Bypassing URL Authentication and Authorization with HTTP Verb Tampering

Source: http://www.derkeiler.com/Mailing−Lists/securityfocus/bugtraq/2008−05/msg00319.html

- *From*: "Arshan Dabirsiaghi" <arshan.dabirsiaghi@xxxxxxxxxxxxxxxxx>
- *Date*: Wed, 28 May 2008 15:28:59 −0400

Internetizens,

Many URL authentication and authorization mechanisms make security decisions based on the HTTP verb in the request. Many of these mechanisms work in a counter−intuitive way. This fact, in combination with some oddities in the way that both web and application servers handle unexpected HTTP verbs causes the rules dictated by those mechanisms to be bypassable.

Many of us rely on the mechanisms I'm talking about. The Internet is not exactly going to burn down when this email goes out, but there is probably a fair number of externally facing web applications out there that are relying on the shaky security provided by these configurations.

We have written a whitepaper that goes into some detail discussing the vulnerability and how the various vendors are affected. You can grab the whitepaper from Aspect Security's website:

http://www.aspectsecurity.com/documents/Bypassing_VBAAC_with_HTTP_Verb_Tampering.pdf

Jeff Williams and Jim Manico also put together a demo that shows the attack in progress:

http://www.aspectsecurity.com/documents/Aspect_VBAAC_Bypass.swf

Cheers,

Arshan Dabirsiaghi

Director of Research

Aspect Security

http://www.aspectsecurity.com/