

Forum:[Hack Forums](#)

Thread: [OWASP remote OS injection - advice needed](#)

pebblak - March 15, 2016, 1:27 pm

So I need a bit of advice on how to proceed here, maybe some pointers to some useful resources I could look into.

I scanned a website with OWASP ZAP, and it flagged up a high risk vulnerability: a POST request at a particular URL with parameter `__VIEWSTATEGENERATOR`.

The Attack is: `8D0E13E6";sleep 5s;"`

It provides references to read what the vulnerability is about. It appears it is supposed to allow execution of arbitrary commands on the server. However, I am at a loss on how to actually do this. I can view the request made in the program, so I'm thinking I could edit it to contain my code...the problem is, I have no idea how to send a custom POST request to the server.

I know this sounds very noobish, that's because I'm a noob. Is there some kind of tool to craft parameters? How would you go about doing this?

EDIT: I found a way to send custom requests straight from OWASP ZAP, which is a step in the right direction. However, whatever command I write, the server responds with this:

Invalid postback or callback argument. Event validation is enabled using <pages enableEventValidation="true"/> in configuration or <%@ Page EnableEventValidation="true" %> in a page. For security purposes, this feature verifies that arguments to postback or callback events originate from the server control that originally rendered them. If the data is valid and expected, use the ClientScriptManager.RegisterForEventValidation method in order to register the postback or callback data for validation.

Does this mean the website actually is not vulnerable?

Reece Morgan - March 15, 2016, 2:57 pm

This sounds like a false positive, sorry to disappoint OP. If your really curious, you could post the vulnerability information and vulnerable site here so someone else more experienced could take a look at it.

pebblak - March 15, 2016, 5:11 pm

Dang. Oh well. The site is

`alpeshfuriya(dot)com`

You can actually get into the admin section with simple SQL injection, but it doesn't let you change anything in there, or not me, at least. Something about verifying MAC.

It gives massive error logs though, so that must be useful for someone who knows a lot about how servers of this kind work.

If anyone manages to get into the actual box, let me know how you did it, even if you choose to keep it for yourself ;)