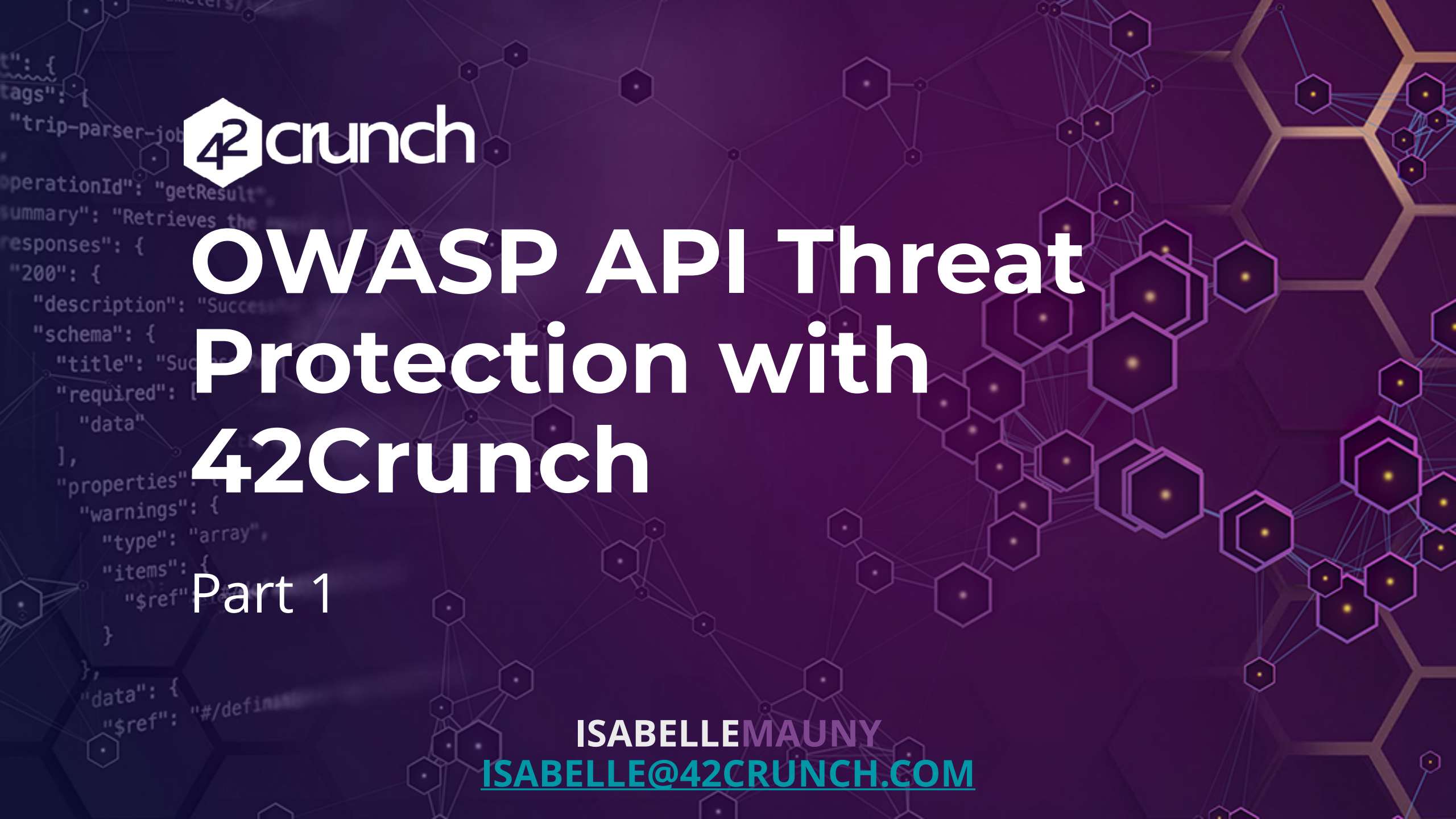


OWASP API Threat Protection with 42Crunch

Part 1

ISABELLEMAUNY
ISABELLE@42CRUNCH.COM

API Breaches are on the rise!

- 300+ breaches reported on apisecurity.io since Oct. 2018
- And those are just the public ones!
- Most recurrent causes (combination of):
  - Lack of Input validation
  - Lack of Rate Limiting
  - Data/Exception leakage
  - BOLA/IDOR (Authorization)

Facebook - 50 million users' personal information was exposed

PayPal - 1.6 million customers at risk of data exposure

T-Mobile - 76 million users' phone numbers and addresses stolen

Instagram - 49 million users' emails and phone numbers exposed

Uber - 57 million riders and drivers accounts were compromised

Justdial - Over 100 million Indian users' personal data at risk

Equifax - 147 million users personal data stolen

Starbucks - 100 million customer records accessed

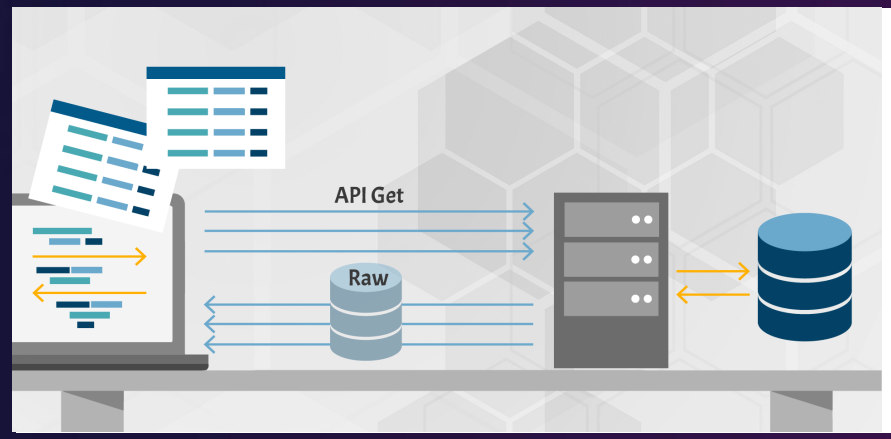
Verizon - 14 million subscribers phone numbers and PINs exposed

OWASP API Security Top 10

APIs have different vulnerabilities

- API1 : Broken Object Level Access Control
- API2 : Broken Authentication
- API3 : Excessive Data Exposure
- API4 : Lack of Resources & Rate Limiting
- API5 : Missing Function Level Access Control
- API6 : Mass Assignment
- API7 : Security Misconfiguration
- API8 : Injection
- API9 : Improper Assets Management
- API10 : Insufficient Logging & Monitoring

API3 : Excessive Data Exposure



Looking forward to generic implementations, developers tend to expose all object properties without considering their individual sensitivity, relying on clients to perform the data filtering before displaying it to the user.

FIZIKAL

Uber

tinder

Grindr

3Fun

הליכוד
Likud Party

jCrush®

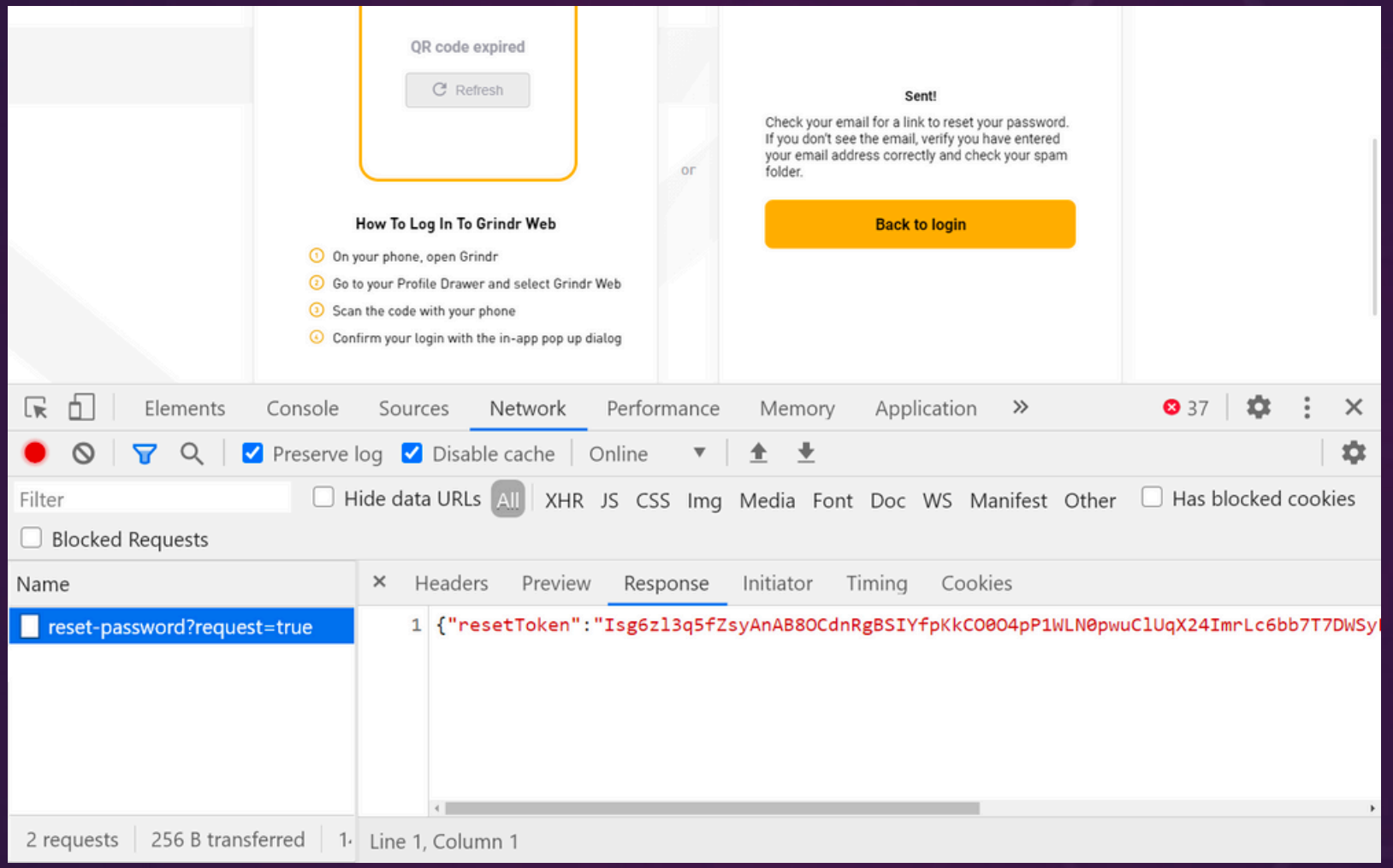
venmo

GRINDR (SEPT 2020)

https://www.troyhunt.com/hacking-grindr-accounts-with-copy-and-paste/

- The Attack
  - ✓ Full account takeover for any Grindr account from an email address via password reset
- The Breach
  - ✓ Unknown. Company thinks they fixed the issue before anyone could find it.
- Core Issues
  - ✓ On password reset, the API leaks the actual reset token which is sent to the user via email (and of course, only the user should know...)

Leaked Data



https://neo-account.grindr.com/v3/user/password/reset?resetToken=Isg6zl3q5fZsyAnAB8OCdnRgBSIYfpKkCO0O4pP1WLN0pwuClUqX24ImrLc6bb7T7DWSyFMG5lREHQmS4CsFR5uh8GEYQxF6Z6V5hsi3vSTuilXzgKRRItwdDIjmSWdq&email=test@scotthelme.co.uk

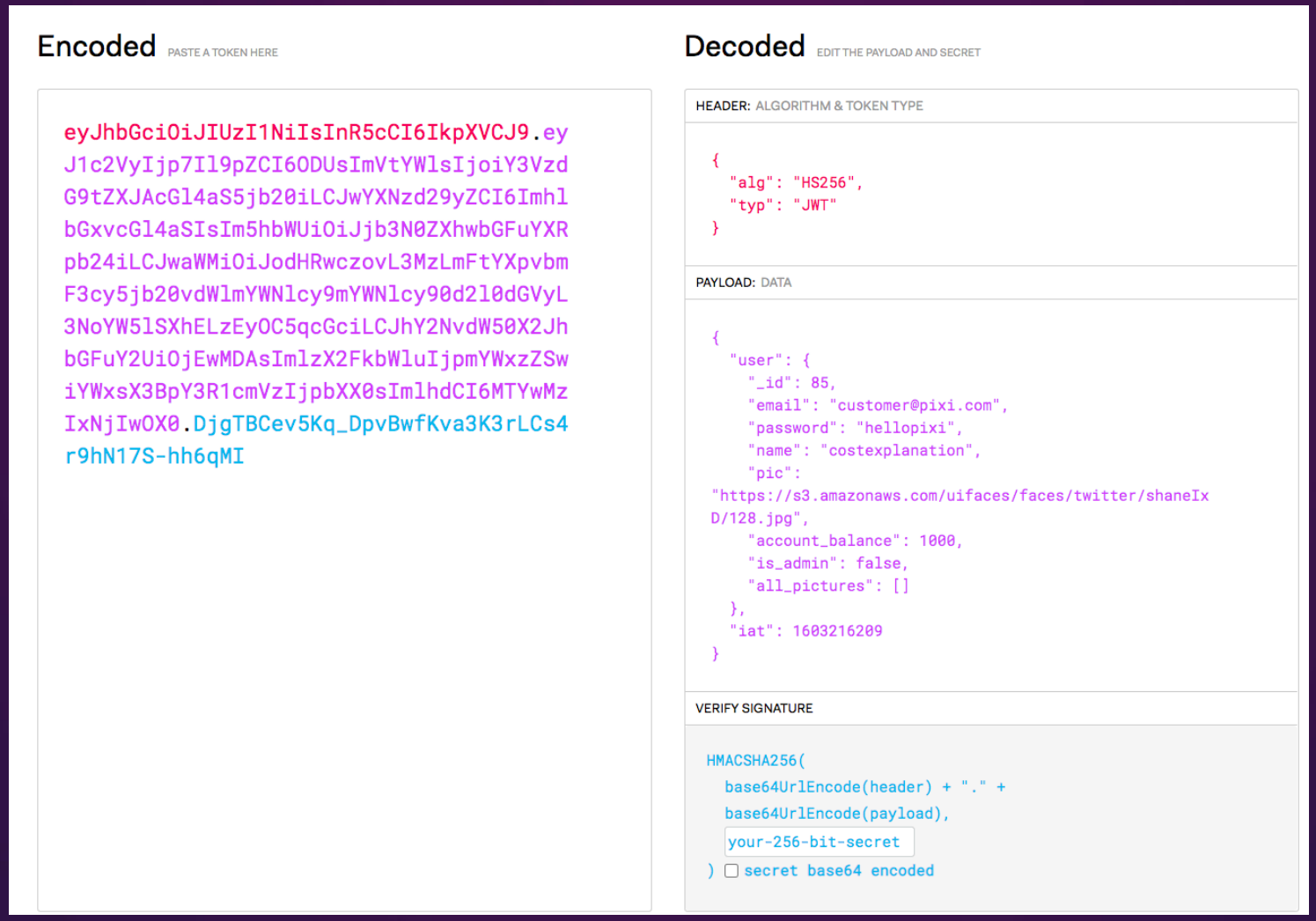
API3 MITIGATION

- Take control of your JSON schemas !
  - ✓ Describe the data thoroughly and enforce the format at runtime (outbound)
  - ✓ Review and approve data returned by APIs
- Never expose tokens/sensitive/exploitable data in API responses
- Never rely on client apps to filter data : instead, create various APIs depending on consumer, with just the data they need

- Beware of GraphQL queries!
  - ✓ Validate fields accessed via query

Another API3 vector: JWTs!

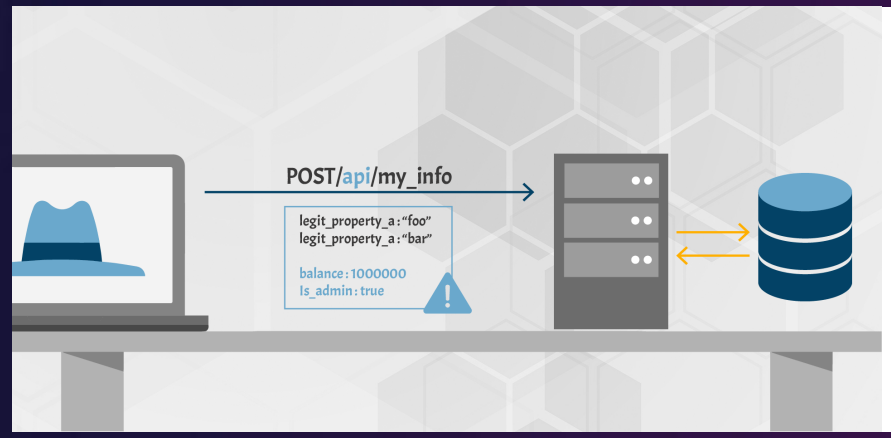
- Recommended best practice:
  - Use opaque tokens for external consumption
  - Use JWTs for internal consumption



How 42Crunch addresses API3

API SECURITY AUDIT (DEVELOPMENT/TEST)	**CONFORMANCE SCAN** (DEVELOPMENT/TEST)	**MICRO-API FIREWALL** (RUNTIME PROTECTION)
• Flag loose response schemas • Flag missing error codes and/or schemas	• Test schemas compliance	• Blocks responses which do not match the schemas

API6 : Mass Assignment



Binding client provided data (e.g., JSON) to data models, without proper properties filtering based on an allowlist, usually leads to Mass Assignment. Either guessing objects properties, exploring other API endpoints, reading the documentation, or providing additional object properties in request payloads, allows attackers to modify object properties they are not supposed to.

Harbor Registry

myGator -The start of life's adventures

Uber

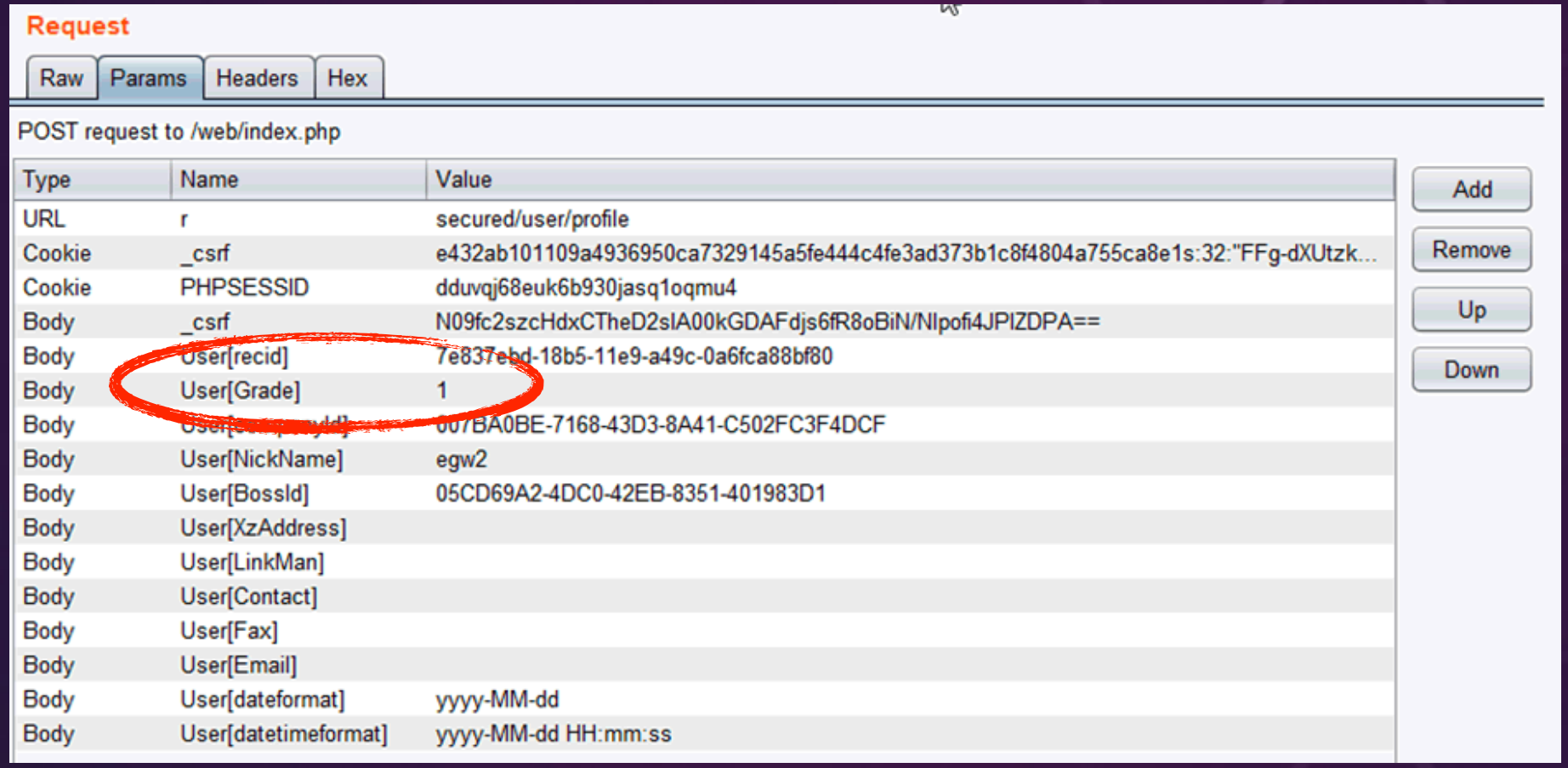
New Relic

GATOR WATCHES (APRIL 2019)

https://www.pentestpartners.com/security-blog/gps-watch-issues-again/

- The Attack
  - ✓ Become admin of the Gator platform
- The Breach
  - ✓ Admin can see the location of any child wearing the smartwatch
- Core Issues
  - ✓ Anyone can set their User[Grade] to `0`, which automatically elevates privileges to admin.

Becoming Admin



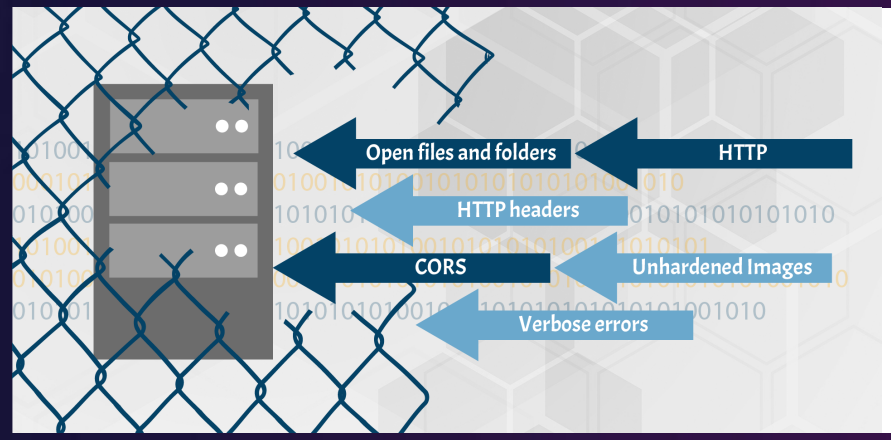
API 6 MITIGATION

- Do not blindly update data from input structure
  - ✓ Use frameworks that map directly database records to JSON objects with caution
- Do not use the same data structures for GET and POST/PUT
- Validate Inputs
  - ✓ Only accept information specified in JSON schema (contract-based, whitelist approach) - Reject all others.

How 42Crunch addresses API6

API SECURITY AUDIT (DEVELOPMENT/TEST)	**CONFORMANCE SCAN** (DEVELOPMENT/TEST)	**MICRO-API FIREWALL** (RUNTIME PROTECTION)
• Flag loose request schemas	• Test schemas compliance	• Blocks requests which do not match schemas

API7 : Security Misconfiguration



Security misconfiguration is commonly a result of un-secure default configurations, incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information.

EQUIFAX®

Uber

GITHUB (NOV 2019)

https://blog.teddykatz.com/2019/11/05/github-oauth-bypass.html

- The Attack
  - ✓ Bypassing GitHub's OAuth flow
- The Breach
  - ✓ None. This was part of a bug bounty.
- Core Issues
  - ✓ Hacker was able to decompile Github Enterprise code
  - ✓ Github API accepts HEAD request, which under the hood is handled by their dev framework as a POST (Rails)

API 7 MITIGATION

- Reject requests with unknown path/verbs
- TLS is on by default
  - ✓ TLS 1.2 minimum with strong cipher suites
  - ✓ Test your API endpoints with SSLLabs.com
- Change default credentials/ports
- Automatically inject security headers

- Keep systems and software at latest level
- Limit your external dependencies
- Control those dependencies in-house (enterprise repository)
- No Trust !! Continuously test for vulnerabilities and leaking secrets (OS, libraries, docker images, kubernetes deployment files, etc.)

API 7 MITIGATION

July 22, 2020

Anatomy of a Kubernetes Attack - How Untrusted Docker Images Fail Us

PART TWO OF A SERIES.

This post illustrates how an attacker could use a poisoned docker image to break out of a container and gain access to the hosts\nodes in a Kubernetes cluster.

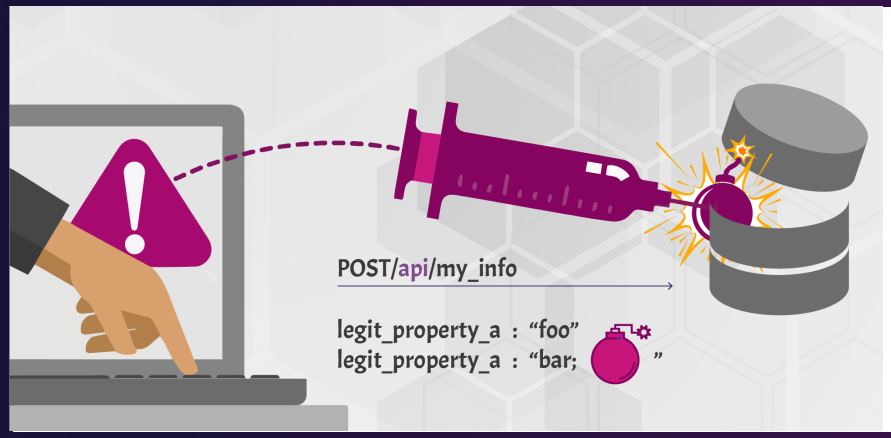
In the first part of this blog series, Infrastructure as Code: Terraform, AWS EKS, Gitlab & Prisma Cloud, I went through the scenario of building out an Amazon EKS cluster using Terraform and a VCS integration with Gitlab. I also covered an initial Daemonset deployment of the Palo Alto Networks Prisma agent to the nodes on the newly provisioned cluster. In the second part of this series, we will look at some aspects of a Kubernetes attack and in a follow-up installment, how Palo Alto Networks Prisma Compute can be used to prevent related Kubernetes attacks.

Microsoft recently released a Kubernetes attack matrix (similar to MITRE's ATT&CK framework) that I feel is a good reference for walking through some of the aspects of an example Kubernetes attack. For this blog, I'll be covering techniques in Initial Access, Execution, Persistence and Privilege Escalation Tactic phases.

How 42Crunch addresses API7

API SECURITY AUDIT (DEVELOPMENT/TEST)	**CONFORMANCE SCAN** (DEVELOPMENT/TEST)	**MICRO-API FIREWALL** (RUNTIME PROTECTION)
• Audit is used to discover potential issues early in lifecycle and is automated for security governance	• Tests automatically for API implementation security issues at early development stages	• Secure TLS configuration • Blocks by default • Safe error messages • Automatic injection of security headers • Automatic enforcement of API contract

API8 : Injection



Injection flaws, such as SQL, NoSQL, Command Injection, etc., occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s malicious data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

EQUIFAX

Kiwi

STARBUCKS (NOV 2019)

https://hackerone.com/reports/592400

- The Attack
  - ✓ Blind SQLi leading to RCE (Remote Command Execution)
- The Breach
  - ✓ None - This was a bug bounty
- Core Issues
  - ✓ SQL Injection allowed to get access to backend production database and execute shell commands on the database server.

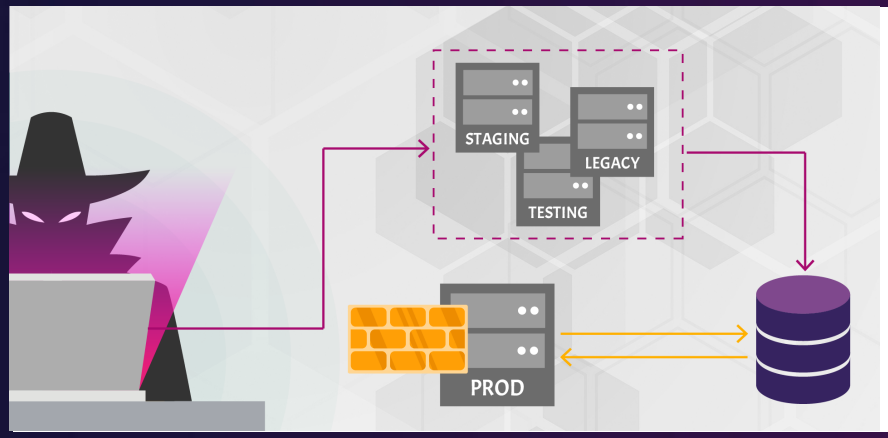
API 8 MITIGATION

- No Trust! (even for internal APIs and for East-West traffic)
- Validate user input, including headers like Content-Type or Accept
- Check behaviour of your dev frameworks when wrong Content-Type is used
  - ✓ Many default to sending an exception back but experience varies

How 42Crunch addresses API8

API SECURITY AUDIT (DEVELOPMENT/TEST)	**CONFORMANCE SCAN** (DEVELOPMENT/TEST)	**MICRO-API FIREWALL** (RUNTIME PROTECTION)
• Flags loose schemas and data definitions (headers, query and path params)	• Tests resistance to bad data formats and invalid data types	• Protect from injections through validation of all data against API contract

API9 : Improper Assets Management



APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. Proper hosts and deployed API versions inventory also play an important role to mitigate issues such as deprecated API versions and exposed debug endpoints.

Justdial™
India's No.1 local search engine

facebook®

venmo

FACEBOOK (FEB 2018)

https://appsecure.security/blog/we-figured-out-a-way-to-hack-any-of-facebook-s-2-billion-accounts-and-they-paid-us-a-15-000-bounty-for-it

- The Attack
  - ✓ Account takeover via password reset at https://www.facebook.com/login/identify?ctx=recover&lwv=110.
  - ✓ facebook.com has rate limiting, beta.facebook.com does not!
- The Breach
  - ✓ None. This was a bug bounty.
- Core Issues
  - ✓ Rate limiting missing on beta APIs, which allows brute force guessing on password reset code
  - ✓ Misconfigured security on beta endpoints

API9 MITIGATION

- Govern all endpoints
- Protect APIs from abuse independently from their development stage (dev, QA, staging, etc.)
  - ✓ Start introducing security in early development stages and automate!
- Separate non-production from production data!

How 42Crunch addresses API9

API SECURITY AUDIT (DEVELOPMENT/TEST)	**CONFORMANCE SCAN** (DEVELOPMENT/TEST)	**MICRO-API FIREWALL** (RUNTIME PROTECTION)
• Integration of audit with CI/CD pipeline for automatic discovery of APIs • Single pane of glass view of all APIs security status across the enterprise	• Tests for unknown verbs • Detects unknown responses	• Unknown traffic is blocked by default • Non-blocking mode can be enabled for discovery/monitoring

OUR PHILOSOPHY

- We believe good security starts at design time
  - ✓ Encourage good security practices from early days of development
  - ✓ Help developers understand the vulnerabilities that some development practices may lead to.
- We bring tools that easily fit in the development cycle
  - ✓ Fast execution (no burden on productivity)
  - ✓ Actionable reports
- We allow security teams to enforce automatically their requirements along the API lifecycle (dev and ops)
  - ✓ Automation of security testing and deployment of firewall via CI/CD integration
- We use OpenAPI as the single source of truth across Dev, Ops and Security teams.

Thank you!

Contact us | info@42crunch.com | 42crunch.com

Free security tools from 42Crunch

https://42crunch.com/resources-free-tools/


APIsecurity.io
News and tools for better API Security
SUBSCRIBE TODAY!