

## Fastweb Myfastpage authorization control bypass via XSS.

Sfruttando una vulnerabilità XSS presente nel sito che ospita i pannelli di controllo Fastweb myfastpage, è possibile accedere abusivamente ai pannelli di configurazione di abbonamenti internet e telefono degli utenti Fastweb, semplicemente invitandoli a visitare un URL appositamente forgiato.

In maniera simile ad un *cookie stealing* si sottraggono le credenziali di accesso alle myfastpage personali. Il token autentificativo non è nel cookie ma nella URL per accedere al pannello, sotto forma di parametro *checksum* generato dinamicamente ad ogni richiesta di accesso ai pannelli. Una volta sottratto l'indirizzo del pannello **chiunque può accedervi anche fuori dalla rete fastweb e senza autenticazione**, basta che conosca l'URL. Via XSS forziamo il browser di un utente a comunicare gli URL dei pannelli di controllo ad un attaccante esterno.

### Login standard

Un normale login ai pannelli di controllo consiste in:

1. Visita a <http://www.fastweb.it/login> , senza autenticazione se da rete Fastweb
2. GET alla pagina <http://www.fastweb.it/myfastpage/goto/momi/?id=<nome-pannello>> , che viene redirezionato su <http://fastmomi.fastweb.it/?service=<nome-pannello>&checksum=<secret-session-token>&account=<account-number>&channel=MYFP>
3. GET verso l'URL del pannello.

I primi due passaggi sono fattibili solo da IP interni alla rete, e il secondo GET necessita i cookie settati nel primo. L'URL al pannello a cui punta il redirect è invece visitabile da tutti, a patto di conoscerlo.

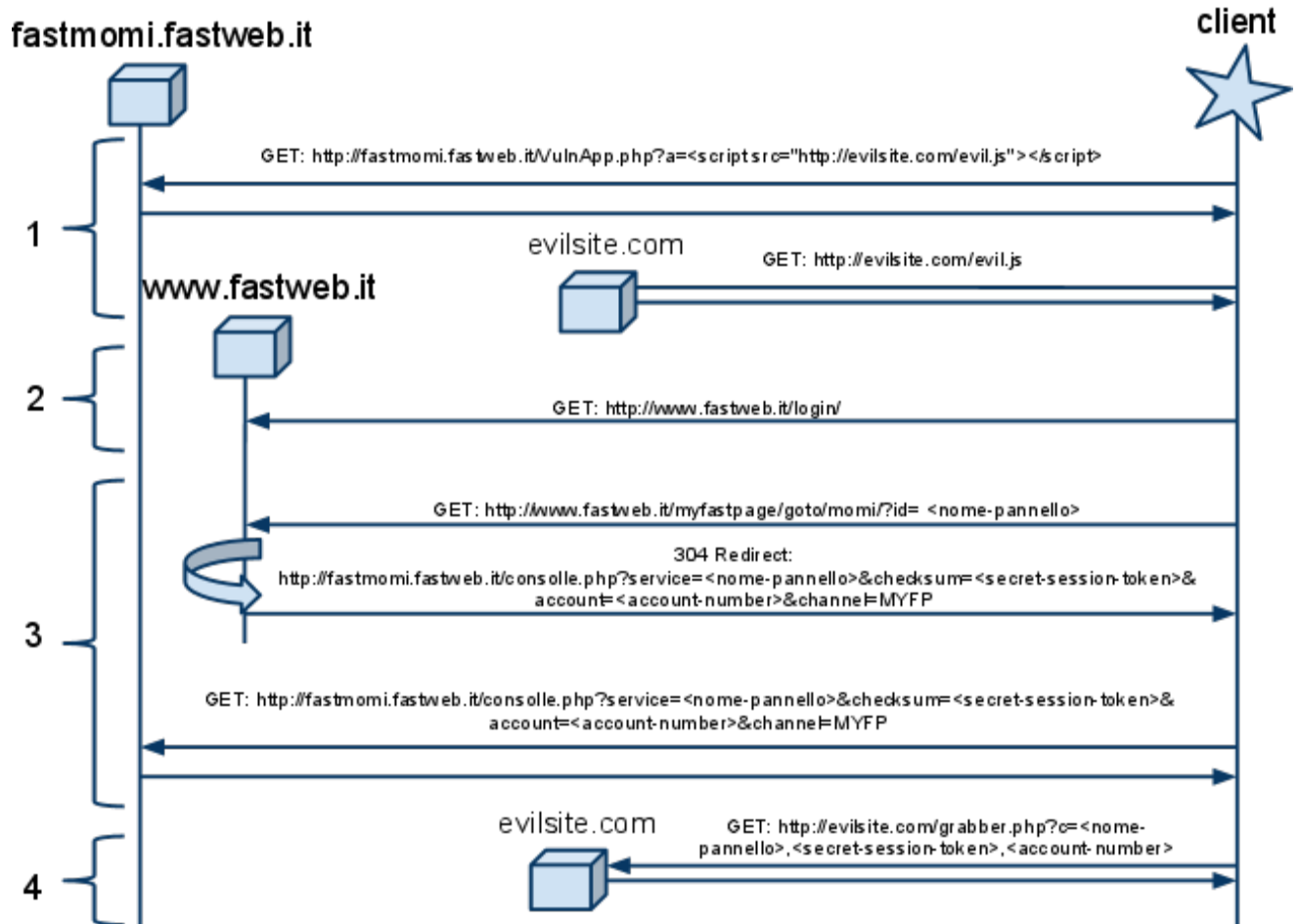
### L'attacco

L'XSS permette di forzare un browser a fare i 3 passaggi, estrarre l'URL finale e mandarlo a un *cookie grabber* installato su una macchina remota. L'attacco è più complicato del solito, a causa delle necessarie richieste su domini diversi pur rispettando la *same origin policy* dei browser.

### Diagramma dell'attacco

1. Il browser vittima punta all'XSS e esegue il javascript dell'attaccante.
2. Un IFRAME carica <http://www.fastweb.it/login> e genera i cookies iniziali.  
- *Same origin policy rispettata: la richiesta è su un'altro dominio ma la richiesta è blind (non ci interessa la risposta)*
3. Più IFRAME caricano i diversi pannelli <http://www.fastweb.it/myfastpage/goto/momi/?id=<nome-pannello>> , che ridirezionano automaticamente verso l'URL da catturare.  
- *Same origin policy rispettata? Sì, perchè nonostante l'url iniziale sia in un altro dominio, l'url destinazione del redirect è nel dominio che ospita l'XSS.*
4. Gli URL a cui puntano le .location degli IFRAME caricati vengono inviati alla macchina dell'attaccante che possiede il corretto URL per accedere dall'esterno al pannello di

controllo.



### Mitigazione del problema

1. Fix degli XSS presenti nel sito
2. Restrizione degli accessi ai pannelli a seconda di cookie, e provenienza dell'IP oltre che al token già utilizzato.
3. Richiedere nome utente e password per accedere alla Myfastpage anche da IP interni alla rete Fastweb.

### Disclosure

7 Maggio 2010: segnalazione dei problemi al reparto IT security di Fastweb

3 Giugno 2010: pubblicazione dell'advisory.