

**BitReverse**

We can see what others can't...

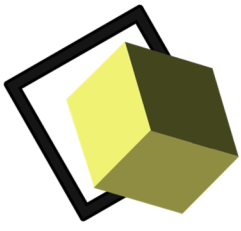
65123  
Ak. Zabolotnogo str. 38  
Odessa, Ukraine

<http://bitreverse.org>

---

Отчёт о выполненном  
автоматическом сканировании  
ресурса

[www.example.com](http://www.example.com)



# BitReverse

We can see what others can't...

65123  
Ak. Zabolotnogo str. 38  
Odessa, Ukraine

<http://bitreverse.org>

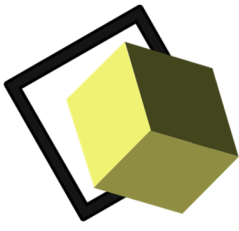
---

Заказчик:

...

Исполнитель:

...

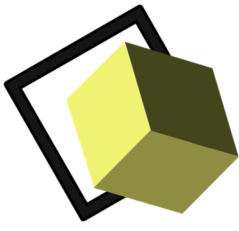


**Тип тестирования:** автоматическое сканирование веб-ресурса.

**Классификация** обнаруженных уязвимостей производилась согласно стандарту OWASP TOP 10:

- A1 Injection;
- A2 Broken Authentication and Session Management;
- A3 Cross-Site Scripting (XSS);
- A4 Insecure Direct Object References;
- A5 Security Misconfiguration;
- A6 Sensitive Data Exposure;
- A7 Missing Function Level Access Control;
- A8 Cross-Site Request Forgery (CSRF);
- A9 Using Components with Known Vulnerabilities;
- A10 Invalidated Redirects and Forwards.

**Уровень уязвимостей:** каждой уязвимости, обнаруженной в процессе проведения аудита, присваивается определенная степень риска. Наиболее критичные уязвимости отмечены красным цветом; уязвимости средней степени риска - желтым; прочие уязвимости, эксплуатация которых не приводит к компрометации ресурса, но может быть использована потенциальным злоумышленником для сбора информации и формирования векторов атак отмечены зеленым.



# BitReverse

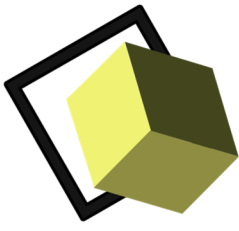
We can see what others can't...

65123  
Ak. Zabolotnogo str. 38  
Odessa, Ukraine

<http://bitreverse.org>

---

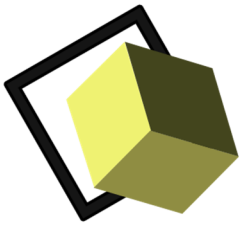
**Модель нарушителя:** внешний нарушитель - лицо, мотивированное, как правило, коммерческим интересом, имеющее возможность доступа к внешнему периметру, не обладающий знаниями об исследуемой ИС, имеющий среднюю квалификацию в вопросах обеспечения сетевой безопасности.



## Обнаруженные уязвимости:

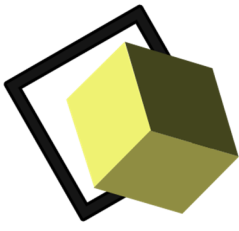
### OWASP A1 SQL injection

- **Вид:** внедрение операторов SQL
- **Тип:** time based blind
- **URL:** <http://www.example.com/enter/?act=login>
- **Параметр:** login
- **Описание:** внедрение SQL, в зависимости от типа используемой СУБД и условий внедрения, может дать возможность атакующему выполнить произвольный запрос к базе данных (например, прочитать содержимое любых таблиц, удалить, изменить или добавить данные), получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере.
- **Риск:** такие уязвимости позволяют получить доступ к критичным данным, клиентским аккаунтам, панели управления сайтом (для последующей компрометации веб-сервера).



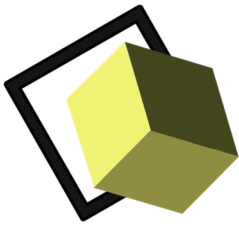
## OWASP A1 SQL injection

- **Вид:** внедрение операторов SQL
- **Тип:** error based
- **URL:** <http://www.example.com/news/2015/>
- **Параметр:** news\_title
- **Описание:** внедрение SQL, в зависимости от типа используемой СУБД и условий внедрения, может дать возможность атакующему выполнить произвольный запрос к базе данных (например, прочитать содержимое любых таблиц, удалить, изменить или добавить данные), получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере.
- **Риск:** такие уязвимости позволяют получить доступ к критичным данным, клиентским аккаунтам, панели управления сайтом (для последующей компрометации веб-сервера).



## OWASP A3 XSS cross site scripting

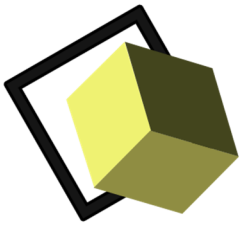
- **Вид:** межсайтовый скриптинг
- **Тип:** stored
- **URL:** <http://www.example.com/list.php>
- **Параметр:** pagename
- **Описание:** межсайтовое выполнение сценариев (XSS) связано с возможностью внедрения HTML-кода в уязвимую страницу. Внедрение кода осуществляется через все доступные способы ввода информации. Успешная эксплуатация уязвимости может позволить злоумышленникам использовать значения различных переменных, доступных в контексте сайта, записывать информацию, перехватывать сессии пользователей и т.д.
- **Риск:** такие уязвимости могут позволить злоумышленнику перехватить чужую сессию, в том числе и администраторов ресурса.



## OWASP A3 XSS cross site scripting

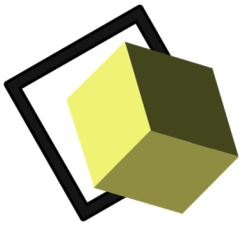
- **Вид:** межсайтовый скриптинг
- **Тип:** reflected
- **URL:** <http://www.example.com/search.php>
- **Параметр:** `pagename`
- **Описание:** межсайтовое выполнение сценариев (XSS) связано с возможностью внедрения HTML-кода в уязвимую страницу. Внедрение кода осуществляется через все доступные способы ввода информации. Успешная эксплуатация уязвимости может позволить злоумышленникам использовать значения различных переменных, доступных в контексте сайта, записывать информацию, перехватывать сессии пользователей и т.д.
- **Риск:** такие уязвимости могут позволить злоумышленнику перехватить чужую сессию, в том числе и администраторов ресурса.





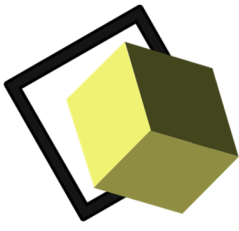
## OWASP A8 CSRF cross site request forgery

- **Вид:** межсайтовая подделка запросов
- **URL:** <http://www.example.com/profile.php>
- **Описание:** вектор атаки CSRF, также известный как XSRF, позволяет злоумышленнику выполнять от имени жертвы действия на сервере, где не реализованы дополнительные проверки.
- **Риск:** основное применение CSRF — вынуждение выполнения каких-либо действий на уязвимом сайте от лица жертвы (изменение пароля, секретного вопроса для восстановления пароля, почты, добавление администратора и т. д.). Также с помощью CSRF возможна эксплуатация отраженных XSS, обнаруженных на другом сервере.



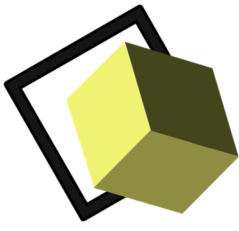
## OWASP A8 CSRF cross site request forgery

- **Вид:** межсайтовая подделка запросов
- **URL:** <http://www.example.com/cart.php>
- **Описание:** вектор атаки CSRF, также известный как XSRF, позволяет злоумышленнику выполнять от имени жертвы действия на сервере, где не реализованы дополнительные проверки.
- **Риск:** основное применение CSRF — вынуждение выполнения каких-либо действий на уязвимом сайте от лица жертвы (изменение пароля, секретного вопроса для восстановления пароля, почты, добавление администратора и т. д.). Также с помощью CSRF возможна эксплуатация отраженных XSS, обнаруженных на другом сервере.



## OWASP A8 CSRF cross site request forgery

- **Вид:** межсайтовая подделка запросов
- **URL:** <http://www.example.com/cart.php>
- **Описание:** вектор атаки CSRF, также известный как XSRF, позволяет злоумышленнику выполнять от имени жертвы действия на сервере, где не реализованы дополнительные проверки.
- **Риск:** основное применение CSRF — вынуждение выполнения каких-либо действий на уязвимом сайте от лица жертвы (изменение пароля, секретного вопроса для восстановления пароля, почты, добавление администратора и т. д.). Также с помощью CSRF возможна эксплуатация отраженных XSS, обнаруженных на другом сервере.



# BitReverse

We can see what others can't...

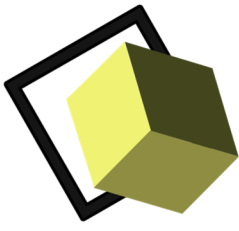
65123  
Ak. Zabolotnogo str. 38  
Odessa, Ukraine

<http://bitreverse.org>

---

## OWASP A6 Sensitive Data Exposure

- **Вид:** утечка чувствительных данных
- **Тип:** phpinfо
- **URL:** <http://www.example.com/phpinfo.php>
- **Описание:** файл содержит информацию о текущей конфигурации PHP.
- **Риск:** злоумышленник может получить информацию о компонентах системы для формирования векторов атаки.



# BitReverse

We can see what others can't...

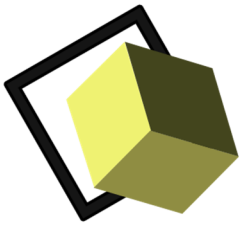
65123  
Ak. Zabolotnogo str. 38  
Odessa, Ukraine

<http://bitreverse.org>

---

## OWASP A6 Sensitive Data Exposure

- **Вид:** утечка чувствительных данных
- **Тип:** full path disclosure
- **URL:** <http://www.example.com/admin/test.php>
- **Описание:** полное раскрытие путей относительно корня веб-сервера.
- **Риск:** злоумышленник может получить информацию о структуре вебсервера (и возможной версии ПО) для формирования векторов атаки.



# BitReverse

We can see what others can't...

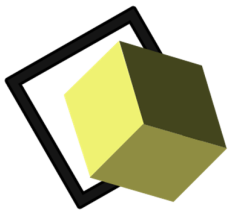
65123  
Ak. Zabolotnogo str. 38  
Odessa, Ukraine

<http://bitreverse.org>

---

## OWASP A6 Sensitive Data Exposure

- **Вид:** утечка чувствительных данных
- **Тип:** .git repository
- **URL:** <http://www.example.com/.git>
- **Описание:** указание, git репозитория.
- **Риск:** злоумышленник может получить критичную информацию о веб-приложении, включая исходный код и данные для авторизации.



## **Заключение:**

Совокупность выявленных уязвимостей свидетельствует о крайней незащищенности веб-сайта. Подобные уязвимости с большей долей вероятности позволят злоумышленнику получить несанкционированный доступ к ресурсу, скомпрометировать данные, использовать ресурс для атаки как на его пользователей, так и на внутреннюю сеть.

Аудит в автоматическом режиме позволяет выявить большинство известных уязвимостей и предотвратить распространённые атаки на тестируемый ресурс.

Для качественной оценки защищенности и реализации адекватных средств обеспечения безопасности веб-сайта рекомендуется проводить комплексный аудит, включающий:

- инструментальный и ручной анализ, в том числе:
  - выявление ошибок логики веб-приложения;
  - манипуляцию пользовательскими данными;
  - проверку ресурса на получение доступа к конфиденциальной информации;
  - атаки класса "race condition" и другие техники, основанные на многолетнем опыте наших сотрудников;
- анализ веб-окружения и веб-сервера;
- анализ смежной инфраструктуры;
- нагрузочное тестирование (опционально).

Более подробную информацию Вы можете получить на сайте [www.bitreverse.org/](http://www.bitreverse.org/) или же связавшись с нами по e-mail: [bitreverse@gmail.com](mailto:bitreverse@gmail.com).