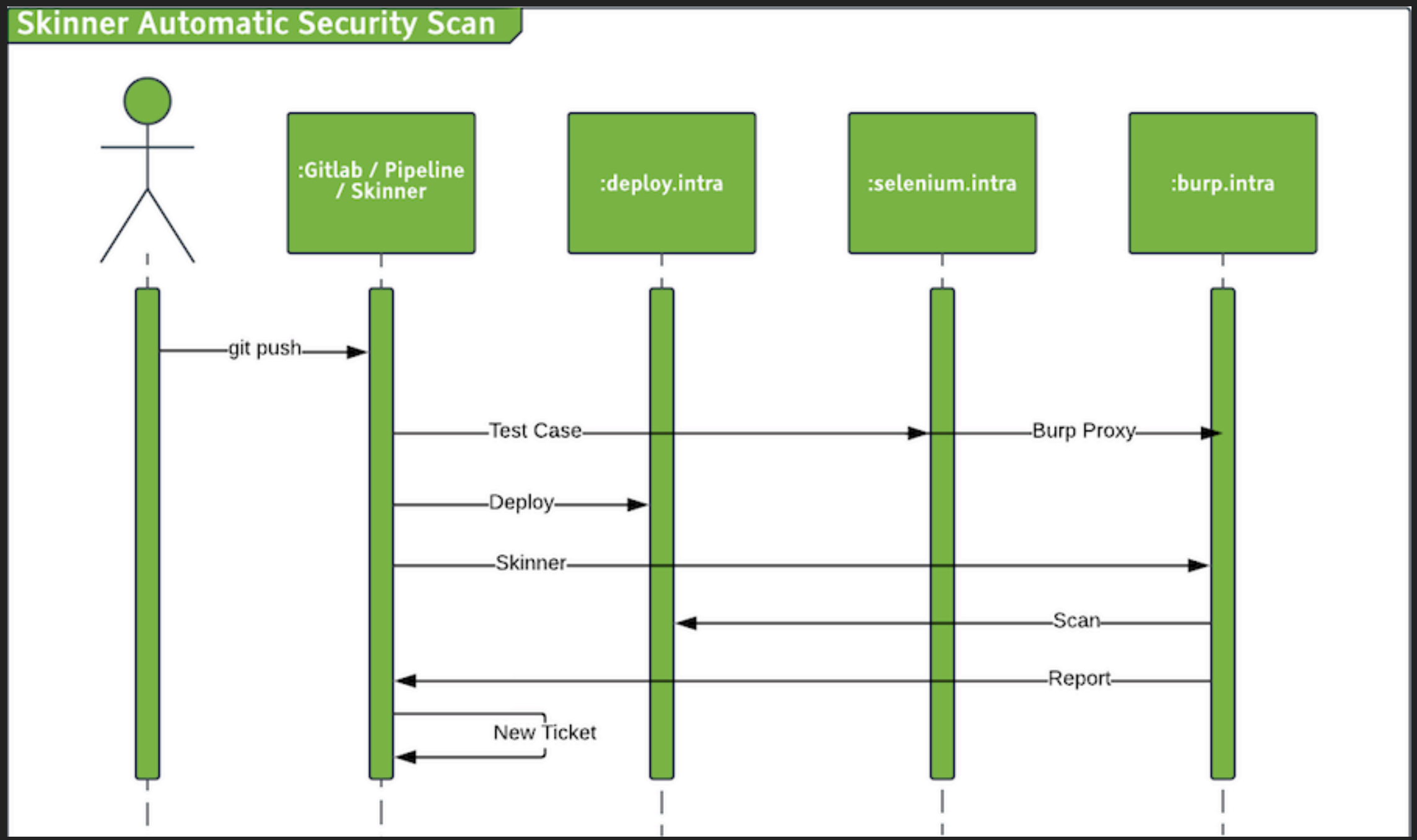

Develop
UnitTest
Staging
Deploy
Security
Test
Production
Deploy

RUN THE TEST

MAKE DECISION

REPORT

FIX


Skinner Automatic Security Scan
:Gitlab / Pipeline / Skinner
:deploy.intra
:selenium.intra
:burp.intra
git push
Test Case
Burp Proxy
Deploy
Skinner
Scan
Report
New Ticket

THE NEVERHOOD

https://www.youtube.com/watch?v=5fYzq4OELhI

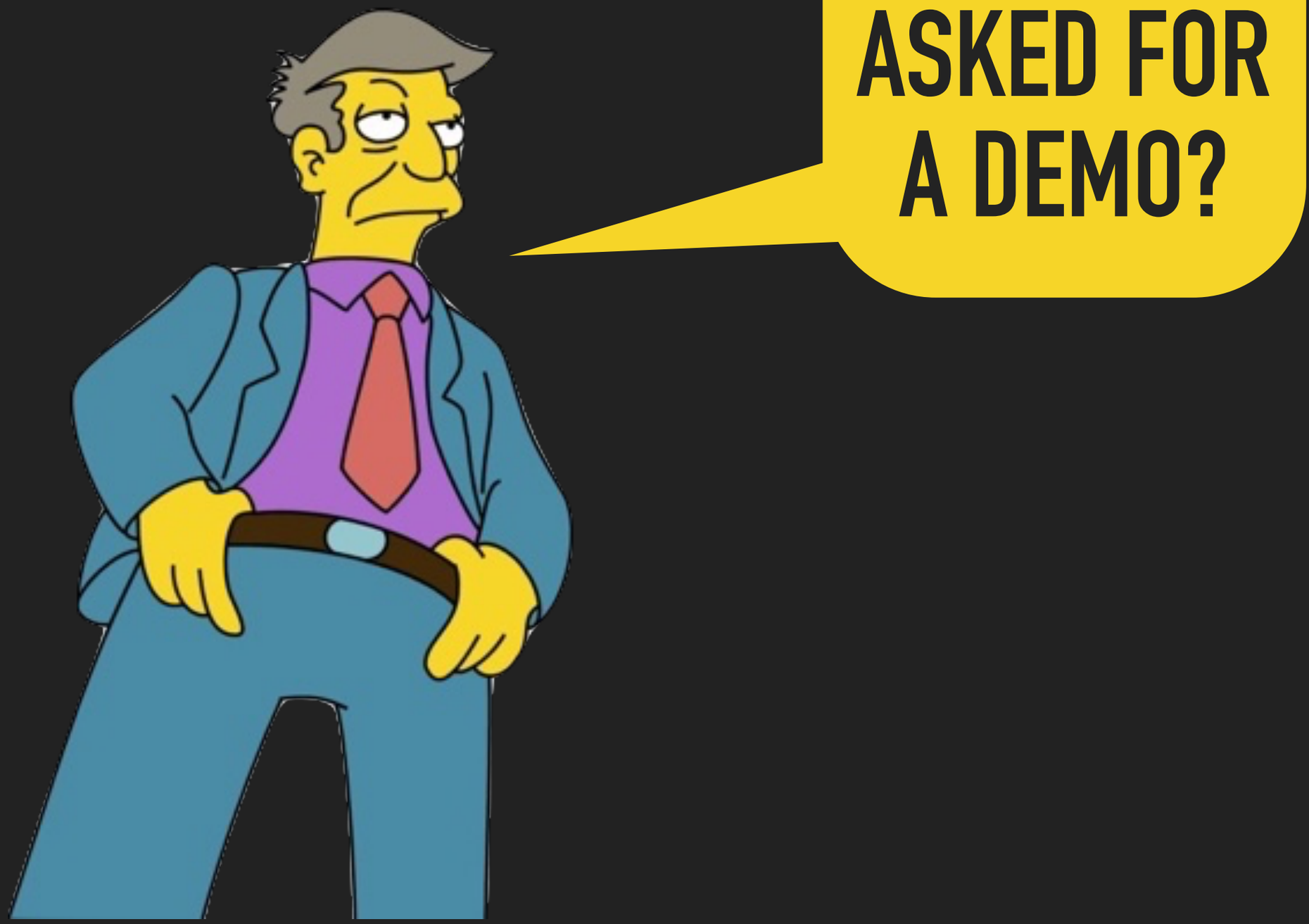
DATA

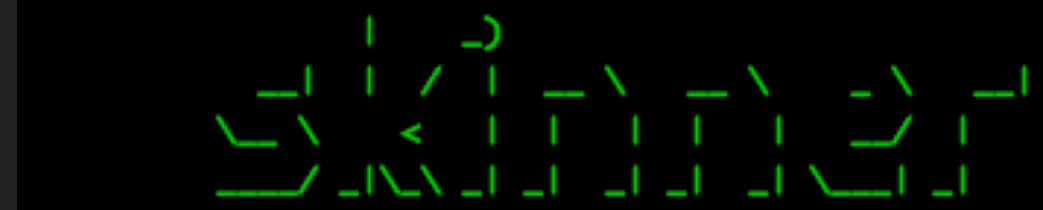
STORY ABOUT GOOD AND STORY ABOUT BAD!

https://goo.gl/3Kx2fk


aws


Se


WHO
ASKED FOR
A DEMO?



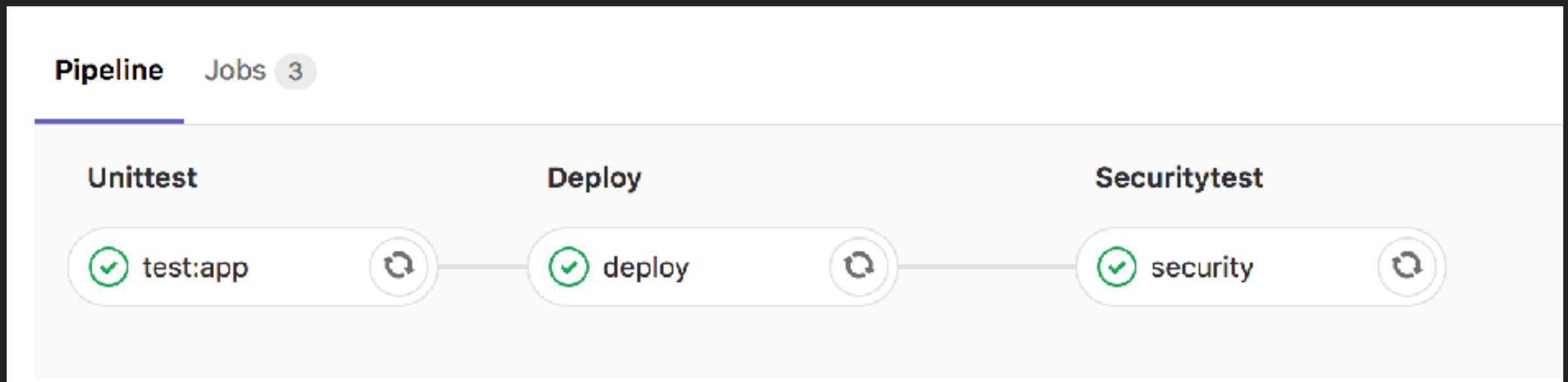
Skinner - Automatic WebApp Security Tests via Burp

```
usage: main.py [-h] [-v] -b BURP [-u URL] [-r {mattermost,database,all}]
               [-t {html,xml}] [-p BURP_PROXY_PORT] [-a BURP_API_PORT]
               [-sU SELENIUM_URL] [-sP SELENIUM_PORT] -id PROJECT_ID

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         Installed version of the Skinner script
  -b BURP, --burp BURP  Burp API base address, e.g. http://burp.intra
  -u URL, --url URL     The address of target for scan via Burp Pro, e.g.
                        http://app.intra
  -r {mattermost,database,all}, --report {mattermost,database,all}
                        Ways of storing Burp scan report, Default is
                        Mattermost
  -t {html,xml}, --type {html,xml}
                        Burp report file type, Default is HTML
  -p BURP_PROXY_PORT, --burp-proxy-port BURP_PROXY_PORT
                        Burp proxy port, default is 8080
  -a BURP_API_PORT, --burp-api-port BURP_API_PORT
                        Burp API port, default is 9080
  -sU SELENIUM_URL, --selenium-url SELENIUM_URL
                        Selenium URL for generating traffic to Burp, e.g.
                        http://selenium.intra
  -sP SELENIUM_PORT, --selenium-port SELENIUM_PORT
                        Selenium webdriver port, default is 4444
  -id PROJECT_ID, --project-id PROJECT_ID
                        Gitlab Project ID, Gitlab ci variable is
                        $CI_PROJECT_ID

Basic usage from Gitlab CI pipeline: python3 ./skinner/main.py -b
http://burp.intra -u http://deploy.intra -sU selenium.intra -id $CI_PROJECT_ID
```

```
13
14  stages:
15    - unittest
16    - deploy
17    - securitytest
18
```



```php
$options = new ChromeOptions();
$options->addExtensions([$pluginForProxyLogin]);
$capabilities = DesiredCapabilities::chrome();
$capabilities->setCapability(ChromeOptions::CAPABILITY, $options);
$driver = RemoteWebDriver::create($host, $capabilities, 5000);

//Login to auth following page will redirect to auth page
$driver->get('                              ;
$targetUsername =
$targetPassword =
sleep(5);
$element = $driver->findElement(WebDriverBy::name('login'));
$driver->getKeyboard()->sendKeys($targetUsername);
$driver->getKeyboard()->pressKey(WebDriverKeys::ENTER);
sleep(5);
$element = $driver->findElement(WebDriverBy::name('password'));
$driver->getKeyboard()->sendKeys($targetPassword);
$driver->getKeyboard()->pressKey(WebDriverKeys::ENTER);
sleep(5);


// Browse pages that need to be scanned
$driver->get('                              nstallations');
sleep(5);
$driver->get('                              ccounts/create-email-list');
sleep(5);
$driver->get(                               /projects/add');

// Destroy Seleninum session at the end
$driver->quit();

```

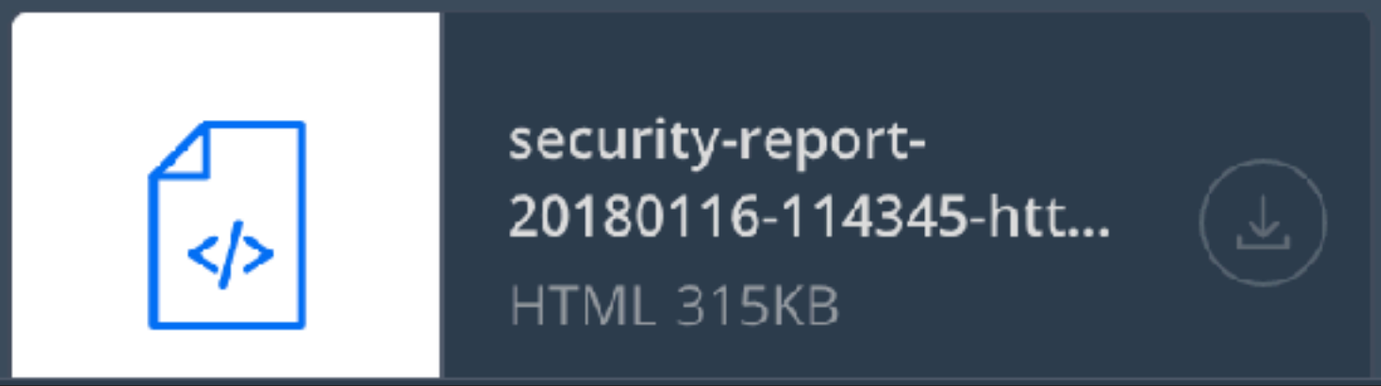
```
$ python3 ./skinner/main.py -b http://burp.intra -u http://deploy.intra -sU selenium.intr
a -id $CI_PROJECT_ID
```

```
          |    _)
      __|  |  /  |  __ \   __ \    _ \   __|
    \__ \    <   |  |   |  |   |   __/  |
    ____/ _|\_\ _| _|  _| _|  _| \___| _|
```

Skinner - Automatic WebApp Security Tests via Burp

```
[+] Updating Burp scope
[+] Starting scan for http://deploy.intra
0.0% 4.0% 9.0% 19.0% 30.0% 37.0% 41.0% 49.0% 53.0% 55.0% 55.0% 55.0% 55.0% 55.0% 56.0% 5
8.0% 59.0% 59.0% 60.0% 60.0% 60.0% 60.0% 62.0% 62.0% 64.0% 65.0% 65.0% 65.0% 66.0% 66.0%
 67.0% 69.0% 69.0% 70.0% 70.0% 70.0% 71.0% 72.0% 73.0% 73.0% 74.0% 74.0% 75.0% 77.0% 78.
0% 78.0% 79.0% 79.0% 79.0% 86.0% 92.0% 96.0% 96.0% 96.0% 96.0% 97.0%
[+] List of issues:
[!] Issue: Cookie without HttpOnly flag set, Severity: Low
[!] Issue: Open redirection (reflected), Severity: Information
[!] Issue: Robots.txt file, Severity: Information
[!] Issue: Client-side HTTP parameter pollution (reflected), Severity: Low
[!] Issue: Frameable response (potential Clickjacking), Severity: Information
[!] Issue: Cross-domain script include, Severity: Information
[!] Issue: Private IP addresses disclosed, Severity: Information
[!] Issue: Input returned in response (reflected), Severity: Information
[!] Issue: Cross-domain Referer leakage, Severity: Information
[!] Issue: Cross-site request forgery, Severity: Information
[!] Issue: Password field with autocomplete enabled, Severity: Low
[!] Issue: Content type incorrectly stated, Severity: Low
[!] Issue: Referer-dependent response, Severity: Information
[!] Issue: Unencrypted communications, Severity: Low
[!] Issue: Email addresses disclosed, Severity: Information
[!] Issue: Cleartext submission of password, Severity: High
[!] Issue: Content type is not specified, Severity: Information
[+] Adding founded critical issues to gitlab
[+] Mattermost message sent, 'Burp Scan Report' channel, report file: security-report-201
80111-123111-http-deploy.intra.html
Job succeeded
```

1: Issue: Client-side HTTP parameter pollution (reflected), Severity: Low
2: Issue: Content type is not specified, Severity: Information
3: Issue: Content type incorrectly stated, Severity: Low
4: Issue: Frameable response (potential Clickjacking), Severity: Information
5: Issue: Cross-site request forgery, Severity: Information
6: Issue: Cross-domain Referer leakage, Severity: Information
7: Issue: Email addresses disclosed, Severity: Information
8: Issue: Open redirection (reflected), Severity: Information
9: Issue: Cookie without HttpOnly flag set, Severity: Low
10: Issue: Unencrypted communications, Severity: Low
11: Issue: Referer-dependent response, Severity: Information
12: Issue: Cross-domain script include, Severity: Information
13: Issue: Private IP addresses disclosed, Severity: Information
14: Issue: Robots.txt file, Severity: Information
15: Issue: Cleartext submission of password, Severity: High
16: Issue: Password field with autocomplete enabled, Severity: Low
17: Issue: Input returned in response (reflected), Severity: Information



Cleartext submission of password

URL: http
Severity: High
Confidence: Certain

Issue Background

Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have re-used their password elsewhere at risk.

Issue Detail

The page contains a form with the following action URL, which is submitted over clear-text HTTP:

- http

The form contains the following password field:

- password

Remediation

Todo Add todo »

Assignee Edit
No assignee - assign yourself

Milestone Edit
None

Time tracking
No estimate or time spent

Due date Edit
No due date

Labels Edit
security-test

Weight Edit
None

Confidentiality Edit
Not confidential

Lock issue Edit
Unlocked

WE GOTTA TRY HARDER…

https://goo.gl/wPVYQQ

THANK YOU
ANY QUESTIONS?

@n3tg33k