netsparker

10/24/2020 3:14:31 PM (UTC+05:30)

SANS Top 25 Report

https://www.paypal.com/

Scan Time	10/20/2020 6:08:13 PM (UTC+05:30)
Scan Duration	03:20:46:44

Total Requests: 644,179
Average Speed: 1.9r/s

Risk Level: MEDIUM

Explanation

This report is generated based on SANS Top 25 classification.
There are 7 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

VULNERABILITIES

60	1	0	0	54	2	1	3
IDENTIFIED	CONFIRMED	CRITICAL	HIGH	MEDIUM	LOW	BEST PRACTICE	INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	54
Low	2
Best Practice	1
Information	3
TOTAL	**60**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	0
Low	1
Best Practice	0
Information	0
TOTAL	**1**

Vulnerabilities By CWE

SEVERITY FILTER : CRITICAL HIGH MEDIUM LOW BEST PRACTICE INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
79 - IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION ('CROSS-SITE SCRIPTING')				
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/authflow/password-recovery/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x008EA8)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/dz/webapps/mpp/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x006AE1)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/au/webapps/mpp/givingfund/policies/donation-refunds?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x040D29)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/dz/webapps/mpp/home?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x009DD3)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/ppcreditapply/he/de/errorFlow?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x011A6D)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/signin&country.x=US&locale.x=fr_XC&langTgl=fr?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x007F83)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/cgi-bin/wv_web/plJAG0g3PyHWSRcAOEb1ZWl4B8V-HK.zs.5fuFnclGjb6GG42thU9x8iEfIPs80xlo.DUA/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x045B44)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/lk/welcome/https:/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00ECC2)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/signin&country.x=US&locale.x=zh_XC&langTgl=zh?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x008283)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/fundraiser/charity/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0015A0)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/uk/webapps/mpp/business/platforms-and-marketplaces/directory?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x03FBAC)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/cgi-bin/wv_web/Hs6w.7IvQ3mDJIGRiW0FmtlU3gj.NlxNbrFnJQj8w7x0hg2UGCCNk.kvMjqG6-S4BZeE2A/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x041260)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/lk/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00017B)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/us/webapps/mpp/mobile-apps/paypal-app?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00A124)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	POST	https://www.paypal.com/us/brc/topics/paypal-account-management?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x03FF60)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/us/webapps/mpp/for-you/transfer-money/send-money?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00A450)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/webapps/mpp/ua/privacy-full?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00C579)%3C/scRipt%3E#User	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/cgi-bin/wv_web/ZJBI23HNmQwQxk2nrCnV4.2-tw-AWUsmW2.CPuQCQhPZNiuZCdu8o34wedXqxM85mzmYVg/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x012B0B)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/sitemap.xml?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000A12)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/welcome/https:/t.paypal.com/ts?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00B82B)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/us/webapps/mpp/account-selection?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x006567)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/lk/https:/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003878)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/cgi-bin/wv_web/vQZNYZVYDtHQqIHTrHSZvIl7t-QeVdnhV..ptsA06uTb4Jsw0JmTueh7npURXLXTg1xzVQ/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x03F870)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/cgi-bin/wv_web/s16Zcp5A6cNgl3hQDBVvIrafDeUEF8wWqNZhm..8P.RtV05rRzT6vuLjXZwEx61UsiTynA/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0422C5)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/cgi-bin/wv_web/csWXHVXP6hrv0qC5pbKOzWfZxQwFBXDUdZ5vd0Hs-O0dNMY8fCqNnp-wRuAADB.bcU3otw/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x014DED)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/lk/welcome/https:/t.paypal.com/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00EE71)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/.well-known/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00026F)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/crossdomain.xml?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0060AF)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/xoplatform/logger/api/log?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0077B2)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/ad/https:/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x017C72)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/tmui/locallb/workspace/fileRead.jsp?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00D6AF)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/signin&country.x=US&locale.x=en_US&langTgl=en?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x007DEF)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/fundraiser/charity/*?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00172E)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/cgi-bin/wv_web/.CFXO8b67BwWLLXHgC1oPQKOCbVAKp7p4wdj5sgHiqaMkVblcXf0fBRwGP1tecAMRNL-Tw/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x043A87)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/lk/webapps/mpp/pay-on-ebay?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004D76)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/webapps/mpp/ua/legalhub-full?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00C713)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/myaccount/profile/api/cookies/accept?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0097B0)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/inspire/listing/get/listing_leadership_bios?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x036DBF)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/cgi-bin/wv_web/gvx3U9xo2re3KRzV.XV3UAuNhy7MRlxb-ramBDlLJI.XjIWPgkQoj.vVWFegkLsEV-5i-A/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x044066)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/signin/connect/mobile/link?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0022A0)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/myaccount/money/push/opt-in?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0027A3)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/cm/home?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004739)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/ppcreditapply/he/gb/errorFlow?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x011C08)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/us/brc/article/einvoicing-solutions-vs-paper-invoicing?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x01F0CB)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/ar/webapps/mpp/ua/legalhub-full?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00E882)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000165)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/lk/home?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00026C)%3C/scRipt%3E#n1	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/lk/webapps/mpp/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004A53)%3C/scRipt%3E#n1	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/us/https:/t.paypal.com/ts?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x017543)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/uk/webapps/mpp/business/platforms-and-marketplaces/directory/platform-marketplace?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x03FDBD)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/signin&country.x=US&locale.x=es_XC&langTgl=es?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x008117)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/lk/webapps/mpp/ua/privacy-full?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x005D70)%3C/scRipt%3E#1	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/au/webapps/mpp/givingfund/policies/donor-terms-of-service?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x040981)%3C/scRipt%3E	MEDIUM
	[Possible] Cross-site Scripting	GET	https://www.paypal.com/https:/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x010995)%3C/scRipt%3E	MEDIUM
200 - INFORMATION EXPOSURE				
	[Possible] Internal IP Address Disclosure	GET	https://www.paypal.com/welcome/signup	LOW
	Referrer-Policy Not Implemented	GET	https://www.paypal.com/lk/home	BEST PRACTICE
	[Possible] Internal Path Disclosure (Windows)	GET	https://www.paypal.com/authflow/password-recovery/c:/https:/t.paypal.com/ts	INFORMATION
	Email Address Disclosure	GET	https://www.paypal.com/us/webapps/mpp/ua/privacy-full	INFORMATION
	ExpressJS Identified	GET	https://www.paypal.com/mobile/checkout	INFORMATION
20 - IMPROPER INPUT VALIDATION				
	User Controllable Cookie	GET	https://www.paypal.com/lk/https:/t.paypal.com/ts?bchn=mktg&bzsr=main&c_prefs=P%3D1%2CF%3D1%2Ctype%3Dimplicit&calc=a5dc8e7b1e444&ccpg=lk&comp=mppnodeweb&csci=83339922e411410d9f52996aab0aa205&cu=3&ef_policy=ccpa&env=live&lgcook=3&lgin=out&nojs=1&nsid=Vwz-tedrscABQZExHgW4Om-h6ZwIYd26&page=main%3Amktg%3Apersonal%3A%3Ahome%3A%3A%3A&pgld=ts&pgrp=main%3Amktg%3Apersonal%3A%3Ahome&pgsf=personal&pgst=Unknown&pgtf=Nodejs&pros=3&rsta=en_LK&s=ci&shir=ma...	LOW

1. [Possible] Cross-site Scripting

MEDIUM 54

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.

Vulnerabilities

- 1.1. https://www.paypal.com/.well-known/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00026F)%3C/scRipt%3E
- 1.2. https://www.paypal.com/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000165)%3C/scRipt%3E
- 1.3. https://www.paypal.com/ad/https:/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x017C72)%3C/scRipt%3E
- 1.4. https://www.paypal.com/ar/webapps/mpp/ua/legalhub-full?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00E882)%3C/scRipt%3E
- 1.5. https://www.paypal.com/au/webapps/mpp/givingfund/policies/donation-refunds?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x04…
- 1.6. https://www.paypal.com/au/webapps/mpp/givingfund/policies/donor-terms-of-service?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(…
- 1.7. https://www.paypal.com/authflow/password-recovery/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x008EA8)%3C/scRipt%3E
- 1.8. https://www.paypal.com/cgi-bin/wv_web/.CFXO8b67BwWLLXHgC1oPQKOCbVAKp7p4wdj5sgHiqaMkVblcXf0fBRwGP1tecAMRNL-Tw/?'%22--%3E%3C/st…
- 1.9. https://www.paypal.com/cgi-bin/wv_web/csWXHVXP6hrv0qC5pbKOzWfZxQwFBXDUdZ5vd0Hs-O0dNMY8fCqNnp-wRuAADB.bcU3otw/?'%22--%3E%3C/s…
- 1.10. https://www.paypal.com/cgi-bin/wv_web/gvx3U9xo2re3KRzV.XV3UAuNhy7MRlxb-ramBDlLJI.XjIWPgkQoj.vVWFegkLsEV-5i-A/?'%22--%3E%3C/style%3E…
- 1.11. https://www.paypal.com/cgi-bin/wv_web/Hs6w.7IvQ3mDJIGRiW0FmtlU3gj.NlxNbrFnJQj8w7x0hg2UGCCNk.kvMjqG6-S4BZeE2A/?'%22--%3E%3C/style%…
- 1.12. https://www.paypal.com/cgi-bin/wv_web/plJAG0g3PyHWSRcAOEb1ZWl4B8V-HK.zs.5fuFnclGjb6GG42thU9x8iEfIPs80xlo.DUA/?'%22--%3E%3C/style%3…
- 1.13. https://www.paypal.com/cgi-bin/wv_web/s16Zcp5A6cNgl3hQDBVvIrafDeUEF8wWqNZhm..8P.RtV05rRzT6vuLjXZwEx61UsiTynA/?'%22--%3E%3C/style%…
- 1.14. https://www.paypal.com/cgi-bin/wv_web/vQZNYZVYDtHQqIHTrHSZvIl7t-QeVdnhV..ptsA06uTb4Jsw0JmTueh7npURXLXTg1xzVQ/?'%22--%3E%3C/style…
- 1.15. https://www.paypal.com/cgi-bin/wv_web/ZJBI23HNmQwQxk2nrCnV4.2-tw-AWUsmW2.CPuQCQhPZNiuZCdu8o34wedXqxM85mzmYVg/?'%22--%3E%3C…
- 1.16. https://www.paypal.com/cm/home?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004739)%3C/scRipt%3E
- 1.17. https://www.paypal.com/crossdomain.xml?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0060AF)%3C/scRipt%3E
- 1.18. https://www.paypal.com/dz/webapps/mpp/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x006AE1)%3C/scRipt%3E
- 1.19. https://www.paypal.com/dz/webapps/mpp/home?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x009DD3)%3C/scRipt%3E
- 1.20. https://www.paypal.com/fundraiser/charity/*?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00172E)%3C/scRipt%3E
- 1.21. https://www.paypal.com/fundraiser/charity/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0015A0)%3C/scRipt%3E
- 1.22. https://www.paypal.com/https:/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x010995)%3C/scRipt%3E
- 1.23. https://www.paypal.com/inspire/listing/get/listing_leadership_bios?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x036DBF)%3C/s…
- 1.24. https://www.paypal.com/lk/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00017B)%3C/scRipt%3E
- 1.25. https://www.paypal.com/lk/home?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00026C)%3C/scRipt%3E#n1
- 1.26. https://www.paypal.com/lk/https:/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003878)%3C/scRipt%3E
- 1.27. https://www.paypal.com/lk/webapps/mpp/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004A53)%3C/scRipt%3E#n1
- 1.28. https://www.paypal.com/lk/webapps/mpp/pay-on-ebay?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004D76)%3C/scRipt%3E
- 1.29. https://www.paypal.com/lk/webapps/mpp/ua/privacy-full?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x005D70)%3C/scRipt%3E…
- 1.30. https://www.paypal.com/lk/welcome/https:/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00ECC2)%3C/scRipt%3E
- 1.31. https://www.paypal.com/lk/welcome/https:/t.paypal.com/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00EE71)%3C/scRipt%3E
- 1.32. https://www.paypal.com/myaccount/money/push/opt-in?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0027A3)%3C/scRipt%3E
- 1.33. https://www.paypal.com/myaccount/profile/api/cookies/accept?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0097B0)%3C/scRi…
- 1.34. https://www.paypal.com/ppcreditapply/he/de/errorFlow?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x011A6D)%3C/scRipt%3E
- 1.35. https://www.paypal.com/ppcreditapply/he/gb/errorFlow?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x011C08)%3C/scRipt%3E
- 1.36. https://www.paypal.com/signin&country.x=US&locale.x=en_US&langTgl=en?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x007…
- 1.37. https://www.paypal.com/signin&country.x=US&locale.x=es_XC&langTgl=es?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0081…
- 1.38. https://www.paypal.com/signin&country.x=US&locale.x=fr_XC&langTgl=fr?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x007F8…
- 1.39. https://www.paypal.com/signin&country.x=US&locale.x=zh_XC&langTgl=zh?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0082…
- 1.40. https://www.paypal.com/signin/connect/mobile/link?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0022A0)%3C/scRipt%3E
- 1.41. https://www.paypal.com/sitemap.xml?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000A12)%3C/scRipt%3E
- 1.42. https://www.paypal.com/tmui/locallb/workspace/fileRead.jsp?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00D6AF)%3C/scRipt…
- 1.43. https://www.paypal.com/uk/webapps/mpp/business/platforms-and-marketplaces/directory/platform-marketplace?'%22--%3E%3C/style%3E%3C/scRipt%3…
- 1.44. https://www.paypal.com/uk/webapps/mpp/business/platforms-and-marketplaces/directory?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enets…
- 1.45. https://www.paypal.com/us/brc/article/einvoicing-solutions-vs-paper-invoicing?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x01F…
- 1.46. https://www.paypal.com/us/brc/topics/paypal-account-management?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x03FF60)%3C…
- 1.47. https://www.paypal.com/us/https:/t.paypal.com/ts?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x017543)%3C/scRipt%3E
- 1.48. https://www.paypal.com/us/webapps/mpp/account-selection?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x006567)%3C/scRipt…
- 1.49. https://www.paypal.com/us/webapps/mpp/for-you/transfer-money/send-money?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00…
- 1.50. https://www.paypal.com/us/webapps/mpp/mobile-apps/paypal-app?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00A124)%3C/…
- 1.51. https://www.paypal.com/webapps/mpp/ua/legalhub-full?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00C713)%3C/scRipt%3E
- 1.52. https://www.paypal.com/webapps/mpp/ua/privacy-full?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00C579)%3C/scRipt%3E#…
- 1.53. https://www.paypal.com/welcome/https:/t.paypal.com/ts?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00B82B)%3C/scRipt%3E
- 1.54. https://www.paypal.com/xoplatform/logger/api/log?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0077B2)%3C/scRipt%3E

Show Remediation

2. [Possible] Internal IP Address Disclosure

LOW 1

Netsparker identified a Possible Internal IP Address Disclosure in the page.

It was not determined if the IP address was that of the system itself or that of an internal network.

Impact

There is no direct impact; however, this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

Vulnerabilities

- 2.1. https://www.paypal.com/welcome/signup

Show Remediation

3. User Controllable Cookie

LOW 1 CONFIRMED 1

Netsparker identified a user controllable cookie.

Impact

Attackers can easily set an arbitrary value in the cookie and this may allow them to bypass authentication, carry out attacks such as SQL injection and cross-site scripting or modify inputs in unexpected ways.

Vulnerabilities

- 3.1. https://www.paypal.com/lk/https:/t.paypal.com/ts?bchn=mktg&bzsr=main&c_prefs=P%3D1%2CF%3D1%2Ctype%3Dimplicit&calc=a5dc8e7b1e444&ccpg=l… CONFIRMED

Show Remediation

4. Referrer-Policy Not Implemented

BEST PRACTICE 1

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

- 4.1. https://www.paypal.com/lk/home

Show Remediation

5. [Possible] Internal Path Disclosure (Windows)

INFORMATION 1

Netsparker identified a possible Internal Path Disclosure (Windows) in the document.

Impact

There is no direct impact, however this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

Vulnerabilities

- 5.1. https://www.paypal.com/authflow/password-recovery/c:/https:/t.paypal.com/ts

Show Remediation

6. Email Address Disclosure

INFORMATION 1

Netsparker identified an Email Address Disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Vulnerabilities

- 6.1. https://www.paypal.com/us/webapps/mpp/ua/privacy-full

Show Remediation

7. ExpressJS Identified

INFORMATION 1

Netsparker identified that the target website is using ExpressJS as its web application framework.

This issue is reported as extra information only.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

- 7.1. https://www.paypal.com/mobile/checkout

Show Remediation

Show Scan Detail