

Forum:[Hack Forums](#)

Thread: [What are the most dangerous vulnerabilities out there?](#)

thegooDZguy - June 6, 2022, 2:21 am

Hey everyone

I've been wondering what are the most dangerous vulnerabilities that can be found on a website except SQLI or XSS ...

skull - June 6, 2022, 4:03 am

(Jun 6, 2022 02:21 AM)thegooDZguy Wrote: [\[CITE\]](#) Hey everyone

I've been wondering what are the most dangerous vulnerabilities that can be found on a website except SQLI or XSS ...

Looking for type of vulnerabilities?

Then it's RCE (Remote Code Execution), with that the attacker can almost do anything to the site.

nerdy - June 7, 2022, 1:49 am

// Some dangerous vulnerabilities //

That would be RCE (Remote Code Execution) as the name says, an attacker can execute commands remotely using this vulnerability. Leads to initial access.

CSRF (Cross-Site request forgery) as owasp says, Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

SSI Injection (Server-Side Includes Injection) as owasp says, The Server-Side Includes attack allows the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely. It can be exploited through manipulation of SSI in use in the application or force its use through user input fields

RFD (Reflected File Download) It is a client side vulnerability which allows the attacker to serve a file by setting parameters which specify the file name and the file contents.

OR:

Johne Jacob, medium, rfd

Reflected File Download(RFD) is an attack technique which might enables attacker to gain complete access over a victim's machine by virtually downloading a file from a trusted domain.