Disabling Default Web Pages & Directory Listings: A Reference Guide

The Information Security Office's (ISO) Threat Mitigation Unit (TMU) has identified specific reoccurring issues within the University of Utah's online presence that are centered around University-hosted websites and web applications. This reference guide is made to serve our organization's IT professionals and web community members, as well as our content creators and end users in better understanding positive web security practices. This should serve as an explanation of reoccurring security shortfalls within the University of Utah's web application landscape to promote overall awareness, as well as serve as a guide for simple website hardening tips for those who may be creating websites in the near future.

SECURITY MISCONFIGURATIONS

The Information Security Office has identified specific reoccurring issues within the University of Utah's web application landscape regarding Security Misconfigurations, which is ranked as #5 on the Open Web Application Security Project's (OWASP) 2021 Top 10 most critical security risks to web applications (https://owasp.org/Top10/A05_2021-Security_Misconfiguration/). Security Misconfigurations can take many forms; however, Default Web Pages and Directory Listings are two specific misconfigurations that we tend to identify regularly within our web application landscape.

DEFAULT WEB PAGES

Default Web Pages are content delivered with software usually meant for testing services immediately after installation. While these may seem like benign sites with irrelevant information to the average internet user, to an attacker, default pages suggest lightly monitored or abandoned targets. Attackers expect these targets to offer exploitable vulnerabilities and a safe place to operate with an enhanced probability of their nefarious activities going unnoticed. Additionally, default pages often have detailed version and configuration information, allowing for more detailed target enumeration.

DIRECTORY LISTINGS

Directory Listings indicate that a web server is showing the contents of directory files in one or more directories, which are exposed by this server. This increases the risk of data loss or otherwise exposing sensitive information, whether or not the information exposed via directory listing is deemed "public" or "non-sensitive" information. The most popularly reoccurring web server applications we have seen in our environment are Microsoft IIS, Apache HTTP Server, and Apache Tomcat.

VULNERABLE AND OUTDATED COMPONENTS

The Information Security Office has identified another specific reoccurring issue: the use of Vulnerable and Outdated Components. At #6 on the Open Web Application Security Project's (OWASP) 2021 Top 10 most critical security risks to web applications (https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/), vulnerable and outdated components refer to third-party libraries or frameworks used in web applications that have known vulnerabilities or are no longer supported by their developers. These components can be exploited by attackers to gain unauthorized access to sensitive data or take control of the system.

In the majority of organizations, including our own, this takes the form of End-of-Life (EOL) software that is being used in any capacity. Curious about if the version of software components you are using are EOL? Follow this link: https://endoflife.date/.

CIS BENCHMARKS

The Center for Internet Security (CIS) is a U.S.-based non-profit organization that utilizes the global IT community to protect both public and private organizations against cyber threats. In doing so, CIS created the CIS Benchmarks, which are, "prescriptive configuration recommendations for more than 25+ vendor product families…[that] represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently" (https://www.cisecurity.org/cis-benchmarks). Put simply, the CIS Benchmarks are a list of configuration recommendations that assist in hardening specific products to effectively defend against cyber threats and potential attacks.

You can utilize the CIS Benchmarks for specific versions of Apache HTTP Server, Apache Tomcat, and Microsoft IIS to compare and better secure the current configurations you have. Navigate to CIS Workbench and create an account to be able to view any benchmarks you may be interested in: https://workbench.cisecurity.org/registration. While it is always highly recommended that you utilize the single most up to date version of software, it is understood that situations may exist where this is not inherently possible. Please see the resources for the most up to date software and their predecessors:

1- Microsoft IIS 10: https://workbench.cisecurity.org/benchmarks/13949
2- Microsoft IIS 8: https://workbench.cisecurity.org/benchmarks/14293
3- Apache HTTP Server 2.4: https://workbench.cisecurity.org/benchmarks/6258
4- Apache HTTP Server 2.2: https://workbench.cisecurity.org/benchmarks/687
5- Apache Tomcat 10: https://workbench.cisecurity.org/benchmarks/11652
6- Apache Tomcat 9: https://workbench.cisecurity.org/benchmarks/6487

For those who would like to dynamically compare their machines to both levels 1 and 2 of the CIS benchmarks for Microsoft IIS 10 and Apache Tomcat 10, as well as any other questions you may have—please contact the Threat Mitigation Unit at vulnerabilitymanagement@iso.utah.edu.

DEFAULT WEB PAGE REMOVAL GUIDES

Below are lists of steps to follow to effectively remove default web pages that are shown on currently running web services. The easiest and most effective way to remove a default web page from production is to stop or "kill" the Apache or Microsoft IIS web service that is running on a specific machine. However, if running the service is necessary and stopping it is not possible, please follow the instructions below to remove the default web page and ensure a directory is not listed in its place:

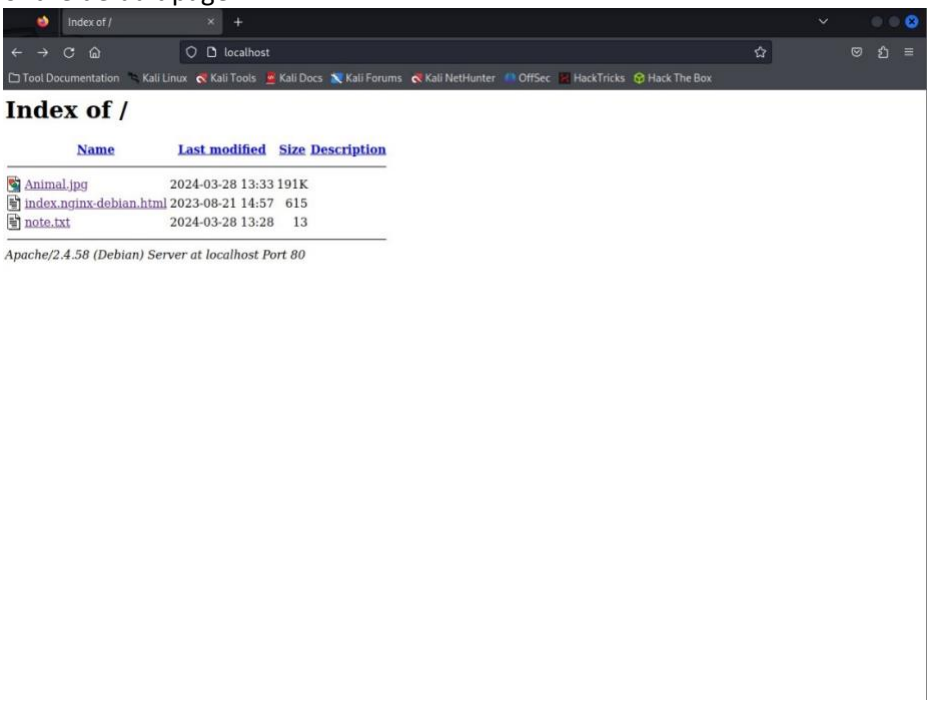
APACHE HTTP SERVER REMOVAL (FYI: different Linux distributions use different naming conventions. Debian historically uses, "apache2", while Red Hat uses, "httpd")

Invoke a 403 Forbidden

1- Navigate to your default web page within your web browser

2- In a terminal window, navigate to /var/www/html/ and either delete or change the name of index.html to remove the default web page.

3- Refresh your browser. You will notice an index of the contents of /var/www/html/ show in place of the default page.



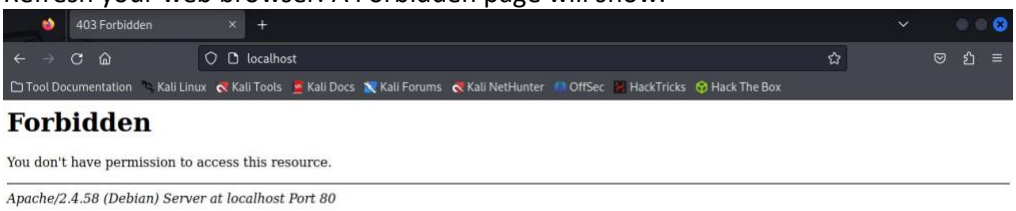
4- In your terminal window, navigate to your default configuration file & open with a text editor (ex. nano). The name and location of your config file is subject to change based on which Linux

distribution you are utilizing (default config file & location: /etc/apache2/apache2.conf or /etc/httpd/conf/httpd.conf)

5- Navigate to the Directory tag that contains the path to your virtual host (in this case '<Directory /var/www/>') and change "Require all granted" to "Require all denied", then restart the Apache service.

```
# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all denied

</Directory>

#<Directory /srv/>
#       Options Indexes FollowSymLinks
#       AllowOverride None
#       Require all granted
#</Directory>
```

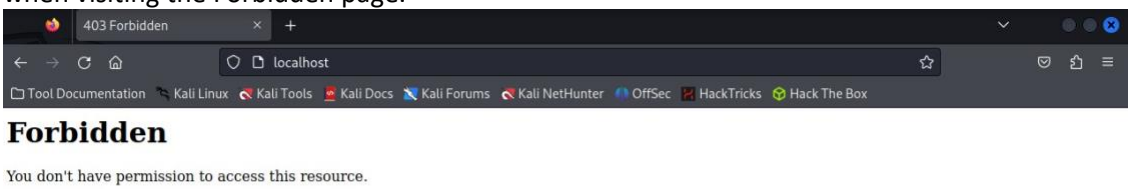
6- Refresh your web browser. A Forbidden page will show.



7- Next, disable all banner information by going to the Apache security config file (e.g. /etc/apache2/conf-available/security.conf) and changing 'ServerTokens OS' to 'ServerTokens Prod' and 'ServerSignature On' to 'ServerSignature Off', saving, and restarting the service.

```
#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#ServerSignature Off
ServerSignature Off
```

This will remove the banner information that shares server and Apache versioning information when visiting the Forbidden page.

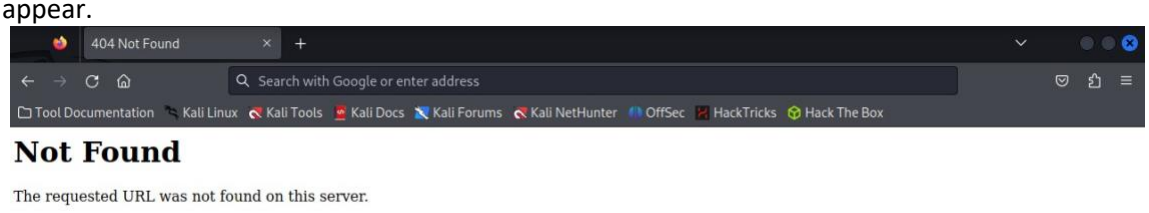


Invoke a 404 Not Found

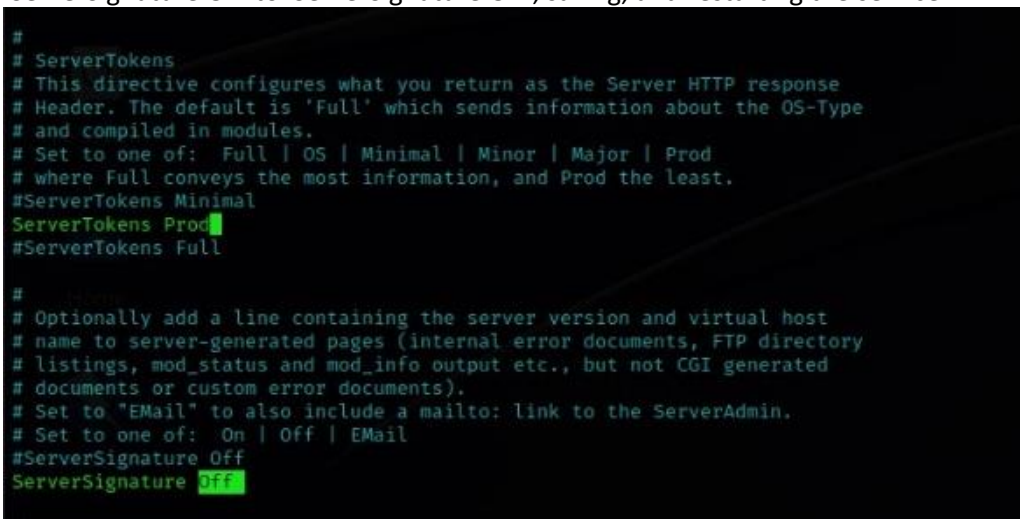
1- Navigate to the Apache security config file (e.g. /etc/apache2/conf-available/security.conf) and add “RedirectMatch 404 /\.*”

```
#
# Forbid access to version control directories
#
# If you use version control systems in your document root, you should
# probably deny access to their directories.
#
# Examples:
#
#RedirectMatch 404 /\.git
RedirectMatch 404 /\.*

#
```

2- Restart the Apache service & reload your browser window. A Not Found server response should appear.

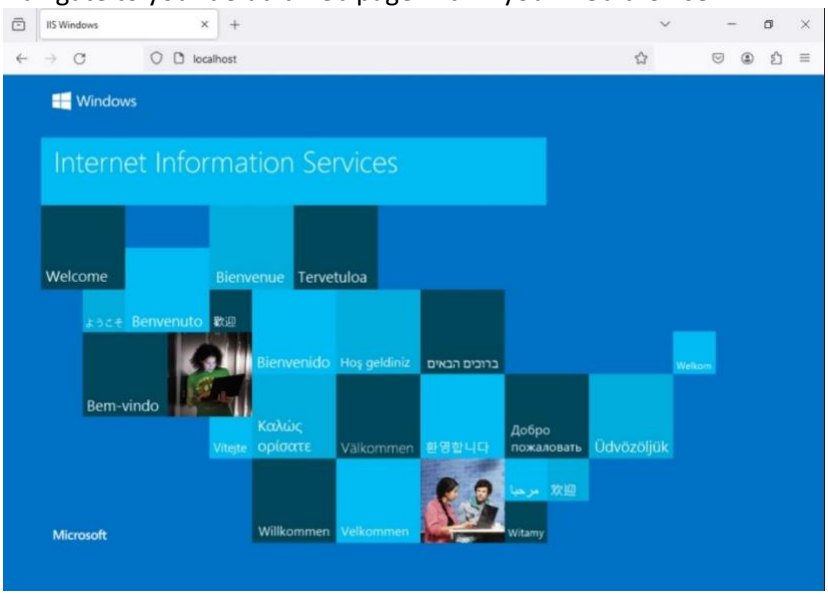


3- If the Not Found page returns with an information banner at the bottom, please disable all banner information by going to the Apache security config file (e.g. /etc/apache2/conf-available/security.conf) and changing 'ServerTokens OS' to 'ServerTokens Prod' and 'ServerSignature On' to 'ServerSignature Off', saving, and restarting the service.

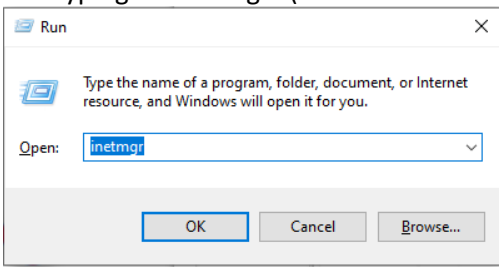


MICROSOFT IIS REMOVAL

1- Navigate to your default web page within your web browser.



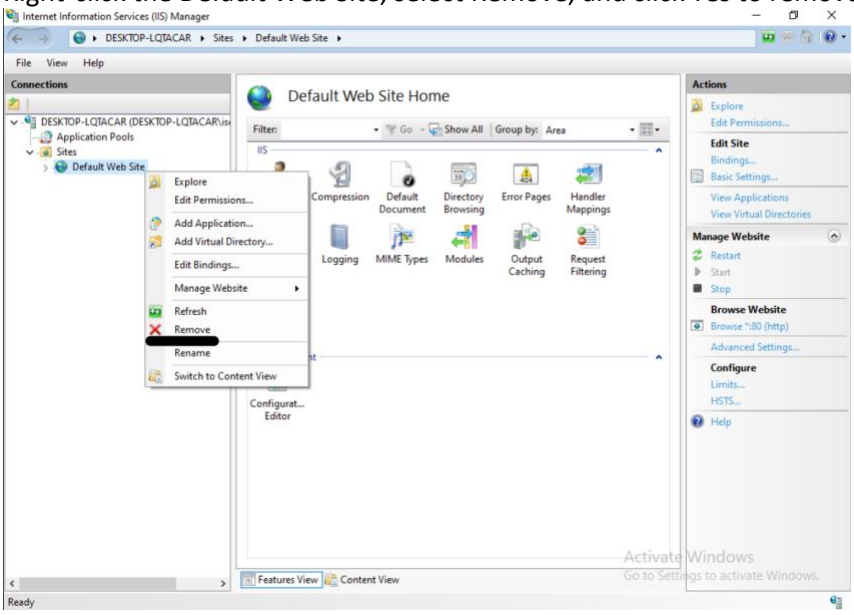
2- Open Internet Information Services (IIS) Manager. Do this by pressing Windows + R to open Run and typing in "inetmgr" (Default location: %windir%\system32\inetsrv\InetMgr.exe).



3- Expand the Server.

4- Expand Sites.

5- Right-click the Default Web Site, select Remove, and click Yes to remove the selected site.



6- Select Application Pools.
7- Right-click the DefaultAppPool, select Remove, and click Yes to remove the selected site.
8- Open File Explorer and navigate to your website root folder (Default location: C:\inetpub\wwwroot) Remove all files and folders located in the folder.
9- Reload your browser. Nothing should resolve.