Proposal Info Title
Tinker Tailor Web App Spy: Investigate & Respond to Modern Web Application Attacks

Status
Accepted

Session Type
Briefings

Speaker
Bruce Wayne

Tracks
Application Security; Threat Hunting & Incident Response

Format
40-Minute Briefings

Abstract

It’s coming, and you aren’t ready—your first major web application security incident. Modern web apps power business-critical services and customer interactions in real time. But when your production application starts leaking sensitive data, executing unauthorized actions, or serving malicious responses, who are they going to call? You.

You’ve seen demos of SQL injection, XSS, and authentication bypasses and may even be aware of defenses like WAFs and secure coding practices. But are you prepared to investigate and respond when those protections fail? Would you know where to begin?

This talk connects traditional incident response methodology with the fast-moving world of modern web application attacks. You’ll learn how to investigate, contain, and remediate real-world attacks targeting web platforms. You’ll leave with a practical playbook for responding to web application incidents and preparation steps to take before your organization’s application is trending—for all the wrong reasons.

Presentation Outline

1. INTRODUCTION

We've spent years discussing vulnerabilities and defenses in web applications, yet incident responders often enter the picture only after damage occurs.

This section provides a concise overview of modern web application architectures, attack surfaces, and how security failures actually manifest in production environments.

---

2. WEB APPLICATION RISKS

To establish context, I'll outline risk levels associated with web applications:

1. Application serves public content
2. Application handles sensitive user data
3. Application performs privileged actions

Then I'll cover common web risks including data leakage, injection flaws, authentication bypass, privilege escalation, insecure APIs, business logic abuse, resource exhaustion, and supply-chain vulnerabilities.

---

3. WEB APPLICATION DEFENSE TOOLING

Incident response teams must understand application architecture, data flows, logging sources, and control points before incidents occur—not during them.

This section introduces defense mechanisms such as:

- Input validation and sanitization layers
- Output encoding and filtering
- Web Application Firewalls (WAFs)
- Runtime Application Self-Protection (RASP)

- API gateways and rate limiting

I'll also discuss detection strategies including:

1. Signature-based detection
2. Behavioral analysis
3. Anomaly detection models
4. Correlation across logs and telemetry

---

4. INCIDENT SCENARIO: INJECTION ATTACK LEADS TO RCE

With fundamentals established, we'll walk through a real-world scenario where a crafted payload exploits an injection vulnerability leading to remote code execution.

We'll investigate:

- Identifying malicious requests in logs
- Tracing attacker activity paths
- Determining blast radius
- Mapping exploit chain

---

5. INCIDENT SCENARIO: APPLICATION GOES VIRAL FOR MALICIOUS OUTPUT

In this scenario, an application begins serving harmful or malicious responses, triggering public exposure and reputational damage.

We'll explore:

- Detecting abnormal traffic spikes

- Identifying exploit patterns spreading publicly
- Assessing whether controls were blocking or only alerting
- Handling automated exploit campaigns

---

6. CONCLUSION & TAKEAWAYS

The session concludes with consolidated lessons learned from each incident type, highlighting common detection signals, investigation workflows, and response patterns.

You'll walk away with:

- A structured incident response playbook for web application attacks
- Preparation steps for security and IR teams
- Practical strategies to reduce investigation time and impact

---