

Forum: [Hack Forums](#)

Thread: [Time based Injection?](#)

pwntoken - December 15, 2013, 8:14 am

Is this really happening or just a false alarm?

Code

```
http://internationalhotels.yatra.com/hotel/search/search?currencyCode=INR&additionalDataString=v  
rBookingSource|null&locale=en_IN&cid=317676&1%2527=1
```

There is this time delay burp took up. If this could be down I really would need a conformation on this? thanks mates.

EDIT: also here.

Code <http://railtourpackages.yatra.com/trainpackages/home>
I submit the USER-AGENT as:

```
Code Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;  
Trident/5.0)%20and%201%20in%20(select%20benchmark(200%2csha1(1))--%20  
Burp says it's time based? ???
```

also here

Code [http://js1.yatra.com/web/guest?1%2bbenchmark\(200%2csha1\(1\)\)--%20=1](http://js1.yatra.com/web/guest?1%2bbenchmark(200%2csha1(1))--%20=1)

Mx. - December 15, 2013, 4:38 pm

It's a false alarm generated by the delay in burp.

pwntoken - December 16, 2013, 8:48 am

(Dec 15, 2013 05:38 PM)Mx. Wrote: [\[CITE\]](#) It's a false alarm generated by the delay in burp.
damn this means the delay in burp and the timeout's produce a MySQL time based Injection
possibility? and how come the developers didn't fixed this yet? ?

Zixem - December 16, 2013, 1:10 pm

Like Mx. said, it's a false alarm. Don't trust burp when it comes to Time-Based injection. Always
double check with Tamper Data to make sure it's really vulnerable.

Here's my result when I tried make a delay of five seconds with time():

User agent injection:

```
Code 23:07:59.175[544ms][total 2592ms] Status: 200[OK]Third link:  
Code 23:01:14.036[1137ms][total 1137ms] Status: 302[Moved Temporarily]see? it barely gets to  
4000ms of response time...no chance to time based here.  
about the first link...the server return 404 response...is this supposed to be like that?
```

pwntoken - December 16, 2013, 1:23 pm

(Dec 16, 2013 02:10 PM)Zixem Wrote: [\[CITE\]](#) Like Mx. said, it's a false alarm. Don't trust burp when
it comes to Time-Based injection. Always double check with Tamper Data to make sure it's really
vulnerable.

Here's my result when I tried make a delay of five seconds with time():

User agent injection:

Code 23:07:59.175[544ms][total 2592ms] Status: 200[OK]Third link:

Code 23:01:14.036[1137ms][total 1137ms] Status: 302[Moved Temporarily]see? it barely gets to 4000ms of response time...no chance to time based here.

about the first link...the server return 404 response...is this supposed to be like that?
gave me 200 Status code, I have no clue how it gives 404 for you.

hellozephyr123 - December 17, 2013, 9:15 am

Encrypted is right i dont see anything wrong with the code itslef

pwntoken - December 17, 2013, 10:14 am

(Dec 17, 2013 10:15 AM)hellozephyr123 Wrote: [\[CITE\]](#) Encrypted is right i dont see anything wrong with the code itslef

No, it's false alarm IMO. The buro delay does it. I wouldn't had posted this if I was sure it was a real pick :P I was sure about 80% that this was burp doing it. So I rechecked.