Cheatography

Web Application Hacking Cheat Sheet

by fahad via cheatography.com/77149/cs/18939/

Web Application Concepts

Web application : are that applications that are running on a remote application server and available to the client via the internet.

We have three Users of web application :

Server Administrator : is the one who take care of the web server in terms of safety,security,functioning, and preformance. it is responsible for estimating Security measures and deploying security models,finding and eliminating vulnerbilites.

Application Administrator : is responsible for the management and configuration required for the web application. it ansures the avalibility and high preformance of the web application.

Clients: are those endpoints which interact with the web server or application server.

How does Web Application Works ?

A Web Application functions in two steps, i.e., **Front-end and Back-end**

Front-end : where the user is interacting with the web pages.

How does Web Application Works ? (cont)

Back-end : All processing was controlled and processed on the back-end.

Server-side languages include:

Ruby on Rails ,PHP, C#,Java, Python.

Client-side languages include:

Css.Javascript,HTML.

The web application is basically working on the following layers: -

• **Presentation Layer**: Presentation Layer Responsible for displaying and presenting the information to the user on the client end.

• **Logic Layer**: Logic Layer Used to transform, query, edit, and otherwise manipulate information to and from the forms.

• **Data Layer**: Data Layer Responsible for holding the data and information for the application as a whole.

Web 2.0 :

Web 2.0 is the generation of world wide web websites that provide dynamic and flexible user interaction.

Web App Hacking Methodology

Analyze web Applications

Analyzing Web application includes observing the functionality and other parameters to identify the vulnerabilities, entry points and server technologies

Attack Authentication Mechanism

By exploiting the authentication mechanism using different techniques, an attacker may bypass the authentication or steal information.

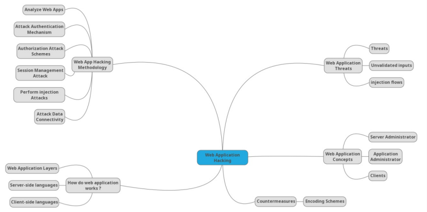
Authorization Attack Schemes

Attacker by accessing the web application using low privilege account, escalate the privileges to access sensitive information.

Session Management Attack

As defined earlier, Session management attack is perforrned by bypassing the authentication in order to impersonate a legitimate authorized user.

Mind map



Countermeasures

Encoding schemes

web Applicaitons uses different encoding schemes for securing their data.

These encoding schemes are categorized into the two categories.

URL Encoding

URL Encoding is The encoding technique for secure handling of URL. In URL Encoding, URL is convened into an ASCII Format for secure

HTML Encoding

Similar to URL Encoding, HTML encoding is a technique to represent unusual Characters with an HTML code.

Web Application Threats

Cookie Poisoning : Cookie poisoning is an effort by an unauthorized person to access and control aspects of the data in a cookie, usually in order to steal someone's identity or financial information.

Web Application Threats (cont)

Insecure Storage : a common vulnerability that occurs when sensitive data is not stored securely.
Information Leaking : category of software vulnerabilities in which information is unintentionally disclosed to end-users.
Directory Traversal : is an HTTP attack which allows attackers to access restricted directories and execute commands outside of the web server's root directory.
Parameter/Form Tempering : is a form of Web-based attack in which certain parameters in the URL or Web page form field data entered by a user are changed without that user's authorization.
DOS Attack : is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.
Buffer Overflow : is a bug in a computer program that can lead to a security vulnerability.

Web Application Threats (cont)

Log tampering : involve an attacker injecting, deleting or otherwise tampering with the contents of web logs typically for the purposes of masking other malicious behavior.
SQL injection : SQL Injection is basically the injection of malicious SQL queries.
Cross-Site(XSS): is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users.
Cross-Site Request Forgery : is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.
Secuirty Misconfiguration : Security misconfiguration vulnerabilities could occur if a component is susceptible to attack due to an insecure configuration option.
Broken Session Management : these types of weaknesses can allow an attacker to either capture or bypass the authentication methods that are used by a web application.

Web Application Threats (cont)

DMZ(demilitarized zone) Attack : is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network.
Session Hijacking : is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system.
Network Access Attacks : is a type of vulnerability that is used to acess a network unauthorized.

Web Application Threats More in-depth

Unvalidated Input : refers to the processing of non-validated input from the
client to the web application or backend sewers.
Injection Flaws: Injection attacks work with the support of web application Vulnerabilities if a web application is vulnerable that it allows untrusted input to be executed. Injection flaws include the following:
. SQL Injection
. Command Injection
. LDAP Injection

Web Application Threats More in-depth (cont)

command injection can be done by any oi the following methods:
- Shell Injection
- File Injection
- HTML Embedding
-LDAP injection is a technique that also takes advantage of non-validated
input vulnerability.
Denial—of—Service DoS Attack : An attacker may perform a Dos attack in the following ways: -
1. User Registration DoS
An attacker may automate the process to keep registering with fake
accounts.
2. Login DoS
Attacker attempt to send login requests repeatedly.
3. User Enumeration
An attacker may attempt to Lry different usernarne password combinations from a dictionary file.
4. Account Lockout
An attacker is attempting to lock the legitimate account by attempting invalid passwords.