**EBook Gratuito**

# APPRENDIMENTO

# XSS

Free unaffiliated eBook created from
**Stack Overflow contributors.**

#xss

# Sommario

# Di

# Capitolo 1: Iniziare con xss

## Osservazioni

**Panoramica** Cross-Site Scripting, comunemente indicato come XSS, è un tipo di attacco di iniezione di applicazioni Web in cui gli script dannosi vengono iniettati in siti Web affidabili.

Gli attacchi XSS si verificano quando un utente malintenzionato sfrutta, o "sfrutta", un difetto in un'applicazione Web per inviare il carico utile dell'attaccante al browser del client. Questi difetti si verificano in genere quando un'applicazione Web invia l'input dell'utente al browser senza prima convalidarlo o codificarlo.

Un payload XSS viene eseguito all'interno del dominio del "sito attendibile" e ha il potenziale per accedere ai cookie di quel sito Web, modificando il DOM della pagina e persino abusando del browser o delle estensioni del client.

**Tipi XSS**

Sebbene il risultato finale sia lo stesso per tutti gli attacchi XSS (un carico utile controllato da un utente malintenzionato nella risposta del server), esistono tre diversi tipi di vulnerabilità XSS.

- **XSS memorizzato** è un attacco in cui il carico utile XSS è *memorizzato in modo* permanente sul sito Web di destinazione, ad esempio in un database. Quando un client (ad esempio una vittima) carica una pagina come una sezione forum o una sezione commenti che carica il payload, verrà eseguita nel proprio browser.
- **L'XSS riflesso** è un attacco in cui il carico utile XSS viene inviato con la richiesta al server e *riflesso* nella risposta. Questi attacchi possono essere attivati facendo clic su un collegamento creato, inviando un modulo o molti altri meccanismi di consegna.
- **L'XSS lato client** , noto anche come **XSS basato su DOM** , è un attacco che si svolge esclusivamente nel browser del client (ovvero non viene inviato dalla risposta dal server) manipolando l'ambiente del DOM per forzare gli script affidabili esistenti nella pagina da eseguire il carico utile XSS.

## Examples

### Esempio di risultati di ricerca

Supponiamo di avere una pagina dei risultati di ricerca che riporta la query di ricerca dell'utente a loro. Il codice seguente è un esempio di come ciò potrebbe essere fatto in PHP:

```
Results for "<?php echo $_GET['query'] ?>"
```

Affinché ciò funzioni, accederai alla pagina con un URL come:

```
https://yoursite.test/search?query=stackoverflow
```

Nella risposta, otteniamo:

```
Results for "stackoverflow"
```

Ora tenteremo di iniettare il nostro carico utile nella risposta:

```
https://yoursite.test/search?query=<script>alert(1)</script>
```

E la nostra nuova risposta:

```
Results for "<script>alert(1)</script>"
```

Abbiamo iniettato con successo il nostro carico utile XSS.

Leggi Iniziare con xss online: https://riptutorial.com/it/xss/topic/10229/iniziare-con-xss

# Titoli di coda

| S. No | Capitoli | Contributors |
|---|---|---|
| 1 | Iniziare con xss | Community, newfurniturey |