

Forum:[Hack Forums](#)

Thread: [What are Server Side & Client Side vulnerabilities ?](#)

zoombiero - September 30, 2015, 7:17 pm

I want to know the names of vulnerabilities which are based on Client Side and Server side respectively.

Please tell me the names only.

hahdbwoannniabs - September 30, 2015, 8:37 pm

There really aren't any client-side vulnerabilities other than non-persistent XSS and sometimes CSRF, not that I can think of at least.

The most known server side vulnerabilities includes

Structured query language injection

Persistent cross-site scripting

Local/Remote file inclusion

XML external entities injection

Remote command (or code) execution

Cross-site request forgery

Directory traversal (can also be called arbitrary file reading or some shit) - similar to local file inclusion, except in LFI the file resource is executed whereas in directory traversal, you can only read the file.

Don't get me wrong, there are tons more out there. The ones I listed above are just usually the first things that come to mind regarding the topic of webapp hacking.

How bout using your brain - October 1, 2015, 3:25 am

(Sep 30, 2015 08:37 PM)_anthrax Wrote: [\[CITE\]](#) There really aren't any client-side vulnerabilities other than non-persistent XSS and sometimes CSRF, not that I can think of at least.

There is a whole bunch more. Buffer overflows, integer overflow, use-after-free, type confusion and whatnot. Browsers and their plugins are just as vulnerable as any other software, so there is a shitload of possibilities for vulnerabilities.

hahdbwoannniabs - October 1, 2015, 5:06 am

(Oct 1, 2015 03:25 AM)SirRootALot is awesome. Wrote: [\[CITE\]](#) There is a whole bunch more. Buffer overflows, integer overflow, use-after-free, type confusion and whatnot. Browsers and their plugins are just as vulnerable as any other software, so there is a shitload of possibilities for vulnerabilities.

He posted this in "Beginner Hacking" so it's only natural that I assumed he was talking about web-based vulnerabilities. He isn't going to know jack shit about what you just said.

Ozedath - October 1, 2015, 11:08 am

Well let's see what a client and a server are before getting into more detail.

The client is a process that requires a resource from another process called the server. The client and the server must each speak the same language. In this context the language is called a protocol. While writing this post I'm using a process that identifies my browser, use a protocol(HTTP, strangely hf doesn't use TLS :() to send it to the server and ask it to store it for later use, so that

other clients(i.e. you) may view it as well.

That being said, client side vulnerabilities are the ones that affect mostly the client in a security context, as in, a third potentially malicious runs commands on the client's box without the client being aware. When the surface of attack is defined by a web browser, these attacks are related to the language the browser understands: html and javascript for the most part. You can lookup vulnerabilities such as XSS and CSRF on OWASP. Other attacks were common on the past such as stack/heap buffer overflows determined by how the browser was sanitizing input.

The later category of vulnerabilities apply to a much broader range of clients aside from a web browser.

Server side vulnerabilities involve a process called the server which performs the requests of clients if the latter are authorized. When restricted to the web such vulnerabilities are LFI, RFI, SQLi, command injection, directory traversal attacks and so on. You can again check them up on OWASP. Similarly to client processes server processes might be vulnerable to stack/heap buffer overflows.

You can start here with stack buffer overflows:

Code [securitytube.net<slash>groups?operation=view&groupId=4](http://securitytube.net/slash>groups?operation=view&groupId=4)

zoombierobo - *October 6, 2015, 6:28 am*

Thanks to all who replied here.