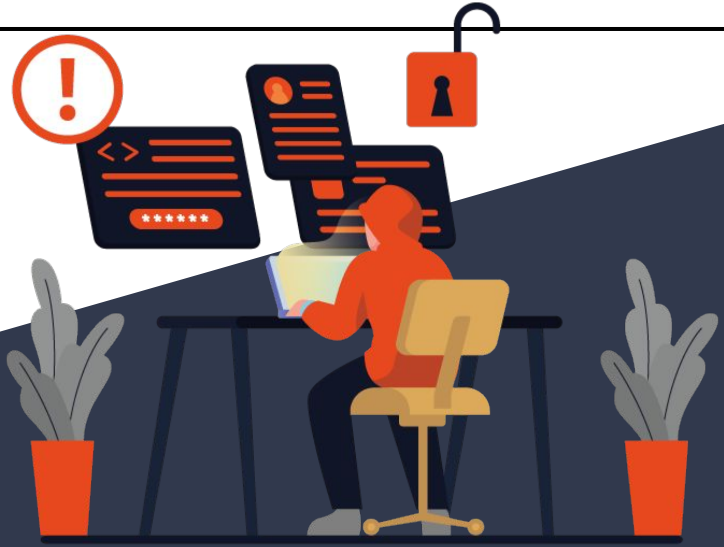
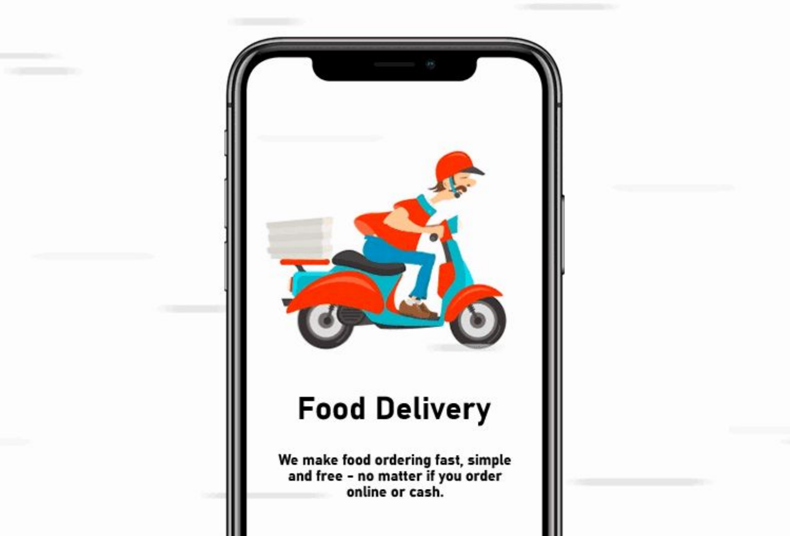
Introduction to Web Application Penetration Testing

Cybersecurity Club Session 2
10th March, 2023

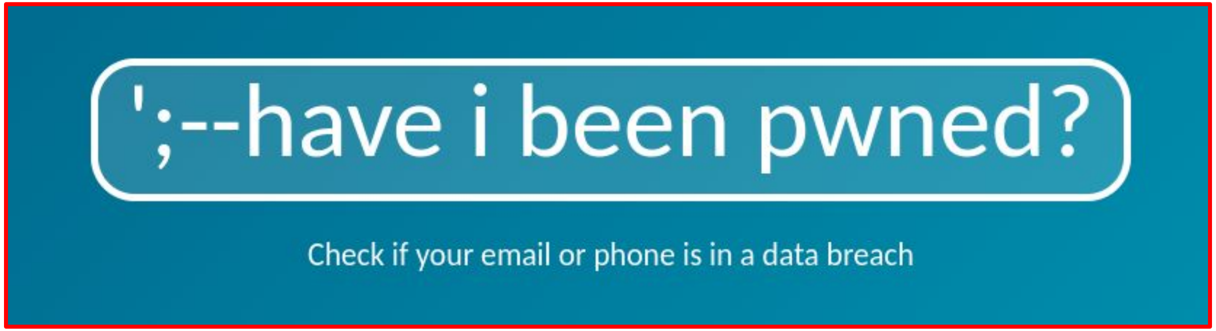


Today’s Digital Ecosystem


Food Delivery
We make food ordering fast, simple and free - no matter if you order online or cash.

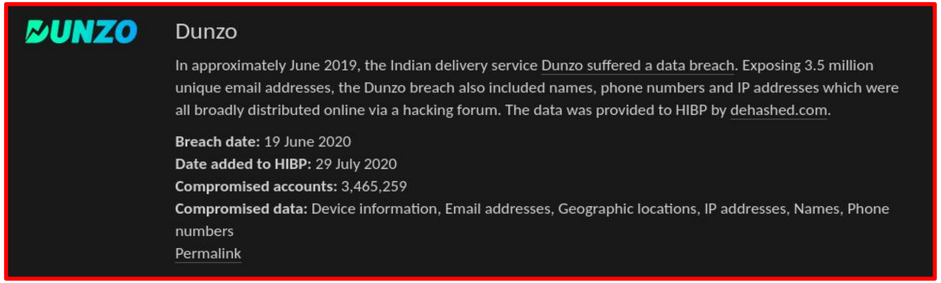
A large amount of data is being collected:

1. E-mail Addresses
2. Phone Numbers
3. GPS Coordinates
4. Passwords
5. IP Addresses, and lot more



';--have i been pwned?

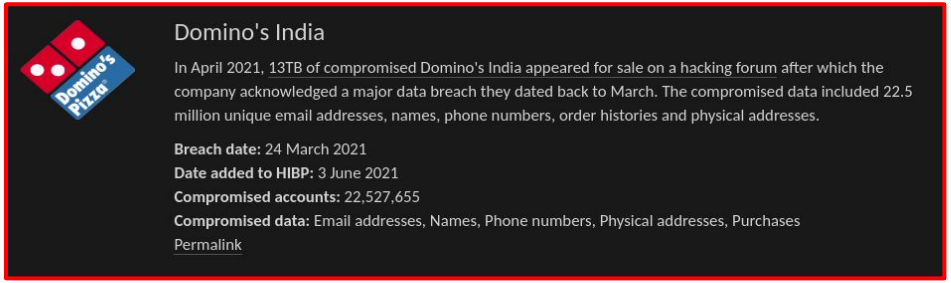
Check if your email or phone is in a data breach



Dunzo

In approximately June 2019, the Indian delivery service Dunzo suffered a data breach. Exposing 3.5 million unique email addresses, the Dunzo breach also included names, phone numbers and IP addresses which were all broadly distributed online via a hacking forum. The data was provided to HIBP by dehashed.com.

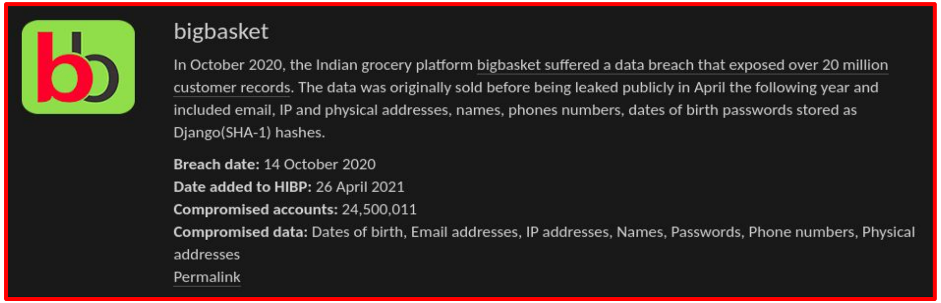
Breach date: 19 June 2020
Date added to HIBP: 29 July 2020
Compromised accounts: 3,465,259
Compromised data: Device information, Email addresses, Geographic locations, IP addresses, Names, Phone numbers
Permalink



Domino's India

In April 2021, 13TB of compromised Domino's India appeared for sale on a hacking forum after which the company acknowledged a major data breach they dated back to March. The compromised data included 22.5 million unique email addresses, names, phone numbers, order histories and physical addresses.

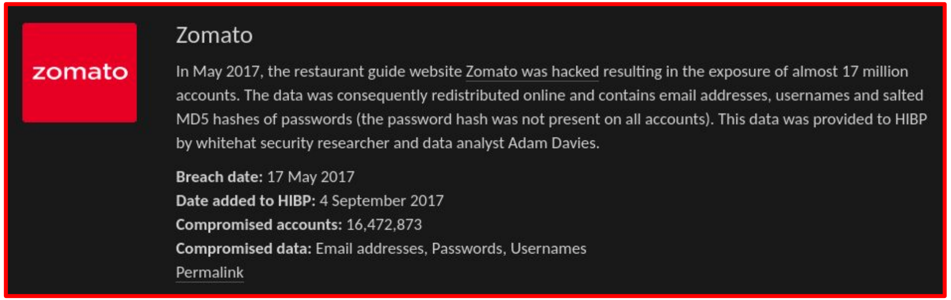
Breach date: 24 March 2021
Date added to HIBP: 3 June 2021
Compromised accounts: 22,527,655
Compromised data: Email addresses, Names, Phone numbers, Physical addresses, Purchases
Permalink



bigbasket

In October 2020, the Indian grocery platform bigbasket suffered a data breach that exposed over 20 million customer records. The data was originally sold before being leaked publicly in April the following year and included email, IP and physical addresses, names, phones numbers, dates of birth passwords stored as Django(SHA-1) hashes.

Breach date: 14 October 2020
Date added to HIBP: 26 April 2021
Compromised accounts: 24,500,011
Compromised data: Dates of birth, Email addresses, IP addresses, Names, Passwords, Phone numbers, Physical addresses
Permalink



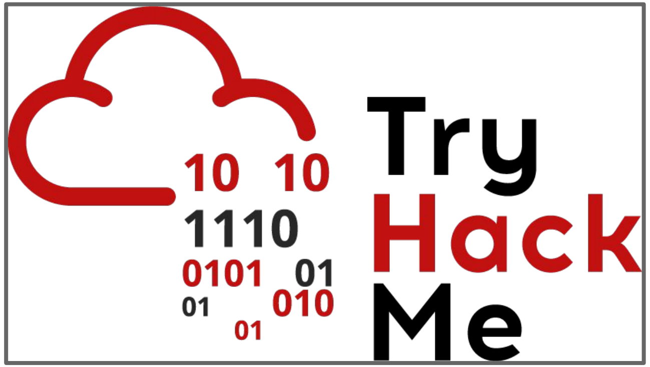
Zomato

In May 2017, the restaurant guide website Zomato was hacked resulting in the exposure of almost 17 million accounts. The data was consequently redistributed online and contains email addresses, usernames and salted MD5 hashes of passwords (the password hash was not present on all accounts). This data was provided to HIBP by whitehat security researcher and data analyst Adam Davies.

Breach date: 17 May 2017
Date added to HIBP: 4 September 2017
Compromised accounts: 16,472,873
Compromised data: Email addresses, Passwords, Usernames
Permalink

OWASP®

HACKTHEBOX

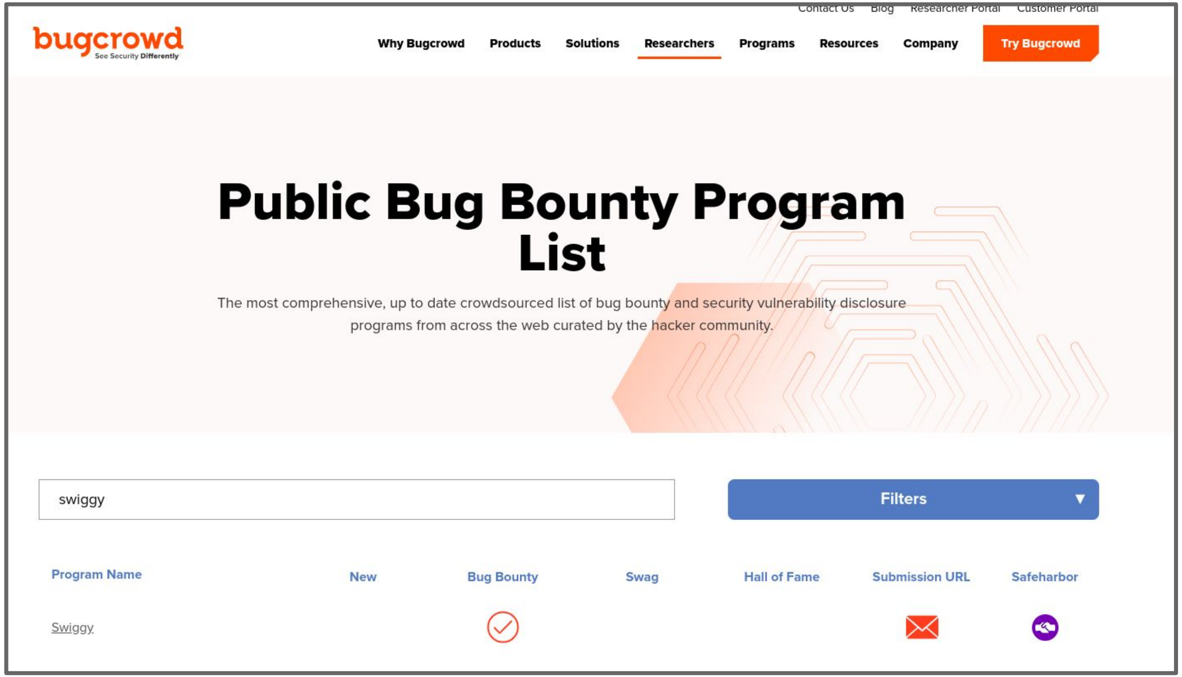

10 10
1110
0101 01
01 010
01
Try
Hack
Me

VULNHUB
VULNERABLE BY DESIGN

bugcrowd

hackerone

Synack

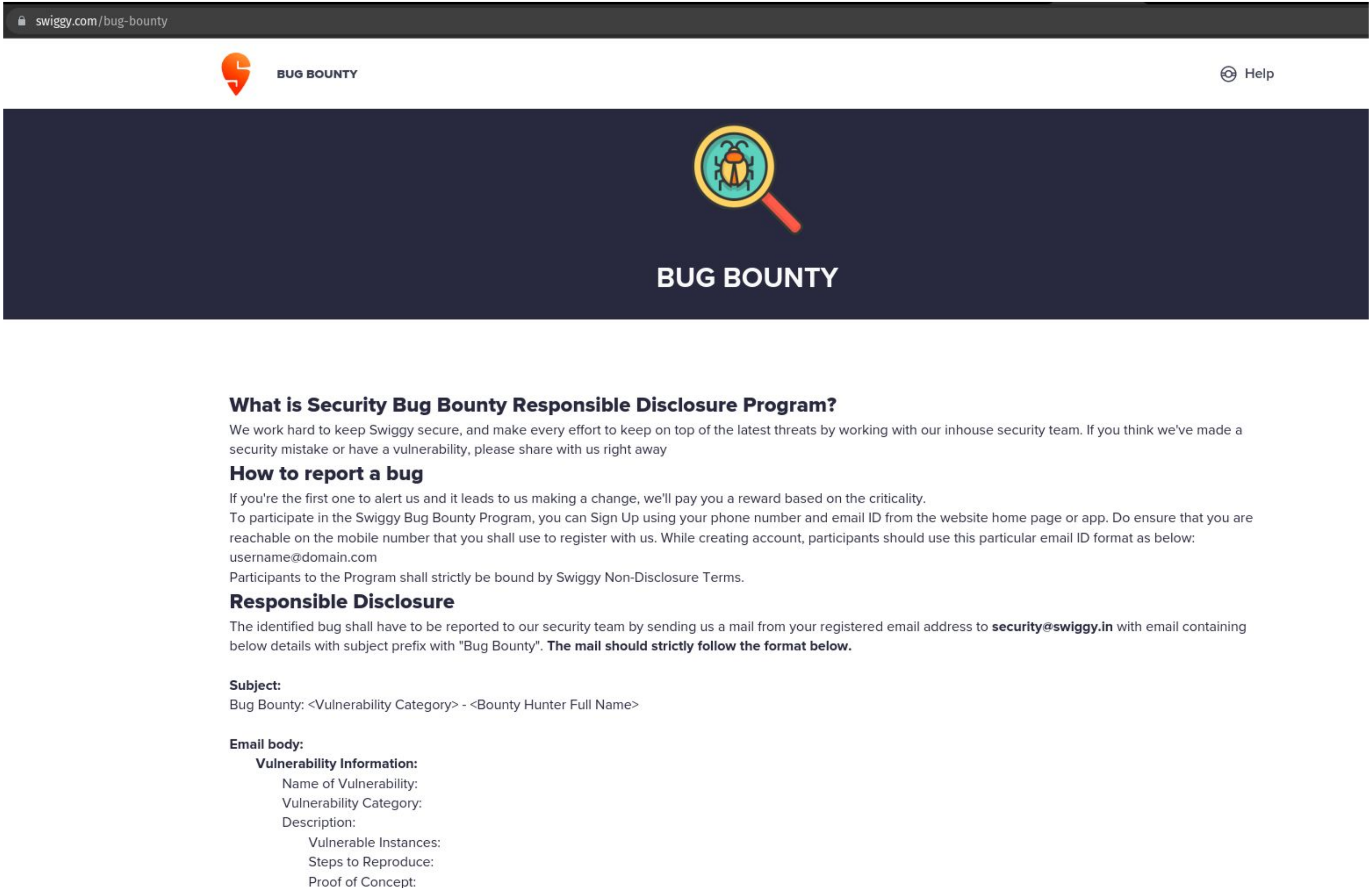


Public Bug Bounty Program List

The most comprehensive, up to date crowdsourced list of bug bounty and security vulnerability disclosure programs from across the web curated by the hacker community.

swiggy

Program Name	New	Bug Bounty	Swag	Hall of Fame	Submission URL	Safeharbor
Swiggy		✓			✉	●



BUG BOUNTY

What is Security Bug Bounty Responsible Disclosure Program?

We work hard to keep Swiggy secure, and make every effort to keep on top of the latest threats by working with our inhouse security team. If you think we've made a security mistake or have a vulnerability, please share with us right away

How to report a bug

If you're the first one to alert us and it leads to us making a change, we'll pay you a reward based on the criticality.

To participate in the Swiggy Bug Bounty Program, you can Sign Up using your phone number and email ID from the website home page or app. Do ensure that you are reachable on the mobile number that you shall use to register with us. While creating account, participants should use this particular email ID format as below:

username@domain.com

Participants to the Program shall strictly be bound by Swiggy Non-Disclosure Terms.

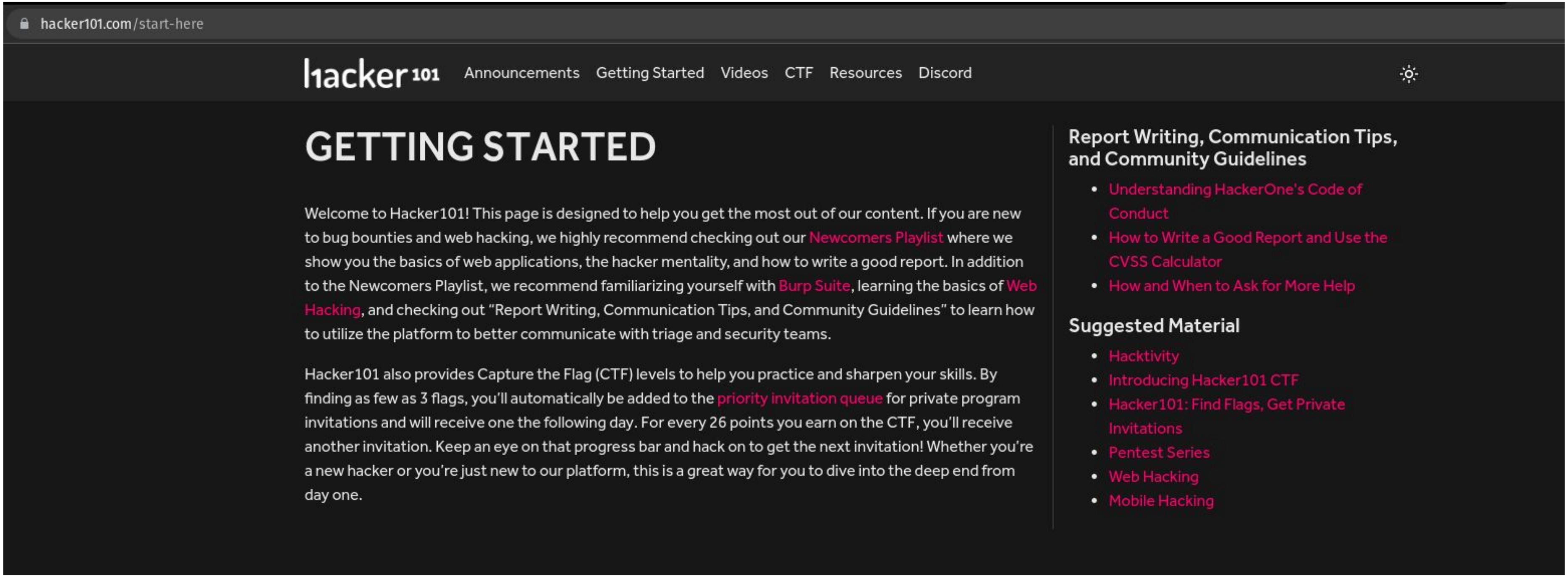
Responsible Disclosure

The identified bug shall have to be reported to our security team by sending us a mail from your registered email address to **security@swiggy.in** with email containing below details with subject prefix with "Bug Bounty". **The mail should strictly follow the format below.**

Subject:
Bug Bounty: <Vulnerability Category> - <Bounty Hunter Full Name>

Email body:

- **Vulnerability Information:**
  - Name of Vulnerability:
  - Vulnerability Category:
  - Description:
    - Vulnerable Instances:
    - Steps to Reproduce:
    - Proof of Concept:



GETTING STARTED

Welcome to Hacker101! This page is designed to help you get the most out of our content. If you are new to bug bounties and web hacking, we highly recommend checking out our Newcomers Playlist where we show you the basics of web applications, the hacker mentality, and how to write a good report. In addition to the Newcomers Playlist, we recommend familiarizing yourself with Burp Suite, learning the basics of Web Hacking, and checking out "Report Writing, Communication Tips, and Community Guidelines" to learn how to utilize the platform to better communicate with triage and security teams.

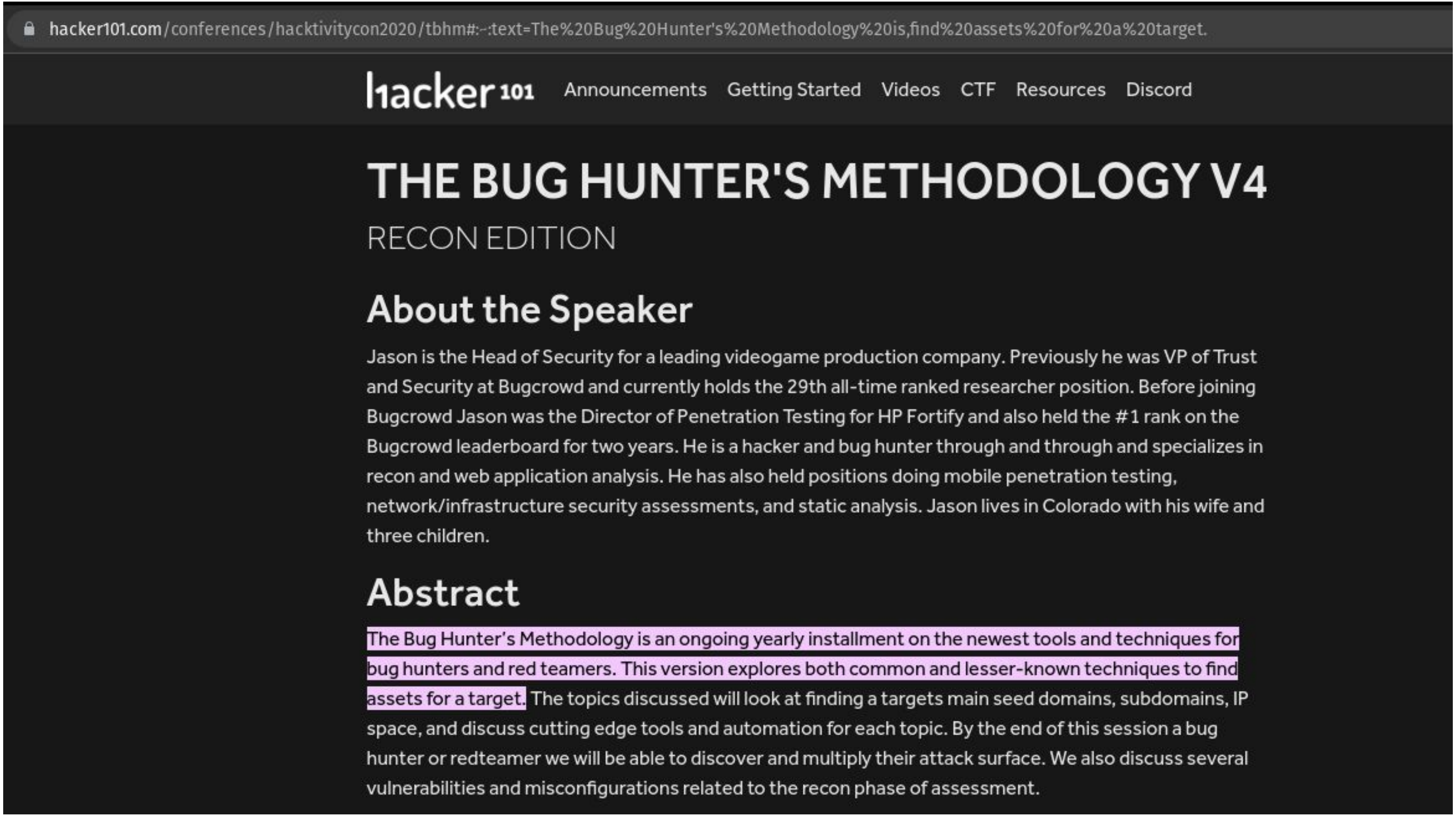
Hacker101 also provides Capture the Flag (CTF) levels to help you practice and sharpen your skills. By finding as few as 3 flags, you'll automatically be added to the priority invitation queue for private program invitations and will receive one the following day. For every 26 points you earn on the CTF, you'll receive another invitation. Keep an eye on that progress bar and hack on to get the next invitation! Whether you're a new hacker or you're just new to our platform, this is a great way for you to dive into the deep end from day one.

Report Writing, Communication Tips, and Community Guidelines

- Understanding HackerOne's Code of Conduct
- How to Write a Good Report and Use the CVSS Calculator
- How and When to Ask for More Help

Suggested Material

- Hacktivity
- Introducing Hacker101 CTF
- Hacker101: Find Flags, Get Private Invitations
- Pentest Series
- Web Hacking
- Mobile Hacking


hacker101.com/conferences/hacktivitycon2020/tbhm#:~:text=The%20Bug%20Hunter's%20Methodology%20is,find%20assets%20for%20a%20target.
hacker101
Announcements
Getting Started
Videos
CTF
Resources
Discord

THE BUG HUNTER'S METHODOLOGY V4

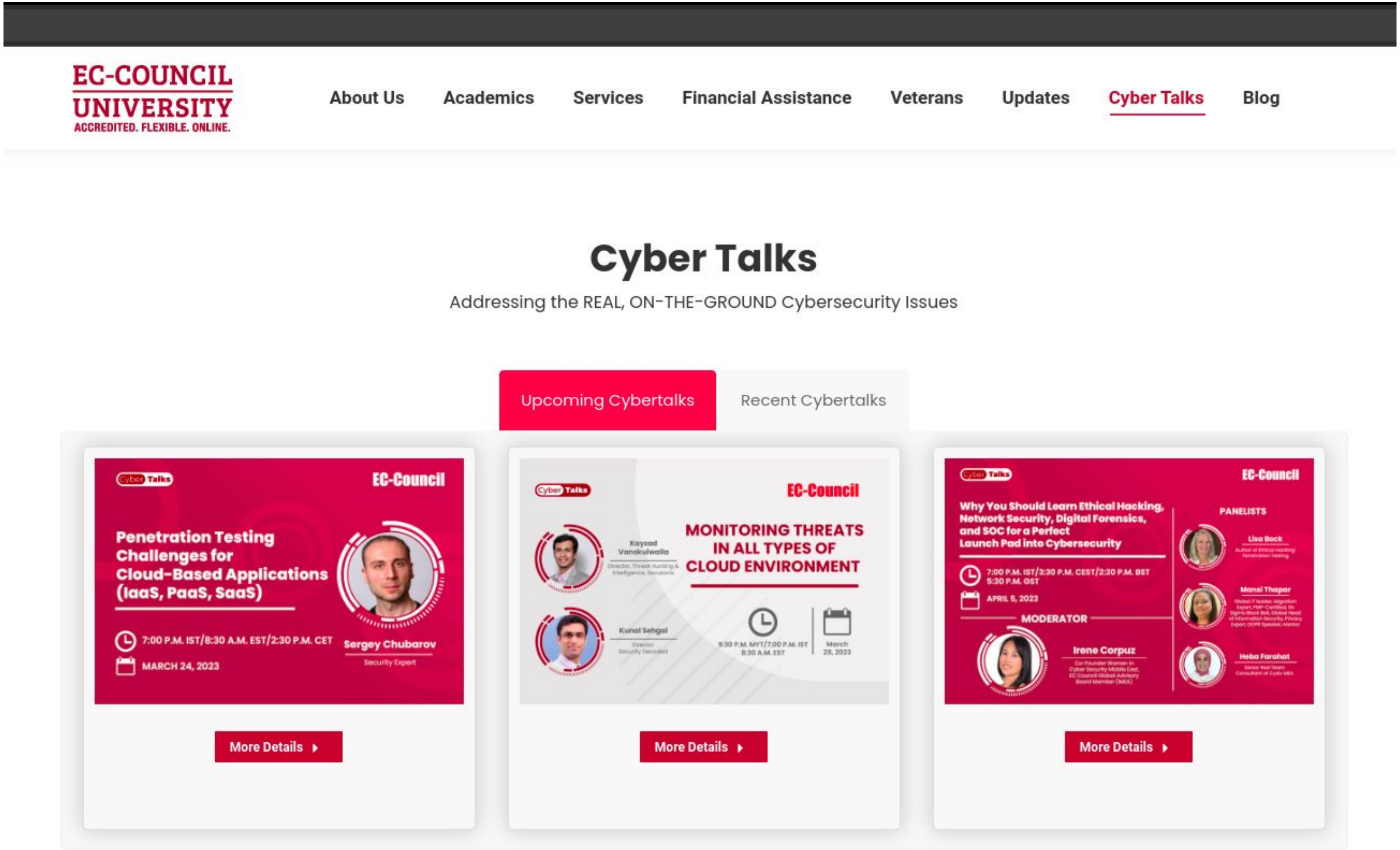
RECON EDITION

About the Speaker

Jason is the Head of Security for a leading videogame production company. Previously he was VP of Trust and Security at Bugcrowd and currently holds the 29th all-time ranked researcher position. Before joining Bugcrowd Jason was the Director of Penetration Testing for HP Fortify and also held the #1 rank on the Bugcrowd leaderboard for two years. He is a hacker and bug hunter through and through and specializes in recon and web application analysis. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason lives in Colorado with his wife and three children.

Abstract

The Bug Hunter's Methodology is an ongoing yearly installment on the newest tools and techniques for bug hunters and red teamers. This version explores both common and lesser-known techniques to find assets for a target. The topics discussed will look at finding a targets main seed domains, subdomains, IP space, and discuss cutting edge tools and automation for each topic. By the end of this session a bug hunter or redteamer we will be able to discover and multiply their attack surface. We also discuss several vulnerabilities and misconfigurations related to the recon phase of assessment.



EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

About Us | Academics | Services | Financial Assistance | Veterans | Updates | Cyber Talks | Blog

Cyber Talks

Addressing the REAL, ON-THE-GROUND Cybersecurity Issues

Upcoming Cybertalks | Recent Cybertalks

Cyber Talks
EC-Council

Penetration Testing Challenges for Cloud-Based Applications (IaaS, PaaS, SaaS)

7:00 P.M. IST/8:30 A.M. EST/2:30 P.M. CET
MARCH 24, 2023

Sergey Chubarov
Security Expert

More Details ▸

Cyber Talks
EC-Council

MONITORING THREATS IN ALL TYPES OF CLOUD ENVIRONMENT

Kayzad Vanskuiwalla
Director, Threat Hunting & Intelligence, Securonix

Kunal Sehgal
Director
Security Decoded

9:30 P.M. MYT/7:00 P.M. IST
8:30 A.M. EST

March 28, 2023

More Details ▸

Cyber Talks
EC-Council

Why You Should Learn Ethical Hacking, Network Security, Digital Forensics, and SOC for a Perfect Launch Pad into Cybersecurity

7:00 P.M. IST/3:30 P.M. CEST/2:30 P.M. BST
5:30 P.M. GST
APRIL 5, 2023

MODERATOR

Irene Corpuz
Co-Founder Women in Cyber Security Middle East; EC Council Global Advisory Board Member (MEA)

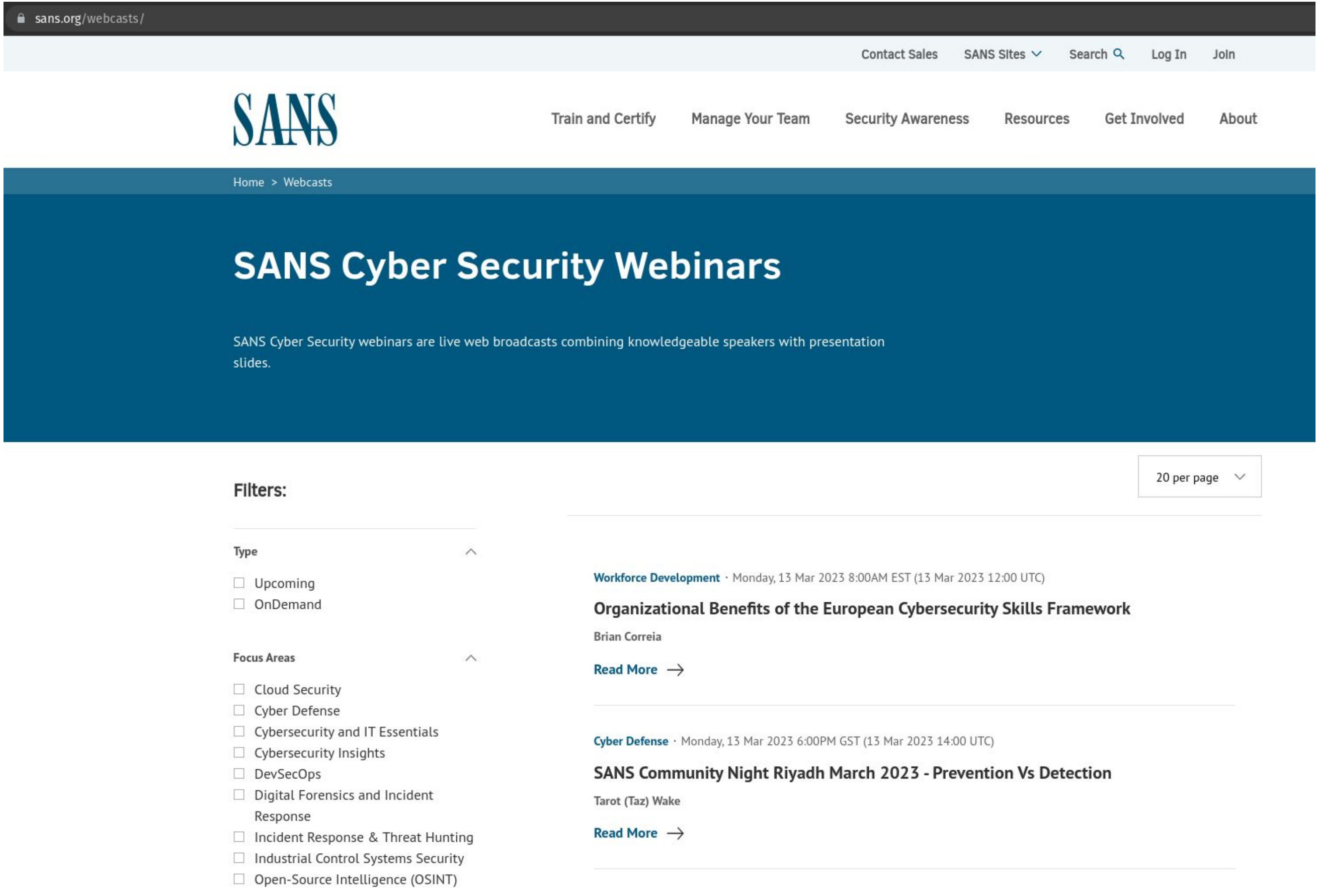
PANELISTS

Lisa Bock
Author of Ethical Hacking Penetration Testing

Mansi Thapar
Global IT leader, Migration Expert, PMP-Certified, Six Sigma Black Belt, Global Head of Information Security, Privacy Expert, GDPR Speaker, Mentor

Heba Farahat
Senior Red Team Consultant at Cyber MEA

More Details ▸



SANS Cyber Security Webinars

SANS Cyber Security webinars are live web broadcasts combining knowledgeable speakers with presentation slides.

20 per page

Filters:

Type

□ Upcoming
□ OnDemand

Focus Areas

□ Cloud Security
□ Cyber Defense
□ Cybersecurity and IT Essentials
□ Cybersecurity Insights
□ DevSecOps
□ Digital Forensics and Incident Response
□ Incident Response & Threat Hunting
□ Industrial Control Systems Security
□ Open-Source Intelligence (OSINT)

Workforce Development · Monday, 13 Mar 2023 8:00AM EST (13 Mar 2023 12:00 UTC)

Organizational Benefits of the European Cybersecurity Skills Framework

Brian Correia

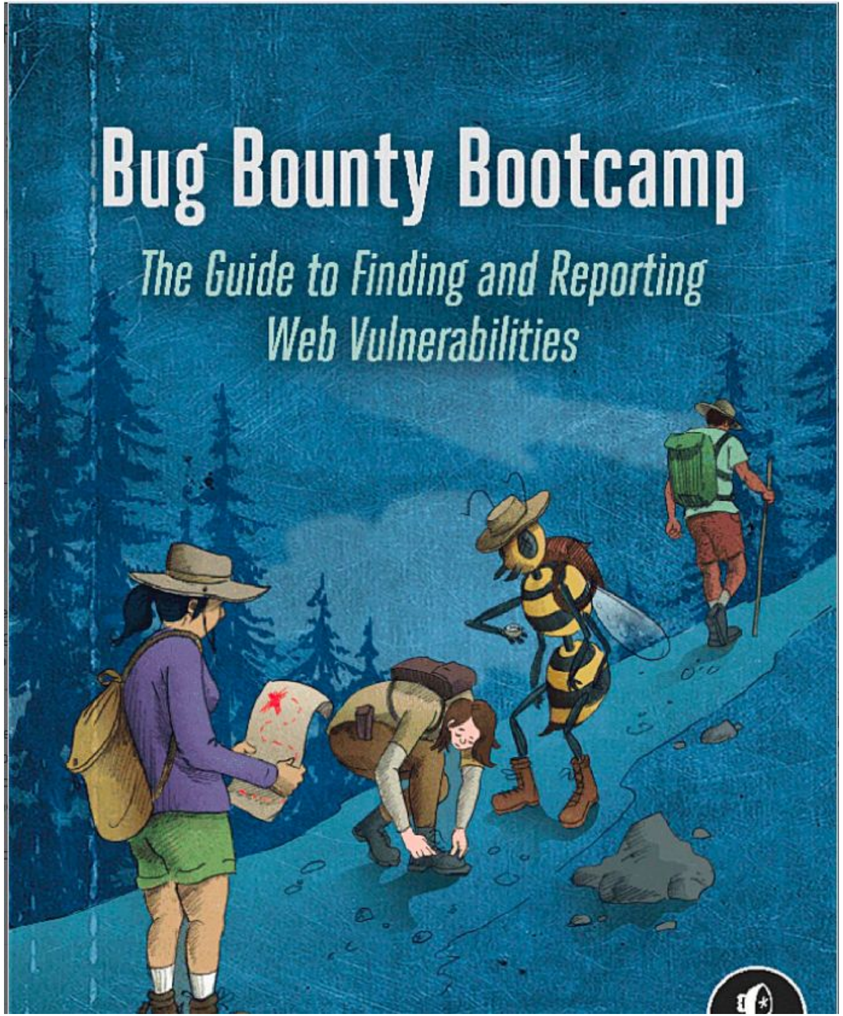
Read More →

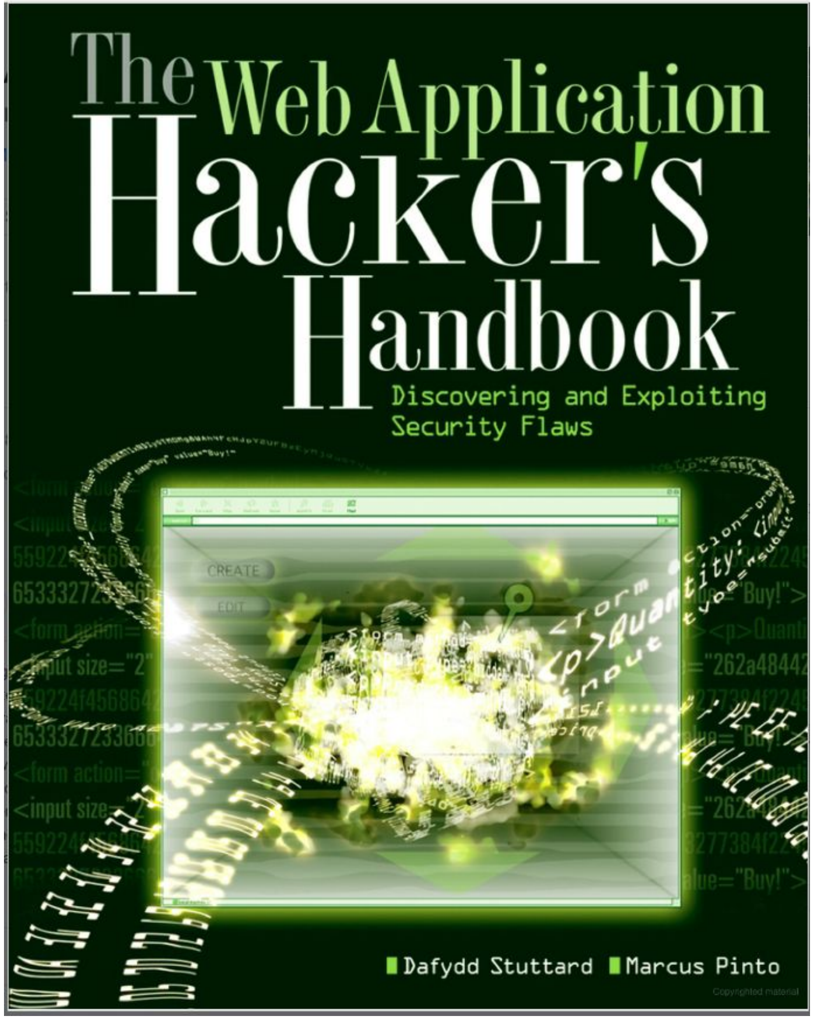
Cyber Defense · Monday, 13 Mar 2023 6:00PM GST (13 Mar 2023 14:00 UTC)

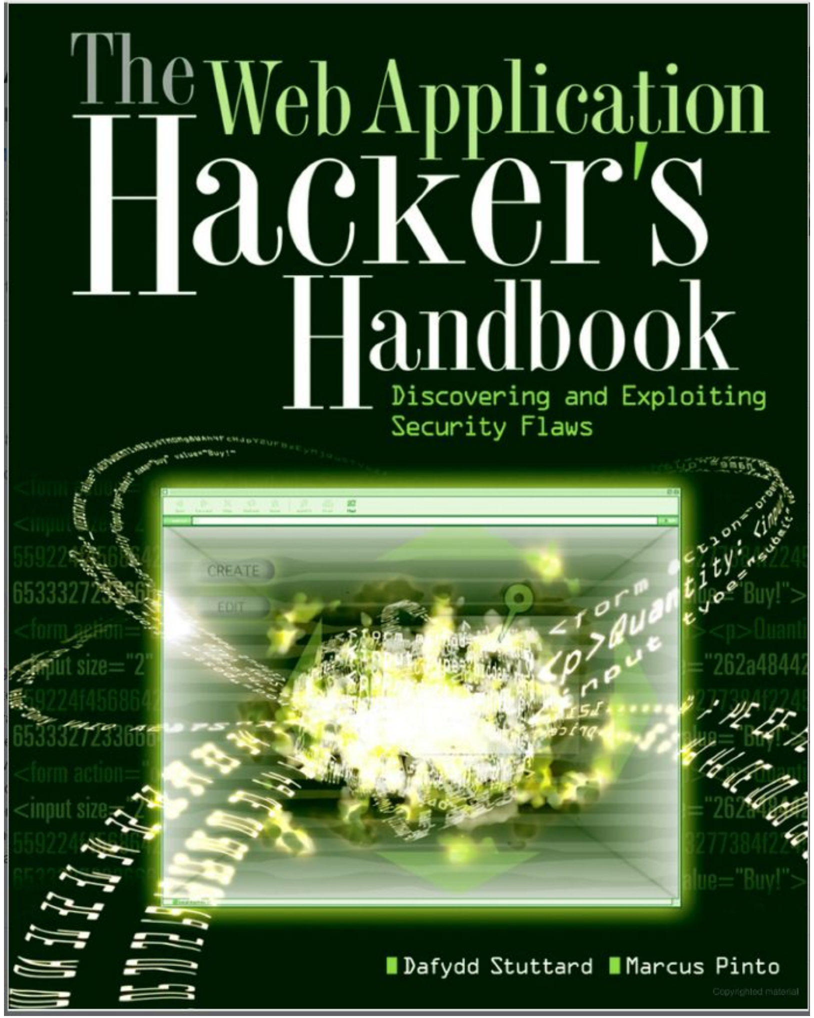
SANS Community Night Riyadh March 2023 - Prevention Vs Detection

Tarot (Taz) Wake

Read More →


Bug Bounty Bootcamp
The Guide to Finding and Reporting Web Vulnerabilities


The Web Application Hacker's Handbook
Discovering and Exploiting Security Flaws
Dafydd Stuttard
Marcus Pinto
CREATE
EDIT
Copyrighted material

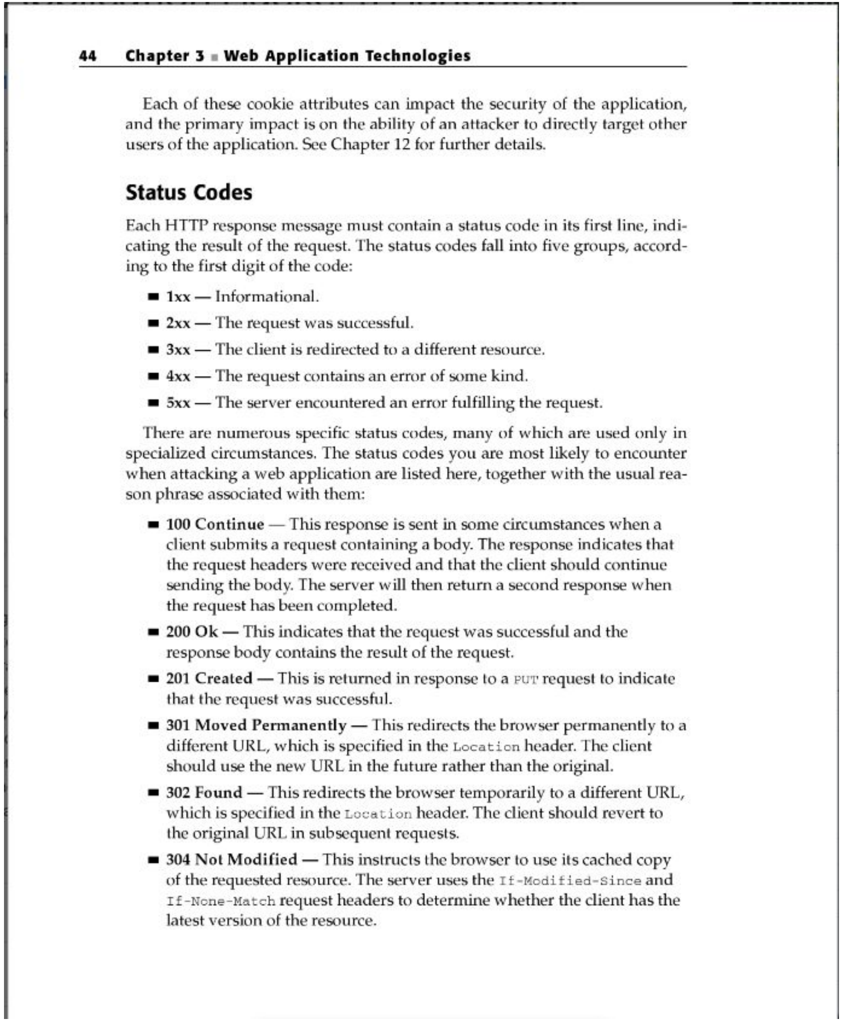


The Web Application Hacker's Handbook

Discovering and Exploiting Security Flaws

■ Dafydd Stuttard ■ Marcus Pinto

Copyrighted material



Each of these cookie attributes can impact the security of the application, and the primary impact is on the ability of an attacker to directly target other users of the application. See Chapter 12 for further details.

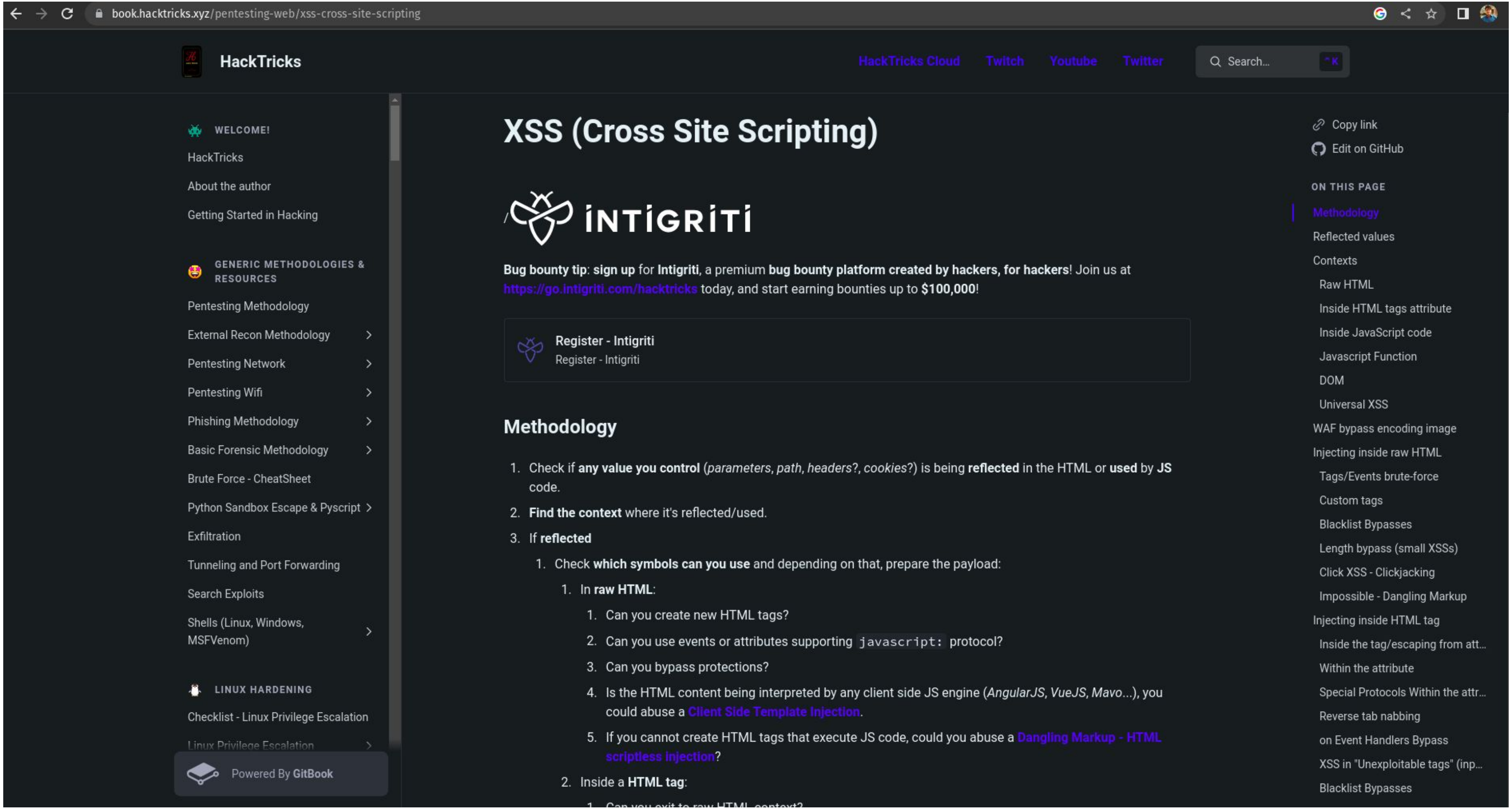
Status Codes

Each HTTP response message must contain a status code in its first line, indicating the result of the request. The status codes fall into five groups, according to the first digit of the code:

- **1xx** — Informational.
- **2xx** — The request was successful.
- **3xx** — The client is redirected to a different resource.
- **4xx** — The request contains an error of some kind.
- **5xx** — The server encountered an error fulfilling the request.

There are numerous specific status codes, many of which are used only in specialized circumstances. The status codes you are most likely to encounter when attacking a web application are listed here, together with the usual reason phrase associated with them:

- **100 Continue** — This response is sent in some circumstances when a client submits a request containing a body. The response indicates that the request headers were received and that the client should continue sending the body. The server will then return a second response when the request has been completed.
- **200 Ok —** This indicates that the request was successful and the response body contains the result of the request.
- **201 Created —** This is returned in response to a `PUT` request to indicate that the request was successful.
- **301 Moved Permanently —** This redirects the browser permanently to a different URL, which is specified in the `Location` header. The client should use the new URL in the future rather than the original.
- **302 Found —** This redirects the browser temporarily to a different URL, which is specified in the `Location` header. The client should revert to the original URL in subsequent requests.
- **304 Not Modified —** This instructs the browser to use its cached copy of the requested resource. The server uses the `If-Modified-Since` and `If-None-Match` request headers to determine whether the client has the latest version of the resource.



XSS (Cross Site Scripting)

Methodology

1. Check if **any value you control** (*parameters*, *path*, *headers*?, *cookies*?) is being **reflected** in the HTML or **used** by **JS** code.
2. **Find the context** where it's reflected/used.
3. If **reflected**
   1. Check **which symbols can you use** and depending on that, prepare the payload:
      1. In **raw HTML**:
         1. Can you create new HTML tags?
         2. Can you use events or attributes supporting `javascript:` protocol?
         3. Can you bypass protections?
         4. Is the HTML content being interpreted by any client side JS engine (*AngularJS*, *VueJS*, *Mavo*...), you could abuse a Client Side Template Injection.
         5. If you cannot create HTML tags that execute JS code, could you abuse a Dangling Markup - HTML scriptless injection?
      2. Inside a **HTML tag**:
         1. Can you exit to raw HTML context?