The Kooples - Pentest Report

This report was generated by PenAutomate, providing insights into security vulnerabilities and potential threats identified during the automated penetration testing process. It aims to help fortify the security posture by addressing the vulnerabilities discovered.

1) Domain Analysis of thekooples.com

1.1 Basic Information

IP Address	104.16.89.23
Hostname	Not available
City	San Francisco
Region	California
Country	US
Location	37.7621,-122.3971
Organization	AS13335 Cloudflare, Inc.
Postal Code	94107
Timezone	America/Los_Angeles

1.2 Subdomains

Subdomain	IP Address
www.thekooples.com	**104.16.88.23**
www.thekooples.com	**104.16.89.23**

mail.thekooples.com	165.160.13.20
mail.thekooples.com	165.160.15.20
ftp.thekooples.com	52.208.113.59
smtp.thekooples.com	193.70.18.144
autodiscover.thekooples.com	52.98.202.72
autodiscover.thekooples.com	52.98.159.232
autodiscover.thekooples.com	52.98.206.200
autodiscover.thekooples.com	52.98.159.248
autodiscover.thekooples.com	52.97.215.120
autodiscover.thekooples.com	52.98.159.200
autodiscover.thekooples.com	52.98.202.88
autodiscover.thekooples.com	52.97.214.152
pop3.thekooples.com	193.70.18.144
dev.thekooples.com	104.16.37.69
dev.thekooples.com	104.17.22.82
admin.thekooples.com	213.218.128.146
news.thekooples.com	165.160.13.20
news.thekooples.com	165.160.15.20
docs.thekooples.com	90.115.49.5
email.thekooples.com	161.71.33.242
intranet.thekooples.com	195.154.252.75
api.thekooples.com	90.115.49.3
staging.thekooples.com	104.18.43.193

staging.thekooples.com	172.64.144.63
fr.thekooples.com	104.18.36.55
fr.thekooples.com	172.64.151.201
training.thekooples.com	195.154.171.231
us.thekooples.com	104.18.36.55
us.thekooples.com	172.64.151.201
event.thekooples.com	165.160.15.20
event.thekooples.com	165.160.13.20
careers.thekooples.com	137.74.145.234
erp.thekooples.com	165.160.13.20
erp.thekooples.com	165.160.15.20
eu.thekooples.com	104.18.36.55
eu.thekooples.com	172.64.151.201
prod.thekooples.com	199.232.169.124
www-test.thekooples.com	172.64.151.201
www-test.thekooples.com	104.18.36.55
sb.thekooples.com	172.246.17.32
imp.thekooples.com	193.70.18.144

1.3 Resolve DNS

Type	Value
A	165.160.13.20, 165.160.15.20
NS	indom30.indomco.fr., indom80.indomco.hk., indom10.indomco.com., indom20.indomco.net.

MX	0 thekooples.in.tmes.trendmicro.eu.
SOA	indom10.indomco.com. hostmaster.cscdns.net. 2018091412 86400 7200 604800 300
TXT	"_globalsign-domain-verification=G38FSO6JU3WTtDbUAKe5gKfqSzvCJ9_JHLtpsJITnr", "apple-domain-verification=DNkEIAMo9nLGeita", "facebook-domain-verification=oevh9qedp91tl9m6z3qb5e7wnhcnzh", "google-site-verification=X25sxTPkGerqia4qZisdUUYMAV-W776rFUXcAtMaWIM", "google-site-verification=Zb5O_RWlg1iW7rVxLf4RyHJ5HgutoLQ_Wph7M1u4h9A", "klaviyo-site-verification=S95LkB", "tmes=8ee6b7f3215a82dd542946d18867c8bb", "v=spf1 include:spf1.thekooples.com include:spf2.thekooples.com -all", "MS=ms87496788", "Sendinblue-code:154ce1be09edec8ed03a959805898061"

1.4 Email and Social Media

Emails Found	serviceclients@thekooples.com, servicelients@thekooples.com

Social Media Links	https://www.instagram.com/thekooples/, https://www.facebook.com/thekooples/, https://www.youtube.com/channel/UCWVsA_WpDlKiv0r3Q3AeQ3g

2) Exploitation

Selected IPs	
IP Address 1	**192.168.1.58**
IP Address 2	**192.168.1.161**

2.1 Directories finder (dirbuster)

IP Address	**Discovered Directories**
192.168.1.58	http://192.168.1.58/index http://192.168.1.58/test http://192.168.1.58/twiki http://192.168.1.58/tikiwiki http://192.168.1.58/ http://192.168.1.58/phpinfo

IP Address	Discovered Directories
192.168.1.161	http://192.168.1.161/uploads http://192.168.1.161/chat http://192.168.1.161/drupal http://192.168.1.161/phpmyadmin http://192.168.1.161/

2.2 Web Vulnerability

IP Address	Vulnerability Description
192.168.1.58	**Insecure server configuration: Exploiting insecure communication protocols**
192.168.1.58	**SQL injection vulnerability: Injecting SQL code into input fields**
192.168.1.58	**Insecure server configuration: Exploiting insecure communication protocols**
192.168.1.58	**SQL injection vulnerability: Injecting SQL code into input fields**
192.168.1.58	**Insecure server configuration: Exploiting insecure communication protocols**
192.168.1.58	**Insecure server configuration: Exploiting insecure communication protocols**
192.168.1.58	**Insecure server configuration: Exploiting insecure communication protocols**

IP Address	Vulnerability Description
192.168.1.161	**Insecure server configuration: Exploiting insecure communication protocols**
192.168.1.161	**Insecure server configuration: Exploiting insecure communication protocols**
192.168.1.161	**Insecure server configuration: Exploiting insecure communication protocols**
192.168.1.161	**Insecure server configuration: Exploiting insecure communication protocols**
192.168.1.161	**Insecure server configuration: Exploiting insecure communication protocols**
192.168.1.161	**SQL injection vulnerability: Injecting SQL code into input fields**
192.168.1.161	**Insecure server configuration: Exploiting insecure communication protocols**
192.168.1.161	**Insecure server configuration: Exploiting insecure communication protocols**

192.168.1.161	**Insecure server configuration: Exploiting insecure communication protocols**

2.3 Brute Force FTP

IP Address	Username	Password	Result
192.168.1.58	anonymous	anonymous	Success for FTP Brute Force
192.168.1.161			Failed

2.4 Brute Force SSH

IP Address	Username	Password	Result
192.168.1.58	user	user	for SSH Brute Force
192.168.1.161	vagrant	vagrant	for SSH Brute Force

3) Scan and Vulnerabilities

IP Address: 192.168.1.58 - OS Details: Linux 2.6.9 - 2.6.33

Service: ftp vsftpd 2.3.4 (Port 21/tcp)
Vulnerabilities: CVE-2011-2523

Service: ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) (Port 22/tcp)
Vulnerabilities: CVE-2012-1577, CVE-2011-2168, CVE-2010-4816, CVE-2011-4327, CVE-2008-3259, CVE-2010-4755, CVE-2012-0814, CVE-2010-4478, CVE-2011-1013, CVE-2011-5000, CVE-2010-5107, CVE-2010-4754, CVE-2023-51767, CVE-2008-1657

Service: telnet Linux telnetd (Port 23/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: smtp Postfix smtpd (Port 25/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: domain ISC BIND 9.4.2 (Port 53/tcp)
Vulnerabilities: CVE-2021-25219, CVE-2022-2795, CVE-2016-2848, CVE-2016-9444,

CVE-2012-3817, CVE-2012-1667, CVE-2009-0696, CVE-2012-1033, CVE-2016-2775, CVE-2009-4022, CVE-2010-0382, CVE-2015-8000, CVE-2020-8617, CVE-2020-8622, CVE-2021-25216, CVE-2017-3142, CVE-2009-0025, CVE-2016-9131, CVE-2010-0290, CVE-2012-4244, CVE-2010-3614, CVE-2016-1286, CVE-2015-8704, CVE-2012-5166, CVE-2010-0097, CVE-2016-6170, CVE-2017-3145, CVE-2016-1285, CVE-2021-25215, CVE-2015-8461, CVE-2020-8616, CVE-2015-8705, CVE-2016-8864, CVE-2008-0122, CVE-2017-3143, CVE-2008-4163, CVE-2023-3341, CVE-2014-8500, CVE-2011-1910, CVE-2017-3141, CVE-2011-4313

Service: http Apache httpd 2.2.8 ((Ubuntu) DAV/2) (Port 80/tcp)
Vulnerabilities: CVE-2011-4317, CVE-2012-3499, CVE-2012-0883, CVE-2017-7679, CVE-2010-1452, CVE-2007-6750, CVE-2016-8743, CVE-2015-3183, CVE-2007-6420, CVE-2011-3607, CVE-2022-37436, CVE-2009-1195, CVE-2009-3095, CVE-2011-4415, CVE-2008-0455, CVE-2016-4975, CVE-2012-2687, CVE-2009-3094, CVE-2024-24824, CVE-2013-5704, CVE-2014-0098, CVE-2009-3720, CVE-2017-3167, CVE-2023-31122, CVE-2013-1896, CVE-2023-45802, CVE-2012-4558, CVE-2017-9798, CVE-2009-2699, CVE-2016-5387, CVE-2017-9788, CVE-2009-0023, CVE-2024-24823, CVE-2010-0434, CVE-2017-12171, CVE-2011-3368, CVE-2008-2939, CVE-2013-1862, CVE-2009-1956, CVE-2012-0031, CVE-2024-2406, CVE-2014-0226, CVE-2011-3192, CVE-2013-6438, CVE-2016-8612, CVE-2010-0408, CVE-2014-0118, CVE-2010-1623, CVE-2008-2364, CVE-2012-0053, CVE-2009-1891, CVE-2008-0456, CVE-2009-1890, CVE-2014-0231, CVE-2006-20001, CVE-2009-3555, CVE-2011-3639, CVE-2009-3560

Service: rpcbind 2 (RPC #100000) (Port 111/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) (Port 445/tcp)
Vulnerabilities: CVE-2021-44141, CVE-2021-3670, CVE-2023-0225, CVE-2022-37967, CVE-2018-14628, CVE-2022-3437, CVE-2020-25722, CVE-2018-1057, CVE-2022-32745, CVE-2016-2123, CVE-2022-1615, CVE-2018-1050, CVE-2017-12151, CVE-2020-10745, CVE-2017-2619, CVE-2018-16852, CVE-2022-0336, CVE-2017-12163, CVE-2021-23192, CVE-2017-12150, CVE-2022-32742, CVE-2020-14323, CVE-2022-2031, CVE-2018-10919, CVE-2022-3592, CVE-2020-27840, CVE-2020-14318, CVE-2018-16860, CVE-2022-32744, CVE-2020-10760, CVE-2016-2124, CVE-2019-19344, CVE-2016-2125, CVE-2021-20316, CVE-2019-14833, CVE-2023-0614, CVE-2020-14303, CVE-2022-45141, CVE-2019-14861, CVE-2017-7494, CVE-2019-14847, CVE-2018-16841, CVE-2019-10218, CVE-2019-14902, CVE-2022-38023, CVE-2018-16851, CVE-2018-1139, CVE-2020-25717, CVE-2021-20277, CVE-2018-10918, CVE-2021-3738, CVE-2019-14907, CVE-2018-1140, CVE-2020-10704, CVE-2023-0922, CVE-2020-25721, CVE-2020-25718, CVE-2022-32746, CVE-2011-3585, CVE-2020-10700, CVE-2020-10730, CVE-2019-3870, CVE-2020-14383, CVE-2022-32743, CVE-2020-1472, CVE-2019-3880, CVE-2018-16857, CVE-2019-10197, CVE-2019-14870, CVE-2020-25719, CVE-2021-20251, CVE-2021-3671, CVE-2020-17049, CVE-2018-14629, CVE-2018-16853, CVE-2018-10858, CVE-2021-20254

Service: exec netkit-rsh rexecd (Port 512/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: login? (Port 513/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: tcpwrapped (Port 514/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: java-rmi GNU Classpath grmiregistry (Port 1099/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: bindshell Metasploitable root shell (Port 1524/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: nfs 2-4 (RPC #100003) (Port 2049/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: ftp ProFTPD 1.3.1 (Port 2121/tcp)
Vulnerabilities: CVE-2017-7418, CVE-2008-4242, CVE-2009-0542, CVE-2023-51713, CVE-2008-7265, CVE-2020-9272, CVE-2019-18217, CVE-2010-3867, CVE-2019-19271, CVE-2019-19272, CVE-2011-1137, CVE-2021-46854, CVE-2010-4652, CVE-2016-3125, CVE-2019-19270, CVE-2019-12815, CVE-2011-4130, CVE-2009-0543, CVE-2009-3639, CVE-2012-6095

Service: mysql MySQL 5.0.51a-3ubuntu5 (Port 3306/tcp)
Vulnerabilities: CVE-2012-4452, CVE-2012-0484, CVE-2012-0087, CVE-2010-3834, CVE-2010-3838, CVE-2008-3963, CVE-2012-0075, CVE-2009-4484, CVE-2010-3833, CVE-2010-3682, CVE-2012-0102, CVE-2010-3837, CVE-2010-1626, CVE-2008-2079, CVE-2008-7247, CVE-2008-4098, CVE-2009-2446, CVE-2010-1850, CVE-2012-0490, CVE-2010-3836, CVE-2009-4028, CVE-2012-0101, CVE-2010-1849, CVE-2009-5026, CVE-2009-4019, CVE-2008-0226, CVE-2010-3677, CVE-2010-1848, CVE-2012-0114

Service: postgresql PostgreSQL DB 8.3.0 - 8.3.7 (Port 5432/tcp)
Vulnerabilities: CVE-2010-1170, CVE-2022-2625, CVE-2015-0243, CVE-2020-1720, CVE-2019-10164, CVE-2013-1902, CVE-2010-0733, CVE-2012-3488, CVE-2021-23214, CVE-2010-3433, CVE-2012-0866, CVE-2013-1903, CVE-2014-0061, CVE-2012-3489, CVE-2014-8161, CVE-2015-3166, CVE-2023-2455, CVE-2009-0922, CVE-2021-3393, CVE-2012-0867, CVE-2013-1900, CVE-2009-3230, CVE-2022-41862, CVE-2010-0442, CVE-2023-2454, CVE-2012-0868, CVE-2009-3231, CVE-2014-0062, CVE-2015-0242, CVE-2012-2655, CVE-2015-0244, CVE-2017-7548, CVE-2017-7547, CVE-2021-20229, CVE-2009-4034, CVE-2014-0065, CVE-2009-3229, CVE-2010-1169, CVE-2021-32027, CVE-2015-0241, CVE-2010-4015, CVE-2017-7486, CVE-2018-10915, CVE-2009-4136, CVE-2014-0066, CVE-2014-0064, CVE-2015-3167, CVE-2010-1447, CVE-2013-0255, CVE-2014-0067, CVE-2014-0063, CVE-2012-2143, CVE-2011-2483, CVE-2014-0060, CVE-2021-3677, CVE-2010-1975

Service: vnc VNC (protocol 3.3) (Port 5900/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: X11 (access denied) (Port 6000/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: irc UnrealIRCd (Port 6667/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: ajp13 Apache Jserv (Protocol v1.3) (Port 8009/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: http Apache Tomcat/Coyote JSP engine 1.1 (Port 8180/tcp)
Vulnerabilities: CVE-2023-26044, CVE-2022-36032

IP Address: 192.168.1.161 - OS Details: Not available

Service: ftp ProFTPD 1.3.5 (Port 21/tcp)
Vulnerabilities: CVE-2017-7418, CVE-2019-19271, CVE-2016-3125, CVE-2015-3306, CVE-2019-19272, CVE-2023-51713, CVE-2013-4359, CVE-2021-46854, CVE-2019-19270, CVE-2020-9272, CVE-2019-18217

Service: ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0) (Port 22/tcp)
Vulnerabilities: CVE-2012-1577, CVE-2010-4816, CVE-2015-5600, CVE-2015-6564, CVE-2018-15919, CVE-2020-14145, CVE-2015-5352, CVE-2015-6563, CVE-2020-16088

Service: http Apache httpd 2.4.7 ((Ubuntu)) (Port 80/tcp)
Vulnerabilities: CVE-2018-17199, CVE-2022-26377, CVE-2020-1934, CVE-2017-7679, CVE-2020-35452, CVE-2021-40438, CVE-2016-8743, CVE-2015-3183, CVE-2018-1302, CVE-2022-37436, CVE-2018-1301, CVE-2014-8109, CVE-2022-22719, CVE-2016-2161, CVE-2016-0736, CVE-2020-1927, CVE-2022-22720, CVE-2021-39275, CVE-2021-26691, CVE-2016-4975, CVE-2021-34798, CVE-2022-22721, CVE-2024-24824, CVE-2013-5704, CVE-2022-28615, CVE-2022-29404, CVE-2014-0098, CVE-2015-3185, CVE-2021-26690, CVE-2017-3167, CVE-2023-31122, CVE-2023-45802, CVE-2022-30556, CVE-2019-0220, CVE-2017-9798, CVE-2018-1303, CVE-2015-0228, CVE-2018-1312, CVE-2016-5387, CVE-2017-9788, CVE-2014-0117, CVE-2024-24823, CVE-2017-12171, CVE-2021-44790, CVE-2014-3581, CVE-2022-23943, CVE-2018-1283, CVE-2019-17567, CVE-2024-2406, CVE-2014-0226, CVE-2013-6438, CVE-2016-8612, CVE-2019-0217, CVE-2014-0118, CVE-2022-31813, CVE-2021-44224, CVE-2019-10098, CVE-2017-15715, CVE-2022-28614, CVE-2022-36760, CVE-2014-0231, CVE-2006-20001, CVE-2023-25690, CVE-2019-10092, CVE-2020-11985, CVE-2017-15710

Service: netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) (Port 445/tcp)
Vulnerabilities: CVE-2021-44141, CVE-2021-3670, CVE-2023-0225, CVE-2022-37967, CVE-2018-14628, CVE-2022-3437, CVE-2020-25722, CVE-2018-1057, CVE-2022-32745, CVE-2016-2123, CVE-2022-1615, CVE-2018-1050, CVE-2017-12151, CVE-2020-10745, CVE-2017-2619, CVE-2018-16852, CVE-2022-0336, CVE-2017-12163, CVE-2021-23192, CVE-2017-12150, CVE-2022-32742, CVE-2020-14323, CVE-2022-2031, CVE-2018-10919, CVE-2022-3592, CVE-2020-27840, CVE-2020-14318, CVE-2018-16860, CVE-2022-32744, CVE-2020-10760, CVE-2016-2124, CVE-2019-19344, CVE-2016-2125, CVE-2021-20316, CVE-2019-14833, CVE-2023-0614, CVE-2020-14303, CVE-2022-45141, CVE-2019-14861, CVE-2017-7494, CVE-2019-14847, CVE-2018-16841, CVE-2019-10218, CVE-2019-14902, CVE-2022-38023, CVE-2018-16851, CVE-2018-1139, CVE-2020-25717, CVE-2021-20277, CVE-2018-10918, CVE-2021-3738, CVE-2019-14907, CVE-2018-1140, CVE-2020-10704,

CVE-2023-0922, CVE-2020-25721, CVE-2020-25718, CVE-2022-32746, CVE-2011-3585, CVE-2020-10700, CVE-2020-10730, CVE-2019-3870, CVE-2020-14383, CVE-2022-32743, CVE-2020-1472, CVE-2019-3880, CVE-2018-16857, CVE-2019-10197, CVE-2019-14870, CVE-2020-25719, CVE-2021-20251, CVE-2021-3671, CVE-2020-17049, CVE-2018-14629, CVE-2018-16853, CVE-2018-10858, CVE-2021-20254

Service: ipp CUPS 1.7 (Port 631/tcp)
Vulnerabilities: CVE-2021-25317, CVE-2012-5519, CVE-2012-6094, CVE-2013-6891, CVE-2014-3537, CVE-2014-2856, CVE-2014-5031, CVE-2014-5030

Service: mysql MySQL (unauthorized) (Port 3306/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: http Jetty 8.1.7.v20120910 (Port 8080/tcp)
Vulnerabilities: No CVE vulnerabilities found

IP Address: 192.168.1.46 - OS Details: Linux 3.2 - 4.9

Service: ftp (Port 21/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: http nginx (reverse proxy) (Port 65000/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: netbios-ssn Samba smbd 4.6.2 (Port 445/tcp)
Vulnerabilities: CVE-2021-44141, CVE-2023-34966, CVE-2021-3670, CVE-2023-4154, CVE-2023-34968, CVE-2023-0225, CVE-2022-37967, CVE-2018-14628, CVE-2022-3437, CVE-2020-25722, CVE-2018-1057, CVE-2022-32745, CVE-2016-2123, CVE-2023-42669, CVE-2022-1615, CVE-2018-1050, CVE-2017-12151, CVE-2020-10745, CVE-2017-2619, CVE-2018-16852, CVE-2022-0336, CVE-2017-12163, CVE-2021-23192, CVE-2017-12150, CVE-2022-32742, CVE-2020-14323, CVE-2022-2031, CVE-2018-10919, CVE-2022-3592, CVE-2020-27840, CVE-2020-14318, CVE-2018-16860, CVE-2022-32744, CVE-2020-10760, CVE-2023-34967, CVE-2016-2124, CVE-2019-19344, CVE-2016-2125, CVE-2021-20316, CVE-2019-14833, CVE-2023-0614, CVE-2020-14303, CVE-2022-45141, CVE-2019-14861, CVE-2023-5568, CVE-2017-7494, CVE-2023-4091, CVE-2019-14847, CVE-2018-16841, CVE-2019-10218, CVE-2019-14902, CVE-2022-38023, CVE-2018-16851, CVE-2018-1139, CVE-2020-25717, CVE-2017-14746, CVE-2021-20277, CVE-2018-10918, CVE-2021-3738, CVE-2019-14907, CVE-2018-1140, CVE-2020-10704, CVE-2023-42670, CVE-2023-0922, CVE-2017-11103, CVE-2020-25721, CVE-2020-25718, CVE-2022-32746, CVE-2011-3585, CVE-2020-10700, CVE-2020-10730, CVE-2019-3870, CVE-2020-14383, CVE-2022-32743, CVE-2020-1472, CVE-2019-3880, CVE-2018-16857, CVE-2019-10197, CVE-2023-3961, CVE-2019-14870, CVE-2017-15275, CVE-2020-25719, CVE-2021-20251, CVE-2021-3671, CVE-2020-17049, CVE-2018-14629, CVE-2018-16853, CVE-2018-10858, CVE-2021-20254

Service: ssl/http nginx (reverse proxy) (Port 443/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: iscsi Synology DSM Snapshot Replication iSCSI LUN (Port 3261/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: secureidprop? (Port 5510/tcp)
Vulnerabilities: No CVE vulnerabilities found

Service: synobtrfsreplicad Synology Snapshot Replication shared folder (Port 5566/tcp)
Vulnerabilities: No CVE vulnerabilities found