

Лабораторная работа 1

Защита разработчика программного обеспечения

Панченко Денис 1132229056

Савурская Полина 1132222827

Кочарян Никита 1132221541

Норсоян Шушаник 1132221545

Сухальская Ксения 1132229052

Умярова Камилла 1132229051

Содержание

1 Цель работы	3
2 Обнаружение атаки	4
3 Выполнение лабораторной работы	6
3.1 Уязвимость XML Injection и последствие Webmarket PHP backdoor	6
3.2 Уязвимость TeamCity RCE и последствие TeamCity DB Deleter	8
3.3 Уязвимость JS Sandbox escape и последствие Node DOS	10
4 Выводы	13

1 Цель работы

Злоумышленник решает предпринять атаку на инфраструктуру небольшой ИТ-компании, занимающейся веб-разработкой. Просканировав сеть организации, он обнаруживает уязвимость на веб-сайте компании. Закрепившись в системе, нарушитель атакует один из узлов внутренней инфраструктуры разработчика. Нужно защитить разработчика программного обеспечения.

2 Обнаружение атаки

Событие 1: Выполнение XXE-инъекции на узле Webmarket (рис. 2.1).

Правило анализа		
Класс	policy-violation	
Группа	policy	
Название	ET POLICY Executable and linking format (ELF) file download var1	
Описание:	Сигнатурой возможного нарушения политики информационной безопасности	
Текст:	alert tcp \$EXTERNAL_NET !\$HTTP_PORTS -> \$HOME_NET any (msg: "ET POLICY Executable and linking format (ELF) file download var1";flow: established;content: " [7F] ELF ";fast_pattern;content: " 00 00 00 00 00 00 00 00 ";distance: 0;flowbits: set,ET,ELFDownload;reference: url,web.archive.org/web/20131114024152/https://www.itee.uq.edu.au/~cristina/students/david/honoursThesis96/bff.htm;reference: url,doc.emergingthreats.net/bin/view/Main/2000418;classtype: policy-violation;sid: 312191 5;rev: 6;metadata: affected_asset dst, affected_product generic_linux/linux, affected_vendor generic_linux, attack_target Client_Endpoint, created_at 2010_07_20, tag A_MARMA, tag T1190, tias_category Info, updated_at 2017_02_03)	
Описание уязвимостей	url: web.archive.org/web/20131114024152/https://www.itee.uq.edu.au/~cristina/students/david/honoursThesis96/bff.htm url: doc.emergingthreats.net/bin/view/Main/2000418	

Рисунок 2.1: Событие 1

Событие 2: Обход аутентификации и выполнение удаленного кода в TeamCity (рис. 2.2).

Правило анализа		
Класс	policy-violation	
Группа	policy	
Название	ET POLICY Executable and linking format (ELF) file download var1	
Описание:	Сигнатурой возможного нарушения политики информационной безопасности	
Текст:	alert tcp \$EXTERNAL_NET !\$HTTP_PORTS -> \$HOME_NET any (msg: "ET POLICY Executable and linking format (ELF) file download var1";flow: established;content: " [7F] ELF ";fast_pattern;content: " 00 00 00 00 00 00 00 00 ";distance: 0;flowbits: set,ET,ELFDownload;reference: url,web.archive.org/web/20131114024152/https://www.itee.uq.edu.au/~cristina/students/david/honoursThesis96/bff.htm;reference: url,doc.emergingthreats.net/bin/view/Main/2000418;classtype: policy-violation;sid: 312191 5;rev: 6;metadata: affected_asset dst, affected_product generic_linux/linux, affected_vendor generic_linux, attack_target Client_Endpoint, created_at 2010_07_20, tag A_MARMA, tag T1190, tias_category Info, updated_at 2017_02_03)	
Описание уязвимостей	url: web.archive.org/web/20131114024152/https://www.itee.uq.edu.au/~cristina/students/david/honoursThesis96/bff.htm url: doc.emergingthreats.net/bin/view/Main/2000418	

Рисунок 2.2: Событие 2

Событие 3: Атака на песочницу NodeJS Sandbox (рис. 2.3).

Правило анализа

Класс	attempted-user
Группа	exploit
Название	ET EXPLOIT bin bash base64 encoded Remote Code Execution 3

Описание:

Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости

Текст:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS any (msg: "ET EXPLOIT bin bash base64 encoded Remote Code Execution 3";flow: established,to_server,content: "VY mluL2Jhc2";classtype: attempted-user;sid: 2025806;rev: 3;metadata: affected_asset dst, affected_product n/a, affected_vendor n/a, attack_target Web_Server, confidence High, created_at 2018_07_09, deployment Datacenter, mitre_tactic_id Initial_Access, mitre_tactic_id TA0001, mitre_technique_id Exploit_Public_Facing_Application, mitre_technique_id T1190, signature_severity Major, tias_category Exploitation, updated_at 2018_07_09)
```

Рисунок 2.3: Событие 3

3 Выполнение лабораторной работы

3.1 Уязвимость XML Injection и последствие Webmarket PHP backdoor

Обнаруживаем вредоносную сессию (рис. 3.1).

```
rroot@Webmarket:~# cd /var/log/apache2
rroot@Webmarket:/var/log/apache2# ls -la
total 64
drwxr-x--- 2 root adm 4096 Sep 10 16:52 .
drwxrwxr-x 12 root syslog 4096 Sep 10 16:52 ..
-rw-r----- 1 root adm 1220 Sep 10 20:36 access.log
-rw-r----- 1 root adm 984 Sep 10 16:55 error.log
-rw-r----- 1 root adm 818 Jul 21 19:07 error.log.1
-rw-r----- 1 root adm 523 Oct 31 2024 error.log.10.gz
-rw-r----- 1 root adm 233 Sep 5 2024 error.log.11.gz
-rw-r----- 1 root adm 123 Aug 7 2024 error.log.12.gz
-rw-r----- 1 root adm 277 Apr 28 13:25 error.log.2.gz
-rw-r----- 1 root adm 277 Apr 25 10:09 error.log.3.gz
-rw-r----- 1 root adm 324 Feb 6 2025 error.log.4.gz
-rw-r----- 1 root adm 433 Dec 26, 2024 error.log.5.gz
-rw-r----- 1 root adm 326 Dec 21, 2024 error.log.6.gz
-rw-r----- 1 root adm 277 Dec 2, 2024 error.log.7.gz
-rw-r----- 1 root adm 271 Nov 22 2024 error.log.8.gz
-rw-r----- 1 root adm 318 Nov 5 2024 error.log.9.gz
-rw-r----- 1 root root 0 Sep 29 2023 other vhosts.access.log
```

Рисунок 3.1: Сканирование файловой системы

Рисунок 3.2: Сканирование файловой системы

```
2025-02-10T10:51:19.369149+03:00      16 Connect  root@localhost on website using TCP/IP
2025-02-10T10:51:19.369582+03:00      16 Query   SELECT * FROM products WHERE product_name IL
```

Рисунок 3.3: Сканирование файловой системы

Изменяем исполняемы файл (рис. 3.4).

```
root@Webmarket:/var/log/mysql# cd /var/www/html/api
root@Webmarket:/var/www/html/api# ls -la
total 16
drwxr-sr-x 2 www-data www-data 4096 Sep 10 16:55 .
drwxrwsrwx 4 www-data www-data 4096 Sep 10 16:55 .
-rw-r--r-- 1 www-data www-data 1115 Sep 10 16:55 meterpreter.php
-rwxr-xr-x 1 www-data www-data 2610 Oct 31 2024 xml-api.php
```

Рисунок 3.4: Изменение файла

```
as
if ($_SERVER['REQUEST_METHOD'] != 'GET') {
    $xml = file_get_contents('php://input');
    libxml_disable_entity_loader(true);
}
$dom = new DOMDocument();
$dom->loadXML($xml, LIBXML_NOENT | LIBXML_DTDLOAD);
$request = simplexml_import_dom($dom);
```

Рисунок 3.5: изменения файла

Удаляем вредоносный файл (рис. 3.6).

```
root@Webmarket:/var/www/html/api# rm meterpreter.php
root@Webmarket:/var/www/html/api# ls -l
total 4
-rwxr-xr-x 1 www-data www-data 2650 Sep 10 20:43 xml-api.php
```

Рисунок 3.6: Удаление вредоносного файла

Завершаем вредоносную сессию (рис. 3.7).

```
root@Webmarket:/var/www/html/api# ss -tp
          Recv-Q           Send-Q             Local Address:Port          Peer Address:Port
  Process
ESTAB      0           0           10.10.1.34:ssh        195.239.174.11:40547
ESTAB      0           0           10.10.1.34:48368       195.239.174.11:5557
ESTAB      0           0           10.10.1.34:48344       10.10.1.253:36400
ESTAB      0           0           10.10.1.34:4344        195.239.174.11:9765
ESTAB      0           0           10.10.1.34:43668       195.239.174.11:freeclv
ESTAB      0           0           10.10.1.34:43444      195.239.174.11:40547
usersr((("dpsz",pid=1215,fd=12))
usersr((("dpsz",pid=1215,fd=12))
usersr((("apache2",pid=116,fd=12))
usersr((("apache2",pid=116,fd=12))
usersr((("dpsz",pid=1215,fd=3))
```

Рисунок 3.7: Завершение вредоносной сессии

Удаляем вредоносный исполняемый файл (рис. 3.8).

```

root@Webmarket:/var/www/html/api# cd /var/www/html
root@Webmarket:/var/www/html# ls -la
total 36
drwxrwsrwx 4 www-data www-data 4096 Sep 10 16:55 .
drwxr-xr-x 5 www-data root 4096 Sep 10 16:56 ..
drwxr-sr-x 2 www-data www-data 4096 Sep 10 20:43 api
-rw-r--r-- 1 www-data www-data 33 Sep 10 16:55 caidao.php
drwxrwsrwx 2 www-data www-data 4096 Apr 27 2024 ccc
-rwxr-xr-x 1 root www-data 17 Jul 12 2024 in2.php
-rwxrwxrwx 1 www-data www-data 2263 Oct 31 2024 index.php
-rwxrwxrwx 1 www-data www-data 34 Nov 29 2023 robots.txt
-rw-r--r-- 1 root www-data 267 Oct 31 2024 site-map.txt
root@Webmarket:/var/www/html# rm caidao.php

```

Рисунок 3.8: Удаление вредоносного файла

Уязвимость устранена (рис. 3.9).

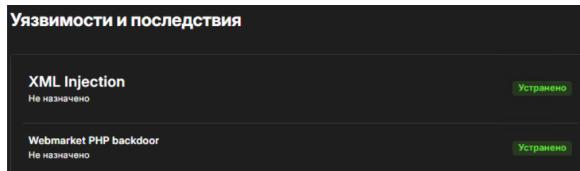


Рисунок 3.9: Устранение уязвимости

3.2 Уязвимость TeamCity RCE и последствие

TeamCity DB Deleter

На TeamCity совершена атака (рис. 3.10).

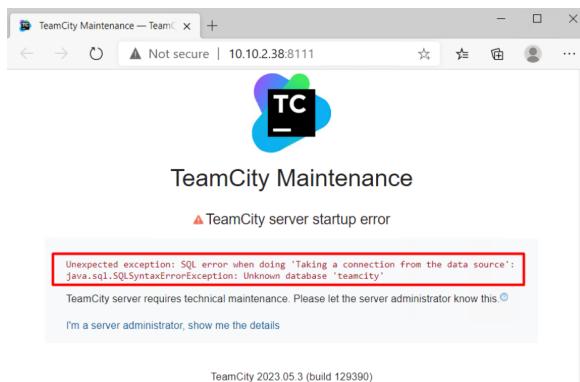


Рисунок 3.10: Атака на TeamCity

Восстанавливаем TeamCity из резервной копии (рис. 3.11).

```
user@teamcity:~$ cd /home/
user@teamcity:/home$ ls -la
total 212
drwxr-xr-x  3 root root  4096 сен 10 16:57 .
drwxr-xr-x 24 root root  4096 сен 16  2023 ..
-rw-r-----  1 root root 203098 сен 10 16:57 backup_10092025-095536.tar.gz
drwxr-xr-x 16 user user  4096 июн 21 15:43 user
user@teamcity:/home$ tar -xvf backup_10092025-095536.tar.gz --strip 3 -C /var/li
b/mysql/
```

Рисунок 3.11: Восстановление

Перезапускаем TeamCity (рис. 3.12).

```
user@teamcity:/home$ sudo systemctl restart teamcity
```

Рисунок 3.12: Перезапуск

Входим в TeamCity (рис. 3.13).

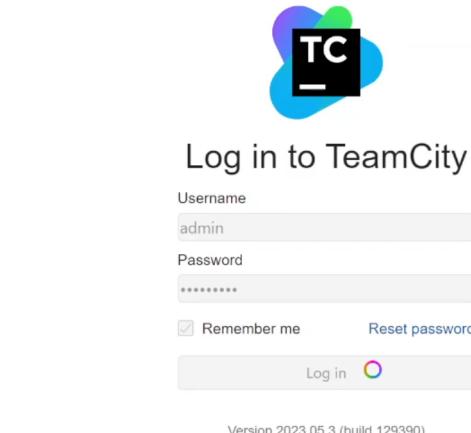


Рисунок 3.13: Авторизация

Устанавливаем плагин для устранения уязвимости (рис. 3.14).

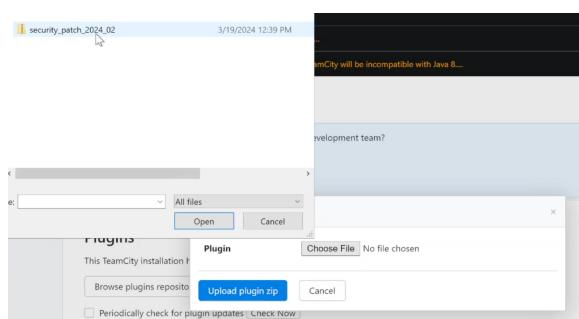


Рисунок 3.14: Загрузка плагина

External plugins			
Plugin Name	Version	Vendor	Home Path
fix CVE-2024-21917, CVE-2024-27198, CVE-2024-27199 The plugin has automatically applied fixes CVE-2024-21917, CVE-2024-27198, CVE-2024-27199	1.2	JetBrains, s.r.o.	<TeamCity Data Directory>/plugins/security_patch_2024_02.zip

Рисунок 3.15: Загрузка плагина

Уязвимость устранена (рис. 3.16).

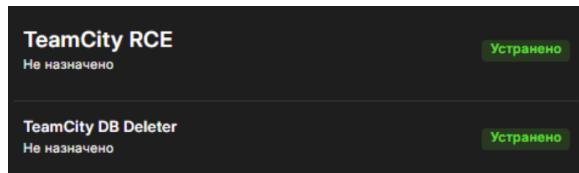


Рисунок 3.16: Устранение уязвимости

3.3 Уязвимость JS Sandbox escape и последствие Node DOS

Сканируем файлы (рис. 3.17).

```
user@vm:~/var/log/apache2$ cat access.log
10.10.1.34 - - [10/Sep/2025:16:57:47 +0300] "POST /api/execute HTTP/1.1" 200 306
"-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
```

Рисунок 3.17: Сканирование файлов

```
user@vm:~$ cd /var/www/www-data/app/node_modules/vm2/lib
user@vm:~/var/www/www-data/app/node_modules/vm2/lib$ ls -la
total 216
drwxr-xr-x 2 www-data www-data 4096 апр 26 2023 .
drwxr-xr-x 4 www-data www-data 4096 мая 5 2023 ..
-rw-r--r-- 1 www-data www-data 29197 апр 26 2023 bridge.js
-rw-r--r-- 1 www-data www-data 718 апр 26 2023 cli.js
-rw-r--r-- 1 www-data www-data 2308 апр 26 2023 compiler.js
-rw-r--r-- 1 www-data www-data 28143 апр 26 2023 events.js
-rw-r--r-- 1 www-data www-data 1299 апр 26 2023 filesystem.js
-rw-r--r-- 1 www-data www-data 361 апр 26 2023 main.js
-rw-r--r-- 1 www-data www-data 16877 апр 26 2023 nodevm.js
-rw-r--r-- 1 www-data www-data 11427 апр 26 2023 resolver-compat.js
-rw-r--r-- 1 www-data www-data 33633 апр 26 2023 resolver.js
-rw-r--r-- 1 www-data www-data 9082 апр 26 2024 script.js
-rw-r--r-- 1 www-data www-data 11177 апр 26 2023 setup-node-sandbox.js
-rw-r--r-- 1 www-data www-data 12441 апр 26 2023 setup-sandbox.js
-rw-r--r-- 1 www-data www-data 6072 апр 26 2023 transformer.juc
-rw-r--r-- 1 www-data www-data 14760 апр 26 2024 vm.js
```

Рисунок 3.18: Сканирование файлов

Редактируем исполняемый файл (рис. 3.19).

```
user@vm:~/var/www/www-data/app/node_modules/vm2/lib$ sudo nano setup-sandbox.js
```

Рисунок 3.19: Редактирование файла

```

if (!localReflectOnGetProperty(localError, "preparedStackTrace")) {
    configurable = false;
    descriptor = undefined;
    get() {
        return currentPreparedStackTrace;
    }
    set(value) {
        if (typeof(value) === "function") {
            currentPreparedStackTrace = value;
            return;
        }
        wrapped = localReflectApply(localNewMapGet, wrappedPrepareStackTrace, [value]);
        if (wrapped) {
            currentPreparedStackTrace = wrapped;
            return;
        }
        const needsDrop = error.stack.indexOf(`at ${descriptor.name}:`) > -1;
        const sandboxSet = ensureThis(error);
        if (localReflectDeleteProperty(error, L)) {
            for (let i = 0; i < sandboxSet.length; i++) {
                for (let j = 0; j < error.stack.length; j++) {
                    if (error.stack[j] === sandboxSet[i]) {
                        if (typeof(error.stack[j + 1]) === "object" && localReflectGetPrototypeOf(error.stack[j + 1]) === OriginalCallSite.prototype) {
                            error.stack[i] = new CallSite(error);
                        }
                    }
                }
            }
        } else {
            let i = 0;
            for (let i = 0; i < sandboxSet.length; i++) {
                localReflectDeleteProperty(error, L[i]);
                proto = null;
                value = error.stack[i];
                enumerable = true;
                configurable = true;
                writable = true;
                proto = Object.getPrototypeOf(error);
                if (proto) {
                    for (let j = 0; j < proto.length; j++) {
                        if (proto[j] === value) {
                            enumerable = false;
                            configurable = false;
                            writable = false;
                            break;
                        }
                    }
                }
            }
        }
        else {
            needsDrop = true;
        }
    }
}
localReflectDeleteProperty(error, L);
wrappedPrepareStackTrace = wrapped;
currentPreparedStackTrace = wrapped;
}

```

Рисунок 3.20: Редактирование файла

Редактируем следующий исполняемый файл (рис. 3.21).

```

root@vm:/var/www/www-data/app/node_modules/vm2/lib$ cd /var/www/www-data/app/controllers/
user@vm:/var/www/www-data/app/controllers$ ls -la
total 12
drwxr-xr-x 2 www-data www-data 4096 мар 17 2023 .
drwxr-xr-x 5 www-data www-data 4096 сен 10 16:58 ..
-rw-r--r-- 1 www-data www-data 814 мар 17 2023 app-controllers.js

```

Рисунок 3.21: Редактирование файла

```

user@vm:/var/www/www-data/app/controllers$ sudo nano app-controllers.js

```

Рисунок 3.22: Редактирование файла

```

        require: {
            external: true,
            builtin: ["*"]
        }
        allowAsync: false
    });

    result = vmInstance.run(command);
    if (result == undefined) {

```

Рисунок 3.23: Редактирование файла

Завершаем вредоносную сессию (рис. 3.24).

```

user@vm-3 ps -ef | grep overload
www-data 1377 1377 23 1090 460 0 16:58 ? 00:00:00 /bin/bash /var/www/www-data/app/.overload.sh
www-data 1378 1377 23 1090 104 0 16:58 ? 01:20:53 /bin/bash /var/www/www-data/app/.overload.sh
www-data 1379 1377 23 1090 104 0 16:58 ? 01:20:53 /bin/bash /var/www/www-data/app/.overload.sh
www-data 1380 1377 23 1090 104 0 16:58 ? 01:20:53 /bin/bash /var/www/www-data/app/.overload.sh
www-data 1381 1377 23 1090 104 0 16:58 ? 01:20:53 /bin/bash /var/www/www-data/app/.overload.sh
user 6230 5762 0 4467 2344 0 22:15 pts/0 00:00:00 grep --color=auto overload
user@vm-3 sudo kill -9 1377

```

Рисунок 3.24: Завершение вредоносной сессии

Удаляем вредоносный файл (рис. 3.25).

```
user@vm:~$ cd /var/www/www-data/app/
user@vm:/var/www/www-data/app$ ls -la
total 60
drwxr-xr-x  5 www-data www-data 4096 сен 10 16:58 .
drwxr-xr-x  5 www-data www-data 4096 май  3  2023 ..
-rw-r--r--  1 www-data www-data  474 апр 26 2023 app.js
drwxr-xr-x  2 www-data www-data 4096 сен 10 22:33 controllers
-rw-r--r--  1 www-data www-data    9 апр 26 2023 .env
drwxr-xr-x  64 www-data www-data 4096 мая 15 2023 node_modules
-rwxrwxrwx  1 www-data www-data 311 сен 10 16:58 package.json
-rw-r--r--  1 www-data www-data 23534 май 15 2023 package-lock.json
drwxr-xr-x  2 www-data www-data 4096 мая 15 2023 routes
user@vm:/var/www/www-data/app$ rm ^C
user@vm:/var/www/www-data/app$ rm .overload.sh
```

Рисунок 3.25: Удаление вредоносного файла

Уязвимость устранена (рис. 3.26).

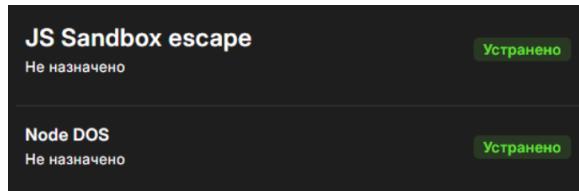


Рисунок 3.26: Устранение уязвимости

4 Выводы

В результате выполнения работы мы успешно устранили все уязвимости и их последствия: Webmarket XML Injection → Webmarket PHP backdoor; TeamCity RCE → TeamCity DB Deleter; JS Sandbox escape → Node DOS.