Agenda

- Web Application Attacks
- Case Study: Remote Code Execution on Shopify
- Cookies
Web Application

- Almost everything that can be accessed via a browser is called a "web application".

- Web applications vs web sites: websites are primarily informational (static contents), web applications primarily allow the user to perform actions (dynamic content). They are not entirely exclusive.

- websites: [http://www.cnn.com](http://www.cnn.com). Most of the work is done at the server.

- web applications: gmail, google docs. Work is done at the browser.
Web Application Attacks

Web application attacks involve performing intrusive penetration tests on public-facing web servers, applications, and back-end databases.
Remote code execution: Having gained privileged access or sys admin rights access, the attacker can run commands or execute a command at will on the remote systems.
Case Study: a remote code execution vulnerability on Shopify

- https://hackerone.com/reports/73567
- https://prakharprasad.com/shopify-remote-code-execution/
- https://www.youtube.com/watch?v=ht77VFp0TKc
Other remote code execution bugs on hackerone

- Remote code execution on an Army website
  https://hackerone.com/reports/188284
- RCE in profile picture upload on Hackerone
  https://hackerone.com/reports/135072
- uber.com may RCE by Flask Jinja2 Template Injection
  https://hackerone.com/reports/125980
- RCE on Yahoo
  https://hackerone.com/reports/6674
- Twitter offers a minimum of $15,000 for remote code execution vulnerabilities.
  https://hackerone.com/twitter?view_policy=true
- Want to see more RCE stories? Just search "remote code execution hackerone"
Buffer Overflow

Buffer overflow: Attempting to push more data than the buffer can handle, thus creating a condition where further compromise might be possible.
Buffer overflow vulnerabilities on hackerone

- AddressSanitizer reports a global buffer overflow in `mkgmtime()` function
  [https://hackerone.com/reports/104011](https://hackerone.com/reports/104011)
- hotshot pack_string Heap Buffer Overflow
  [https://hackerone.com/reports/104022](https://hackerone.com/reports/104022)
- heap buffer overflow in `enchant_broker_request_dict()`
  [https://hackerone.com/reports/104013](https://hackerone.com/reports/104013)
- PHP Heap Overflow Vulnerability in `imagecrop()`
  [https://hackerone.com/reports/1356](https://hackerone.com/reports/1356)
Client-side attack: Using malware on a user’s workstation or laptop, within an internal network, acting in tandem with a malicious server or application on the Internet (outside the protected network).
Cookies and attachments: Using cookies or other attachments (or the information they contain) to compromise security.
Cross-site scripting (XSS)

Cross-site scripting: a code injection attack that allows an attacker to execute malicious JavaScript in another user’s browser. This is not an attack on the web application but rather on users of the server to launch attacks on other computers that access it.
Directory traversal/command injection: Exploiting a web application server, gaining root file directory access from outside the protected network, and executing commands, including data dumps. Visit here for more information: http://www.acunetix.com/websitesecurity/directory-traversal/
Header manipulation: Stealing cookies and browser URL information and manipulating the header with invalid or false commands to create an insecure communication or action.
Integer overflow: Creating a mathematical overflow which exceeds the maximum size allowed. This can cause a financial or mathematical application to freeze or create a vulnerability and opening.
LDAP is often used by organizations as a central repository for user information and as an authentication service.

**LDAP injection**: Creating fake or bogus ID and authentication LDAP commands and packets to falsely ID and authenticate to a web application.
Malicious add-ons: Using software plug-ins or add-ons that run additional malicious software on legitimate programs or applications.
SQL injection: Injecting Structured Query Language (SQL) commands to obtain information and data in the back-end SQL database.
Watering-hole attack: a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected. - wikipedia
Zero-day: Exploiting a new vulnerability or software bug for which no specific defenses yet exist.
Cookies
HTTP and HTTPs websites

- HTTP websites: http://nicolekidmanofficial.com/
  http://www.brunomars.com/
- HTTPs websites: https://www.google.com,
  https://www.bankofamerica.com
Cookies: To help a web server track a user’s history, web browsers allows the web servers to store a cookie on the user’s hard drive. A cookie is simply a text file that contains details gleaned from past visits to a website. A cookie might include the user’s username, credit card information the user has entered, and so on. Later, when the user sends a request to the web server, the server can access the cookie instead of requiring that the user reenter the information.
Security Features of Cookies

- secure flag - send for secure connections only
- HttpOnly - not accessible to script
View, Delete, Edit Cookies

- Google Chrome - Settings-Privacy-Content settings-All cookies and site data.
- Google Chrome - F12-Application-Cookies
- Google Chrome - EditThisCookie https://chrome.google.com/webstore/detail/editthiscookie/fngmhnnpilhplaeedifhccceomclgf?hl=en
- Firefox - Firebug cookies editor
References

A large portion of the material is adapted from:

- Fundamentals of Information Systems Security - David Kim, Michael G. Solomon
- Excess XSS A comprehensive tutorial on cross-site scripting, created by Jakob Kallin and Irene Lobo Valbuena
  https://excess-xss.com/
- Web application http://searchsoftwarequality.techtarget.com/definition/Web-application-Web-app
- Cookie Stealing by Cross Site Scripting Tutorial
  https://www.youtube.com/watch?v=4SS1KQuSffI
  http://docs.spring.io/spring-security/site/docs/3.1.x/reference/springsecurity.html