CTF-8: Exploiting Web Application Session IDs

Due Nov 15, 2021 at 11:59pm **Points** 100 **Questions** 6
Available Nov 8, 2021 at 7am - Nov 18, 2021 at 11:59pm **Time Limit** None

Instructions

MODULE 12

CTF 8: Exploiting Web Application Sessions IDs

The contents and instructions for this assignment are documented in the CTF Lab Assignment titled "Lab-Assignment-8: Exploiting Web Application Session IDs". The objective of this assignment is to demonstrate the common problem within web applications and network protocols of enumeration sequencing. This has been a common problem throughout the history of network resources, resulting in man-in-the-middle attack, hijacking and session playback attacks. In this exercise, we will implement the technique used to evaluate the entropy of a packet based on the amount of information which is being changed for each packet being sent over the wire, specifically analyzing session ID negotiation transactions. In this exercise, we will use the DVWA web application and generate automated packets to mimic real network traffic, then analyze the results to determine how well the application protocol generates its session IDs. To perform this activity, we will use a **Web Browser Proxy called Burp (https://usflearn.instructure.com/courses/1598910/files/116260896/download?wrap=1)** **(https://usflearn.instructure.com/courses/1598910/files/116260896/download?download_frd=1)** , which will monitor the traffic being produced and provide analytics on the results from our capture. In the process of this exercise, you will also learn how to setup a web-based proxy, common activity for an IT network administrator.

This quiz is no longer available as the course has been concluded.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	180 minutes	80 out of 100 *

* Some questions not yet graded

Score for this quiz: **80** out of 100 *
Submitted Nov 15, 2021 at 11:13pm
This attempt took 180 minutes.

Question 1 — 20 / 20 pts

What is the name of the variable that contains the session ID created when the "Generate" button is invoked?

Correct!

dvwaSession

Correct Answers

dvwaSession

dvwaSession=

Correct it is "dvwaSession"

Question 2

10 / 10 pts

If you had to use one mathematical word to describe the uniqueness of the session IDs being generated when the security level was set to low, it would be?

Correct!

ascending

Correct Answers

sequential

ascending

+1

+one

ordered

incremental

Correct, anyone of the following describe the order, sequential, +1, ascending

Question 3

20 / 20 pts

What HTTP Request header tag contains the session ID?

Correct!

cookie

Correct Answers

Cookie

The Cookie tag

"Cookie"

Set-Cookie

Set-Cookie:

Cookie:

Correct, it is the Cookie tag

Question 4

10 / 10 pts

What is the name of the local web proxy used within this exercise?

Correct!

burp

Correct Answers

Burp Suite

Burp

Correct, it is the Burp Suite

Unanswered

Question 5

0 / 20 pts

Upload a screenshot of your results using the Burp Suite and showing the Proxy/HTTP History tab after invoking multiple session ID generation request.

Question 6

20 / 20 pts

Using the Burp Suite and running the sequencer with the security level set to high, what is the "effective entropy to be in bits"?

- Less then 10
- 11 to 30
- 31 to 60
- 61 to 90

Correct!

- 91 to 150

- 151 to 170
- Higher then 170

Correct, it generally is in the range of 91 to 150 bits

Quiz Score: **80** out of 100