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

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

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;

Классификация 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 Evolution	1.0.10	Требует обновления
Обнаруженные модули		
Doc Manager	1.1	Требует обновления
easy2	-	-
QuickEdit		Требует обновления
Shopkeeper	0.9.6	Требует обновления
Обнаруженные плагины		
ManagerManager	0.3.9	Требует обновления
Quick Manager+	1.5.5	Требует обновления
TinyMCE Rich Text Editor	3.5.8	Требует обновления
TransAlias	1.5	Требует обновления
Search Highlight	1.5	Требует обновления
PHx	-	-

3.Уязвимости без классификации

1. Обнаружены резервные копии баз данных(БД) с неконтролируемым доступом, например:

https://*****/assets/backup/06-05-2015-180545.sql

https://*****/assets/backup/06-05-2015-205659.sql

https://*****/assets/backup/16-07-2015-151503.sql

https://*****/assets/backup/24-07-2013-154038.sql

Злоумышленник может получить доступ к дампу БД, из которого вычислить критическую Важную информацию, такую как учетные записи административных пользователей CMS, ip адреса пользователей и.т.д. Данная информация может использоваться для дальнейшей атаки.

Для устранения данной уязвимости рекомендуется ограничить доступ к каталогу либо удалить копии из каталога:

/www/*****/www/htdocs/assets/backup

2. Обнаружена незащищенная форма позволяющая загрузить вредоносный код:

https://*****/assets/plugins/tinymce3201/jscripts/tiny_mce/plugins/upload/upload.php

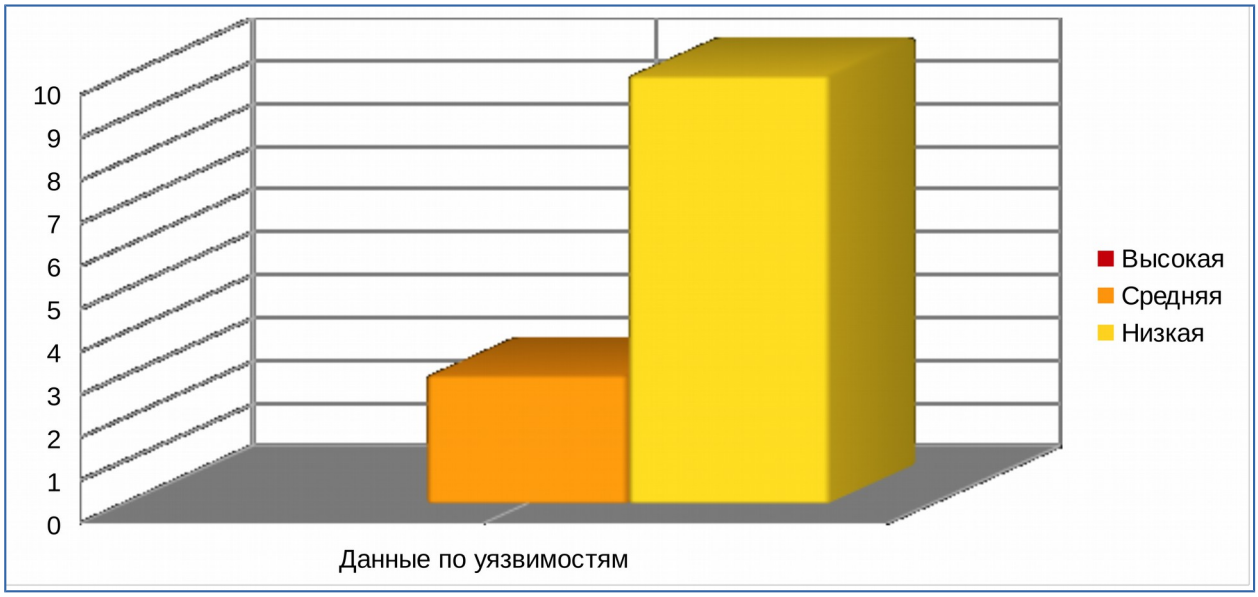
Злоумышленник может загрузить через форму любой вредоносный код, в том числе web-shell, тем самым получив полный доступ к сайту и ресурсам хостинга.

Для устранения необходимо ограничить доступ к форме. Стоит отметить, данная форма принадлежит отключенному плагину сайта Tiny Mce(на сайте используется более новая версия), старый плагин содержавший уязвимость можно удалить.

4.Данные по уязвимостям по степени риска

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

Высокая	0
Средняя	3
Низкая	10



Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	http://*****/731.html
URL	http://*****/1041.html
URL	http://*****/assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	http://*****/assets/snippets/shopkeeper/lang/russian-UTF8.js
URL	http://*****/assets/snippets/shopkeeper/js/shopkeeper.js
Instances	5
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Other information	At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://*****/
URL	https://*****/robots.txt
URL	https://*****/sitemap.xml
URL	https://*****/english.html
URL	https://*****/731.html
URL	https://*****/40.html
URL	https://*****/about.html
URL	https://*****/help.html

URL	https://*****/19.html
URL	https://*****/21.html
URL	https://*****/4.html
URL	https://*****/65.html
URL	https://*****/23.html
URL	https://*****/25.html
URL	https://*****/27.html
URL	https://*****/261.html
URL	https://*****/1653.html
URL	https://*****/1879.html
URL	https://*****/2361.html
URL	https://*****/2362.html
Instances	5346
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Other information	At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
Description	The page includes mixed content, ie content accessed via http instead of https.
URL	https://*****/1041.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js

URL	https://*****/1688.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1687.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1686.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1685.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1684.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1683.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1682.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1681.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js

URL	https://*****/1041.html?start=8
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1041.html?start=16
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1072.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1073.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1076.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1039.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	https://*****/1040.html
Attack	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Evidence	http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
Instances	16
Solution	A page that is available over TLS must be comprised completely of content which is transmitted over TLS. The page must not contain any content that is transmitted over unencrypted

	HTTP. This includes content from unrelated third party sites.
Other information	tag=script src=http://*****//assets/snippets/shopkeeper/js/jquery-1.4.2.min.js tag=script src=http://*****//assets/snippets/shopkeeper/lang/russian-UTF8.js tag=script src=http://*****//assets/snippets/shopkeeper/js/shopkeeper.js
Reference	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

Low (Medium) **Web Browser XSS Protection Not Enabled**

Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://*****/731.html
URL	http://*****/1041.html
URL	http://*****/assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	http://*****/assets/snippets/shopkeeper/lang/russian-UTF8.js
URL	http://*****/assets/snippets/shopkeeper/js/shopkeeper.js
Instances	5
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).

Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14

Low (Medium) **X-Content-Type-Options Header Missing**

Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://*****/731.html
URL	http://*****/1041.html
URL	http://*****/assets/snippets/shopkeeper/js/jquery-1.4.2.min.js
URL	http://*****/assets/snippets/shopkeeper/lang/russian-UTF8.js
URL	http://*****/assets/snippets/shopkeeper/js/shopkeeper.js
Instances	5
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
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

WASC Id	15

Low (Medium) **Incomplete or No Cache-control and Pragma HTTP Header Set**

Description The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.

URL	https://*****/
Evidence	private, must-revalidate
URL	https://*****/robots.txt
Evidence	private, must-revalidate
URL	https://*****/sitemap.xml
Evidence	private, must-revalidate
URL	https://*****/english.html
Evidence	private, must-revalidate
URL	https://*****/731.html
Evidence	private, must-revalidate
URL	https://*****/40.html
Evidence	private, must-revalidate
URL	https://*****/about.html
Evidence	private, must-revalidate
URL	https://*****/help.html
Evidence	private, must-revalidate
URL	https://*****/19.html
Evidence	private, must-revalidate
URL	https://*****/21.html
Evidence	private, must-revalidate

URL	https://*****/4.html
Evidence	private, must-revalidate
URL	https://*****/65.html
Evidence	private, must-revalidate
URL	https://*****/23.html
Evidence	private, must-revalidate
URL	https://*****/25.html
Evidence	private, must-revalidate
URL	https://*****/27.html
Evidence	private, must-revalidate
URL	https://*****/261.html
Evidence	private, must-revalidate
URL	https://*****/1653.html
Evidence	private, must-revalidate
URL	https://*****/1879.html
Evidence	private, must-revalidate
URL	https://*****/2361.html
Evidence	private, must-revalidate
URL	https://*****/2362.html
Evidence	private, must-revalidate
Instances	5338
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate, private; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_C

	ontent_Caching
CWE Id	525

Low (Medium) **Cookie set without HttpOnly flag**

Description: A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

URL	https://*****/
Parameter	SN51e915cb255a7=3cc7a5147a6f31ab20d456d587f9d98e; path=/
Evidence	SN51e915cb255a7=3cc7a5147a6f31ab20d456d587f9d98e; path=/
URL	https://*****/robots.txt
Parameter	SN51e915cb255a7=2b376c5ca160d166f29dcb0b94948af5; path=/
Evidence	SN51e915cb255a7=2b376c5ca160d166f29dcb0b94948af5; path=/
URL	https://*****/
Parameter	SN51e915cb255a7=a885199dc70bd6e364cbd236a31f432c; path=/
Evidence	SN51e915cb255a7=a885199dc70bd6e364cbd236a31f432c; path=/
URL	https://*****/sitemap.xml
Parameter	SN51e915cb255a7=2a1e568225079e997330385f8e4afed0; path=/
Evidence	SN51e915cb255a7=2a1e568225079e997330385f8e4afed0; path=/
URL	https://*****/45.html
Parameter	SN51e915cb255a7=0b3be04cc764ced78c5de3da348a79a0; path=/
Evidence	SN51e915cb255a7=0b3be04cc764ced78c5de3da348a79a0; path=/
URL	https://*****/english.html
Parameter	SN51e915cb255a7=3434665d60c3da5c1da44580515ea92d; path=/
Evidence	SN51e915cb255a7=3434665d60c3da5c1da44580515ea92d; path=/
URL	https://*****/731.html

Parameter	SN51e915cb255a7=983cb7cafb8f7b18a24dacdfd6a33630; path=/
Evidence	SN51e915cb255a7=983cb7cafb8f7b18a24dacdfd6a33630; path=/
URL	https://*****/40.html
Parameter	SN51e915cb255a7=0434b8ca184ea576e2465aa7cd4d1175; path=/
Evidence	SN51e915cb255a7=0434b8ca184ea576e2465aa7cd4d1175; path=/
URL	https://*****/about.html
Parameter	SN51e915cb255a7=ac59314ef2d1dbf57157349dd07d11ba; path=/
Evidence	SN51e915cb255a7=ac59314ef2d1dbf57157349dd07d11ba; path=/
URL	https://*****/help.html
Parameter	SN51e915cb255a7=7f7b84753f121edb4b98042bfcf8536a; path=/
Evidence	SN51e915cb255a7=7f7b84753f121edb4b98042bfcf8536a; path=/
URL	https://*****/19.html
Parameter	SN51e915cb255a7=d5e201267fc4d5b3c39e42fd55f178b3; path=/
Evidence	SN51e915cb255a7=d5e201267fc4d5b3c39e42fd55f178b3; path=/
URL	https://*****/21.html
Parameter	SN51e915cb255a7=fbcf4db3151a0f42816f1a049e24a08d; path=/
Evidence	SN51e915cb255a7=fbcf4db3151a0f42816f1a049e24a08d; path=/
URL	https://*****/4.html
Parameter	SN51e915cb255a7=7a9e32526c1f0f60209bc6b57c747b03; path=/
Evidence	SN51e915cb255a7=7a9e32526c1f0f60209bc6b57c747b03; path=/
URL	https://*****/65.html
Parameter	SN51e915cb255a7=e1073116efe059fec762f0d035cbee53; path=/
Evidence	SN51e915cb255a7=e1073116efe059fec762f0d035cbee53; path=/
URL	https://*****/23.html

Parameter	SN51e915cb255a7=e323b91c4dfdc779dcc628065e54b049; path=/
Evidence	SN51e915cb255a7=e323b91c4dfdc779dcc628065e54b049; path=/
URL	https://*****/25.html
Parameter	SN51e915cb255a7=ca3131892339369348 0329db38177d13; path=/
Evidence	SN51e915cb255a7=ca3131892339369348 0329db38177d13; path=/
URL	https://*****/27.html
Parameter	SN51e915cb255a7=be595a99a7996b73ef2f7f3050cacc30; path=/
Evidence	SN51e915cb255a7=be595a99a7996b73ef2f7f3050cacc30; path=/
URL	https://*****/261.html
Parameter	SN51e915cb255a7=35f26cd4cffa233dc97363884a34b181; path=/
Evidence	SN51e915cb255a7=35f26cd4cffa233dc97363884a34b181; path=/
URL	https://*****/1653.html
Parameter	SN51e915cb255a7=c9d388e74085a86d0b3157a1a3355524; path=/
Evidence	SN51e915cb255a7=c9d388e74085a86d0b3157a1a3355524; path=/
URL	https://*****/1879.html
Parameter	SN51e915cb255a7=b1311c7562150c81c4ebed1d61e11f23; path=/
Evidence	SN51e915cb255a7=b1311c7562150c81c4ebed1d61e11f23; path=/
Instances	7436
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	www.owasp.org/index.php/HttpOnly
WASC Id	13

Low (Medium) **Cookie set without secure flag**

Description A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

URL	https://*****/
Parameter	SN51e915cb255a7=3cc7a5147a6f31ab20d456d587f9d98e; path=/
Evidence	SN51e915cb255a7=3cc7a5147a6f31ab20d456d587f9d98e; path=/
URL	https://*****/robots.txt
Parameter	SN51e915cb255a7=2b376c5ca160d166f29dcb0b94948af5; path=/
Evidence	SN51e915cb255a7=2b376c5ca160d166f29dcb0b94948af5; path=/
URL	https://*****/
Parameter	SN51e915cb255a7=a885199dc70bd6e364cbd236a31f432c; path=/
Evidence	SN51e915cb255a7=a885199dc70bd6e364cbd236a31f432c; path=/
URL	https://*****/sitemap.xml
Parameter	SN51e915cb255a7=2a1e568225079e997330385f8e4afed0; path=/
Evidence	SN51e915cb255a7=2a1e568225079e997330385f8e4afed0; path=/
URL	https://*****/45.html
Parameter	SN51e915cb255a7=0b3be04cc764ced78c5de3da348a79a0; path=/
Evidence	SN51e915cb255a7=0b3be04cc764ced78c5de3da348a79a0; path=/
URL	https://*****/english.html
Parameter	SN51e915cb255a7=3434665d60c3da5c1da44580515ea92d; path=/
Evidence	SN51e915cb255a7=3434665d60c3da5c1da44580515ea92d; path=/
URL	https://*****/731.html
Parameter	SN51e915cb255a7=983cb7cafb8f7b18a24dacdfd6a33630; path=/
Evidence	SN51e915cb255a7=983cb7cafb8f7b18a24dacdfd6a33630; path=/
URL	https://*****/40.html
Parameter	SN51e915cb255a7=0434b8ca184ea576e2465aa7cd4d1175; path=/
Evidence	SN51e915cb255a7=0434b8ca184ea576e2465aa7cd4d1175; path=/

URL	https://*****/about.html
Parameter	SN51e915cb255a7=ac59314ef2d1dbf57157349dd07d11ba; path=/
Evidence	SN51e915cb255a7=ac59314ef2d1dbf57157349dd07d11ba; path=/
URL	https://*****/help.html
Parameter	SN51e915cb255a7=7f7b84753f121edb4b98042bfcf8536a; path=/
Evidence	SN51e915cb255a7=7f7b84753f121edb4b98042bfcf8536a; path=/
URL	https://*****/19.html
Parameter	SN51e915cb255a7=d5e201267fc4d5b3c39e42fd55f178b3; path=/
Evidence	SN51e915cb255a7=d5e201267fc4d5b3c39e42fd55f178b3; path=/
URL	https://*****/21.html
Parameter	SN51e915cb255a7=fbcf4db3151a0f42816f1a049e24a08d; path=/
Evidence	SN51e915cb255a7=fbcf4db3151a0f42816f1a049e24a08d; path=/
URL	https://*****/4.html
Parameter	SN51e915cb255a7=7a9e32526c1f0f60209bc6b57c747b03; path=/
Evidence	SN51e915cb255a7=7a9e32526c1f0f60209bc6b57c747b03; path=/
URL	https://*****/65.html
Parameter	SN51e915cb255a7=e1073116efe059fec762f0d035cbee53; path=/
Evidence	SN51e915cb255a7=e1073116efe059fec762f0d035cbee53; path=/
URL	https://*****/23.html
Parameter	SN51e915cb255a7=e323b91c4dfdc779dcc628065e54b049; path=/
Evidence	SN51e915cb255a7=e323b91c4dfdc779dcc628065e54b049; path=/
URL	https://*****/25.html
Parameter	SN51e915cb255a7=ca31318923393693480329db38177d13; path=/
Evidence	SN51e915cb255a7=ca31318923393693480329db38177d13; path=/

URL	https://*****/27.html
Parameter	SN51e915cb255a7=be595a99a7996b73ef2f7f3050cacc30; path=/
Evidence	SN51e915cb255a7=be595a99a7996b73ef2f7f3050cacc30; path=/
URL	https://*****/261.html
Parameter	SN51e915cb255a7=35f26cd4cffa233dc97363884a34b181; path=/
Evidence	SN51e915cb255a7=35f26cd4cffa233dc97363884a34b181; path=/
URL	https://*****/1653.html
Parameter	SN51e915cb255a7=c9d388e74085a86d0b3157a1a3355524; path=/
Evidence	SN51e915cb255a7=c9d388e74085a86d0b3157a1a3355524; path=/
URL	https://*****/1879.html
Parameter	SN51e915cb255a7=b1311c7562150c81c4ebed1d61e11f23; path=/
Evidence	SN51e915cb255a7=b1311c7562150c81c4ebed1d61e11f23; path=/
Instances	7436
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted tunnel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13

Low (Medium) **Cross-Domain JavaScript Source File Inclusion**

Description	The page at the following URL includes one or more script files from a third-party domain
URL	https://*****/
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730

URL	https://*****/robots.txt
Parameter	//yandex.st/share/share.js
Evidence	//yandex.st/share/share.js
URL	https://*****/robots.txt
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
URL	https://*****/sitemap.xml
Parameter	//yandex.st/share/share.js
Evidence	//yandex.st/share/share.js
URL	https://*****/sitemap.xml
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
URL	https://*****/english.html
Parameter	//yandex.st/share/share.js
Evidence	//yandex.st/share/share.js
URL	https://*****/english.html
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
URL	https://*****/731.html
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
URL	https://*****/40.html
Parameter	//yandex.st/share/share.js
Evidence	//yandex.st/share/share.js

URL	https://*****/40.html
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
URL	https://*****/about.html
Parameter	//yandex.st/share/share.js
Evidence	//yandex.st/share/share.js
URL	https://*****/about.html
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
URL	https://*****/help.html
Parameter	//yandex.st/share/share.js
Evidence	//yandex.st/share/share.js
URL	https://*****/help.html
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
URL	https://*****/19.html
Parameter	//yandex.st/share/share.js
Evidence	//yandex.st/share/share.js
URL	https://*****/19.html
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
URL	https://*****/21.html
Parameter	//yandex.st/share/share.js
Evidence	//yandex.st/share/share.js

URL	https://*****/21.html
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
URL	https://*****/4.html
Parameter	//yandex.st/share/share.js
Evidence	//yandex.st/share/share.js
URL	https://*****/4.html
Parameter	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Evidence	https://w.uptolike.com/widgets/v1/zp.js?pid=1274730
Instances	7293
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application
Reference	

Low (Medium) **Web Browser XSS Protection Not Enabled**

Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	https://*****/
URL	https://*****/robots.txt
URL	https://*****/sitemap.xml
URL	https://*****/english.html
URL	https://*****/731.html
URL	https://*****/40.html
URL	https://*****/about.html
URL	https://*****/help.html
URL	https://*****/19.html

URL	https://*****/21.html
URL	https://*****/4.html
URL	https://*****/65.html
URL	https://*****/23.html
URL	https://*****/25.html
URL	https://*****/27.html
URL	https://*****/261.html
URL	https://*****/1653.html
URL	https://*****/1879.html
URL	https://*****/2361.html
URL	https://*****/2362.html
Instances	5346
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

	https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14

Low (Medium) **X-Content-Type-Options Header Missing**

Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://*****/
URL	https://*****/robots.txt
URL	https://*****/sitemap.xml
URL	https://*****/english.html
URL	https://*****/731.html
URL	https://*****/40.html
URL	https://*****/about.html
URL	https://*****/help.html
URL	https://*****/19.html
URL	https://*****/21.html
URL	https://*****/4.html
URL	https://*****/65.html
URL	https://*****/23.html
URL	https://*****/25.html
URL	https://*****/27.html
URL	https://*****/261.html
URL	https://*****/1653.html

URL	https://*****/1879.html
URL	https://*****/2361.html
URL	https://*****/2362.html
Instances	5346
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
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
WASC Id	15

Low (Medium) **Secure page includes mixed content**

Description	The page includes mixed content, ie content accessed via http instead of https.
URL	https://*****/37.html
Attack	http://wikimapia.org/#lat=53.1941751&
Evidence	http://wikimapia.org/#lat=53.1941751&
URL	https://*****/234.html
Attack	http://timepad.ru/event/register/1148
Evidence	http://timepad.ru/event/register/1148
URL	https://*****/184.html
Attack	http://timepad.ru/event/register/1073

Evidence	http://timepad.ru/event/register/1073
URL	https://*****/448.html
Attack	http://timepad.ru/event/register/1885
Evidence	http://timepad.ru/event/register/1885
Instances	4
Solution	A page that is available over TLS must be comprised completely of content which is transmitted over TLS. The page must not contain any content that is transmitted over unencrypted HTTP. This includes content from unrelated third party sites.
Other information	tag=iframe src=http://wikimapia.org/#lat=53.1941751&lon=45.0223589&z=17&l=1&ifr=1&m=b
Reference	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

Low (Medium) **Private IP Disclosure**

Description	A private IP such as 10.x.x.x, 172.x.x.x, 192.168.x.x has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	https://*****/1983.html
Attack	10-03-15-08
Evidence	10-03-15-08
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Other information	10-03-15-08
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200

5.Проверка стойкости парольной фразы устойчивость к bruteforce атакам

Форма авторизации в административный интерфейс(https://*****/manager/) была проверена методом bruteforce по словарю из 500 популярных парольных фраз(логин: admin) по результатам проверки подобрать парольную фразу не получилось. Кроме того на сайте настроены и успешно работают механизмы защиты от подобного типа атак на уровне CMS, что значительно усложняет подобный тип атаки.

5.Рекомендации

Для обеспечения безопасности требуется обновление CMS, а так же модулей и плагинов до последних стабильных версий, а а так же устранение уязвимостей приведенных в данном отчете. Стоит отметить, на сайте используется SSL шифрование, что обеспечивает дополнительную защиту и устойчивость к атакам по перехвату данных.

Приложение 1

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.