

# Berlusconi si dimette? No, è un bug di Repubblica

2009-10-09 00:20:39



**berlusconi-joker** Nei giorni scorsi alcuni avranno letto una pagina del sito di Repubblica.it nella quale era indicata la notizia delle dimissioni del Presidente del Consiglio Silvio Berlusconi. La notizia era completamente falsa, ed è stata inserita da un giovane informatico. Gli addetti del noto quotidiano non si erano accorti di una falla presente nel loro sito, sfruttabile mediante **attacchi XSS**, ovvero mediante inserzione di codici all'interno dell'indirizzo URL del portale.

L'informatico in questione, **Valentino Marangi**, aveva già segnalato a Repubblica la presenza di una vulnerabilità nel loro sito, della quale si era in qualche modo accorto, **ma i responsabili del portale avevano tralasciato del tutto la segnalazione**. Per far strabuzzare loro gli occhi sulla pericolosità delle vulnerabilità sfruttabili mediante attacchi XSS, il giovane ha così pensato bene di utilizzare un espediente di ingegneria sociale: modificare un titolo del sito del giornale utilizzando un argomento che sicuramente avrebbe destato l'attenzione dei giornalisti diretti da Mauro: Berlusconi.

Gli attacchi XSS sono spesso sottovalutati dagli esperti informatici di portali bancari o giornalistici, ma, ove sfruttati, sono decisamente efficaci perché riescono ad eludere le riserve di sicurezza utilizzate da software e seguite dagli utenti

Qui il report dell'anomalia riscontrata dal giovane visualizzabile direttamente dal suo [blog](#).

Immaginate che un qualsiasi estraneo alla redazione possa far visualizzare articoli e contenuti sul sito de La Repubblica, ora immaginate quali usi potrebbe farne, soprattutto a livello politico, e quali ne sarebbero le conseguenze. Una bufala diffusa utilizzando come strumento il **sito Repubblica.it**, quanti non la prenderebbero per vera? Tutto questo purtroppo è possibile, e occorre diffondere la notizia, soprattutto tra gli utenti meno esperti!

Qualche giorno fa navigando nel sito de LaRepubblica ho scoperto la presenza di una falla nell'area ricerca. Si tratta di un semplice bug di tipo XSS, ma che la cui presenza, su un sito così di rilievo, permetterebbe ad utenti malintenzionati di effettuare attacchi di phishing (truffe online) o di **pubblicare notizie false che, se provenienti da un sito del genere, non ci metterebbero molto a fare il giro della rete come vere**.

Andando ad effettuare una ricerca nel sito del quotidiano, la parola cercata viene passata alla pagina dei risultati tramite l'indirizzo, in questo modo:

# Anti-Phishing Italia: il portale contro le truffe on-line

Berlusconi si dimette? No, è un bug di Repubblica

<http://ricerca.repubblica.it/repubblica?query=PAROLACERCATA&view=archivio>

Andando a sostituire nell'indirizzo della pagina del codice html o javascript, al posto della parola cercata, questo verrebbe poi eseguito nella pagina dei risultati senza alcuna precauzione. Facendo in questo modo, inserendo il codice javascript opportuno nell'indirizzo, è possibile modificare totalmente la pagina dei risultati.

Chiunque sfruttando questo bug può ad esempio far comparire un annuncio del tipo "ATTENZIONE: dal prossimo mese Repubblica.it diventa a pagamento, clicca qui per abbonarti" truffando così i visitatori di Repubblica.it. O può addirittura far comparire notizie false spacciandole per vere. **Basterebbe poi linkare la pagina di Repubblica modificata su Facebook o ad esempio su OkNotizie**, e poi attendere che questa faccia il giro del mondo grazie all'effetto amplificatore della rete.

Dopo diverse prove sono riuscito, sfruttando il bug scoperto, a far visualizzare una notizia falsa su Repubblica.it:



bug\_repubblica

Chi andrebbe a dubitare di una notizia, se l'url di provenienza fosse proprio <http://ricerca.repubblica.it?> L'utente medio ci sarebbe cascato in pieno!

Potete verificare voi stessi andando a questo indirizzo:

<http://ricerca.repubblica.it/repubblica?query=Berlusconi:%20Lascio%20la%20politica%20-%20LaRpubblica.it%3C/title%3E%3C/head%3E%3Cbody%3E%3Cimg%20src=http://www.valentinomarangi.com/larepubblica.jpg%3E%3Cbr%3E%3Cbr%3E%3Cbr%3E%3C/body%3E%3C/html%3E&view=archivio>

Ho segnalato il problema alla redazione di Repubblica.it, ma non ho ricevuto alcuna risposta. Finché la falla non sarà corretta occhio alle notizie che vi linkano provenienti da Repubblica.it!

**EDIT 5/09/2009 23.14:** Richiamando file esterni dall'url adesso compare una pagina di errore (Errore 403), nessuna comunicazione ancora dalla redazione. Inserendo comunque del codice tramite l'url questo non viene ancora filtrato.

Tratto da [Valentino Marangi](#)

Fonte: Anti-Phishing Italia – [www.anti-phishing.it](http://www.anti-phishing.it)