

UNIT II:

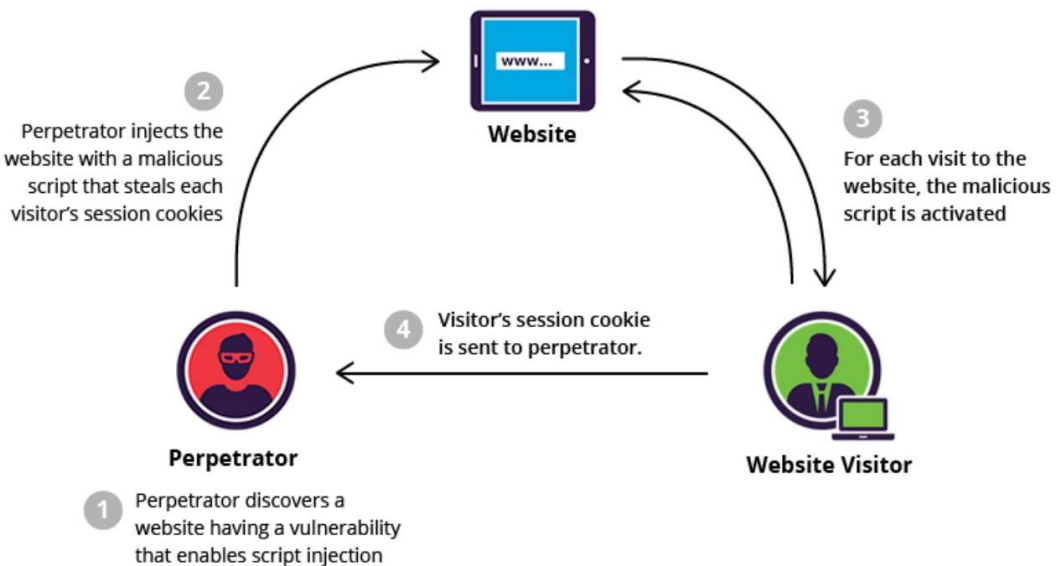
Web Vulnerabilities & Countermeasures



Christian B. Peña



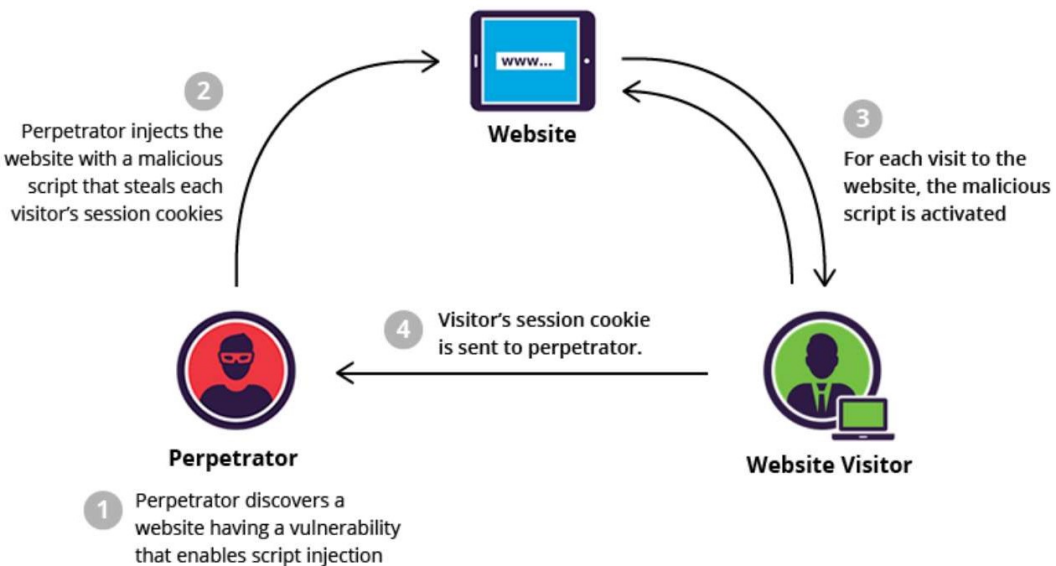
CROSS-SITE SCRIPTING (XSS)



Cross-site scripting (XSS) is a type of vulnerability which is usually found in web applications. XSS allows an attacker to inject client-side script to the web pages accessed by the other users.

When cybercriminals use cross-site scripting, they inject code on a site via form fields or other areas of user inputs in order to target website users. When the user's browser executes this code, attackers can hijack user sessions, covertly track session data, or even display spam content on an otherwise legitimate site.

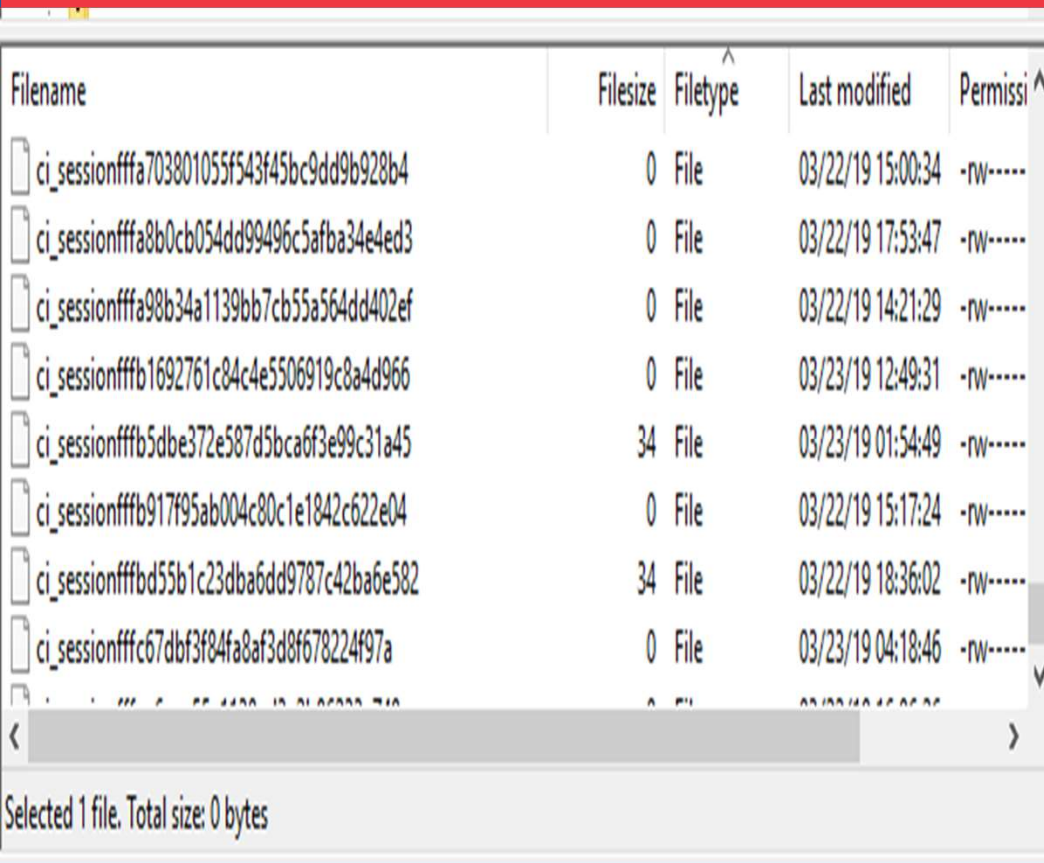
CROSS-SITE SCRIPTING (XSS)



How to Prevent Cross-Site Scripting

- Keep Software Updated
- Sanitize Input Fields
- Use Client and Server-Side Form Validation
- Use a Web Application Firewall

TEMPORARY FILE ABUSE



Filename	Filesize	Filetype	Last modified	Permissi
ci_sessionffa703801055f543f45bc9dd9b928b4	0	File	03/22/19 15:00:34	-rw-----
ci_sessionffa8b0cb054dd99496c5afba34e4ed3	0	File	03/22/19 17:53:47	-rw-----
ci_sessionffa98b34a1139bb7cb55a564dd402ef	0	File	03/22/19 14:21:29	-rw-----
ci_sessionfffb1692761c84c4e5506919c8a4d966	0	File	03/23/19 12:49:31	-rw-----
ci_sessionfffb5dbe372e587d5bca6f3e99c31a45	34	File	03/23/19 01:54:49	-rw-----
ci_sessionfffb917f95ab004c80c1e1842c622e04	0	File	03/22/19 15:17:24	-rw-----
ci_sessionfffb55b1c23dba6dd9787c42ba6e582	34	File	03/22/19 18:36:02	-rw-----
ci_sessionfffc67dbf3f84fa8af3d8f678224f97a	0	File	03/23/19 04:18:46	-rw-----

Selected 1 file. Total size: 0 bytes

Many applications and utilities could never even run without temporary files, which typically provide accessible behind-the-scenes workspace. We list here just a few examples of the practical roles temporary files fulfill:

- Interim versions of files being manipulated by applications like word processors or graphics programs.
- Temporary database query caches, providing accessibility to previously selected data without requiring another database access. While not normally used for transactions involving a local database, they are a regular feature of applications that make queries to remote databases or XML-based web services.

TEMPORARY FILE ABUSE

Filename	Filesize	Filetype	Last modified	Permissi
ci_sessionffa703801055f543f45bc9dd9b928b4	0	File	03/22/19 15:00:34	-rw-----
ci_sessionffa8b0cb054dd99496c5afba34e4ed3	0	File	03/22/19 17:53:47	-rw-----
ci_sessionffa98b34a1139bb7cb55a564dd402ef	0	File	03/22/19 14:21:29	-rw-----
ci_sessionfffb1692761c84c4e5506919c8a4d966	0	File	03/23/19 12:49:31	-rw-----
ci_sessionfffb5dbe372e587d5bca6f3e99c31a45	34	File	03/23/19 01:54:49	-rw-----
ci_sessionfffb917f95ab004c80c1e1842c622e04	0	File	03/22/19 15:17:24	-rw-----
ci_sessionfffb55b1c23dba6dd9787c42ba6e582	34	File	03/22/19 18:36:02	-rw-----
ci_sessionfffc67dbf3f84fa8af3d8f678224f97a	0	File	03/23/19 04:18:46	-rw-----
Selected 1 file. Total size: 0 bytes				

- Temporary storage for files in the process of being transferred. These are the files named by PHP's superglobal `$_FILES['userfile']['tmp_name']` variable.
- System files being used to store session properties (or other temporary data) between HTTP requests. For session properties, these are the files named for the session ID (typically something like `sess_7483ae44d51fe21353afb671d13f7199`).
- Interim storage for data being passed either to other applications or libraries that expect file-based input, or to later instances of the same application (like messages in a mail queue).

TEMPORARY FILE ABUSE

Filename	Filesize	Filetype	Last modified	Permissi
ci_sessionffa703801055f543f45bc9dd9b928b4	0	File	03/22/19 15:00:34	-rw-----
ci_sessionffa8b0cb054dd99496c5afba34e4ed3	0	File	03/22/19 17:53:47	-rw-----
ci_sessionffa98b34a1139bb7cb55a564dd402ef	0	File	03/22/19 14:21:29	-rw-----
ci_sessionfffb1692761c84c4e5506919c8a4d966	0	File	03/23/19 12:49:31	-rw-----
ci_sessionfffb5dbe372e587d5bca6f3e99c31a45	34	File	03/23/19 01:54:49	-rw-----
ci_sessionfffb917f95ab004c80c1e1842c622e04	0	File	03/22/19 15:17:24	-rw-----
ci_sessionfffb55b1c23dba6dd9787c42ba6e582	34	File	03/22/19 18:36:02	-rw-----
ci_sessionfffc67dbf3f84fa8af3d8f678224f97a	0	File	03/23/19 04:18:46	-rw-----
Selected 1 file. Total size: 0 bytes				

As this brief list suggests, temporary files are perfectly capable of containing some of the most private information on your computer.

In most cases, an exploit would require that the attacker have shell or FTP access to the locations of your temporary files. But if such an attacker were to get in, a file named `2020_Confidential_Sales_Strategies.tmp` would probably be of great interest to him, especially if he worked for your employer's biggest competitor. Similarly, a file named something like `sess_95971078f4822605e7a18c612054f658` could be interesting to someone looking to hijack a session containing a user's login to a shopping site.

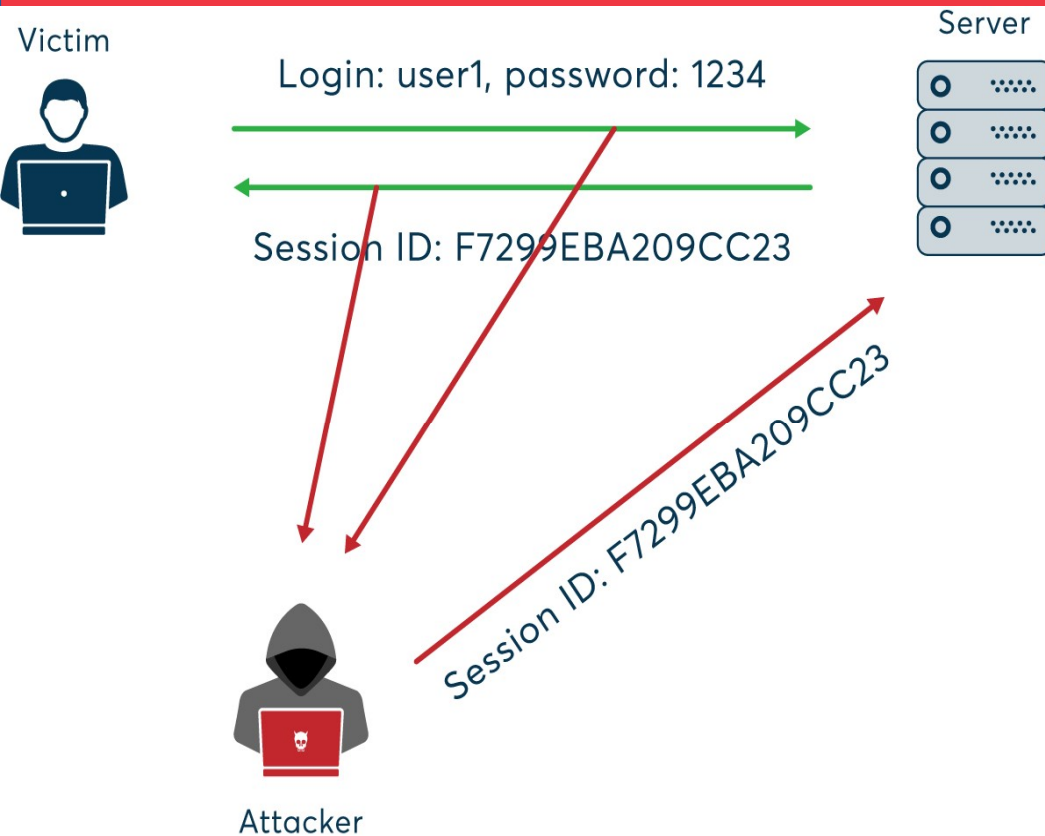
TEMPORARY FILE ABUSE

Filename	Filesize	Filetype	Last modified	Permissi
ci_sessionffa703801055f543f45bc9dd9b928b4	0	File	03/22/19 15:00:34	-rw-----
ci_sessionffa8b0cb054dd99496c5afba34e4ed3	0	File	03/22/19 17:53:47	-rw-----
ci_sessionffa98b34a1139bb7cb55a564dd402ef	0	File	03/22/19 14:21:29	-rw-----
ci_sessionfffb1692761c84c4e5506919c8a4d966	0	File	03/23/19 12:49:31	-rw-----
ci_sessionfffb5dbe372e587d5bca6f3e99c31a45	34	File	03/23/19 01:54:49	-rw-----
ci_sessionfffb917f95ab004c80c1e1842c622e04	0	File	03/22/19 15:17:24	-rw-----
ci_sessionffbd55b1c23dba6dd9787c42ba6e582	34	File	03/22/19 18:36:02	-rw-----
ci_sessionfffc67dbf3f84fa8af3d8f678224f97a	0	File	03/23/19 04:18:46	-rw-----
Selected 1 file. Total size: 0 bytes				

How to Prevent Temporary File Abuse

1. Regularly check temporary files and remove those not needed anymore
2. Do not store confidential information in a temporary file.

SESSION HIJACKING



Session hijacking occurs when a session token is sent to a client browser from the Web server following the successful authentication of a client login. A session hijacking attack works when it compromises the token by either confiscating or guessing what an authentic token session will be, thus acquiring unauthorized access to the Web server.

COOKIE STEALING WITH XSS

COOKIE STEALING WITH XSS

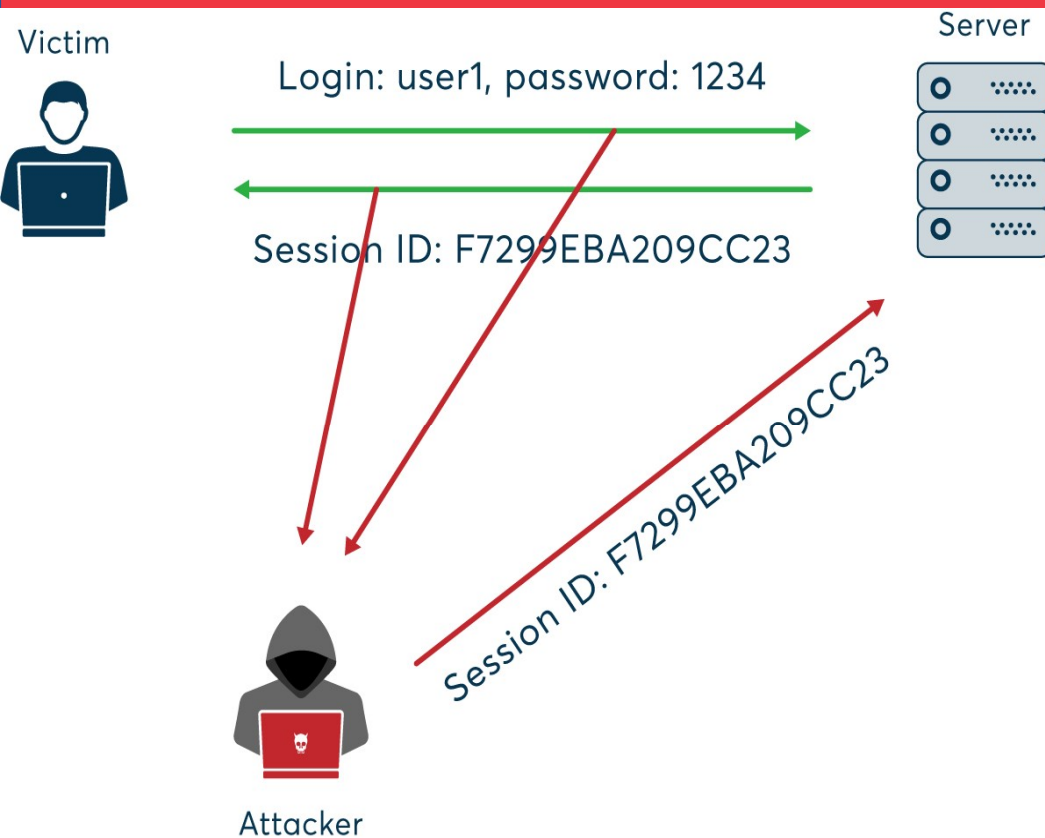


One of the ways you can do to hijack other user's session is by using XSS attack to steal their cookies.

What are Cookies?

Cookies are files created by websites you visit. They make your online experience easier by saving browsing information. With cookies, sites can keep you signed in, remember your site preferences, and give you locally relevant content.

SESSION HIJACKING



How to Prevent Session Hijacking

1. Install an SSL Certificate
2. Install a Security Plugin
3. Update your Website



**THE
END**