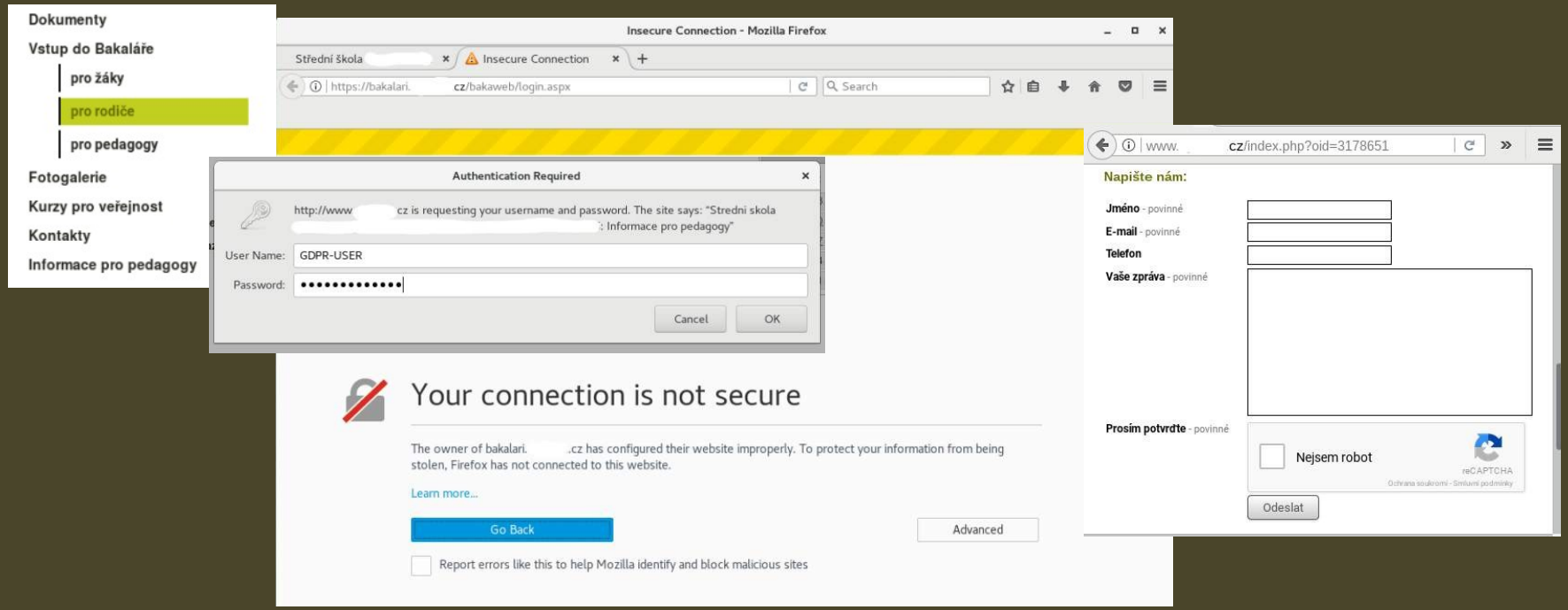
“Penetrační testy webových stránek pro GDPR“

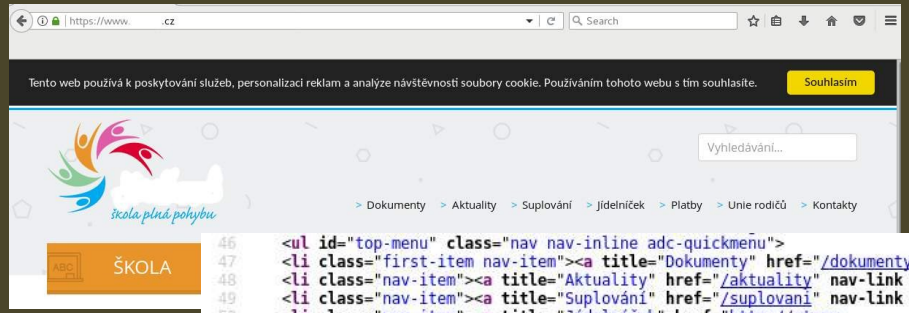
společnosti AARTKOM s.r.o.

a vybrané zákazníky

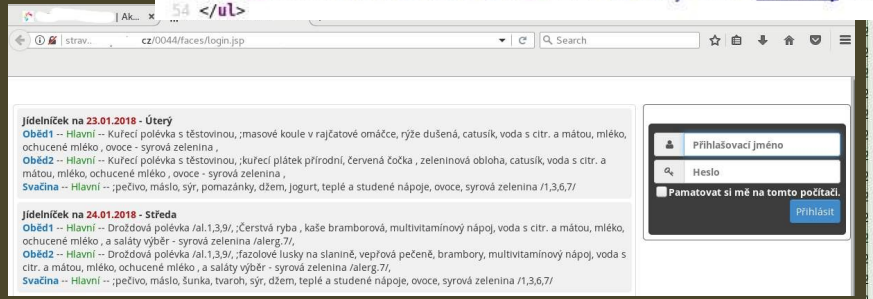
Co Hledáme – Příklad 1

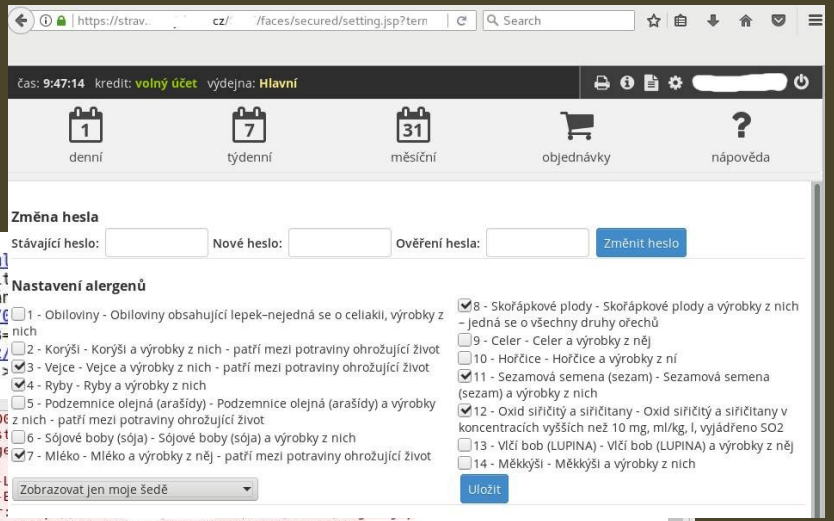


Co Hledáme – Příklad 2




```
<ul id="top-menu" class="nav nav-inline adc-quickmenu">
<li class="first-item nav-item"><a title="Dokumenty" href="/dokumenty-a-formul
<li class="nav-item"><a title="Aktuality" href="/aktuality" nav-link >Aktualit
<li class="nav-item"><a title="Suplování" href="/suplovani" nav-link >Suplovár
<li class="nav-item"><a title="Jídelníček" href="http://strav.          .cz/
<li class="nav-item" id='1' ><a title="Platby" href="/platby" nav-link  class=
<li class="nav-item"><a title="Unie rodičů" href="http://          .webnode.cz/
<li class="last-item nav-item"><a title="Kontakty" href="/kontakty" nav-link >
</ul>
```






```
POST /0
Host: st
User-Age
Accept:
Accept-L
Accept-E
Referer:
Cookie: JSESSIONID=D961584FD79C333DBA4DDFD0058EBF1F
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 171

j_username=GDPR-User&j_password=GDPR-Password&terminal=false&type=web&targetUrl=%
2Ffaces%2Fsecured%2Fmain.jsp%3Fterminal%3Dfalse%26status%3Dtrue%26printer%3D%26keyboard
%3DHTTP/1.1 302 Found
Date: Tue, 23 Jan 2018 08:36:49 GMT
```

Neočekávané Nálezy

Neplánovali jsme to, ale přišlo nám to relevantní

- 25% škol nebylo vlastníkem domény školy
- 50% škol nepoužívá pro email doménu školy*
- 31% škol neuvedly jméno technika školy
- 50% škol neuvedly u technika kontaktní údaje

** jedna škola zrušila objednávku z nedůvěrného emailu „administrátor to nedovolí“*

Šifrování Dat

Koukali jsme jak škola přenáší data uživatelům

- 75% škol automaticky přesměruje uživatele na HTTP*
- 25% škol používá HTTPS *(šifrování na přenos dat)*
  - *z toho 25% použila slabé šifrování a zastaral protokol (SSL3)*
- Další 6% škol umožnilo použít HTTPS *(ale měly to špatně nastavené)*
- 0% škol měly nastaveno HSTS *(tzv. vynucení HTTPS, znemožňuje MITM)*

** Google v nové verzi Chrome 68 (od června) bude označovat veškeré HTTP spojení za „nedůvěryhodné“*

Používání Cookies

Koukaly jsme jak škola nakládá s „tracking cookies“

- 63% škol ukládá „cookies“ do prohlížečů uživatele *(dlohodobé/persistant)*
- 56% škol používá „cookies“ pro vlastní potřebu *(session/persistant)*
- 44% škol umožnilo načtení „cookies“ třetích stran *(z cizích serverů)*
  - *z toho 90% „cookies“ se uložilo do prohlížeče na 6 měsíců a více*
  - *zbývajících 10% „cookies“ se načetlo jen po dobu otevřeného prohlížeče*
- 1 z 10 škol upozornila uživatele o použití „cookies“ *(a žádala souhlas)*

Bezpečnostní Kód

Koukali jsme na bezpečnostní kód v hlavičkách Webu

- 0% škol použily header „*Referrer-Policy*“
- 0% škol použily header „*Cross-Domain JavaScript*“
- 0% škol použily header „*Content-Security-Policy*“
- 0% škol použily header „*X-Content-Type-Options*“
- 6% škol použily header „*XSS-Protection*“
- 6% škol použily header „X-Frame-Options“

Použití Obsahu Třetích Stran

Koukali jsme zda školy přesměrovávají uživatele třetím stranám

- 75% škol směruje uživatele aby načetli obsah z cizích serverů
  - *50% škol odkazuje uživatele k stáhnutí cizího „scriptu“*
  - *38% škol odkazuje uživatele k stáhnutí cizího souboru*
  - *44% škol načítá cizí obsah Webu prostřednictvím „iframe“*
  - *z toho 58% škol používá dvě a více metod popsané výše*
- 38% škol používá Google Analytics k sledování pohybu uživatele

Přístup do Aplikací

Koukali jsme jak školy umožňují uživatelům přístup do aplikací

- 88% škol umožnilo uživateli se heslem připojit do informačního systému
- 75% škol používá přístup do interního systému *(eg. Web administrativa, atd.)*
  - *z toho 75% škol nabídlo přístup uživateli přes otevřené spojení (bez šifrování)*
- 38% škol používá přístup do externího systému *(tzv. aplikace jídelny)*
  - *z toho 33% škol nabídlo přístup uživateli přes otevřené spojení (bez šifrování)*

Další Nalezené Anomality

Na Webových stránek jsme nadále narazili na věci typu:

- schovaný odkaz na Home page na doménu *.com.ua
- časté úložiště fotek na cizích serverech jako součást Webu
  - *které instalovaly až 25 dlouhodobých „cookies“ do prohlížeče*
- z Home page přístup přímo na analytiku o provozu domény

- 13% hostovaných domén používalo aplikační firewall

Podpořte nás a přitom pomozte své škole !

společnosti AARTKOM s.r.o.
Marek Hencl, jednatel

+420 326 210 940
hencl@aartkom.com

Děkujeme za pozornost !