

# CYBR/CITA 352 Week 1 Lab

*Find a Google Hacking Database Web site.*

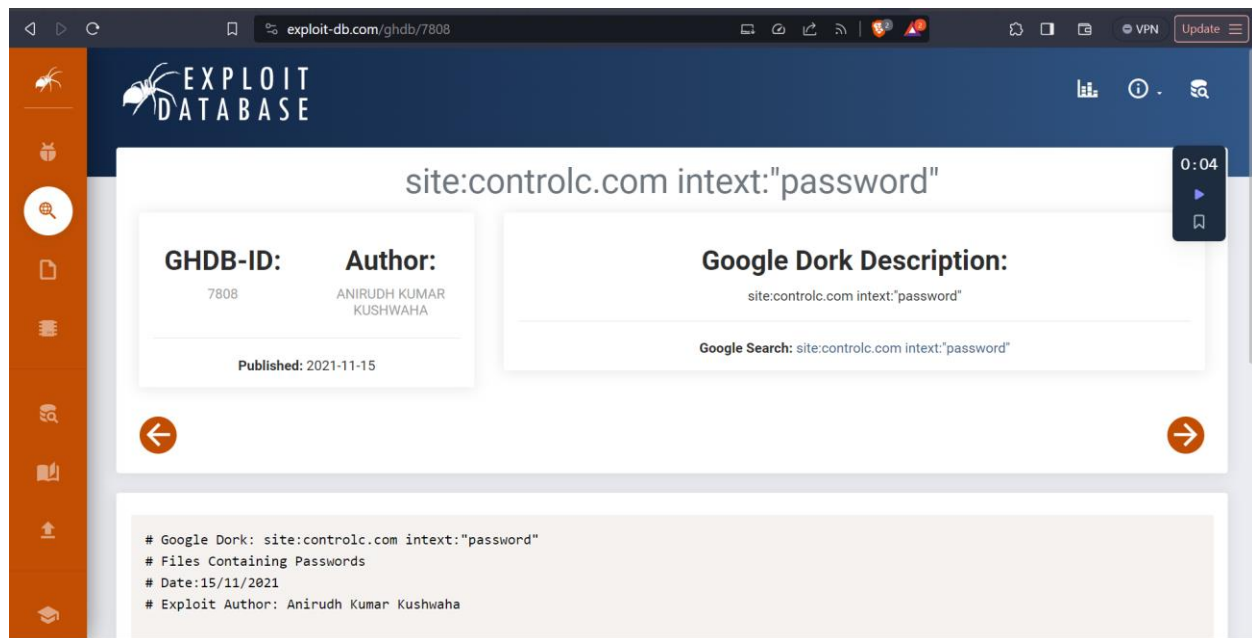
The website I found was called Exploit Database: <https://www.exploit-db.com/google-hacking-database>

The screenshot shows the 'Google Hacking Database' page on the Exploit Database website. The page has a dark blue header with the 'EXPLOIT DATABASE' logo and a sidebar with various icons. The main content area is white and contains a table of search results. The table has four columns: 'Date Added', 'Dork', 'Category', and 'Author'. There are also buttons for 'Filters', 'Reset All', and a 'Quick Search' input field. The table lists several search results, including one for 'OpenVpn Status Monitor' and another for 'Froxl Server Management Panel - Installation'.

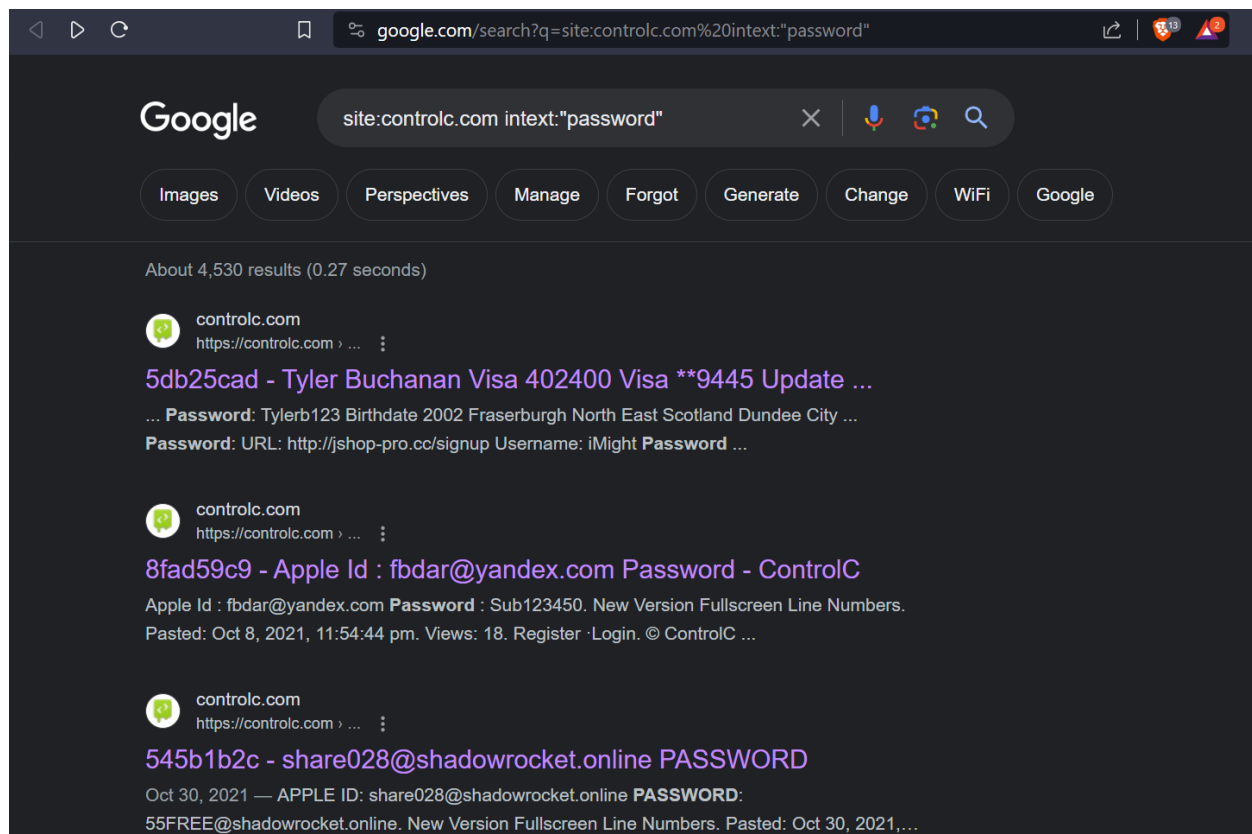
Date Added	Dork	Category	Author
2024-01-29	intitle:"OpenVpn Status Monitor"	Vulnerable Servers	Sabeen Technology
2024-01-23	(site:jsonformatter.org   site:codebeautify.org) & (intext:aws   intext:bucket   intext:password   intext:secret   intext:username)	Files Containing Juicy Info	letmewin cyber
2024-01-23	filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS	Files Containing Juicy Info	web work
2024-01-23	inurl:install.php intitle:"Froxl Server Management Panel - Installation"	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-01-23	intitle:"index of" database.properties	Sensitive Directories	Odela Rohith
2024-01-23	Apache Struts 2.x Path Traversal Vulnerability (CVE-2023-50164) Detection Dork	Vulnerable Servers	Parth Jamodkar
2023-12-21	inurl:"?url=http"	Files Containing Juicy Info	Jeel Patel
2023-12-21	intext:"user" filetype:php intext:"account" inurl:/admin	Files Containing Juicy Info	saurabh kode

The google hacking database anyone can submit searches that can have certain sensitive information.

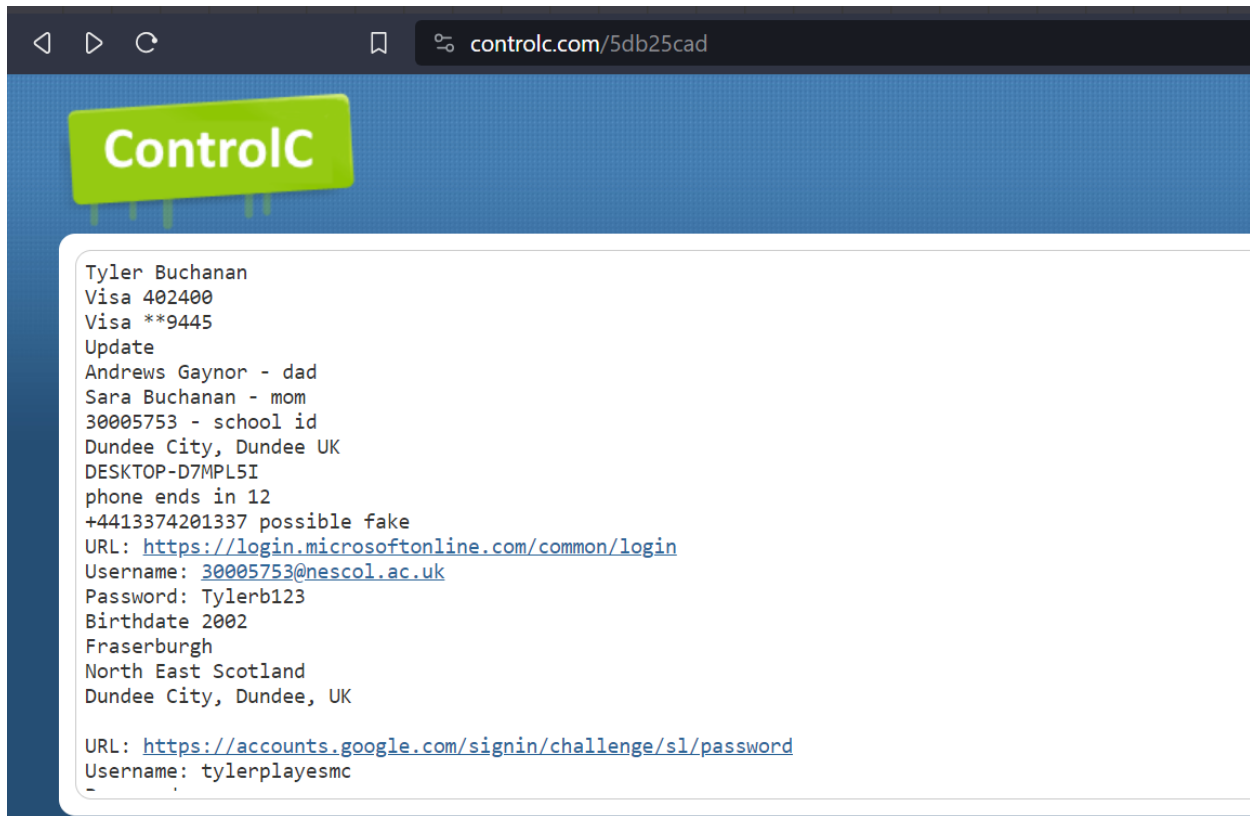
*Use a Google dork in Google hacking to find a password publicly accessible on a Web page.*

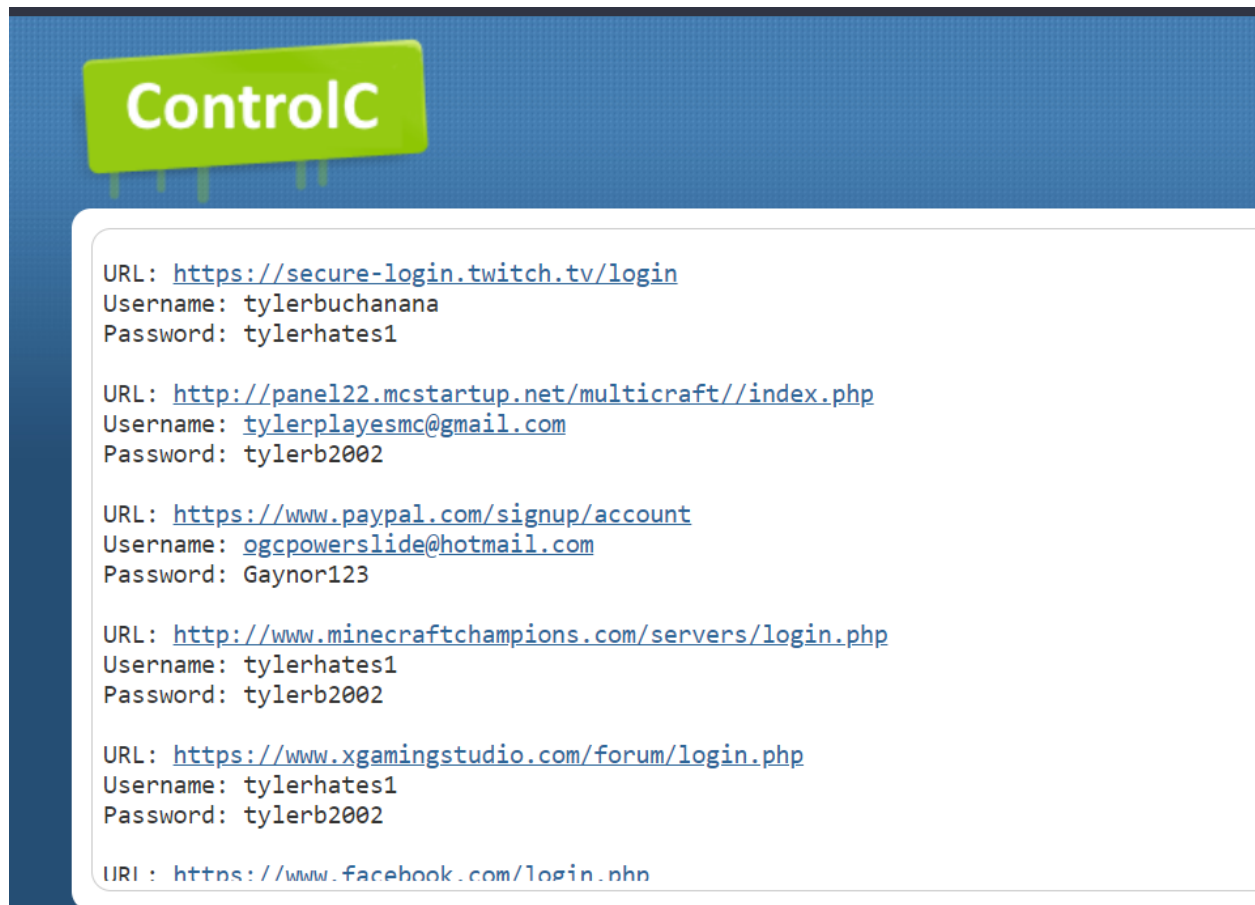


From the database, I found this Google dork ‘site:controlc.com intext:”password”’. Controlc.com is a website similar to Pastebin.com, where anyone can save text online. The Google dork is searching for pages on controlc.com that have the text “password”.



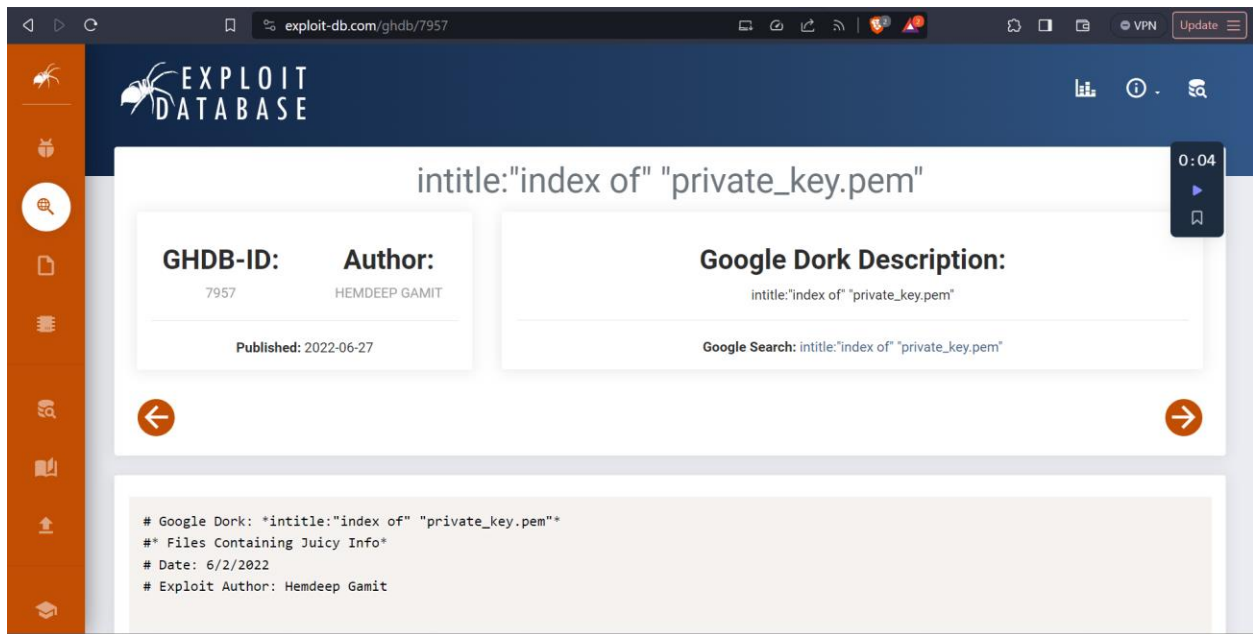
The search came up with a couple of results, but the first search was the most interesting one.



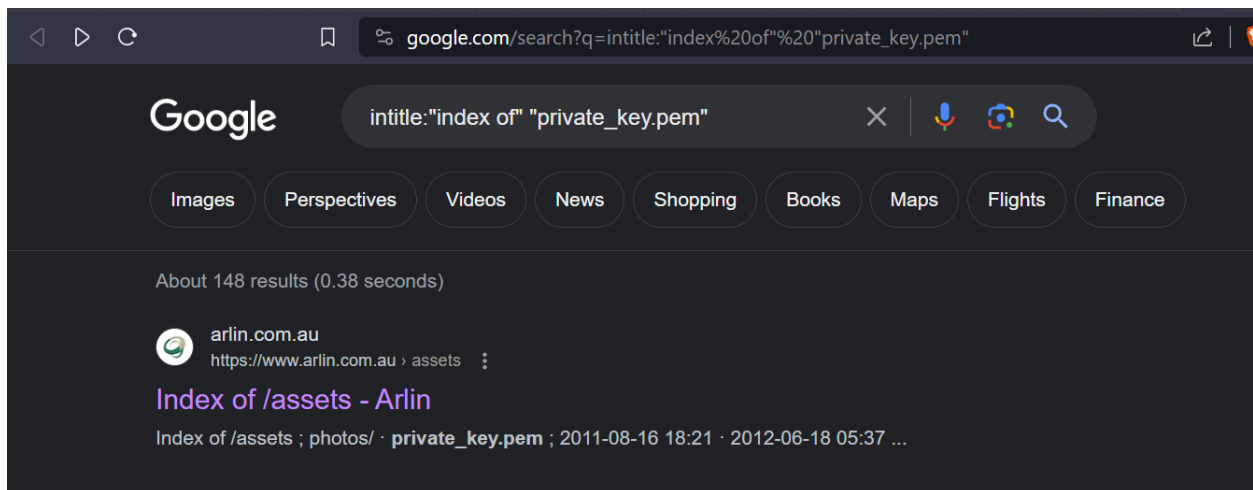


The page saved a lot of sensitive information for a person called Tyler Buchanan, and the rest contained usernames and passwords to many websites. Someone was collecting this person's information for malicious intent, or maybe the owner of this information was saving it himself, but this is unlikely because the beginning of the text gives it a tone that it is a different person.

*Use a Google dork in Google hacking to find a private key (in a container format) publicly accessible on a Web page.*



From the database I found this Google dork: 'intitle:'index of' 'private\_key.pem'.



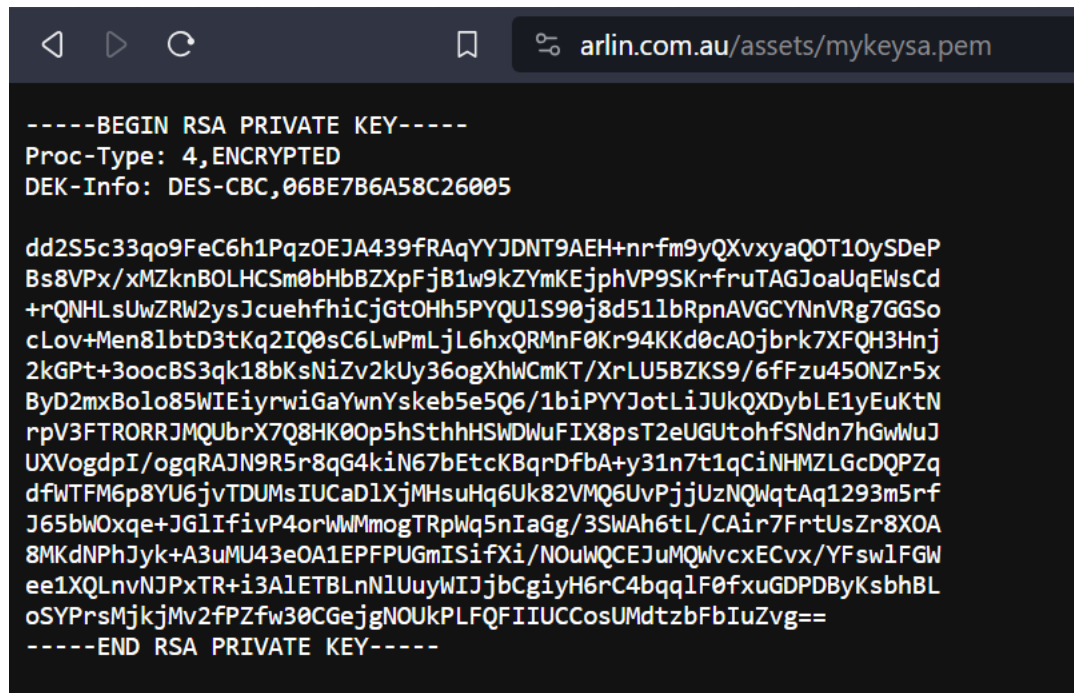


# Index of /assets

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">arlin.swf</a>	2011-12-15 21:24	29K	
<a href="#">ckeditor/</a>	2013-05-29 21:47	-	
<a href="#">ckfinder/</a>	2013-12-22 07:13	-	
<a href="#">css.zip</a>	2015-02-16 16:03	3.3M	
<a href="#">css/</a>	2012-07-22 00:21	-	
<a href="#">data_tables/</a>	2012-06-18 05:43	-	
<a href="#">fancybox/</a>	2011-08-16 18:13	-	
<a href="#">images/</a>	2012-06-18 05:46	-	
<a href="#">js/</a>	2012-07-27 22:32	-	
<a href="#">media/</a>	2012-08-29 00:06	-	
<a href="#">modules/</a>	2011-12-14 00:31	-	
<a href="#">mykeysa.pem</a>	2013-03-15 20:51	958	
<a href="#">photos/</a>	2011-08-16 18:21	-	
<a href="#">private_key.pem</a>	2012-06-18 05:37	1.7K	
<a href="#">public.pem</a>	2013-03-15 20:51	272	
<a href="#">public_key.pem</a>	2011-11-17 19:25	455	
<a href="#">test.php%00.jpg</a>	2022-07-17 15:55	21	
<a href="#">test.php%001.jpg</a>	2022-07-17 15:55	21	
<a href="#">test.php.jpg</a>	2022-07-17 15:57	21	
<a href="#">test.php.png</a>	2022-07-17 15:58	21	
<a href="#">test.php1.png</a>	2022-07-17 15:58	21	
<a href="#">test.php2.png</a>	2022-07-17 15:58	21	

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,C62AED1F6D8D804B

mnkdGeykwLyhJrMhCRU5aEYkvR4s/2/cqzaCfF47svwBHZZmq6J8cLfbUubMOqqp
rsoYmkF4I/kj10wb7dMqXL15fiFb/3Etet4H4TPmdB9ZQPFBBwpgOA/sRVPx9eJi
JwByl6xL+x7Fh0hd+QCQSR9ehHchZVrg1ra50dUdWuhAmshGYNxMpleYyV1Xmu9m
RSbUzP1bRD50S5eEo1YgRL6JQwsYapkKFocGXqcMbJAI12uhi9N9Ujl0Fqi4yJV5
XX150wjXRRIAM73muHHNwIN5ic57u+tK6AprNdTwhpbVtWJz39orndZn2w04q8Vw
fp56847a9d3PFbAzqowwPf/erOPjTcrGKjga07cifQTDoQKWYIfcZkeepKM//iK
3QMn1Vdp2SJsSVi9D4rsAioqWue020vRXxqW/DJAPKvuzW0LcU3rae/qhWmOWqW6
W9NV9eAyzd1EwZOLR2azCQZMSNh5cKMCPrHdJ6A09z5U9uW36GiXba/HgKhKMPH9
yWjEfM0TuN28tbOUmwUvGvMdttdR+akBOHRt+aAb6PHNuEbgs1zCR5qgc5gviGN
s1SOW+LnnZD+mSI010/xm6C+jSYFSkQ4AA4cCQ6QEbQa68a2tPL8TIJ80lr4h6cT
vuzoybTpJfShZ8S122XhmFNj8/DXWejevCWs7M7ADeg6r4Mpwc2AlaylWtZfdfpk
ElqGrSuymMdF9gqDYN5Wwnsm2F9yE7ohdwLEz6gwxeaTh8p10gXlVI89wyi+tOUp
mS2iLyYaM5F81RzvIpLzSb0/FeKEoNneJJIAXXRbz3ugrS9FKNLH8cBWy/rW51Rp
qjrtFm1n/nz86fXdH4hfRExdkYP3zBP2kEC19K+ZVX001rB57pO/C+B35k7G0Ae/
2tDvE+OoRn+4JHSAixNI8Wgt2uUbRe6jmS9SnGetgLrTIsCHH8614M28K+rDQTAU
PR1+CK/MuSWR3froROgVlEFRHTE6FAEeQuD3p+z01QNhWhwMWr0Wi5rwVs5HeA7G
4qDpYw2LzWuXIDkLkwLo1gBXgYQeL5IfIyb0wmJIgpGSsV/EM43c3JmDhee/uf+M
tou514LJVWvYvxEVKA6MEZ9sbFvVwHUDEE7EX1cqDHZvcCWRBG6I4YulLsEPE7pj
xmszQ8ur8v3iA/jQkHIPSL6oAuERcSAs8IANm1zZAKgpeshmjWlngxNNerTF77Rc
thCgpK92Z5SV7E+qXs01+1CyAKAYIkhuyacrYycVJx4s9ckn6i+M/TpAFiAPjBHx
NZZ0fxFmawPuef9eXhGH7ASFvVtXTKSYp2ug4jk5RugLkN11cRdLYbQprptWLkSZ
exSClK/fCdIEKxtRjuUaQp1rb4xZumDQu3Rg15F33BqXtHSUS9DiPtN1WKaC/wnv
a71yXYkZpT7t9BHOPMh18vxONlyaBi2j9bk2NW4rvZ/P6PUGAgjUxRz1wRvGgzVO
2Bngfasi94GYBlgzbwW0crChc2qsnCD14r4ZW0Q5gyMx6fLJdaf1bmbpbqmW5ZkrE
M058mI62d+TfwjXiW6g/KIscLtDXIVEk8vaM/fXz+2x1A8iwUZqVms0Cstn7aPrj
-----END RSA PRIVATE KEY-----
```

A screenshot of a web browser window. The address bar shows the URL 'arlin.com.au/assets/mykeysa.pem'. The page content displays a private key in PEM format. It starts with '-----BEGIN RSA PRIVATE KEY-----', followed by 'Proc-Type: 4, ENCRYPTED' and 'DEK-Info: DES-CBC,06BE7B6A58C26005'. The main body of the key is a long string of base64-encoded characters. It ends with '-----END RSA PRIVATE KEY-----'.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-CBC,06BE7B6A58C26005

dd2S5c33qo9FeC6h1PqzOEJA439fRAqYYJDNT9AEH+nr-fm9yQXvxyaQ0T10ySDeP
Bs8VPx/xMZknBOLHCsm0bHbBZXpFjB1w9kZYMKEjphVP9SKr-fruTAGJoaUqEwsCd
+rQNHLSUwZRW2ysJcuehfhiCjGtOHh5PYQULS90j8d51lbRpnAVGCYNnVRg7GGSo
cLov+Men81btD3tKq2IQ0sC6LwPmLjL6hxQRMnF0Kr94KKd0cAOjbrk7XFQH3Hnj
2kGPt+3oocBS3qk18bKsNiZv2kUy36ogXhWcmKT/XrLU5BZKS9/6fFzu450NZr5x
ByD2mxBo1o85WIEiyrwiGaYwnYskeb5e5Q6/1biPYyJotLiJUKQXDyblE1yEuKtN
rpV3FTRORRJMQUbrX7Q8HK0Op5hSthhHSDWuFiX8psT2eUGUtohfSNdn7hGwWuJ
UXVogdpI/ogqRAJN9R5r8qG4kiN67bEtcKBqrDfbA+y31n7t1qCiNHMZLGcDQPZq
dfWTFM6p8YU6jvTDUMsIUCaDlXjMHsuHq6Uk82VMQ6UvPjjUzNQWqtAq1293m5rf
J65bWOxqe+JG1IfivP4orWwMmogTRpwq5nIaGg/3SWAh6tL/CAir7FrtUsZr8X0A
8MKdNPhJyk+A3uMU43e0A1EPFPUGmISifXi/NOuWQCEJuMQWvcxECvx/YFswlFGW
ee1XQLnvNJPxTR+i3A1ETBLnN1UuyWIjCbCgiyH6rC4bqq1F0fxuGDPDBYKsbhBL
oSYPPrsMjkjMv2fPZfw30CGejgNOUkPLFQFIUCCosUMdtzbFbIuZvg==
-----END RSA PRIVATE KEY-----
```

The search led me to index of arlin.com.au, which is an Australian hardware store. It contained two private keys, “private\_key.pem” and “mykeysa.pem”.