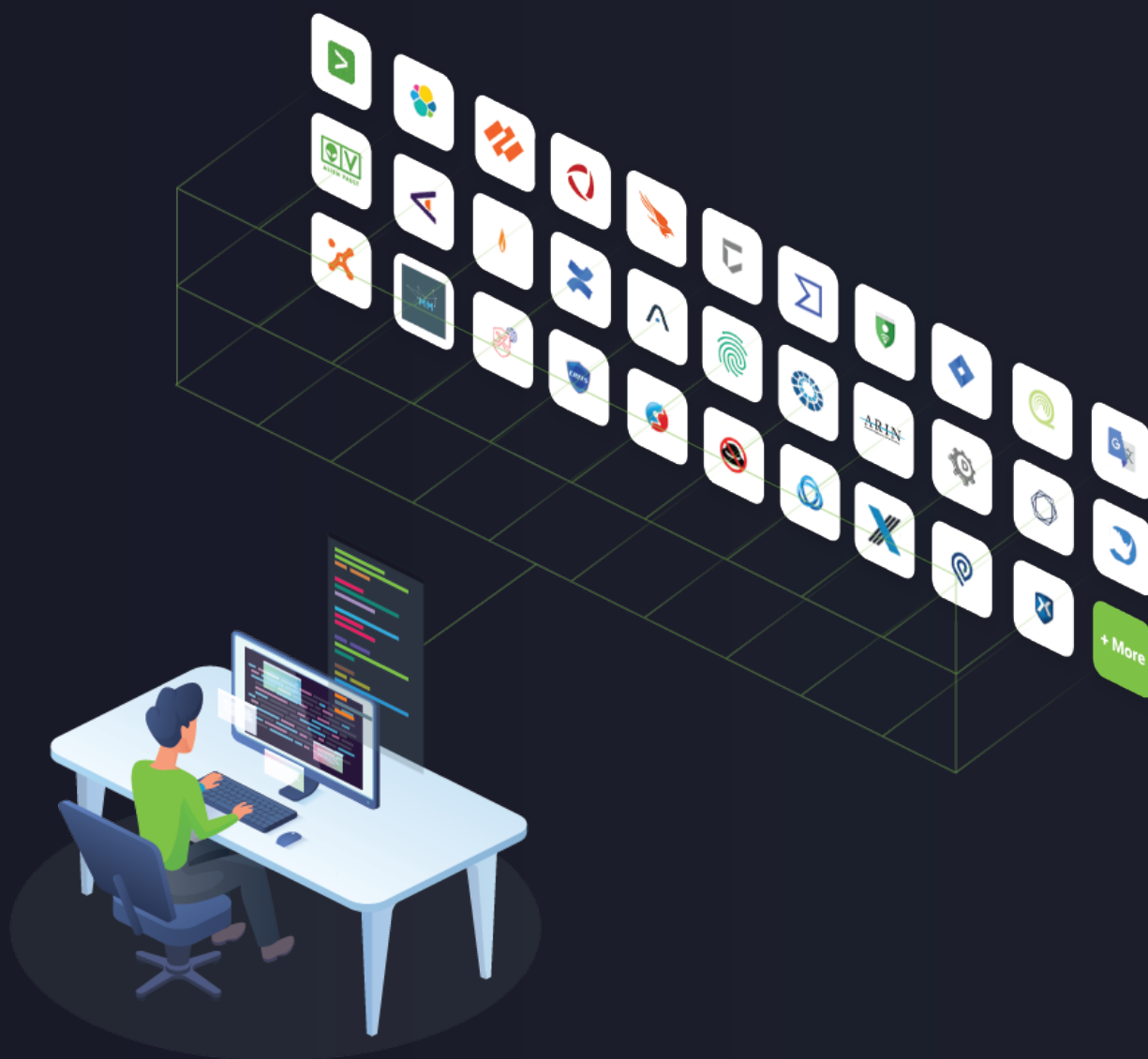


# Use Cases and Quick Wins for Offensive Security and Vulnerability Management



## How to use this Document

Polarity is committed to continually demonstrating value and increasing the value it provides to its customers.

This document is intended to illustrate popular use cases that Polarity customers are using to enhance their vulnerability risk and adversary simulation processes. These use cases include:

Vulnerability Triage	3
Vulnerability Exposure Assessment	6
Asset Awareness / Exception Tracking	8
Engagement Control & Collection	10
Passive Target Discovery	12
Tactical Offensive Execution	14
Exploitation Planning & Coordination	17
Command Execution	19

## Introduction

The evolving technology landscapes of an enterprise can present a fair number of challenges for organizational blue teamers, however, a growing number of technological assets, multi-cloud strategies, containerization strategies, work-from-home models, and the general diversification of technologies can also present their own complexities for those teams responsible for taking a more proactive approach to organizational cyber hygiene.

Exacerbating the challenges associated with more complex environments, most cyber security forums and new outlets have continuously forecasted that organizations will “aim to be doing more with less” throughout the early 2020’s. The “doing more” component of the statement is less nebulous than its later half. “With less” can be interpreted many ways: Less budget? Fewer people? Fewer tools?

When considering how to achieve more offensive security objectives with less resources, a decision maker is served well by understanding that offensive practitioners are regarded as having somewhat of a niche skill that is less easily duplicated, emulated, or transferred across a team. Further, there are requirements or traits of successful offensive security pros, such as tenacity, creativity, and curiosity that are not easily compensated for by technology. A reduction in headcount will only result in one outcome: fewer material proactive discoveries of significant technical exposures.

When considering what an organization truly needs “less” of when seeking to “do more” in offensive security, they should strive to do less re-work, less duplication of effort, make fewer mistakes, and drastically reduce the amount of manual research performed by offensive personnel so that they can achieve more positive outcomes for the organization.

Polarity can be applied within any practice or process. As it relates to offensive security, Polarity helps offensive practitioners spend more time on what they are good at: using their talents and skills in the identification, management, and exploitation of vulnerabilities, and less time on those activities that are research or task oriented.

Polarity does not replace analyst intuition; it does not work against it by asking analysts to open another dashboard or tool. Its unified view feeds their intuition with data so they can see the full story and see it faster. It is NOT a new place to search, it is an overlay on top of all existing technology and tools used by the SOC today.

Polarity overlays contextual information as you work for thoroughness and speed. The unified view gives you the right data at the right time to make informed decisions and act with speed. With Polarity, teams are no longer forced to balance between being thorough and getting the job done quickly.

## Vulnerability Triage

### Description:

Vulnerabilities are often rated and ranked by suppliers, but seasoned security practitioners should not implicitly trust those suppliers to rank vulnerabilities as the circumstances surrounding the vulnerability may vary between organizations. Upon detection of a vulnerability via traditional discovery processes (e.g., vulnerability scan, agent report, penetration test), security personnel will increase or decrease the severity of vulnerabilities based on information collected from internal, public, and commercial sources.

Within those sources, security practitioners will also seek to understand which threat actors may seek to exploit identified vulnerability, the ease of exploitation, and if the correlation between these factors increases the overall risk of the identified exposure.

Polarity enables rapid research and assessment of these factors, and ultimately more efficient and effective vulnerability triage.



### Capabilities

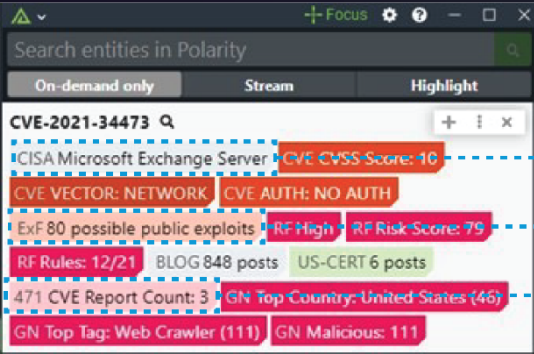
- Polarity allows for the triage analysis of Common Vulnerability and Exposure (CVE) designations.
- Information regarding the CVE can be queried from public records including those produced by the US Government.
- Polarity allows for the retrieval of OSINT and commercial threat intelligence regarding vulnerabilities.
- Polarity allows for the retrieval of information that informs an analyst as to the availability of exploit code. (**Also see “Exploitation Planning”**)



### Benefits

- Analysts can more quickly understand their exposure to published vulnerabilities.
- If the exposure exists, analysts can immediately tap into insights related to viability of threats or threat actors that might seek to exploit the vulnerability.

## Vulnerability Triage - Example



**Search entities in Polarity**

On-demand only Stream Highlight

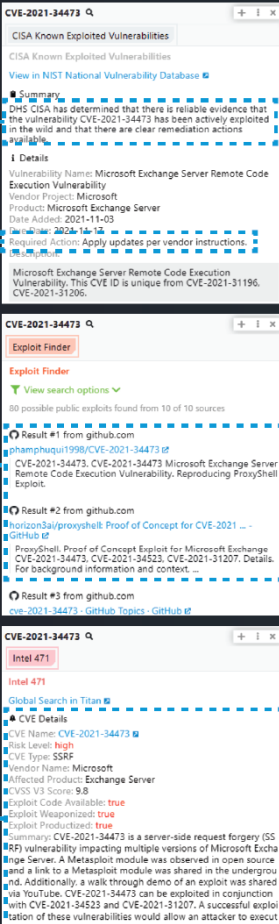
**CVE-2021-34473**

- CISA Microsoft Exchange Server **CVE CVSS Score: 10**
- CVE VECTOR: NETWORK** **CVE AUTH: NO AUTH**
- ExF 80 possible public exploits **RF High** **RF Risk Score: 79**
- RF Rules: 12/21** **BLOG 848 posts** **US-CERT 6 posts**
- 471 CVE Report Count: 3 **GN Top Country: United States (46)**
- GN Top Tag: Web Crawler (111)** **GN Malicious: 111**

**Polarity provides insights into exploitability and remedial actions.**

**Polarity allows for the retrieval of information that discloses availability of exploit code.**

**Polarity allows for the retrieval of OSINT and commercial threat intelligence regarding vulnerabilities.**



**CVE-2021-34473**

CISA Known Exploited Vulnerabilities

View in NIST National Vulnerability Database

**Summary**

CISA has determined that there is reliable evidence that the vulnerability CVE-2021-34473 has been actively exploited in the wild and that there are clear remediation actions available.

**1 Details**

Vulnerability Name: Microsoft Exchange Server Remote Code Execution Vulnerability

Vendor Project: Microsoft

Product: Microsoft Exchange Server

Date Added: 2021-11-03

**Required Action:** Apply updates per vendor instructions.

Microsoft Exchange Server Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2021-31196, CVE-2021-31206.

**Exploit Finder**

View search options

80 possible public exploits found from 10 of 10 sources

**Result #1 from github.com**

phamphuquai1990/CVE-2021-34473 id

CVE-2021-34473, CVE-2021-34473 Microsoft Exchange Server Remote Code Execution Vulnerability. Reproducing ProxyShell Exploit.

**Result #2 from github.com**

keron33/proxyshell: Proof of Concept for CVE-2021 ...

GitHub id

ProxyShell: Proof of Concept Exploit for Microsoft Exchange CVE-2021-34473, CVE-2021-34523, CVE-2021-31207. Details For background information and context.

**Result #3 from github.com**

cve-2021-34473 - GitHub Topics · GitHub id

**CVE-2021-34473**

Intel 471

Global Search in Titan

**CVE Details**

CVE Name: CVE-2021-34473

Risk Level: high

CVE Type: SSOF

Vendor Name: Microsoft

Affected Product: Exchange Server

CVSS V3 Score: 9.8

Exploit Code Available: true

Exploit Weaponized: true

Exploit Productized: true

**Summary:** CVE-2021-34473 is a server-side request forgery (SSRF) vulnerability impacting multiple versions of Microsoft Exchange Server. A Metasploit module was observed in open source and a link to a Metasploit module was shared in the underground. Additionally, a walk through demo of an exploit was shared on YouTube. CVE-2021-34473 can be exploited in conjunction with CVE-2021-34523 and CVE-2021-31207. A successful exploitation of these vulnerabilities would allow an attacker to execute

## Customer Quotes

”

Polarity is a product I cannot work without! Product is very easy to deploy, and the team will bend over backwards to help you out and make sure you are successful.

**Sr. Manager, Cybersecurity**  
Advanced Threat

”

Polarity is a force-multiplier for our security team whether its threat hunting or another discipline. In Highlight or On-demand mode we have confidence that all of our most valuable information is delivered, cross referenced against multiple sources, and is acted upon at the right time.

**Michael Francess**  
Manager, Cyber Security  
Advanced Threat

”

Our investment in Polarity led to an annual ROI of nearly 200% based on just its initial use cases. Since purchase, we continue to find ways to use Polarity to increase the speed and thoroughness of the team.

**Cybersecurity Manager**  
Leading Financial Service  
Company

## Vulnerability Exposure Assessment

### Description:

Given executive awareness, top-down dedication to information security and the headline-grabbing nature of security vulnerabilities, broadcasts of zero-day exploits or prolific security flaws spark responses that reverberate through an enterprise. On every occasion, a member of the security team is going to be asked by an organization leader, **“Are we vulnerable to this?”**

Whether an event of this scale, or of lesser magnitude occurs, security teams often must react to industry news and scour their tools and data sets for evidence that proves that they are not affected by new and old vulnerabilities – and if they are vulnerable, that they have not been exploited.

**Polarity allows for both a rapid and thorough assessment of vulnerabilities exposure through on-screen overlays.**



### Capabilities

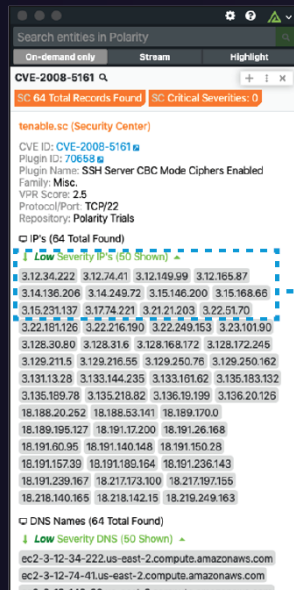
- Polarity provides real time access into vulnerability scan data that can inform the analyst as to the presence of a specific exposure within their environment.
- Via Polarity's annotation framework, analysts can document known mitigating controls specific to their enterprise as it relates to historical CVEs under investigation or a specific IP/host/device.
- Ticket and other workflow platforms can be queried in real time to inform the analyst as to work that is complete, incomplete, or in-flight regarding a CVE.



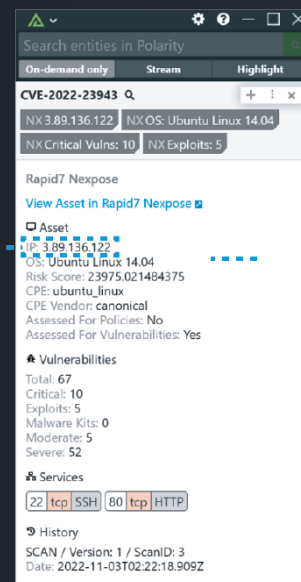
### Benefits

- Analysts can pursue mitigations more rapidly and with more certainty given the confidence of making the most informed decision.

# Vulnerability Exposure Assessment - Example



Polarity provides real time access to vulnerability scan data and asset systems to enable rapid association of vulnerability to enterprise assets.



## Customer Reviews

Gartner



**Fantastic Security Tool to Augment your Workflow and Analysts.**

Polarity is a great product and helps bridge the experience gap between new and established analysts.



**IT Security Specialist**

Gartner



**Great Platform To Bring Your Cyber Threat Intel And Data Sources Together**

Overall experience has been great. We were early adopters and have now been a customer for 3+ years.



**SR. DIRECTOR - Cybersecurity**



## Asset Awareness / Exception Tracking

### Description:

In nearly every commercial or federal environment, asset management is likely to be an existing area of focus or an opportunity for improvement. In part, this stems from the human element required to capture what a system does, what makes it important, what makes it more or less risky, who owns it, and why it's configured the way it is. Even if one were to capture everything, and have 100% knowledge and awareness of enterprise assets, the pace of change will soon result in degradation of data quality.

When managing vulnerabilities, or planning to exploit them, this information is critical to understanding the impacts of a planned or unplanned cyber aggression.

While these can be tedious tasks, they are perhaps some of the most important steps in the performance of offensive security activities. Failure to draw correlations between assets can result in ineffective or inefficient testing but could also result in significant downstream liabilities.

Polarity supports the closing of gaps in asset management and awareness by allowing access to organizational asset information on the fly. Further, Polarity establishes a process-aligned knowledge capture mechanism that allows analysts to take asset-oriented annotations and disseminate knowledge to colleagues, reducing the time to understanding.



### Capabilities

- Access asset management systems (e.g., ServiceNow) for asset information, allowing for a reliable / repeatable process for asset discovery. In parallel, such integrations allow analysts to avoid monotonous search.
- When an organization has deployed assets to the cloud, or has adopted a multi-cloud strategy, asset information is more likely to be distributed. Polarity can access the distributed assets repositories, or those technologies designed to consolidate it (e.g., Orca), ensuring that analysts are aware of cloud specific asset details.
- Polarity can access workflow or ticketing systems that tract exceptions. Often times, when a vulnerability is discovered, an organization may have already approved its existence provided that other measurable controls are in place. When Polarity accesses exception management systems, offensive security personnel can quickly understand why the vulnerability is present.



## Asset Awareness / Exception Tracking - Continued



### Capabilities

- Polarity allows offensive security teams to capture notes about assets, vulnerabilities, services, application names, and virtually any other string that may be the subject of their research. With this capability, a security practitioner can annotate:
  - False positives
    - Mis-identified vulnerabilities (e.g., “Underlying dependency not present within environment”)
  - Gaps in asset management
    - Current owners (e.g., “The real owner of this server is Alice,” “Bob doesn’t own anymore”)
    - Less tangible asset specifics “e.g., MySQL database installed is supported by the COTS vendor.”
  - Application codes
  - Details regarding services and fields such that other team members can ramp up quick on offensive efforts.
    - Service rationalization (SSH is wrapped over FTP service)



### Benefits

- Analysts can quickly understand the context of an asset that might inform the severity of a vulnerability, the value of exploitation or the circumstances that might surround doing so.
- Analysts can avoid lengthy research into exposures that are either false positives or have been recently investigated by colleagues.

## Engagement Control & Collection

### Description:

Often, offensive security pretensioners will operate under strict parameters that ensure that the risk to in-scope systems or environments is mitigated to a level acceptable by management. These parameters are commonly referred to as “Rules of Engagement”

The “Rules of Engagement” are typically agreed upon in advance of offensive operations, and memorialized in some form of document, distributed to stakeholders and stored in a knowledge base.

Polarity can be leveraged as a supporting layer to ensure that engagement control is achieved, by ensuring that rules or engagement parameters are socialized to offensive security pros at the time of need.



### Capabilities

- For assets, applications, network ranges, and other security targets, the following can be annotated into Polarity.
  - Permitted hours for testing activities
  - “Do no harm” protocols
  - Expressly excluded activities (e.g., persistent (stored) cross-site scripting)
  - Hosting providers that do not permit offensive activities
  - Contact information for “control/deconfliction agents” or system owners
  - Flags (if they are defined as an objective of the engagement)
- Polarity can automatically log all the searches performed during the normal course of an engagement.

As an additional layer of control, the assets leveraged to perform offensive security assessments can be annotated into the Polarity platform to achieve fusion between red and blue teams. The following are examples of annotations that can be saved with in a “fusion” channel to enable cross-team collaboration:

- The IP addresses of vulnerability scanners
- The user agent strings of approved scanners
- The network block/IP addresses of third-party penetration testing partners
- File attributes associated with benign payloads

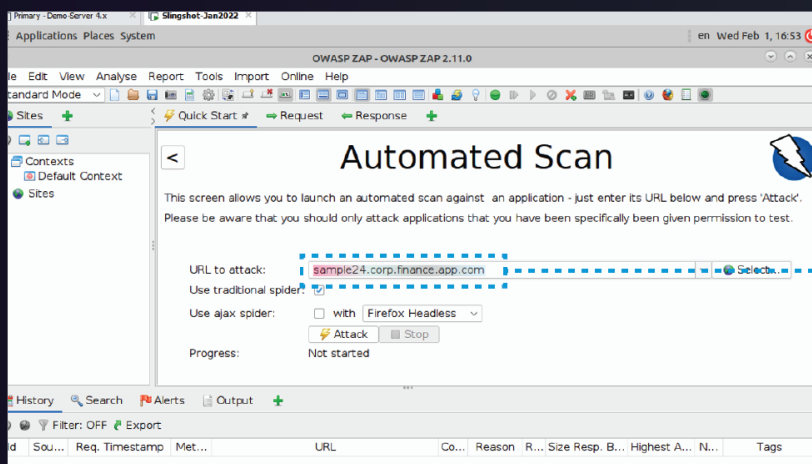
## Engagement Control & Collection - Continued



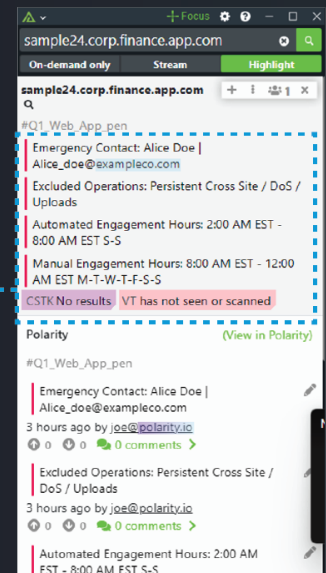
### Benefits

- Management can have greater confidence that offensive security professionals are avoiding execution-oriented risks to the business.
- Security teams garner additional trust from business stakeholders that might be weary of offensive engagement.
- Offensive personnel (who may be working on shifted schedules due to associate business requirements) understand operating procedures for specific in-scope assets, and are less likely to make a mistake.
- Security analysts spend more time focusing on the identification, management, and exploitation of vulnerabilities, and less time referencing control documentation.

## Engagement Control & Collection - Example



Polarity overlays rules of engagement over an offensive tester's purpose-built web application scanner.



## Passive Target Discovery

### Description:

Not all offensive teams are performing tests from an internal perspective. Many perform their offensive security operations while assuming the role of an external actor, or a party with less knowledge of the internal operations of target enterprise.

When assuming this role, one of the earlier stages of engagement execution involves performing reconnaissance against in-scope targets. Typically, reconnaissance is performed via two core methods.

- Active: When an offensive actor engages with the target system directly, typically initiating various probes to learn more about the system, its configuration, and available services.
- Passive: When an offensive actor attempts to obtain similar details about the target system that can be gleaned from active activities, without engaging directly with the target system.

In preliminary stages of a penetration test, this can involve a degree of open-source intelligence gathering and cursory reviews of in-scope systems to determine what basic services and or functions are, and confirmation as to the owner of in-scope systems.



## Capabilities

- Polarity can connect to core sources of information that are historically manually interrogated to determine target system specifics:
  - Services that map the Internet
  - Services that scan the Internet for vulnerabilities
  - Services that grab system / service banners
- Polarity can be leveraged to quickly identify the environments / hosting providers that targets reside within.
- Information provided from Polarity integrations can provide details regarding protections / controls implemented to help defend target systems (e.g., Cloudflare).
- In some cases, Polarity integrations will return the banners associated with listening services. These banners can yield details regarding products, service versions or other target details.
- Polarity provides a seamless method to leverage offline passive scan databases to check open ports/services without sending any traffic to the internet (e.g., Polarity's integration with Shodan's offline binary database).

## Passive Target Discovery - Continued



### Benefits

- Faster acclimation to the environment an offensive team is evaluating
- Immediate identification of security exposures, without active engagement of a target
  - Quicker identification of “low hanging fruit”
- Repeatable performance of passive intelligence collection
- Better informed strategies and more likely paths towards exploitation
- More opportunity for other stages of engagement execution (tuning, testing, exploitation)
- Seamless method to compare passive scan results with current manual scan. Results can be leveraged as if the scan was run from two different locations.

## Passive Target Discovery - Example

Below is an example of how an offensive tester might use a rudimentary nmap scan to “actively” probe a target for service details.

```

C:\Users\joeri>nmap polarity.io
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-01 12:16 Eastern Standard Time
Nmap scan report for polarity.io (18.67.65.95)
Host is up (0.017s latency).
Other addresses for polarity.io (not scanned): 18.67.65.70 18.67.65.86 18.67.65.42 2600:
9000:2269:4c00:2:3f8e:1280:93a1 2600:9000:2269:0:2:3f8e:1280:93a1 2600:9000:2269:7a00:2:
3f8e:1280:93a1 2600:9000:2269:6c00:2:3f8e:1280:93a1 2600:9000:2269:aa00:2:3f8e:1280:93a1
2600:9000:2269:f800:2:3f8e:1280:93a1 2600:9000:2269:1e00:2:3f8e:1280:93a1 2600:9000:226
9:5200:2:3f8e:1280:93a1
rDNS record for 18.67.65.95: server-18-67-65-95.iad89.r.cloudfront.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.13 seconds
C:\Users\joeri>
  
```

Polarity offers mechanisms to better understand the business functionality of an offensive target using passive means.

Polarity provides a seamless method to leverage offline passive scan database to check open ports/services without sending any traffic to the internet.

Search entities in Polarity

On-demand only Stream Highlight

18.67.65.95

SHO South Riding, United States

SHO ISP: Amazon.com, Inc.

SHO Org: Amazon.com, Inc. SHO Ports: 80, 443

SHO cde: SHO cloud | URLS Not Malicious

URLS Score: 0 | URLS Results: 1

Shodan

View in Shodan

Summary

City: South Riding

Country: United States

Org: Amazon.com, Inc.

ISP: Amazon.com, Inc.

Last Update: 2023-02-01T13:52:27.881187

Hostnames: server-18-67-65-95.iad89.r.cloudfront.net

ASN: AS16509

Ports

80 443

Services

80 tcp http 443 tcp https

Search entities in Polarity

On-demand only Stream Highlight

polarity.io

Uriscan

Screenshot

Stop wasting time searching. Just know how important it is to stop.

5x

200%

1000s

Knowledge and data is spread across disparate systems.

Screenshot URL: https://uriscan.io/screenshots/4a593fcc-3465-410a-8a50-21b61239b96b.png

## Tactical Offensive Execution

### Description:

As previously stated, certain offensive security activities require tenacity, creativity, and curiosity – but understanding both the fundamentals of technology and the expected functionality of target systems is paramount if security personnel are to determine the means by which the target can be exploited.

While certain tools can be useful in the identification of possible exposures, more significant security flaws may only be identified through persistence, trial and error, and the manual inspection of a system through very specific lenses.

These lenses take on the form of point solutions, nuanced browsers, and proxies that allow for the interrogation of system communications at various layers. Most of these technologies have developed over time for very specific purposes borne from need – and have become go-to solutions for practitioners in the field. As many of these solutions are open sourced, interoperability across tooling is limited. Further, many of these solutions were designed to support a lone practitioner, versus a team.

Polarity offers an extended capability on top of any tool, which allows the security practitioner to capture specifics of the target, recall difficult-to-remember environmental attributes that may (or may not) be material to the security engagement, and be used as a ready reference platform for solution syntax.



### Capabilities

- Establish technology libraries or reference channels that can be used to better understand system responses and errors. For example:
  - HTTP Responses / Error Codes
  - SQL Error codes
  - Unix command line messages
- Annotate and create awareness of string values/variables that should / should not appear in ongoing system communications, like:
  - SessionIDs
  - Tokens
  - Passwords
  - Other codes / identifiers
- Maintain libraries of common/default passwords for encountered technologies that can be leveraged as a quick “cheat sheet” to check for.

## Tactical Offensive Execution - Continued



### Capabilities

- Store go-to / reliable syntax within reference channels to reduce the time spent in help docs and man-pages.
- Tactical research of variables or other systems components that require clarification in order to understand the system being targeted. Instead of needing to open a browser tab to “Google” an unknown variable, Polarity provides the results at the touch of a keystroke.
- Annotation of byte sequences within an IDE (integrated development environment) when developing exploit code.
- Integration with command line tools.

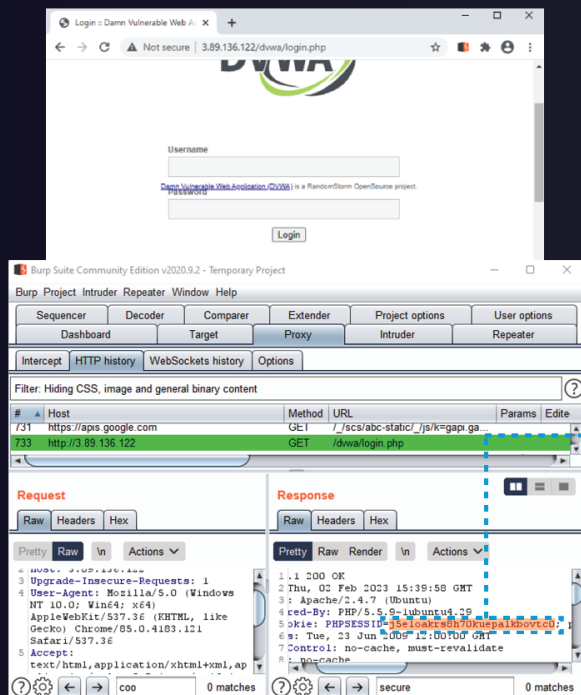


### Benefits

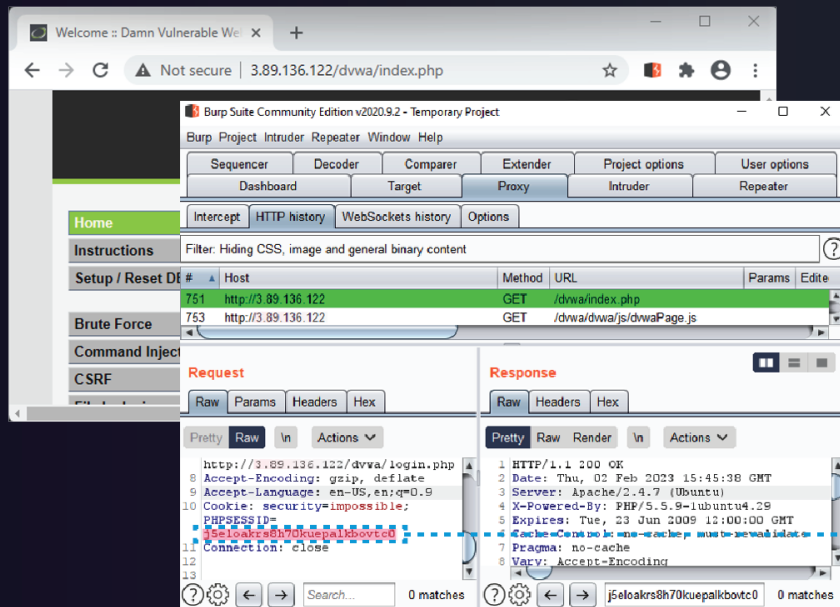
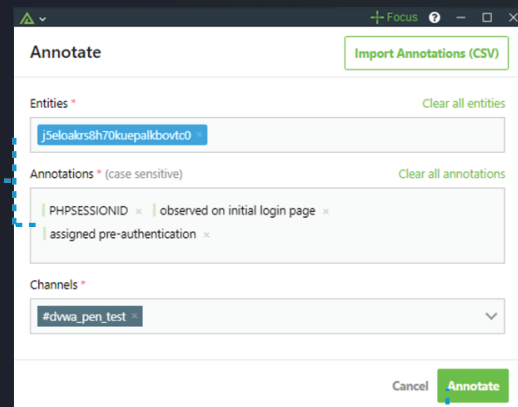
- Lessons learned by colleagues (present or past) can be shared across a distributed offensive team.
- When performing tactical activities, security practitioners will spend more time pushing beyond the capabilities of automated tools.
- When errors or responses are received from tactical probes, offensive pro's can spend less time researching and more time reacting, enhancing and progressing towards better operational outcomes.



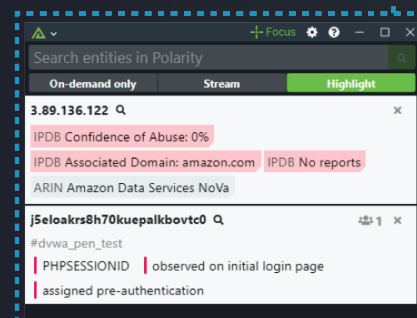
# Tactical Offensive Execution - Example



Polarity allows for annotations of strings. In this example, a session ID is annotated by a manual tester.



When the session string is observed in later testing stages, Polarity creates awareness of the string and returns tester notes.



## Exploitation Planning & Coordination

### Description:

Even if you develop custom exploit code, many practitioners will seek to leverage existing public (yet trusted) exploit code in the performance of exploitation activities. This helps to demonstrate both the impact of exploitation on the target, as well as the likelihood of exploitation to business stakeholders that will need to determine the path towards remediation.

Polarity reduces the time required to search for exploit code, and arms practitioners with the means to achieve offensive security objectives.



### Capabilities

- Polarity automatically scours trusted sources on the internet for exploit code to be leveraged in the later stages of offensive security operations.
- Polarity is used to establish internal knowledge bases of exploit code.
- Polarity can access wikis and knowledge repositories (e.g., Confluence, GitHub, SharePoint, Google Drive) for exploit code developed or modified by a team.
- Polarity can be used to direct team members to exploit code as made available in exploitation technologies (e.g., Metasploit).
- Polarity integrations identify available Yara rules that disclose existing mechanisms for exploit detection, which could inform an evasive strategy.



### Benefits

- Automating busy work such as internet research speeds up analysis and increases quality of work.
- Teams capitalize on the work of their colleagues and predecessors.
- Teams achieve outcomes faster.
- Opportunities are created to expand breadth of coverage, depth of engagement or focus on other organizational initiatives.

# Exploitation Planning & Coordination - Example

```
Fingerprinting the version - Time: 00:00:00
[-] WordPress version 5.6 identified (Insecure, released on 2020-12-08).
Found By: Unique Fingerprinting (Aggressive Detection)
- http://[redacted]/wp-admin/js/customize-controls.js md5sum is 60fd86fb779d8562016277fa549883c

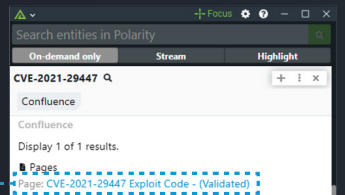
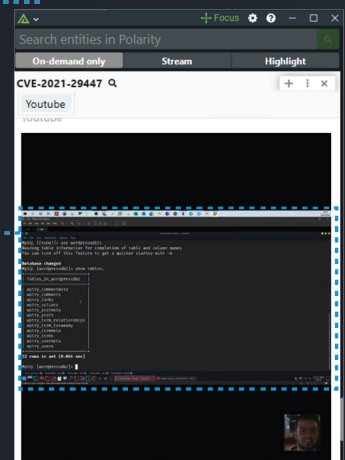
[+] 3 vulnerabilities identified:
[+] Title: WordPress 5.6-5.7 - Authenticated XXE Within the Media Library Affecting PHP 8
Fixed in: 5.6.3
References:
- https://wpscan.com/vulnerability/cbbe6c17-b24e-4be4-8937-c78472a138b5
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29447
- https://wordpress.org/news/2021/04/wordpress-5-7-1-security-and-maintenance-release/
- https://core.trac.wordpress.org/changeset/29378
- https://blog.wpscan.com/2021/04/15/wordpress-571-security-vulnerability-release.html
- https://github.com/WordPress/WordPress-develop/security/advisories/GHSA-rv47-pc52-qrhk
- https://blog.sonarsource.com/wordpress-xxe-security-vulnerability/
- https://hackerone.com/reports/1095645
- https://www.youtube.com/watch?v=3NBxcmqCgt
```

When searching a CVE with Polarity Focus Mode, available exploit code is returned.

A video on how to exploit this vulnerability is also returned to help up-skill the tester.

```
Authenticated XXE Within the Media Library Affecting PHP 8
Fixed in: 5.6.3
References:
- https://wpscan.com/vulnerability/cbbe6c17-b24e-4be4-8937-c78472a138b5
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29447
- https://wordpress.org/news/2021/04/wordpress-5-7-1-security-and-maintenance-release/
- https://core.trac.wordpress.org/changeset/29378
- https://blog.wpscan.com/2021/04/15/wordpress-571-security-vulnerability-release.html
- https://github.com/WordPress/WordPress-develop/security/advisories/GHSA-rv47-pc52-qrhk
- https://blog.sonarsource.com/wordpress-xxe-security-vulnerability/
- https://hackerone.com/reports/1095645
- https://www.youtube.com/watch?v=3NBxcmqCgt
```

Internal exploit code for the vulnerability is delivered to the tester from internal tools. (e.g., Confluence).



## Command Execution

### Description:

Penetration testing requires the practitioner to pivot within and between tools continuously. Every pivot slows down the tester and is an opportunity for an unintentional copy-past or transcription error.



### Capabilities

- Polarity could be used to execute commands that trigger repeatable offensive actions, such as active reconnaissance, brute force attempts, banner grabbing or maybe even exploitation. For example, any time you pass an IP to Polarity you could have a button to kick off a nmap scan. Or maybe it is more convenient to run the dig command with the touch of a keystroke instead of copy pasting or typing in the target.
- At the touch of a keystroke, Polarity can run conversions or encoding. For example, Polarity can quickly encode an attack string into base64 for use in a PowerShell script or disassemble a hexadecimal string into assembly language.
- At the touch of a keystroke, Polarity can run translation of foreign language text into your native language of choice or vice versa. Maybe you are on a target system with a foreign language set and trying to navigate a directory structure; it is simple to get quick translations with Polarity. The other way around is also possible, maybe you would like to name dropper files in the native language of the target.



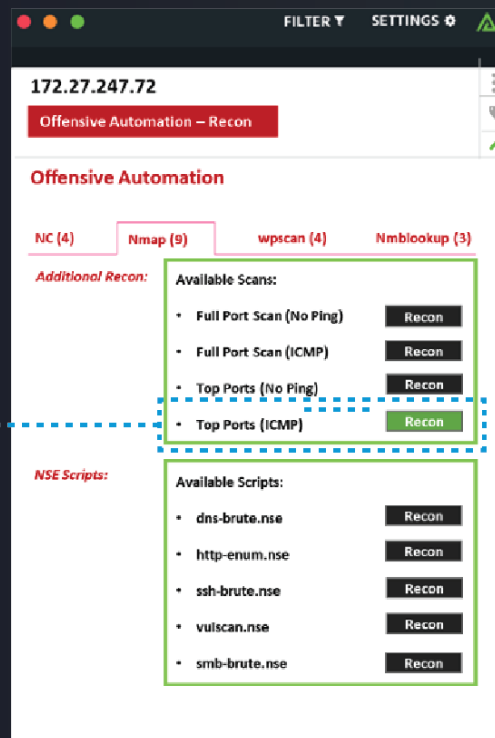
### Benefits

- Democratization of capability – For example, a user does not need to know the exact syntax to run an NMAP “stealth” scan, they just need to pick the desired scan type from a list.
- Built-in training – Upon execution of a command, the user can be informed exactly what was run.
- Built-in awareness – During the normal course of work, the user is made aware of available capabilities.
- Speed – Users do not need to pivot or copy and paste as often because it is simple for them to hit the Polarity keystroke and have available commands in front of them.
- Consistency of tradecraft – A team will have access to a common set of tools and commands that can be configured to execute in a preferred, non-attributable, and consistent manner.

## Command Execution - Example

```
Command Prompt
Host is up (0.00s latency).
MAC Address: 00:FF:9B:4F:85:C3 (Unknown)
Nmap scan report for ip-172-27-247-254.ec2.internal (172.27.247.254)
Host is up (0.00s latency).
MAC Address: 00:FF:9B:4F:85:C3 (Unknown)
Nmap scan report for ip-172-27-247-255.ec2.internal (172.27.247.255)
Host is up (0.00s latency).
MAC Address: 00:FF:9B:4F:85:C3 (Unknown)
Nmap scan report for ip-172-27-247-72.ec2.internal (172.27.247.72)
Host is up.
Nmap done: 255 IP addresses (5 hosts up) scanned in 18.00 seconds
C:\Users\joeri>
```

Polarity could be used to execute commands that trigger repeatable offensive actions.



POLARITY  
+ ThreatConnect.

Try it free at  
[www.threatconnect.com](http://www.threatconnect.com)