

# *Обеспечение информационной безопасности*



С.С. Кочетов  
ФГУП ЦНИИС

# Портал виртуальная лаборатория



VIRTUAL LABORATORY

[Главная](#) [Узнать больше](#) [Новости](#) [Наши сервисы](#) **[Обучающие видео](#)** [Отзывы](#) [Партнеры](#) [Контакты](#)

## Mutillidae

Mutillidae  
Spirent test center

### Bypass Authentication using SQL Injection



on=com\_content&view=article&id=22&Itemid=129

### Авторизация

Запомнить меня

**Войти**

[Регистрация](#)  
[Забыли логин?](#)  
[Забыли пароль?](#)

### Схема

#### Оборудование



Spirent TestCenter SPT-N4U-220  
IXIA 400T и IxVM  
Формирователь IP-соединений  
«АМУЛЕТ»  
Формирователь телефонных

### Сопутствующие сайты

[Официальный сайт ФГУП  
ЦНИИС](#)  
[База знаний  
Mutillidae](#)



# Open Web Application Security Project (OWASP)

- 
- › A1 Внедрение кода (SQL Injection)
  - › A2 Некорректная аутентификация и управление сессией
  - › A3 Межсайтовый скриптинг (XSS)
  - › A4 Небезопасные прямые ссылки на объекты
  - › A5 Небезопасная конфигурация
  - › A6 Утечка чувствительных данных
  - › A7 Отсутствие контроля доступа к функциональному уровню
  - › A8 Подделка межсайтовых запросов (CSRF)
  - › A9 Использование компонентов с известными уязвимостями
  - › A10 Невалидированные редиректы
- 

# Mail.ru Group



› [Почта Mail.Ru](#)

› e.mail.ru

› touch.mail.ru

› m.mail.ru

› [Облако Mail.Ru](#)

› cloud.mail.ru

› [Календарь Mail.Ru](#)

› calendar.mail.ru

› [Mail.Ru для бизнеса](#)

› biz.mail.ru

› [Авторизационный центр Mail.Ru](#)

› auth.mail.ru

› swa.mail.ru

А также в мобильных приложениях Mail.Ru Group для iOS и Android, которые так или иначе работают с личной информацией пользователей:

› [Почта Mail.Ru для iOS](#)

› [Почта Mail.Ru для Android](#)

› [Календарь Mail.Ru для Android](#)


› [Облако Mail.Ru для iOS](#)

› [Облако Mail.Ru для Android](#)



# Mail.ru Group



- › Cross-Site Scripting
  - › SQL Injection
  - › Remote Code Execution
  - › Cross-Site Request Forgery
  - › Directory Traversal
  - › Information Disclosure
  - › Content Spoofing
- 

# Интерфейс веб-приложения
















## OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.10    Security Level: 0 (Hosed)    Hints: Disabled (0 - I try harder)    Not Logged In

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Toggle Security](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#) | [Hide Popup Hints](#) | [Enforce SSL](#)

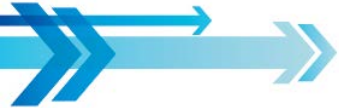
### Mutillidae: Deliberately Vulnerable Web Pen-Testing Application


 [Like Mutillidae? Check out how to help](#)

 <a href="#">What Should I Do?</a>	 <a href="#">Video Tutorials</a>
 <a href="#">Help Me!</a>	 <a href="#">Listing of vulnerabilities</a>
 <a href="#">Bug Tracker</a>	 <a href="#">Bug Report Email Address</a>
 <a href="#">What's New? Click Here</a>	 <a href="#">Release Announcements</a>
 <a href="#">PHP MyAdmin Console</a>	 <a href="#">Feature Requests</a>
	



# Задания на Mutillidae





**Version: 2.0.7**


[Home](#)

**Core Controls** ▾

**OWASP Top 10 2010**

**Others**

**Resources**





**Site hacked...err...quality-  
with Samurai WTF, Back  
Firefox, Paros, Netc**

- A1 - Injection (SQL and Command) ▸
- A2 - Cross Site Scripting (XSS) ▸
- A3 - Broken Authentication and Session Management ▸
- A4 - Insecure Direct Object References ▸
- A5 - Cross Site Request Forgery (CSRF) ▸
- A6 - Security Misconfiguration ▸
- A7 - Insecure Cryptographic Storage ▸
- A8 - Failure to Restrict URL Access ▸
- A9 - Insufficient Transport Layer Protection ▸
- A10 - Unvalidated Redirects and Forwards ▸

- Login
- User Info
- DNS Lookup
- Register
- HTTP Response Splitting (Hint: Very Difficult)
- Text File Viewer
- ... errors. They are not compatible with location C:\xampp\php\php.ini) and cl
- ... page to read about a vulnerability, ti
- ... modes: secure and insecure (defau
- ... attempts to protect the pages with sen
- ... the user to see how the defense worl



# Open Web Application Security Project (OWASP)

- 
- › A1 Внедрение кода (SQL Injection)
  - › A2 Некорректная аутентификация и управление сессией
  - › A3 Межсайтовый скриптинг (XSS)
  - › A4 небезопасные прямые ссылки на объекты
  - › A5 небезопасная конфигурация
  - › A6 утечка чувствительных данных
  - › A7 Отсутствие контроля доступа к функциональному уровню
  - › A8 Подделка межсайтовых запросов (CSRF)
  - › A9 Использование компонентов с известными уязвимостями
  - › A10 невалидированные редиректы
- 



# Образовательная функция



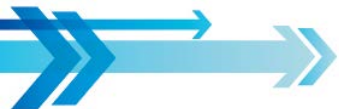
```
SELECT * FROM accounts WHERE username='<username submitted>'  
AND password='<password submitted>'
```

```
SELECT * FROM accounts WHERE username=' or 'r' = 'r' -- ' AND password='anything'
```

```
SELECT * FROM accounts
```



# Образовательная функция



## Методические рекомендации

Методические указания

Технические условия

### Схема

### Оборудование

Spirent TestCenter SPT-N4U-220  
IXIA 400T и IxVM  
Формирователь IP-соединений  
«АМУЛЕТ»  
Формирователь телефонных  
соединений ПРИЗМА  
Универсальный модульный  
анализатор STT-7000  
Анализатор протоколов ОКCN№7  
и EDSS A8619  
wiSLA и wiProbe

### Сопутствующие сайты

Официальный сайт ФГУП  
ЦНИИС  
База знаний  
Mutillidae

Методические  
рекомендации



# Регистрация на портале



[Главная](#) [Узнать больше](#) [Новости](#) [Наши сервисы](#) [Обучающие видео](#) [Отзывы](#) [Партнеры](#)

**Ошибка**  
Для просмотра этой информации необходимо пройти авторизацию


Некоторые материалы, требуют более Высокого уровня доступа, поэтому пользователю предлагается пройти регистрацию на портале, которая дает больше возможностей для взаимодействия с материалами на портале

## Авторизация





Запомнить меня

[Регистрация](#) 

[Забыли логин?](#)

[Забыли пароль?](#)



# Регистрация на портале



## Регистрация пользователя

---

\* Обязательное поле

Имя \*

Логин \*

Пароль \*


Повтор пароля \*

Адрес электронной  
почты \*

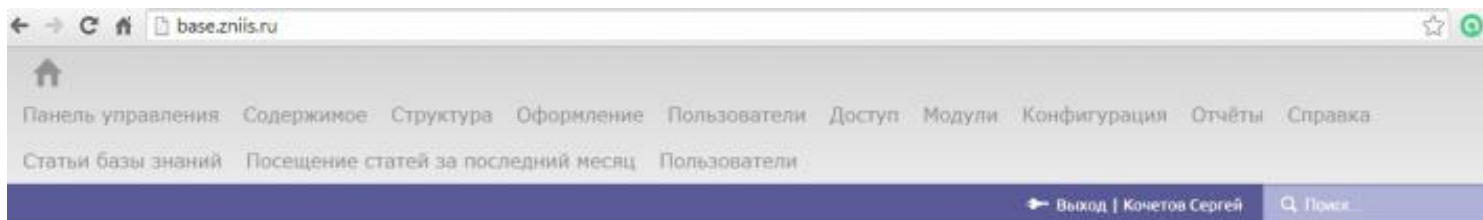
Подтверждение адреса  
электронной почты: \*

Регистрация

Отмена



# База знаний



ПРОЕКТЫ

КОНТРАКТЫ

МОЙ ЦНИИС



Нет добавленных статей.

## Последние изменения

Статей на страницу 10 ▾

### Мосгортелеком

Автор: Скоков Олег

Обновлено: 19 февраля 2014 года, 13:24

### Материалы

Автор: Скоков Олег

Обновлено: 6 февраля 2014 года, 18:19

### Отчет по НИР Разработка программы стандартизации

Автор: Коноплина Елена

Обновлено: 19 декабря 2013 года, 17:05

### Методики

Автор: Скоков Олег

Обновлено: 19 декабря 2013 года, 17:04


Мпр Администрирование

Отчет ТЗ Бизнес-процесс



# Структура базы знаний



- Тестирование – формализация и объединение всех возможных данных по тестированию Средств Телекоммуникаций (оборудование, системно-сетевые решения, услуги, сети связи, QoS и т.д.);
  - Публикации – объединение информации о имеющихся научно-технических и общеобразовательных публикациях в области телекоммуникаций;
  - Обучение – объединение информации о обучающих семинарах и курсах в рамках проекта МЦТТ;
  - Реестры – база данных по всем проводимым и проведенным тестированиям.
- 

**СПАСИБО!**