

Forum:[Hack Forums](#)

Thread: [Apache Http Cookie Disclosure Vulnerability](#)

Coded Indisoul - June 26, 2013, 3:24 am

Apache Http Cookie Disclosure Vulnerability

Before Proceeding With The Topic Let Me Tell First That When httponly come into existence. Actually Httponly Come Into Existence In 2002 by Microsoft Internet Explorer developers for Internet Explorer 6 SP1 by Jordan Wiens.

What Is HttpOnly : httponly is an additional flag included in a Set-Cookie HTTP response header and also Using the HttpOnly flag the risk of client side scripting to access the protected cookie when generating a cookie decreased.

Apache http cookie disclosure: Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request or 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

Scope Of The Vulnerability:

? Scope=Medium

It Can Just Harmful For The Clients Not For The Admin Or In Other Words You Can't Hack Site Through This method.

Now Let's Proceed With The Topic !

Requirements:

- ? Internet Explorer (any supported Browser)
- ? Knowledge About Apache Cookie Disclosure
- ? Target Website

So Now First Of All Find The Vulnerable If You Are Lucky Then You Would Find 1 out 100 Web Sites Vulnerable To This Attack ! because this vulnerability exists in the Apache versions (up to 2.0.21) And this vulnerability even could be found into the big sites like twitter or SBI(bank) my friend named Praveen Nair found one of them in SBI.

So This exploit creates a big cookie for forcing a 404 error bad request and makes a request. When Apache 2.2 send a 400 status, it does not properly restrict header information, exposing secure cookies because the cookie which is created is very big.

So Let's Take An Example Of The Site

<http://www.un.org>

This Site Is Vulnerable To The Apache Cookie Disclosure Vulnerability So To Check The Vulnerability just type

[illegible]

<http://www.un.com/Cookie:>

[illegible]

and if you get an error page like this then it means your target is vuln to the apache cookie disclosure vulnerability

and yes for the Info You can't Hack Site With This Vulnerability and it is not considered under the big bounty programs too.

and This Is For Education Purpose Only ! And With This You can Steal Cookies To and if you are lucky some time then you will be able to turn off the website for short period of time ! ! !!!! ! ! Hope You Enjoyed it ! and Sorry For Little BAd English !

himanshu raj - January 16, 2015, 8:59 am

nice tutorial dude hope it works :)