Microsoft Security

Cloudy with a Chance of SSRF

Vulnerability Trends & Techniques
GrrCon 2023

Dr. Jared DeMott
Michael Fowl

Microsoft Security

Introduction

Dr. Jared DeMott
Microsoft Security Response Center

- Manager of Cloud Vulnerability and Mitigations Team
- Former NSA, MSU, Entrepreneur, Mentor, frequent Speaker and Trainer
- Love spending time with family and friends
  - Both kids are in Marching band, so we do a lot of that in the fall :)
  - Married 25 years

Microsoft Security

Introduction

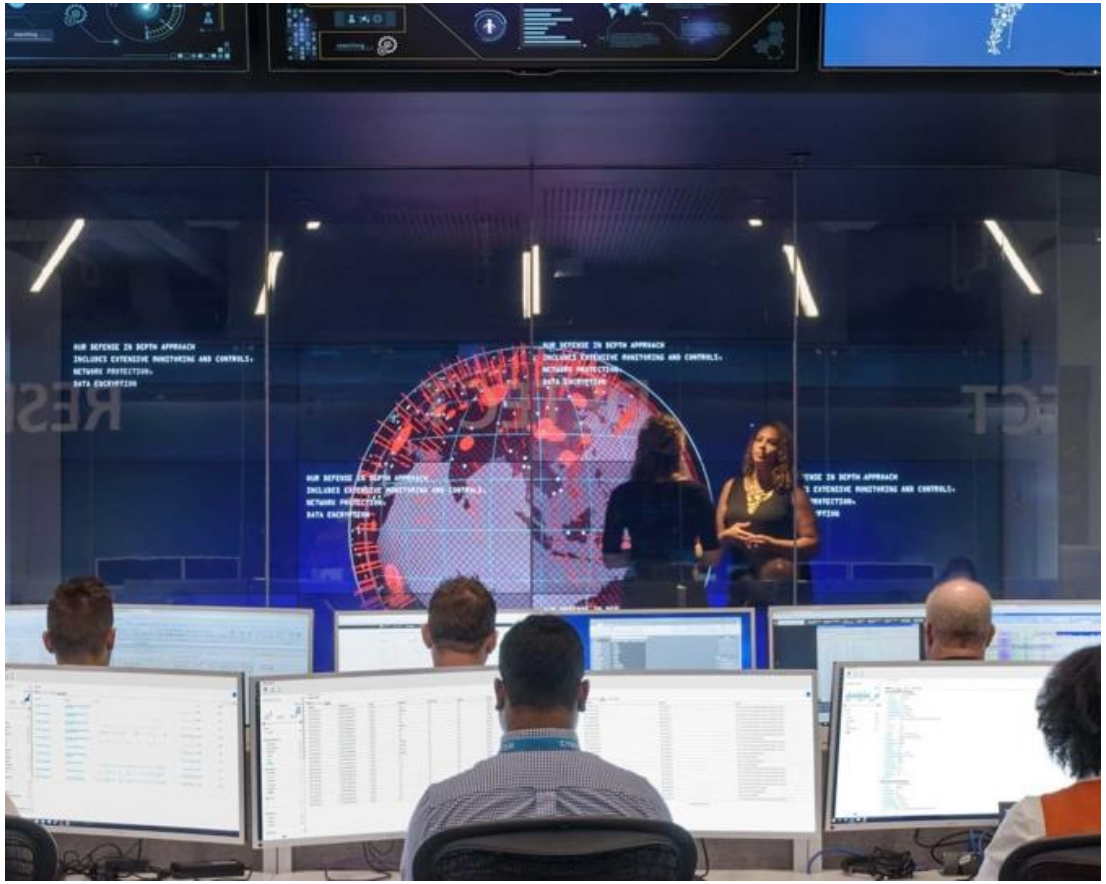
Michael Fowl
Microsoft Security Response Center

- Senior Security Researcher Cloud Vulnerability and Mitigations Team
- Enjoys using an adversarial mindset to achieve mission goals and solve hard security problems
- Always likes discussions about topics like:
  - Bug bounty hunting
  - Adversary simulation
  - Exploit chains
  - Leveraging AI

Microsoft Bounty Programs

All the SDLC Things

Internal SOC, Redteam, TI, …



External Collaboration

Microsoft Bounty Programs

July 01, 2022 to June 30, 2023

$13.8M

in bounty rewards

17

Bounty programs

1,180

Eligible vulnerability reports

345

Researchers awarded

$200K

Biggest reward

Platform

Cloud

A Detailed Look at Cloud Bounty Growth

92%

140%

500%

AZURE SECURITY LAB SCENARIO CHALLENGE

https://www.microsoft.com/en-us/msrc/bounty

In Azure Security Lab scenario challenges, we provide more content and resources to better arm security researchers with the tools needed to research high-impact vulnerabilities in the cloud. Please see ongoing challenges on the Azure Security Lab page.

HIGH IMPACT SCENARIOS

Target	Scenario	Award
Key Vault	Compromise logging or auditing keys	+50%
	Leaking keys	+40%
	Editing or deleting keys	+30%
Azure Kubernetes Service	All bounty eligible submissions targeting this service	+20%

In all scenarios, please follow the Azure Research Rules of Engagement to ensure your research does not harm customer data, privacy, or service availability. If in doubt, please contact bounty@microsoft.com.

GENERAL AWARDS

Security Impact	Report Quality	Severity			
		Critical	*Important*	*Moderate*	*Low*
Remote Code Execution	High Medium Low	$40,000 $20,000 $10,000	$30,000 $20,000 $10,000	$0	$0
Elevation of Privilege	High Medium Low	$40,000 $30,000 $20,000	$10,000 $4,000 $2,000	$0	$0
Information Disclosure	High Medium Low	$12,000 $6,000 $4,500	$7,500 $3,000 $1,500	$0	$0

https://msrc.microsoft.com/report/vulnerability/new

Microsoft MSRC | Researcher Portal

Report a security vulnerability

Please fill out the following form if you have found a security related bug in a Microsoft product. Fields marked with an asterisk (*) are required.

Impact

Select the type of the potential issue you have discovered, and the product it impacts.

Proposed security impact *

Select option

Products *

Select option

Version/Build

99999.1.amd64fre.fs5_release.180914

Proof of concept

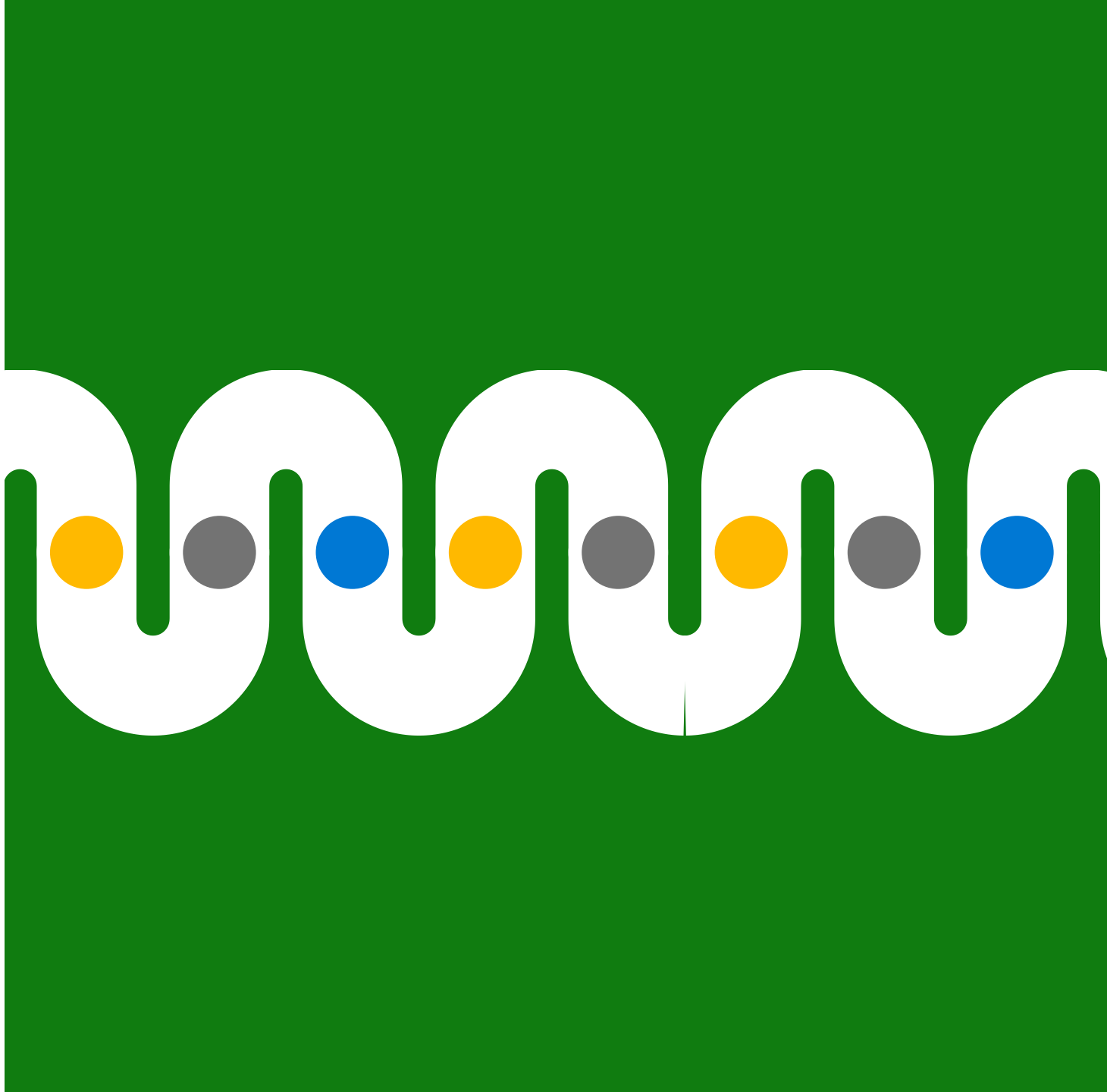
Clear, reproducible steps will help us validate this issue as quickly as possible. Reports with a clear proof of concept achieve higher report quality ratings. Visit the Microsoft Bounty page for more guidance.

Submit

Case Flow


Triage
Does it meet the definition of a vulnerability?
Case
If accepted, assign a case manager
Send case number to the researcher
Review
Engineering team attempts to reproduce
Follow up questions may be sent to researcher
If reproduced, send confirmation to the researcher
Develop
Product engineers work to develop a fix
Cases that qualify for bounty are assessed for reward
Release
Prepare build for product release
Coordinate release announcements
Assign CVE if applicable
Complete
Fix has been deployed
CVE published
Acknowledgement published, as appropriate

Most Common Web Vulnerabilities



Most Common Issues last Year (Aug 22 – Aug 23)

Our Top 5 Root Causes in OLS:

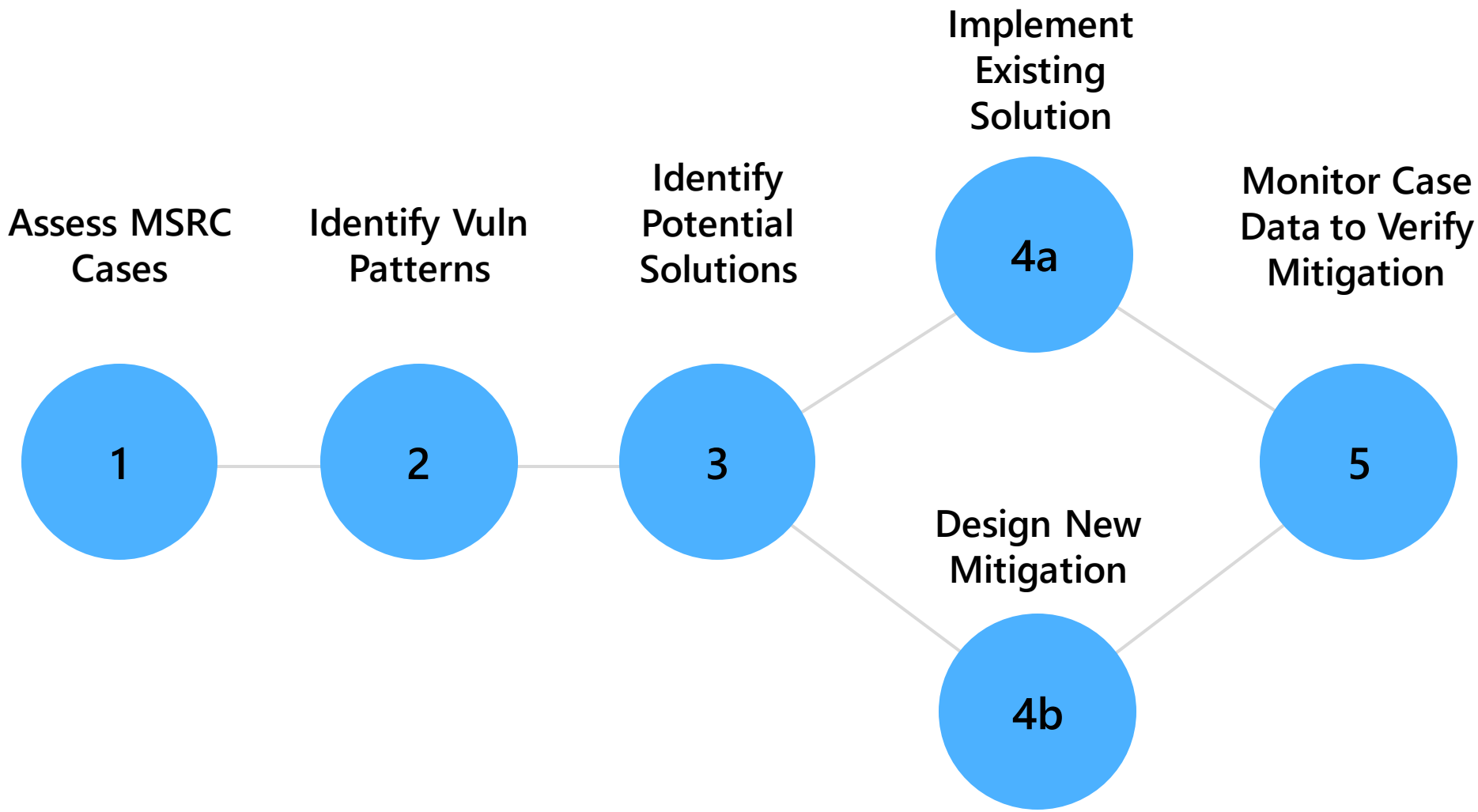
- Cross-Site Scripting (XSS)
- CSRF/SSRF
- Improper Access Control
- Improper Authorization
- Code **Injection/Command** Injection

Example:

- Fields in Dashboards
- Request that touches our internals
- **Missing** authentication on an **API** endpoint
- **AuthZ** data leak, or a role that can do something it shouldn't be able to
- Sandbox or workflow type execution

Mitigation Strategies

Mitigating Vuln Patterns



Why Focus on SSRF?

- Every cloud service provider has SSRF concerns
  - Google - Researcher finds SSRF bug in internal Google Cloud project, nabs $10,000 bounty | The Daily Swig (portswigger.net)
  - AWS - Steal EC2 Metadata Credentials via SSRF - Hacking The Cloud
  - Oracle - Oracle Server Side Request Forgery (SSRF) | Orca Security
- Substantial impact
  - Access to internal resources, bypassing security controls, performing malicious actions, token disclosure, chained with other vulnerabilities…

Server-side Request Forgery (SSRF)

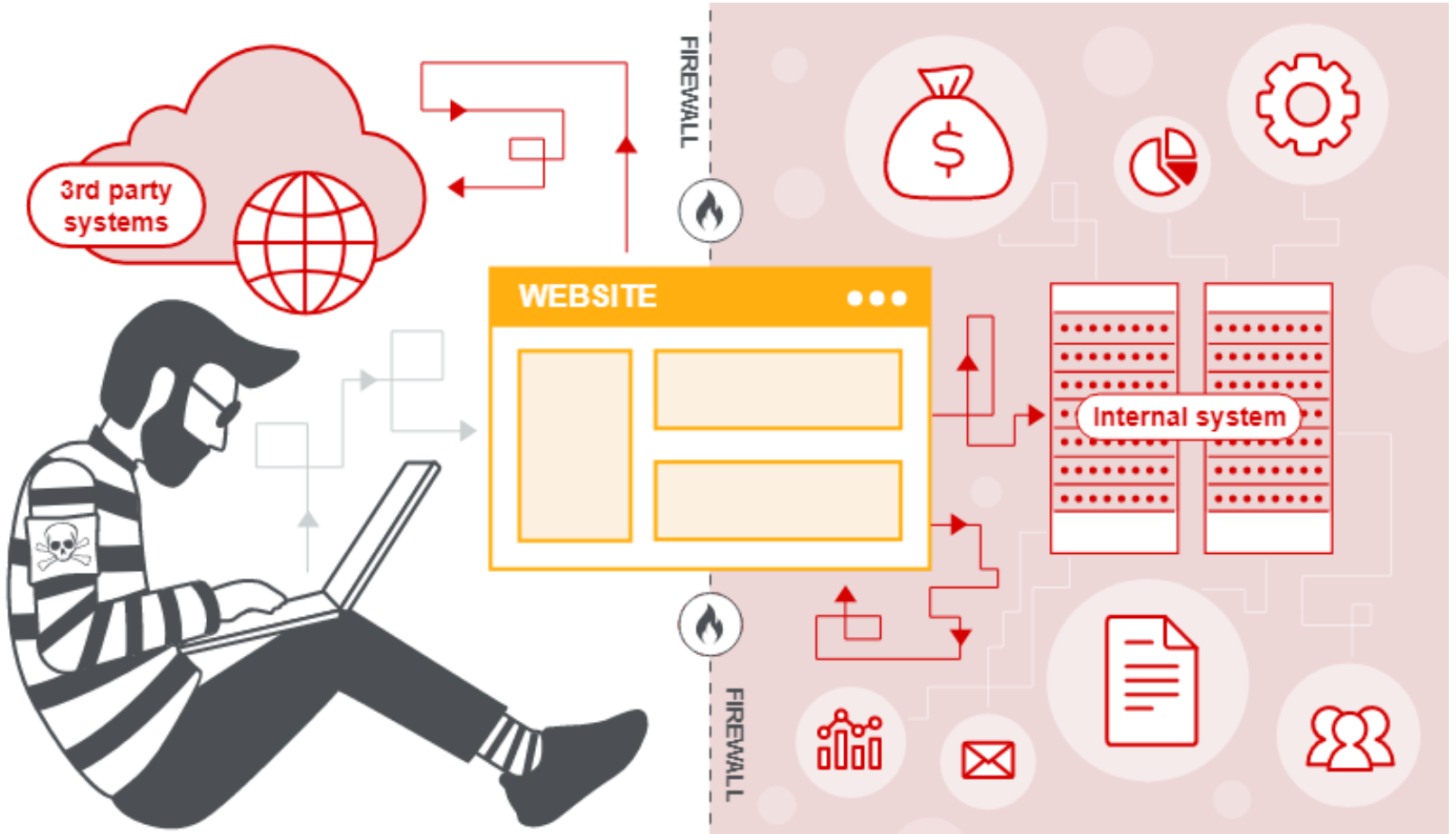


Image from https://portswigger.net/web-security/ssrf

Demonstrating Impact Struggles

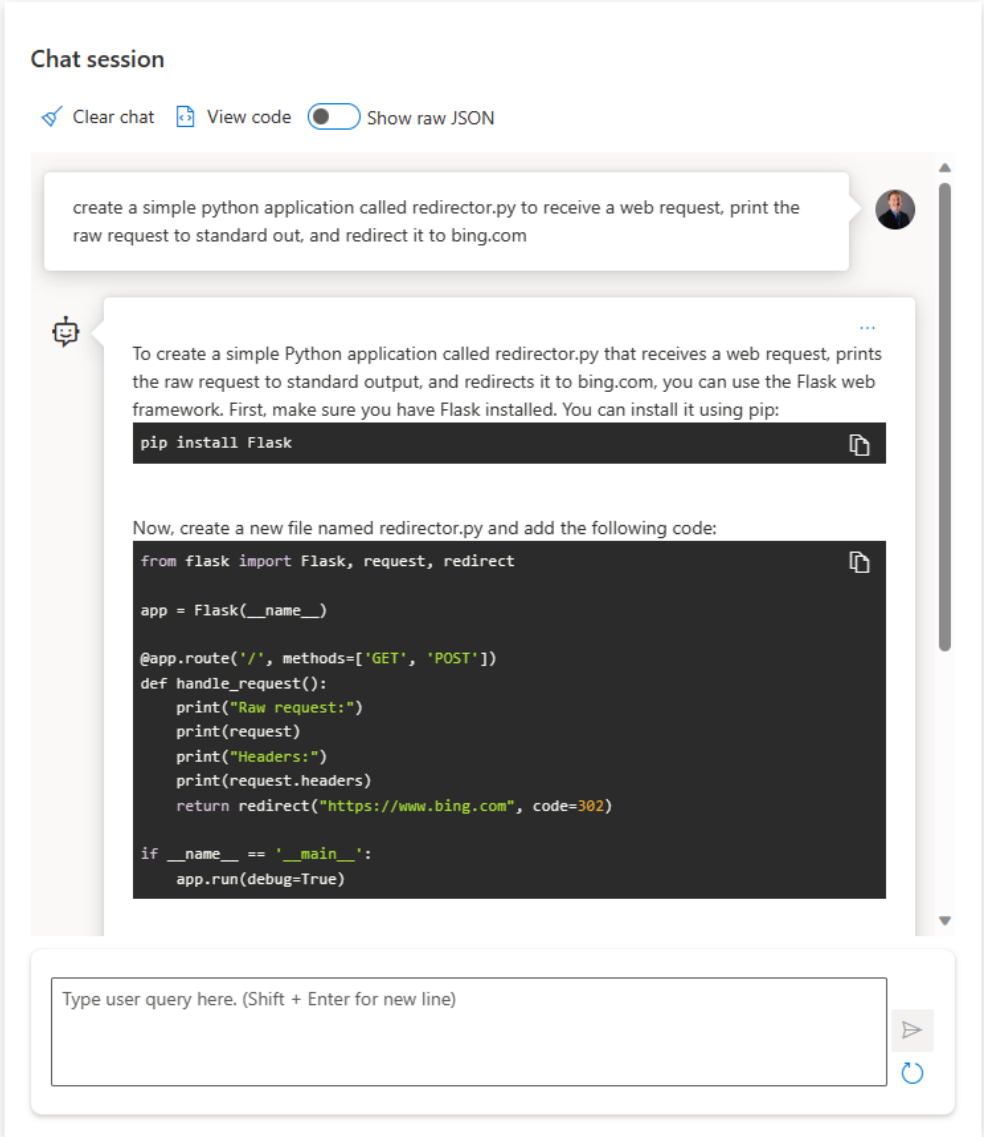
- MSRC triages lots of submissions
- We do care about every SSRF
  - Impact analysis, variant hunting, etc.
- SSRF submissions often lack impact
  - "I found a CRITICAL SSRF that tries to get an image from collaborator..."
  - You can often do better than port scanning
- High quality report helps triage
  - More impact = higher severity
  - Include a video recording, etc.
  - https://microsoft.com/en-us/msrc/bounty-example-report-submission

Bag of Tricks: What is helpful?

- Knowledge
  - Adversary mindset
  - Techniques
  - Doing vs. observing
- Interception Proxy
  - BurpSuite/MitM Proxy
  - Collaborator is limited
- Custom Web Server
  - Redirect requests/Modify response
- Custom DNS Server
  - Manipulate records

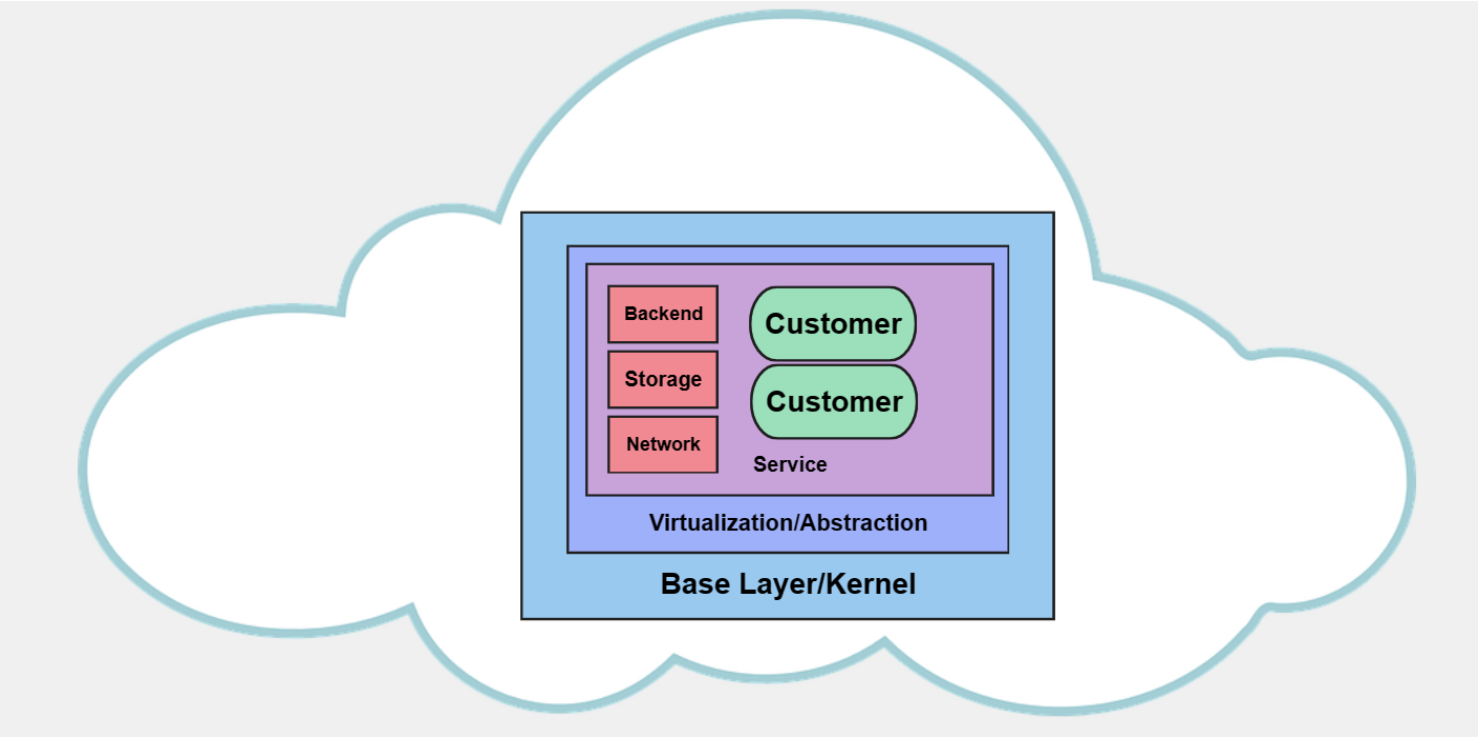
SSRF Training Dojo

- Practice like you hunt
  - Understanding
  - Experience
    - Recognize patterns
- Azure OpenAI/GitHub Copilot
  - Writing code has never been easier!
  - Labs written by an LLM
- Link
  - https://github.com/microsoft/MSRC-Security-Research/tree/master/presentations/2023_09_GrrCON/ssrf_dojo/



Modern Cloud Architecture: Security Boundaries

- Intent
  - Not a comprehensive architecture
  - Is where vulnerabilities often arise
- Base Layers/Plumbing
  - "Just somebody's computer..."
  - Cloud "Kernel"
- Abstraction Layers
  - Virtualization
  - Service Fabric/k8s/Etc.



Modern Cloud Architecture: Security Boundaries

- Control Plane/Data Plane
  - Pivot from data to control
    - https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/control-plane-and-data-plane
- Network Isolation/Injection
  - Firewalls, Proxy, Segmentation
  - VNET
    - Route Tables, ARP, DNS
- Micro Services
  - State/Timing Issues
    - Service chains can have security gaps

SSRF Technique: Reaching Sensitive Endpoints

- AWS
  - http://169.254.169.254 (IMDSv1)
- Google
  - http://169.254.169.254
  - http://metadata.google.internal
- Azure
  - http://169.254.169.254/metadata (IMDS)
  - http://168.63.129.16/machine/?comp=goalstate (Wireserver: CVE-2021-27075)
- Better list (Including required headers)
  - https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery/cloud-ssrf

SSRF Technique: Reaching Sensitive Endpoints

- Loopback
  - Common ports, services
- Know your RFCs
  - RFC 1918
    - 10.0.0.0–10.255.255.255 (10/8 prefix)
    - 172.16.0.0–172.31.255.255 (172.16/12 prefix)
    - 192.168.0.0–192.168.255.255 (192.168/16 prefix)
  - RFC 6598
    - 100.64.0.0/10
  - Many more…
- Local link range
  - https://en.wikipedia.org/wiki/Link-local_address

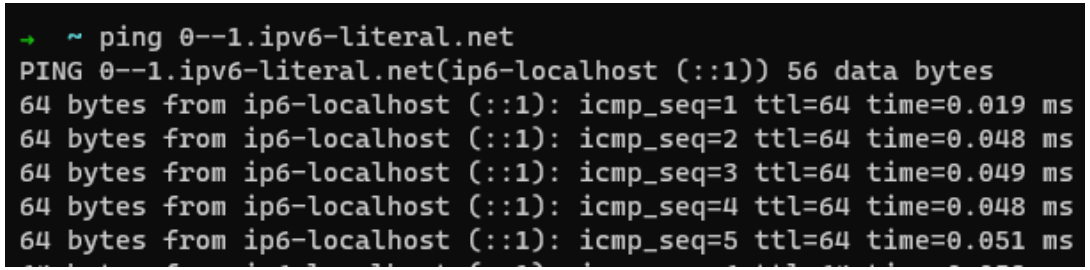
SSRF Technique: IP Address Confusion

- Are allow/deny lists enough?
  - https://www.hacksparrow.com/networking/many-faces-of-ip-address.html
- 127.0.0.1 can look like:
  - 0177.0.0.01
  - 000177.0000.00000.01
  - %31%32%37%2E%30%2E%30%2E%31
- IP wrap around/overflow
  - 1.0.513 = 1.0.2.1
- DNS records
  - ssrf.mydomain.com > 127.0.0.1

```
PING 1.0.513 (1.0.2.1) 56(84) bytes of data.
From 10.26.0.59 icmp_seq=1 Destination Net Unreachable
From 10.26.0.59 icmp_seq=2 Destination Net Unreachable
From 10.26.0.59 icmp_seq=3 Destination Net Unreachable
```

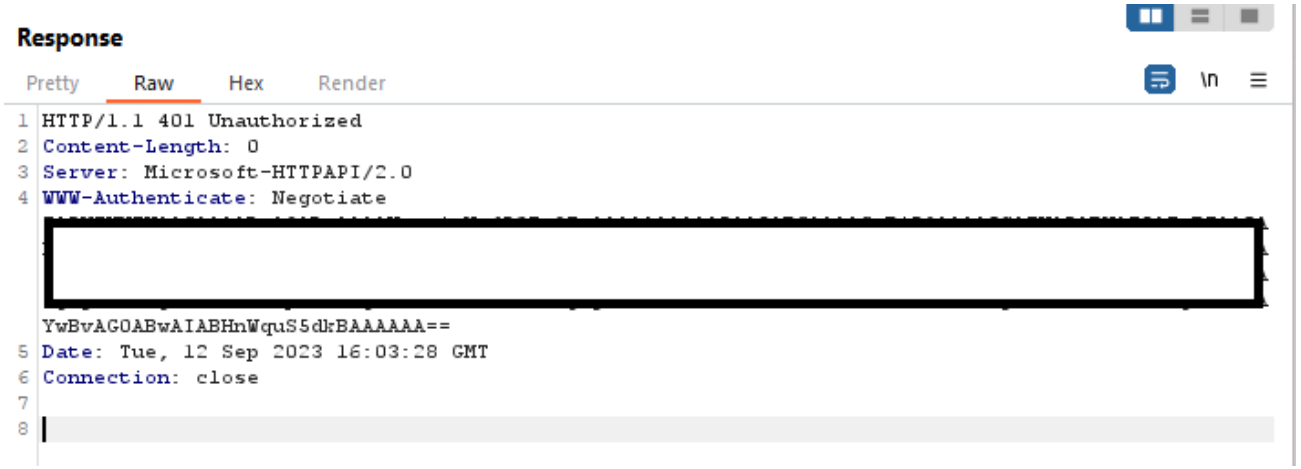
SSRF Technique: Don't Forget IPv6 Confusion

- Clouds can run out of IPv4
- ::1 can look like:
  - 0:0:0:0::0:0:1, 0000:0000:0000:0000:0000:0000:0000:0001, and more...
- IPv6 URL
  - http://[::1]
- Universal Naming Convention
  - Windows sees a colon, assumes drive letter
  - IPv6 literal Windows
    - 0--1.ipv6-literal.net = ::1
    - 2001-db8-85a3--8a2e-370-7334.ipv6-literal.net = 2001:db8:85a3::8a2e:370:7334
    - https://ipv6-literal.com/?ipv6=%3A%3A1



SSRF Technique: Authentication/Session Leak

- Examine the request
  - Headers
  - Body
- Response Modification
  - What happens if you impersonate?
    - 401 Unauthorized
    - Exchange server auth flow
    - Others?
- Write your own collaborator
  - https://github.com/microsoft/MSRC-Security-Research/tree/master/presentations/2023_09_GrrCON/ssrf_dojo/redirector.py



SSRF Technique: Redirection Strategy

- Many types of redirects
  - 301, 302, 303, 307, or 308
- Some will change request type
  - 303: POST > GET
    - https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/303
- Client-Side Request Forgery (not really SSRF)
  - DOM-based open redirection
    - Avoid dynamically setting redirection location with untrusted input
    - Can leak session tokens/account takeover
  - Meta refresh
    - <meta http-equiv="refresh" content="0; url=https://www.bing.com/">

SSRF Technique: URL Parsers

- Clouds have pieces in many programming languages
  - Parsers can behave differently
- Special Characters
  - #, @, :, ?, &
- Encoding
  - URL, Multiple URL, Unicode, etc.
- Regex issues
  - Are these both valid?
    - http://mysub.bing.com/index.html
    - http://mysub2.bing.com.xyz/index.html

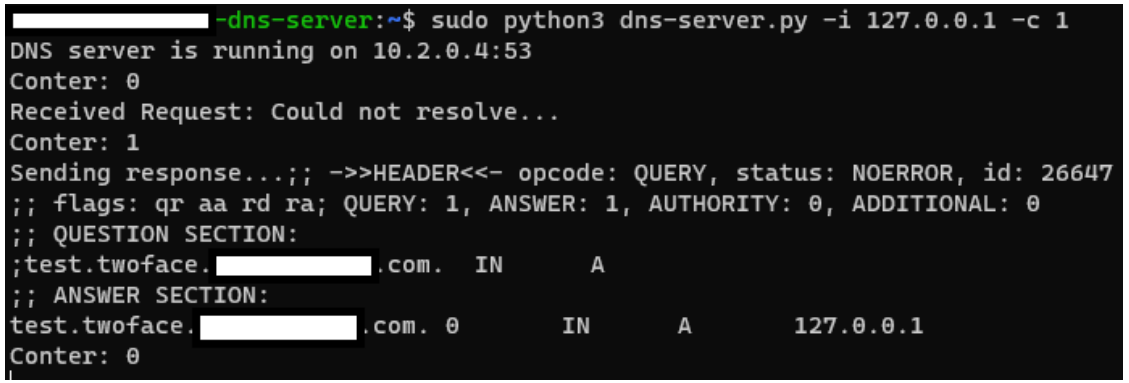
```
def is_bing_url(url):
    pattern = r"https?://([a-zA-Z0-9-]+\.)*bing\.com.*"
    return re.fullmatch(pattern, url) is not None
```

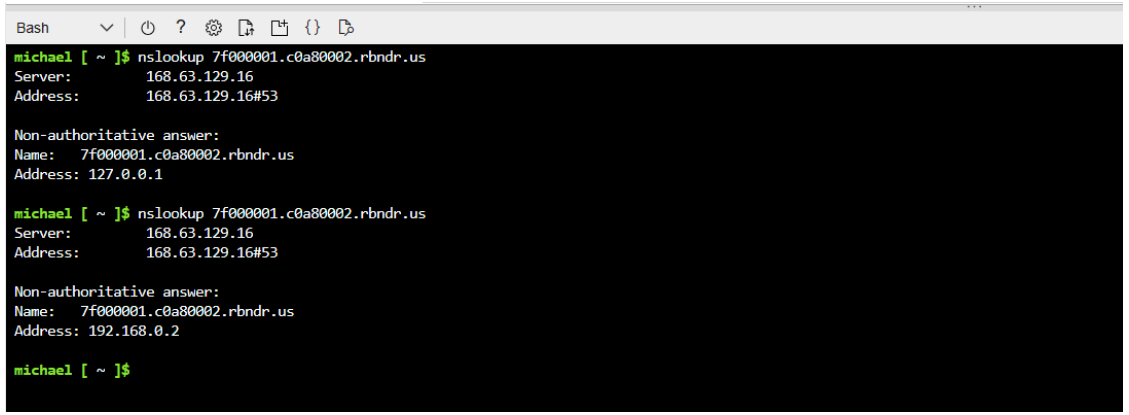
SSRF Technique: URL Parsers

- Additional resources
  - https://regex101.com/
  - https://qaz.wtf/u/convert.cgi?text=127.0.0.1%3A8000
  - https://www.blackhat.com/docs/us-17/thursday/us-17-Tsai-A-New-Era-Of-SSRF-Exploiting-URL-Parser-In-Trending-Programming-Languages.pdf

SSRF Technique: DNS Rebinding

- Time of Check, Time of Use (TOCTOU)
  - DNS A record with very low Time To Live (TTL)
  - Respond with different IPs
  - Sometimes requires specific count
    - Exactly n requests
- Example tool
  - https://github.com/taviso/rbndr
  - https://lock.cmpxchg8b.com/rebinder.html





SSRF Technique: Think ~~Outside the Box~~ Inside the Process!

- Interception proxies have limitations
  - No proxy options
  - Encryption
  - Blackbox/Reverse Engineering
- Attach Windbg to a process = SSRF?
  - HEXACON2022 - Hunting for cloudy SSRFs by Nicolas Joly
    - https://youtu.be/Q-N-LR_NoSY?t=764
    - https://www.hexacon.fr/slides/Hexacon22_Hunting_For_Cloudy_SSRFs.pdf
- Chain SSRF with Open Redirect
  - Many additional strategies

SSRF Mitigations

- Fix vulnerability is obvious
  - Remove functionality
  - Often need additional mitigations
- Allow/Deny Lists
  - Network level
  - Application level
    - Regex/Encoding challenges
    - "Wack a mole" issues
- Develop a library
  - Available to all developer teams

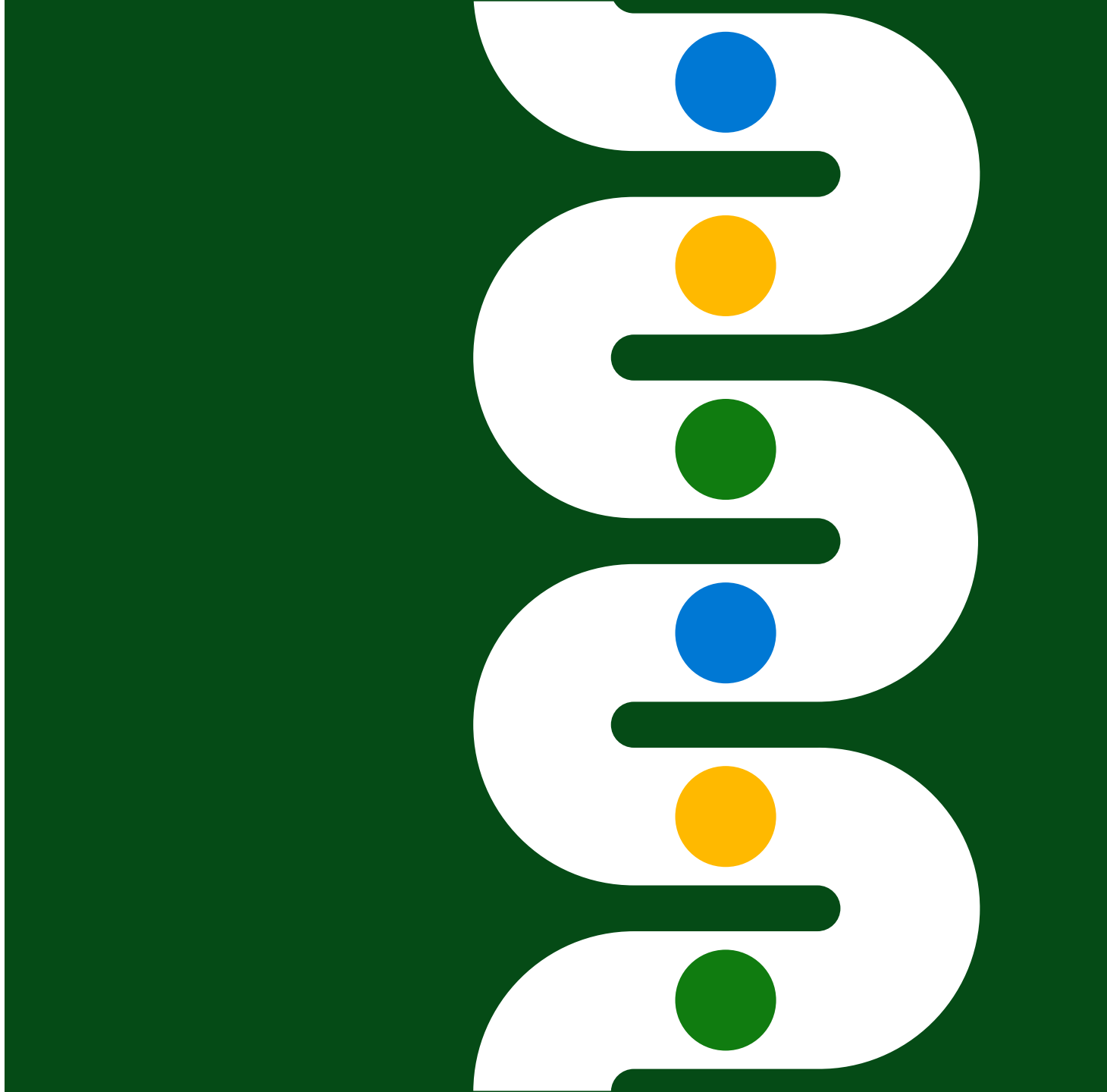
SSRF Mitigations

- Require special header
  - Metadata: true
  - Session token is better
- Disable anonymous access
  - Mutual authentication ideal
- Enforce URL schemas
  - Often no need for:
    - ftp://, file://, etc…
- When resolving DNS
  - Every time you send a web request
  - Use centralized allow/deny logic

SSRF Dojo Demo

- List of challenges
  - CornerKick – Use your header to score.
  - LeakyFaucet – Ask nicely and check your server.
  - ShapeShifter – Not all IPs are as they seem.
  - MisguidedParser – To error is code.
  - Detour – Headed off-road. Redirection skills required.
  - BaitAndSwitch – It's always DNS.
- Winning
  - Reach http://127.0.0.1:8000/flag with each challenge
- Download
  - https://github.com/microsoft/MSRC-Security-Research/tree/master/presentations/2023_09_GrrCON/ssrf_dojo/dojo.py

Additional Learning Resources



Learning Resources – Become an Ethical Hacker

Web Security Academy

OWASP Top 10

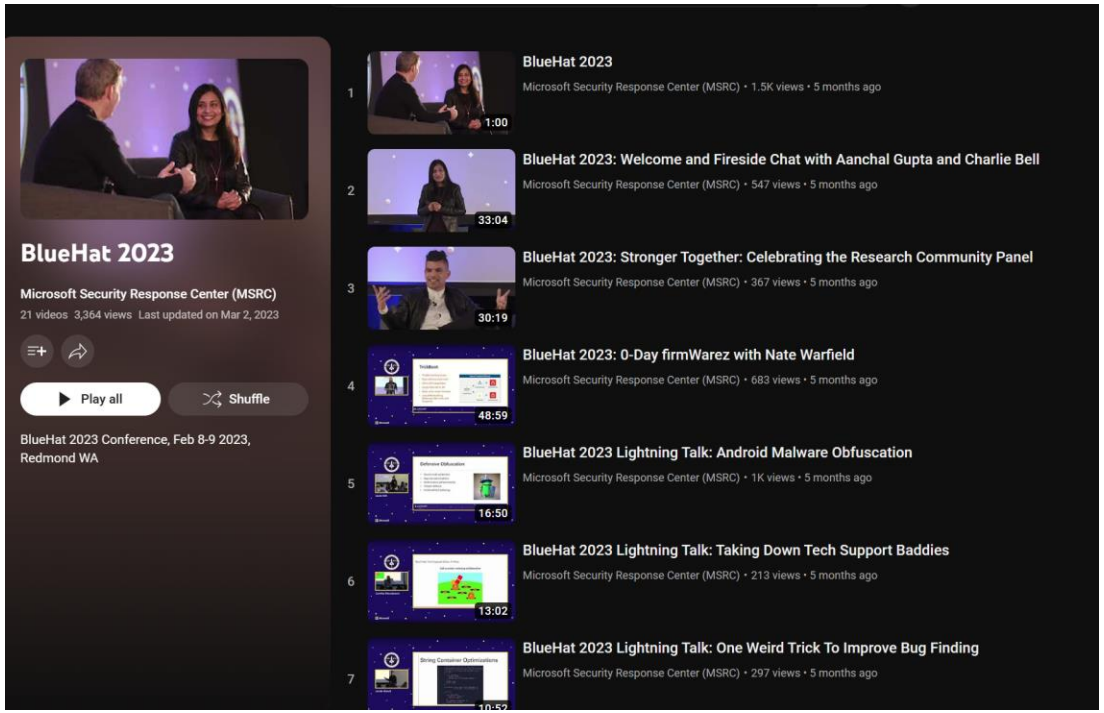
Online Courses

Community

We’re hiring!

- Security Folks of all Types
- Remote friendly
- https://careers.microsoft.com

BlueHat: Come Join an Epic Event, Or Watch Prior




Thank you