

Lesson 07



Web Application Security

Overview

Web applications are often the first face that users see in a service or application. They are usually also the surface areas most targeted by attackers and often the most vulnerable. In this lesson, we'll look at advanced techniques and methods for attacking web applications and will practice these techniques. In exploring how various security mechanisms can be bypassed, you will strengthen your fundamental understanding of how mechanisms in defending web applications work and how they can be properly implemented.

Objectives

After completing this lesson, students will be able to:

1. describe advanced techniques used to attack web applications;
2. describe and communicate common techniques for protecting web applications;
3. describe and communicate basic and advanced security issues such as click jacking and DOM based XSS; and
4. perform and describe advanced techniques and attacks such as CSRF

Lesson Resources

Topics	Required Reading?	Resource
What is a DOM?	Yes	http://www.w3schools.com/js/js_htmlDOM.asp
Cookie Security	No, but highly recommended	https://www.usenix.org/system/files/conference/usenixsecurity15/sec'paper-zheng-updated.pdf
HSTS	No	https://www.owasp.org/index.php/HTTP_Strict_Transport_Security
DOM XSS	Yes	https://www.owasp.org/index.php/DOM_Based_XSS
CSRF	Yes	https://owasp.org/www-community/attacks/csrf
cookies	Yes	http://www.w3schools.com/js/js_cookies.asp