

Challenge


3 Solves

×

Tranqsite 496

Sebuah web terkena serangan jitu heker mematikan. Temukan *secret key* yang digunakan oleh penyerang ketika melakukan autentikasi pada web target.

Flag: LKSIBER30{the_secret_key_here}

 traffic.pcapng

Flag

Submit

Diberikan file pcap dan diperintahkan untuk mencari secret key yang tersembunyi di file pcap tersebut. Ketika saya mendownload file pcap tersebut bisa dibilang filenya memiliki ukuran yang cukup besar jadi kecurigaan saya langsung mengarah kalau pcap ini mengandung file. Langsung saya Export File yang berada di dalam pcap tersebut.

File bisa didownload di sini

https://drive.google.com/file/d/1URO-mIniEvM4sP3KuzKyQIOqRHfL3f5_/view?usp=sharing

Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
781	www.mail4india.com	image/vnd.microsoft.icon	1406 bytes	favicon.ico
792	storage.googleapis.com	application/octet-stream	3792 bytes	371c0e56df0cec70a5174e172e1732d7d5dc1
841	www.mail4india.com	text/html	12 kB	login.php
850	www.mail4india.com	image/vnd.microsoft.icon	1406 bytes	favicon.ico
1039	r2---sn-2b5njvh-jb3e.gvt1.com	application/octet-stream	7399 bytes	GoogleUpdateSetup.exe?cms_redirect=yes
1066	r2---sn-2b5njvh-jb3e.gvt1.com	application/octet-stream	10 kB	GoogleUpdateSetup.exe?cms_redirect=yes
1092	r2---sn-2b5njvh-jb3e.gvt1.com	application/octet-stream	10 kB	GoogleUpdateSetup.exe?cms_redirect=yes
1146	r2---sn-2b5njvh-jb3e.gvt1.com	application/octet-stream	9814 bytes	GoogleUpdateSetup.exe?cms_redirect=yes
1203	r2---sn-2b5njvh-jb3e.gvt1.com	application/octet-stream	21 kB	GoogleUpdateSetup.exe?cms_redirect=yes
1283	r2---sn-2b5njvh-jb3e.gvt1.com	application/octet-stream	44 kB	GoogleUpdateSetup.exe?cms_redirect=yes
1366	r2---sn-2b5njvh-jb3e.gvt1.com	application/octet-stream	60 kB	GoogleUpdateSetup.exe?cms_redirect=yes
1577	r2---sn-2b5njvh-jb3e.gvt1.com	application/octet-stream	184 kB	GoogleUpdateSetup.exe?cms_redirect=yes
1964	r2---sn-2b5njvh-jb3e.gvt1.com	application/octet-stream	366 kB	GoogleUpdateSetup.exe?cms_redirect=yes
2736	r2---sn-2b5njvh-jb3e.gvt1.com	application/octet-stream	682 kB	GoogleUpdateSetup.exe?cms_redirect=yes
2795	redirector.gvt1.com	text/html	468 bytes	AJ_YRYeZaj9aEBuPMINveAA
2809	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	6168 bytes	AJ_YRYeZaj9aEBuPMINveAA?cms_redirect=
2854	redirector.gvt1.com	text/html	484 bytes	AJ_YRYeZaj9aEBuPMINveAA
2878	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	10 kB	AJ_YRYeZaj9aEBuPMINveAA?cms_redirect=
2919	redirector.gvt1.com	text/html	468 bytes	AJ_YRYeZaj9aEBuPMINveAA
2927	r2---sn-2b5njvh-jb3l.gvt1.com	application/octet-stream	3418 bytes	AJ_YRYeZaj9aEBuPMINveAA?cms_redirect=
3062	www.mail4india.com	application/x-www-form-urlencoded	112 bytes	redirect.php
3072	ocsp.digicert.com	application/ocsp-response	471 bytes	MFEwTzBNMEswSTAJBgUrDgMCGGUABBTf
3373	www.mail4india.com	text/html	2802 bytes	redirect.php
3401	www.mail4india.com	text/css	5162 bytes	snm.css

Save Save All Preview Close Help

Melihat dari nama file file yang diatas ada beberapa file yang mencurigakan dari login.php dll. Sampai ke redirect.php ketika membuka file tersebut ada secretkey didalamnya

```
js_autodetect_results=1&just_logged_in=1&login_username=user%40user.com&secretkey=S0tTSTIwMT17Q11CM3JfQUQhISEhfQ
```

Flag: LKSIBER20{S0tTSTIwMT17Q11CM3JfQUQhISEhfQ}