




WEB APPLICATION PENTEST USE CASE

THE CHALLENGE

A global, multi-tenant professional services organization faced a website defacement attack and extortion from a malicious cyber actor. Redpoint provided weekend emergency response to gather information on the breach and identify a way forward. Redpoint engineers conducted a comprehensive web application PenTest (“web-app PenTest”) to identify possible breach points and vulnerabilities. The website was severely vulnerable to attacks, which allowed the attacker to gain unauthorized access to the backend MySQL database.





FINDINGS & OBSERVATIONS

-  The website was vulnerable to **Cross Site Scripting (XSS)** in seven locations, allowing the attacker to **steal session cookies and capture login credentials**. There were an additional 40 Document Object Model (DOM) XSS injection points throughout the website.
-  Redpoint engineers were able to identify two administrator login portals through brute forcing directories. These administrator login portals were both vulnerable to **Remote Code Execution (RCE) “Jackson”**. This particular attack has the potential to allow an attacker to **execute code on the application server** and OS commands due to failed object deserialization.
-  The website had numerous security weaknesses pertaining to **browser XSS misconfiguration, lack of an anti-CSRF Token, and failure to enforce strict transport security**. These vulnerabilities were embedded throughout the website, providing the attacker with a larger attack surface.








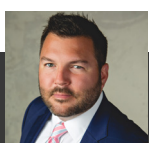
TOOLS & TECHNIQUES

-  **Manual web-app PenTest:** Certified penetration tester conducted a test in under three days to identify the most critical vulnerabilities. In **under 96 hours**, we were able to test **eight subdomains** and **43 directories** with over **8,500 exploits** leveraged against the network.
-  **Open Web Application Security Project (OWASP):** The web-app PenTest follows the OWASP top 10 web application security risks, exploiting the website to the fullest extent possible and mimicking a malicious actor.



OUTCOMES

-  Rapidly identified **383 vulnerabilities** coupled with remediation for the top 10 most critical vulnerabilities.
-  Provided an **in-depth report** highlighting vulnerabilities, attack vectors, and insight to support a holistic cyber security approach.
-  Enabled leadership across the organization to gain a better understanding of cyber security and **how to better secure their website from future attacks**, informing them about website exploitation and demonstrating how it could lead to network compromise and takeover.
-  Based on recommendations from Redpoint’s engineers, the organization directed their third-party website developers to **implement the security control recommendations** to **secure the website from future attacks**.
-  Through Redpoint’s recommendation, the client **retained counsel** to assess the data privacy concerns.



TAB BRADSHAW
 tab@redpointcyber.com
 Chief Operating Officer
 Redpoint Cybersecurity
 www.redpointcyber.com