

8-2 Cyber Playbook Submission

Joshua Merren

Southern New Hampshire University

CYB-310-13414-M01 Network Defense

Professor Megan Buckner

22 October 2024

The screenshot shows the Microsoft OneNote application interface. The title bar at the top reads "OneNote". The ribbon menu includes "Home", "Insert", "Draw", "View", and "Tell me". The "Home" tab is active, showing options for "Paste", "Cut", "Copy", "Format", and "Dictate". The "Dictate" button is highlighted with a microphone icon. The left sidebar shows a list of sections under the "Cyber Playbook" folder. The sections are: "Component Security", "Sample Scripts", "Connection Security", "Data Security", "Threat Modeling and Analysis", "Human Security", "Organizational Security", "Societal Security", "CIS Critical Security Controls", "Software Security", "System Security", "Legal", and "New Section 1". The "Component Security" section is selected, and its content is displayed in the main area. The content is titled "OWASP Best Practices: Use of Web Application Firewalls" and includes a date "Tuesday, October 22, 2024" and a time "10:39 AM". Below the title is a PDF icon and the text "Best_Practices_WAF_v...". The main content area shows a large image of the OWASP logo and the text "Best Practice: Use of Web Application Firewalls" and "OWASP Papers Program". The text "Best Practices:" and "Use of Web Application" is visible at the bottom of the image.

In our cyber playbook, I find the "OWASP Best Practices: Use of Web Application Firewalls" section handy for me now and in the future. This part discusses how to set up and use web application firewalls (WAFs), which are essential for protecting websites from online threats and hacks. WAFs are great because they check and control the data from a website, helping to block harmful content and prevent attacks.

Understanding how to use WAFs is crucial because the number of cyber attacks is going up as more businesses and services move online. Following the OWASP best practices is not just about learning, it's about gaining practical knowledge on the best ways to set up these firewalls

to make them as effective as possible. This knowledge is not just theoretical; it's something I can apply directly to protect a company's website, making me feel empowered and capable in the face of cyber threats.

Considering how common problems like hacking attempts and data theft are, knowing how to defend against them using WAFs is very important. This section is precious as I plan to focus on network security in my career. It offers clear and practical advice on managing and fixing issues with web application firewalls. By understanding these best practices, I'm better equipped to keep websites safe and secure in any job I take on in the future.