

RE: Scripts found on web server

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-09/0442.html>

From: Josh Perrymon (perrymonj_at_networkarmor.com)

Date: 09/29/05

Date: Thu, 29 Sep 2005 08:39:15 -0500

To: "Hussein Ghazy (ProtechT)" <hussein.ghazy@protecht-me.com>, <pen-test@securityfocus.com>

Are the .asp scripts valid and used on the website for auth?

Login.asp should call to a backend DB for authentication so I'd try some SQL injection on it and see what you get.

Type in ' in the user name a password box and see if it gives you a server error and not a verification error.

If it does then you could try entering--

Test' or 1=1-- in both fields and see what happens. This is very basic SQL injection and if it works it will log you in as the first user in the DB (Usually admin)

What it's doing is making the SQL statement true so it parses the query.

JP

Network Armor

-----Original Message-----

From: Hussein Ghazy (ProtechT) [<mailto:hussein.ghazy@protecht-me.com>]

Sent: Tuesday, September 27, 2005 2:09 PM

To: pen-test@securityfocus.com

Subject: Scripts found on web server

Hi,

I was doing a penetration testing on one of our client's website, I found some scripts. How can I exploit them & how can I hide them from end users.

Example:

<http://www.xyz.com/login.asp>

Thanks & Best Regards

Hussein Ghazy

SecurityFocus Penetration: RE: Scripts found on web server

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do!

Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do!

Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831
