

Forum:[Hack Forums](#)

Thread: [Need help with Brute Force \(BurpSuite\)](#)

Linusky - November 18, 2017, 8:24 am

Hi guys

The website I am testing here does not have any captcha (which is ez for brute force), however it does only allow one login per ticket. It does not affect regular users because the ticket gets regenerated when browser gets refreshed. How do I get burp suite to generate new ticket every time it does a new payload?

A snapshot of it

```
user_session%5Busername%5D=fakeusername&user_session%5Bpassword%5D=$password&lt=LT-1511018798r8EB3B66739CF2C09B5&service=&commit=Log+In
```

As you can see, the lt=LT-xxxxxx specifies the ticket. The website does not allow the usage of same tickets. Is there a way to get around this? (In browser when the page gets refreshed, new ticket will be generated but not in burp suite).

I tried generating some random string with 29 digits but it is not working.

SIM-99893 - November 18, 2017, 8:40 am

hmm, burpsuite? why not use SentryMba.

Linusky - November 18, 2017, 9:56 am

(Nov 18, 2017 09:40 AM)Marichu™ Wrote: [\[CITE\]](#) hmm, burpsuite? why not use SentryMba.

Okay, no. SentryMBA is for mass account dumping. What I am doing here is to crack a password of a specific user on a very specific website.

(website is vhlcentral.com)

website has several test banks for couples books, used to have an account but someone changed password.

Las3rz - November 18, 2017, 12:51 pm

(Nov 18, 2017 10:56 AM)Linusky Wrote: [\[CITE\]](#) Okay, no. SentryMBA is for mass account dumping. What I am doing here is to crack a password of a specific user on a very specific website.

(website is vhlcentral.com)

website has several test banks for couples books, used to have an account but someone changed password.

Not true, Sentry is for brute forcing whether that means 1 account, or multiple accounts. You could load a wordlist with that "specific user" as the only user. Or load a username list and password list (same concept).

bob:pass1

bob:pass2

bob:pass3

etc..

As well Sentry allows for the variables computed during a login attempted to be refreshed at each attempt (thus refreshing your unique ticket) ...with the "Refresh Data" box when making a configuration for that site.

Don't dismiss a tool just because you've never used it or are unfamiliar with it. Which clearly you are, by saying it's for mass account dumping, whatever that even really means.

Linusky - November 18, 2017, 1:35 pm

(Nov 18, 2017 01:51 PM)Las3rz Wrote: [\[CITE\]](#) Not true, Sentry is for brute forcing whether that means 1 account, or multiple accounts. You could load a wordlist with that "specific user" as the only user. Or load a username list and password list (same concept).

bob:pass1
bob:pass2
bob:pass3
etc..

As well Sentry allows for the variables computed during a login attempted to be refreshed at each attempt (thus refreshing your unique ticket) ...with the "Refresh Data" box when making a configuration for that site.

Don't dismiss a tool just because you've never used it or are unfamiliar with it. Which clearly you are, by saying it's for mass account dumping, whatever that even really means.

Sorry for my lack of knowledge. I was so confused with SentryMBA because whenever I do any research related to Sentry, all I see is massive account dumping tutorials of netflix, hulu, etc.

Is there some guide I can use? Thanks for the help!

CyberStrike - November 19, 2017, 5:16 am

Linsuky I am guessing that intruder is using the same value for the session check out repeater which will carry out a new request and hopefully a new session number

[https://portswigger\[.\]net/burp/help/repeater_using](https://portswigger[.]net/burp/help/repeater_using)
[https://portswigger\[.\]net/burp/help/repeater_options](https://portswigger[.]net/burp/help/repeater_options)
[http://resources.infosecinstitute\[.\]com/burps-session-handling-mechanisms/](http://resources.infosecinstitute[.]com/burps-session-handling-mechanisms/)

[https://support.portswigger](https://support.portswigger[.]net/customer/portal/articles/1964073-using-burp-to-hack-cookies-and-manipulate-sessions)

[\[.\]net/customer/portal/articles/1964073-using-burp-to-hack-cookies-and-manipulate-sessions](https://support.portswigger[.]net/customer/portal/articles/1964073-using-burp-to-hack-cookies-and-manipulate-sessions)

Edit: I see lots of people here using sentry MBA and I think if you kept popping in the same user name for each password value it would be pretty much at one user only not a mass dumping.

Linusky - November 19, 2017, 7:00 am

(Nov 19, 2017 06:16 AM)sirru5h Wrote: [\[CITE\]](#) Linsuky I am guessing that intruder is using the same value for the session check out repeater which will carry out a new request and hopefully a new session number

[https://portswigger\[.\]net/burp/help/repeater_using](https://portswigger[.]net/burp/help/repeater_using)
[https://portswigger\[.\]net/burp/help/repeater_options](https://portswigger[.]net/burp/help/repeater_options)
[http://resources.infosecinstitute\[.\]com/burps-session-handling-mechanisms/](http://resources.infosecinstitute[.]com/burps-session-handling-mechanisms/)

[https://support.portswigger](https://support.portswigger[.]net/customer/portal/articles/1964073-using-burp-to-hack-cookies-and-manipulate-sessions)

[\[.\]net/customer/portal/articles/1964073-using-burp-to-hack-cookies-and-manipulate-sessions](https://support.portswigger[.]net/customer/portal/articles/1964073-using-burp-to-hack-cookies-and-manipulate-sessions)

Edit: I see lots of people here using sentry MBA and I think if you kept popping in the same user name for each password value it would be pretty much at one user only not a mass dumping.

OMG THANK YOU!!! I did not realize that!!!

CyberStrike - November 19, 2017, 7:05 am

Well I hope it helps web apps are not my strong point to be honest.

Las3rz - November 19, 2017, 7:54 am

(Nov 18, 2017 02:35 PM)Linusky Wrote: [\[CITE\]](#) Sorry for my lack of knowledge. I was so confused with SentryMBA because whenever I do any research related to Sentry, all I see is massive account dumping tutorials of netflix, hulu, etc.

Is there some guide I can use? Thanks for the help!

You can start with Googling 'Sentry MBA tutorials' or 'Sentry MBA configs'. It will get you started in the right direction understand the tool and finding other places more into that field. Sentry is more of a "cracking" tool between cracking and hacking, which you will notice by the forums that appear from the search results.

ernestmiller - November 19, 2017, 9:40 am

is there anyway to get the Sentry MBA tool on Linux or is it purely a Windows thing??

CyberStrike - November 19, 2017, 10:14 am

That is a good question checking on WineHQ looks like it has some issues with Wine. But all you need is a userlist and password list and you can mass crack in hydra or in burpsuite.

ernestmiller - November 19, 2017, 10:34 am

The hydra syntax is so finnecky though and sensitive as well would rather use the sentry mba GUI if I could get