Keamanan Jaringan

Reconnaissance Dan Vulnerability Website

Nama : Rafli Eggy Ilham

Nim : 09011281520088

Dosen pengampuh : Deris Setiawan, M.T.,Ph.D

Jurusan Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

Tahun Ajaran 2019

RECONNAISSANCE

Reconnaissance merupakan tahap persiapan di mana attacker atau hacker mencari informasi-informasi mengenai target sebanyak-banyaknya untuk meluncurkan serangan. Dalam hal ini, pengumpulan data target dapat berupa informasi tentang organisasi yang diikuti oleh target, pegawai, operasi, jaringan, dan sistem yang dimiliki oleh target. Reconnaissance dibagi menjadi 2 tipe:

- Passive Reconnaissance

  Tipe ini digunakan ketika attacker mengumpulkan informasi tanpa berinteraksi langsung dengan target. Contohnya, mencari informasi lewat internet, majalah, media sosial target.

- Active Reconnaissance

  Attacker mencari informasi secara langsung berinteraksi dengan target. Bisa jadi tipe ini sangat beresiko. Ini berfungsi agar attacker dapat mencari celah untuk melakukan serangan. Contohnya seperti menelepon targetnya, atau bertanya kepada rekan kerja target.

Berikut contoh 3 Reconnaissance website

1. Website pemerintah : www.padang.go.id

- DNS record adalah data yang menyajikan pemetaan dan pengalamatan sebuah nama domain internet .Berikut adalah DNS Records untuk padang.go.id

DNS Records for padang.go.id — cache expires in 1 minutes and 11 seconds

Hostname	Type	TTL	Priority	Content
padang.go.id	SOA	3599		asa.ns.cloudflare.com dns@cloudflare.com 2030117510 10000 2400 604800 3600
padang.go.id	NS	21599		asa.ns.cloudflare.com
padang.go.id	NS	21599		terry.ns.cloudflare.com
padang.go.id	A	299		36.66.19.43
padang.go.id	MX	299	10	padang.go.id
www.padang.go.id	A	299		36.66.19.43
www.padang.go.id	CNAME	299		padang.go.id
www.padang.go.id	MX	299	10	padang.go.id

- Similliar Domain padang.go.id

Similar Domains

padan-art.com | padan-elc.com | padan-peleg.com | padan.biz | padan.cl | padan.cn | padan.co.il | padan.co.ir | padan.co.uk | padan.com | padan.com.cn | padan.de | padan.desa.id | padan.ir | padan.net | padan.org | padan.org.uk | padan.pl | padana-autoattrezzature.com | padana-cleanroom.com |

padan-art.com | padan-elc.com | padan-peleg.com | padan.biz | padan.cl | padan.cn | padan.co.il | padan.co.ir | padan.co.uk | padan.com | padan.com.cn | padan.de | padan.desa.id | padan.ir | padan.net | padan.org | padan.org.uk | padan.pl | padana-autoattrezzature.com | padana-cleanroom.com

- Informasi tentang web hosting yang digunakan website padang.go.id

Hosting Info for Website:	**www.padang.go.id**	**#235,568** position in world sites rating
Popularity:	3,570 visitors per day	« Show Ma
IP Address:	36.66.19.43	
IP Location:	Indonesia, Jakarta, Jakarta	
IP Reverse DNS (Host):	36.66.19.43	
Hosting Company:	**Telekomunikasi Indonesia**	
Hosting IP Range:	36.64.0.0 - 36.95.255.255 (2,097,152 ip)	Other Sites on IP »
Hosting Address:	Pt. Telkom Indonesia, Sto Telkom Gambir 3Th Floor, Medan Merdeka Selatan, Jakarta	
Hosting Country:	Indonesia	
Hosting Phone:	+62-21-34353699	
Hosting CIDR:	36.64.0.0/11	

IP Address Change History:	**Www.padang.go.id Website used IP Addresses -** • 222.124.132.206 (222.124.132.206) used on 13 March 2018 • 222.124.132.203 (222.124.132.203) used on 07 January 2017 • 222.124.132.206 (222.124.132.206) used on 23 October 2016 • 222.124.132.203 (222.124.132.203) used on 09 September 2016 • ... ... *Found: 7 ip addresses ... ... more »* • 36.66.19.43 - site using this IP address now
Website Nameservers:	**www.padang.go.id using 2 DNS:** asa.ns.cloudflare.com [3,449 sites] (173.245.58.246) terry.ns.cloudflare.com [3,033 sites] (173.245.59.237) *More Information »*

No	Nameserver (DNS)	Nameserver IP Address	Country	Total Websites using Nameserver	TOP World Websites using Nameserver	Update Time
1	asa.ns.cloudflare.com	173.245.58.246	USA	3,451 sites	76 sites	08 Feb 2019, 09:40
2	terry.ns.cloudflare.com	173.245.59.237	USA	3,034 sites	72 sites	08 Feb 2019, 09:36

- Berikut adalah IP Range dari padang.go.id

Current IP Range:	**36.66.19.0 - 36.66.19.255**
IP Range Location:	Indonesia, Jakarta, Jakarta
IP Owner:	**Telekomunikasi Indonesia**
Owner Full IP Range:	36.64.0.0 - 36.95.255.255
Owner Address:	Pt. Telkom Indonesia, Sto Telkom Gambir 3Th Floor, Medan Merdeka Selatan, Jakarta
Owner Country:	Indonesia
Owner Phone:	+62-21-34353699
All Owner IP Ranges:	203.130.192.0 - 203.130.255.255, 36.64.0.0 - 36.95.255.255, 222.124.0.0 - 222.124.255.255, 125.160.0.0 - 125.163.255.255, 61.94.0.0 - 61.94.255.255, 61.5.0.0 - 61.5.127.255
All Owner CIDR:	203.130.192.0/18, 36.64.0.0/11, 222.124.0.0/16, 125.160.0.0/14, 61.94.0.0/16, 61.5.0.0/17
All Owner IP Reverse DNS (Host)s:	132.subnet222.mma-astinet.telkom.net.id, 36.66.135.140, 156.subnet222-124-211.astinet.telkom.net.id, 18.subnet125-162-173.speedy.telkom.net.id, 61.94.100.60, ppp-kbb-b.telkom.net.id
ASN:	AS17974

- Traceroute adalah suatu perintah untuk menunjukan rute yang dilewati paket untuk mencapai tujuan. Berikut adalah Tracerout dari padang.go.id

Ping

```
PING padang.go.id (36.66.19.43) 56(84) bytes of data.
64 bytes from 36.66.19.43: icmp_seq=1 ttl=46 time=237 ms
64 bytes from 36.66.19.43: icmp_seq=2 ttl=46 time=240 ms
64 bytes from 36.66.19.43: icmp_seq=3 ttl=46 time=237 ms
64 bytes from 36.66.19.43: icmp_seq=5 ttl=46 time=238 ms

--- padang.go.id ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 25895ms
rtt min/avg/max/mdev = 237.671/238.647/240.693/1.278 ms
```

Traceroute

```
traceroute to padang.go.id (36.66.19.43), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  3.713 ms  3.671 ms  3.682 ms
 2  216.182.226.32 (216.182.226.32)  23.160 ms 216.182.226.50 (216.182.226.50)  17.228 ms 216.182.231.38 (216.182.231.38)  25.696 ms
 3  100.66.8.60 (100.66.8.60)  19.251 ms 100.66.8.24 (100.66.8.24)  22.513 ms 100.66.8.168 (100.66.8.168)  22.524 ms
 4  100.66.14.16 (100.66.14.16)  19.782 ms 100.66.11.98 (100.66.11.98)  22.805 ms 100.66.11.60 (100.66.11.60)  48.698 ms
 5  100.66.7.73 (100.66.7.73)  18.892 ms 100.66.6.191 (100.66.6.191)  17.491 ms 100.66.6.17 (100.66.6.17)  29.116 ms
 6  100.66.5.127 (100.66.5.127)  17.841 ms 100.66.5.25 (100.66.5.25)  22.649 ms 100.66.5.21 (100.66.5.21)  22.679 ms
 7  100.65.12.81 (100.65.12.81)  0.869 ms 100.65.15.241 (100.65.15.241)  0.914 ms 100.65.15.177 (100.65.15.177)  1.198 ms
 8  52.93.28.177 (52.93.28.177)  1.229 ms 52.93.28.187 (52.93.28.187)  1.377 ms 52.93.28.181 (52.93.28.181)  1.797 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  eqix-dc2.pttelekomunikasi.com (206.126.237.47)  2.305 ms  2.293 ms 52.93.114.36 (52.93.114.36)  20.608 ms
14  54.239.111.237 (54.239.111.237)  3.925 ms 180.240.192.150 (180.240.192.150)  233.062 ms  231.115 ms
15  eqix-dc2.pttelekomunikasi.com (206.126.237.47)  1.640 ms  1.610 ms  1.552 ms
16  180.240.193.30 (180.240.193.30)  239.617 ms 180.240.192.150 (180.240.192.150)  231.212 ms 180.240.193.30 (180.240.193.30)  231.435 ms
17  * 180.240.192.73 (180.240.192.73)  290.613 ms *
18  180.240.193.30 (180.240.193.30)  226.579 ms  231.694 ms *
19  36.66.19.43 (36.66.19.43)  237.452 ms !X * *
```

- Berikut untuk mengetahui website padang.go.id bias dibuka dari suatu Negara lain atau tidak . jika hasil ping mengatakan 100% Loss Packet ,kemungkinan situs padang.go.id tidak bias diakses di Negara tersebut :

Ping to: www.padang.go.id					
Checkpoint	**Result**	**min. rtt**	**avg. rtt**	**max. rtt**	**IP**
Australia - Perth (auper01)	OK	213.814	213.873	213.988	36.66.19.43
Australia - Brisbane (aubne02)	OK	244.401	244.460	244.617	36.66.19.43
Argentina - Buenos Aires (arbue01)	Not available				
Australia - Sydney (ausyd04)	OK	297.153	297.229	297.308	36.66.19.43
United States - Atlanta (usatl02)	OK	232.656	232.909	233.636	36.66.19.43
Australia - Sydney (ausyd03)	OK	226.913	227.041	227.147	36.66.19.43
Brazil - Sao Paulo (brsao04)	OK	348.465	348.518	348.592	36.66.19.43
Brazil - Porto Alegre (brpoa01)	OK	368.949	369.070	369.183	36.66.19.43
Brazil - Rio de Janeiro (brrio01)	OK	349.583	349.857	350.549	36.66.19.43
Canada - Vancouver (cavan03)	OK	298.822	298.993	299.789	36.66.19.43
Belgium - Antwerp (beanr03)	OK	181.777	182.161	182.663	36.66.19.43
Bulgaria - Sofia (bgsof02)	OK	210.205	210.296	210.425	36.66.19.43
India - Bangalore (inblr01)	OK	153.061	153.113	153.226	36.66.19.43
United States - Boulder (uswbu01)	OK	243.247	243.298	243.350	36.66.19.43
United States - Boston (usbos02)	OK	248.988	249.195	249.982	36.66.19.43
Canada - Toronto (cator02)	OK	263.297	263.702	264.357	36.66.19.43
China - Hangzhou (cnhgh01)	Packets lost (20%)	332.327	332.865	333.518	36.66.19.43
United States - Santa Clara (usscz03)	OK	244.045	244.341	245.196	36.66.19.43
China - Beijing (cnbjs02)	OK	448.429	467.189	481.789	36.66.19.43
Switzerland - Zurich (chzrh01)	OK	264.376	264.783	265.404	36.66.19.43
United States - Charlotte (usclt02)	OK	243.117	243.760	244.415	36.66.19.43
Costa Rica - San Jose (crsjo01)	OK	316.106	316.321	316.665	36.66.19.43
Czech Republic - Prague (czprg01)	OK	261.899	262.043	262.804	36.66.19.43
Germany - Munich (demuc02)	OK	155.376	155.410	155.466	36.66.19.43
Germany - Frankfurt (defra03)	OK	184.041	184.102	184.233	36.66.19.43
Germany - Berlin (deber01)	OK	263.585	263.746	263.868	36.66.19.43
United Arab Emirates - Dubai (aedxb01)	OK	138.123	138.327	139.315	36.66.19.43
Ireland - Dublin (iedub03)	OK	189.066	189.158	189.238	36.66.19.43
Egypt - Cairo (egcai02)	OK	332.510	332.974	333.848	36.66.19.43
Spain - Madrid (esmad02)	OK	196.274	196.369	196.474	36.66.19.43
France - Paris (frpar04)	OK	186.707	186.740	186.798	36.66.19.43
France - Lille (frlle02)	OK	154.971	155.000	155.028	36.66.19.43
United Kingdom - Edinburgh (gbedi01)	OK	264.951	265.043	265.098	36.66.19.43
Greece - Athens (grath01)	OK	210.593	210.681	210.858	36.66.19.43
Switzerland - Geneva (chgva01)	OK	246.170	246.330	247.245	36.66.19.43
China - Hong Kong (hkhkg02)	OK	32.550	32.676	32.905	36.66.19.43
Hungary - Budapest (hubud01)	OK	185.618	185.680	185.804	36.66.19.43
India - Mumbai (inbom02)	OK	154.013	154.455	155.869	36.66.19.43
India - New Delhi (inicd02)	OK	367.898	368.257	369.227	36.66.19.43
Italy - Milan (itmil01)	OK	246.320	246.586	247.304	36.66.19.43
Indonesia - Jakarta (idjkt02)	OK	22.655	22.824	22.990	36.66.19.43

Italy - Padova (itpda01)	OK	152.581	152.708	152.874	36.66.19.43
Japan - Tokyo (jptok02)	OK	72.793	72.827	72.895	36.66.19.43
South Africa - Johannesburg (zajnb01)	OK	346.934	347.349	348.597	36.66.19.43
Denmark - Copenhagen (dkcph02)	OK	172.491	172.597	172.671	36.66.19.43
Israel - Kiryat-Matalon (ilktm02)	OK	225.449	225.582	225.795	36.66.19.43
Korea, Republic of - Seoul (krsel01)	OK	67.014	67.046	67.065	36.66.19.43
Ukraine - Kiev (uaiev01)	OK	184.124	184.172	184.279	36.66.19.43
United States - Ashburn (usabn07)	OK	236.737	236.849	237.022	36.66.19.43
Lithuania - Vilnius (ltvno02)	OK	267.797	268.435	268.934	36.66.19.43
United States - Los Angeles (uslax02)	OK	181.831	181.889	181.999	36.66.19.43
Australia - Melbourne (aumel04)	OK	90.469	90.728	91.140	36.66.19.43
United States - Miami (usmia02)	OK	247.693	248.138	248.738	36.66.19.43
United States - Seattle (ussea03)	OK	211.371	211.569	211.866	36.66.19.43
Canada - Montreal (camtr02)	OK	239.956	240.241	240.976	36.66.19.43
Mexico - Guadalajara (mxgdl02)	OK	238.130	238.843	239.297	36.66.19.43
Malaysia - Kuala Lumpur (mykul02)	OK	180.959	181.798	185.289	36.66.19.43
Netherlands - Groningen (nlgrq02)	OK	163.491	163.602	163.708	36.66.19.43
United States - New York (usnyc03)	OK	244.281	244.840	245.332	36.66.19.43
Netherlands - Amsterdam (nlams05)	OK	159.247	159.631	160.484	36.66.19.43
Norway - Oslo (noosl03)	OK	221.699	221.800	222.052	36.66.19.43
Panama - Panama City (papty02)	OK	253.357	253.887	254.757	36.66.19.43
United States - Phoenix (usphx02)	OK	253.438	253.536	253.604	36.66.19.43
Portugal - Lisbon (ptlis02)	OK	274.244	274.676	275.270	36.66.19.43
Poland - Warsaw (plwrs01)	OK	204.886	241.073	276.760	36.66.19.43
United States - Philadelphia (usphl01)	OK	238.089	238.279	239.090	36.66.19.43
United States - Dallas (usdal02)	OK	215.788	216.023	216.354	36.66.19.43
Russian Federation - St. Petersburg (ruled01)	OK	205.562	205.645	205.702	36.66.19.43
Italy - Rome (itrom02)	OK	198.036	200.488	207.869	36.66.19.43
Russian Federation - Moscow (rumow02)	OK	197.819	197.894	197.987	36.66.19.43
United States - San Diego (ussan01)	OK	238.222	238.300	238.372	36.66.19.43
Sweden - Stockholm (sesto02)	OK	204.452	204.498	204.570	36.66.19.43
Singapore - Singapore (sgsin03)	OK	2.451	2.497	2.590	36.66.19.43
United States - Salt Lake City (usslc01)	OK	212.137	212.739	213.232	36.66.19.43
Saudi Arabia - Riyadh (saruh01)	OK	306.999	307.673	311.196	36.66.19.43
United States - Austin (usaus02)	OK	216.423	216.725	217.430	36.66.19.43
United States - St. Louis (usstl01)	OK	250.617	250.901	251.609	36.66.19.43
Finland - Tampere (fitmp03)	OK	186.215	186.315	186.538	36.66.19.43
Thailand - Bangkok (thbkk02)	OK	55.625	55.746	55.990	36.66.19.43
Turkey - Istanbul (trist02)	OK	293.035	293.312	294.272	36.66.19.43
United Kingdom - Manchester (gbmnc01)	OK	256.826	256.884	256.928	36.66.19.43
Ukraine - Kharkov (uahrk02)	OK	203.713	203.829	203.905	36.66.19.43
United Kingdom - London (gblon01)	OK	190.382	190.859	192.977	36.66.19.43
Austria - Vienna (atvie01)	OK	274.323	274.415	274.473	36.66.19.43
Viet Nam - Ho Chi Minh City (vnsgn01)	OK	263.655	263.739	263.823	36.66.19.43
South Africa - Durban (zadur01)	OK	351.107	352.011	354.815	36.66.19.43
South Africa - Cape Town (zacpt02)	OK	314.161	314.260	314.315	36.66.19.43

2. Website dalam negeri (www.detik.com)

- DNS record adalah data yang menyajikan pemetaan dan pengalamatan sebuah nama domain internet, Record DNS memberikan Informasi penting tentang lokasi dan jenis server diantaranya . Berikut adalah DNS Records untuk detik.com :

DNS Records for detik.com

Hostname	Type	TTL	Priority	Content
detik.com	SOA	899		ns.detik.com sysnet@detik.com 20
detik.com	NS	899		ns.detik.net.id
detik.com	NS	899		ns1.detik.com
detik.com	NS	899		ns.detik.com
detik.com	NS	899		ns1.detik.net.id
detik.com	NS	899		ns2.detik.net.id
detik.com	NS	899		ns2.detik.com
detik.com	A	56		203.190.242.211
detik.com	A	56		103.49.221.211
detik.com	MX	3599	10	aspmx.l.google.com
detik.com	MX	3599	20	alt1.aspmx.l.google.com
detik.com	MX	3599	20	alt2.aspmx.l.google.com
detik.com	MX	3599	30	aspmx2.googlemail.com
detik.com	MX	3599	30	aspmx3.googlemail.com
detik.com	MX	3599	30	aspmx4.googlemail.com
detik.com	MX	3599	30	aspmx5.googlemail.com
www.detik.com	A	76		103.49.221.211
www.detik.com	A	76		203.190.242.211
www.detik.com	CNAME	5395		detik.com
www.detik.com	MX	3599	20	alt1.aspmx.l.google.com
www.detik.com	MX	3599	20	alt2.aspmx.l.google.com
www.detik.com	MX	3599	30	aspmx2.googlemail.com
www.detik.com	MX	3599	30	aspmx3.googlemail.com
www.detik.com	MX	3599	30	aspmx4.googlemail.com
www.detik.com	MX	3599	30	aspmx5.googlemail.com
www.detik.com	MX	3599	10	aspmx.l.google.com

- Registrar Info www.detik.com

  Name : NETWORK SOLUTIONS, LLC.

  Whois Server : whois.networksolutions.com

  Referral URL : http://networksolutions.com

  Status :clientTransferProhibited https://icann.org/epp#clientTransferProhibited

- Important Dates

  Expires On :2020-05-28

  Registered On :1998-05-29

  Updated On : 2018-05-24

- Name Servers

  NS.DETIK.COM : 203.190.242.2

  NS.DETIK.NET.ID :203.190.242.2

  NS1.DETIK.COM :203.190.240.131

  NS1.DETIK.NET.ID :203.190.240.131

  NS2.DETIK.COM :103.49.220.220

- Similar Domains

detik-aturan.com | detik-bandung.com | detik-berita.com | detik-berita.net | detik-bisnis.com | detik-bola.com | detik-bola.info | detik-detik.com | detik-finance.com | detik-food.com | detik-hot.com | detik-id.com | detik-iklan.com | detik-iklan.info | detik-islam.com | detik-loker.com | detik-maluku.com | detik-medan.net | detik-mobil.com | detik-net.com

- Registrar Data

  Registrant Contact Information:

  Name : PT. Trans Digital Media

  Organization :PT. Trans Digital Media

  Address : Jl. Kapten Tendean Kav 12-14A

  City : Jakarta

  State / Province : DKI Jakarta

  Postal Code : 12790

  Country ID Phone : +62.2179187722

  Fax : +62.2179187759

Email : sarwani@detik.com

- Informasi tentang web hosting yang digunakan website detik.com

Hosting Info for Website:	**www.detik.com**
Popularity:	2,500,000 visitors per day
IP Address:	103.49.221.211
IP Location:	Indonesia, Jakarta, Jakarta
IP Reverse DNS (Host):	s211-cast-211-221-49-103.detik.com
Top Level Host Usage:	186 sites use XXX.detik.com as IP Reverse DNS
Hosting Company / IP Owner:	**Pt Detik Ini Juga**
Owner IP Range:	103.49.220.0 - 103.49.223.255 (1,024 ip) Other Sites on IP »
Owner Address:	Pt Detik Ini Juga, Jakarta Selatan
Owner Country:	Indonesia
Owner Phone:	+62-21-7941177, +62-21-79187722
Owner Website:	www.detik.net.id, www.idnic.net
Owner CIDR:	103.49.220.0/22
IP Address Change History:	**Www.detik.com Website used IP Addresses -** • 203.190.241.43 (203.190.241.43) used on 18 October 2016 • 103.49.221.211 - site using this IP address now *More Information »*

Current IP Range:	**103.49.221.1 - 103.49.221.254**
IP Range Location:	Indonesia, Jakarta, Jakarta
IP Owner:	**Pt Detik Ini Juga**
Owner Full IP Range:	103.49.220.0 - 103.49.223.255
Owner Address:	Pt Detik Ini Juga, Jakarta Selatan
Owner Country:	Indonesia
Owner Phone:	+62-21-7941177, +62-21-79187722
Owner Website:	www.detik.net.id, www.idnic.net
All Owner IP Ranges:	103.49.220.0 - 103.49.223.255, 203.190.240.0 - 203.190.247.255
All Owner CIDR:	103.49.220.0/22, 203.190.240.0/21
All Owner IP Reverse DNS (Host)s:	s211-cast-211-221-49-103.detik.com, s1.dtk43.detik.com

- www.detik.com using 6 DNS:

ns.detik.com [37 sites] (203.190.242.2)

ns.detik.net.id [38 sites] (203.190.242.2)

ns1.detik.com [37 sites] (203.190.240.131)

ns1.detik.net.id [38 sites] (203.190.240.131)

ns2.detik.com [34 sites] (103.49.220.220)

ns2.detik.net.id [34 sites] (103.49.220.220)

No	Nameserver (DNS)	Nameserver IP Address	Country	Total Websites using Nameserver	TOP World Websites using Nameserver	Update Time
1	ns1.detik.net.id	203.190.240.131	Indonesia	38 sites	4 sites	07 Feb 2019, 22:34
2	ns.detik.net.id	203.190.242.2	Indonesia	38 sites	4 sites	07 Feb 2019, 22:34
3	ns.detik.com	203.190.242.2	Indonesia	37 sites	4 sites	07 Feb 2019, 22:34
4	ns1.detik.com	203.190.240.131	Indonesia	37 sites	4 sites	07 Feb 2019, 22:34
5	ns2.detik.com	103.49.220.220	Indonesia	34 sites	3 sites	07 Feb 2019, 22:34
6	ns2.detik.net.id	103.49.220.220	Indonesia	34 sites	3 sites	07 Feb 2019, 22:34

- **Domain Status:** clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Whois Archive for domain/s with the same ip address - 203.190.241.43

No	Web Site	Whois date
1	detikinet.com	26 Apr 2015, 20:42
2	detikfood.com	23 Apr 2015, 09:26
3	detikhealth.com	20 Apr 2015, 05:59
4	detikfinance.com	26 Feb 2015, 08:41
5	detikinet.com	21 Nov 2014, 02:30
6	detikfood.com	31 Jul 2014, 13:36
7	detikhot.com	27 Jun 2014, 09:27
8	detiknews.com	16 Apr 2014, 09:58
9	detikinet.com	06 Jan 2014, 04:57
10	detikfinance.com	12 Oct 2013, 18:40
11	detiksport.com	16 Sep 2013, 00:11
12	detikbandung.com	24 Nov 2015, 02:04
13	vpn-edydarkopi.tk	08 Apr 2015, 23:37

Total: **13** records

Detik.com Sites Whois Lookup Archive

No	Url	Owner	Owner Address	Site Ip Address	Hosting Nserver 1	Domain Created	Domain Expired	Whois date
1	detik.com	Aldevco Octagon Building It 2	Jl. Warung Jati Barat Raya 75 Jakarta, DKI Jakarta 12740 IN	203.190.242.69	203.190.242.2	13 May 2004	28 May 2016	14 Oct 2013, 10:36
2	detik.com			203.190.242.69	203.190.242.2	29 May 1998	28 May 2016	18 Jul 2015, 20:25
3	detik.com			203.190.242.211	203.190.242.2	29 May 1998	28 May 2018	03 Jan 2017, 17:33
4	detik.com			203.190.242.211	203.190.242.2	29 May 1998		18 Sep 2017, 07:13
5	detik.com			203.190.242.211	203.190.242.2	29 May 1998		21 Oct 2017, 08:34
6	detik.com			203.190.242.211	203.190.242.2	29 May 1998		20 May 2018, 02:49
7	detik.com			103.49.221.211	203.190.242.2	29 May 1998		19 Sep 2018, 15:15

Total: **7** records

Go Sites Whois Lookup Archive »

Websites IP Address Change History for IP - 103.49.221.211

No	Website	Old IP Address was	Host was	Date when site was using this IP	World Site Popular Rating was
1	detikhot.com	103.49.221.211	103.49.221.211	29 Jul 2018	# 5,963,789
2	detikshop.com	103.49.221.211	103.49.221.211	07 Apr 2018	# 3,780,613
3	www.cimbclicks.co.id	103.49.221.211	103.49.221.211	22 May 2017	# 24,501
4	www.indo-hadiah.com	103.49.221.211	103.49.221.211	22 Feb 2017	# 62,545

Total: **4** records

- Traceroute detik.com

```
PING detik.com (103.49.221.211) 56(84) bytes of data.
64 bytes from s211-cast-211-221-49-103.detik.com (103.49.221.211): icmp_seq=1 ttl=33 time=250 ms
64 bytes from s211-cast-211-221-49-103.detik.com (103.49.221.211): icmp_seq=2 ttl=33 time=250 ms
64 bytes from s211-cast-211-221-49-103.detik.com (103.49.221.211): icmp_seq=3 ttl=33 time=250 ms
64 bytes from s211-cast-211-221-49-103.detik.com (103.49.221.211): icmp_seq=4 ttl=33 time=250 ms
64 bytes from s211-cast-211-221-49-103.detik.com (103.49.221.211): icmp_seq=5 ttl=33 time=250 ms

--- detik.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 250.304/250.420/250.488/0.070 ms
```

```
traceroute to detik.com (203.190.242.211), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  0.691 ms  0.536 ms  0.832 ms
 2  216.182.231.52 (216.182.231.52)  20.231 ms 216.182.226.42 (216.182.226.42)  19.443 ms 216.182.231.34 (216.182.231.34)  21.138 ms
 3  100.66.8.102 (100.66.8.102)  20.148 ms 100.66.8.208 (100.66.8.208)  13.260 ms 100.66.8.110 (100.66.8.110)  19.670 ms
 4  100.66.14.62 (100.66.14.62)  16.640 ms 100.66.14.212 (100.66.14.212)  60.228 ms 100.66.10.220 (100.66.10.220)  16.582 ms
 5  100.66.6.247 (100.66.6.247)  21.580 ms 100.66.7.117 (100.66.7.117)  14.603 ms 100.66.7.63 (100.66.7.63)  28.349 ms
 6  100.66.5.33 (100.66.5.33)  14.648 ms 100.66.5.43 (100.66.5.43)  14.188 ms 100.66.5.117 (100.66.5.117)  11.029 ms
 7  100.65.13.225 (100.65.13.225)  0.995 ms 100.65.12.49 (100.65.12.49)  0.961 ms 100.65.15.129 (100.65.15.129)  18.018 ms
 8  52.93.28.181 (52.93.28.181)  1.767 ms 52.93.28.169 (52.93.28.169)  1.738 ms 52.93.28.191 (52.93.28.191)  1.858 ms
 9  * * *
10  * * *
```

```
11  * * 52.93.114.84 (52.93.114.84)  23.309 ms
12  * * *
13  52.93.114.96 (52.93.114.96)  30.882 ms 52.93.114.36 (52.93.114.36)  30.339 ms eqix-dc2.pttelekomunikasi.com (206.126.237.47)  7.734 ms
14  180.240.192.149 (180.240.192.149)  236.579 ms * *
15  eqix-dc2.pttelekomunikasi.com (206.126.237.47)  1.731 ms  1.703 ms *
16  180.240.193.78 (180.240.193.78)  236.411 ms *  236.785 ms
17  * 36.66.26.97 (36.66.26.97)  254.045 ms *
18  * * 180.240.193.78 (180.240.193.78)  237.280 ms
19  s2-211-242.190.203.detik.com (203.190.242.211)  255.992 ms  252.725 ms  255.937 ms
```

3. Website Luar Negeri (www.usatoday.com)

- Registrar Info

  Name :MarkMonitor, Inc.

  Whois Server :whois.markmonitor.com

  Referral URL :http://www.markmonitor.com

  Status :

  clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)

  clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)

  clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)

  serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)

  serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)

  serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

- Important Dates

  Expires On : 2023-04-30

  Registered On : 1994-04-29

  Updated On : 2019-01-09

- Name Servers

  dns1.p04.nsone.net : 198.51.44.4

  dns2.p04.nsone.net :198.51.45.4

  dns3.p04.nsone.net :198.51.44.68

  dns4.p04.nsone.net :198.51.45.68

  ns01.gannett-dns.com :45.54.66.1

  ns02.gannett-dns.com :45.54.66.65

  ns03.gannett-dns.com :45.54.66.129

  ns04.gannett-dns.com :45.54.66.193

- Similar Domains

usato-adserver.com | usato-adserver.net | usato-artigrafiche.com | usato-audi.com | usato-auto.com | usato-auto.net | usato-bimbi.com | usato-bimbi.net | usato-ch.com | usato-ci.com | usato-day.com | usato-dentale.com | usato-doc.com | usato-ferrari.com | usato-fotografico.info | usato-fotografico.it | usato-garantito.com | usato-garantito.it | usato-hifi.it | usato-informatica.com

- Registrar Data

  Registrant Contact Information:

  Name :DNS Administrator

  Organization **:**Gannett Satellite Information Network, Inc.

  Address **:** 7950 Jones Branch Drive,

  City **:**McLean

  State / Province **:** va

  Postal Code **:** 22107

  Country **:**US

  Phone **:**+1.7038546000

  Fax **:**+1.7038546001

  Email **:** DOMAIN-REGISTRANT@GMTI.GANNETT.COM

- DNS Records

DNS Records for usatoday.com

Hostname	Type	TTL	Priority	Content
usatoday.com	SOA	1199		dns1.p04.nsone.net hostmaster@nsone.net 1549667623 1200 600 604800 300
usatoday.com	NS	1199		dns1.p04.nsone.net
usatoday.com	NS	1199		dns2.p04.nsone.net
usatoday.com	NS	1199		dns3.p04.nsone.net
usatoday.com	NS	1199		dns4.p04.nsone.net
usatoday.com	NS	1199		ns01.gannett-dns.com
usatoday.com	NS	1199		ns02.gannett-dns.com
usatoday.com	NS	1199		ns03.gannett-dns.com
usatoday.com	NS	1199		ns04.gannett-dns.com
usatoday.com	A	753		159.54.242.176
usatoday.com	MX	501	200	us-smtp-inbound-1.mimecast.com
usatoday.com	MX	501	200	us-smtp-inbound-2.mimecast.com
www.usatoday.com	A	29		151.101.2.62

www.usatoday.com	A	29	151.101.66.62
www.usatoday.com	A	29	151.101.130.62
www.usatoday.com	A	29	151.101.194.62
www.usatoday.com	CNAME	488	domains.gannett.map.fastly.net

- Informasi tentang web hosting yang digunakan website usatoday.com

Hosting Info for Website:	**www.usatoday.com** **#460** position in world sites rating
Popularity:	700,000 visitors per day « Show Map
IP Address:	151.101.250.62
IP Location:	USA, California, San Francisco
IP Reverse DNS (Host):	151.101.250.62
Hosting Company:	**Fastly**
Hosting IP Range:	151.101.0.0 - 151.101.255.255 (65,536 ip) Other Sites on IP »
Hosting Address:	Po Box 78266, San Francisco, CA, 94107, US
Hosting Country:	USA
Hosting Phone:	+1-410-703-8240, +1-415-758-0146, +1-415-404-9374
Hosting CIDR:	151.101.0.0/16
Whois Record Created:	01 Feb 2016
Whois Record Updated:	13 Aug 2018

Www.usatoday.com Website used IP Addresses -

- 151.101.22.62 (151.101.22.62) used on 07 February 2019
- 159.54.242.176 (host-176.242.54.159.gannett.com) used on 14 January 2019
- 151.101.22.62 (151.101.22.62) used on 14 October 2018
- 151.101.34.62 (151.101.34.62) used on 28 September 2018
- ... ... Found: 53 ip addresses ... ... more »
- 151.101.250.62 - site using this IP address now

www.usatoday.com using 8 DNS:

- dns1.p04.nsone.net (198.51.44.4)
- dns2.p04.nsone.net (198.51.45.4)
- dns3.p04.nsone.net (198.51.44.68)
- dns4.p04.nsone.net (198.51.45.68)
- ns01.gannett-dns.com (45.54.66.1)
- ns02.gannett-dns.com (45.54.66.65)
- ns03.gannett-dns.com (45.54.66.129)
- ns04.gannett-dns.com (45.54.66.193)

No	Nameserver (DNS)	Nameserver IP Address	Country	Total Websites using Nameserver	TOP World Websites using Nameserver	Update Time
1	dns1.p04.nsone.net	198.51.44.4	USA	4,383 sites	51 sites	09 Feb 2019, 04:31
2	dns2.p04.nsone.net	198.51.45.4	USA	4,356 sites	50 sites	09 Feb 2019, 04:31
3	dns3.p04.nsone.net	198.51.44.68	USA	4,348 sites	48 sites	09 Feb 2019, 04:31
4	dns4.p04.nsone.net	198.51.45.68	USA	4,348 sites	48 sites	09 Feb 2019, 04:31
5	ns02.gannett-dns.com	45.54.66.65	USA	363 sites	33 sites	09 Feb 2019, 04:31
6	ns03.gannett-dns.com	45.54.66.129	USA	363 sites	33 sites	09 Feb 2019, 04:31
7	ns01.gannett-dns.com	45.54.66.1	USA	363 sites	33 sites	09 Feb 2019, 04:31
8	ns04.gannett-dns.com	45.54.66.193	USA	361 sites	33 sites	09 Feb 2019, 04:31

- Treacareout use.today.com

```
PING usatoday.com (159.54.242.176) 56(84) bytes of data.
64 bytes from host-176.242.54.159.gannett.com (159.54.242.176): icmp_seq=1 ttl=238 time=4.66 ms
64 bytes from host-176.242.54.159.gannett.com (159.54.242.176): icmp_seq=2 ttl=238 time=56.4 ms
64 bytes from host-176.242.54.159.gannett.com (159.54.242.176): icmp_seq=3 ttl=238 time=5.01 ms
64 bytes from host-176.242.54.159.gannett.com (159.54.242.176): icmp_seq=4 ttl=238 time=4.95 ms
64 bytes from host-176.242.54.159.gannett.com (159.54.242.176): icmp_seq=5 ttl=238 time=4.78 ms

--- usatoday.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 4.664/15.167/56.421/20.627 ms
```

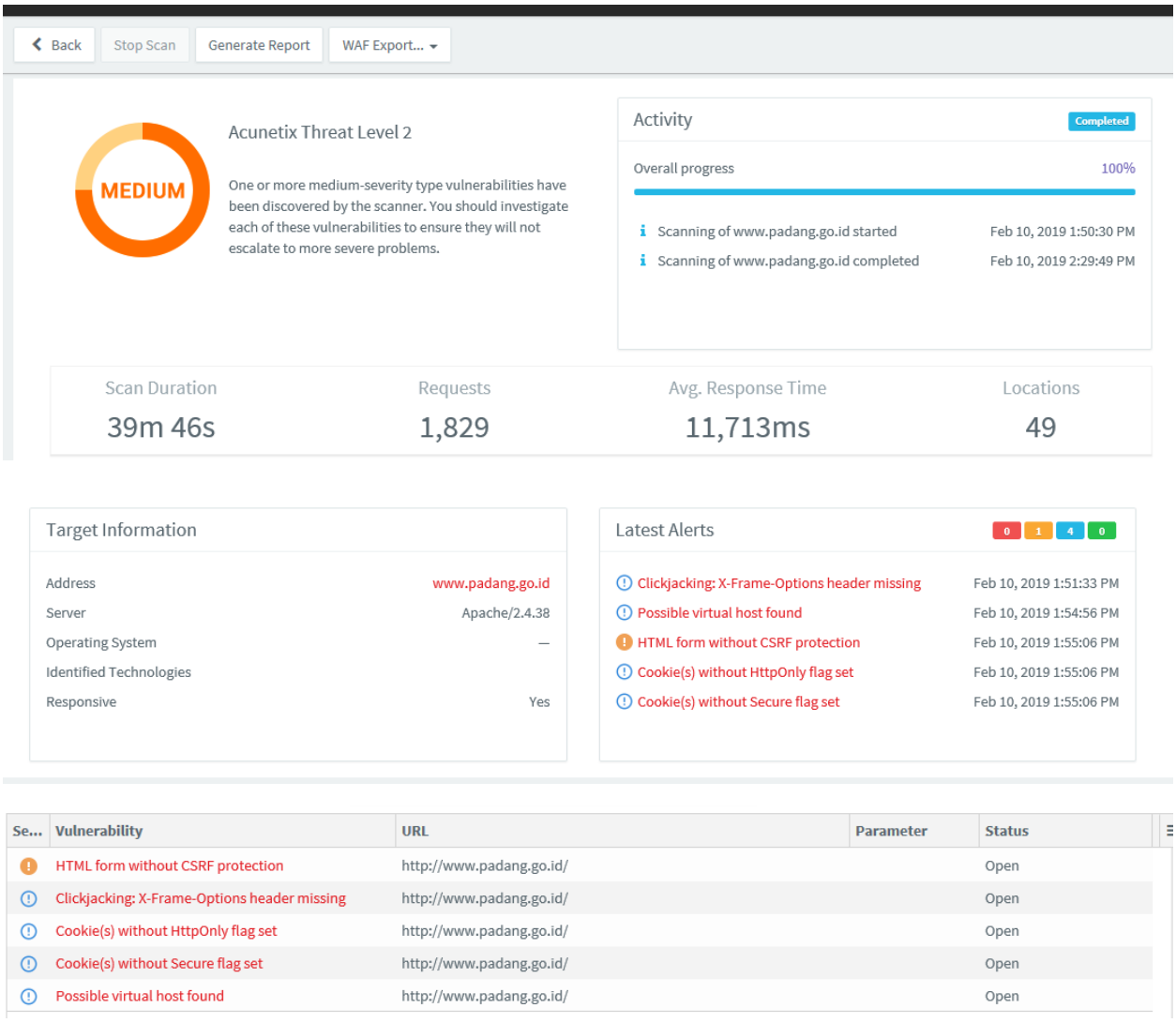
```
traceroute to usatoday.com (159.54.242.176), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  0.569 ms  0.505 ms  0.743 ms
 2  216.182.231.48 (216.182.231.48)  22.850 ms 216.182.231.52 (216.182.231.52)  6.244 ms 216.182.226.60 (216.182.226.60)  57.689 ms
 3  100.66.13.62 (100.66.13.62)  11.939 ms 100.66.9.170 (100.66.9.170)  17.924 ms 100.66.8.178 (100.66.8.178)  13.149 ms
 4  100.66.10.118 (100.66.10.118)  16.362 ms 100.66.11.232 (100.66.11.232)  15.401 ms 100.66.11.204 (100.66.11.204)  22.287 ms
 5  100.66.6.91 (100.66.6.91)  59.613 ms 100.66.6.127 (100.66.6.127)  12.773 ms 100.66.6.63 (100.66.6.63)  22.862 ms
 6  100.66.5.135 (100.66.5.135)  12.766 ms 100.66.5.227 (100.66.5.227)  21.040 ms 100.66.5.73 (100.66.5.73)  13.083 ms
 7  100.65.13.65 (100.65.13.65)  6.124 ms 100.65.15.17 (100.65.15.17)  1.282 ms 100.65.12.97 (100.65.12.97)  0.769 ms
 8  52.93.28.197 (52.93.28.197)  1.637 ms 52.93.28.195 (52.93.28.195)  2.381 ms 52.93.28.177 (52.93.28.177)  2.018 ms
 9  * * *
10  * * *
11  52.93.114.32 (52.93.114.32)  18.502 ms * *
12  54.239.108.143 (54.239.108.143)  1.902 ms * *
13  54.240.201.201 (54.240.201.201)  1.647 ms 52.93.114.86 (52.93.114.86)  17.192 ms 54.240.201.205 (54.240.201.205)  1.458 ms
14  54.239.108.173 (54.239.108.173)  2.727 ms 54.239.108.111 (54.239.108.111)  3.270 ms host-2.43.54.159.gannett.com (159.54.43.2)  2.758 ms
15  host-5.159.54.159.gannett.com (159.54.159.5)  4.806 ms  4.788 ms  4.534 ms
16  host-176.242.54.159.gannett.com (159.54.242.176)  4.799 ms  4.751 ms host-2.43.54.159.gannett.com (159.54.43.2)  2.395 ms
```

- **VULNERABILITY (KELEMAHAN)**

Vulnerability adalah suatu kelemahan program/infrastruktur yang memungkinkan terjadinya exploitasi system. kerentanan atau vulnerability ini terjadi akibat ksalahan dalam merancang,membuat atau mengimplementasikan sebuah system . Berikut tipe kerentanan atau vulnerability :

1. **High Risk Alert Level 3 :** Kerentanan dikategorikan sebagai yang paling berbahaya, yang menempatkan target scan pada risiko maksimum untuk hacking dan pencurian data.
2. **Medium Risk Alert Level 2 :** Kerentanan disebabkan oleh server misconfiguration dan sitecoding yang lemah, yang memfasilitasi gangguan server dan intrusi.
3. **Low Risk Alert Leve 1 :** Kerentanan berasal dari kurangnya enkripsi lalu lintas data atau jalur direktori pengungkapan.
4. **Information Alert :** ini adalah item yang telah ditemukan selama scan dan yang dianggap menarik, misalnya kemungkinan pengungkapan alamat internal IP atau alamat email, atau pencocokan string pencarian ditemukan di database Google Hacking, atau informasi tentang layanan yang telah ditemukan selama scanning.

1. Berikut adalah Vulnerability dalam website www.padang.go.id menggunakan Acunetix :



Pada website www.padang.go.id kerentanan atau vulnerability terletak pada Medium Risk Alert Level 2 itu artinya server misconfiguration dan sitecoding yang lemah, yang memfasilitasi gangguan server dan intrusi.

Berikut beberapa deskripsi kerentanan pada situs pemerintah padang.go.id :

1. Clickjacking

- Deskripsi kerentanan Clickjacking

  Clickjacking adalah teknik kejahatan untuk menipu pengguna Web agar mengklik sesuatu yang berbeda dari apa yang dilihat pengguna yang dikliknya, sehingga berpotensi

mengungkapkan informasi rahasia atau mengendalikan komputer mereka sementara mengklik halaman web yang tampaknya tidak berbahaya. Server tidak mengembalikan header X-Frame-Options yang berarti bahwa situs web ini bisa berisiko terhadap serangan clickjacking.

- Dampak dari kerentanan ini
  Dampaknya tergantung pada aplikasi web yang terpengaruh
- Cara memperbaiki kerentanan ini
  Konfigurasikan server web Anda untuk menyertakan header X-Frame-Options. Header respons HTTP X-Frame-Options dapat digunakan untuk menunjukkan apakah browser diizinkan membuat halaman situs yang lain . Situs dapat menggunakan header X-frame-options ini untuk menghindari serangan clickjacking, dengan memastikan bahwa konten mereka tidak tertanam ke situs lain.

2. Possible virtual host found

- Deskripsi kerentanan :
  Hosting virtual adalah metode hosting beberapa nama domain (dengan penanganan masing-masing nama yang terpisah) pada satu server (atau kumpulan server). Ini memungkinkan satu server untuk berbagi sumber dayanya, seperti siklus memori dan prosesor, tanpa memerlukan semua layanan yang disediakan untuk menggunakan nama host yang sama. Server web ini merespons secara berbeda ketika header Host dimanipulasi dan berbagai host virtual umum diuji.

- Dampak dari kerentanan ini
  Kemungkinan pengungkapan informasi sensitive

- Cara memperbaiki kerentanan ini
  Konsultasikan dengan konfigurasi host virtual dan periksa apakah host virtual ini harus dapat diakses public

3. HTML Form Without CSRF Protection

- Deskripsi kerentanan

Pemalsuan Permintaan Lintas Situs (CSRF, atau XSRF) adalah kerentanan di mana penyerang menipu korban untuk mengajukan permintaan yang tidak ingin dilakukan oleh korban. Oleh karena itu, dengan CSRF, penyerang menyalahgunakan kepercayaan yang dimiliki aplikasi web dengan browser korban. Acunetix menemukan formulir HTML tanpa perlindungan anti-CSRF yang jelas dilaksanakan. Baca bagian 'Detail serangan' untuk informasi lebih lanjut tentang formulir HTML yang terpengaruh.

- Dampak dari kerentanan ini

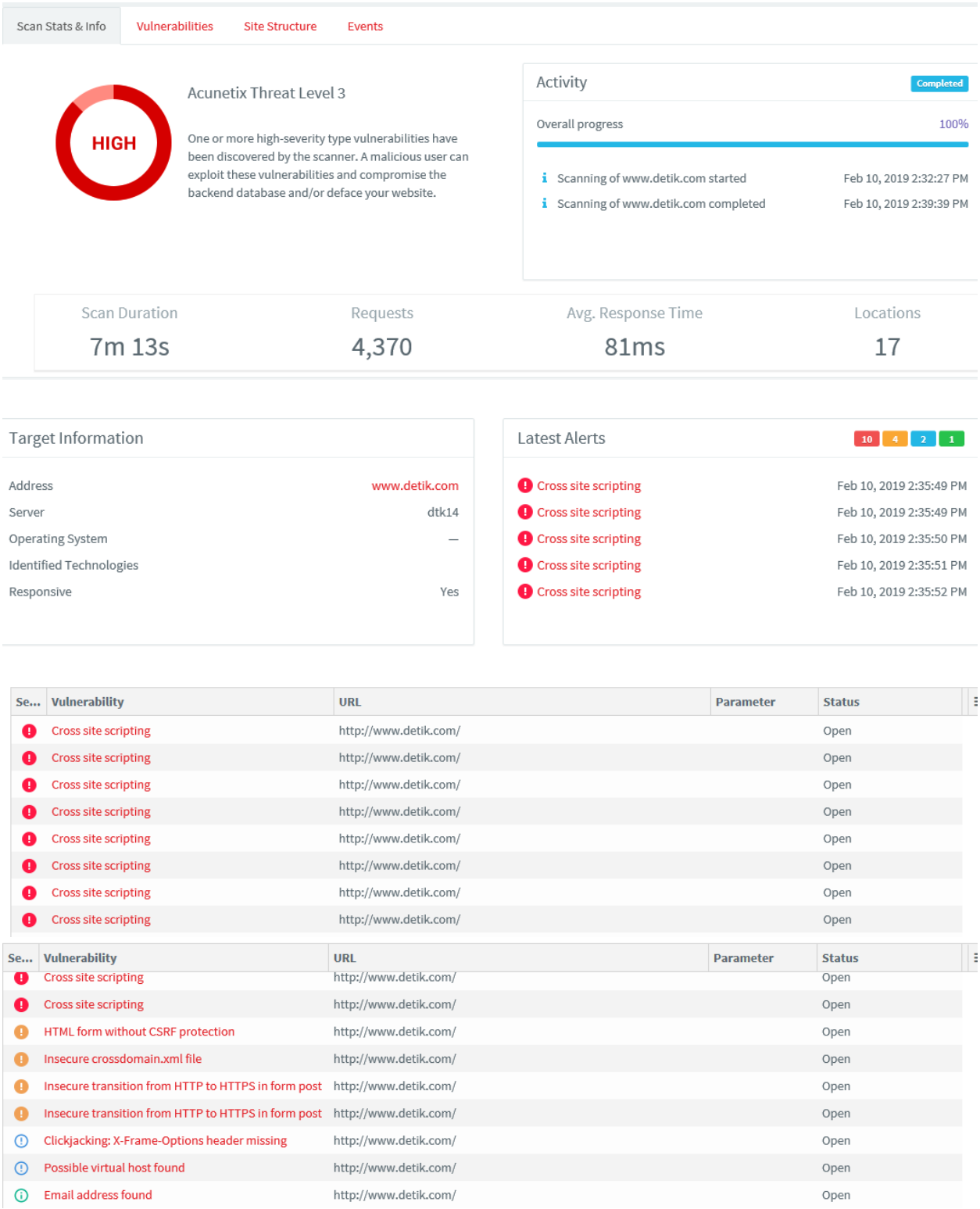
  Penyerang dapat menggunakan CSRF untuk menipu korban agar mengakses situs web yang dihosting oleh penyerang, atau mengklik URL yang berisi permintaan jahat atau tidak sah. CSRF adalah jenis serangan 'wakil bingung' yang memanfaatkan otentikasi dan otorisasi korban ketika permintaan yang dipalsukan dikirim ke server web. Oleh karena itu, jika kerentanan CSRF dapat memengaruhi pengguna yang sangat istimewa seperti administrator, kompromi aplikasi penuh mungkin dilakukan

- Cara memperbaiki kerentanan ini

  Verifikasi apakah formulir ini membutuhkan perlindungan anti-CSRF dan implementasikan penanggulangan CSRF jika perlu. Teknik yang direkomendasikan dan paling banyak digunakan untuk mencegah serangan CSRF dikenal sebagai The anti-CSRF token, juga kadang-kadang disebut sebagai token sinkronisasi. Karakteristik sistem anti-CSRF yang dirancang dengan baik melibatkan atribut-atribut berikut.

  - Token anti-CSRF harus unik untuk setiap sesi pengguna Sesi akan berakhir secara otomatis setelah waktu yang sesuai
  - Token anti-CSRF harus berupa nilai acak kriptografis yang panjangnya signifikan
  - Token anti-CSRF harus aman secara kriptografis, yaitu, dihasilkan oleh algoritma Pseudo-Random Number Generator (PRNG) yang kuat
  - Token anti-CSRF ditambahkan sebagai bidang tersembunyi untuk formulir, atau di dalam URL (hanya diperlukan jika permintaan GET menyebabkan perubahan status, yaitu, permintaan GET tidak idempoten) Server harus menolak tindakan yang diminta jika token anti-CSRF gagal validasi

2. Berikut adalah Vulnerability dalam website www.detik.com menggunakan Acunetix :



Scan Stats & Info | Vulnerabilities | Site Structure | Events

HIGH

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Activity — Completed

Overall progress 100%

Scanning of www.detik.com started Feb 10, 2019 2:32:27 PM

Scanning of www.detik.com completed Feb 10, 2019 2:39:39 PM

Scan Duration	Requests	Avg. Response Time	Locations
7m 13s	4,370	81ms	17

Target Information

Address	www.detik.com
Server	dtk14
Operating System	—
Identified Technologies	
Responsive	Yes

Latest Alerts — 10 4 2 1

Cross site scripting	Feb 10, 2019 2:35:49 PM
Cross site scripting	Feb 10, 2019 2:35:49 PM
Cross site scripting	Feb 10, 2019 2:35:50 PM
Cross site scripting	Feb 10, 2019 2:35:51 PM
Cross site scripting	Feb 10, 2019 2:35:52 PM

Se...	Vulnerability	URL	Parameter	Status
	Cross site scripting	http://www.detik.com/		Open
	Cross site scripting	http://www.detik.com/		Open
	Cross site scripting	http://www.detik.com/		Open
	Cross site scripting	http://www.detik.com/		Open
	Cross site scripting	http://www.detik.com/		Open
	Cross site scripting	http://www.detik.com/		Open
	Cross site scripting	http://www.detik.com/		Open
	Cross site scripting	http://www.detik.com/		Open

Se...	Vulnerability	URL	Parameter	Status
	Cross site scripting	http://www.detik.com/		Open
	Cross site scripting	http://www.detik.com/		Open
	HTML form without CSRF protection	http://www.detik.com/		Open
	Insecure crossdomain.xml file	http://www.detik.com/		Open
	Insecure transition from HTTP to HTTPS in form post	http://www.detik.com/		Open
	Insecure transition from HTTP to HTTPS in form post	http://www.detik.com/		Open
	Clickjacking: X-Frame-Options header missing	http://www.detik.com/		Open
	Possible virtual host found	http://www.detik.com/		Open
	Email address found	http://www.detik.com/		Open

Pada website www.detik.com kerentanan atau vulnerability terletak pada **High Risk Alert Level 3** yaitu Kerentanan dikategorikan sebagai yang paling berbahaya, yang menempatkan target scan pada risiko maksimum untuk hacking dan pencurian data.

Deskripsi kerentanan pada situs dalam negeri www.detik.com :

- Deskripsi kerentanan Cross-site Scripting (XSS)

  Cross-site Scripting (XSS) mengacu pada serangan injeksi kode sisi klien di mana penyerang dapat mengeksekusi skrip berbahaya ke situs web atau aplikasi web yang sah. XSS terjadi ketika aplikasi web menggunakan input pengguna yang tidak divalidasi atau tidak terenkripsi dalam output yang dihasilkannya
- Dampak dari kerentanan ini

  JavaScript berbahaya memiliki akses ke semua objek yang sama dengan sisa halaman web, termasuk akses ke cookie dan penyimpanan lokal, yang sering digunakan untuk menyimpan token sesi. Jika penyerang dapat memperoleh cookie sesi pengguna, mereka kemudian dapat menyamar sebagai pengguna itu. Selain itu, JavaScript dapat membaca dan membuat modifikasi sewenang-wenang untuk konten halaman yang sedang ditampilkan kepada pengguna. Oleh karena itu, XSS bersama dengan beberapa rekayasa sosial yang cerdik membuka banyak kemungkinan bagi penyerang
- Cara memperbaiki kerentanan ini

  Terapkan pengkodean dan / atau validasi yang bergantung pada konteks ke input pengguna yang diberikan pada sebuah pag

- Deskripsi kerentanan Insecure crossdomain.xml file

  Model keamanan browser biasanya mencegah konten web dari satu domain mengakses data dari domain lain. Ini umumnya dikenal sebagai "kebijakan asal yang sama". File kebijakan URL memberikan izin lintas-domain untuk membaca data. Mereka mengizinkan operasi yang tidak diizinkan secara default. File kebijakan URL terletak, secara default, di direktori root server target, dengan nama crossdomain.xml (misalnya, di www.example.com/crossdomain.xml).

Ketika suatu domain ditentukan dalam file crossdomain.xml, situs menyatakan bahwa ia bersedia mengizinkan operator dari server mana pun di domain itu untuk mendapatkan dokumen apa pun di server tempat file kebijakan berada. File crossdomain.xml yang digunakan di situs web ini membuka server ke semua domain (penggunaan tanda bintang "*" saat wildcard murni didukung) seperti:

```
<cross-domain-policy>
<allow-access-from domain="*" />
</cross-domain-policy>
```

Praktik ini cocok untuk server publik, tetapi tidak boleh digunakan untuk situs yang berlokasi di belakang firewall karena dapat mengizinkan akses ke area yang dilindungi. Seharusnya tidak digunakan untuk situs yang memerlukan otentikasi dalam bentuk kata sandi atau cookie. Situs yang menggunakan praktik umum otentikasi berdasarkan cookie untuk mengakses data pribadi atau khusus pengguna harus sangat berhati-hati saat menggunakan file kebijakan lintas domain.

- Dampak dari kerentanan ini
  Menggunakan file kebijakan lintas domain yang tidak aman dapat membuat situs Anda terkena berbagai serangan.

- Cara memperbaiki kerentanan ini
  Hati-hati mengevaluasi situs mana yang akan diizinkan untuk melakukan panggilan lintas domain. Pertimbangkan topologi jaringan dan mekanisme otentikasi apa pun yang akan dipengaruhi oleh konfigurasi atau implementasi kebijakan lintas domain.

- Deskripsi kerentanan Email address found
  Satu atau lebih alamat email telah ditemukan di halaman ini. Mayoritas spam berasal dari alamat email yang dipanen dari internet. Spam-bot (juga dikenal sebagai pemanen email dan ekstraktor email) adalah program yang menjelajahi internet mencari alamat email di situs web apa pun yang mereka temui. Program Spambot mencari string seperti myname@mydomain.com dan kemudian mencatat semua alamat yang ditemukan

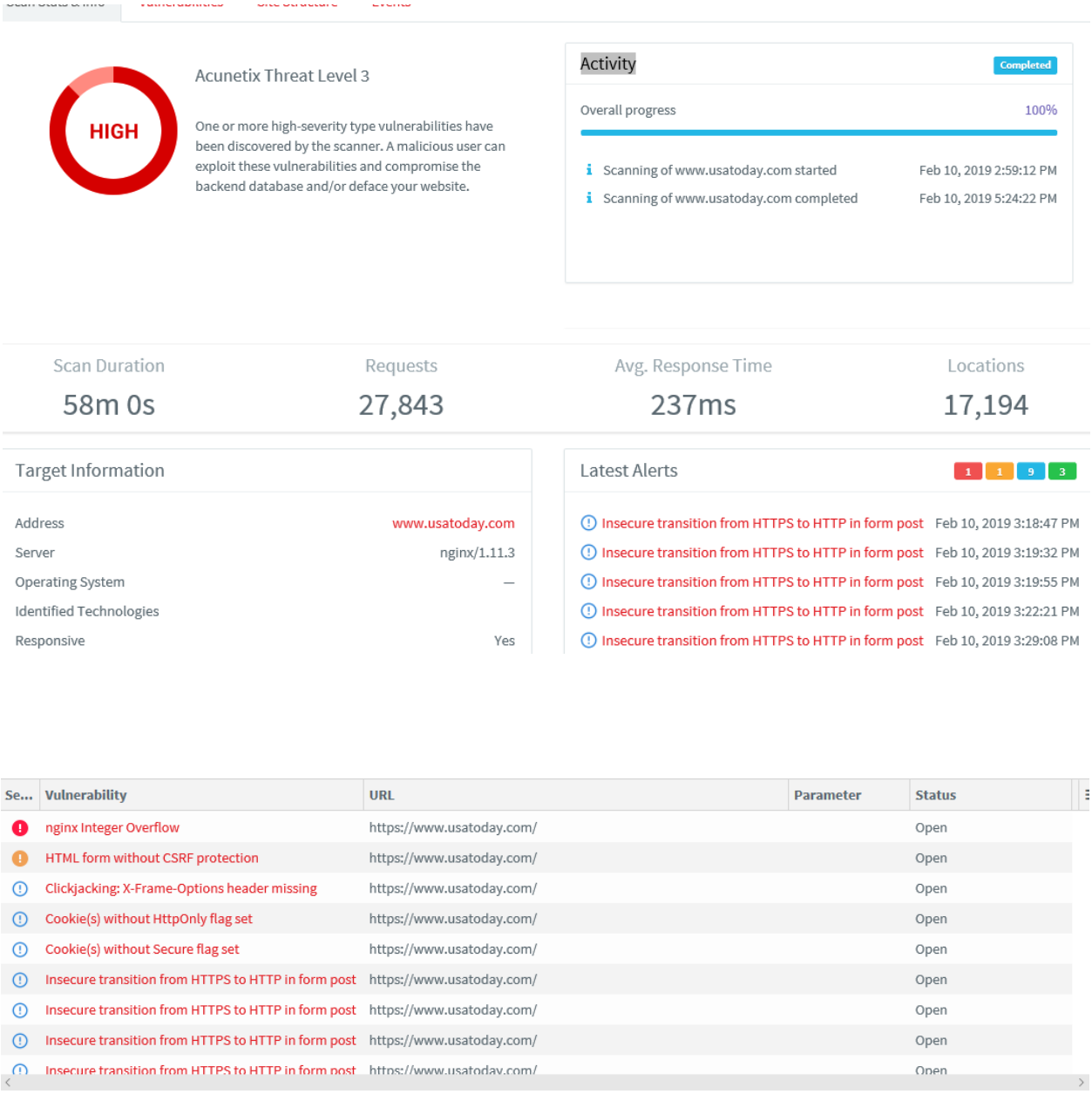
- Dampak dari kerentanan ini

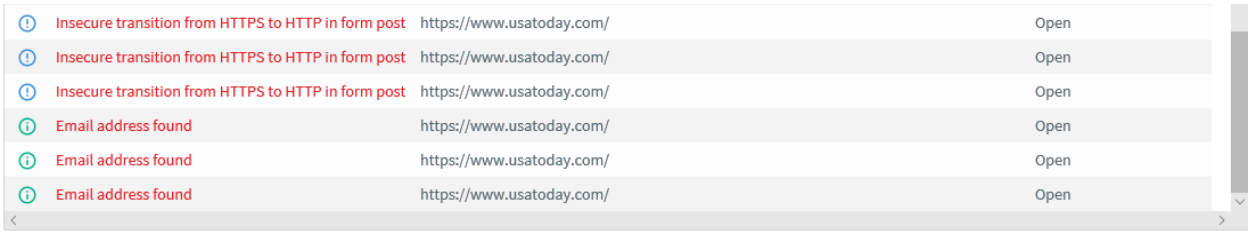
  Alamat email yang diposkan di situs Web dapat menarik spam.

- Cara memperbaiki kerentanan ini

  Periksa referensi untuk detail tentang cara mengatasi masalah ini

3. Berikut adalah Vulnerability dalam website www.usatoday.com menggunakan Acunetix:





Pada website www.usatoday.com kerentanan atau vulnerability terletak pada **High Risk Alert Level 3** yaitu Kerentanan dikategorikan sebagai yang paling berbahaya, yang menempatkan target scan pada risiko maksimum untuk hacking dan pencurian data.

Pada 2 website sebelumnya telah dijelaskan tentang kelemahan atau kerentanan seperti clickjacking,HTML Form without CSRF protection,cookie(s)without HttpOnly flag set ,kerentanan itu juga terdapat dalam website www.usatoday.com . namun website www.usatoday.com memiliki kelemahan yang lain yaitu Nginx Integer Overflow berikut deskripsi kelemahannya :

- Deskripsi kelemahan :

  Berpotensi mengakibatkan kebocoran informasi sensitif (CVE-2017-7529). Saat menggunakan nginx dengan modul standar ini memungkinkan penyerang untuk mendapatkan header file cache jika respons dikembalikan dari cache. Dalam beberapa konfigurasi, header file cache mungkin berisi alamat IP server backend atau informasi sensitif lainnya. Selain itu, dengan modul pihak ke-3, sangat mungkin bahwa masalah tersebut dapat mengarah pada penolakan layanan atau pengungkapan memori proses pekerja.

- Dampak kelemahan

  Keterbukaan Informasi, Penolakan Layanan

- Cara memperbaiki kerentanan ini

  Tingkatkan nginx ke versi terbaru atau terapkan tambalan yang disediakan oleh vendor tersebut