Assignment - PSO 6

Purdue CS426 - Computer Security - Prof. Spafford

Harris Christiansen - April 22, 2018
christih@purdue.edu

Read the following:

- Get vs. Post - https://www.youtube.com/watch?v=UObINRj2EGY
- HTTPWatch - http://blog.httpwatch.com/2009/02/20/how-secure-are-query-strings-over-https/
- Session Cookie (note random number is Session ID) - https://www.youtube.com/watch?v=90PsaIatDYo
- Stored XSS - https://www.youtube.com/watch?v=7M-R6U2i5iI
- Reflected XSS - https://www.youtube.com/watch?v=V79Dp7i4LRM
- HttpOnly Cookie - https://stackoverflow.com/questions/14691654/set-a-cookie-to-httponly-via-javascript
- Cross Site Request Forgery - https://www.youtube.com/watch?v=vRBihr41JTo
- SQL Injection - https://www.youtube.com/watch?v=_jKylhJtPmI
- https://www.youtube.com/watch?v=ciNHn38EyRc
- OWASP Top 10 Vulnerabilities - https://www.owasp.org/index.php/Top_10-2017_Top_10
- NMAP -https://www.networkcomputing.com/networking/nmap-tutorial-common-commands/520799832https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/
- TCP Dump - https://www.tcpdump.org/tcpdump_man.html
- RAW Sockets - http://opensourceforu.com/2015/03/a-guide-to-using-raw-sockets/

Problem 1

(60 pts.)

What are HTTP Cookies in a few sentences?

- Answer

How can HTTP Cookies be used to create a stateful connection with a webserver?

- Answer

When a server side app responds with a session cookie what is the minimum information that is usually stored in the cookie sent to the client machine?

- Answer

What could potentially happen if an attacker gets access of your cookie that contains session information (i.e. session id)? Explain two ways this risk is mitigated.

- Answer

Problem 2

Is it a good idea to store sensitive information in a cookie sent back to a client device? Explain. (20 pts.)

- Answer

Problem 3

What is Stored Cross Site Scripting (XSS) and where is the malicious code run (i.e. web server or client machine)? Explain how the exploit works and how you can mitigate the risk as a software developer and user. (40 pts.)

- Answer

Problem 4

What is Reflected Cross Site Scripting (XSS) and where is the malicious code run (i.e. web server or client machine)? Explain how the exploit works and how you can mitigate the risk as a software developer and user. (40 pts.)

- Answer

Problem 5

What is Cross Site Request Forgery and where is the malicious code run? Are web pages that use GET or POST request for forms more or less susceptible to the attack? Explain how the exploit works and how you can mitigate the risk as a software developer and user. (60 pts.)

- Answer

Problem 6

What is a SQL Injection Attack and where is the malicious code run? Explain how the exploit works and how you can mitigate the risk as a software developer and user. (40 pts.)

- Answer

Problem 7

(40 pts.)

What is the difference between a GET and POST Request? Explain.

- Answer

If you use HTTPS, will the query arguments of the GET be encrypted? Explain.

- Answer

If you use HTTPS, will the arguments of the POST be encrypted? Explain.

- Answer

Why are GET requests considered less secure than POST Requests? Explain.

- Answer

Problem 8

List 5 things NMAP can do and the associated commands. If you are an attacker, how can you use NMAP as part of an attack? Explain. (70 pts.)

- Answer

Problem 9

List 5 things TCP Dump can do and the associated commands. If you are an attacker, how can you use TCP Dump as part of an attack? Explain. (70 pts.)

- Answer

Problem 10

From the readings on an Evening with Bernard and Stalking the Wiley Hacker explain how an attacker can conceal his/her location and identity when carrying out attacks. What challenges does this create for security professionals responsible for preventing these types of attacks (40 pts.)

- Answer

Problem 11

(60 pts.)

- What is the Raw Socket API?
  - Answer

- How can you use it to prevent/detect an attack?
  - Answer

- How can it be used to execute an attack?
  - Answer