ООО КОМТЕТ 440000, г. Пенза ул. Суворова, 92

Отчет по услуге «Анализ безопасности сайта»
Проверяемый сайт: *****.ru

1.Введение

Данный отчёт включает в себя информацию по анализу безопасности сайта, в рамках услуги было выполнено следующее:

- определение версии движка сайта для дальнейшего определения возможных уязвимостей;
- сравнение текущих версий расширений движка сайта с актуальными версиями этих же расширений;
- анализ работы шаблона сайта;
- проверка скриптов сайта на наличие распространенного вредоносного кода;
- составление рекомендаций по устранению вредоносного кода с сайта и предотвращению повторного заражения сайта вредоносным кодом.
- проверка стойкости парольной фразы
- подготовка подробного отчета по проведенному анализу;

Класификация и критерии уязвимостей

Каждая уязвимость имеет степень риска в зависимости от возможного нанесения урона веб-приложению , подробная информация представлена в таблице ниже:

Высокая степень риска
Данный тип уязвимостей может вызывать отказ в работоспособности сайта, критические ошибки, выполнение произвольного кода(web-shell). При наличии подобных уязвимостей у злоумышленника есть возможность компрометации всех данных веб-ресурса
Средняя степень риска
Данный тип уязвимостей представляет возможность злоумышленнику раскрыть критически важные данные, которые в дальнейшем можно использовать для компрометации ресурса.
Низкая степень риска
К данному типу относятся остальные уязвимости.

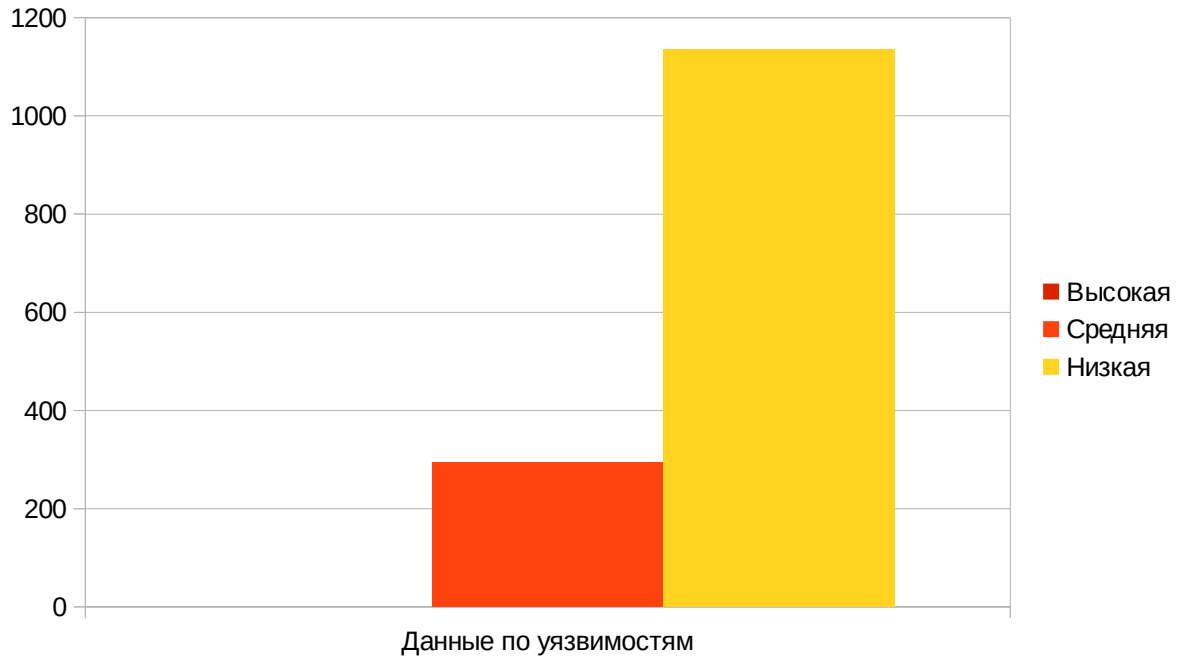
2.Общие данные

Название	Версия	Актуальность
Обнаруженная версия CMS		
MODX	1.0.15	Актуальная версия, не требует обновлений
Обнаруженные модули		
Doc Manager	1.1	Актуальная версия, не требует обновлений
Обнаруженные плагины		
CodeMirror	1.2b	Актуальная версия, не требует обновлений
FileSource	0.1	Актуальная версия, не требует обновлений
Forgot Manager Login	1.1.6	Актуальная версия, не требует обновлений
Inherit Parent Template	1.0	Актуальная версия, не требует обновлений
ManagerManager	0.3.8	Актуальная версия, не требует обновлений
Quick Manager	1.5.6	Актуальная версия, не требует обновлений
TinyMCE Rich Text Editor	3.5.11 J	Актуальная версия, не требует обновлений
Search Highlight	1.5	Актуальная версия, не требует обновлений
Show Image Tvs	1.0	Актуальная версия, не требует обновлений

3.Данные по уязвимостям по степени риска

Используется классификация используются классификации “The Common Vulnerability Scoring System (CVSSv2)”, MITRE(CAPEC) и OWASP.

Высокая	0
Средняя	294
Низкая	1135



Описание	X-Frame-Options header заголовок не включен в ответ HTTP, для защиты от атак типа -"ClickJacking '.
URL	http://*****.ru/vegetablesvidi.html
Решение	Необходимо разрешить вставлять фреймы с сайтом только с самого сайта. Отвечает за это заголовок X-Frame-Options:SAMEORIGIN. SAMEORIGIN разрешает использование фреймов только с самого сайта Все

	современные браузеры поддерживают заголовок X-Frame-Options. Он разрешает или запрещает отображение страницы, если она открыта во фрейме. Браузеры игнорируют заголовок, если он определен в META тег. Таким образом, <meta http-equiv="X-Frame-Options"...> будет проигнорирован.
Ссылка на дополнитеную информацию	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

Описание	Страница с ошибкой может содержать важную информацию, позволяющую злоумышленнику собрать дополнительные сведения о ресурсе.
URL	http://*****.ru/*
Параметр	N/A
Код ошибки	HTTP 500 Internal server error
Решение	Проверить исходный код этой страницы, по возможности исправить ошибку, если решения по исправлению ошибки нет, необходимо установить пользовательские уведомления о ошибках
Reference	
CWE Id	200
WASC Id	13

Низкая	**Cookie без HttpOnly флага**
Описание	Cookie без флага HttpOnly могут быть доступны JavaScript'ам .Если вредоносный код будет запущен на данной странице, то Cookie может быть передан на сторонний сайт, если Cookie сессии, то становится возможен перехват сессии(hijacking)
URL	http://*****.ru
Parameter	SN54a3bb86b97ea=59f7bceee600d0e83c0e21c79b2ed2bc; path=/

Evidence	SN54a3bb86b97ea=59f7bceee600d0e83c0e21c79b2ed2bc; path=/
Решение	Убедится в том что флаг HttpOnly установлен для всех cookies
Reference	www.owasp.org/index.php/HttpOnly
WASC Id	13

Низкая **Cross-Domain JavaScript Source File Inclusion**

Описание	Страница включает JavaScript сторонних ресурсов
URL	http://*****.ru
Parameter	http://pagead2.googlesyndication.com/pagead/show_ads.js
Evidence	http://pagead2.googlesyndication.com/pagead/show_ads.js
Решение	Убедится в том что JavaScript загружается только из достоверных источников
Reference	

Низкая **X-Content-Type-Options не указанный заголовок**

Описание	Возможность Internet Explorer «угадывать» тип файла, игнорируя его MIME-тип (обычно соответствует расширению файла). При передаче от сервера к браузеру все файлы имеют тот или иной тип (css, javascript, jpeg, xml и т. д.), который прямо указывает на суть содержимого файла. Однако, Internet Explorer имеет встроенный механизм, который позволяет по содержимому файла переопределить его тип. Таким образом, обычные текстовые файлы могут быть интерпретированы как JavaScript со всеми вытекающими последствиями. Например, если у вас на сайте запрещена загрузка текстовых файлов с расширениями .js пользователями, то они могут загрузить в виде картинок текстовый файл, содержащий JavaScript-код, который может быть исполнен браузером.
URL	http://*****.ru
Решение	Для отключения такого поведения достаточно добавить заголовок на стороне сервера X-Content-Type-Options: nosniff
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers

4.Проверка стойкости парольной фразы устойчивость к bruteforce атакам

Форма авторизации в административный интерфейс(http://*****.ru/manager/) была проверена методом bruteforce по словарю из 500 популярных парольных фраз(см. Приложение 1) по результатам проверки подобрать парольную фразу не получилось. Кроме того на сайте настроены и успешно работают механизмы защиты от подобного типа атак, а так же используется нестандартный логин(adminka), что значительно усложняет подобный тип атаки.

5.Рекомендации

Сайт достаточно защищен и устойчив к большинству типов атак. Для обеспечения наиболее максимальной безопасности рекомендуем выполнить рекомендации из пункта 3 , а так же перейти на выделенный сервер для возможности внесения более гибких параметров безопасности.

Приложение 1

Список парольных фраз использованных при проверке на стойкость пароля:

123456 password 12345678 1234 pussy 12345 dragon qwerty 696969 mustang letmein baseball master michael football shadow monkey abc123 pass fuckme 6969 jordan harley ranger iwantu jennifer hunter fuck 2000 test batman trustno1 thomas tigger robert access love buster 1234567 soccer hockey killer george sexy andrew charlie superman asshole fuckyou dallas jessica panties pepper 1111 austin william daniel golfer summer heather hammer yankees joshua maggie biteme enter ashley thunder cowboy silver richard fucker orange merlin michelle corvette bigdog cheese matthew 121212 patrick martin freedom ginger blowjob nicole sparky yellow camaro secret dick falcon taylor 111111 131313 123123 bitch hello scooter please porsche guitar chelsea black diamond nascar jackson cameron 654321 computer amanda wizard xxxxxxxx money phoenix mickey bailey knight iceman tigers purple andrea horny dakota aaaaaa player sunshine morgan starwars boomer cowboys edward charles girls booboo coffee xxxxxx bulldog ncc1701 rabbit peanut john johnny gandalf spanky winter brandy compaq carlos tennis james mike brandon fender anthony blowme ferrari cookie chicken maverick chicago joseph diablo sexsex hardcore 666666 willie welcome chris panther yamaha justin banana driver marine angels fishing david maddog hooters wilson butthead dennis fucking captain bigdick chester smokey xavier steven viking snoopy blue eagles winner samantha house miller flower jack firebird butter united turtle steelers tiffany zxcvbn tomcat golf bond007 bear tiger doctor gateway gators angel junior thx1138 porno badboy debbie spider melissa booger 1212 flyers fish porn matrix teens scooby jason walter cumshot boston braves yankee lover barney victor tucker princess mercedes 5150 doggie zzzzzz gunner horney bubba 2112 fred johnson xxxxx tits member boobs donald bigdaddy bronco penis voyager rangers birdie trouble white topgun bigtits bitches green super qazwsx magic lakers rachel slayer scott 2222 asdf video london 7777 marlboro srinivas internet action carter jasper monster teresa jeremy 11111111 bill crystal peter pussies cock beer rocket theman oliver prince beach amateur 7777777 muffin redsox star testing shannon murphy frank hannah dave eagle1 11111 mother nathan raiders steve forever angela viper ou812 jake lovers suckit gregory buddy whatever young nicholas lucky helpme jackie monica midnight college baby cunt brian mark startrek sierra leather 232323 4444 beavis bigcock happy sophie ladies naughty giants booty blonde fucked golden admin fire sandra pookie packers einstein dolphins 0 chevy winston warrior sammy slut 8675309 zxcvbnm nipples power victoria asdfgh vagina toyota travis hotdog paris rock xxxx extreme redskins erotic dirty ford freddy arsenal access14 wolf nipple iloveyou alex florida eric legend movie success rosebud jaguar great cool cooper 1313 scorpio mountain madison 987654 brazil lauren japan naked squirt stars apple alexis aaaa bonnie peaches jasmine kevin matt qwertyui danielle beaver 4321 4128 runner swimming dolphin gordon casper stupid shit saturn gemini apples august 3333 canada blazer cumming hunting kitty rainbow 112233 arthur cream calvin shaved surfer samson kelly paul mine king racing 5555 eagle hentai newyork little redwings smith sticky cocacola animal broncos private skippy marvin blondes enjoy girl apollo parker qwert time sydney women voodoo magnum juice abgrtyu 777777 dreams maxwell music rush2112 russia scorpion rebecca tester mistress phantom billy 6666

Приложение 2

Определения использованные в отчете:

Web-shell - Это некий вредоносный скрипт (программа), который злоумышленники используют для управления чужими сайтами и серверами: выполнения команд терминала, перебора паролей, доступа к файловой системе и т.п. Для размещения скрипта чаще всего используются уязвимости в коде сайта или подбор паролей.

ClickJacking - Это механизм обмана пользователей интернета, при котором злоумышленник может получить доступ к конфиденциальной информации или даже получить доступ к компьютеру пользователя, заманив его на внешне безобидную страницу или внедрив вредоносный код на безопасную страницу. Принцип основан на том, что поверх видимой страницы располагается невидимый слой, в который и загружается нужная злоумышленнику страница, при этом элемент управления (кнопка, ссылка), необходимый для осуществления требуемого действия, совмещается с видимой ссылкой или кнопкой, нажатие на которую ожидается от пользователя. Возможны различные применения технологии — от подписки на ресурс в социальной сети до кражи конфиденциальной информации и совершения покупок в интернет-магазинах за чужой счёт.

Hijacking - разновидность MITM-атаки при которой злоумышленник способен просматривать просматривать пакеты пользователей и посылать свои собственные пакеты в сеть. Атака использует особенности установления соединения в протоколе TCP, и может осуществляться как во время «тройного рукопожатия», так и при установленном соединении

Bruteforce - Так называемые атаки методом "грубой силы". Как правило, пользователи применяют простейшие пароли, например "123", "admin" и т.д. Этим и пользуются компьютерные злоумышленники, которые при помощи специальных троянских программ вычисляют необходимый для проникновения в сеть пароль методом подбора - на основании заложенного в эту программу словаря паролей или генерируя случайные последовательности символов.