



“Penetrační testy webových stránek pro GDPR“

společnosti AARTKOM s.r.o.

a vybrané zákazníky



- Dokumenty
- Vstup do Bakaláře
 - pro žáky
 - pro rodiče
 - pro pedagogy
- Fotogalerie
- Kurzy pro veřejnost
- Kontakty
- Informace pro pedagogy

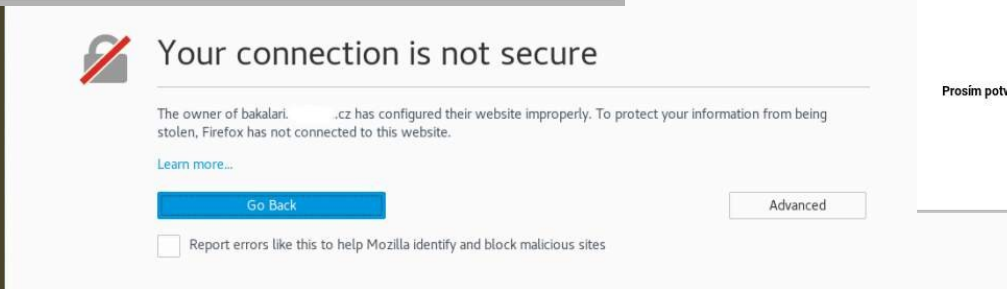


Authentication Required x

http://www.cz is requesting your username and password. The site says: "Stredni skola : Informace pro pedagogy"

User Name:

Password:



www.cz/index.php?oid=3178651

Napište nám:

Jméno - povinné

E-mail - povinné

Telefon

Vaše zpráva - povinné

Prosím potvrďte - povinné Nejsm robot

Ochrana soukromí - Smluvní podmínky

https://www. .cz

Tento web používá k poskytování služeb, personalizaci reklam a analýze návštěvnosti soubory cookie. Používáním tohoto webu s tím souhlasíte. **Souhlasím**

škola plná pohybu

Vyhledávání...

> Dokumenty > Aktuality > Suplování > Jidelníček > Platby > Unie rodičů > Kontakty

```

46 <ul id="top-menu" class="nav nav-inline adc-quickmenu">
47 <li class="first-item nav-item"><a title="Dokumenty" href="/dokumenty-a-formu
48 <li class="nav-item"><a title="Aktuality" href="/aktuality" nav-link >Aktualit
49 <li class="nav-item"><a title="Suplování" href="/suplovani" nav-link >Suplovár
50 <li class="nav-item"><a title="Jidelníček" href="http://strav.
51 <li class="nav-item" id="1" ><a title="Platby" href="/platby" nav-link class=
52 <li class="nav-item"><a title="Unie rodičů" href="http://
53 <li class="last-item nav-item"><a title="Kontakty" href="/kontakty" nav-link >
54 </ul>
    
```

strav. .cz/0044/faces/login.jsp

Jidelníček na 23.01.2018 - Úterý
Oběd1 -- Hlavní -- Kuřečí polévka s těstovinou; masové koule v rajčatové omáčce, rýže dušená, catusik, voda s citr. a mátou, mléko, ochucené mléko, ovoce - syrová zelenina
Oběd2 -- Hlavní -- Kuřečí polévka s těstovinou, kuřečí plátek přírodní, červená čočka, zeleninová obloha, catusik, voda s citr. a mátou, mléko, ochucené mléko, ovoce - syrová zelenina
Svačina -- Hlavní -- pečivo, máslo, sýr, pomazánky, džem, jogurt, teplá a studená nápoje, ovoce, syrová zelenina /1,3,6,7/

Jidelníček na 24.01.2018 - Středa
Oběd1 -- Hlavní -- Droždová polévka /ai.1,3,9/; čerstvá ryba, kaše bramborová, multivitaminový nápoj, voda s citr. a mátou, mléko, ochucené mléko, a saláty výběr - syrová zelenina /alerg.7/;
Oběd2 -- Hlavní -- Droždová polévka /ai.1,3,9/; fazolové lusky na slanině, vepřová pečeně, brambory, multivitaminový nápoj, voda s citr. a mátou, mléko, ochucené mléko, a saláty výběr - syrová zelenina /alerg.7/;
Svačina -- Hlavní -- pečivo, máslo, šunka, tvaroh, sýr, džem, teplá a studená nápoje, ovoce, syrová zelenina /1,3,6,7/

https://strav. .cz/ /faces/secured/setting.jsp?term

čas: 9:47:14 kredit: **volný účet** výdejna: **Hlavní**

dení 7 týdně 31 měsíční

objednávky nápověda

Změna hesla

Stávající heslo: Nové heslo: Ověření hesla:

Nastavení alergenů

1 - Obiloviny - Obiloviny obsahující lepek-nejedná se o celiakii, výrobky z nich
 2 - Korišl - Korišl a výrobky z nich - patří mezi potravinu ohrožující život
 3 - Vejce - Vejce a výrobky z nich - patří mezi potravinu ohrožující život
 4 - Ryby - Ryby a výrobky z nich
 5 - Podzemnice olejná (arašíd) - Podzemnice olejná (arašíd) a výrobky z nich - patří mezi potravinu ohrožující život
 6 - Sójové boby (sója) - Sójové boby (sója) a výrobky z nich
 7 - Mléko - Mléko a výrobky z něj - patří mezi potravinu ohrožující život

8 - Skořápkové plody - Skořápkové plody a výrobky z nich - jedná se o všechny druhy ořechů
 9 - Celer - Celer a výrobky z něj
 10 - Hořčice - Hořčice a výrobky z ní
 11 - Sezamová semena (sezam) - Sezamová semena (sezam) a výrobky z nich
 12 - Oxid siřičitý a siřičitany - Oxid siřičitý a siřičitany v koncentracích vyšších než 10 mg. ml/kg, l, vyjádřeno SO2
 13 - Vlčí bob (LUPINA) - Vlčí bob (LUPINA) a výrobky z něj
 14 - Měkkýši - Měkkýši a výrobky z nich

```

POST /0044/faces/secured/setting.jsp?term HTTP/1.1
Host: strav. .cz
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100801 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://strav. .cz/0044/faces/secured/setting.jsp?term
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%3DHHTTP/1.1 302 Found
Date: Tue, 23 Jan 2018 08:36:49 GMT
    
```

Neplánovali jsme to, ale přišlo nám to relevantní

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

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

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“

Koukaly jsme jak škola nakládá s „tracking cookies“

- 63% škol ukládá „cookies“ do prohlížečů uživatele (*dlohodobé/persistent*)
- 56% škol používá „cookies“ pro vlastní potřebu (*session/persistent*)
- 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*)

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*“

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

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)

Na Webových stránkách 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 !