



QUALYS SECURITY CONFERENCE 2020

Moving Security up the Stack

Web Application and API Security

Dave Ferguson

Director of Product Management, Qualys, Inc.

Agenda

Recent trends in Application Security

Web Application Scanning (WAS)

Qualys Periscope

Building Securing APIs

Trends in Application Security

Web app breaches continue

E-commerce sites targeted

API attacks

Trends in AppSec testing

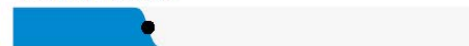
Shifting left

Coverage

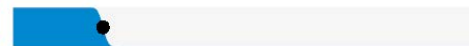
Automation

Breaches

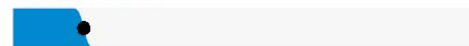
Web Applications



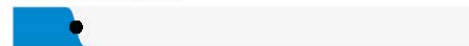
Miscellaneous Errors



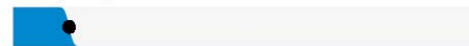
Privilege Misuse



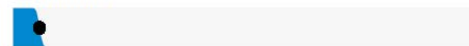
Cyber-Espionage



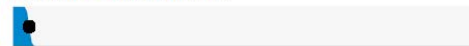
Everything Else



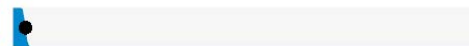
Crimeware



Lost and Stolen Assets



Point of Sale



Source: 2019 Verizon DBIR

The background is a solid blue color with a pattern of small white dots arranged in a grid. Three of these dots are highlighted in red, one on the left side and two on the right side. The text "Web Application Scanning" is centered in the middle of the image in a white, sans-serif font.

Web Application Scanning

WAS Overview

Detects application-layer vulnerabilities in web apps & APIs

Browser engine

Automated crawling

Play back of Selenium scripts

API to integrate with other systems

Unique integration with Qualys WAF

Mature product



2019 Highlights

WAS Jenkins plugin v2

Updated Qualys Browser Recorder

TLS 1.3

Full HTTP requests

Enhanced crawling

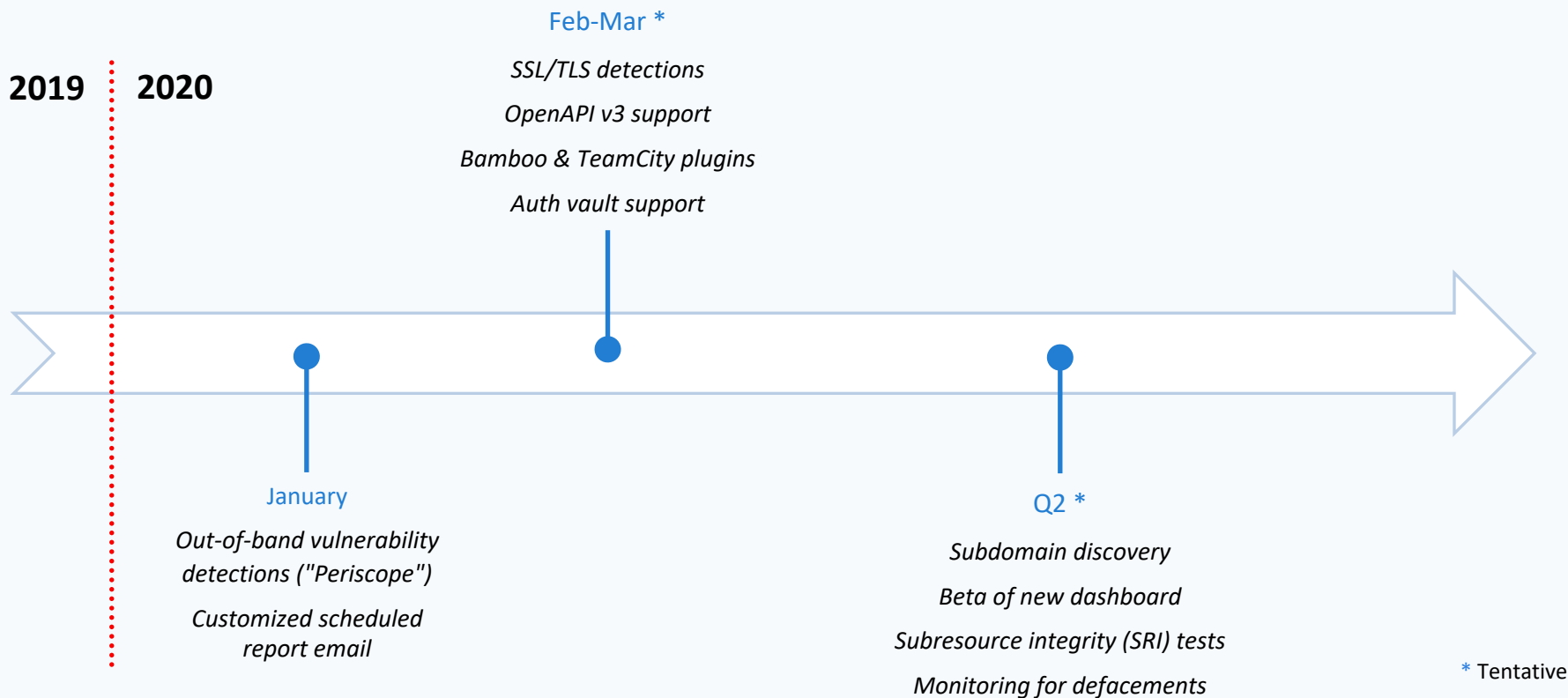
Postman Collections

WAS Burp extension v2

Editable QID severity



WAS Roadmap



Out-of-Band Vulnerabilities

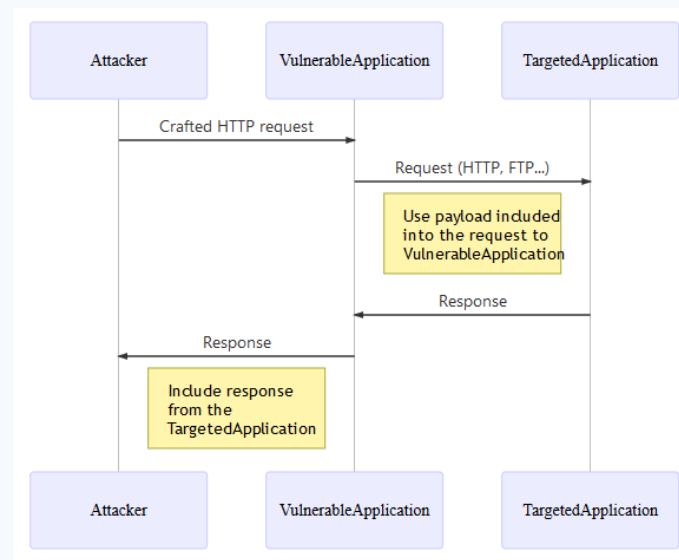
Some issues can't be detected by traditional request-response

SSRF

SMTP header injection

Blind XXE injection

Detecting these vulnerabilities requires a different approach



Source: OWASP

Introducing Periscope

Detection mechanism for out-of-band web app vulnerabilities

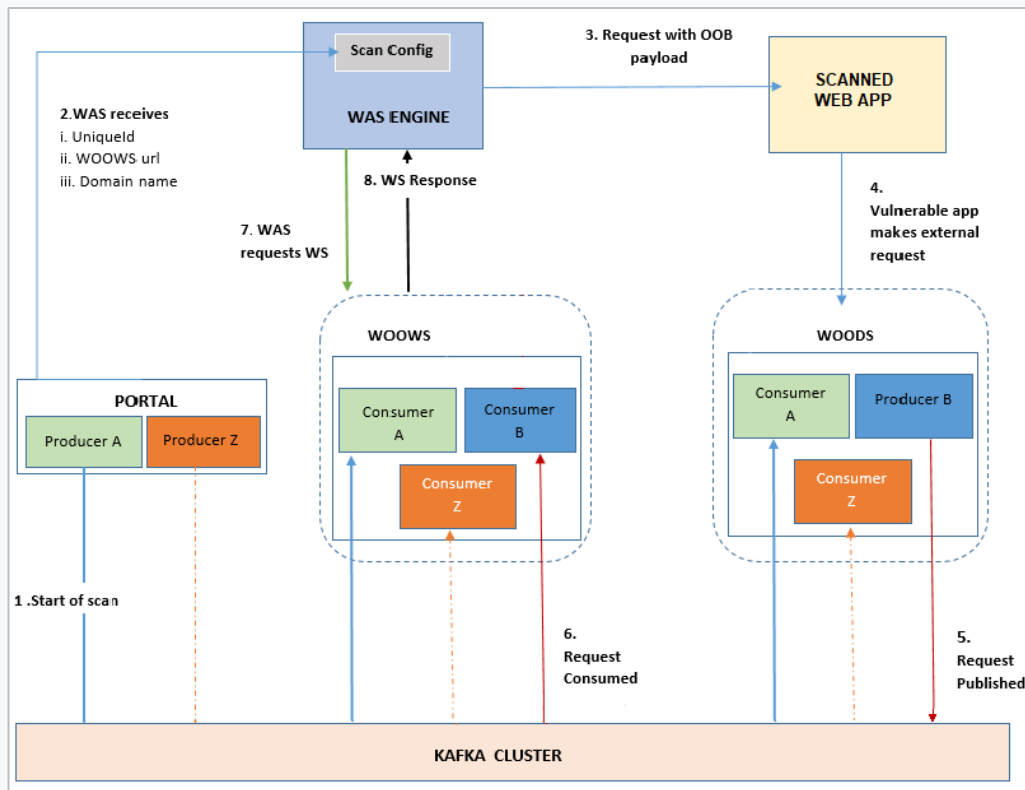
Scanner sends a test; POST request body is:

`p1=joe&p2=smith&p3=http%3A%2F%2Fe528efddaa51766cb86afb19f22de54b6da1093c.1454156_35626.2086421852.ssrff01.ssrff.qualysperiscope.com`

The web app tries to resolve this FQDN:

`e528efddaa51766cb86afb19f22de54b6da1093c.1454156_35626.2086421852.ssrff01.ssrff.qualysperiscope.com`

Qualys Periscope



The background is a solid blue color with a pattern of small white dots arranged in a grid. Three of these dots are highlighted in red, one on the left side and two on the right side. The text "Building Secure APIs" is centered in the middle of the image in a white, sans-serif font.

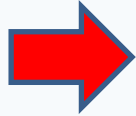
Building Secure APIs

OWASP API Security Top 10



1	Broken Object Level Authorization (BOLA)
2	Broken User Authentication
3	Excessive Data Exposure
4	Lack of Resources & Rate Limiting
5	Broken Function Level Authorization
6	Mass Assignment
7	Security Misconfiguration
8	Injection
9	Improper Assets Management
10	Insufficient Logging & Monitoring

Example API – Pet Store



pet Everything about your Pets		
GET	/pet/{petId} Find pet by ID	🔒
POST	/pet/{petId} Updates a pet in the store with form data	🔒
DELETE	/pet/{petId} Deletes a pet	🔒
POST	/pet/{petId}/uploadImage uploads an image	🔒
POST	/pet Add a new pet to the store	🔒
PUT	/pet Update an existing pet	🔒
GET	/pet/findByStatus Finds Pets by status	🔒

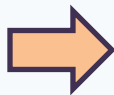
Relevant portion of the Swagger File

```
{
  "swagger": "2.0",
  "info": {
    "version": "1.0",
    "title": "Petstore",
  },
  "host": "api.petstore.com",
  "basePath": "/v1",
  "schemes": [
    "http", "https"
  ],
  "paths": {
    "/pet/{petId}": {
      "get": {
        "summary": "Get info for a specific pet",
        "operationId": "showPetById",
        "parameters": [
          {
            "name": "petId",
            "in": "path",
            "required": true,
            "description": "The ID of the pet to retrieve",
            "type": "integer"
          }
        ],
        "responses": {
          "200": {
            "description": "Expected successful response",
            "schema": {
              "$ref": "#/definitions/Pet"
            }
          }
        }
      }
    }
  }
}
...snip...
```

How Does this Help with Security?

We can leverage the Swagger spec to harden the API endpoints in a declarative way

```
"paths": {
  "/pet/{petId}": {
    "get": {
      "summary": "Get info for a specific pet",
      "operationId": "showPetById",
      "parameters": [
        {
          "name": "petId",
          "in": "path",
          "required": true,
          "description": "The ID of the pet",
          "type": "integer"
        }
      ]
    }
  }
},
```



```
"paths": {
  "/pet/{petId}": {
    "get": {
      "summary": "Get info for a specific pet",
      "operationId": "showPetById",
      "parameters": [
        {
          "name": "petId",
          "in": "path",
          "required": true,
          "description": "The ID of the pet",
          "type": "integer",
          "minimum": 1,
          "maximum": 999999
        }
      ]
    }
  }
},
```

Capabilities Coming to Qualys API Security

Static Assessment of Swagger/OpenAPI file

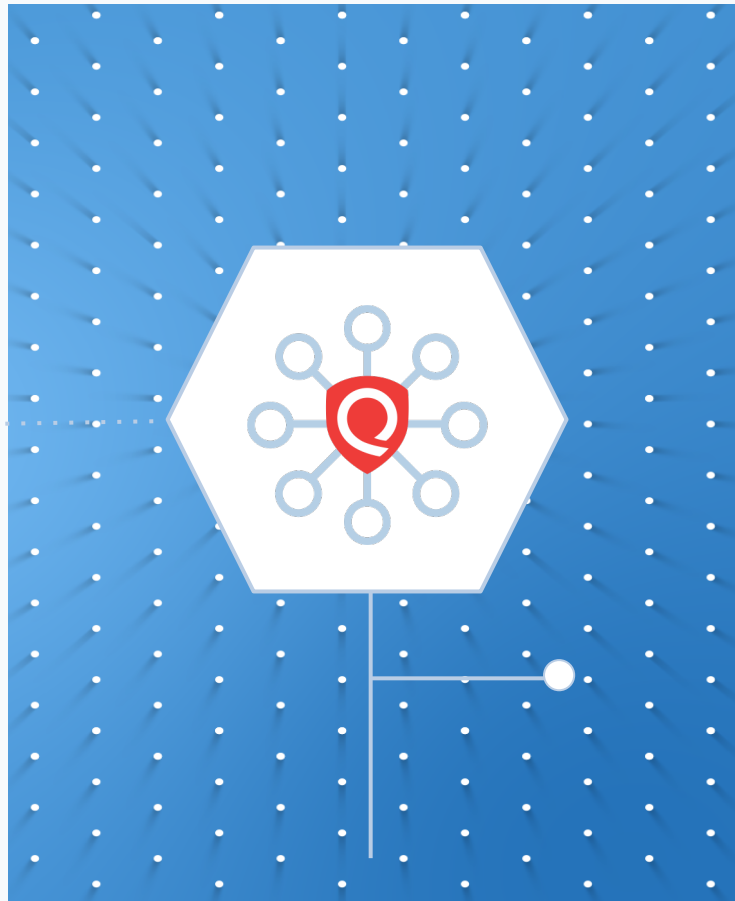
Get recommended changes to harden your API

Conformance Scan to check the API's actual behavior

Test the API endpoints for behavior that violates the Swagger file

Vulnerability Scan to check the API for security flaws

Current feature in Qualys Web Application Scanning (WAS)





QUALYS SECURITY CONFERENCE 2020

Thank You

Dave Ferguson

dferguson@qualys.com