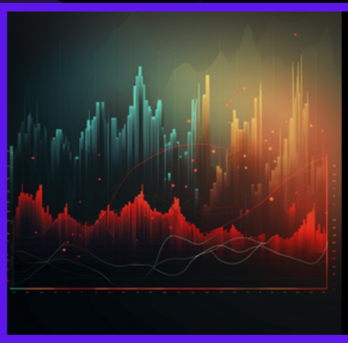
# THE BUG HUNTER'S METHODOLOGY LIVE

THE BUG HUNTER'S METHODOLOGY LIVE IS OUR FLAGSHIP TRAINING COURSE. IT IS DESIGNED FOR ASPIRING AND SEASONED OFFENSIVE SECURITY PROFESSIONALS, INCLUDING WEB APPLICATION SECURITY TESTERS, RED TEAMERS, AND BUG BOUNTY HUNTERS.

THE BUG HUNTER'S METHODOLOGY AIMS TO EQUIP YOU WITH THE LATEST TOOLS, TECHNIQUES, AND STRATEGIES, PLUS PROVIDE A DATA-DRIVEN METHODOLOGY ON HOW AND WHERE TO SEARCH FOR VULNERABILITIES THAT ARE CURRENTLY COMMON IN THE WILD.

THE EMPHASIS IS ON EXPERT TIPS, TIME-SAVING TRICKS, PRACTICAL Q&A'S, AUTOMATION STRATEGIES, VETTED RESOURCES, AND ENGAGEMENT VIA THE DEDICATED COMMUNITY ON DISCORD.

SHODAN++



ACQUISITIONS ++

CLOUD RECON++

AUTOMATED VULN DISCOVERY [CVEs]

LINKED DISCOVERY

JAVASCRIPT ANALYSIS

# THE BUG HUNTER'S METHODOLOGY LIVE SECTION 1 SYLLABUS

## GENERAL TOPICS

- PROJECT TRACKING FOR LARGE SCOPE ASSESSMENTS (RED TEAM AND BOUNTY)
- MENTAL HEALTH IN OFFENSIVE SECURITY
- TEMPLATING AND REPORTING
- TESTING ENV
- PROVIDERS
- TOOLS

## RECON TOPICS

- RECON CONCEPTS
- INTRODUCTION TO RECON
- RECON TECHNIQUES:
- ACQUISITIONS AND DOMAINS
- SHODAN
- ASN ANALYSIS
- CRUNCHBASE ++
- SSL RECON
- RECONGTP
- REVERSE WHOIS
- REVERSE DNS
- REVERSE IP
- DMARC ANALYSIS
- ADD AND ANALYTICS RELATIONSHIPS
- SUPPLY CHAIN INVESTIGATION AND SAAS
- GOOGLE-FU (TRADEMARK & PRIV POL)
- TLDS SCANNING
- 0365 ENUMERATION FOR APEX DOMAINS
- SUBDOMAIN SCRAPING
- SOURCES
- BRUTE FORCE
- WILDCARDS
- PERMUTATION SCANNING
- LINKED DISCOVERY
- WORDLISTS
- ADVANTAGEOUS SUBS (WAF BYPASS - ORIGINS)
- FAVICON ANALYSIS
- SUB SUB DOMAINS
- PORT SCANNING
- SCREENSHOTTING
- ESOTERIC TECHNIQUES
- SERVICE BRUTEFORCE

# THE BUG HUNTER'S METHODOLOGY LIVE SECTION 2 SYLLABUS

ARCANUM

## APPLICATION ANALYSIS TOPICS PT 1

- BEST RESOURCES TO FOLLOW TO STAY SHARP

RECON ADJACENT VULNERABILITY ANALYSIS

- CVE SCANNERS VS DYNAMIC ANALYSIS
- SUBTAKOVER
- S3 BUCKETS
- QUICK HITS (SWAGGER, .GIT, CONFIGS, PANEL ANALYSIS)

ANALYSIS CONCEPTS

- INDENTED USAGE (NOT HOLISTIC, CONTEXTUAL)
- ANALYSIS LAYERS
- APPLICATION LAYERS AS RELATED TO SUCCESS.
- TECH PROFILING
- THE BIG QUESTIONS
- CHANGE MONITORING

VULNERABILITY AUTOMATION

- MORE ON CVE AND DYNAMIC SCANNERS
- DEPENDENCIES
- EARLY RUNNING SO YOU CAN FOCUS ON MANUAL.
- SECRETS OF AUTOMATION KINGS

# THE BUG HUNTER'S METHODOLOGY LIVE SECTION 2 SYLLABUS

## APPLICATION ANALYSIS TOPICS PT 2

CONTENT DISCOVERY

- INTRO TO CD (WALKING, BRUTE/FUZZ, HISTORICAL, JS, SPIDER, MOBILE, PARAMS)
- IMPORTANCE OF WALKING THE APP
- BRUTEFORCE TOOLING
- BRUTEFORCE TOOLING LISTS:
  - BASED ON TECH
  - MAKE YOUR OWN (FROM-INSTALL, DOCKERHUB, TRIALS, FROM WORD ANALYSIS)
  - BEST BASE WORDLISTS
  - QUICK CONFIGS
  - API LISTS
- BRUTEFORCE TOOLING TIPS: RECURSION
- BRUTEFORCE TOOLING TIPS: SUB AS PATH
- BRUTEFORCE TOOLING TIPS: 403 BYPASS
- HISTORICAL CONTENT DISCOVERY
- SPIDERING
- MOBILE CONTENT DISCOVERY
- PARAMETER CONTENT DISCOVERY

APPLICATION ANALYSIS: JAVASCRIPT

- CHEATSHEETS (BETA)
- RAW ANALYSIS
- INLINE JS
- OBFUSCATED JS
- LAZY LOADED JS
- MOBILE JS ANALYSIS

# THE BUG HUNTER'S METHODOLOGY LIVE SECTION 2 SYLLABUS

## APPLICATION ANALYSIS TOPICS PT 3

APPLICATION ANALYSIS: THE BIG QUESTIONS

- HOW DOES THE APP PASS DATA?
- HOW/WHERE DOES THE APP TALK ABOUT USERS?
- DOES THE SITE HAVE MULTI-TENANCY OR USER LEVELS?
- DOES THE SITE HAVE A UNIQUE THREAT MODEL?
- HAS THERE BEEN PAST SECURITY RESEARCH & VULNS?
- HOW DOES THE APP HANDLE COMMON VULN CLASSES?
- WHERE DOES THE APP STORE DATA?

APPLICATION ANALYSIS: APPLICATION HEAT MAPPING

- COMMON ISSUE PLACE: UPLOAD FUNCTIONS
- COMMON ISSUE PLACE: CONTENT TYPE MULTIPART-FORM
- COMMON ISSUE PLACE: CONTENT TYPE XML / JSON
- COMMON ISSUE PLACE: ACCOUNT SECTION AND INTEGRATIONS
- COMMON ISSUE PLACE: ERRORS
- COMMON ISSUE PLACE: PATHS/URLS PASSED IN PARAMETERS
- COMMON ISSUES PLACE: CHATBOTS

APPLICATION ANALYSIS: WEB FUZZING & ANALYZING FUZZING RESULTS

- PARAMETERS AND PATHS (GENERIC FUZZING)
- REDUCING SIMILAR URLS
- DYNAMIC ONLY FUZZING
- FUZZING RESOURCES SSWLR - "SENSITIVE SECRETS WERE LEAKED RECENTLY"
- BACKSLASH POWERED SCANNER