

Diario di lavoro

Luogo	Canobbio
Data	20.09.2019

Lavori svolti

13h15 – 14h45

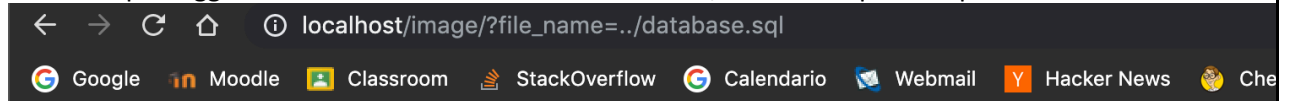
Ho implementato la possibilità di pubblicare degli articoli all'interno del sito web.

Al momento è possibile caricare anche delle immagini. I controlli per contenuto e titolo possono considerarsi sicuri, mentre la chiamata per ricavare le immagini dei post è vulnerabile ad un attacco di tipo Directory Traversal.

La chiamata per la lettura delle immagini è la seguente:

http://localhost/image/?file_name=FILE_NAME

Mettendo al posto di FILE_NAME per esempio il valore "../database.sql" è possibile sfruttare questa chiamata per leggere il file che si trova nella cartella codice/database.sql e stamparne il contenuto.



```
#
# HackerLab
# Filippo finke
#
# Creazione database
#
DROP DATABASE IF EXISTS hackerlab;
CREATE DATABASE hackerlab;
USE hackerlab;

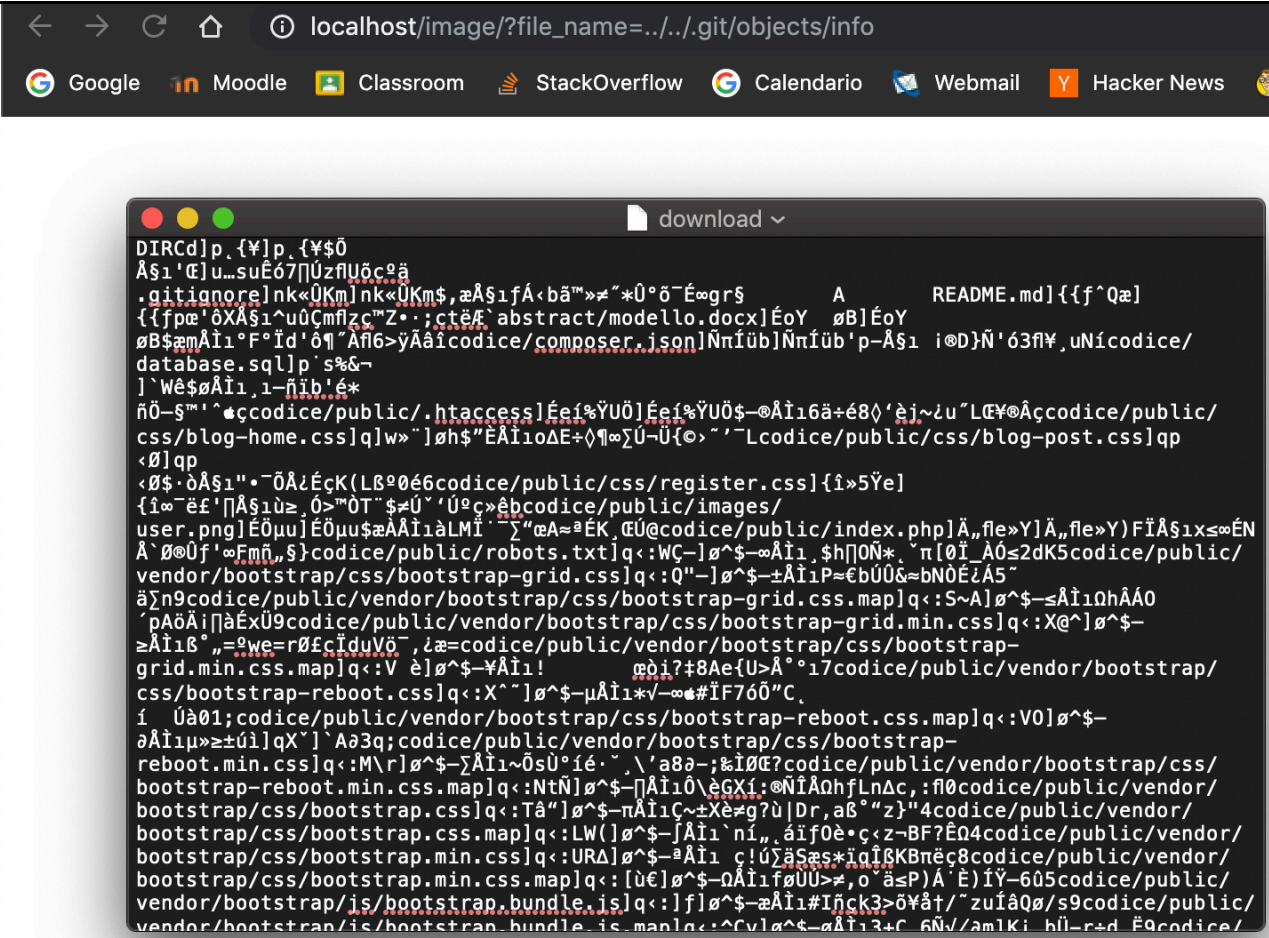
#
# Creazione tabelle
#

# Tabella permessi
CREATE TABLE permissions(
    name VARCHAR(30) PRIMARY KEY
);

# Tabella utenti
CREATE TABLE users(
    id INT AUTO_INCREMENT PRIMARY KEY,
    email VARCHAR(255) NOT NULL,
    password VARCHAR(255) NOT NULL,
    permission VARCHAR(30),
    full_name VARCHAR(30) NOT NULL,
    reset_token VARCHAR(255) DEFAULT NULL,
    created_at TIMESTAMP(1) DEFAULT CURRENT_TIMESTAMP(1)
```

Figura 1 Esempio vulnerabilità

Questa vulnerabilità è pericolosa nonostante non si possa eseguire del codice remoto, questo perché è possibile caricare dei file html contenenti javascript vulnerabile per fare eseguire azioni all'utente involontariamente. Inoltre si può navigare completamente il sistema del server.



localhost/image/?file_name=../../.git/objects/info

Google Moodle Classroom StackOverflow Calendario Webmail Hacker News

download

```

DIRCd]p.{¥}p.{¥$0
Å§i'@]u...suÊ67ΠUzflUöcä
.gitignorelnk«ÜKm]nk«ÜKm$,æÅ§ifÄ«bää»≠*Ü°ö-Éøgrs      A      README.md][f^Qæ]
{fjpe'òXÅ§i^uücmflzc"Z·;ctèÆ'abstract/modello.docx]ÉoY  ØB]ÉoY
ØB$æmÅi1°F°id'ð¶"Åfl6>ÿÅäicodice/composer.json]Nntiüb]Nntiüb'p-Å§i  i@D}Ñ'63fl¥,uNícodice/
database.sql]p's&-
]Wè$øÅi1,1-ñib'É*
ñö-s™'^æccodice/public/.htaccess]Éeí%YUÜ]Éeí%YUÜ$-@Åi16ä+é8ð'èj~zu"LE¥@Åccodice/public/
css/blog-home.css]qlw»"]øh$"ÉÅi1oΔE+ð¶∞ΣÜ-U@>~'~Lcodice/public/css/blog-post.css]qp
<Ø]qp
<Ø$·òÅ§i1"-ÖÄzÉçK(LB°0é6codice/public/css/register.css][i>5Yel
{í∞-ëf'ΠÅ§i1ù≥,Ü>™ÖT"$≠Ü'Ü°ç»èbcodice/public/images/
user.png]ÉÖµu]ÉÖµu$æÅÅi1àLMÍ'~Σ"æA=æEK,ÆÜ@codice/public/index.php]Ä,,fle»Y]Ä,,fle»Y)FíÅ§i1x≤∞ÉN
Å`Ø@Üf'∞Fmñ,§}codice/public/robots.txt]q<:WC-]ø^$-∞Åi1, $hΠ0N*. `n[Øi_Å0≤2dK5codice/public/
vendor/bootstrap/css/bootstrap-grid.css]q<:Q"-]ø^$-±Åi1P≈EbÜÜ&=bN0ÉzÅ5"
äÿn9codice/public/vendor/bootstrap/css/bootstrap-grid.css.map]q<:S~A]ø^$-±Åi1QhÅÄ0
'pAöÅi]àÉxÜ9codice/public/vendor/bootstrap/css/bootstrap-grid.min.css]q<:X@^]ø^$-
±Åi1B°, „=æwe=rØfciduVö", ðæ=codice/public/vendor/bootstrap/css/bootstrap-
grid.min.css.map]q<:V è]ø^$-¥Åi1!      øði?#8Ae{U>Å°°17codice/public/vendor/bootstrap/
css/bootstrap-reboot.css]q<:X`"]ø^$-µÅi1*√-∞#IF76Ö"C,
í  Üà01;codice/public/vendor/bootstrap/css/bootstrap-reboot.css.map]q<:V0]ø^$-
øÅi1µ»±üilqX`] Að3q;codice/public/vendor/bootstrap/css/bootstrap-
reboot.min.css]q<:M\rl]ø^$-ΣÅi1~0sÜ°ié.~, \a8ð-;æIØE?codice/public/vendor/bootstrap/css/
bootstrap-reboot.min.css.map]q<:NtN]ø^$-ΠÅi10\èGXí:®NíÅÑhfLnΔc,:flØcodice/public/vendor/
bootstrap/css/bootstrap.css]q<:Tâ"]ø^$-πÅi1ç~±Xè≠g?ù|Dr, aB°"z}"4codice/public/vendor/
bootstrap/css/bootstrap.css.map]q<:LW(]ø^$-fÅi1'ñi,, áif0è·ç<z~BF?ÉQ4codice/public/vendor/
bootstrap/css/bootstrap.min.css]q<:URΔ]ø^$-±Åi1 ç!úÿäSæ$*iqi§KBñèç8codice/public/vendor/
bootstrap/css/bootstrap.min.css.map]q<:[ùè]ø^$-QÅi1fØUU>≠, o`ä≤P)Á`È)ÍY-6Ü5codice/public/
vendor/bootstrap/js/bootstrap.bundle.js]q<:]f]ø^$-æÅi1#Ifçk3>ö¥â†/~zuíâQØ/s9codice/public/
vendor/bootstrap/js/bootstrap.bundle.js.map]q<:ÇVlø^$-æÅi13+C 6N\am1Ki hül-r+d É9codice/

```

Figura 2 Secondo esempio

In questo secondo esempio si può notare come attraverso questa vulnerabilità si possa ricostruire l'intera struttura del progetto.

15h00 – 15h10

Ho risolto un problema grafico per i dispositivi mobile, ora le immagini hanno una larghezza massima come la larghezza della finestra, questo per prevenire che le foto sforino dallo schermo. Vedi sezione problemi del diario.

15h10 – 16h20

Ho implementato la parte mancante del pannello di amministrazione, ora è possibile eliminare gli articoli.

HackerLab

HomeProfiloPannello di amministrazioneEsci

Gestione articoli

test

Test

Vai all'articolo →

Elimina

Pubblicato il 20.09.2019 da Administrator

Password leaks

Vai all'articolo →

Elimina

Pubblicato il 20.09.2019 da Administrator

← Recenti

Vecchi →

Copyright © HackerLab 2019

Figura 3 Pannello amministrazione

16h20 – 16h30
Stesura diario.

Problemi riscontrati e soluzioni adottate

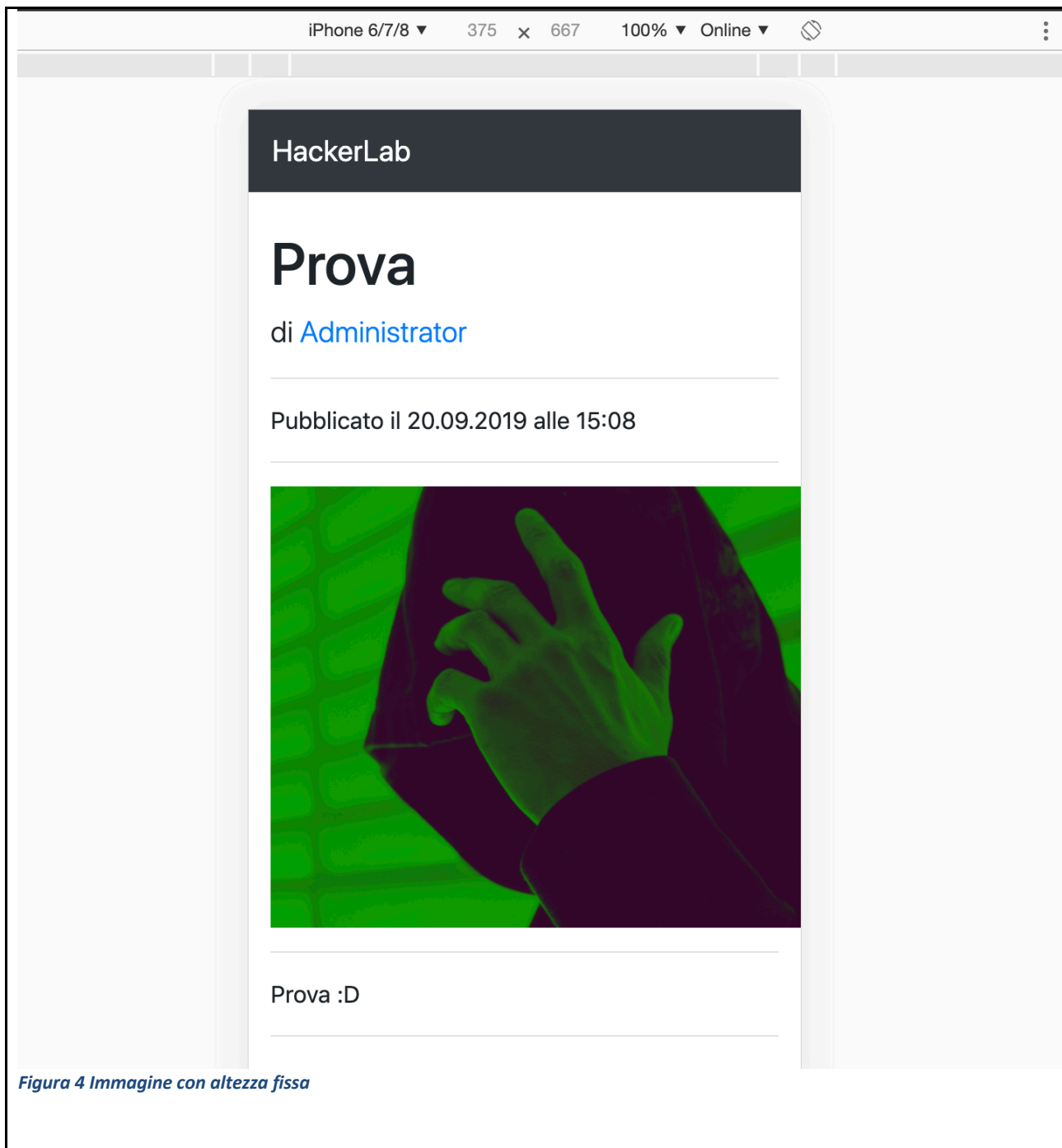
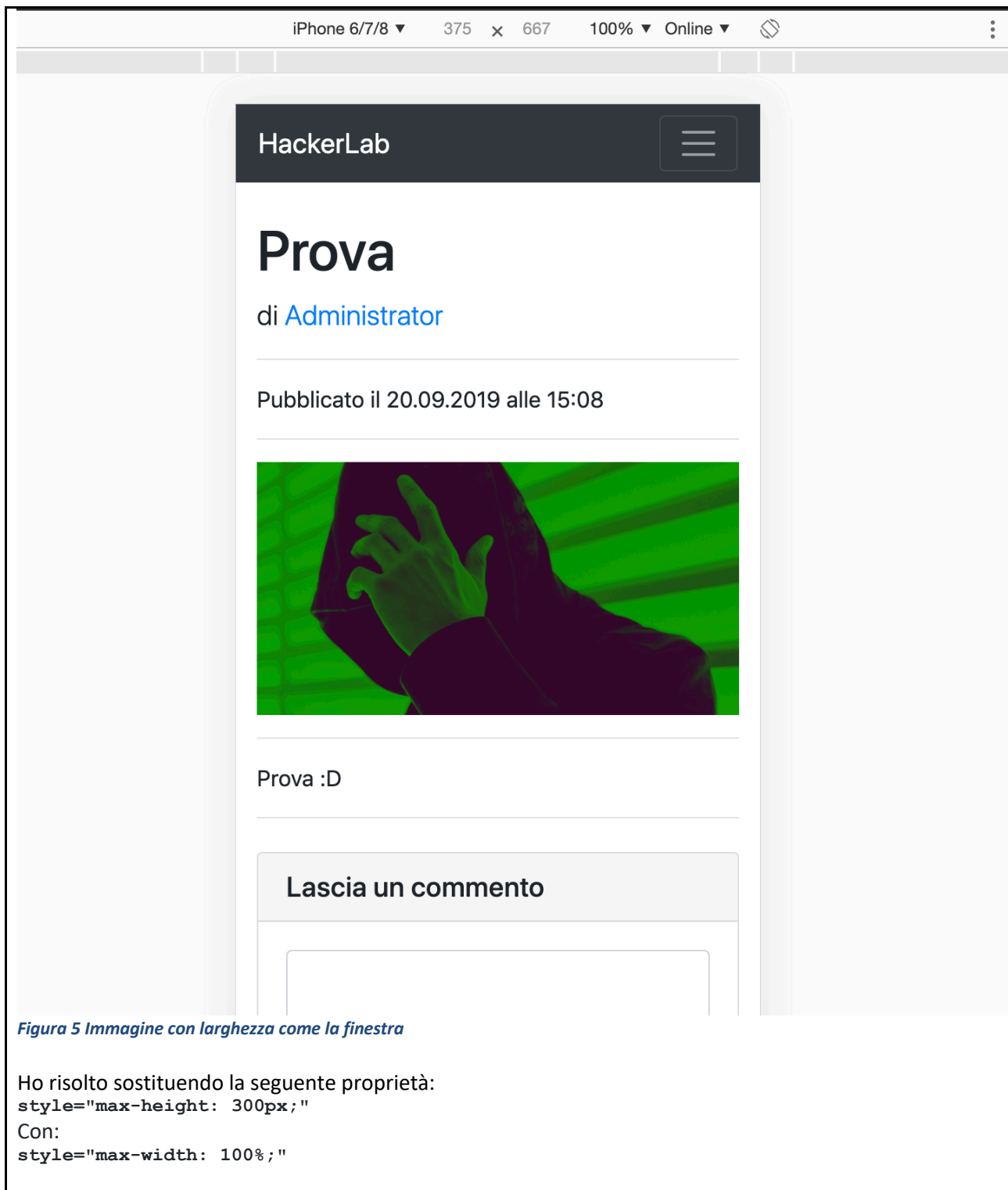


Figura 4 Immagine con altezza fissa



Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianificazione preventiva.

Programma di massima per la prossima giornata di lavoro

Rivedere il codice e valutare le vulnerabilità.