Session Hijacking

Michael J. Teske

Principal Author Evangelist-Pluralsight

Module Overview

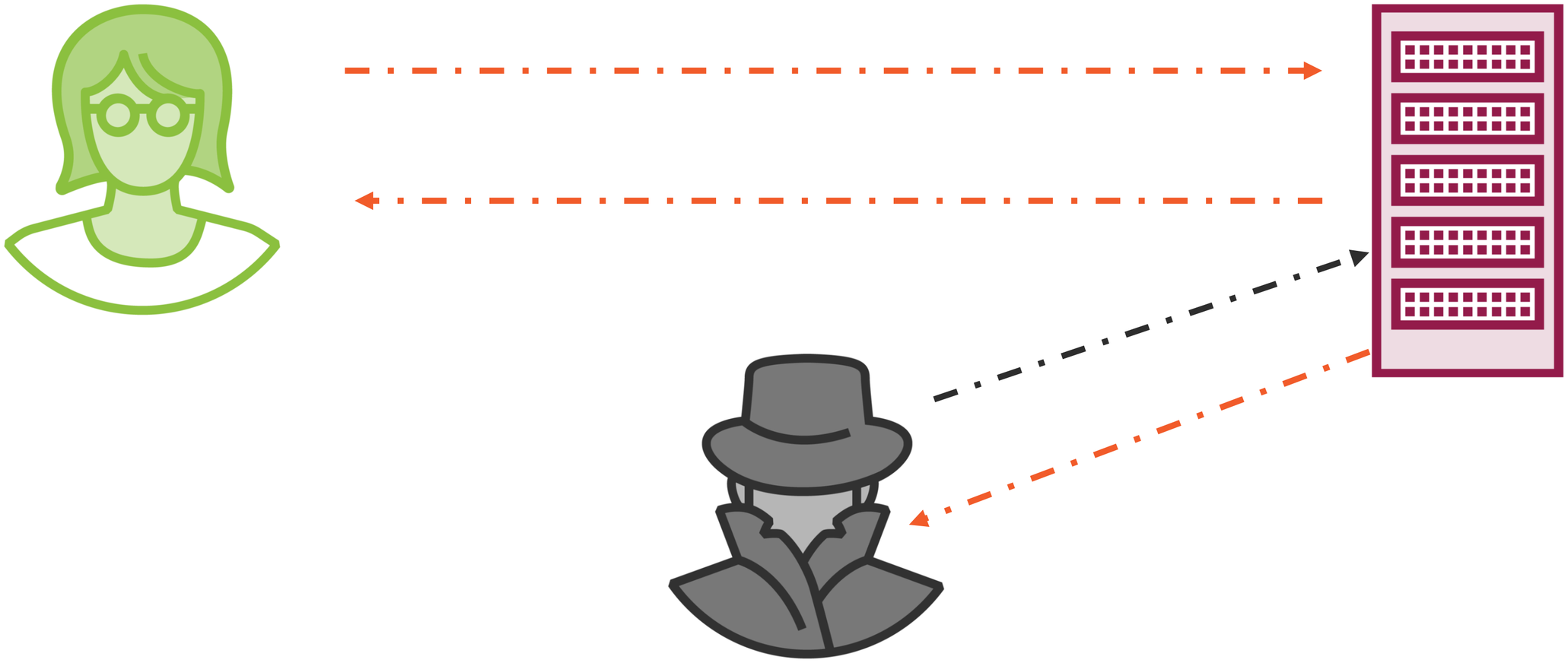
Session Hijacking

- Session Hijacking Concepts
  - Application layer
  - Network layer
- Tactics & Techniques
- Countermeasures

Session Hijacking Concepts

Targeting a session between two machines to gain access by guessing or stealing a valid session token

What Is Session Hijacking?



Session Hijacking

- Sniff the traffic between the user and server
- Monitor the traffic to help predict sequence numbering
- Desynchronize the session with the client
- Predict the session token and take over the session
- Inject packets to the target server

applications were tested for some form of misconfiguration, with an average incidence rate of 4.5%, and over 208k occurrences of CWEs mapped to this risk category. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for **A4:2017-XML External Entities (XXE)** is now part of this risk category.

- **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
- **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
- **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. **A8:2017-Insecure Deserialization** is now a part of this larger category.
- **A09:2021-Security Logging and Monitoring Failures** was previously **A10:2017-Insufficient Logging & Monitoring** and is added from the Top 10 community survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

A07:2021 – Identification and Authentication Failures

Factors

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage
22	14.84%	2.55%	7.40	6.50	79.51%	45.72%

Overview

Previously known as *Broken Authentication*, this category slid down from the second position and now includes Common Weakness Enumerations (CWEs) related to identification failures. Notable CWEs included are *CWE-297: Improper Validation of Certificate with Host Mismatch*, *CWE-287: Improper Authentication*, and *CWE-384: Session Fixation*.

Types of Session Hijacking

Passive session hijacking

Active session hijacking

Application Layer

Network Layer

Demo

Review sequencing from a packet capture

Tactics and Techniques

Tactics and Techniques

Man-in-the-middle

Man-in-the-browser

Session token prediction

Session sniffing

Cross site scripting

TCP/IP hijacking

Session Hijacking Tools

Burp Suite

Zed Attack Proxy

Burp Project Intruder Repeater Window Help — Burp Suite Community Edition v2022.6.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to https://globomantics.com:443 [52.26.82.140]

Forward Drop Intercept is on Action Open Browser

Comment this item

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: globomantics.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: navigate
8 Sec-Fetch-User: ?1
9 Sec-Fetch-Dest: document
10 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
11 Sec-Ch-Ua-Mobile: ?0
12 Sec-Ch-Ua-Platform: "Windows"
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

Inspector

Back

Method

Value

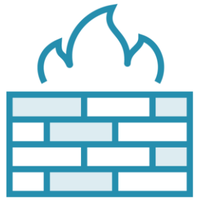
GET

Decoded from: Select

Cancel Apply changes

Countermeasures

Countermeasures



Use unpredictable session IDs

Use encryption and authentication measures via VPN or IPSec

Terminate sessions if not in use

Regenerate session key after authentication

Learning Check

- Passive session hijacking
- Application layer attack
- Network layer attack
- Burp Suite

Module Review

Key Learnings

Session hijacking concepts

Tactics, techniques and tools

Countermeasures

Up Next:
Evading IDS, Firewalls, and Honeypots