Web portals - gateway to information or a hole in our perimeter defenses.

By Deral Heiland CISSP

Web portals are a phenomenon that initially received their start in the late 90's. The purpose of portal technology is to make available a single point of access to a potential vast array of information and resources. Some key types of portals can include Corporate Enterprise information and Consumer based portal systems. This growing need for information and a single point of origin has fueled the growth of portal technology across the internet over the last decade. The technology has grown from simple web links to information resources, into a technology that aggregates the information from a multitude of sources and delivers the requested information as if it was stored at that point of origin (figure 1).

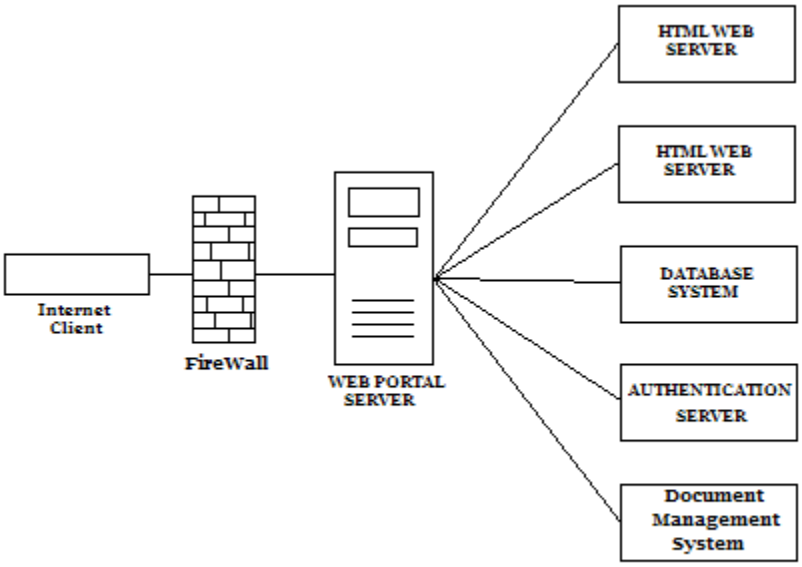

Figure 1

Unfortunately, a potentially new type of vulnerability may exist where attackers can use vulnerable user interface modules within a portal to tunnel into internal resources behind the corporate firewall (figure 2). It is Also possible to send queries to other systems on the internet, all tunneled or proxied by the vulnerable web portal server (figure 3).

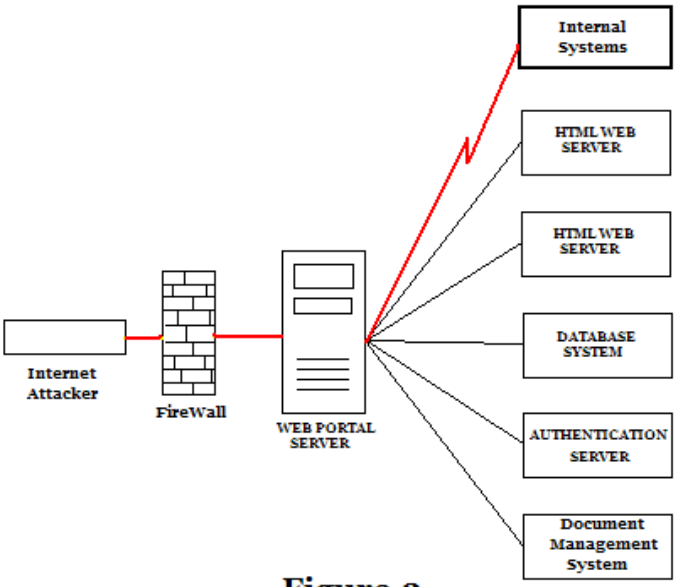

Figure 2

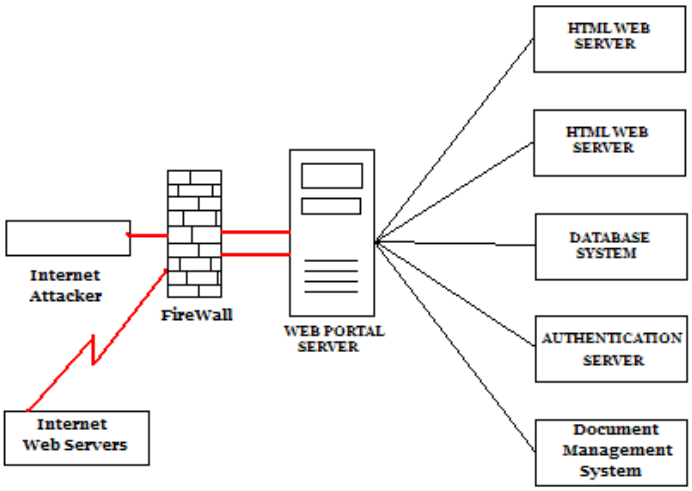

Figure 3

This vulnerability was discovered while testing a portal system for cross site scripting issues. During the cross-site-scripting (XSS) test, we modified the URL so the attack would retrieve text data from a third-party site and embed it into the web page on the vulnerable web site. At first this vulnerability appeared to be like most basic XSS issues. Where we expected the data to be retrieved by the client's web browser from the 3rd party site, but during deeper examination this was discovered not to be the case. With a packet sniffer running, we captured all the data being served from the portal server. No calls were made from the client to the 3rd part site. With this bit of critical information, we tested the vulnerability against an internal resource not available from the internet - a printer on a 192.168.*.* subnet. To our surprise the printer's configuration web page was displayed within our web portal page.

We are at the very early stages of researching this issue. Presently we are not releasing the product name that we discovered this initial vulnerability in until further testing and research can be conducted on other portal products. If we would go back and take a closer look at the multitude of XSS vulnerabilities exposed already, we may find that this exploit has been discovered already and reported as XSS vulnerabilities. As stated, this vulnerability was first discovered in what appeared as a simple XSS issue where data could be embedded in the web page from a third party web site. This specific example was discovered within a web portal's user interface module. These modules are known by various names based on the web portal product being used (gadgets, portlets, blocks, web modules or web parts).

Protecting potentially vulnerable systems from this type of attack can be accomplished with a few simple steps.

1. Ensure the portal server is in a DMZ
2. Do not allow the portal server to initiate connections to the Internet.
3. Only allow the portal server to make internal connections to authorized resources.
4. Restrict portal connectivity only to ports needed.

Definitions:

Packet sniffer is an application that listens and captures network communication packets while in transit and decodes and displays that information.

DMZ Demilitarized Zone is a network subnets that sets between the internet and internal network .

Cross-site scripting (**XSS**) is a type of computer security vulnerability typically found in web application which allow code and content injection by malicious web users into web pages viewed by other users.

References:

WEB PORTALS The New Gateways to Internet Information and Services By Arthur Tatnall
ISBN 159140439-8 IDEA Group Publishing

WIKIPEDIA The Free Encyclopedia http://en.wikipedia.org/wiki/Main_Page

Understanding the Cause and Effect of CSS (XSS) Vulnerabilities By Gunter Ollmann
http://www.technicalinfo.net/papers/CSS.html