Request for Service

RFS No : 2015/A190 Date: 13 Sept 2015

Client Name and address:

ASCL, Pune, India.

Client's authorised representative:

Name: Mr R Nagpal	Email: rn@asianlaws.org	Phone: +91-45-868756	Fax: +91-45-868758

Background of the case:

CS is a very popular online gaming site. Recently a lot of users have complained to the CS support staff that their login credentials have been compromised and their "kills" have been "gifted" to other users.

Details of computer(s), media etc:

CS website can be accessed online at http://www.asianlaws.net/dlp_module.php?course=cci&module=cci_case_study_cs

Have the computer(s), media etc mentioned above been accessed / examined prior to being handed over to me? If yes, give details.

N.A.

Services requested from me

Investigate and prepare a detailed report that answers the following questions: 1. What are the vulnerabilities in the CS site that have been misused by hackers to compromise user credentials? 2. How can the CS tech team obtain evidence to track the hackers?

For internal ASCL use only (Pls leave blank)

Case recd on 13 September 2015	Case recd by : Ravi K Shakya	Referred by: Mr R Nagpal

Tax Priority 1 2 3 4 5 6 7 8 9 10
Porn
Financial
Cyber

Investigation report:

1) I signed up as a new user with name: A36140902223138, password : 5439094643349327 and email_address: ravi.shakya@gmail.com at the site http://www.asianlaws.net/cases/cs/signup.php

2) After clicking 'Sign-up' button, an verification email was sent to the provided email address.

3) I clicked on the verification link sent via the verification email.

4) After which, my account was verified and I was able to login using the login credentials created by the system.

5) After logging-in, I explored the system for sometime. I noticed that 'Gift A Kill' section was disabled.

6) I clicked on 'ME' button and noticed it displayed my name, username, email address, number of kills I had. It also contained sections to update email address and password.

7) I checked the HTML source of 'ME' page (http://www.asianlaws.net/cases/cs/success.php) using browser's 'View Source' function. It was like in figure 1 below.

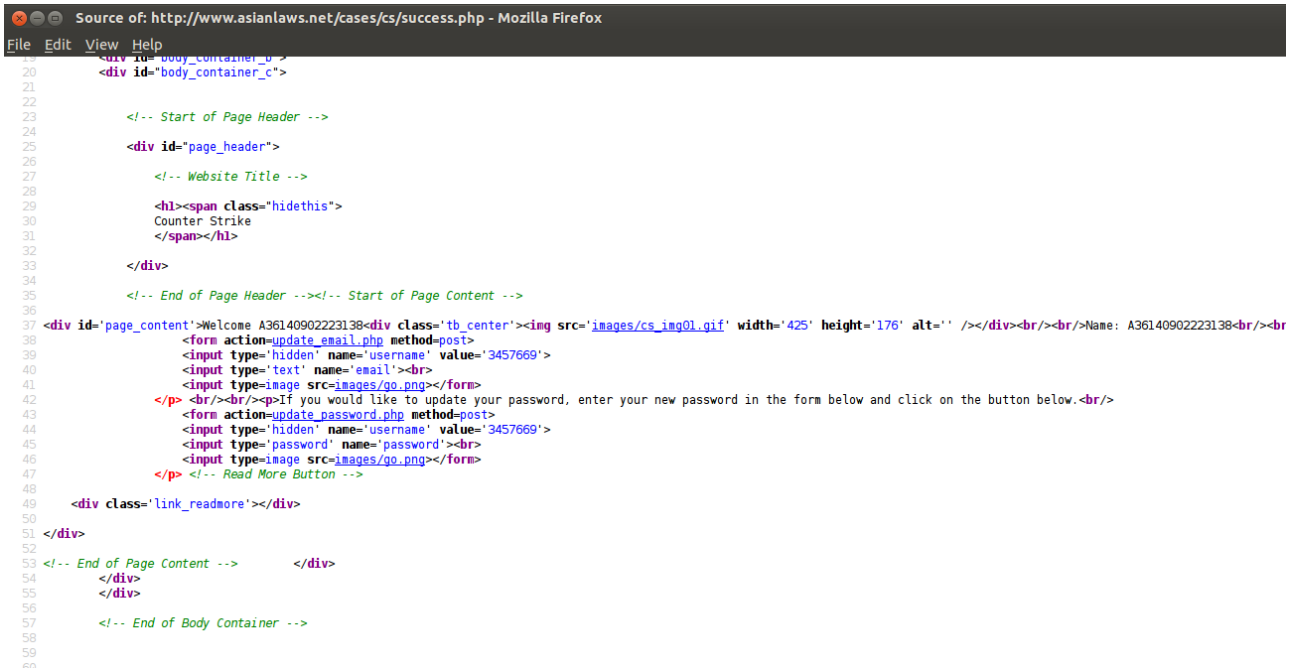

Figure 1. HTML Source code of http://www.asianlaws.net/cases/cs/success.php

8) To change password, POST request with parameters : username and password was made to update_password.php file.

9) I tried to change password of user: 3457669 (username consisted of number) by submitting a POST request with username : 3457669 and password : kamalpasha via a REST client like POSTMAN. Please refer to the attached screenshot in Figure 2.
The request was successfully accepted by update_password.php script and it responded with HTTP status code 200. I checked by logging-out and then logging-in using the old password

and the site did not allow me in. I logged in with the new password and the site allowed me in. This proved that update_password.php can be used by anyone with random username to change the password to whatever the attacker desired.
Hence I concluded that this loophole of update_password.php has been exploited by the hackers to change passwords of the users after which they were able to login and gift the 'kills' of the user to others.

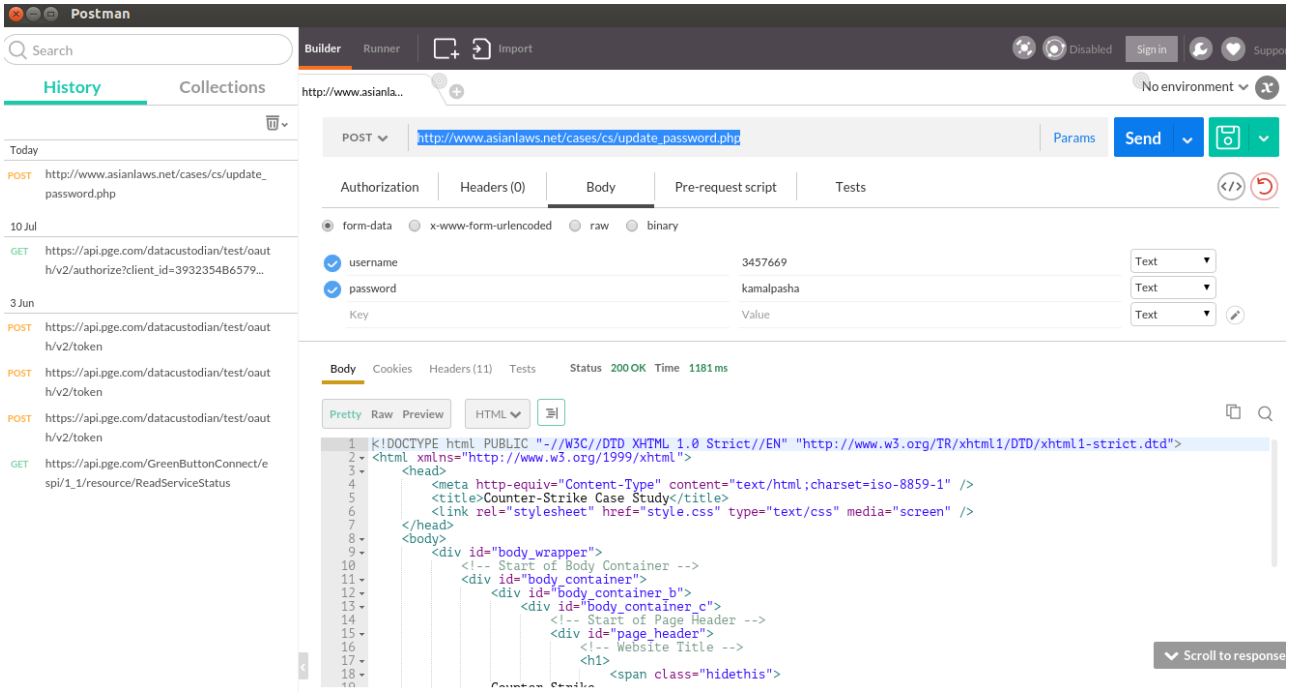

Fig. 2 POST request to update_password.php using REST client like POSTMAN

Approach to be followed by CS Tech team to track hackers:

1) Firstly I tried to see the behavior of password change feature in 'ME' section of CS website. When a password is successfully changed via website, log entry of type shown in Figure 3 is generated.

2) When I change the password of the same user using POST request submission using POSTMAN (as in Figure 2), no log entry is generated in 'LOG' section of CS Website. This provided additional challenge in obtaining evidence to nab the hackers.

3) Now we need to obtain and investigate copies of access.log files of the web server used to host CS website to check for requests of type http://www.asianlaws.net/cases/cs/update_password.php (for the compromised user accounts) and find the IP addresses and timestamps of accesses.

4) Once the IP addresses are obtained, WHOIS service can be used to zero-in on the ISP associated with the hackers. With the help of ISP, we can find out the actual contact address/numbers of the intruders. Then we can use conventional investigation techniques to nab the hackers if needed.

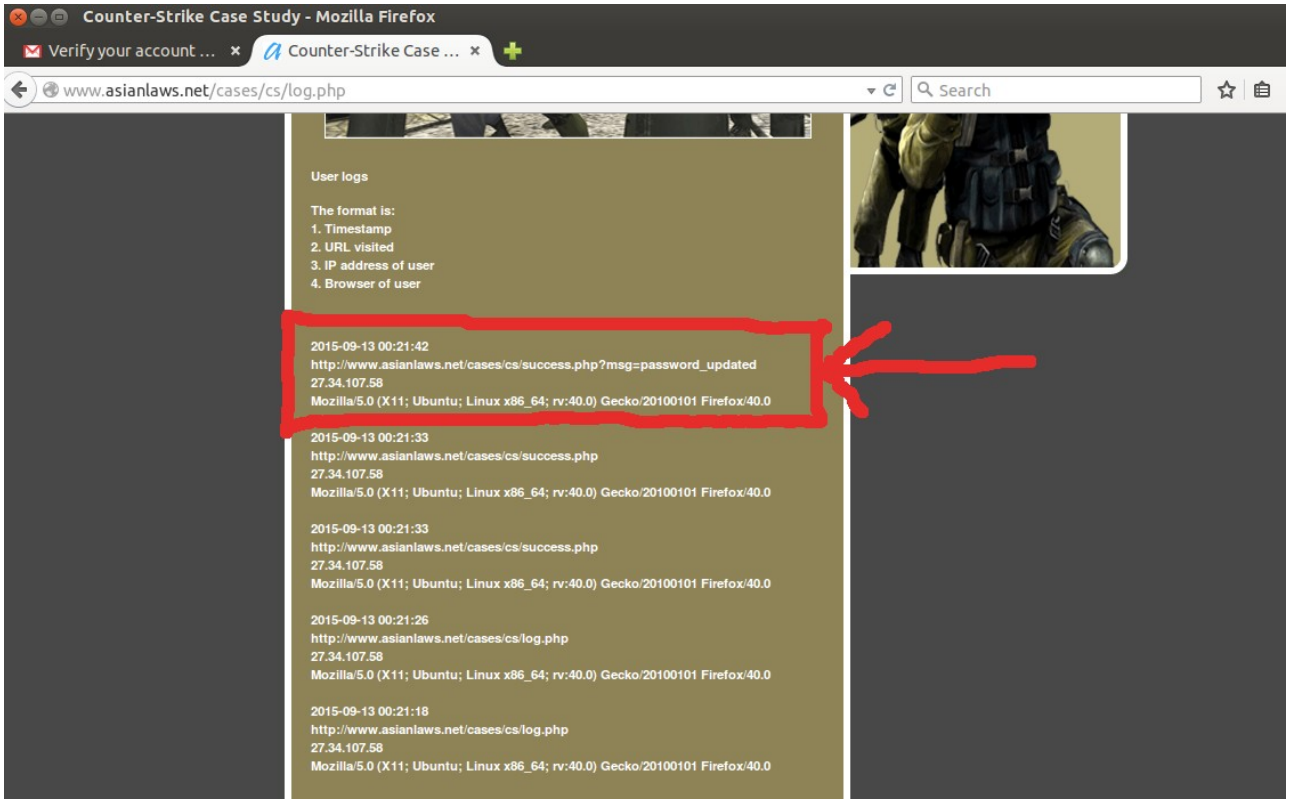

Figure 3 . log entry of password change via CS website.