Yahoo Babelfish - Possible Frame Injection Attack

Yahoo Babelfish - Possible Frame Injection Attack - Aditya K Sood, zeroknock.blogspot.com.

- Published: date not stated
- Original: <https://zeroknock.blogspot.com/2009/12/yahoo-babelfish-possible-inline-iframe.html>
- Preserved from: https://zeroknock.blogspot.com/2009/12/yahoo-babelfish-possible-inline-iframe.html (live) on 2026-08-10
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

[[image: image]]
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhFYnbaBnNSi00otFO74HPVhfTQzLfcut5Wo34ZaXO10PTs9yPOewCVa5xSqaCkmE2wCqEq1OCZDUTrdUci7h5rjMUxloR-CwaPy0qTh3GTRX3UWmg6I-sYZ6Q11UrDa0pWW_n-VA/s1600-h/yahoo_babelfish.png) Yahoo Babel-fish online is a service for translating content to different languages. The stringent design bug leads to the possibility of conducting FRAME injection attacks in the context of yahoo domain there by resulting in third-party attacks. The issues has been demonstrated in some of my recent conferences. The flaw can be summed up as:

1. There is no referrer check on the origin i.e. the source of request.
2. Direct links can be used to send requests.
3. Iframes can be loaded directly into the context of domain.

Points to ponder:

1. Yahoo login Page – perform certain checks , authorized ones.
2. Yahoo implements FRAME Bursting in the main login Page.

It is possible to remove that small piece of code and design a similar page with same elements that can be used further. It is possible to impersonate the trust of primary domain (YAHOO in this case) for legitimate attacks. There is a possibility of different attacks on YAHOO users.

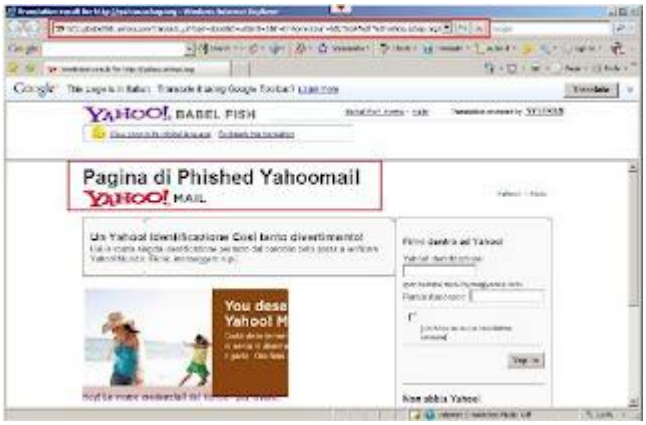
Note: there is no specific notification is displayed on the top of a translated page.

Attacker can conduct a FRAME attack by following below mentioned steps

1. Remove the above stated entities code from the main Login Page.
2. Design the fake domain. Load in the context of Yahoo domain

3. Inline IFRAME provides a familiar fake Login page.
4. Set the backdoor in the Login input boxes for stealing credentials.
5. Trap the victims by diversifying the manipulated URL's on the Web.One can use dedicated spamming.
1. The attack is all set to work.

Step 1: Injecting IFRAME - Modified



Step 2 – Stealing Credentials

DEMONSTRATION

This attack works successfully. This is a demo setup.You can try some credentials and try to login. :)
