

API Security Through External Attack Surface Management

Phillip Wylie, CISSP, OSCP, GWAPT



whoami:

Phillip Wylie, CISSP, OSCP, GWAPT

- Hacker in Residence & Evangelist @ **CYCOGNITO**
- Offensive Cybersecurity Professional & Instructor
- Former Adjunct Instructor
- Concept creator and coauthor of
“The Pentester Blueprint: Starting a Career as an Ethical Hacker”
- “The Hacker Factory Podcast” Host

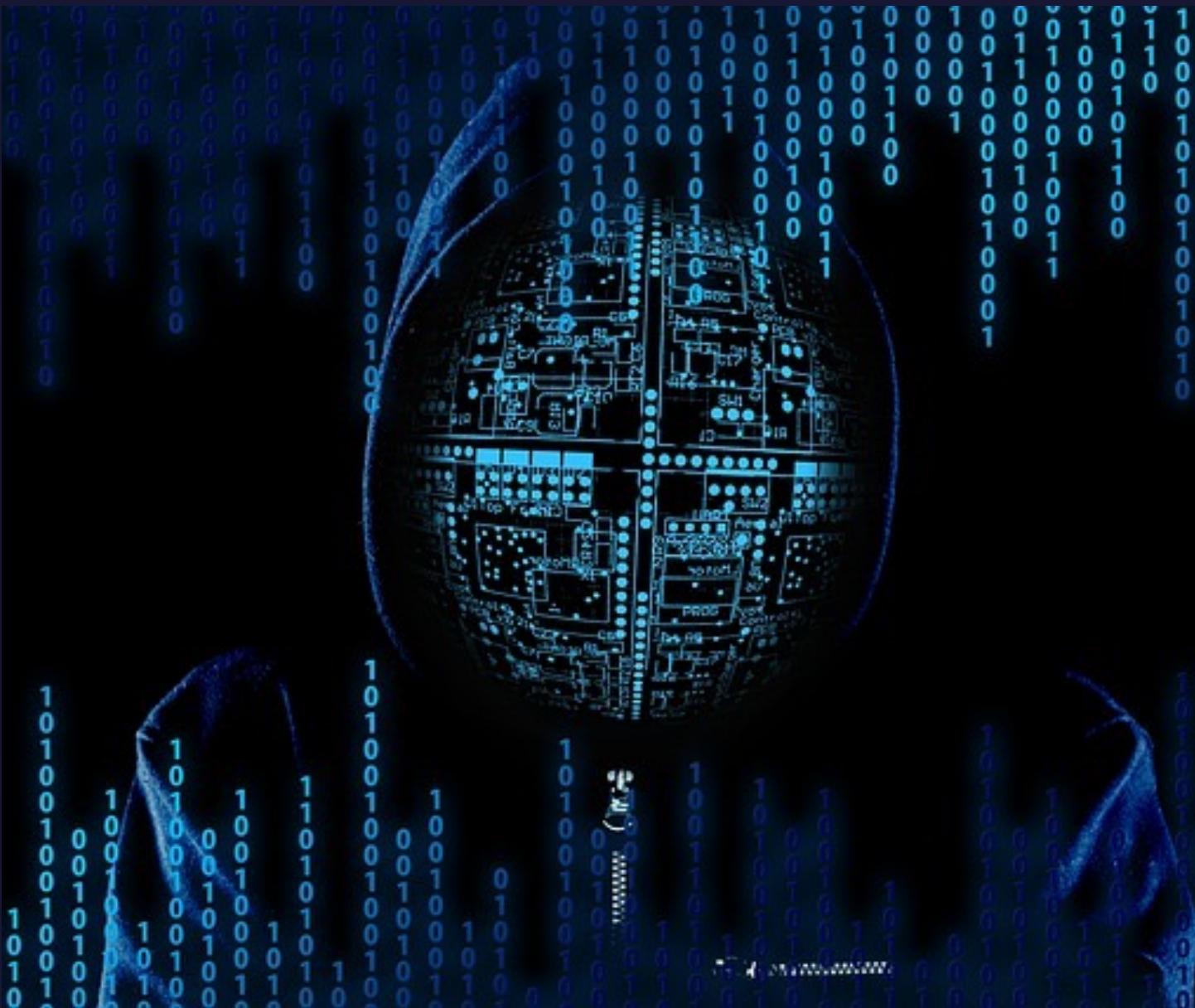
PHILLIP L. WYLIE
KIM CRAWLEY

THE PENTESTER BLUEPRINT
STARTING A CAREER AS AN ETHICAL HACKER

WILEY

Agenda

- Defining Attack Surface Management (ASM)
- Why Prioritize External Attack Surface Management (EASM)?
- Discovering Attack Surface
- API Pentesting & Tools
- Addressing Gaps EASM
- References & Resources



Attack Surface Management (ASM)

- To understand Attack Surface Management (ASM), we must first define Attack Surface.
- The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment. - NIST
- ASM can be simplified as attack vectors



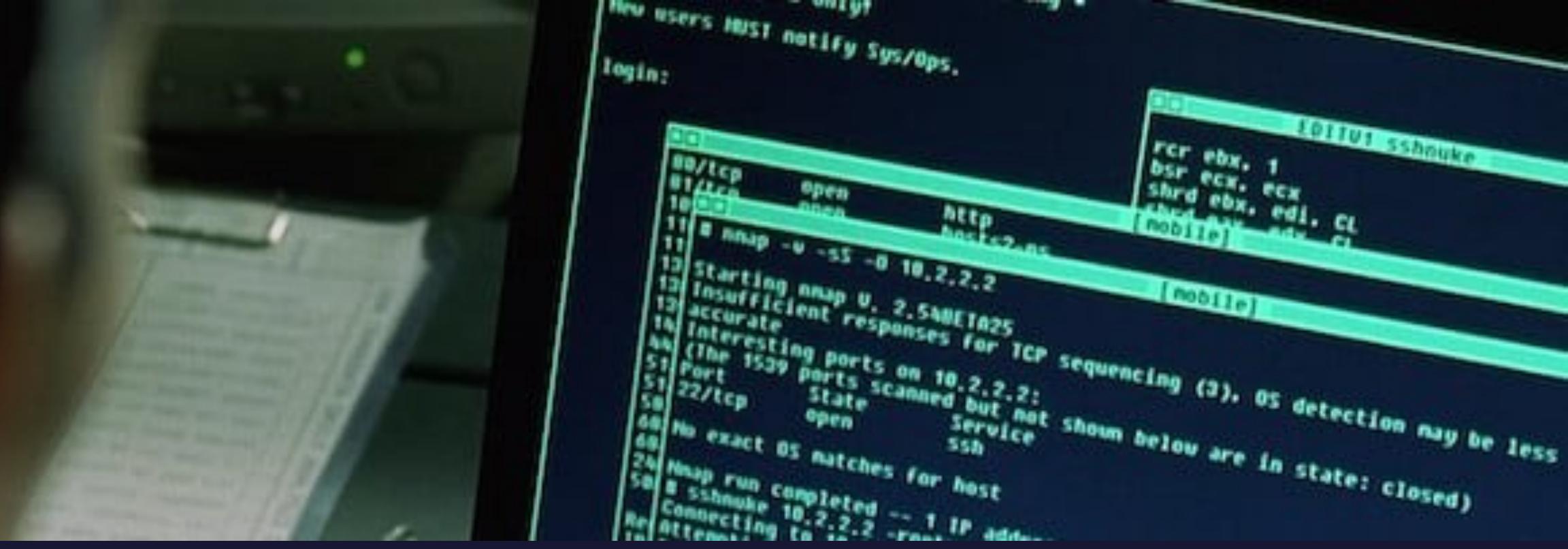
Why is ASM Important?

- It is hard to assess or secure what you don't know about
- Penetration testing once or twice a year is not enough
- Reoccurring vulnerability scans are not enough
- 50% of the exploited vulnerabilities are exploited within 48 hours of a Zero-day exploit being released.
- Assess security from a threat actor perspective



Attack Surface Management (ASM)

- Addresses both internal and external facing systems.
- Both are important, our focus is External Attack Surface Management.



Traditional ASM

- Vulnerability Scanning
- Vulnerability Assessments & Penetration Testing
- Red Teaming aka Adversary Emulation
- Purple Teaming
- Bug Bounties
- Application Security & Testing Integrated in SDLC



Traditional ASM Gaps



- Compliance based penetration testing
- Narrow scopes - miss testing types, systems and whole environments
- Time and resource limitations
- Incomplete and inaccurate asset inventories

Why Prioritize External ASM?



- Internet exposed and highly accessible to threat actors
- Penetration testing once or twice a year is not enough
- Reoccurring vulnerability scans are not enough

Addressing ESAM Gaps

- EASM Discovery
- Reconnaissance Including OSINT (Open-Source Intelligence)



EASM Discovery

- Collect known IP subnets and domain names
- Reconnaissance



Reconnaissance: Collection

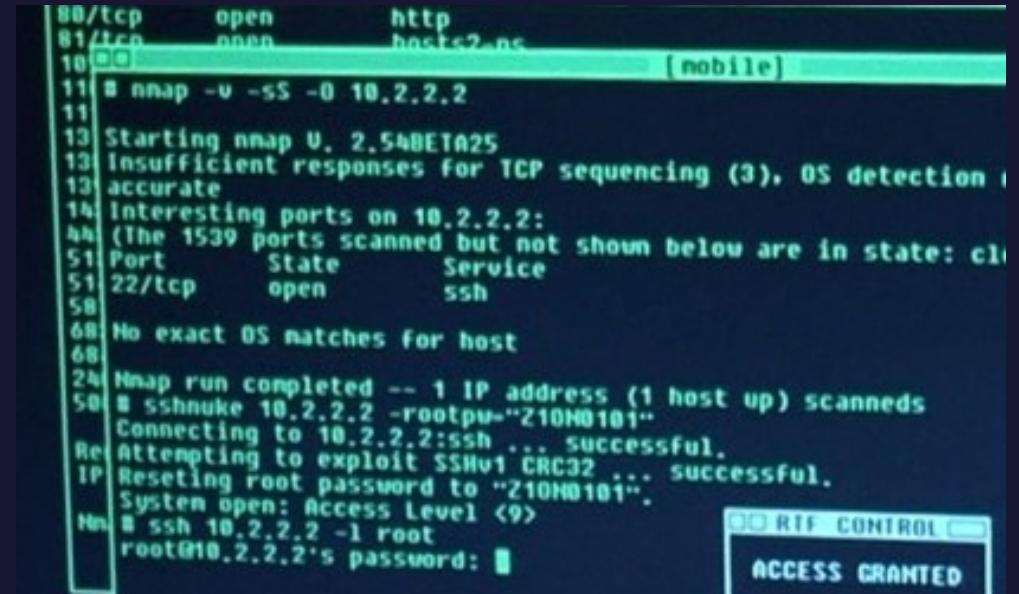


- IP address discovery
 - ASNs (Autonomous System Numbers)
 - ARIN & RIPE regional registrars
- Subdomain enumeration
 - Subfinder
 - AMASS
- Open-Source Intelligence (OSINT)
 - Shodan - locate unknown hosts
 - SpiderFoot
 - Maltego
 - Crunchbase - acquisitions

Reference: Jason Haddix's "The Bug Hunter's Methodology"

Reconnaissance: Scanning

- Scan IP addresses & domains (including subdomains)
 - Nmap scan for live hosts
 - Nmap ports & service scans to identify web resources



The screenshot shows a terminal window with the following output:

```
80/tcp open http hosts2.nsc [nobile]
81/tcp open
10/tcp open
# nmap -v -sS -O 10.2.2.2
Starting nmap 0.2.54BETA25
Insufficient responses for TCP sequencing (3). OS detection is
not accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port      State    Service
22/tcp    open     ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanned
$ sshnuke 10.2.2.2 -rootpw="Z10H0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
IP Resetting root password to "Z10H0101".
System open: Access Level <9>
$ ssh 10.2.2.2 -l root
root@10.2.2.2's password: ■
```

To the right of the terminal window, there is a small window titled "RTF CONTROL" with the text "ACCESS GRANTED".

API Endpoint Discovery

API Enumeration Tools

- Kiterunner - Restful API discovery
- FUFF - Wordlist based API discovery

Reference:

Katie Paxton-Fear aka InsiderPhD - My API

Testing Automated Toolbox

<https://www.youtube.com/c/InsiderPhD>



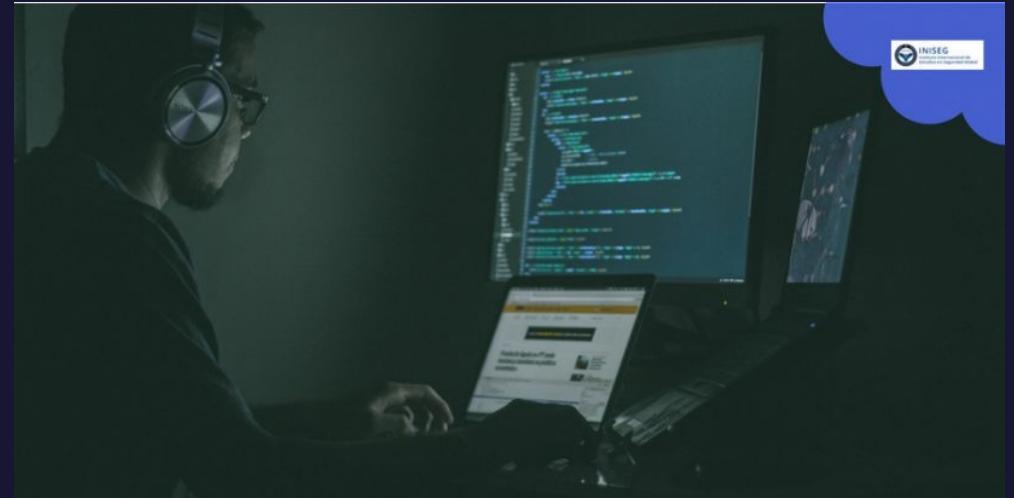
API Vulnerability Testing

API Vulnerability Testing Tools

- Autorize - Burp Suite extension for detecting IDOR
- Logger++ - Multithreaded logging extension for Burp Suite
- SQLMap - SQL injection testing tool
- NoSQLMap - NoSQL testing tool
- JWT_Tool - Java Web Token testing tool
- Burp Suite - Intercepting proxy and vulnerability testing tool

Reference:

Katie Paxton-Fear aka InsiderPhD - My API Testing Automated Toolbox
<https://www.youtube.com/c/InsiderPhD>



API Vulnerability Testing



API Vulnerability Testing Tools

- OWASP ZAP
 - OpenAPI add-on
 - GraphQL add-on
 - SOAP add-on
 - Import files containing URLs add-on

References:

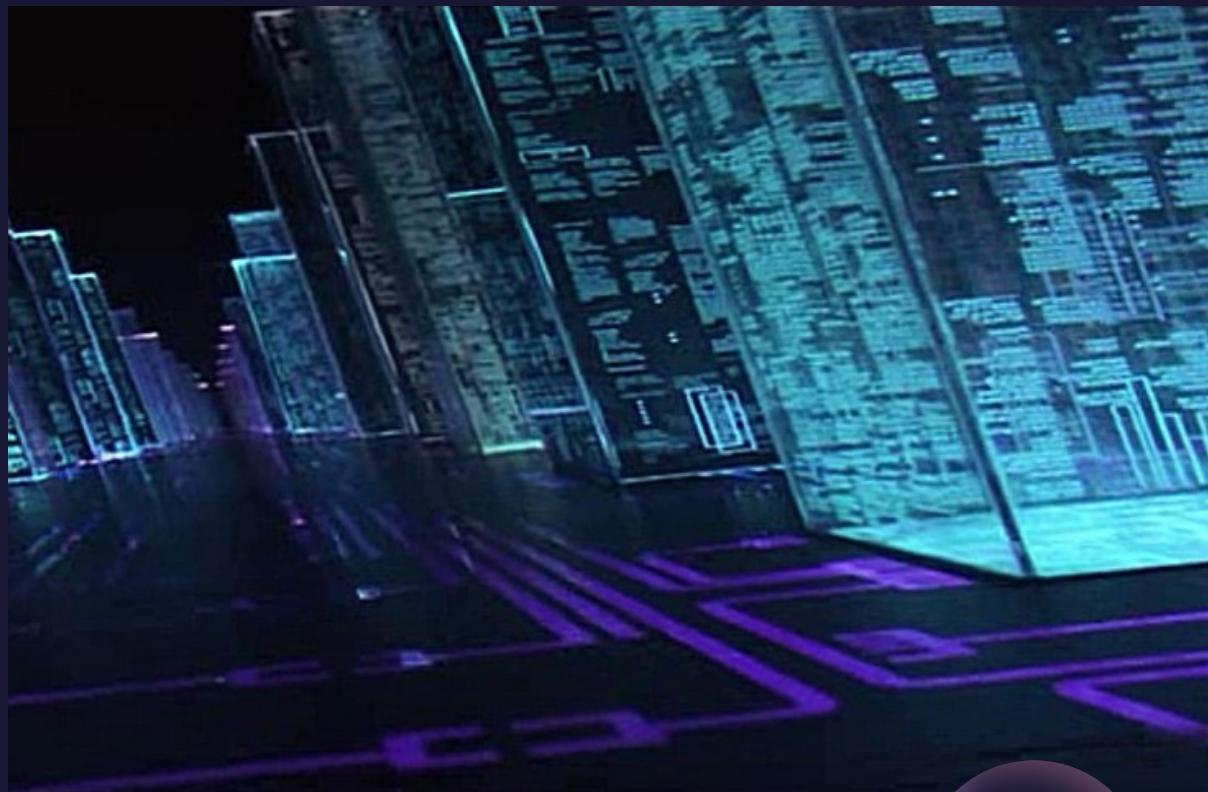
- <https://www.zaproxy.org/faq/how-can-you-use-zap-to-scan-apis/>
- <https://www.zaproxy.org/blog/2017-06-19-scanning-apis-with-zap/>

API Vulnerability Testing

- OWASP API Security Top 10 & API Security Project
 - <https://owasp.org/www-project-api-security/>



Addressing Gaps with ESAM

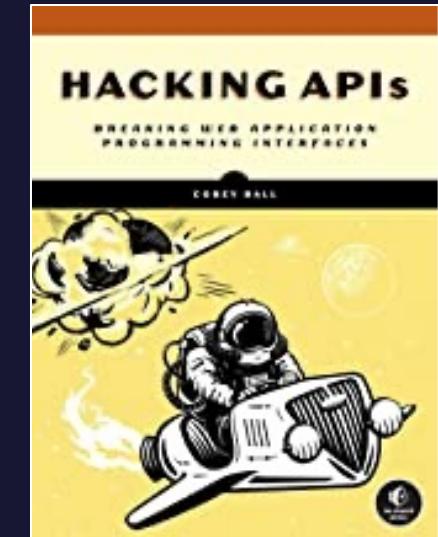


- Continuous discovery
 - Achieve and maintain more accurate asset inventory
- Continuous testing
 - Vulnerability scanning
 - Pentesting
 - ESAM platforms
- Automation
 - Improves scalability and resource limitations
 - Improves consistency
- Remediation
 - Timely and complete

References & Resources

- <https://www.uscybersecurity.net/csmag/securing-apis-through-external-attack-surface-management-easm/Vulnerability scanning> - by Phillip Wylie
- Reconnaissance reference: Jason Haddix's "The Bug Hunter's Methodology." <https://www.youtube.com/watch?v=uKWu6yhnhbQ>
- API discovery credit: Katie Paxton-Fear aka InsiderPhD - My API Testing Automated Toolbox <https://www.youtube.com/c/InsiderPhD>
- For further information on API penetration testing, get the new API hacking book by Corey Ball titled "Hacking APIs: Breaking Web Application Programming Interfaces."

ISBN-13: 9781718502444
Publisher: No Starch Press





Thank you!

Connect with Me

[linkedin.com/in/PhillipWylie/](https://www.linkedin.com/in/PhillipWylie/)

twitter.com/PhillipWylie

Phillip.Wylie@CyCognito.com

CYCOGNITO