Web Security - Attacchi Web

Web browser è un applicazione che permette di renderizzare una pagina web.

Normalmente codice js in un browser viene eseguito dentro una sandbox.

Il comando `netstats tulpn` servizi in ascolto del sistema. `net-tools` per installare `netstats`

`php -S 0.0.0.0:8000` per avviare ed esporre il server verso esterno dal docker. php server ha una convenzione che manda pagina `index.php` per ogni pagina 404.

`netcat <ip> <port>` apre una connessione con il server `<ip><port>`

```
GET /test.html # una get request dal netcat
```

Cross site scripting - XSS

Cross site scripting è un attacco web che inietta del codice maligno (normalmente Javascript) dal lato client-side per rubare dati di session oppure altre attività maligni. Principalmente, questi attacchi sono dovuti all'assenza di controlli sull'input inserito dall'utente (input sanitization).

Reflected XSS

In cui la vittima è convinto a cliccare un link (come un search query) che contiene del codice maligno. Il codice viene eseguito mediante la risposta del web server oppure come risultato della operazione.

`http://target.com/aform.html?search=<script>alert('XSS by Gaurav');</script>`

Stored XSS

In cui il codice maligno è memorizzato permanentemente sul database e verrà eseguito a in saputa della vittima ogni volta che visita la pagina.

```
strstr(string_to_control, string_to_find);
str_replace(str_to_be_replaced, str_to_replace_with, str)
```

`xss payload` per trovare vari payload di attacco

https://xss-game.appspot.com per esercitarsi

xss stored (lez16_2)

```
htmlspecialchars(str_to_parse);
```

se ce un errore del caricamento dell'immagine viene eseguito la funzione `f()`

```
<img src="x" onerror="f()"><script>function f(){alert(1)}</script>
```