Vulnerability Mapping to ATT&CK Techniques

# Introduction

The number of vulnerabilities being reported is overwhelming. Defenders need help processing vulnerability reports. Standardizing the data in vulnerability reports makes it easier for defenders to interpret the report quickly and accurately. It also enables automation since computers have an even harder time understanding the variations in terminology than humans. This document provides a model that can be used to help standardize the way vulnerabilities are reported by using MITRE ATT&CK.

## What is ATT&CK?

MITRE ATT&CK provides a method for standardizing the language around vulnerabilities. The ATT&CK framework is a knowledge base of adversary tactics and techniques based on real-world observations. ATT&CK techniques provide a standard way of describing the methods adversaries use to exploit a vulnerability and what adversaries hope to achieve by exploiting the vulnerability. In addition, the ATT&CK framework is used as a foundation for the development of threat models and methodologies by many defenders. Using ATT&CK techniques to describe a vulnerability makes it easier for defenders integrating vulnerabilities into their threat modeling.

## Usage

The model has three main groupings of ATT&CK technique mappings:

* **Vulnerability Type** – Common vulnerability types (e.g., cross-site scripting and SQL injection) with common technique mappings are covered in this section. For vulnerability types that don’t have common technique mappings, the other sections are used.
* **Functionality** - This section groups common mappings based on the type of functionality the attacker gains access to by exploiting the vulnerability.
* **Exploit Techniques** – This section groups common mappings depending on the method used to exploit the vulnerability.

The mappings come in three categories:

* **Primary Impact** - the initial benefit gained through exploitation of a vulnerability
* **Secondary Impact** - what the adversary can do by gaining the benefit of the primary impact (e.g., a directory traversal may have a primary impact of reading arbitrary files, which the adversary may use to read the credentials in /etc/password)
* **Exploitation Technique** - the method used to exploit the vulnerability (e.g., a crafted file or malicious link).

The groupings may contain mappings for one, two, or all three categories. It all depends on how likely different vulnerabilities in the group share that technique. For example, vulnerabilities that modify memory (e.g., buffer overflows) share a common primary impact, but the secondary impacts and exploitation techniques are so varied that the model does not include a mapping for those categories. Also, some groupings will have more than one technique listed for a mapping category because there are some common variations within that grouping. In these cases, only the techniques that apply to the vulnerability should be selected. For example, the cross-site scripting (XSS) group includes an option of T1189 (Drive-by Compromise) or T1204.001 (User Execution: Malicious Link) depending on whether the attacked is stored or not.

## Limitations

The model is not meant to be a 100% and cannot cover all the various way systems are exploited. It is meant as an easy-to-use starting point for vulnerability reporters to standardize the way they describe some vulnerability data.

# Vulnerability type mappings

The vulnerability type section contains mappings for many of the common vulnerability types. Mappings for vulnerability types are only included if that type has a common set of techniques used to exploit the vulnerability or that can be executed when the vulnerability is exploited. Each vulnerability type will include a one or more of the following where applicable, a primary and secondary impact and one or more exploitation techniques.

## Table

| **Vulnerability Type** | **Primary Impact** | **Secondary Impact** | **Exploitation Technique** | **Notes** |
| --- | --- | --- | --- | --- |
| General Authentication, Authorization, and Permission Errors | See Section 3 | See Section 3 | N/A | The impacts of authentication, authorization, and permissions errors generally depend on the functionality missing the authentication, authorization or permission. |
| Authentication Bypass by Capture-replay | T1190 (Exploit Public-Facing Application) | N/A | T1040 (Network Sniffing) |  |
| Improper Restriction of Excessive Authentication Attempts | T1078 (Valid Accounts) | N/A | T1110.001 (Brute Force: Password Guessing) |  |
| CWE-645: Overly Restrictive Account Lockout Mechanism | Mobile - T1446 (Device Lockout) Others – T1531 (Account Access Removal) | N/A | T1110 (Brute Force) |  |
| CWE-836: Use of Password Hash Instead of Password for Authentication | T1550.002 (Use Alternate Authentication Material: Pass the Hash) | N/A | N/A |  |
| General Credential Management Errors | T1552 (Unsecure Credentials) | T1078 (Valid Accounts) | N/A | A sub-technique can be chosen where applicable. |
| Cleartext Transmission of Sensitive Information | T1552 (Unsecured Credentials) | T1078 (Valid Accounts) | T1040 (Network Sniffing) | A sub-technique can be chosen where applicable. |
| Hard-coded Credentials | T1078.001 (Default Accounts) | N/A | N/A |  |
| Weak Password/Hashing | N/A | T1078 (Valid Accounts) | T1110 (Brute Force) |  |
| General Cryptographic Issues | Credential storage or transmission – T1078 (Valid Accounts)  Transmitting over network – T1557 (Man-in-the-Middle), T1040 (Network Sniffing)  Sensitive information storage – various techniques from the Collection tactic | N/A | T1110 (Brute Force) |  |
| XML External Entity (XXE) | T1059 (Command and Scripting Interpreter). | T1005 (Data from Local System), T1046 (Network Service Scanning) | N/A |  |
| XML Entity Expansion (XEE) | T1499.004 (Endpoint Denial of Service: Application or System Exploitation) | N/A | N/A |  |
| URL Redirection to Untrusted Site ('Open Redirect') | N/A | T1036 (Masquerading) | T1566.002 (Phishing: Spearphishing Link) |  |
| Cross-site Scripting (XSS) | T1059.007 (Command and Scripting Interpreter: JavaScript/JScript) | T1557 (Man-in-the-Browser) | Stored – T1189 (Drive-by Compromise)  Others – T1204.001 (User Execution: Malicious Link) | There are lots of possible secondary impacts but most of them can be summed up by Man-in-the-Browser. |
| OS Command Injection | T1059 (Command and Scripting Interpreter) | N/A | T1133 (External Remote Service) | Primary depends on the OS being attacked but is often T1059.004. |
| SQL Injection | T1059 (Command and Scripting Interpreter) | T1005 (Data from Local System), T1505.003 (Server Software Component: Web Shell), T1136 (Create Account), T1190 (Exploit Public-Facing Application), T1565.001 (Data Manipulation) | N/A | There currently is not a sub-technique for SQL commands. Not all possible secondary impacts are listed and not all secondary impacts will always apply. |
| Code Injection | T1059 (Command and Scripting Interpreter) | N/A | N/A | A sub-technique can be used depending on the type of injection. |
| Directory Traversal (Relative and Absolute) | See Section 3.9 (File Processing) | See Section 3.9 (File Processing) | T1202 (Indirect Command Execution) | Indirect command execution is used here because the vulnerable application is being used to as a proxy to execute the file handling commands. |
| Symlink Attacks | See Section 3.9 (File Processing) | See Section 3.9 (File Processing) | T1202 (Indirect Command Execution) | Indirect command execution is used here because the vulnerable application is being used to as a proxy to execute the file handling commands. |
| Untrusted/Uncontrolled/Unquoted Search Path | T1574 (Hijack Execution Flow) | N/A | N/A | A sub-technique can be chosen where appropriate. |
| Unrestricted File Upload | T1505.003 (Server Software Component: Web Shell) | T1059 (Command and Scripting Interpreter) | N/A |  |
| Deserialization of Untrusted Data | T1059 (Command and Scripting Interpreter) | N/A | N/A |  |
| Infinite Loop | T1499.004 (Endpoint Denial of Service: Application or System Exploitation) | N/A | N/A |  |
| Cross-site Request Forgery (CSRF) | T1068 (Exploitation for Privilege Escalation) | Depends on the functionality the vulnerability gives access to. See Section 3 for guidance on which techniques are appropriate. | T1204.001 (User Execution: Malicious Link) |  |
| Session Fixation | T1563 (Remote Service Session Hijacking) | N/A | N/A | Often can be used for Initial Access. |
| Uncontrolled Resource Consumption | T1499 (Endpoint Denial of Service) | N/A | N/A | A sub-technique may be chosen depending on the type of resource being consumed |
| Server-Side Request Forgery (SSRF) | T1090 (Proxy) | T1135 (Network Discovery), T1005 (Data from Local System) | T1133 (External Remote Service) | Tactic/Technique mismatch for the primary impact. |

## Authentication, Authorization, and Permission Errors

### General Authentication, Authorization, and Permission Errors

Primary: See Section 2

Secondary: See Section 2

Exploitation techniques: N/A

Notes: The impacts of authentication, authorization, and permissions errors generally depend on the functionality missing the authentication, authorization or permission.

### Authentication Bypass by Capture-replay

Primary: T1190 (Exploit Public-Facing Application)

Secondary: N/A

Exploitation techniques: T1040 (Network Sniffing)

### Improper Restriction of Excessive Authentication Attempts

Primary: T1078 (Valid Accounts)

Secondary: N/A

Exploitation techniques: T1110.001 (Brute Force: Password Guessing)

### CWE-645: Overly Restrictive Account Lockout Mechanism

Primary: Mobile - T1446 (Device Lockout), Others – T1531 (Account Access Removal)

Secondary: N/A

Exploitation techniques: T1110 (Brute Force)

### CWE-836: Use of Password Hash Instead of Password for Authentication

Primary: T1550.002 (Use Alternate Authentication Material: Pass the Hash)

Secondary: N/A

Exploitation techniques: N/A

## Credentials Management Errors

### General Credential Management Errors

Primary: T1552 (Unsecure Credentials)

Secondary: T1078 (Valid Accounts)

Exploitation techniques: N/A

Notes: A sub-technique can be chosen where applicable.

### Cleartext Transmission of Sensitive Information

Primary: T1552 (Unsecured Credentials)

Secondary: T1078 (Valid Accounts)

Exploitation techniques: T1040 (Network Sniffing)

Notes: A sub-technique can be chosen where applicable.

### Hard-coded Credentials

Primary: T1078.001 (Default Accounts)

Secondary: N/A

Exploitation techniques: N/A

### Weak Password/Hashing

Primary: N/A

Secondary: T1078 (Valid Accounts)

Exploitation techniques: T1110 (Brute Force)

## Cryptographic Issues

### General Cryptographic Issues

Primary:

* Credential storage or transmission – T1078 (Valid Accounts)
* Transmitting over network – T1557 (Man-in-the-Middle), T1040 (Network Sniffing)
* Sensitive information storage – various techniques from the Collection tactic

Secondary:

Exploitation techniques: T1110 (Brute Force)

## Data Processing Errors

### XML External Entity (XXE)

Primary: T1059 (Command and Scripting Interpreter).

Secondary: T1005 (Data from Local System), T1046 (Network Service Scanning)

Exploitation techniques: N/A

### XML Entity Expansion (XEE)

Primary: T1499.004 (Endpoint Denial of Service: Application or System Exploitation)

Secondary: N/A

Exploitation techniques: N/A

### URL Redirection to Untrusted Site ('Open Redirect')

Primary: N/A

Secondary: T1036 (Masquerading)

Exploitation techniques: T1566.002 (Phishing: Spearphishing Link)

## Date Representation Errors

### Cross-site Scripting (XSS)

Primary: T1059.007 (Command and Scripting Interpreter: JavaScript/JScript)

Secondary: T1557 (Man-in-the-Browser)

Exploitation techniques: Stored – T1189 (Drive-by Compromise), Others – T1204.001 (User Execution: Malicious Link)

Notes: There are lots of possible secondary impacts but most of them can be summed up by Man-in-the-Browser.

### OS Command Injection

Primary: T1059 (Command and Scripting Interpreter)

Secondary: N/A

Exploitation techniques: T1133 (External Remote Service)

Notes: Primary depends on the OS being attacked but is often T1059.004.

### SQL Injection

Primary: T1059 (Command and Scripting Interpreter)

Secondary: T1005 (Data from Local System), T1505.003 (Server Software Component: Web Shell), T1136 (Create Account), T1190 (Exploit Public-Facing Application), T1565.001 (Data Manipulation)

Exploitation techniques: N/A

Notes: There currently is not a sub-technique for SQL commands

Not all possible secondary impacts are listed and not all secondary impacts will always apply.

### Code Injection

Primary: T1059 (Command and Scripting Interpreter)

Secondary: N/A

Exploitation techniques: N/A

Notes: A sub-technique can be used depending on the type of injection.

## File Handling Issues

### Directory Traversal (Relative and Absolute)

Primary: See Section 2.9 (File Processing)

Secondary: See Section 2.9 (File Processing)

Exploitation techniques: T1202 (Indirect Command Execution)

Notes: Indirect command execution is used here because the vulnerable application is being used to as a proxy to execute the file handling commands.

### Symlink Attacks

Primary: See Section 2.9 (File Processing)

Secondary: See Section 2.9 (File Processing)

Exploitation techniques: T1202 (Indirect Command Execution)

Notes: Indirect command execution is used here because the vulnerable application is being used to as a proxy to execute the file handling commands.

### Untrusted/Uncontrolled/Unquoted Search Path

Primary: T1574 (Hijack Execution Flow)

Secondary: N/A

Exploitation techniques: N/A

Notes: A sub-technique can be chosen where appropriate.

## Misc.

### Unrestricted File Upload

Primary: T1505.003 (Server Software Component: Web Shell)

Secondary: T1059 (Command and Scripting Interpreter)

Exploitation techniques: N/A

### Deserialization of Untrusted Data

Primary: T1059 (Command and Scripting Interpreter)

Secondary: N/A

Exploitation techniques: N/A

### Infinite Loop

Primary: T1499.004 (Endpoint Denial of Service: Application or System Exploitation)

Secondary: N/A

Exploitation techniques: N/A

### Integer Overflow

If it results in memory corruption, see Section 2.10 (Memory Modification)

Otherwise, use the Section 2.

### Cross-site Request Forgery (CSRF)

Primary: T1068 (Exploitation for Privilege Escalation)

Secondary: Depends on the functionality the vulnerability gives access to. See Section 2 for guidance on which techniques are appropriate.

Exploitation techniques: T1204.001 (User Execution: Malicious Link)

### Session Fixation

Primary: T1563 (Remote Service Session Hijacking)

Secondary: N/A

Exploitation techniques: N/A

Notes: Often can be used for Initial Access.

### Uncontrolled Resource Consumption

Primary: T1499 (Endpoint Denial of Service)

Secondary: N/A

Exploitation techniques: N/A

Notes: A sub-technique may be chosen depending on the type of resource being consumed

### Server-Side Request Forgery (SSRF)

Primary: T1090 (Proxy)

Secondary: T1135 (Network Discovery), T1005 (Data from Local System)

Exploitation techniques: T1133 (External Remote Service)

Note: Tactic/Technique mismatch for the primary impact.

# Functionality

The ATT&CK techniques enabled by exploiting a vulnerability may depend on the functionality the attacker gains access to. For example, insecure permissions on a file may allow the attacker to read the file and obtain sensitive information, mapping to T1005 (Data from Local System), whereas a different set of insecure permissions might allow the attacker to overwrite the file, resulting in T1565.001 (Data Manipulation). The following section documents some of the different types of functionality an attacker may gain access to and which techniques map to that functionality.

## Table

| **Functionality** | **Primary Impact** | **Secondary Impact** | **Notes** |
| --- | --- | --- | --- |
| Modify Configuration | T1478 (Install Insecure or Malicious Configuration) |  |  |
| Create Account | T1136 (Create Account) | T1078 (Valid Accounts) |  |
| Disable protections | T1562 (Impair Defenses) |  |  |
| Restart/Reboot | T1529 (System Shutdown/Reboot) |  |  |
| Install App | T1476 (Deliver Malicious App via Other Means) |  |  |
| Read from Memory | T1005 (Data from Local System) |  |  |
| Obtain sensitive information: Credentials | T1552 (Unsecured Credentials) |  |  |
| Obtain sensitive information: Other data | T1005 (Data from Local System) |  |  |
| Password Reset | T1098 (Account Manipulation) |  |  |
| Read files | T1005 (Data from Local System) | T1003.008 (OS Credential Dumping: /etc/passwd and /etc/shadow), T1552.001 (Unsecured Credentials: Credentials in Files) | The list of secondary impacts covers common techniques included in proof-of-concepts but is not exhaustive. |
| Delete files | T1485 (Data Destruction) | T1499.004 (Endpoint Denial of Service: Application or System Exploitation) |  |
| Create/Upload file | T1505.003 (Server Software Component: Web Shell) | T1059 (Command and Scripting Interpreter) | The techniques mapped here are the ones most used when reporting vulnerabilities that create or upload files. There are likely other techniques that could apply. |
| Write to existing file | T1565.001 (Data Manipulation) | T1059 (Command and Scripting Interpreter), T1574 (Hijack Execution Flow), T1554 (Compromise Client Software Binary) | The list of secondary impacts covers common techniques included in proof-of-concepts but is not exhaustive. |
| Change ownership or permissions | T1222 (File and Directory Permissions Modification) |  |  |
| Memory Modification (Memory Buffer Errors, Pointer Issues, Type Errors, etc.) | T1574 (Hijack Execution Flow), T1499.004 (Endpoint Denial of Service: Application or System Exploitation) |  | T1574 is not in the right tactic for this vulnerability. Propose adding it to Execution. "Hijack Execution Flow" is used here because exploitation for memory modification usually involves changing the execution flow of a process to execute the attacker’s code. |
| Memory Read (Memory Buffer Errors, Pointer Issues, Type Errors, etc.) | T1005 (Data from Local System), T1499.004 (Endpoint Denial of Service: Application or System Exploitation) | T1211 (Exploitation for Defense Evasion), T1212 (Exploitation for Credential Access) | May need a sub-technique. |

## Modify Configuration

Primary: T1478 (Install Insecure or Malicious Configuration)

## Create Account

Primary: T1136 (Create Account)

Secondary: T1078 (Valid Accounts)

## Disable protections

Primary: T1562 (Impair Defenses)

## Restart/Reboot

Primary: T1529 (System Shutdown/Reboot)

## Install App

Primary: T1476 (Deliver Malicious App via Other Means)

## Read from Memory

Primary: T1005 (Data from Local System)

## Obtain sensitive information

### Credentials

Primary: T1552 (Unsecured Credentials)

### Other data

Primary: T1005 (Data from Local System)

## Password Reset

Primary: T1098 (Account Manipulation)

## File Processing

### Read files

Primary: T1005 (Data from Local System)

Secondary: T1003.008 (OS Credential Dumping: /etc/passwd and /etc/shadow), T1552.001 (Unsecured Credentials: Credentials in Files)

Note: The list of secondary impacts covers common techniques included in proof-of-concepts but is not exhaustive.

### Delete files

Primary: T1485 (Data Destruction)

Secondary: T1499.004 (Endpoint Denial of Service: Application or System Exploitation)

### Create/Upload file

Primary: T1505.003 (Server Software Component: Web Shell)

Secondary: T1059 (Command and Scripting Interpreter)

Note: The techniques mapped here are the ones most used when reporting vulnerabilities that create or upload files. There are likely other techniques that could apply.

### Write to existing file

Primary: T1565.001 (Data Manipulation)

Secondary: T1059 (Command and Scripting Interpreter), T1574 (Hijack Execution Flow), T1554 (Compromise Client Software Binary)

Note: The list of secondary impacts covers common techniques included in proof-of-concepts but is not exhaustive.

### Change ownership or permissions

Primary: T1222 (File and Directory Permissions Modification)

## Memory Modification (Memory Buffer Errors, Pointer Issues, Type Errors, etc.)

Primary: T1574 (Hijack Execution Flow), T1499.004 (Endpoint Denial of Service: Application or System Exploitation)

Notes: T1574 is not in the right tactic for this vulnerability. Propose adding it to Execution.

“Hijack Execution Flow” is used here because exploitation for memory modification usually involves changing the execution flow of a process to execute the attacker’s code.

## Memory Read (Memory Buffer Errors, Pointer Issues, Type Errors, etc.)

Primary: T1005 (Data from Local System) ), T1499.004 (Endpoint Denial of Service: Application or System Exploitation)

Secondary: T1211 (Exploitation for Defense Evasion), T1212 (Exploitation for Credential Access)

Notes: May need a sub-technique.

# Exploitation techniques

This section provides common mappings for exploit techniques to ATT&CK IDs. Use this list together with the vulnerability type mappings section to determine the appropriate exploitation technique where applicable. This list can also be used independently to determine the appropriate exploitation technique

Tips for mapping exploitation techniques:

* What steps are necessary to exploit this vulnerability?

User executes a malicious file: T1204.002 (User Execution: Malicious File)

Where did this file come from?

A malicious link: T1204.001 (User Execution: Malicious Link)

An email: T1566.001 (Phishing: Spearphishing Attachment)

A third-party service: T1566.003 (Phishing: Spearphishing via Service)

Removable media: T1091 (Replication Through Removable Media)

User clicks a malicious link: T1204.001 (User Execution: Malicious Link)

Where did this link come from?

An email: T1566.002 (Phishing: Spearphishing Link)

A third-party service: T1566.003 (Phishing: Spearphishing via Service)

User visits a malicious website: T1189 (Drive-by Compromise)

Attacker exploits remote system application: T1190 (Exploit Public-Facing Application)

Attacker exploits an external service: T1133 (External Remote Services), T1210 (Exploitation of Remote Services)

Attacker uses valid/default credentials: T1078 (Valid Accounts)

Target uses hardcoded credentials: T1078 (Valid Accounts)

Attacker "sniffs" unencrypted network traffic: T1040 (Network Sniffing)