



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ  
Τμήμα Πληροφορικής



Εργασία Μαθήματος **Ασφάλεια Πληροφοριακών Συστημάτων**

Άσκηση <<αριθμός άσκησης>>	<b>7η Άσκηση - Ασφάλεια web εφαρμογών</b>
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουνής Κωνσταντίνος p14086
Ημερομηνία παράδοσης	14-1-2019



1. Στο πρώτο μέρος της άσκησης, καλείστε να χρησιμοποιήσετε το DVWA (Damn Vulnerable Web App) και να εκμεταλλευτείτε τις ευπάθειες μίας συγκεκριμένης τρωτότητας και στα τρία επίπεδα δυσκολίας που προσφέρει η εφαρμογή. Συγκεκριμένα, θα χρειαστεί να επιλέξετε κατά σειρά προτίμησης τρεις τρωτότητες από την παρακάτω λίστα και να στείλετε mail με αυτές στο [ghuntu@gmail.com](mailto:ghuntu@gmail.com). Κάθε ομάδα θα λάβει ως απάντηση μία από τις τρεις τρωτότητες που επέλεξε όπου και θα αναλάβετε για την εργασία σας. Θα τηρηθεί σειρά προτεραιότητας. Αν δηλαδή έχει δοθεί ήδη η πρώτη τρωτότητα στη λίστα σας, θα σας ανατεθεί η δεύτερη κ.ο.κ.

- Command Injection
- SQL Injection
- XSS (Reflected)
- XSS (Stored)
- CSRF
- File Inclusion
- File Upload

#### 7η Άσκηση - Ασφάλεια web εφαρμογών p14086 Kousounnis Kwnstantinos

Είσερχόμενα ✕



Κώστας Κουσουννής

p14086 Command Injection,XSS(REFLECTED),SQL Injection,



George Chatzisofoinou <sophron@latthi.com>

προς εγώ, George ▾

Σας ανατίθεται η ευπάθεια "XSS (Reflected)".

Το DVWA είναι στημένο εδώ:

<http://83.212.174.87/dvwa-f561aaf6ef0bf14d4208bb46a4ccb3ad/DVWA/login.php>

Τα credentials είναι: admin/password

Για το δεύτερο σκέλος της άσκησης η εφαρμογή βρίσκεται εδώ:

<http://83.212.174.87/hackme-f0bf14d42jsu82/>

Καλή τύχη,

Γιώργος

On Mon, Jan 7, 2019 at 4:19 PM Κώστας Κουσουννής <[kwstas654321@gmail.com](mailto:kwstas654321@gmail.com)> wrote:

>

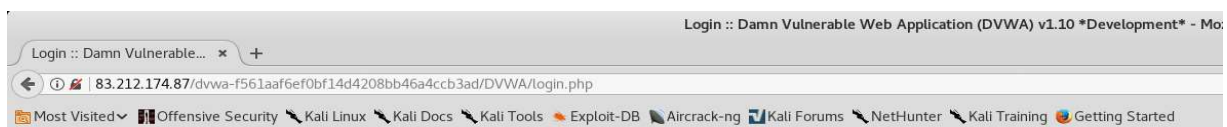
> p14086 Command Injection,XSS(REFLECTED),SQL Injection,

Rectangular Snip



Μου έχει ανατεθεί η ευπάθεια XSS (REFLECTED).

Παίρνω την διεύθυνση και συνδέομαι στο μηχανήμα με admin/password.



Username

Password

 This connection is not secure. Logins entered here could be compromised. [Learn More](#)

You have logged out



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

### More Information

- [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- [https://www.owasp.org/index.php/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Πάω κατευθείαν στο xss (Reflected)

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?    
  
Hello kwstas

### More Information

- [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))



Παω και κάνω καποια παραδείγματα πάνω στο πλαίσιο.

Ρυθμίζω το επίπεδο δυσκολίας σε low στις ρυθμίσεις

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

## DVWA Security

### Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.  
Prior to DVWA v1.9, this level was known as 'high'.

Low

▼

Submit

### PHPIDS

**PHPIDS** v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

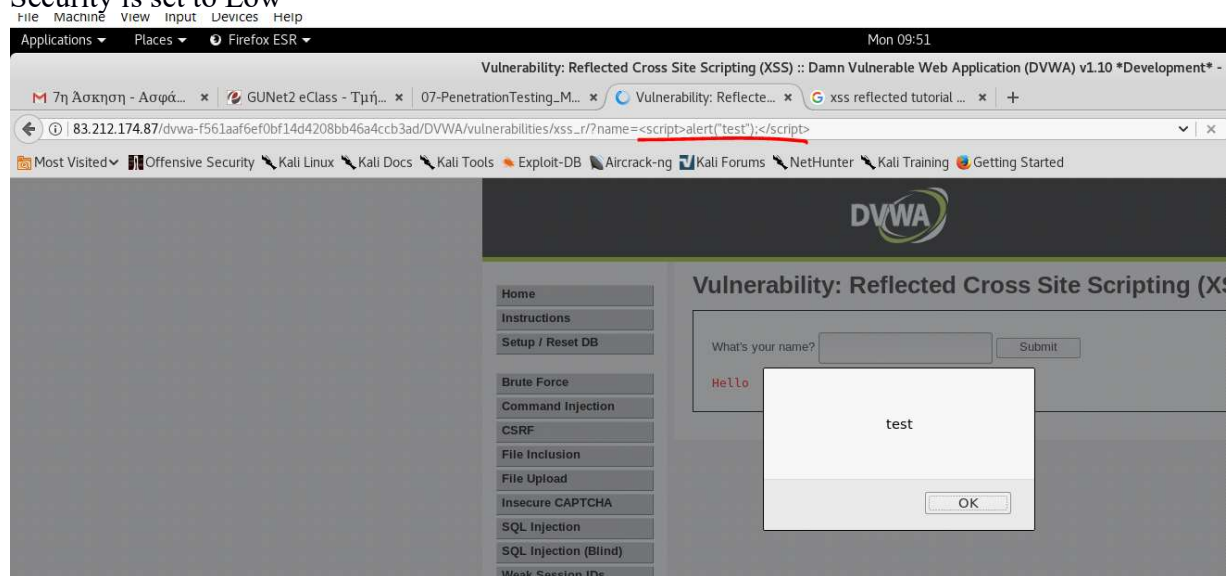
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)



## Security is set to Low



Και πηγαίνω στο xss stored και πληκτολογώ την αντιστοιχη εντολή.

`<script>alert("test1")</script>`

Προσοχή πληκτρολογώ την εντολή πάνω στο αντιστοιχο url μου.

και βλέπουμε οτι αντι το πλαίσιο να μας εμφανίζει hello `<script>alert("test1")</script>` μας εμφανίζει ένα πλαίσιο με προειδοποίηση.



[Kali Tools](#) [Exploit-DB](#) [Aircrack-ng](#) [Kali Forums](#) [NetHunter](#) [Kali Training](#) [Getting Started](#)

[Home](#)  
[Instructions](#)  
[Setup / Reset DB](#)  
  
[Brute Force](#)  
[Command Injection](#)  
[CSRF](#)  
[File Inclusion](#)  
[File Upload](#)  
[Insecure CAPTCHA](#)  
[SQL Injection](#)  
[SQL Injection \(Blind\)](#)  
[Weak Session IDs](#)  
[XSS \(DOM\)](#)  
[XSS \(Reflected\)](#)  
[XSS \(Stored\)](#)  
[CSP Bypass](#)  
[JavaScript](#)  
  
**[DVWA Security](#)**  
[PHP Info](#)  
[About](#)  
  
[Logout](#)

## DVWA Security

### Security Level

Security level is currently: **medium**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.  
Prior to DVWA v1.9, this level was known as 'high'.

Medium

Submit

### PHPIDS

**PHPIDS** v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Ρυθμίζουμε το επίπεδο σε μέτριο.  
Security is set to medium



Kali Linux [running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Applications Places Firefox ESR Mon 10:09

Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.10 \*Development\* - Mozilla Firefox

7η Άσκηση - Ασφα... x GUNet2 eClass - Τμή... x 07-PenetrationTesting\_M... x Vulnerability: Reflecte... x http://83.212.174.87/dvw... x http://83.212.174.87/dvw... x +

83.212.174.87/dvwa-f561aaf6ef0bf14d4208bb46a4ccb3ad/DVWA/vulnerabilities/xss\_r?name=<script>alert("test");</script>

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

**DVWA**

**Vulnerability: Reflected Cross Site Scripting (XSS)**

What's your name?  Submit

Hello alert("test");

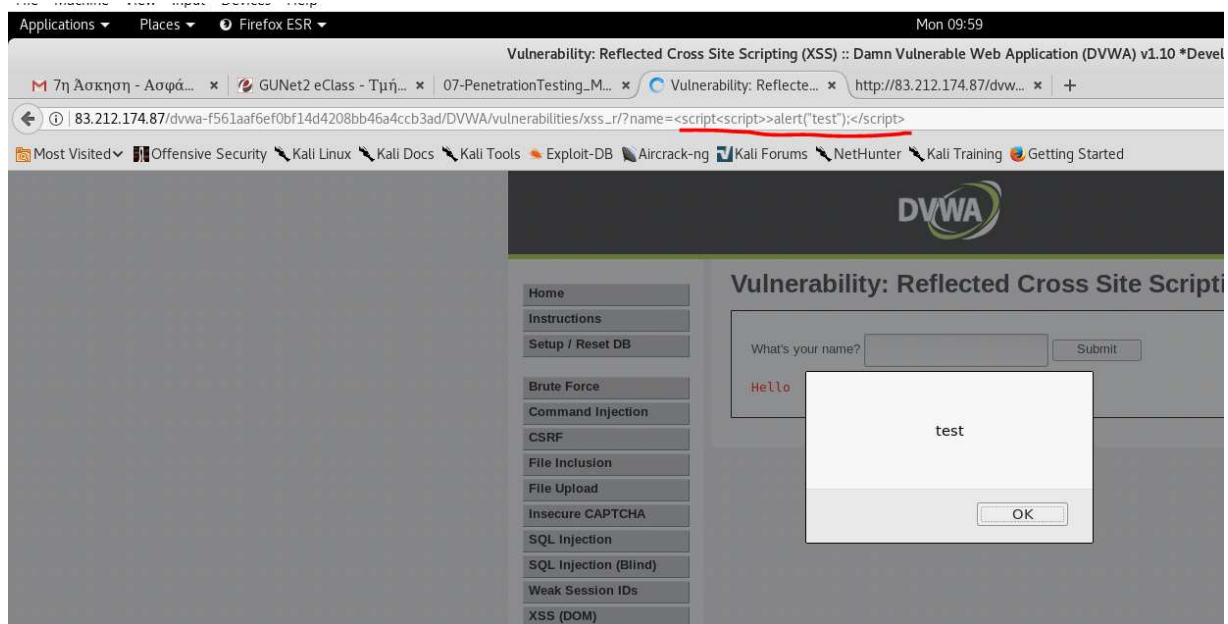
**More Information**

- [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- [https://www.owasp.org/index.php/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Home  
Instructions  
Setup / Reset DB  
Brute Force  
Command Injection  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
SQL Injection  
SQL Injection (Blind)

Ξανα πληκτολογούμε την εντολή αλλά αυτήν την φορά απο ότι φέρεται υπάρχει καποιο επίπεδο ασφαλείας.





Αυτο που χριαστηκε να πληκτρολογήσουμε είναι ενα πάραπάνω `<script>` μεσα στο `<script>` μέσα στην εντολή γιατι απο οτι φένεται κανει εναν έλεγχο στο κείμενο και τα βγάζει.

Οποτε πληκτρολογούμε `<script<script>>alert("test1");</script>`

Βλέπουμε οτι μας εμφανίζεται alert textbox όπως και προηγουμένος.

Στην συνέχεια ρυθμιζουμε τον βαθμό δυσκολίας σε high



Applications ▾ Places ▾ Firefox ESR ▾ Mon 10:02

DVWA Security :: Damn Vulnerable Web Application (DVWA) v1.10 \*Development\* - Mozilla Firefox

7η Άσκηση - Ασφάλ... x GUNet2 eClass - Τμή... x 07-PenetrationTesting\_M... x DVWA Security :: Da... x http://83.212.174.87/dvwa... x +

83.212.174.87/dvwa-f561aaf6ef0bf14d4208bb46a4ccb3ad/DVWA/security.php

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

**DVWA**

**DVWA Security** 📄

**Security Level**

Security level is currently: **high**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

High

**PHPIDS**

**PHPIDS** v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

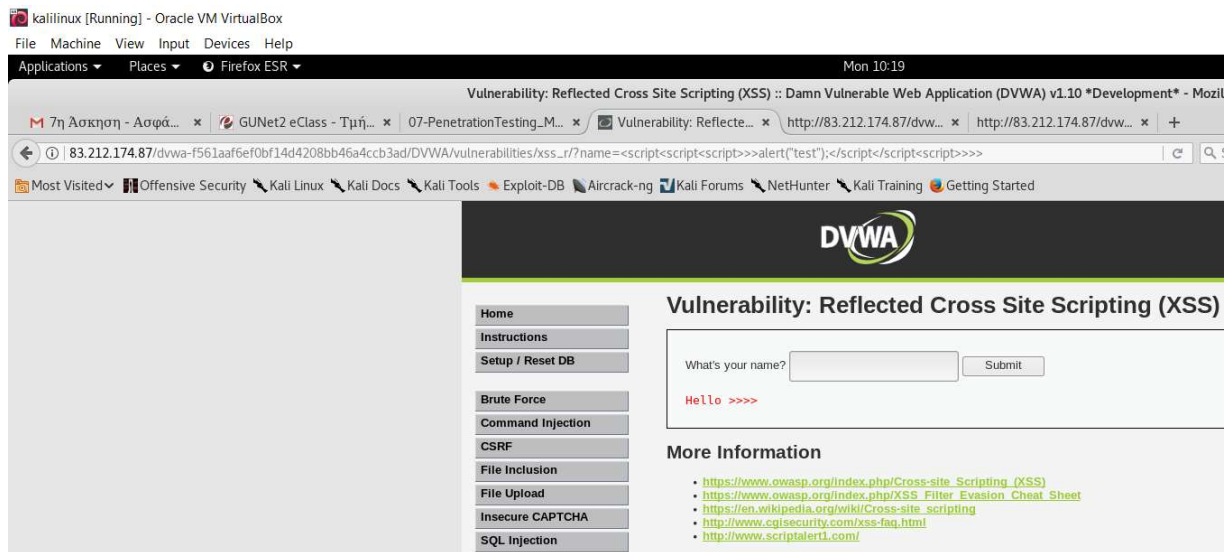
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to high

Security is set to high



Πληκτρολογώ την αντιστοιχη εντολή και βλέπω οτι μου εμφανίζει τα τελευταία γράμματα.  
Που αυτό σημαίνει οτι έχει καποιον έλεγχο που δεν δέχεται `<script></script>`

2. Στο δεύτερο μέρος της άσκησης θα χρειαστεί να εκμεταλευτείτε τις ευπάθειες μιας διαδικτυακής εφαρμογής. Το URL της εφαρμογής θα συμπεριλαμβάνεται στο mail που θα λάβετε ως απάντηση για το πρώτο σκέλος. Συγκεκριμένα, για την επιτυχή εκπλήρωση της άσκησης θα πρέπει:

- Να παραβιάσετε την πρώτη φόρμα που είναι ευάλωτη σε SQL Injection.
- Με την παραβίαση της πρώτης φόρμας, θα χρειαστεί να παραβιάσετε τη δεύτερη φόρμα που είναι ευάλωτη σε Local File Inclusion (LFI).
- Με την παραβίαση και της δεύτερης φόρμας, θα χρειαστεί να παραβιάσετε το guestbook και να κάνετε ένα stored XSS που με τη χρήση Javascript θα εμφανίζει alert box με τους Αριθμούς Μητρώου της ομάδας σας.

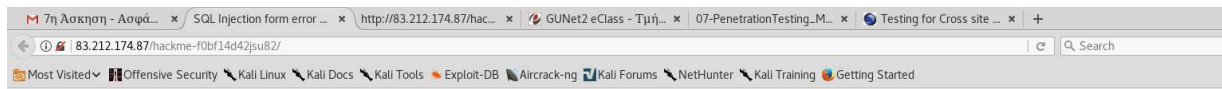
Συνδεομαι στο site που έχουμε.

Τα credentials είναι: admin/password



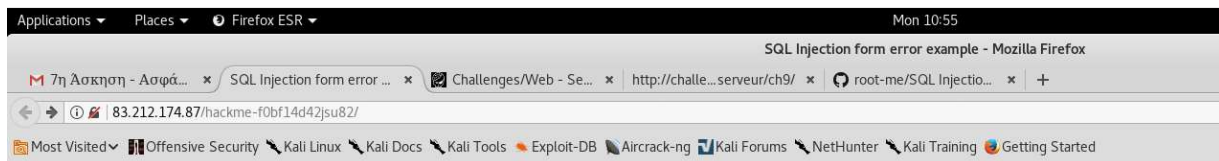
Για το δεύτερο σκέλος της άσκησης η εφαρμογή βρίσκεται εδώ:  
<http://83.212.174.87/hackme-f0bf14d42jsu82/>

Καλή τύχη,



YOU SHALL NOT PASS!

Username:	<input type="text"/>
User ID	<input type="text"/>
Password:	<input type="password"/>
	<input type="password"/>
<input type="submit" value="Submit"/>	

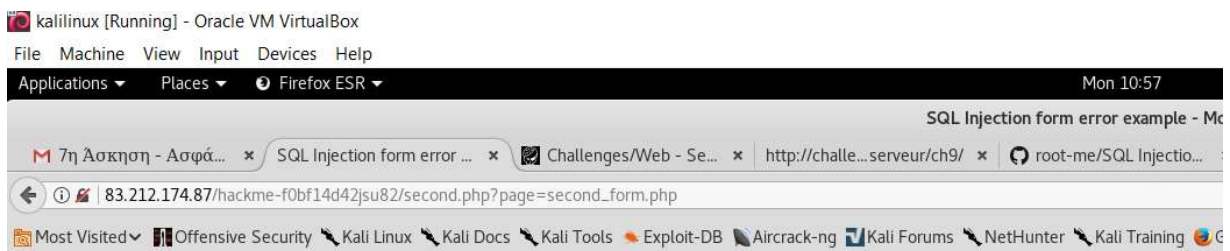


Username:

Password:

This connection is not secure. Logins entered here could be compromised.  
[Learn More](#)

Πληκτρολογούμε τυχαία για Username:admin και Password:Password για να δούμε τι θα συμβεί.

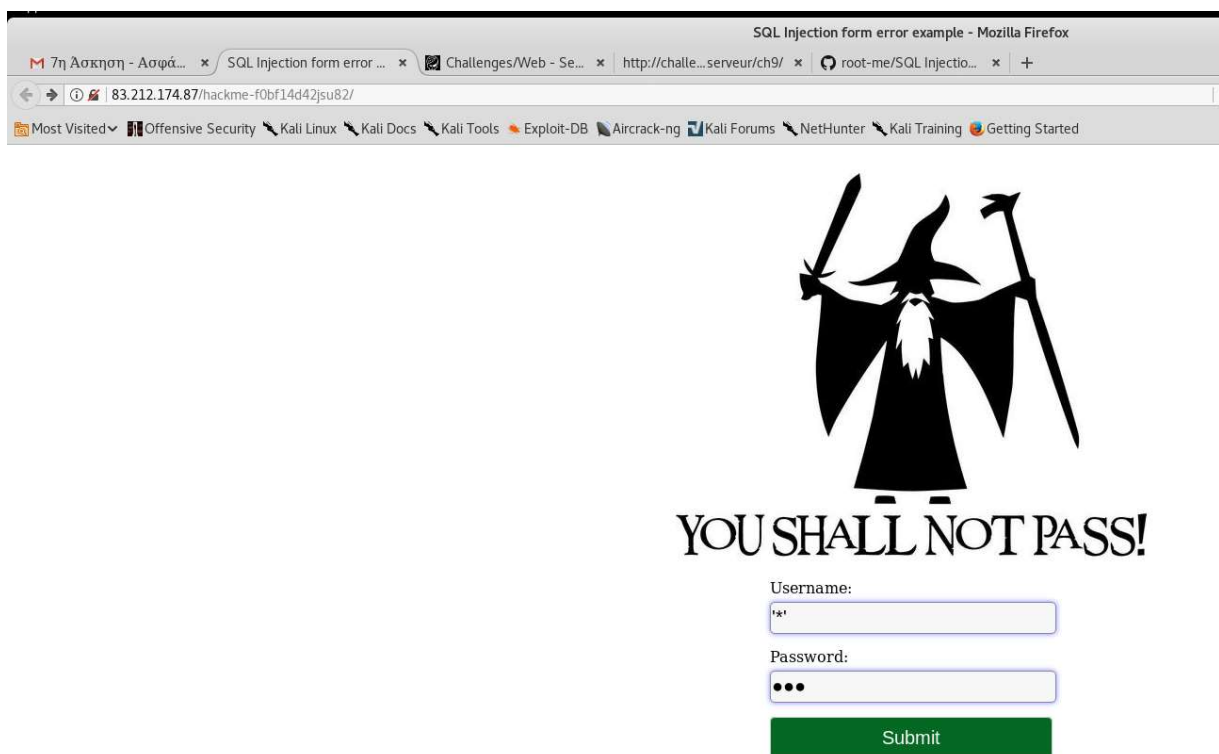


Login failed.

Executed query: `SELECT user_id FROM users WHERE password = 'admin' AND username = 'admin' LIMIT 1;`



Βλέπουμε ότι δέχεται κάποια sql ερωτήματα.



Αρα αυτο που θα κάνουμε είναι να πληκτολογήσουμε sql κώδικα θα βάλουμε για

Username: '\*'

Password: '\*'

Στην ουσία θέλουμε να πάρουμε οποιοδήποτε για να συνδεθούμε.



kali linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Firefox ESR

SQL Injection form error example - Mozilla Firefox

7η Άσκηση - Ασφάλεια / SQL Injection form error ... Challenges/Web - Se... http://challe...seigneur/ch9/ root-me/SQL Injectio... +


83.212.174.87/hackme-f0bf14d42jsu82/second.php?page=second\_form.php

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

Login success.

You are already passed level 1!

Hahaha. The password to pass this level is protected in "password.txt". But you won't get it :)



Οπότε συνδεθήκαμε με επιτυχία και περάσαμε το επίπεδο 1.  
Στην συνέχεια βλέπουμε οτι μας βγάζει ένα πλαίσιο.

7η Άσκηση - Ασφάλεια / SQL Injection form error ... Challenges/Web - Se... http://challe...seigneur/ch9/ root-me/SQL Injectio... +


83.212.174.87/hackme-f0bf14d42jsu82/second.php?page=second\_form.php

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

Login success.

You are already passed level 1!

Hahaha. The password to pass this level is protected in "password.txt". But you won't get it :)

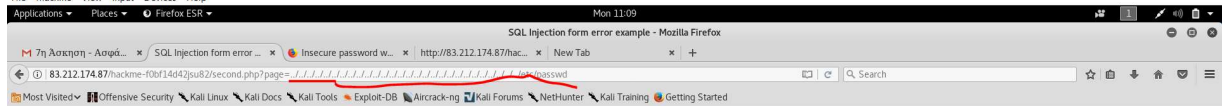


→ Password:  Submit



β. Με την παραβίαση της πρώτης φόρμας, θα χρειαστεί να παραβιάσετε τη δεύτερη φόρμα που είναι ευάλωτη σε Local File Inclusion (LFI).

Πληκτρολογούμε `../../../../../../../../../../../../../../../../etc/passwd` και μας εμφανίζει διαφορά πράγματι το αρχείο `password.txt`



Login failed.

Executed query: SELECT user\_id FROM users WHERE password = " AND username = " LIMIT 1;

You are already passed level 1!

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization:/:run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management:/:run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver:/:run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy:/:run/systemd:/bin/false apt:x:104:65534:/nonexistent:/bin/false messagebus:x:105:109:/var/run/dbus:/bin/false sshd:x:106:65534:/run/sshd:/usr/sbin/nologin admin:x:1000:1000:/home/admin:/bin/bash test:x:1001:1002:/home/test:/bin/bash john:x:1002:1003:/home/john:/bin/bash mysql:x:107:112:MySQL Server:/nonexistent:/bin/false bob:x:1003:1004:/home/bob:/bin/bash jane:x:1004:1005:/home/jane:/bin/bash mary:x:1005:1006:/home/mary:/bin/bash alex:x:1006:1007:/home/alex:/bin/bash tom:x:1007:1008:/home/tom:/bin/bash karl:x:1008:1009:/home/karl:/bin/bash neil:x:1009:1010:/home/neil:/bin/bash tim:x:1010:1011:/home/tim:/bin/bash katie:x:1011:1012:/home/katie:/bin/bash kevin:x:1012:1013:/home/kevin:/bin/bash debra:x:1013:1014:/home/debra:/bin/bash
```