

Forum:[Hack Forums](#)

Thread: [Why does this GET parameter trigger a loop?](#)

8220347 - April 20, 2016, 5:04 pm

I am testing this website, and when I add the parameter '?index=0' to the end of the .asp page, it triggers some strange code that loops through numbers 1 to 258. (For EX, I load <http://website.com/test.asp?index=0> and it will refresh my page and load <http://website.com/test.asp?index=1>, and repeat the process all the way to 258).

Has anyone ever heard of this before? Is it exploitable?

Also, when I add a large number as input into 'index', the page returns a pop up box with a random value (EX: 88308.799)

Thanks

SIM-1725686 - April 20, 2016, 5:28 pm

You should share your code with us. We have no idea what's going on behind the scenes.

8220347 - April 20, 2016, 5:39 pm

Here is the code:

```
function initPage() {
    setCookie("region", "US", getExpDate(10 * 365))
    removeFromSession("region")
    document.forms[0].SESSION.value += "region=US;"
    var url = getDocumentLocation()
    var offset = url.indexOf("?")
    if (offset == -1) return
    var params = "&" + url.substring(offset + 1)
    var indexStr = "&index="
    if ((offset = params.indexOf(indexStr)) != -1) {
        var index = params.substring(offset + indexStr.length)
        if ((offset = index.indexOf("&")) != -1) {
            index = index.substring(0, offset)
        }
        index = parseInt(index)
        if (index == 0) {
            setCookie("timer", new Date().getTime(), "")
        }
        var form = getForm()
        var menu = form.countryList
        if (index < menu.options.length) {
            menu.selectedIndex = index
            fields["reportType"].setValue("BOTH")
            if (doSubmit()) {
                form.action = "agentLinkResults.asp?index=" + index
                form.submit()
            }
        }
    }
}
```

```

    } else {
        var startTime = parseInt(getCookie("timer"))
        alert(((new Date().getTime()) - startTime)/1000)
    }
}
}
}

```

```

function customValidation() {
    var form = getForm()
    var type = fields["reportType"].getValue()
    var countryList = getListValues(form.countryList, type)
    form.SESSION.value = "NEW_DISPLAY=" + countryList + ";" + form.SESSION.value
}

```

```

function getListValues(listObj, type) {
    var result = ""
    for (var i = 0; i < listObj.options.length; i++) {
        if (listObj.options[i].selected) {
            result += (result != "" ? "," : "") + listObj.options[i].value + "_" + (type == "BOTH" ? "CSL" : type)
            if (type == "BOTH") {
                result += "," + listObj.options[i].value + "_EAD"
            }
        }
    }
    return result
}

```

chillingwitha9 - April 22, 2016, 8:46 am

```

Code if (offset == -1) return
var params = "&" + url.substring(offset + 1)
var indexStr = "&index="
if ((offset = params.indexOf(indexStr)) != -1) {

```