

## Re: Bruteforce HTTP Basic authentication

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-08/0231.html>

---

**From:** Chris Kuethe ([chris.kuethe\\_at\\_gmail.com](mailto:chris.kuethe_at_gmail.com))

**Date:** 08/18/05

Date: Thu, 18 Aug 2005 14:05:49 -0600

To: Serg Belokamen <[serg.belokamen@gmail.com](mailto:serg.belokamen@gmail.com)>, Pen Test <[pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)>

By optimized alphabet, I mean sort the letters to be tried by order of frequency in your probably target language. You could try AAAAAAAAA, AAAAAAAB, AAAAAAAC, ... but there's a reason why they give you "RSTLNE" for free on Wheel of Fortune.

The last big brute force I did, I took the standard unix dictionaries, plus the text of a bunch of ebooks I had on my laptop and came up with frequency distributions for the first through fourth letters of the average english word. As I was targetting a system where most of the users were native english-speakers, I figured this was a safe assumption to make. It took some minutes for my frequency counter to run, but when I was finished, I had a set of alphabets that made it a lot more effective to search for dictionary words, their leetspeak variants, and finally alphanumeric keyboard smashing...

CK

On 8/17/05, Serg Belokamen <[serg.belokamen@gmail.com](mailto:serg.belokamen@gmail.com)> wrote:

> *What do you "optimised alphabet" ... any URL's etc?*

>

> *Cheers,*

> *Serg*

>

> *On 18/08/05, Chris Kuethe <[chris.kuethe@gmail.com](mailto:chris.kuethe@gmail.com)> wrote:*

>> *On 8/17/05, nik <[nik@adminzone.ru](mailto:nik@adminzone.ru)> wrote:*

>>> *Hello list!*

>>> *I'm doing little pen-test of a web-application for a small company.*

>>> *This application uses HTTP Basic authentication. So the question is:*

>>> *does any one know some tools (such as brutus) for*

>>> *brutforce usernames*

>>> *and passwords for this type of authentication. These*

>>> *tools must run*

>>> *under Linux or FreeBSD.*

>>

>> *The LWP perl module will do quite nicely. Combine that with an*

SecurityFocus Penetration: Re: Bruteforce HTTP Basic authentication

> > *optimized alphabet or 4, and you can have a very effective brute  
> > forcer in a couple of screenfuls of code. Optimizing your alphabet can  
> > be very effective, taking the time to crack a password down from hours  
> > to minutes or even seconds if you have a good idea about the letter  
> > distribution. ;)*  
> >  
> > **CK**  
> >  
> > --  
> > *GDB has a 'break' feature; why doesn't it have 'fix' too?*  
> >  
> >

---

> > *FREE WHITE PAPER – Wireless LAN Security: What Hackers Know That You Don't  
> > Learn the hacker's secrets that compromise wireless LANs. Secure your  
> > WLAN by understanding these threats, available hacking tools and proven  
> > countermeasures. Defend your WLAN against man-in-the-Middle attacks and  
> > session hijacking, denial-of-service, rogue access points, identity  
> > thefts and MAC spoofing. Request your complimentary white paper at:  
> > [http://www.securityfocus.com/sponsor/AirDefense\\_pen-test\\_050801](http://www.securityfocus.com/sponsor/AirDefense_pen-test_050801)*  
> >

---

> >  
> >  
>

--  
GDB has a 'break' feature; why doesn't it have 'fix' too?

---

FREE WHITE PAPER - Wireless LAN Security: What Hackers Know That You Don't  
Learn the hacker's secrets that compromise wireless LANs. Secure your  
WLAN by understanding these threats, available hacking tools and proven  
countermeasures. Defend your WLAN against man-in-the-Middle attacks and  
session hijacking, denial-of-service, rogue access points, identity  
thefts and MAC spoofing. Request your complimentary white paper at:  
[http://www.securityfocus.com/sponsor/AirDefense\\_pen-test\\_050801](http://www.securityfocus.com/sponsor/AirDefense_pen-test_050801)

---