**GenCyber 2023 PreCamp Day 2: Session 1 - Web Security with Adversary Mindset – Answer-Key**

**1) What is the goal of thinking like an adversary in web security?**

B. To identify and anticipate potential security threats and vulnerabilities in your web application

**2) What are some examples of potential adversaries in web security?**

A. Script kiddies and hackers

**3) What is the process for identifying and prioritizing potential threats and vulnerabilities to a system or application?**

D. Threat modeling

**4) What is the purpose of the Threat Modeling Manifesto?**

B. To provide a framework for understanding the purpose and scope of threat modeling

**5) What is OWASP Threat Dragon?**

C. An open-source, web-based threat modeling tool

**6) What is the Microsoft Threat Modeling Tool?**

C. A free, standalone tool for creating and analyzing threat models for software applications

**7) What should be included in a vulnerability report?**

A. A detailed description of the vulnerability, including its potential impact and severity

**8) What is the recommended course of action for software vendors when responding to vulnerability reports?**

B. Provide patches or updates to address identified vulnerabilities as soon as possible

**9) What is Cobalt Strike?**

C. A commercial penetration testing tool with advanced features

**10) What is Nmap used for in web security?**

C. Scanning and mapping network hosts and services

**Please provide screenshots from the completion screen for each level (11 in total):**

1. Plaintext answer inside of the HTML
2. Didn’t upload password so there is no password submit anything to the box
3. HTML form has password.php listed, put in URL to go to this file
4. Change HTML form so it sends to your email instead of the listed email
5. Change HTML form so it sends to your email instead of the listed email
6. Put 11111111 and aaaaaaaa into converter to see what type of encryption it is, it should follow ASCII id +0 then ASCII id +1 etc.
7. use (;) to escape Sam’s script and then ls to list the directory (;ls), find the php file and put it in the URL to go to this file
8. The program is a shtml file, use <!--#exec cmd="ls ../"--> to inject into the server side program, this will list the directory, give use the name of the php file like in #7
9. Go back to 8 and change injection to <!--#exec cmd="ls ../../9"--> so that it will show lvl 9 directory, same steps as 8 and 7
10. Directory of songs, song given was a Elton john song, and e to the end of the url, this lets you see other directories, (cant see hidden directories) add [.htaccess](https://httpd.apache.org/docs/current/howto/htaccess.html) to the end of the directory list (/e/l/t/o/n/.htaccess) says it is ignoring DaAwnser, put this into url, “password is (easy) just look a bit harder”