

Forum:[Hack Forums](#)

Thread: [Thinking Local DoS: Recursive Exhaustion attacks](#)

Th3PonyWizard - May 6, 2014, 3:57 am

I've been thinking about other ways to utilize Recursion in WebApp attack patterns. One of the ideas that hit me was abusing the amount of resources the coding technique takes into a proportion of which it's completely intentional: Local DoS. This is beyond useful when attacking your own hosting company, or simply being able to inject RFI/LFI or any other from of RCE only to discover you're just not good enough to bypass these filter evasions / WAFs / functions you know are disabled.

My first approach was a common one. I took off a random example from a bug tracker report and re-coded it to make it functional on all environments.

PHP Code

```
<?php
```

```
@rename($_SERVER['PHP_SELF'], "file.php");
```

```
@fopen("http://server.com/file.php","r");
```

?>Or something. Sort the URL accordingly, allow_url_fopen should be ON over php.ini. This will kill off the PHP on the local system for a good while on rather old systems, didn't check new ones. This will rename itself to file.php, then it will open itself (For the lazy ones) Again. Again. Again. And again.

In JS you can do a similar DoS thingie with just a loop running around opening Java applets etc. Lets form a discussion over what ways you would do to cause a client-sided or server-sided self dos attack.

PRNDL - July 23, 2014, 4:22 pm

this looks interesting and im surprised no one elaborated on it with you.

godspeed my brother. ?

TheWholeWorldExplodes - July 24, 2014, 6:06 am

lel, this is simple but effective, signing up on shared hosting could take down a lot of websites, cheers!

ljeremy - July 24, 2014, 6:15 am

Really, really good idea. I'm gonna try this out myself!